

Infrastructure Manager / Infrastructure Manager for PRIMEFLEX V3.1.0

User's Guide

CA92344-5875-01
March 2025

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.

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

Product Manuals

Manual Name	Description
Infrastructure Manager / Infrastructure Manager for PRIMEFLEX V3.1.0 First Step Guide	This manual is for those using this product for the first time. This manual summarizes the procedures for the use of this product, the product system, and licensing. In this manual, it is referred to as "First Step Guide."
Infrastructure Manager / Infrastructure Manager for PRIMEFLEX V3.1.0 User's Guide	This manual describes the functions of this product, the installation procedure, and procedures for operation. It allows you to quickly grasp all functions and all operations of this product. In this manual, it is referred to as "User's Guide."
Infrastructure Manager / Infrastructure Manager for PRIMEFLEX V3.1.0 Operating Procedures	This manual describes the installation procedure and usages for the operations of this product. In this manual, it is referred to as "Operating Procedures."
Infrastructure Manager / Infrastructure Manager for PRIMEFLEX V3.1.0 REST API Reference Manual	This manual describes how to use the required APIs and provides samples and parameter information for using user-created applications that integrate with this product. In this manual, it is referred to as "REST API Reference Manual."
Infrastructure Manager / Infrastructure Manager for PRIMEFLEX V3.1.0 Messages	This manual describes the messages that are output when using ISM or ISM for PRIMEFLEX and the actions to take for these messages. In this manual, it is referred to as "ISM Messages."
Infrastructure Manager for PRIMEFLEX V3.1.0 Messages	This manual describes the messages that are output when using ISM for PRIMEFLEX and the actions to take for these messages. In this manual, it is referred to as "ISM for PRIMEFLEX Messages."
Infrastructure Manager / Infrastructure Manager for PRIMEFLEX V3.1.0 Items for Profile Settings (for Profile Management)	This manual describes detailed information for the items set when creating profiles for managed devices. In this manual, it is referred to as "Items for Profile Settings (for Profile Management)."
Infrastructure Manager for PRIMEFLEX V3.1.0 Cluster Creation and Cluster Expansion Parameter List	This manual describes Cluster Definition Parameters that are used for the automatic settings in Cluster Creation and Cluster Expansion when using ISM for PRIMEFLEX. In this manual, it is referred to as "ISM for PRIMEFLEX Parameter List."
Infrastructure Manager / Infrastructure Manager for PRIMEFLEX V3.1.0 Glossary	This document defines the terms that you need to understand in order to use this product. In this manual, it is referred to as "Glossary."

Manual Name	Description
Infrastructure Manager / Infrastructure Manager for PRIMEFLEX V3.1.0 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"> - Infrastructure Manager Plug-in for Microsoft System Center Operations Manager - Infrastructure Manager Plug-in for Microsoft System Center Virtual Machine Manager - Infrastructure Manager Plug-in for VMware vCenter Server Appliance - Infrastructure Manager Plug-in for Microsoft Windows Admin Center <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.

<https://support.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.



Point

Describes the content of an important point.



Note

Describes an item that requires your attention.

Variables: <xxx>

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

Example: <IP address>

Abbreviation

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

Official name	Abbreviation	
Microsoft(R) Windows Server(R) 2022 Datacenter	Windows Server 2022 Datacenter	Windows Server 2022 or Windows
Microsoft(R) Windows Server(R) 2022 Standard	Windows Server 2022 Standard	
Microsoft(R) Windows Server(R) 2022 Essentials	Windows Server 2022 Essentials	
Red Hat Enterprise Linux 9.3 (for Intel64)	RHEL 9.3	Red Hat Enterprise Linux or Linux
SUSE Linux Enterprise Server 15 SP5 (for AMD64 & Intel64)	SUSE 15 SP5(AMD64) SUSE 15 SP5 (Intel64) or SLES 15 SP5 (AMD64) SLES 15 SP5 (Intel64)	SUSE Linux Enterprise Server or Linux
SUSE Linux Enterprise Server 15 (for AMD64 & Intel64)	SUSE 15(AMD64) SUSE 15(Intel64) or SLES 15(AMD64) SLES 15(Intel64)	
VMware ESXi™ 8.0	VMware ESXi 8.0	VMware ESXi
VMware Virtual SAN	vSAN	
Microsoft Storage Spaces Direct	S2D	

In this document, VMware by Broadcom is referred to as VMware.

Terms

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

Using PDF applications (Adobe Reader, etc.)

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

- Saving to a text file
- Copying and pasting text

High Risk Activity

The Customer acknowledges and agrees that the Product is designed, developed and manufactured as contemplated for general use, including without limitation, general office use, personal use, household use, and ordinary industrial use, but is not designed, developed and manufactured as contemplated for use accompanying fatal risks or dangers that, unless extremely high safety is secured, could lead directly to death, personal injury, severe physical damage or other loss (hereinafter "High Safety Required Use"), including without limitation, nuclear reaction control in nuclear facility, aircraft flight control, air traffic control, mass transport control, medical life support system, missile launch control in weapon system. The Customer shall not use the Product without securing the sufficient safety required for the High Safety Required Use. In addition, Fsas Technologies Inc. (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

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

Trademarks

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

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

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

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

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

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

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

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

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

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

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

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

Xen is a trademark of XenSource, Inc.

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

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

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

All other products are owned by their respective companies.

Copyright

Copyright 2017 - 2025 Fsas Technologies Inc.

This manual shall not be reproduced or copied without the permission of Fsas Technologies Inc.

Modification History

Edition	Issue Date	Modification Overview	Section	
01	March 2025	First edition	-	-

Contents

Chapter 1 Overview of Infrastructure Manager (ISM).....	1
1.1 Overview of Main Functions.....	1
1.1.1 Node Management.....	1
1.1.2 Monitoring.....	1
1.1.3 Profile Management.....	1
1.1.4 Log Management.....	2
1.1.5 Firmware Management.....	2
1.1.6 Network Management.....	2
1.1.7 Virtual Resource Management.....	2
1.1.8 Packet Analysis of Virtual Network.....	3
1.1.9 Cluster Management.....	3
1.1.10 Functions of ISM for PRIMEFLEX.....	3
1.2 Configuration.....	5
1.3 System Requirements.....	7
1.3.1 Requirements for Hypervisor to Run ISM-VA (Virtual Machines).....	7
1.3.2 System Requirements for Management Terminals.....	10
1.3.3 Service Requirements for ISM Operations.....	11
1.3.4 Operation Requirements for ISM for PRIMEFLEX.....	13
1.4 Linking with Other Products.....	14
Chapter 2 Functions of ISM.....	16
2.1 User Interface.....	16
2.1.1 GUI.....	16
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.....	26
2.2.1.5 Registration of node OS information.....	26
2.2.1.6 Discovery of nodes.....	27
2.2.1.7 Adding tags to nodes.....	35
2.2.2 Confirmation of Datacenters/Floors/Racks/Nodes.....	36
2.2.3 Editing of Datacenters/Floors/Racks/Nodes.....	39
2.2.4 Deletion of Datacenters/Floors/Racks/Nodes.....	40
2.3 Monitoring.....	41
2.3.1 Monitoring Items and Threshold Values.....	42
2.3.2 Monitoring of Network Statistics Information.....	43
2.3.3 Action Settings.....	44
2.3.4 Alarm Settings.....	46
2.3.5 Graph Display of Monitoring History.....	49
2.3.6 Anomaly Detection.....	49
2.3.6.1 Operation requirements.....	54
2.3.6.2 Starting and stopping Anomaly Detection.....	56
2.3.6.3 Enable or disable the Prediction of CPU Utilization setting.....	57
2.3.6.4 Anomaly Detection statuses.....	57
2.3.6.5 Displaying Anomaly Detection information.....	58
2.3.6.6 Anomaly Detection events.....	61
2.3.6.7 Anomaly Detection solutions.....	61
2.3.6.8 Suppression of Anomaly Detection	62
2.3.7 Link with Web Interface of PRIMERGY.....	64
2.3.7.1 Web interface screen display with iRMC Login.....	64

2.3.7.2 Displaying AVR screen of PRIMERGY	66
2.3.7.3 Displaying Asset Management Info of iRMC (ISM 3.0.0.010 or later)	66
2.4 Profile Management	67
2.4.1 Profile Usage	68
2.4.2 Profiles and Policies	70
2.4.2.1 Creation of policy groups/policies	73
2.4.2.2 Creation of profile groups/profiles	73
2.4.2.3 Assignment of profiles	74
2.4.2.4 Editing and reassigning profiles	74
2.4.2.5 Releasing and deleting profiles	75
2.4.2.6 Exporting and importing profiles	76
2.4.2.7 Editing/deleting profile groups	77
2.4.2.8 Editing/deleting policy groups	77
2.4.2.9 Specifying behavior when assigning profiles	78
2.4.2.10 Verifying profiles	78
2.4.3 RAID Settings	80
2.4.4 OS Installation Settings	81
2.4.5 Virtual IO Settings	83
2.4.6 Pool Management	85
2.4.7 Confirmation of Boot Information	87
2.4.8 iRMC (User) Settings	87
2.5 Log Management	88
2.5.1 Types of Collectable Logs	89
2.5.2 Setting Log Retention Periods	91
2.5.3 Setting Log Collection Targets, Dates, and Times	92
2.5.4 Operations for Log Collection	93
2.5.5 Searching Node Logs	95
2.5.6 Downloading Node Logs	96
2.5.7 Downloading Archived Logs	97
2.5.8 Deleting Node Logs	98
2.5.9 Deleting Archived Logs	98
2.6 Firmware Management	99
2.6.1 Confirmation of Firmware Versions	100
2.6.2 Confirmation of Documentation that is supplied with Firmware Data	100
2.6.3 Firmware/Driver Update	101
2.6.3.1 How to update firmware	101
2.6.3.2 Behavior during firmware updates	104
2.6.3.3 Execution of a script during updates	105
2.6.3.4 Firmware Updates using firmware data	107
2.6.3.5 Offline Firmware Update using ServerView embedded Lifecycle Management	111
2.6.3.5.1 Update with Repository Server or Fujitsu/Fsas Technologies website firmware data	111
2.6.3.5.2 Update with firmware data imported into ISM	113
2.6.3.6 Online Firmware/Driver Update Using eLCM	114
2.6.3.6.1 Behavior during updates	115
2.6.3.6.2 Execution of firmware/driver updates	115
2.6.4 Job Management	115
2.6.5 Firmware Baseline	115
2.6.5.1 Creating Firmware Baseline definitions	116
2.6.5.2 Assigning Firmware Baseline definitions	119
2.6.5.3 Releasing Firmware Baseline definition assignments	119
2.6.5.4 Firmware update using Firmware Baseline definitions	120
2.6.5.5 Editing Firmware Baseline definitions	120
2.6.5.6 Deleting Firmware Baseline definitions	120
2.7 Network Management	121
2.7.1 Display of Network Connection Information	122
2.7.2 Updates of Network Management Information	123
2.7.3 Confirmation of Information on Changes in Network Connections	124

2.7.4 Setting of Reference Information for Changes in Network Connections.....	125
2.7.5 Display of Network Statistics Information.....	125
2.7.6 Confirmation of VLAN and Link Aggregation Settings.....	126
2.7.7 Change of VLAN Settings.....	127
2.7.8 Change of Link Aggregation Settings.....	127
2.7.9 Manual Setting of Network Connection Information.....	128
2.8 Power Capping (Not available from ISM 3.0.0).....	128
2.9 Virtual Resource Management.....	129
2.9.1 Supported Virtual Resources.....	129
2.9.2 GUI for Virtual Resource Management.....	130
2.9.3 Operation of Virtual Resource Management.....	132
2.9.3.1 Monitoring of the utilization status of storage pools.....	132
2.9.3.2 Identification of the errors in storage pools.....	135
2.9.3.3 Updates of virtual resource information.....	138
2.9.3.4 Display of vSAN disk impact on virtual machines.....	139
2.10 Backup/Restore Hardware Settings.....	143
2.10.1 Backup of the File of Backup Hardware Settings.....	143
2.10.2 Export of the File of Backup Hardware Settings.....	143
2.10.3 Addition of Profiles from the File of Backup Hardware Settings.....	144
2.10.4 Addition of Policies from the File of Backup Hardware Settings.....	144
2.10.5 Import of the File of Backup Hardware Settings.....	144
2.10.6 Restoration of the File of Backup Hardware Settings.....	144
2.10.7 Deletion of the File of Backup Hardware Settings.....	144
2.11 Packet Analysis of Virtual Network.....	145
2.11.1 Support Targets.....	145
2.11.2 Confirmation of Analysis VM.....	145
2.11.3 Display Item of Packet Analysis of Virtual Network.....	145
2.11.4 Function difference of Packet Analysis of Virtual Network.....	146
2.11.5 Operation of Packet Analysis of Virtual Network.....	146
2.11.6 Display Items of Bottleneck Analysis for Virtual Networks.....	147
2.12 Sustainability Monitor.....	148
2.12.1 Support Targets.....	148
2.12.2 GUI for Sustainability Monitor.....	149
2.12.3 Settings of CO2 Emission Factor.....	150
2.12.4 Export in CSV Format.....	150
2.13 Functions of ISM for PRIMEFLEX.....	152
2.13.1 Cluster Management.....	152
2.13.1.1 GUI for Cluster Management.....	153
2.13.1.2 Environments supported by Cluster Management.....	161
2.13.1.3 Refreshing cluster information.....	161
2.13.1.4 Management and monitoring of clusters.....	162
2.13.1.5 Resource Planning.....	165
2.13.1.5.1 Execution of Resource Planning.....	165
2.13.1.5.2 Displaying Resource Planning result.....	166
2.13.2 Cluster Creation.....	167
2.13.2.1 Automatic setting item.....	168
2.13.2.2 Link with Profile Management.....	170
2.13.2.3 Cluster Definition Parameters.....	170
2.13.2.4 Task list.....	171
2.13.3 Cluster Expansion.....	171
2.13.3.1 Automatic setting item.....	172
2.13.3.2 Link with Profile Management.....	174
2.13.3.3 Cluster Definition Parameters.....	175
2.13.3.4 Task list.....	175
2.13.4 Rolling Update.....	176
2.13.4.1 Operation in link with Firmware Management.....	177
2.13.4.2 Task list.....	178

2.13.5 Node Disconnection/Reintegration.....	180
2.13.5.1 Task list.....	181
2.13.6 Backup.....	182
2.13.6.1 Task list.....	183
2.13.7 Restore.....	184
2.13.7.1 Task list.....	185
2.13.8 Cluster Stop.....	186
2.13.8.1 Task list.....	189
2.13.9 Batch Collection of vSAN Logs for a VMware vSAN Cluster.....	189
2.13.9.1 Operation of Batch Collection of vSAN Logs.....	190
2.13.9.2 Output file.....	192
2.13.10 Generation Switching.....	193
2.14 Functions of ISM Operating Platform.....	194
2.14.1 User Management.....	194
2.14.2 Repository Management.....	203
2.14.2.1 Storing and deleting firmware data.....	204
2.14.2.2 Storing and deleting OS installation files.....	208
2.14.2.3 Storing and deleting ServerView Suite DVD.....	209
2.14.3 Installation of Emulex OneCommand Manager CLI and QLogic QConvergeConsole CLI.....	210
2.14.4 Task Management.....	210
2.14.5 ISM-VA Management.....	211
2.14.5.1 List of commands in ISM-VA Management.....	212
2.14.6 Management of Cloud Management Software.....	217
2.14.6.1 Registering cloud management software.....	217
2.14.6.2 Retrieving information from cloud management software.....	217
2.14.6.3 Editing cloud management software.....	218
2.14.6.4 Deleting cloud management software.....	218
2.14.6.5 Changing Event Output Restricted Mode for the cloud management software.....	219
2.14.7 Shared Directory Management.....	220
2.14.7.1 Adding shared directories.....	220
2.14.7.2 Editing shared directories.....	221
2.14.7.3 Deleting shared directories.....	221
2.14.7.4 Mounting shared directories.....	222
2.14.7.5 Unmounting shared directories.....	222
2.14.8 Link with ISM.....	222
2.14.8.1 Link display for the status information of other ISM installations.....	222
2.14.8.2 Certificate management for links to other ISM installations.....	224
2.14.9 Linking with Other Software.....	224
2.14.9.1 Preparations in advance for Deep Security link.....	225
2.14.9.2 Procedure to link with Deep Security.....	227
Chapter 3 Installation.....	229
3.1 Workflow for Installing ISM.....	229
3.2 Installation Design for ISM.....	230
3.2.1 Disk Resource Estimation.....	230
3.2.1.1 Estimation of the required disk space for log storage	232
3.2.1.2 Estimation of the required disk space for repositories.....	232
3.2.1.3 Estimation of the required disk space for node management data.....	233
3.2.1.4 Estimation of the required disk space for ISM RAS log.....	234
3.2.1.5 Estimation of required disk space for maintenance data.....	235
3.2.1.6 Estimation of required disk space for ISM Backup/Restore.....	235
3.2.1.7 Estimation of required disk space for CSV export of Sustainability Monitor.....	235
3.2.2 Network Design.....	235
3.2.3 Node Name Design.....	236
3.2.4 User Design.....	236
3.3 Installation of ISM-VA.....	237
3.3.1 Installation on Microsoft Windows Server Hyper-V.....	237

3.3.2 Installation on VMware vSphere Hypervisor.....	239
3.3.3 Installation on KVM.....	243
3.4 Environment Settings for ISM-VA.....	249
3.4.1 First Start of ISM-VA.....	249
3.4.1.1 For ISM-VA running on Microsoft Windows Server Hyper-V (First Time).....	250
3.4.1.2 For ISM-VA running on VMware vSphere Hypervisor (First Time).....	251
3.4.1.3 For ISM-VA running on KVM (First Time).....	251
3.4.2 Initial Setup of ISM-VA.....	253
3.4.2.1 Initial setup using the Basic Setting Menu.....	253
3.4.2.2 Initial setup using the ismadm command.....	254
3.5 Registration of Licenses.....	257
3.5.1 Procedure to Register Licenses from the Console.....	258
3.5.2 Procedure to Register Licenses on the ISM GUI.....	258
3.6 Registration of Users.....	259
3.7 Allocation of Virtual Disks.....	260
3.7.1 Allocation of Virtual Disks to ISM-VA.....	260
3.7.2 Allocation of Virtual Disks to User Groups.....	263
3.8 Pre-Settings for Managing Virtual Resources/Clusters.....	267
3.8.1 Pre-Settings for vSAN.....	267
3.8.1.1 Addition of vSAN alarm definitions.....	267
3.8.1.2 Procedure to enable vSAN Monitoring.....	270
3.8.2 Pre-settings for Statistics Collection Intervals in vCenter Server.....	274
3.8.3 Pre-settings for ISM.....	275
Chapter 4 Basic Operation.....	277
4.1 Start and Stop of ISM.....	277
4.1.1 Start of ISM-VA.....	277
4.1.1.1 For ISM-VA running on Microsoft Windows Server Hyper-V (after installation).....	277
4.1.1.2 For ISM-VA running on VMware vSphere Hypervisor (after installation).....	278
4.1.1.3 For ISM-VA running on KVM (after installation).....	279
4.1.2 Stop of ISM-VA.....	280
4.1.3 Restart of ISM-.....	281
4.1.4 Start and Stop of ISM Service.....	281
4.2 ISM-VA Basic Settings Menu.....	282
4.3 Modification of Destination Port Number.....	284
4.4 Backup and Restoration of ISM.....	284
4.4.1 Backup of ISM.....	284
4.4.2 Restoration of ISM.....	286
4.5 Collection of Maintenance Data.....	286
4.5.1 Required Maintenance Data.....	286
4.5.2 Changing Log Output Settings.....	287
4.5.2.1 Switching the ISM RAS Log mode.....	287
4.5.2.2 Switching the ISM RAS Log level.....	287
4.5.2.3 Specification of core file collection directory.....	288
4.6 Management of Virtual Disks.....	289
4.6.1 Cancellation of Virtual Disk Allocations.....	289
4.6.2 Allocation of Additional Virtual Disks to ISM-VA.....	290
4.6.3 Allocation of Additional Virtual Disks to User Groups.....	290
4.7 Certificate Activation.....	291
4.7.1 Deployment of SSL Certificates.....	291
4.7.2 Display of SSL Certificates.....	292
4.7.3 Export of SSL Certificates.....	292
4.7.4 Creation of Self-signed Certificates.....	292
4.7.5 Download of CA Certificates.....	293
4.8 License Settings.....	293
4.9 Network Settings.....	294
4.10 Alarm Notification Settings.....	296

4.11 ISM-VA Service Control.....	297
4.12 Display of System Information.....	298
4.13 Modification of Host Names.....	298
4.14 Operation of Plug-in.....	298
4.14.1 Application of Plug-in.....	298
4.14.2 Display of Plug-in.....	299
4.14.3 Deletion of Plug-in.....	299
4.15 ISM-VA Internal DHCP Server.....	300
4.15.1 Settings for ISM-VA Internal DHCP Server.....	300
4.15.2 Operation of ISM-VA Internal DHCP Service.....	301
4.15.3 Confirmation of ISM-VA Internal DHCP Server Information.....	302
4.15.4 Switch of DHCP Servers.....	302
4.16 MIB File Settings.....	302
4.17 Application of Patches.....	303
4.18 Upgrade of ISM-VA.....	304
4.18.1 Migrating with Backup File.....	304
4.18.2 Applying Upgrade File.....	304
4.19 ISM-VA Statistics Information Display.....	305
4.19.1 Overview of Statistics Information Display.....	306
4.19.2 Network Statistics Information Display.....	306
4.19.3 Real Time Information Display.....	307
4.19.4 Output Statistics Information File.....	307
4.20 Change of the SSL/TLS Protocol Version.....	308
4.21 Changing Encryption Suite Settings.....	309
4.22 Settings for Links with Other Software.....	309
4.23 File Upload Using the GUI.....	310
4.24 Settings for Enabling/Disabling Verification of Profiles.....	311
4.25 Display of Verify Status.....	311
4.26 Security Settings for the Network Connection.....	311
4.26.1 SSH Security Settings.....	312
4.26.2 Restrict ISM Communication Ports.....	315
4.26.3 Settings for ISM Session Authentication.....	318
4.27 Port Number of Relay Route.....	318
4.27.1 Confirmation of Port Number of Relay Route.....	318
4.27.2 Change of Port Number of Relay Route.....	319
4.28 Creation of Client Certificate for Relay Route.....	319
4.28.1 Creation of Client Certificate.....	319
4.28.2 Download of Client Certificate for Relay Route.....	320
4.28.3 Installation of Client Certificate for Relay Route.....	320
4.28.4 Display of Client Certificate for Relay Route.....	321
Chapter 5 Maintenance of Nodes.....	322
5.1 Maintenance Mode.....	322
5.2 Investigation of Errors.....	323
5.3 Tasks for Replacing Components.....	323
Appendix A Instructions for Manage and Operate Nodes.....	326
A.1 ISM Environmental Settings.....	326
A.1.1 DHCP/PXE Settings in Using Profile Management/Firmware Management.....	326
A.1.2 Display of ETERNUS DX/AF/AB/HB Enclosures.....	327
A.1.3 Notes on MIB File Import.....	328
A.1.4 List of Available Port Numbers in ISM.....	329
A.2 Details of Managed Nodes Settings.....	330
A.2.1 List of Available Port Numbers.....	330
A.2.2 Details of Node Settings.....	336
A.3 Details of Other Settings for Node Operation.....	341
A.3.1 General Standards for Firmware Update Time.....	341
A.3.2 General Standards for Disk Usage in Using Log Management.....	342

A.3.3 Changing a Protocol to Be Used for Firmware Updates.....	344
Appendix B Settings for Monitoring Target OS and Cloud Management Software.....	345
B.1 List of Settings Required per Monitoring Target OS/Cloud Management Software.....	345
B.1.1 Required Settings per Monitoring OS.....	345
B.1.2 Required Settings per Monitoring Cloud Management Software.....	345
B.1.3 Precautions When Setting a Monitoring Target OS and Cloud Management Software.....	346
B.2 Setting Procedure for Monitoring Targets (OS: Windows).....	347
B.2.1 Confirmation on Starting WinRM Service.....	347
B.2.2 Settings for WinRM Service.....	347
B.2.3 Opening the Firewall Port.....	350
B.2.4 Execution Policy Change for Windows PowerShell.....	350
B.2.5 Settings When Using a Domain User Account.....	351
B.3 Setting Procedure for Monitoring Targets (OS: Red Hat Enterprise Linux).....	352
B.3.1 Confirmation on Starting of ssh Service.....	352
B.3.2 Settings for root user to Enable ssh Connections.....	352
B.3.3 Settings When Using a Domain User Account.....	353
B.3.4 Settings When Using a General User Account.....	353
B.3.5 Common Settings for User Accounts.....	354
B.4 Setting Procedure for Monitoring Targets (OS: SUSE Linux Enterprise Server).....	355
B.4.1 Confirmation on Starting of ssh Service.....	355
B.4.2 Opening the Firewall Port.....	355
B.4.3 Settings When Using a Domain User Account.....	358
B.4.4 Settings When Using a General User Account.....	359
B.4.5 Common Settings for User Accounts.....	359
B.5 Setting Procedure for Monitoring Targets (OS: AlmaLinux).....	360
B.6 Setting Procedure for Monitoring Targets (OS: VMware ESXi).....	360
B.6.1 Settings Required When Enabling VMware ESXi Lockdown Mode.....	360
B.6.2 Settings When Using Domain User Account.....	360
B.7 Setting Procedure for Monitoring Targets (OS: Azure Stack HCI).....	361
B.7.1 Confirmation on Starting WinRM Service.....	361
B.7.2 Settings for WinRM Service.....	361
B.7.3 Opening the Firewall Port.....	364
B.7.4 Execution Policy Change for Windows PowerShell.....	364
B.7.5 Settings When Using a Domain User Account.....	364
B.8 Setting Procedure for Monitoring Targets (Cloud Management Software: vCenter Server).....	365
B.8.1 Adding DNS Information to ISM-VA.....	365
B.8.2 Settings When Using Domain User Account.....	365
B.9 Setting Procedure for Monitoring Targets (Cloud Management Software: Microsoft Failover Cluster).....	365
B.9.1 Settings When Using a Domain User Account.....	366
B.10 Setting Procedure for Monitoring Targets (Cloud Management Software: Microsoft System Center).....	366
B.11 Setting Procedure for Monitoring Targets (Cloud Management Software: KVM).....	366
B.11.1 Setting Procedure for KVM Red Hat Enterprise Linux (Using Domain User).....	367
B.11.2 Setting Procedure for KVM SUSE Linux Enterprise Server (Using Domain User).....	372
B.11.3 Settings When Using a General User Account.....	385
B.12 Setting Procedure for Monitoring Targets (Cloud Management Software: OpenStack).....	386
B.12.1 Setting Procedure for a Controller Node.....	386
B.12.2 Settings when using Virtualized Network Analysis.....	391
B.13 Setting Procedure for Monitoring Targets (Cloud Management Software: Microsoft Failover Cluster (Azure Stack HCI)).....	392
B.13.1 Settings When Using a Domain User Account.....	392
Appendix C Uninstallation of ISM-VA.....	394
Appendix D Requirements for Cluster Creation and Cluster Expansion in PRIMEFLEX HS/PRIMEFLEX for VMware vSAN.....	397
D.1 Addable Servers.....	397
D.2 Cluster Creation and Cluster Expansion for ADVN Configurations.....	397
D.3 Network Configuration.....	397
D.4 Hardware Requirements.....	399

D.4.1 Base unit.....	400
D.4.2 CPU.....	400
D.4.3 Memory.....	400
D.4.4 HDD (Capacity).....	400
D.4.5 SSD (Cache/Capacity).....	401
D.4.6 Onboard LAN (Flexible LOM, etc.).....	402
D.4.7 SAS Controller Card.....	402
D.4.8 Option Card (LAN card that is required to be mounted).....	403
D.4.9 Other Options.....	403
D.5 Software Requirements.....	403
D.5.1 Software Version.....	403
D.5.2 Confirmation of Software Version.....	403
D.5.3 Confirmation of SAS Controller Card Firmware Version.....	404
D.6 Sizing of Management VM.....	404
Appendix E Troubleshooting.....	405
Appendix F Scripts for Rolling Update for PRIMEFLEX HS/PRIMEFLEX for VMware vSAN	410

Chapter 1 Overview of Infrastructure Manager (ISM)

This chapter describes an overview of the functions and system requirements for Infrastructure Manager and Infrastructure Manager for PRIMEFLEX.

1.1 Overview of Main Functions

This section describes an overview of the ISM functions.

1.1.1 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. In addition, 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](#)."

1.1.2 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 actions such as executing a user-created script or sending a mail. You can also monitor nodes according to each user's operating procedure.

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

Anomaly Detection

Anomaly Detection is a function that detects behavior that is not normal for hardware and software configuring the managed nodes. This function supports the operation providing solutions for those behaviors.

- Detects behaviors that are not normal such as detection for items that cannot be detected by the threshold settings.
- Provides examples for resolving problems that have been detected.

For details on Anomaly Detection, refer to "[2.3.6 Anomaly Detection](#)."

1.1.3 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](#)."

1.1.4 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](#)."

1.1.5 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 "[2.6.3 Firmware/Driver Update](#)."

1.1.6 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](#)."

1.1.7 Virtual Resource Management

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

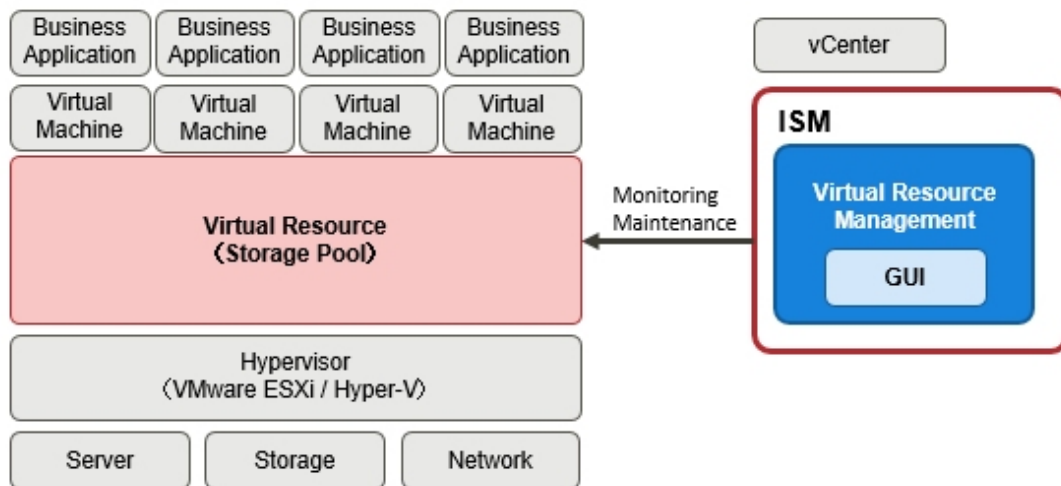
Virtual Resource Management is a function that manages storage pools by displaying status and usage rate of the storage pools.

- 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 1.1 Overview of Virtual Resource Management



1.1.8 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."](#)

1.1.9 Cluster Management

Cluster Management provides the ability to manage a cluster by allowing for monitoring in link with the statuses of the hardware in a cluster and for monitoring storage pools and other virtual storage environments, and this can be used for cluster management. This function is available when the ISM operation mode is "Advanced."

For details on Cluster Management, refer to ["2.13.1 Cluster Management."](#)

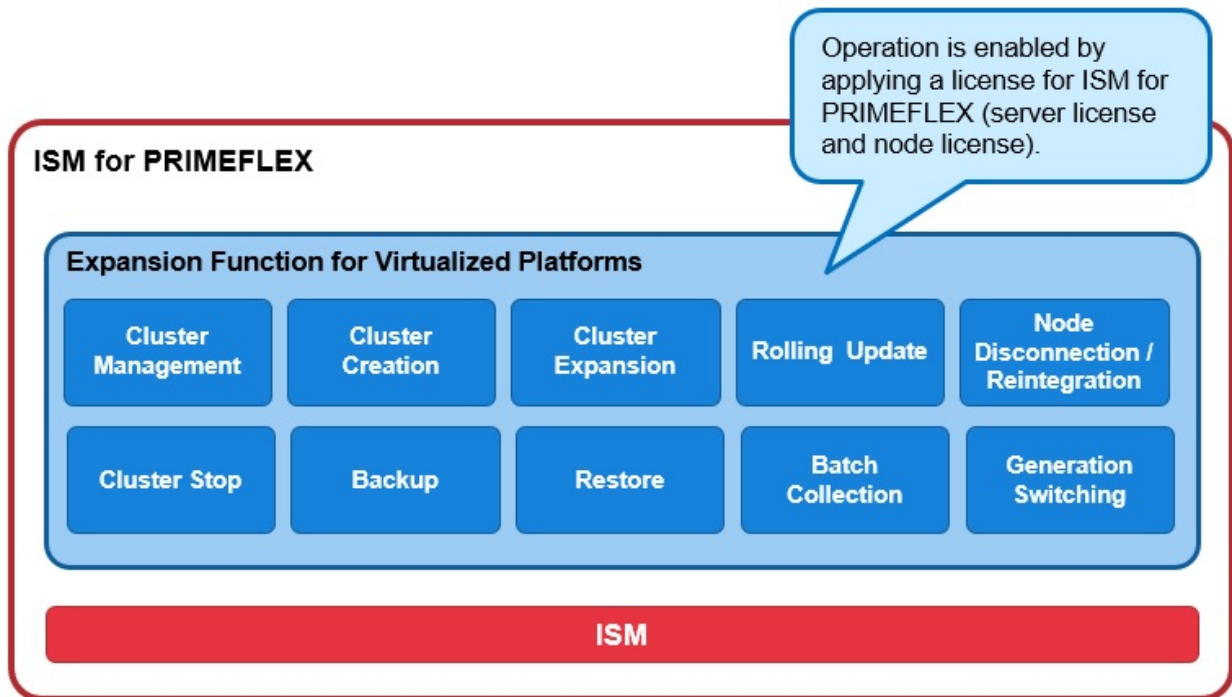
1.1.10 Functions of ISM for PRIMEFLEX

ISM for PRIMEFLEX provides the Virtualized Platform Expansion function in addition to the ISM functions.

ISM for PRIMEFLEX is infrastructure management software that is used in the following environments.

- Integrated System Hyper Converged Infrastructure (HCI)
 - Integrated System PRIMEFLEX HS
 - Integrated System PRIMEFLEX for VMware vSAN

Figure 1.2 Overview of ISM for PRIMEFLEX



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

Note: Y = Supported, N = Not supported

Virtualized Platform Expansion function	Overview of Function	vSAN environment [Note 1]
Cluster Management	Displays the cluster information and various types of information for the related physical resources and virtual resources. Cluster Management can manage resources on a cluster basis.	Y
Cluster Creation	Automates the operation of creating second and later clusters, which differ from the existing one. Cluster Creation can create clusters by using the "Create Cluster" wizard.	Y
Cluster Expansion	Automates the operation of adding servers to expand a cluster when the cluster resources are being depleted. Cluster Expansion can expand clusters by using the "Expand Cluster" wizard.	Y
Rolling Update	Automates the following without stopping the operations for a series of servers configuring the virtualized platform. Execute Rolling Update using the "Rolling Update" wizard.	
	Firmware updates	Y
	Application of ESXi patches	Y
	Application of ESXi offline bundle	Y
	Application of vCSA patches	Y

Virtualized Platform Expansion function	Overview of Function	vSAN environment [Note 1]
	vCSA upgrade	Y
Node Disconnection/Reintegration	Automates maintenance tasks that involve restarting servers in a cluster without stopping operations. Node Disconnection/Reintegration can disconnect or reintegrate servers in a cluster from the "Node Disconnection" screen or "Node Reintegration" screen.	Y
Backup	Automates the backup of the ESXi configuration information files and vCSA VA configuring the virtualized platform. Backup can create a backup of ESXi and vCSA from the "Backup" screen.	Y
Restore	Automates the restoration of a backed up vCSA VA configuring the virtualized platform. Restore can restore vCSA from the "Restore" screen.	Y
Cluster Stop [Note 2]	Automates the operation of stopping a cluster. Cluster Stop can safely stop a cluster from the "Stop Cluster" screen.	Y
Batch Collection of vSAN Logs for a VMware vSAN Cluster	Automates log collection for clusters. Batch Collection of vSAN Logs for a VMware vSAN Cluster can collect logs using the ISM-VA Management "ismadm cluster logcollect" command.	Y
Generation Switching	Updates the current management information of generation of PRIMEFLEX to the successor model of the management information of generation. You can update the PRIMEFLEX generations from the "Switch Generation" screen.	Y

[Note 1]: The following are vSAN environments.

- Integrated System PRIMEFLEX HS
- Integrated System PRIMEFLEX for VMware vSAN

[Note 2]: Cluster Start automates the operation of starting a cluster by executing a Cluster Start command on a management terminal.

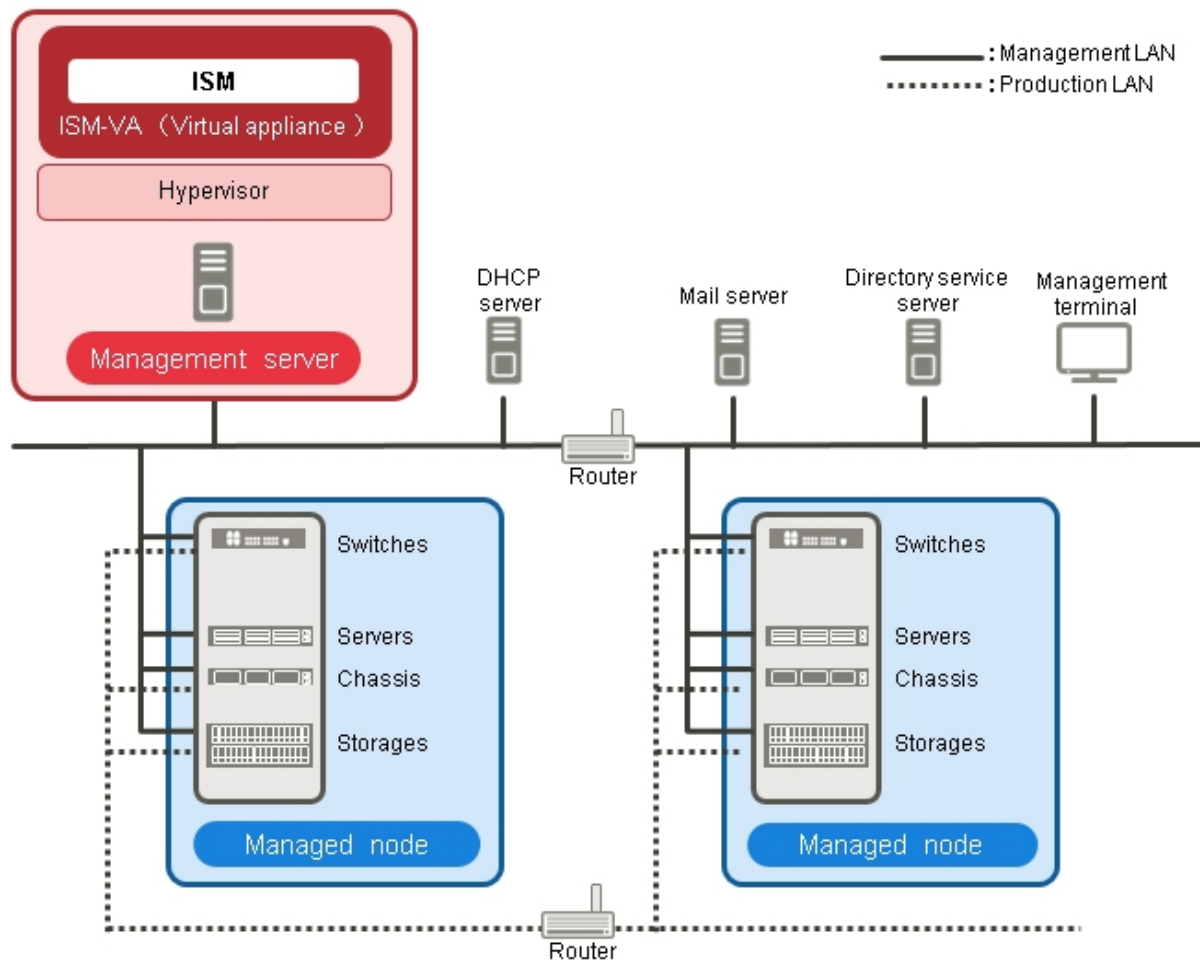
For details on the functions of ISM for PRIMEFLEX, refer to ["2.13 Functions of ISM for PRIMEFLEX."](#)

1.2 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 1.3 Network configuration



Note

- For details on the servers and services shown in "Figure 1.3 Network configuration" that are external to ISM, refer to "1.3.3 Service Requirements for ISM Operations."
- ISM does not support IPv6 networks.

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.

Device and function		Description
Managed nodes	Switches	A node whose status is monitored and controlled by ISM.
	Storage	
	Server (Managed Server)	A node whose status is monitored and controlled by ISM. Connect BMC (iRMC) to the management LAN. To use all the functions in ISM, also connect the onboard LAN and LAN card 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](#)."

1.3 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.

1.3.1 Requirements for Hypervisor to Run ISM-VA (Virtual Machines)

Requirements for a hypervisor to run ISM-VA (virtual machines) are as follows.

Item	Requirements
Applicable model	PRIMEQUEST series PRIMERGY series
Hypervisor	Windows Server Azure Stack HCI OS VMware ESXi Red Hat Enterprise Linux with KVM installed SUSE Linux Enterprise Server with KVM installed Nutanix AHV
Number of CPU cores	2 cores or more
Memory capacity	16 GB or more
Free disk space	70 GB or more
Network	1 Gbps or higher

8 GB of memory capacity and 35 GB of free disk space is required. However, 16 GB or more of memory capacity and 70 GB or more of free disk space are recommended.

The number of CPU cores, memory capacity, and free disk space must be estimated according to the number of nodes being managed and the functions being used.

Applicable models

In addition to the above models in the table, the ISM-VA can be operated on servers running the following hypervisors. However, the servers and hypervisors (Host OS) must be under maintenance contracts with vendors.

Hypervisors

- Supports the following versions of Windows Server, including the Hyper-V role.
 - Windows Server 2012/2012 R2/2016/2019/2022/2025

- Supports the following versions of Azure Stack HCI [Note 1].
 - Azure Stack HCI OS version 20H2/21H2/22H2/23H2
- Supports the following versions of VMware ESXi [Note 2].
 - VMware ESXi 7.0, 7.0b, 7.0 Update 1/2/3
 - VMware ESXi 8.0, 8.0 Update 1/2/3
- Supports the following versions of Red Hat Enterprise Linux with KVM installed.
 - Red Hat Enterprise Linux 7.7
 - Red Hat Enterprise Linux 8.2, 8.4, 8.6, 8.8, 8.9, 8.10
 - Red Hat Enterprise Linux 9.2, 9.3, 9.4, 9.5
- Supports the following versions of SUSE Linux Enterprise Server with KVM installed.
 - SUSE Linux Enterprise Server 12 SP5
 - SUSE Linux Enterprise Server 15, 15 SP 2/3/4/5/6
- Nutanix AHV [Note 2].

[Note 1]: You must connect remotely with the Hyper-V Manager installed on the management terminal.

For more information about Hyper-V Manager, refer to the Microsoft website.

<https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/manage/remotely-manage-hyper-v-hosts>

[Note 2]: For Nutanix Enterprise Cloud on PRIMERGY, it is compatible with VMware ESXi or AHV versions supported by AOS 5.15.5 and later.

Number of CPU cores

Number of nodes	Number of CPU cores
1 to 100	2
101 to 400	4
401 to 1000	8

Using Packet Analysis of Virtual Network

You must add additional CPU cores.

Number of nodes [Note]	Total number of virtual machines	Additional number of CPU cores
1 to 10	100	1 core
11 to 40	400	4 cores
41 to 60	600	8 cores
61 to 100	1000	16 cores

[Note]: Number of nodes that are managed by ISM-VA and registered in Cloud Management Software

To use Packet Analysis and Bottleneck Analysis for one node, you need to add one more core.

Using Anomaly Detection

You must add additional CPU cores. Refer to "[2.3.6.1 Operation requirements](#)" for the number of CPU cores that must be added for Anomaly Detection.

Memory capacity

Additional memory capacity is required depending on the ISM functions used.

Memory Capacity for Manual Discovery of Nodes

There is a limit on the number of the target IP addresses for Manual Discovery depending on the memory capacity. If the number of the target IP addresses for Manual Discovery exceeds the limit, additional memory capacity (200KB per IP address, or 5000 IP addresses per one GB) is required for the number of IP addresses that exceed the limit.

If the memory capacity is 16GB, the number of the target IP addresses for Manual Discovery is 7500 (the total number of IP addresses that can be discovered by multiple users simultaneously).



Note

- When multiple users execute Manual Discovery at the same time, the total memory capacity for the number of IP addresses discovered by each user is required.
- Memory is used temporarily and is released after the user who executed the Manual Discovery logs out.

Using Packet Analysis of Virtual Network

You must add additional memory capacity.

Number of nodes [Note]	Total number of virtual machines	Additional memory capacity
1 to 10	100	1 GB
11 to 40	400	2 GB
41 to 60	600	3 GB
61 to 100	1000	4 GB

[Note]: Number of nodes that are managed by ISM-VA and registered in Cloud Management Software

To use Packet Analysis and Bottleneck Analysis for one node, you need to add 1 GB of memory.

Using Anomaly Detection

You must add additional memory capacity. Refer to "[2.3.6.1 Operation requirements](#)" for the memory capacity that must be added for Anomaly Detection.

Free disk space

The required disk space 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 required disk space, refer to "[3.2.1 Disk Resource Estimation](#)."

Using Packet Analysis of Virtual Network

You must add additional disk capacity.

Number of nodes [Note]	Total number of virtual machines	Additional disk capacity
1 to 10	100	12 GB
11 to 40	400	48 GB
41 to 60	600	72 GB
61 to 100	1000	120 GB

[Note]: Number of nodes that are managed by ISM-VA and registered in Cloud Management Software

To use Packet Analysis and Bottleneck Analysis for one node, you need to add 6 GB of disk capacity.

Using Anomaly Detection

You must add additional memory capacity. Refer to "[2.3.6.1 Operation requirements](#)" for the memory capacity that must be added for Anomaly Detection.

Backing up ISM-VA

You must have at least the same amount of free disk space as ISM-VA.

System updates after applying a patch or upgrade

The following estimated free disk space is required for system updates after applying a patch.

<Number of node logs for all nodes> x 500 bytes

Refer to "9.1 Apply Patches and Upgrade Programs to ISM" in "Operating Procedures" to confirm the number of node logs.

1.3.2 System Requirements for Management Terminals

System requirements for GUI (browser)

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

Item	Description
Device	PC, server, Windows 11 tablet, Android tablet, iPad
Display	<ul style="list-style-type: none">- PC, server, and Windows tablet: 1280 x 768 pixels or more The window size of your browser for displaying the ISM GUI must be at least 1280 x 768 pixels. <ul style="list-style-type: none">- Tablet: built-in display of the devices stated above
Network	100 Mbps or higher
Web browser	<ul style="list-style-type: none">- PC, server, Windows tablet:<ul style="list-style-type: none">- Microsoft Edge 125 or later- Mozilla Firefox 126 or later- Google Chrome 125 or later- Android tablet: Google Chrome 90 or later- iPad: Safari 13 or later To ensure stable operation, use the latest version of each browser.
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 tablet	Android tablet	iPad
Microsoft Edge	Y [Note 3]	Y [Note 1] [Note 3]	N	N
Mozilla Firefox	Y [Note 3]	Y [Note 1] [Note 3]	N	N
Google Chrome	Y [Note 3]	Y [Note 3]	Y [Note 3]	N
Safari	N	N	N	Y [Note 2] [Note 3]

[Note 1]: On the "3d View" screen, you cannot rotate, move in parallel, or zoom in and out using touch operations.

[Note 2]: The following restrictions apply:

- Files cannot be saved. Therefore, you cannot export monitoring data to CSV format, download the node logs or archived logs, or export profiles.
- ISM Restore, patch application, and ISM-VA upgrade are not supported.

[Note 3]: 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 When backing up ISM-VA, you must have at least the same amount of free disk space as ISM-VA.
Network	100 Mbps or higher
Required software	FTP client software
Related software	SSH client software

System requirements for mobile device for Multi-Factor Authentication



The system requirements for the mobile device for Multi-Factor Authentication are as follows.

- Install a multi-factor authentication client application on any mobile device

ISM Multi-Factor Authentication comply with RFC 6238. For the multi-factor authentication client applications, Google Authenticator (iOS, Android) is recommended.

1.3.3 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>A mail server is required when sending notification mail for errors and changes in the statuses of managed nodes.</p> <p>Set up with [Events] - [Alarms] - [SMTP Server].</p> <p>ISM supports the STARTTLS encryption method (based on the SMTP server configuration).</p> <p>ISM supports LOGIN/PLAIN/CRAM-MD5 authentication methods.</p> <p> Note</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">- For User Management in ISM <p>You can use the following two directory services.</p> <ul style="list-style-type: none">- OpenLDAP- Microsoft Active Directory <p>Register the configured directory server in [Settings] - [Users] - [LDAP Server Setting].</p> <p> Note</p> <p>.....</p> <ul style="list-style-type: none">- You can register two directory servers for Link with Users, one primary and one secondary.- You can register up to five domains for Link with groups of Microsoft Active Directory or OpenLDAP.

Item	Description
	<ul style="list-style-type: none"> - When a managed node uses a directory service, ISM does not link with the directory service which a managed node belongs to. Individually set the account to be able to access the managed node.
DHCP server	<p>A DHCP server is required in the following cases.</p> <ul style="list-style-type: none"> - When OS installation is executed using Profile Management - When Offline Update of Firmware Management is used <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> <p> Point</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 "4.15 ISM-VA Internal DHCP Server."</p>
DNS server	<p>A DNS server is required for the following use cases.</p> <ul style="list-style-type: none"> - Accessing ISM by hostname - Using an FQDN for a variety of sever settings of ISM, such as integration with an LDAP server <p>For the procedure to set up a DNS server, refer to "Add DNS server" in "4.9 Network Settings."</p> <p> Point</p> <ul style="list-style-type: none"> - 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 the hostname manually, refer to "4.13 Modification of Host Names." - Settings for ISM servers such as LDAP integration with IP addresses if you are not using a DNS server.
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 "3.4.2 Initial Setup of ISM-VA."</p>
Proxy server	<p>A proxy server is required when accessing ISM from a management client via a proxy server.</p> <p> Note</p> <p>Monitored nodes and ISM cannot be connected via a proxy server.</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 "4.9 Network Settings."</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](#)."

Requirements for using Cluster Management

Refer to the following:

- Requirements for the Cluster Management Environment: "[2.13.1.2 Environments supported by Cluster Management](#)"
- Pre-setting requirements: "[3.8 Pre-Settings for Managing Virtual Resources/Clusters](#)"

1.3.4 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 Server License V3
 - Infrastructure Manager Advanced Edition for PRIMEFLEX Node License V3

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: "[2.13.1.2 Environments supported by Cluster Management](#)"
- Pre-setting requirements: "[3.8 Pre-Settings for Managing Virtual Resources/Clusters](#)"

Requirements for using Cluster Creation or Cluster Expansion

Refer to the following:

- Requirements for PRIMEFLEX HS/PRIMEFLEX for VMware vSAN: "6.8.1 Operation Requirements" in "Operating Procedures"

For successor cluster expansion, refer to "[Appendix D Requirements for Cluster Creation and Cluster Expansion in PRIMEFLEX HS/PRIMEFLEX for VMware vSAN](#)."

Requirements for using Rolling Update

Refer to the following:

- Requirements for Rolling Update: "6.7.1 Operation Requirements" in "Operating Procedures"

Requirements for using Node Disconnection/Reintegration

Refer to the following:

- Requirements for Node Disconnection/Reintegration: "6.11.1 Operation Requirements" in "Operating Procedures"

Requirements for using Backup

Refer to the following:

- Requirements for Backup: "6.12.1 Operation Requirements" in "Operating Procedures"

Requirements for using Restore

Refer to the following:

- Requirements for Restore: "6.13.1 Operation Requirements" in "Operating Procedures"

Requirements for using Cluster Stop

Refer to the following:

- Requirements for Cluster Stop: "6.14.1 Operation Requirements" in "Operating Procedures"

Requirements to use Generation Switching

Refer to the following:

- Requirements for Generation Switching: "6.15.1 Operation Requirements" in "Operating Procedures"

Products supported by ISM for PRIMEFLEX V3.1.0

For the latest information on products supported by ISM for PRIMEFLEX V3.1.0, refer to "Support Matrix."

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

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

Select [DOWNLOADS] and select the target operating system.

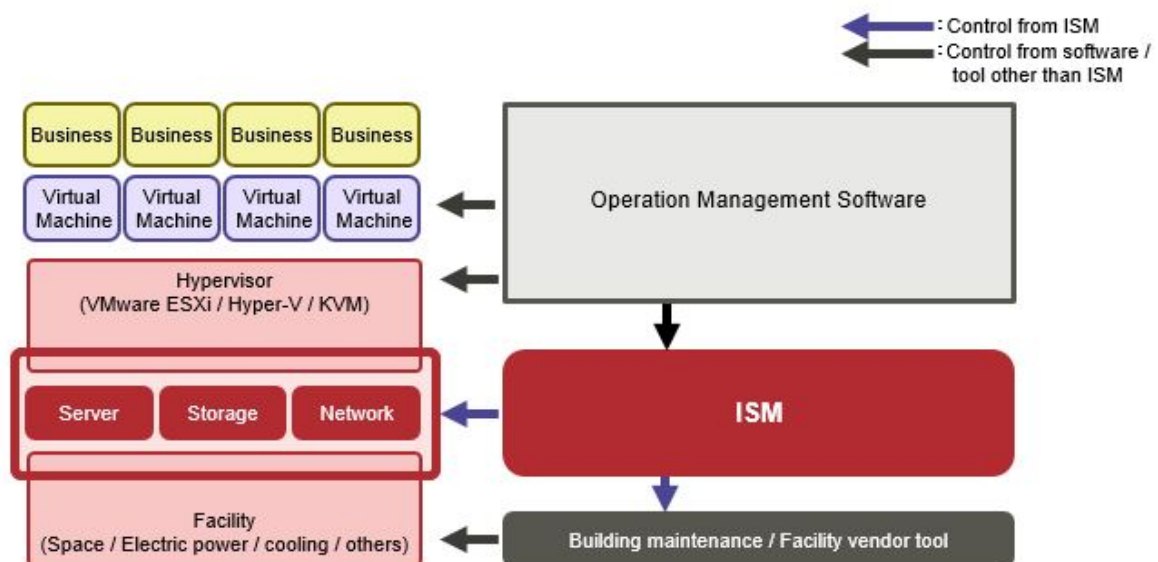
The reference procedures are subject to change without notice.

1.4 Linking with Other Products

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

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

Figure 1.4 Linking with other products



ISM can be linked with the following products.

- Cloud management software
- "Trend Micro Deep Security," Integrated server security product

Linking from cloud management software

Linking the following products to ISM enables seamless operation management of physical resources and virtual resources.

- Microsoft System Center Operations Manager
- Microsoft System Center Virtual Machine Manager
- VMware vCenter Server Appliance
- Microsoft Windows Admin Center

The following plug-in software to link with the above products are provided in ISM.

- Infrastructure Manager Plug-in for Microsoft System Center Operations Manager
- Infrastructure Manager Plug-in for Microsoft System Center Virtual Machine Manager
- Infrastructure Manager Plug-in for VMware vCenter Server Appliance
- Infrastructure Manager Plug-in for Microsoft Windows Admin Center

For details on plug-in software, refer to "ISM Plug-in/MP Setup Guide."

Linking with Trend Micro Deep Security

Linking with Trend Micro Deep Security enables you to display the security monitoring information of a server on the ISM GUI and you can integrate server monitoring with ISM.

For details on linking with Trend Micro Deep Security, refer to "[2.14.9 Linking with Other Software](#)."

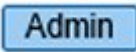





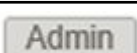



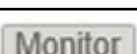
Chapter 2 Functions of ISM

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 "2.14.1 User Management."

The icons shown in the table below indicate which combinations of user groups and user roles can execute operations.

User group to which a user belongs	User role held by the user	Can execute	Cannot execute
Administrator group	Administrator role		
	Operator role		
	Monitor role		
Group other than Administrator group	Administrator role		
	Operator role		
	Monitor role		

The attributes of users who can execute operations are as follows.

Example:



- In the example above, users with the following combinations of groups and roles 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 the Administrator group and have an Administrator role or Operator role
- Users with a Monitor role cannot execute the respective functions, as indicated by the gray icons.

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 (ISM GUI) that can be operated with web browsers.

Required settings for each browser

In your browser, you must enable Cookies, JavaScript, and DOM storage.

Configure the required settings for the browser you are using.

For Mozilla Firefox

The following settings are required. The procedure for version 126 is shown as an example.

1. Open Firefox. From the menu, select [Settings].
2. Select [Privacy & Security].
3. Under [Browser Privacy], select [Standard] or [Custom] for [Enhanced Tracking Protection].
4. If you selected [Custom], clear the [Cookies] checkbox, or select [Cross-site tracking cookies] or [Cross-site tracking cookies, and isolate other cross-site cookies] .
5. Under [Security], select [View Certificates] for [Certificates].
6. On the [Servers] tab, select [Add Exception].
7. Enter "https://<IP address of ISM server> or <FQDN name of ISM server>:25566/" in [Location], and then select [Get Certificate].
8. Confirm that the [Permanently store this exception] checkbox is selected, and then select [Confirm Security Exception].
9. Enter [about:config] in the Firefox address bar.
10. Set [javascript.enabled] to [true].
11. Set [dom.storage.enabled] to [true].

For Google Chrome

The following settings are required. The procedure for version 125 is shown as an example.

1. Open Google Chrome. From the menu, select [Settings].
2. Select [Privacy and security].
3. Select [Site Settings] under [Privacy and security].
4. Select [Third-party cookies] under [Content].
5. Select [Allow third-party cookies] or [Block third-party cookies in Incognito mode].
6. Select the arrow on the left side of [Third-party cookies] displayed on the upper side of the screen to go back to [Site Settings].
7. Select [JavaScript] under [Content].
8. Select [Sites can use Javascript].



Point

.....

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.
-

For Microsoft Edge

The following settings are required. The procedure for version 125 is shown as an example.

1. Open Microsoft Edge. From the menu, select [Settings].

2. Select [Cookies and site permissions].
3. Select [Manage and delete cookies and site data] under [Cookies and data stored].
4. Enable [Allow sites to save and read cookie data].
5. Disable [Block third-party cookies].
6. Select the arrow on the left side of [Cookies and data stored] displayed on the upper side of the screen to go back to [Cookies and data stored].
7. Select [JavaScript] under [Site permissions].
8. Enable [Allowed].

Start the ISM GUI

The procedure to start 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/`

Login screen is displayed.

2. 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 select the [Above contents are correct.] checkbox.
4. Select the [Agree] button.

The procedure to start the ISM GUI as a user with Multi-Factor Authentication enabled is as follows.

1. Start the browser and enter the following URL.

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

Login screen is displayed.

2. 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 user with Multi-Factor Authentication enabled is logging in for the first time, QR Code and Emergency Codes are displayed.

Emergency Codes are used when the mobile device displaying the authentication code cannot be used due to malfunction or loss. The code is displayed only once, so be sure to keep it safe.

3. Scan the displayed QR code with the multi-factor authentication client application that installed on your mobile device (on first login only).
Authentication code is displayed in the multi-factor authentication client application.
4. Enter the authorization code in the ISM GUI, and then select the [Login] 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

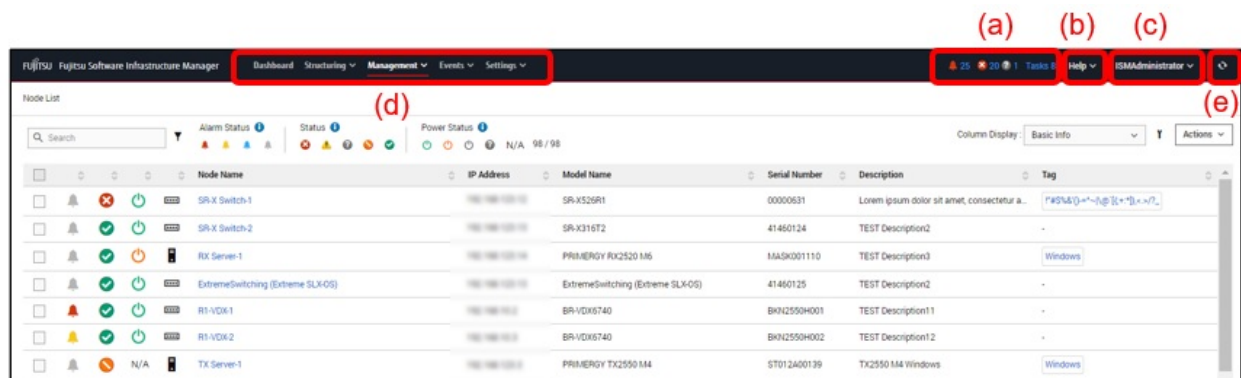


Note

- Do not save the ISM user name and password in the web browser. If you saved them, delete the ISM user name and password.
- If the mobile device that displays the authentication code cannot be used due to malfunction or loss, and the Emergency Codes are unknown, disable Multi-Factor Authentication for the user. When the new device is ready, re-enable Multi-Factor Authentication. For details, refer to "[In case of Multi-Factor Authentication when mobile device malfunction or loss.](#)"
- Emergency Codes you used cannot be reused.

Layout of the ISM GUI screen

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



(a) Alarm status, status, and 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 icon 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 icon 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] to change the settings for the displayed Language, Date Format, and Time Zone on the GUI.

Select [Change password] to change the password for a user that is logged in.

(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 must select the [Refresh] button to update the screen.

If the following screens are set, they will refresh 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 connect.

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

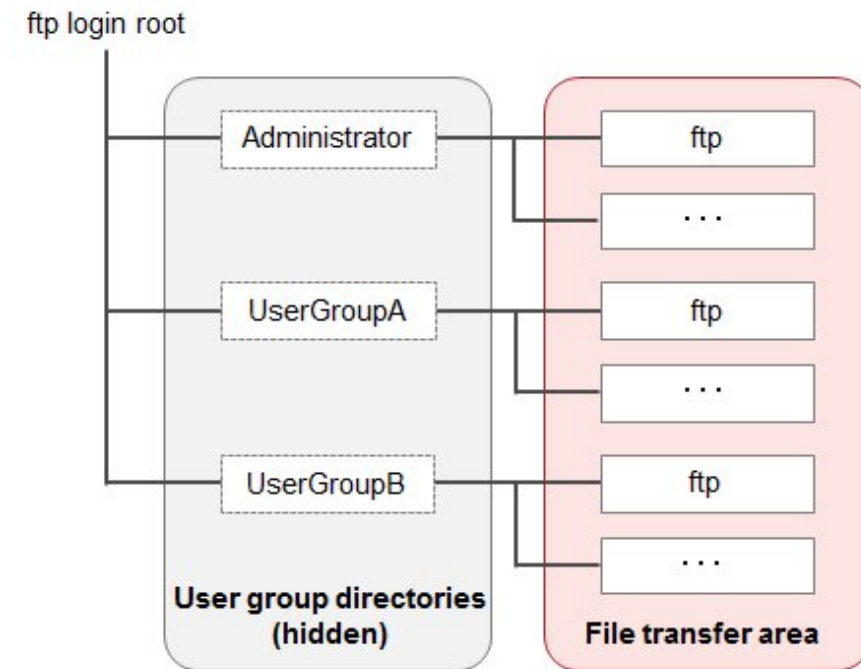
As shown in [Figure 2.1](#), files that are sent or received via FTP are stored under "/<user group name>/ftp."



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 on user group settings, refer to "2.3.2 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 transferring patch files and other binary data, transfer it in binary mode.
- You cannot use the FTPS protocol when connecting.
- When accessing via FTP with a user that is linked with Microsoft Active Directory or OpenLDAP, 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 the 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 connect.

As described in "[2.14.1 User Management](#)," this feature can only be used by users with the following privileges.

- Users who belong to the "Administrator group" and has the "Administrator role."
- Users who belong to the group other than the "Administrator group" that is configured with manage all nodes and who has the "Administrator role."

For the commands that can be used, refer to "[2.14.5.1 List of commands in ISM-VA Management](#)."



Note

- Automatic completion of command parameters by using the [Tab] key is not supported.
- To use Multi-Factor Authentication, use the keyboard interactive authentication method for SSH connections.

For Multi-Factor Authentication, refer to "[2.14.1 User Management](#)" in "[Multi-Factor Authentication](#)."

Note that you cannot set Multi-Factor Authentication unless SSH keyboard interactive authentication of ISM is enabled.

2.1.4 REST API

ISM is equipped with a REST API. With this API, 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.

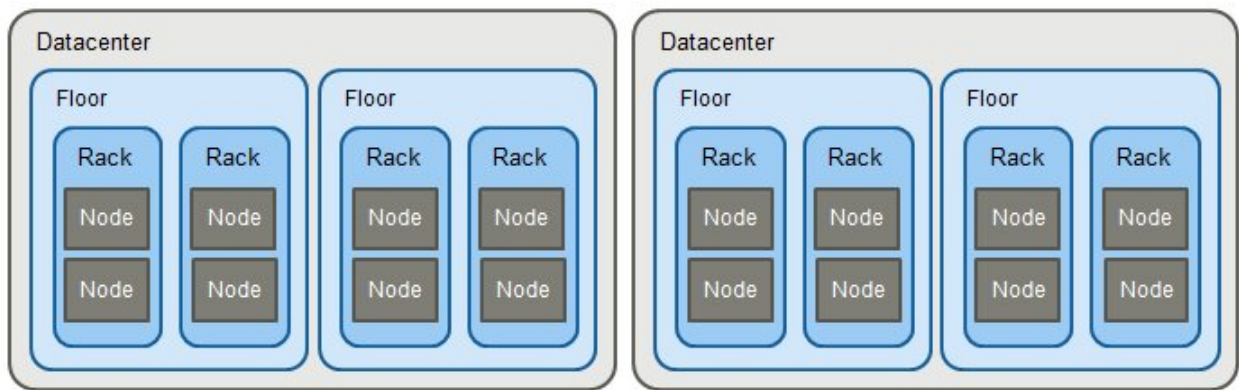
- [2.2.1 Registration of Datacenters/Floors/Racks/Nodes](#)
- [2.2.2 Confirmation of Datacenters/Floors/Racks/Nodes](#)
- [2.2.3 Editing of Datacenters/Floors/Racks/Nodes](#)
- [2.2.4 Deletion of Datacenters/Floors/Racks/Nodes](#)

2.2.1 Registration of Datacenters/Floors/Racks/Nodes

With ISM, you can manage the physical location information of 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 and manage the individual information of each datacenter, floor, rack, and node, as well as their hierarchy 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

Executable user

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

You can register information of new datacenters, floors, and racks in ISM. The datacenter, floor, and rack names that you register must be unique 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

Executable user

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

To manage nodes in ISM, nodes must first be registered in 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 a node that is already registered in ISM.

Nodes with the same cluster UUID cannot be registered if the node is an Ontap cluster.

- To access a node, the required account information must be set in the node information.

In ISM, the specified account information is used to communicate with nodes for operations such as retrieving node information, monitoring, assigning profiles, updating firmware, and collecting logs.

If the node is ETERNUS AB/HB, register the IP address of one of the two controllers. If the registered controller goes down, ISM automatically accesses the other controller. ISM can also receive traps from either controller.

If the node is ETERNUS NR 1000, select "storage" for node type and "OntapCluster" for model. For IP address, enter the IP address of one of the ETERNUS NR 1000 network interfaces that is in the "Management Port (e0M) and where Role is Cluster Management."

If the node is the PRIMEQUEST 4000 series partition, register the IP address for each managed target partition.

If the node is ETERNUS NR/AX/HX, HTTPS is added for the communication method with ISM 2.9.0.021 or later. Register the account that HTTPS can be connected. For ISM 2.9.0.030 or later, the same applies if the node is ETERNUS AC. If the ETERNUS NR/AX/HX node has been registered from ISM 2.9.0.010 or earlier, register the HTTPS account on the node edit screen after applying the ISM 2.9.0.021 patch. You cannot monitor the node status until the HTTPS account is registered.

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.

- 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 of 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.



Note

If the iRMC password is the factory default, ISM cannot manage the following models for node registration:

- PRIMERGY M7 series
- PRIMERGY 1WAY M6
- PRIMERGY RX1440 M2
- PRIMERGY RX2450 M2
- PRIMEQUEST 4000 series

Change the password in one of the following:

- Enter the factory default password and the new password in the [Communication methods] setting when registering nodes in ISM.
- Change the password on the device before registering nodes in ISM. Then enter the new changed password when registering nodes.

Use ICMP (ping command) to determine if ISM and the target node can communicate.

Configure the firewall to allow ICMP communication.

For procedure to register nodes, refer to Step 1 to Step 4 of "3.1.2 Register a Node Directly" in "Operating Procedures."



Point

- You should not monitor the same node with multiple instances of ISM or multiple instances of monitoring software. Monitoring may not operate correctly, because the number of sessions a node can handle simultaneously is typically limited.
- 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.
- To receive traps from nodes with SNMPv3, settings for Trap Reception for SNMP must be specified. For details, refer to "[2.3 Monitoring](#)"-"[Trap reception settings](#)."

Register devices that do not have an option for Model

There are options for "Model" when registering a node for devices supported by ISM.

The following options are available for registering devices that do not have an option in "Model." Configure the appropriate setting based on the capability of the device.

[Model] option	Description
OntapCluster	Select this option if registering ETERNUS NR/HX/AX/AC as the node. There is no difference in terms of monitoring when compared to a device that has an option in [Model].
Generic Server(SNMP)	Select one of these options if the node being registered has an SNMP monitoring function. Refer to "Operating Procedures for General Monitoring" for the required settings and monitoring items.
Generic Switch(SNMP)	
Generic Storage(SNMP)	
Generic Facility(SNMP)	
Generic Server(PING)	Select one of these options if the node being registered responds to the PING command. Normal or error is reflected in the status depending on the result of the PING command.
Generic Switch(PING)	
Generic Storage(PING)	
Generic Facility(PING)	
other	If "Other" is specified, the PING command is used to monitor the activity. If the IP address is not specified or is incorrect, the "Unknown" status is displayed. The specification column for the communication method is displayed, however Monitoring is not performed using the communication method that is input.

There is no problem if you specify the above options for a device that has an option in "Model." However, status notifications are limited.

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 retrieve the 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 a node is registered, the node information is retrieved automatically.

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

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

When retrieval of the node information is completed, a log with the message ID "10020303" is output to the [Events] - [Events] - [Operation Log].

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



Note

- When retrieving the PRIMERGY node information, the device information from the BIOS must be reflected to iRMC. Before executing the retrieval of node information, power on PRIMERGY and check that the BIOS screen of the target node is displayed.

- If retrieval of node information is executed immediately after the PRIMERGY BX chassis (MMB) is powered on, 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.

- Node information can be retrieved from the [Actions] button - [Get Node Information], as well as periodically approximately in 24-hour intervals. This also retrieves OS information and updates the information in the [OS] tab on the Details of Node screen.

To retrieve the OS information, it requires to access the OS, so you can stop this operation. For the setting, refer the following procedures:

- Select the node on the "Node List" screen and from the [Actions] button, select [Set OS Information Retrieval], and then specify Retrieve or Off.
- From the Details of Node screen, select the [OS] tab - [OS Actions] button - [Set OS Information Retrieval], and then specify Retrieve or Off.

If you set the OS Information Retrieval to Off, the information of the [OS] tab on the Details of Node screen does not update.

Point

You can set the time at which node information is periodically retrieved approximately in 24-hour intervals by one of the following.

- On the "Node List" screen, select the check box for the target node, and from the [Actions] button, select [Set Retrieval of Node Information] and set the schedule.
- On the Details of Node screen, from the [Actions] button, select [Set Retrieval of Node Information] and set the schedule.

2.2.1.4 Management of information on node mounting positions in racks

	Administrator group			Other groups		
Executable user	<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

If you have set the mounting positions of nodes in racks, you can confirm the positions on the "Rack View" screen of the GUI.

If you did not set 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 set the mounting positions in the rack after node is registered.

The following is a sample operation for setting the information of a node mounting position in a rack after node registration.

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

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

2.2.1.5 Registration of node OS information

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

If an OS is already installed on a 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, refer to "Support Matrix."

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

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

Select [DOWNLOADS] and select the target operating system.

The reference procedures are subject to change without notice.



Note

- In order to make a server OS a monitoring target in ISM, a separate installation procedure is required for each type of 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 "[Appendix B Settings for Monitoring Target OS and Cloud Management Software](#)."
- To use a domain user to monitor the OS, you must specify the DNS and a domain environment.
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 OSes have 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.
- If the OS type or OS version in the OS information is incorrect, the following symptoms may occur:
 - Retrieval of node information may result in an error.
 - Even if the results of retrieval of node information are displayed, they may not be target to Anomaly Detection.Check the OS installed on the node and enter the correct OS type and OS version in the OS information.

The following is a sample operation.

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

When retrieval of the node information is completed, a log with the message ID "10020303" is output 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

	Administrator group	Other groups
Executable user	<div>Admin Operator Monitor</div>	<div>Admin Operator Monitor</div>

With ISM, you can discover 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 Manual Discovery, you must set the demanded account information that is required to connect 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, refer to "Support Matrix."

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

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

Select [DOWNLOADS] and select the target operating system.

The reference procedures are subject to change without notice.



Point

By setting the IP address of the DNS server in ISM-VA, the following operations (process) become enabled.

- Node can be discovered with FQDN

You can discover node with FQDN.

- Node can be discovered with the host name

Nodes in the same domain as ISM-VA can be discovered with the host name.

If you want to search for node in a different domain than ISM-VA, use FQDN.

In addition to setting the IP address of the DNS server, you must set the host name.

- FQDN of the discovered node can be retrieved

You can retrieve the FQDN of the discovered node. FQDN is set as the initial value of the node name when the node is registered.

Procedure to set the DNS server to ISM, refer to "[4.9 Network Settings](#)" - "Add DNS server."

Procedure to set the host name to ISM, refer to "[4.13 Modification of Host Names](#)."



Note

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

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

Manual Discovery

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

- Execution of 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

Operation requirements

The following function on the target device must be turned on.

Device	Function
PRIMERGY 2/4/8WAY M7 or later, PRIMERGY 1WAY M6 or later, PRIMERGY RX1440/2450 M2 (HTTPS)	SSDP function



Point

For details on Manual Discovery, refer to "[A.2.2 Details of Node Settings.](#)"

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 ISM GUI, 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, FQDN or host name for discovery. The discovery IP address range can be specified up to the third octet.
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.



Note

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

To stop Manual Discovery, select the [Cancel] button on the "Discovery Detail" screen. Note that although you cancel Manual Discovery, the discovery results up to the time of the cancellation are still displayed.

Upload a CSV file and execute Manual Discovery

Upload a CSV file with the required information for the Manual Discovery. Node discovery is executed based on 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 ISM GUI, select [Structuring] - [Node Registration] to display the "Node Registration" screen.
2. From the [Actions] button, select [Discover nodes].
3. In [Discovery method], select "CSV upload."
4. Enter the required information for discovery.

Item	Description
File selection method	Select a specification method for CSV files.

Item	Description
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 must be transferred via FTP to the "/Administrator/ftp" directory in advance.

For FTP connections and how to transfer files via 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." If you are not using encryption, select "Unencrypted."
- When you select "FTP" in [File selection method], if you select the [Delete source file] checkbox in [Action after execute], the CSV file is deleted after discovery has been executed.

CSV file

Download the CSV file template from the ISM GUI.

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

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

You can specify multiple device types.

Note

Delete the second row (the row with the options) of the downloaded CSV file until you are ready to upload the file.

The setting items for the CSV file are described below.

Item Name	Description
IpAddress	IP address of the discovery target node (IPv4, IPv6, FQDN or host name)
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

Item Name	Description
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
NewHttpsPassword	New password for HTTPS Specify the new password if the password for the PRIMERGY M7 series, PRIMERGY 1WAY M6, PRIMERGY RX1440 M2/RX2450 M2 or the PRIMEQUEST 4000 series (iRMC) has not been changed from the factory default (no need to specify if it has been changed). At this time, specify the factory default password in "HttpsPassword."
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	-	-	-	-	-
IpmiPassword	R	-	-	-	-	-
IpmiPort	Y	-	-	-	-	-

Item Name	Account type					
	IPMI	SSH	HTTPS	SNMP		
				V1	V2	V3
SshAccount	-	R	-	-	-	-
SshPassword	-	Y	-	-	-	-
SshPort	-	Y	-	-	-	-
HttpsAccount	-	-	R	-	-	-
HttpsPassword	-	-	R	-	-	-
NewHttpsPassword	-	-	Y	-	-	-
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 prepare the CSV file is as follows.

- Create the CSV file with an arbitrary name.
- Write the item names in the first row.
- Write down the target node information in the second and following rows.
 - Enter the setting values so that they match with the position of the item names in the first row.
 - You must enter a value for the IpAddress.
 - Omit setting values that are not required for the discovery of the target nodes.
 - If an item is not required for discovery of any of the nodes, the corresponding column can be omitted from the item name row.
 - 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 select one or the other method.

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","*****","","","",""
"ism.fujitsu.com","admin3","*****","","","",""
"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 can be viewed while logging into ISM. It is not retained when you log in again.
- 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 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 a physical switch is discovered during node discovery, the result is "Only automatic registration."
- If you operate a CFX switch 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 manually discovered nodes

For procedure to register nodes, refer to Step 7 to Step 12 of "3.1.1 Discover Nodes in the Network and Register Nodes" in "Operating Procedures."

Note

- The IP address set for the device can be changed only for PRIMERGY servers and PRIMEQUEST 3000B that have DHCP enabled.
- If you change the IP address, check that the new IP address is set within 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 registering nodes, set the password for raising the SSH privilege on the node edit screen.

Auto Discovery

For applicable devices to Auto Discovery, refer to "Support Matrix."

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

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

Select [DOWNLOADS] and select the target operating system.

The reference procedures are subject to change without notice.

With 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 in ISM.

Operation requirements

The following requirements must be met.

- The following functions are on the target device side

Device	Function	Detection interval
PRIMERGY server PRIMEQUEST [Note 1]	SSDP function [Note 2]	Every 15 minutes
PSWITCH 2048 T PSWITCH 2048 P PSWITCH 4032 P	Auto Discovery [Note 2]	Every 10 minutes

[Note 1]: PRIMEQUEST 4000 series are not supported.

[Note 2]: To limit Auto Discovery, disable this function.

- The network is configured so that 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 automatically discovered nodes

For procedure to register nodes, refer to Step 7 to Step 12 of "3.1.1 Discover Nodes in the Network and Register Nodes" in "Operating Procedures."



Note

- The devices cannot be managed with Ipv6 link local addresses. If the automatically discovered IP address is only an Ipv6 link local address, you must set an IP address.
- 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 DHCP.
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 for the device, and register it.

- If you change the IP address, check that the new IP address is set within 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.

Hardware settings when registering discovered nodes

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

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



Note

For nodes to which monitoring policy is assigned cannot assign the profile for specific model. To use profile for specific model, do not assign the monitoring policy.

You can apply this setting to the following nodes:

- PRIMERGY and PRIMEQUEST 3000B

The following is a sample operation for hardware settings when registering discovered nodes.

1. Define the Monitoring Policy. For details, refer to "2.4.2 Profiles and Policies."
2. Execute the same procedure as registering discovered nodes.
 - To [Registering manually discovered nodes](#)
Execute Steps 1 to 4.
 - To [Registering automatically discovered nodes](#)
Execute Steps 1 to 5.
3. Select the [Assign the monitoring policy when registering discovered nodes] checkbox, and then select the [Next] button.
If a monitoring policy has not been set or if there are no nodes in which a monitoring policy can be set, you cannot select the checkbox.
A confirmation screen is displayed.
Profile names that reference a monitoring policy and are created automatically are prioritized in the following order:
 1. Default_Profile_<Domain name>
 2. Default_Profile_<Serial number>
 3. Default_Profile_<IP address>
 4. Default_Profile_<Date>
If a profile with the same profile name already exists, "_number (1-)" is added to the end of the profile name and registered.
4. Execute registration.



Point

For details on monitoring settings that can be defined, refer to "Chapter 8. Setting Items of Profiles for Common Policy" in "Items for Profile Settings (for Profile Management)."

2.2.1.7 Adding tags to nodes



In ISM, tags can freely be added to nodes. Tagging 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 is a sample operation for adding tags after node registration.

1. From the Global Navigation Menu on the ISM GUI, 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 apply the changes.

Editing the tags of multiple nodes in a batch

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 ISM GUI, select [Management] - [Nodes].
2. Select the nodes for which you want to edit tags, and then select [Edit Tag] from the [Actions] button.
3. Edit the tag information.
 - To add tags
Input new tags in the [Add tag(s) to multiple nodes] field, or select existing tags and select [Add].
 - To delete multiple tags together
Select tags from the [Delete tag(s) from multiple nodes] field, and select [Delete].
 - To delete tags individually
Select [x] displayed on the [Tag] field in [Target Nodes].
4. Select [Apply] to apply the changes.

Filtering by specifying tags



The following is a sample operation to filter nodes by specifying tags.

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Nodes].
2. In the search box on the upper-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 are displayed on the "Node List" screen.



.....
You can select nodes from the filtering results and execute [Assign Profile] or [Update Firmware/Driver]. For profile assignment and firmware/driver update, refer to "[2.4 Profile Management](#)" and "[2.6.3 Firmware/Driver Update](#)."
.....

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 ISM GUI, 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.



The viewable data is listed below:

- The user who belongs to the Administrator group:
All data can be checked
- The user who does not belong to the Administrator group:
Only the data that one or more nodes are registered can be viewed with your own privilege

Confirming nodes

Confirm the nodes that are registered in ISM.

From the Global Navigation Menu on the ISM GUI, 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.



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 of links with Microsoft Active Directory group or OpenLDAP group
- Central Authentication Service (CAS) settings

For details, refer to "3.7 Use CAS Based Single Sign-On to Log In to the Web Screen of the Server" in "Operating Procedures."

Users who perform settings must meet the following two requirements.

- The user must belong to a user group that manages all nodes
- The user must have a user role higher than the roles specified in the CAS settings

Confirming node OS information

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

If you are monitoring cloud management software by using a domain user ID, enter the FQDN of the realm name of Active Directory in the domain ID field, and enter the user name without the realm name.

In this case, only the information 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 "[Appendix B Settings for Monitoring Target OS and Cloud Management Software](#)."

Downloading a script file to link with AIS Connect Support Gateway



You can download a script file to register managed nodes (PRIMERGY servers only) to AIS Connect Support Gateway (hereafter, referred to as "AIS Gateway").

The procedure to download the script file is as shown below.

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Nodes].
The "Node List" screen is displayed.
2. From the [Actions] button, select [Output AIS Gateway Script].
The "Output AIS Gateway Script" screen is displayed.
3. Set a password for the zip file (Optional).
4. Select the [Output] button.
After the download file has been created, the "Result" screen is displayed.
5. Select "Download."

Overview of the script file

The script file can be executed on the OS (Windows/Linux) on which AIS Gateway is installed.

To check the results of the script file execution, log in to AIS Gateway to confirm the setting information.

The following are the types of script files that can be downloaded.

OS	Type of script file
Windows	Batch file
	PowerShell script
Linux	Shell script (bash)

The setting items for AIS Gateway and their contents are as follows.

To add setting items or to change setting values, edit the script file as required.

AIS Gateway setting item	Setting contents
AssetName	A serial number of a managed node
Model	iRMC_ma
Description	A node name of a managed node
IP Address	An IP address of a managed node
SNMP Community	public



Note

- In the following cases, lines to register applicable managed nodes will be commented out.
Take action as necessary, and download the file again. Or, edit the script file directly.
 - When an IP address is not specified
Set an IP address.
To set an IP address, refer to "[2.2.3 Editing of Datacenters/Floors/Racks/Nodes](#)" - "Editing nodes."
 - When a serial number is not retrieved
Retrieve node information to acquire the serial number.
For retrieving node information, refer to "[2.2.1.3 Management of node information](#)."
- This script overwrites the setting information of the managed node if the node has been registered in AIS Gateway.
If you do not want to overwrite the settings, comment out or delete the lines that include the serial number of the appropriate managed node.

2.2.3 Editing of Datacenters/Floors/Racks/Nodes

Edit the information that is registered in ISM.

Editing datacenters, floors, and racks

Executable user

Administrator group

Other groups

Admin Operator Monitor

Admin Operator Monitor

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 edit 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. Select [Apply] to apply the changes.

Editing nodes

Executable user

Administrator group

Other groups

Admin Operator Monitor

Admin Operator Monitor

The following is the operation procedure for editing node information.

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

When editing a model, the choices displayed are limited to models for which ISM can provide the same services as the model before it is edited.

5. Select [Apply] to apply the changes.

Batch editing nodes

Executable user

Administrator group

Other groups

Admin Operator Monitor

Admin Operator Monitor

The following is the operation procedure for batch editing of the node information.

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Nodes] to display the "Node List" screen.
2. From the [Actions] button, select [Edit in a Batch].
3. Edit the information about the node.
4. Select [Apply] to apply the changes.

Setting enable/disable IPMI

Executable user

Administrator group

Other groups

Admin Operator Monitor

Admin Operator Monitor

You can set enable (to use) or disable (not to use) the IPMI protocol used to communicate with iRMC.

Target models is as follows.

- PRIMERGY M7 series
- PRIMERGY RX1440 M2
- PRIMERGY RX2450 M2
- PRIMEQUEST 4000 series.

The default setting during node registration is Disable IPMI.

To enable IPMI, first set to enable the IPMI in iRMC of the target model (Enable IPMI over LAN). Then, enable IPMI in ISM.

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.

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 the Monitoring History widget is displayed on the Dashboard, remove the node to be deleted from the target node on the "Widget settings: Monitoring History" screen.



Point

.....
If you delete a node while a profile assignment is active, the node will not be deleted. (The profile remains with an "Assigned" status.)
Release the profile assignments individually.
.....



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 this case, refresh the screen contents by one of the following procedures, and then 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 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

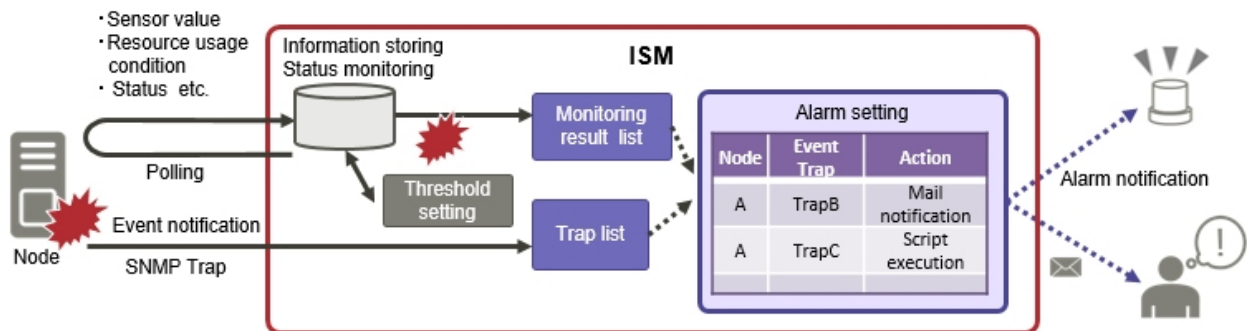
Monitoring is a function you can use for the following purposes.

- Polling for and accumulating information about status and resource usage, such as the CPU usage and the values of sensors such as those for node temperature
- Monitoring the comparison of assigned threshold values and polling results, and the status change
- Receiving incoming event notifications (SNMP Trap) from nodes
- Issuing external alarm notifications of monitoring results and of incoming event notifications from nodes

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

The following shows an operation overview of Monitoring.

Figure 2.3 Image of Monitoring



The default polling interval is 180 seconds. This can be changed in the monitoring interval settings.

The following settings are related to Monitoring.

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

2.3.1 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 details of items 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 is monitored. The IPMI and SNMP protocols are used to access each node every three minutes and the status is displayed in the ISM GUI. The status is displayed in the following areas: <ul style="list-style-type: none">- Node List- [Properties] tab on the Details of Node screen
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.
Power status	The power status is monitored.

Status of the monitoring items takes the following values.

Overall status	Icon on ISM GUI	Status Description
Error		The node has a problem and cannot continue to be used.
Warning		The node is experiencing a problem but can continue to be used.
Unknown		The node has a problem, and its status cannot be determined.
Normal		The node is in a normal status.

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, disk utilization rate, and other resource statuses are monitored.
Fan rotation speed	Rotation speeds of the various fans in managed devices are monitored.
Temperature information (not monitored by default)	Monitor temperatures other than the default target (such as part temperatures).

Procedure for adding monitoring items and threshold values

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

Note

- For Brocade FC switches, different kinds of inlet temperature information can be added for monitoring. However, the only temperature that can actually be monitored is the temperature sensor installed on the device. If the temperature cannot be monitored, "N/A" is displayed for [Latest Value].
- To add resource information such as CPU utilization rate, memory utilization rate, and disk utilization rate to the monitoring item, you must register the node OS information. For details on registering the OS information of the nodes, refer to "[2.2.1.5 Registration of node OS information](#)."

2.3.2 Monitoring of Network Statistics Information



For network switches, statistical information (traffic and so on) can be retrieved on a port basis and threshold monitoring can be set. The following monitoring items are displayed on the [Network statistics] tab.

Monitoring item name	Description
Incoming Traffic	Number of bits received per second
Outgoing Traffic	Number of bits sent per second
Incoming Packets	Number of packets received per second
Outgoing Packets	Number of packets sent per second
Incoming Drop Packets	Difference in the number of received drop packets
Outgoing Drop Packets	Difference in the number of sent drop packets
Incoming Error Packets	Difference in the number of received error packets
Outgoing Error Packets	Difference in the number of sent error packets

[Latest Value] displays the highest value of all ports.

"Difference in the number of XXXX packets" described in the above table is the difference between the total number of packets acquired this time and the total number of packets acquired last time.

This is approximately the number of packets per monitoring interval.

Setting procedure for monitoring of network statistics information/threshold monitoring

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

Note

To use monitoring of network statistics information, use v2c or v3 for the SNMP account of the target node.

2.3.3 Action Settings

Executable user

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

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 methods (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	Send mail with user-defined content.
Send/Forward Trap	<p>Forward the received SNMP trap to an external SNMP manager, or forward an event discovered in ISM as an SNMP trap. Select a "Forwarding Type (Valid only for Trap Forwarding.)" from the following when forwarding.</p> <ul style="list-style-type: none">- ISM forwards the trap as a sender. <p>The sent SNMP trap is processed as if it was sent straight from ISM. Apart from information on the sender, the trap information is sent as-is.</p> <p>The SNMP trap is processed according to the version as follows.</p> <ul style="list-style-type: none">- If forwarded as v1 <p>The trap agent-addr is set to the ISM IP address.</p> <ul style="list-style-type: none">- If forwarded as v2c / v3 <p>The IP address of the trap source is set to variable-bindings for the trap.</p> <p>Specifically, the IP address of the trap source (iRMC of the device) is set to the value 1.3.6.1.6.3.18.1.3 (snmpTrapAddress).</p> <ul style="list-style-type: none">- The received trap is forwarded as-is. <p>The received trap is forwarded to the SNMP manager as-is.</p>
Forward Syslog	Forward events/trap messages to an external Syslog server.



Point

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 "2.2 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 sent emails 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

Macro notation	Overview	Applicable type	
		Node	System
\$_ISM	ISM host name	Y	Y
\$_TRGID	Node ID of target for event (Node)	Y	N

Macro notation	Overview	Applicable type	
		Node	System
\$_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	<p>Mounting position of the node in the rack The display format is different depending on the device.</p> <ul style="list-style-type: none"> - When 1U server is mounted in 2U : 2U - When CX400 chassis (2U) is mounted in 2U, and the target server exists in its slot 2 : 2-3U slot#2 - When BX900 chassis (10U) is mounted in 2U, and the target connection blade exists in its back slot 2 : 2-11U CB#2 - When PDU is mounted : PDU2 - When Rack CDU is mounted : Not displayed 	Y	N
\$_MIB	MIB file name of the SNMP trap	Y	N
\$_SPC	<p>Specific trap code of SNMP trap</p> <p>Last digit of the OID of the SNMP trap</p>	Y	N
\$_TRP	Character string defining the TYPE of MIB of the SNMP trap	Y	N
\$_SEV	<p>Severity of the event</p> <ul style="list-style-type: none"> - When the event type is Trap Critical, Major, Minor, Informational, and Unknown - When the event type is Event Error, Warning, and Info 	Y	Y
\$_EVT	Message ID	Y	Y
\$_MSG	Description	Y	Y
\$_TIM	<p>Time when the event occurred UTC time is displayed in RFC3339 format. (Example: 2018-01-01T00:00:00.000Z)</p>	Y	Y
\$_TIM2	<p>Time when the event occurred Displayed in local time format. (Example: 2018-01-01-00.00.00)</p>	Y	Y



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

For details, refer to "2.2.1.1 Execute a script deployed on the external host" - "Action settings" in "Operating Procedures."

Required preparations before using an action

Execute Remote Script

For details, refer to "2.2.1.1 Execute a script deployed on the external host" - "Pre-settings" in "Operating Procedures."

E-Mail Sending

For details, refer to "2.2.1.2 Send mail" in "Operating Procedures."

Send/Forward Trap

For details, refer to "2.2.1.3 Execute sending/forwarding a trap" in "Operating Procedures."

Procedure for test execution of an action

For details, refer to "2.2.2 Execute Test for Action (notification method)" in "Operating Procedures."

2.3.4 Alarm Settings

The screenshot shows two panels for user selection. The left panel is titled 'Administrator group' and the right panel is titled 'Other groups'. Both panels have a label 'Executable user' to their left. Each panel contains three buttons: 'Admin' (blue), 'Operator' (blue), and 'Monitor' (grey). In both panels, 'Admin' and 'Operator' are highlighted, indicating they are the selected users.

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

Procedure for adding alarms

For details, refer to "2.2.3 Set an Alarm to the ISM Internal Event" in "Operating Procedures."

Event type

There are the following types of events.





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



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	Icon displayed in the ISM GUI	Description
Error	High	 Red bell icon	This icon is displayed when any of the following events are discovered: <ul style="list-style-type: none">- ISM event at Error level- SNMP trap at CRITICAL level
Warning	Medium	 Yellow bell icon	This icon is displayed when any of the following events are discovered: <ul style="list-style-type: none">- ISM event at Warning level- SNMP trap at MAJOR or MINOR level
Info	Low	 Blue bell icon	This icon is displayed when any of the following events are discovered: <ul style="list-style-type: none">- ISM event at Info level- SNMP trap at INFORMATIONAL level
None	-	 White bell icon	This is the status when no event has been discovered.

An alarm status of “Info” or higher means that an event corresponding to that level was discovered. From the Global Navigation Menu on the ISM GUI, 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 ISM GUI, 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.
- You may need to turn off the power of nodes systematically to maintenance nodes. 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 are restricted for nodes that are switched into Maintenance Mode, this function prevents the repeated occurrence of alarms for the node.

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



Note

For PRIMERGY CX series and PRIMEQUEST 4000 series, executing Clear Alarm on the chassis does not clear the alarm status.

The alarm status notified to the chassis of PRIMERGY CX series and PRIMEQUEST 4000 series notifies the alarm status of the nodes belonging to the chassis. If multiple nodes are belonging to the chassis, the alarm status of the chassis will be notified when an event is detected on any node. When events are detected on multiple nodes, the highest priority event is notified to the chassis alarm status.

If the alarm is cleared for all nodes belonging to the chassis, the alarm status of the chassis will be cleared.

Note that chassis of PRIMERGY CX series and PRIMEQUEST 4000 series do not detect events themselves. Therefore, there is no need to clear the alarm of chassis.

.....

Trap reception settings

The image shows a configuration interface for trap reception settings. It features a label 'Executable user' on the left. To its right are two main sections: 'Administrator group' and 'Other groups'. Each section contains three buttons: 'Admin', 'Operator', and 'Monitor'. In the 'Administrator group' section, the 'Admin' button is highlighted with a blue border, while the others are grey. In the 'Other groups' section, all three buttons are grey.

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

Process for adding settings for Trap Reception for SNMP

For details, refer to "3.2.2 Set Trap Reception for SNMP" in "Operating Procedures."

MIB file

MIB is public information regarding the status of the network devices managed with SNMP, and is standardized as MIB-II, which is published as RFC 1213. An MIB file is a text-based file that defines this public information. To send and receive SNMP traps, the receiving side is required to save an 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 the hardware supplied from a vendor other than Fsas Technologies such as ISM unsupported Fsas Technologies devices, Cisco switches, and HP servers.
For the latest information on products supported by ISM, refer to "Support Matrix."
<https://support.ts.fujitsu.com/index.asp>
Select [Select a new Product] on the above site and enter "Infrastructure Manager" in [Product Search:].
Select [DOWNLOADS] and select the target operating system.
The reference procedures are subject to change without notice.
- 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 an 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 multiple occurrences of the same trap were received.
- To manage the severity of traps with ISM, MIB files to be imported must be written in a specific format. If imported MIB files are written in a format other than the specified format, the behavior could differ from the definition. Check that there are no errors in the format before you import MIB files.

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

.....

Registering a MIB file

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 that has the same name as an MIB file already registered on ISM.

.....

Confirming MIB files

You can confirm the names of MIB files that are 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 cancel 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 relationships. If you delete an MIB file that has dependency relationships, traps may no longer be received.

.....

2.3.5 Graph Display of Monitoring History

The history of the monitoring items accumulated through Monitoring can be displayed in a graph on the ISM GUI. The graph display allows you to easily see changes and tendencies in the history of the monitored items. A graph can be displayed for nodes individually, and a graph for multiple nodes can also be displayed as a dashboard widget.

For details, refer to "4.6 Display Monitoring History in a Graph" in "Operating Procedures."

2.3.6 Anomaly Detection

Anomaly Detection continuously monitors the operation of hardware and software configuring the managed nodes and the use of their resources.

When you start Anomaly Detection, you can predict CPU utilization. Enabling this setting allows you to monitor CPU usage and notify the date and time of error occurrences that predicted.

Anomaly Detection monitors the status of the following physical servers.

- VMware ESXi hosts
ESXi hosts managed by vCenter Server or vCenter Server Appliance
Single ESXi hosts that are not managed by vCenter Server or vCenter Server Appliance
- Red Hat Enterprise Linux servers
Physical servers running Red Hat Enterprise Linux

For details, refer to "[2.3.6.1 Operation requirements](#)."

The following functions are provided:

- Start and stop of Anomaly Detection
- Enable or disable of Prediction of CPU Utilization setting
- Display of Anomaly Detection information
- Display of Anomaly Detection history
- Event notification for Anomaly Detection and recovery
- Display of solutions
- Suppression of Anomaly Detection

Information is collected for a fixed period from the target server to create learning data (a prediction model). The normal range for monitoring items is calculated by this learning data, to determine if the current measured values are within the normal range. Period of criteria is as follows:

- VMware ESXi hosts: once every 3 minutes
- Red Hat Enterprise Linux server: once every 24 hours

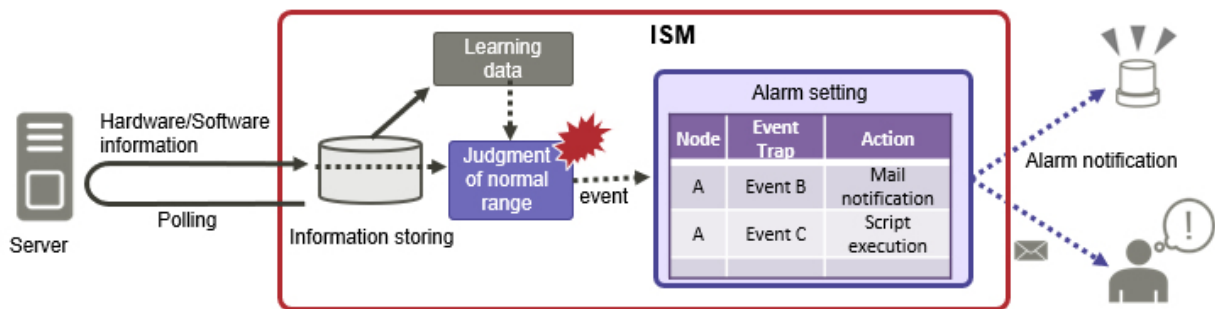
If the measured value is outside the normal range, events of Anomaly Detection are occurred. The event of Anomaly Detection can be notified externally as alarms accordance with configuration.

When Anomaly Detection is persistent, an event occurs every three minutes.

The event occurrence of Anomaly Detection can be suppressed by setting "Suppress Anomaly Detection" (Vmware ESXi only).

"Suppress Anomaly Detection" automatically changes the determination criteria for the notified event of Anomaly-Detection and suppresses subsequent detection.

Figure 2.4 Image of Anomaly Detection



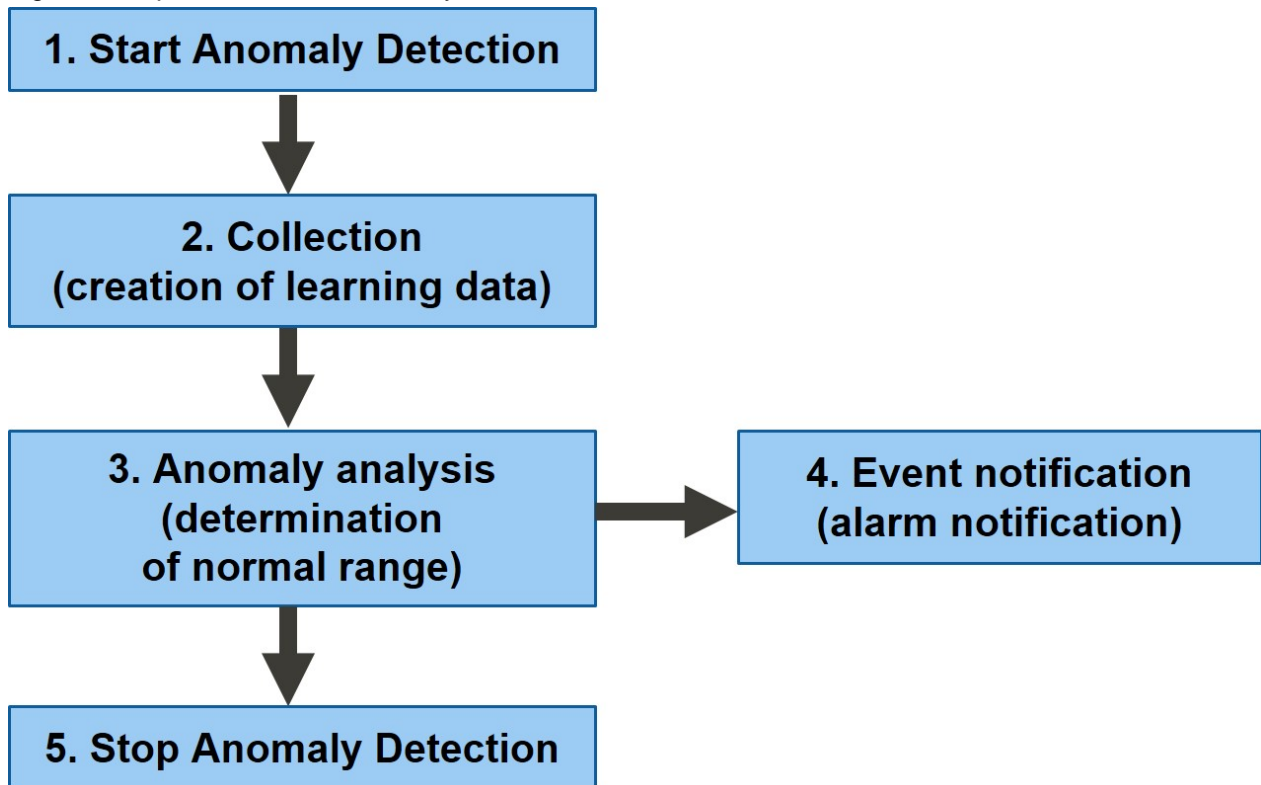
Advantages

- Not necessary to set a threshold for monitoring
- Detection for behavior that is not normal in real time
- Detection for potential errors or unexpected failures not captured by threshold settings
- Support for solutions to problems that have been detected

Operation flow for Anomaly Detection

The following shows the operation flow of Anomaly Detection.

Figure 2.5 Operation flow for Anomaly Detection



Monitoring items

The following shows a list of items for monitoring. Anomaly analysis is performed for each monitoring item and notification is made for each individual event.

Table 2.1 Monitoring item list for Vmware ESXi hosts

Monitoring target	Monitoring item name
Memory	Swapin size
	Swapout size
Storage	Queueing delay
	Disk access time
	Read time
	Write time
Physical NIC	Send packets dropped
	Receive packets dropped
	Send packets errors
	Receive packets errors
Virtual Machine	CPU usage
	Ready time
Virtual Switch Port	Send packets dropped
	Receive packets dropped
packet RX Process	CPU usage
	Ready time

Monitoring target	Monitoring item name
packet TX Process	CPU usage
	Num Of task switching
	Ready time

Table 2.2 Monitoring item list for Red Hat Enterprise Linux servers

Monitoring target	Monitoring item name
CPU	IO waiting time [Note]

[Note]: The IO waiting time for NFS access is monitored.

Prediction items

The following shows a list of items for prediction.

Table 2.3 Prediction item list for Vmware ESXi hosts

Prediction target	Prediction item
Virtual Machine	CPU usage
packet RX Process	CPU usage
packet TX Process	CPU usage

Prediction item list for Red Hat Enterprise Linux servers

None

Collection data

On nodes where Anomaly Detection is started, information is collected for anomaly analysis so that normal behavior can be understood. The collected data becomes "collection data." Collection data is accumulated by continual operation.

Learning data

Learning data is the reference data for the "normal range" (threshold with some leeway), which is the criteria for detecting an anomaly. Learning data is generated from collection data. Anomaly analysis is not started until learning data is created.

The time required to create learning data for the first time and the update timing of learning data are as follows.

Item	Anomaly Detection for Vmware ESXi hosts	Anomaly Detection for Red Hat Enterprise Linux servers
Creation of learning data for the first time	approximately 2.5 days	approximately 7 days
Update timing of the learning data	every 12 hours	every 24 hours

Learning data is retained even if Anomaly Detection is stopped. However, you must create learning data again in the following situations.

- There has been a change to the OS information and the configuration of hardware and cloud management software for the node starting Anomaly Detection
- When the resource usage of the node starting Anomaly Detection has changed
- Anomaly Detection has been stopped for a month or longer

You can select whether to create new learning data or to use learning data that was created previously when you start Anomaly Detection.

If you want to re-create learning data, select the [Initialize] checkbox for [Initialization of Information Collection Data].

On nodes where Anomaly Detection is started for the first time, learning data is created regardless of whether the checkbox is selected.

Prediction data

Prediction data is used to predict CPU utilization. After enabling the Prediction of CPU Utilization setting, the prediction data is created and updated for up to three months from the collection data. The prediction period depends on the period in which the prediction data was accumulated (the accumulation period). The following is a list of periods.

Prediction period	Accumulation period
No prediction	Less than 3 weeks
1 week	3 weeks or more, less than 3 months
1 month	3 months



Note

- If you disable the Prediction of CPU Utilization setting, the prediction data is deleted.
- If you restore using Backup/Restore for ISM, the Prediction of CPU Utilization setting is disabled. Prediction data that has been created is not backed up.

Period of Criteria for Anomaly Detection

By using collection data over a certain period of time, you can create learning data that will be used as criteria for detecting anomalies. This period is called the "period of criteria for Anomaly Detection." The initial value is 7 days.

The period of criteria for Anomaly Detection can be switched between 7 days and 31 days when starting Anomaly Detection. After switching the days, the Anomaly Detection status is "Collecting(Learning Data Creating)" (takes 5 minutes to 1 day). Anomaly Detection begins after the information is collected.



Point

- Information is collected in the following timing:
 - VMware ESXi hosts: every 3 minutes
 - Red Hat Enterprise Linux servers: every 24 hours (based on the 2:00 AM local time zone set in ISM-VA)
- To create learning data (when starting Anomaly Detection for the first time or when you re-create learning data) takes the following times:
 - VMware ESXi hosts: approximately 2.5 days
 - Red Hat Enterprise Linux servers: approximately 7 days

The data learned during this period becomes the basic data for subsequent anomaly detections. The period when learning data is created must not include periods of irregular operation, such as holidays or server maintenance. If you suspect the authenticity of the anomaly detection results, stop Anomaly Detection and create the learning data again.

- Learning data is updated at the following timing:
 - VMware ESXi hosts: every 12 hours
 - Red Hat Enterprise Linux servers: every 24 hours

This analyzes and sets the "Normal Range" which is the standard used for Anomaly Detection. You can get higher accuracy for determining behavior that is not normal by continual use of Anomaly Detection.

- If a month-long period with a mixture of periods with large and small fluctuations is expected (such as with CPU usage), setting "Period of criteria for Anomaly Detection" to 31 days will provide better anomaly detection based on the period (31 days).

- The anomaly detection algorithm has been improved in ISM 2.9.0.030.

For the behaviors that rarely occur can be determined as within the normal range for anomaly detection criteria. With this improvement, it is less likely to detect anomalies for temporarily loaded processes such as node backup operations executed late at night or on weekends.

Note

- Anomaly Detection is not for detecting all of the causes of hardware failures. Furthermore, even if a hardware failure is detected, it does not necessarily mean that an error has occurred. Check the status of the hardware and software based on the content in the notification and consider taking action.
- When learning without using a virtual machine, Anomaly Detection may indicate that the large value for the normal range of the virtual machine at the time of anomaly is detected. If you doubt the validity of the anomaly detection results, execute learning again.
- This function collects information from vCenter Server and vCenter Server Appliance (hereafter referred to as "vCenter"). As a result, the vCenter specification records logins and logouts to the vCenter access log approximately every three minutes.
- This function logs in via SSH from the OS of the Red Hat Enterprise Linux servers and retrieves the information about monitoring items. Therefore, SSH logins and logouts are recorded in the OS access log once every 24 hours.
- Anomaly Detection is stopped for all nodes when a restoration is performed using ISM Backup/Restore. Created learning data is not backed up.

2.3.6.1 Operation requirements

To use Anomaly Detection, the following requirements must be met.

Target node

Nodes that can initiate Anomaly Detection are servers that are running the supported hypervisor and managed by cloud management software or the servers that are running the supported OS.

For information on the supported software environments, refer to "Support Matrix."

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

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

Select [DOWNLOADS] and select the target operating system.

The reference procedures are subject to change without notice.

Resources required for ISM-VA

To use Anomaly Detection, resources must be added to the hypervisor on which ISM-VA is running. The resources required change depending on the environment.

Before using Anomaly Detection, refer to the following table to add the required resources. Also, if your environment changes after you start, add the resources that are expected to increase in advance.

Table 2.4 Resources required for ISM-VA (Vmware ESXi hosts)

Period of Criteria for Anomaly Detection	Additional resource requirements	Additional unit	Additional resource		
			Number of CPU cores	Memory capacity	Disk capacity
7 days	Number of nodes starting Anomaly Detection at the same time	Per 10 nodes	0.4 cores	1.3 GB	4.0 GB
	Total number of virtual machines [Note 1]	Per 100 VMs	0.2 cores	0.4 GB	2.0 GB

Period of Criteria for Anomaly Detection	Additional resource requirements	Additional unit	Additional resource		
			Number of CPU cores	Memory capacity	Disk capacity
	Total number of cloud management software [Note 2]	Per CMS	-	1.0 GB	-
31 days	Number of nodes starting Anomaly Detection at the same time	Per 10 nodes	0.4 cores	2.5 GB	4.0 GB
	Total number of virtual machines [Note 1]	Per 100 VMs	0.2 cores	1.0 GB	2.0 GB
	Total number of cloud management software [Note 2]	Per CMS	-	2.5 GB	-

[Note 1]: Total number of virtual machines registered on a node using Anomaly Detection

[Note 2]: Total number of cloud management software (CMS) registered on a node using Anomaly Detection

Table 2.5 Resources required for ISM-VA (Red Hat Enterprise Linux servers)

Period of Criteria for Anomaly Detection	Additional resource requirements	Additional unit	Additional resource		
			Number of CPU cores	Memory capacity	Disk capacity
7 days	Number of nodes starting Anomaly Detection at the same time	Per 10 nodes	0.8 cores fixed [Note]	0.2 GB fixed [Note]	1.8 GB
31 days	Number of nodes starting Anomaly Detection at the same time	Per 10 nodes	0.8 cores fixed [Note]	0.2 GB fixed [Note]	8.0 GB

[Note]: The number of CPU cores and memory capacity required for the Red Hat Enterprise Linux servers for Anomaly Detection does not vary with the number of nodes.

In addition to the above, additional resources are required to use Prediction of CPU Utilization for the Vmware ESXi hosts. Use the table below to add the required resources.

Table 2.6 Resources required for ISM-VA when using Prediction of CPU Utilization

Additional resource requirements	Additional unit	Additional resource		
		Number of CPU cores	Memory capacity	Disk capacity
Number of nodes starting Prediction of CPU Utilization	Per 10 nodes	0.1 cores	0.6 GB fixed [Note]	0.1 GB

[Note]: The amount of memory required for Prediction of CPU Utilization does not vary with the number of nodes.

Example 1: Based on a PRIMEFLEX configuration (3 nodes, 31 virtual machines per node and 1 cloud management software)

[Total number of virtual machines] $3 * 31 = 93$ virtual machines

[Resources required for Example 1]

Period of Criteria for Anomaly Detection	Prediction of CPU Utilization setting	Number of CPU cores	Memory capacity	Disk capacity
7 days	Disabled	1.0 (0.6) cores	2.7 GB	6.0 GB
31 days	Disabled	1.0 (0.6) cores	6.0 GB	6.0 GB
7 days	Enabled	1.0 (0.7) cores	3.3 GB	6.1 GB
31 days	Enabled	1.0 (0.7) cores	6.6 GB	6.1 GB

Example 2: Based on the PRIMEFLEX configuration (16 nodes, 31 virtual machines per node and 1 cloud management software)

[Total number of virtual machines] $16 * 31 = 496$ virtual machines

[Resources required for Example 2]

Period of Criteria for Anomaly Detection	Prediction of CPU Utilization setting	Number of CPU cores	Memory capacity	Disk capacity
7 days	Disabled	2.0 (1.8) cores	5.6 GB	18.0 GB
31 days	Disabled	2.0 (1.8) cores	12.5 GB	18.0 GB
7 days	Enabled	2.0 cores	6.2 GB	18.2 GB
31 days	Enabled	2.0 cores	13.1 GB	18.2 GB

Example 3: Based on the Red Hat Enterprise Linux server configuration (200 nodes)

[Resources required for Example 3]

Period of Criteria for Anomaly Detection	Prediction of CPU Utilization setting	Number of CPU cores	Memory capacity	Disk capacity
7 days	- [Note]	1.0 (0.8) cores	0.2 GB	36.0 GB
31 days	- [Note]	1.0 (0.8) cores	0.2 GB	160.0 GB

[Note]: The required resources for configuration of the Red Hat Enterprise Linux servers do not affect with the Prediction of CPU Utilization setting.



Note

- Add resources to the hypervisor running ISM-VA, according to your environment. Failure to do so may affect the operation of the GUI.
- The maximum number of nodes that can start Anomaly Detection is as followings:
 - VMware ESXi hosts: maximum 100 nodes (error occurs when 100 nodes are exceeded)
 - Red Hat Enterprise Linux servers: maximum 1000 nodes

2.3.6.2 Starting and stopping Anomaly Detection



Anomaly Detection is started and stopped by node. When Anomaly Detection is started, information is collected, and analysis is performed.

Procedures for starting and stopping Anomaly Detection

Select the target node from the “Node List” screen, and then from the [Actions] button, start or stop Anomaly Detection. You can also perform these actions from the [Anomaly Detection] tab on the Details of Node screen.

For details, refer to “4.11.3 Start Anomaly Detection” and “4.11.7 Stop Anomaly Detection” in “Operating Procedures.”

You can select whether to create new learning data or to use learning data that was created previously when you start Anomaly Detection on the “Start Anomaly Detection” screen. You can also select the period of criteria for Anomaly Detection when starting it.

Note

Anomaly Detection is stopped when the following operations have been performed for a node in which Anomaly Detection has been started.

- OS information for the node has been deleted from the ISM GUI
- Registration for the node has been deleted from the cloud management software
- The node has been removed from the management of cloud management software
- Maintenance mode has been set

2.3.6.3 Enable or disable the Prediction of CPU Utilization setting



Enabling or disabling CPU Usage Prediction is applied to all nodes that are running Anomaly Detection for the VMware ESXi hosts. When Prediction of CPU Utilization is enabled, the accumulation of prediction data begins. Prediction starts three weeks after it is enabled. If the system detects an anomaly and CPU utilization is high, it displays the expected date, time, and value in [Solution] on the [Anomaly Detection] tab.

You can enable or disable the Prediction of CPU Utilization setting from the [Actions] button on the “Node List” screen.

For details, refer to “4.11.2 Enable the Prediction of CPU Utilization Setting” and “4.11.8 Disable the Prediction of CPU Utilization Setting” in the “Operating Procedures.”

Note

If you disable the Prediction of CPU Utilization setting, the prediction data created is deleted.

2.3.6.4 Anomaly Detection statuses

The statuses for nodes executing Anomaly Detection are as follows.

Table 2.7 Anomaly Detection Statuses

Status	Description
Off	Anomaly Detection is not started (initial status)
Collecting(XX%)	Anomaly Detection is started, the necessary information is being collected (learning data is being created) for analysis Anomalies are not detected. This status is displayed when you first start Anomaly Detection on a node or when specify to collect information for initialization and start Anomaly Detection.
Collecting(Learning Data Creating)	Creating the learning data needed for analysis Continues to gather needed information for creating learning data. Anomalies are not detected. This status is displayed if you changed the period of criteria for Anomaly Detection.
Operating(Normal)	Results of the analysis has determined that the behavior is normal (analyzing anomaly detection)

Status	Description
	Continues to gather needed information for creating learning data.
Operating(Anomaly Occurring)	Results of the analysis has determined that the behavior is not normal (analyzing anomaly detection) Continues to gather needed information for creating learning data.
Error	An error has occurred and Anomaly Detection cannot be used
-	A node that is not targeted for Anomaly Detection (except server)

If the status for Anomaly Detection is “Error,” an error message is displayed on the [Anomaly Detection] tab for “Anomaly Detection Status.” Take action according to the message content.

Table 2.8 Error message

Message	Action
The cloud management software (<IP address [Note 1]>) detected an error. Check the cloud management software logs.	Check the vCenter logs and take action.
Failed to log in to the cloud management software (<IP address [Note 1]>). Execute the ISM “Cloud Management Software Test.”	Check that you can connect to vCenter.
Failed to get the information. Check that the node (IP address for the OS=<IP address>) on vCenter is running normally.	Check that the node is turned on. Also, check that the IP address for the OS registered in ISM is correct. [Note 2]
The VMware vCenter Server <Version> does not support Anomaly Detection.	The vCenter version is not supported. Refer to “ 2.3.6.1 Operation requirements ” to confirm the supported version.
The VMware ESXi <Version> does not support Anomaly Detection.	The ESXi version is not supported. Refer to “ 2.3.6.1 Operation requirements ” to confirm the supported version.
Could not get the OS version of VMware ESXi. Please specify the OS version in the Edit OS Information.	The ESXi version could not be retrieved. On the “Edit OS Information” screen, select an OS version other than “Auto.”
Red Hat Enterprise Linux <Version> does not support Anomaly Detection.	This version of Red Hat Enterprise Linux is not supported. Refer to “ 2.3.6.1 Operation requirements ” to confirm the supported version.
Failed to retrieve the information of Red Hat Enterprise Linux <Version>. Confirm that the node (<IP address of the OS>) is started normally.	Check that the node is powered on. Also, confirm that the IP address of the OS registered with ISM is correct.
The package required for Anomaly Detection for the monitoring target is not installed (<IP address of the OS>). Install the package required for the monitoring target OS.	Check “ B.1.3 Precautions When Setting a Monitoring Target OS and Cloud Management Software ”, and install the package to the monitoring target OS.
Failed to login to node (<IP address of the OS>). Either the account name or the password is invalid. Check the OS settings on the node.	Check that account name and password registered in the OS settings are correct.

[Note 1]: IP address of the cloud management software

[Note 2]: If a node has been removed from the management of vCenter, this message will be displayed until the ISM virtualization management software information is updated. In this case, stop Anomaly Detection.

2.3.6.5 Displaying Anomaly Detection information

Information for Anomaly Detection can be checked from the “Node List” screen on the Details of Node screen on the [Properties] and [Anomaly Detection] tabs.

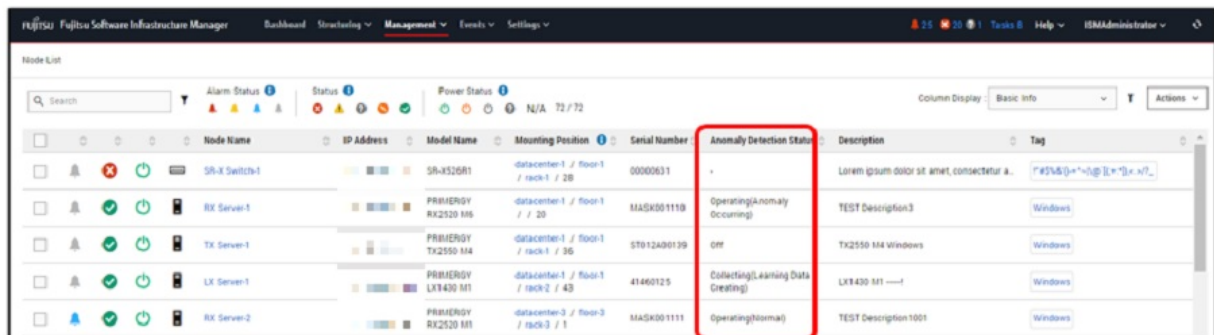
Displaying the “Node List” screen

You can display the “Anomaly Detection Status” column on the Node List screen.

By default, the “Anomaly Detection Status” column is not displayed. In [Column Display], select “Basic Info” to display this column, then from the [Y (column selection)] button on the right, add [Anomaly Detection Status].

For the status of Anomaly Detection, refer to “2.3.6.4 Anomaly Detection statuses.”

Figure 2.6 Display of Anomaly Detection Status on the “Node List” screen



Node Name	IP Address	Model Name	Mounting Position	Serial Number	Anomaly Detection Status	Description	Tag
SA-X Switch-1		SA-X32GR1	datacenter-1 / floor-1 / rack-1 / 2B	00000631	-	Lorem ipsum dolor sit amet, consectetur a...	[Tag]
RX Server-1		PRIMERGY RX2520 M15	datacenter-1 / floor-1 / rack-1 / 2D	MA5K301110	Operating(Anomaly Occurring)	TEST Description3	Windows
TX Server-1		PRIMERGY TX2550 M14	datacenter-1 / floor-1 / rack-1 / 3B	ST912A00139	Off	TX2550 M14 Windows	Windows
LX Server-1		PRIMERGY LX1430 M11	datacenter-1 / floor-1 / rack-2 / 4B	41460125	Collecting(Learning Data Creating)	LX1430 M11 ---f	Windows
RX Server-2		PRIMERGY RX2520 M11	datacenter-3 / floor-3 / rack-3 / 1	MA5K301111	Operating(normal)	TEST Description 1001	Windows

Displaying the [Properties] tab

[Anomaly Detection Status] displays the current status for Anomaly Detection. The number of events notified in [Anomaly Detection Log] are also displayed. You can display the anomaly detection events for the target node by selecting the number of events.

For the status of Anomaly Detection, refer to “2.3.6.4 Anomaly Detection statuses.”

Figure 2.7 Display of the [Properties] tab

Properties

Component

OS

Virtual Machines

Anomaly Detection

Firmware/Driver

Monitoring

Profile

Backup / Restore

Log Collection Settings

Boot Info

SDS

Status

Warning

Alarm Status

None

Power Status

On

Anomaly Detection Status

Operating(Anomaly Occurring)

Event

1000

Operation Log

2000

Audit Log

3000

SNMP Traps

8

Anomaly Detection Log

4000

Alarm Settings

50

Running Task

6000

Node Logs

7000

Archived Logs

Map

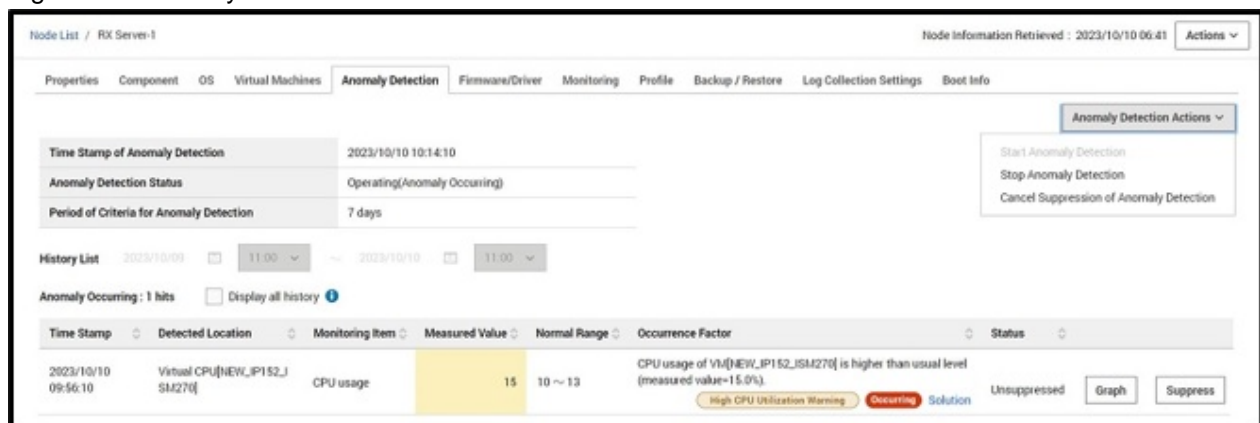
Network

Displaying the [Anomaly Detection] tab

The following items are displayed on the [Anomaly Detection] tab.

- Time Stamp of Anomaly Detection/Anomaly Detection Status
- History List

Figure 2.8 Anomaly Detection Information screen



Time Stamp of Anomaly Detection	Anomaly Detection Status	Period of Criteria for Anomaly Detection
2023/10/10 10:14:10	Operating(Anomaly Occurring)	7 days

Time Stamp	Detected Location	Monitoring Item	Measured Value	Normal Range	Occurrence Factor	Status
2023/10/10 09:56:10	Virtual CPU[NEW_IP152_J SM276]	CPU usage	15	10 ~ 13	CPU usage of Vm[NEW_IP152_JSM276] is higher than usual level (measured value=15.0%).	Unsuppressed

Time Stamp of Anomaly Detection/Anomaly Detection Status

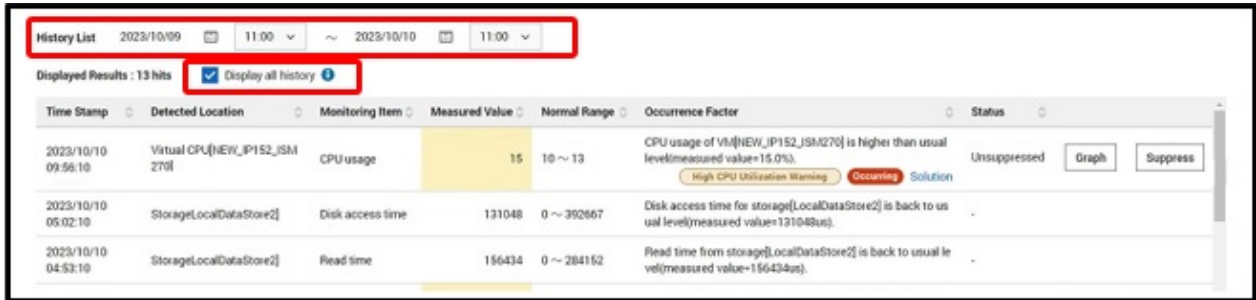
Displays the latest date and time when an anomaly was detected (anomaly analysis) and the status of Anomaly Detection at that time. If “Error” is displayed in Anomaly Detection Status, the error message is also displayed.

History List

Displays the history of past anomaly detections and recoveries. The retention period for history is three months.

Only the unrecovered anomaly detection history is shown when the screen is displayed. You can display the history for any period by checking the [Display all history] checkbox and setting the date and time.

Figure 2.9 Display of the History List for any Period



The number of items that can be displayed in the list at one time is 1,000. Shorten the specified time period for more than 1,000 items.

Table 2.9 History List items

Item	Description
Time Stamp	Date and time of anomaly detection/recovery
Detected Location	Monitoring target in which an anomaly was detected/recovered
Monitoring Item	Monitoring item in which an anomaly was detected/recovered
Measured Value	Actual measured data of the monitoring item of the time stamp This is in yellow when the value is not in the normal range.
Normal Range	Normal range for actual measured data of the monitoring item used for anomaly detection
Occurrence Factor	Factor that determined the anomaly detection/recovery Select “Solution” to display the solution. If CPU utilization is high, the “Solution” section displays the expected date, time, and value.
Status	Suppression status of Anomaly Detection “Unsuppressed”: the status Anomaly Detection is not suppressed “Suppressing”: the status Anomaly Detection is in suppress “-”: the status that no suppression required, or no suppression allowed“
[Graph] button [Note]	Displays the measured graph in which the corresponding anomaly is detected
[Suppress] button [Note]	Resets the normal range so that the corresponding anomaly is not detected. This suppresses the event notification for Anomaly Detection. This button is disabled when [Status] is displayed as “Suppressing”/”-“

[Note]: Supported only for Vmware ESXi hosts.

The button is not displayed for the following history (event).

- Recovering from anomaly
- Anomalies that have been detected for one month

2.3.6.6 Anomaly Detection events

Notification is made for events when Anomaly Detection is started/stopped, anomalies are detected, and recovery is made. From the Global Navigation Menu on the ISM GUI, select [Events] - [Events], and when the “Event List” screen is displayed, select the [Anomaly Detection Log] tab to check for events that have occurred since they are retained as “Anomaly Detection Logs.”

Table 2.10 Types of events

Event type	Content	Message ID	Alarm notifications
Anomaly detection start	Anomaly Detection has started	10038200	N
Anomaly detection stop	Anomaly Detection has stopped	10038201	N
Enable prediction of CPU utilization	Prediction of CPU utilization has enabled	10038202	N
Disable prediction of CPU utilization	Prediction of CPU utilization has disabled	10038203	N
Suppress Anomaly Detection	Anomaly Detection suppressed	10038204	N
Cancel Suppression of Anomaly Detection	Suppression of Anomaly Detection canceled	10038205	N
Anomaly detection result	Anomaly status detected and recovering	10038100 - 10038199 [Note 1]	Y
Anomaly detection event	Anomaly Detection has generated event information Example: Learning data was created.	10038500 - 10038599 [Note 2]	N

[Note 1]: The message ID is different for each monitoring item. You can set external alarms for notifications using the action and alarm settings for events. For action settings, refer to “[2.3.3 Action Settings](#)” and for alarm settings, refer to “[2.3.4 Alarm Settings](#).”

[Note 2]: Each event has a different message ID.

Table 2.11 Display item

Item name	Description
Severity	“Info” (Fixed)
Time	Time the event was notified
Type	Type of event
Message ID	Message ID of the event
Node Name	Node name for which the event was generated You can display the anomaly detection information for the target node by selecting the node name.
Operator	User that started or stopped Anomaly Detection A “-” is displayed for events that are not caused by a user.
Description	Content of the event Select “Solution” to display the solution. After the retention period of the anomaly detection information has expired, a message is displayed and no solution is displayed.

2.3.6.7 Anomaly Detection solutions

You can see the cause and how to resolve it by selecting “Solution” from [History] in anomaly detection events or anomaly detection information.

Check that the anomaly detection status becomes “Normal” by implementing the solution.

Point

From the cause of the anomaly and the vCenter event log information, estimate the cause and location of the anomaly and narrow down the solution.

Note

Depending on the version number of the hypervisor and cloud management software, the names and procedures for the functions described in the solution may be different. In this case, refer to the appropriate manual and apply it as necessary.

2.3.6.8 Suppression of Anomaly Detection

Anomaly Detection may detect and notify normal operation of anomalies depending on the learning data and operation status.

Suppression of Anomaly Detection can reduce the occurrence of events so that they are not detected as anomalies during normal operation by expanding the normal range that is the criterion for Anomaly Detection.

Note







Suppression of Anomaly Detection is supported only for VMware ESXi hosts.

Confirmation of Anomaly Detection

You can confirm the measured values in the graph when the anomaly is detected by selecting the [Graph] button for each anomaly that displays on the [Anomaly Detection] tab.

The graph displays the following data for the 90 minutes before and after the time of Anomaly Detection to confirm the status of the anomaly.

Note that the actual measured values displayed in the Anomaly Detection graph may not match the graph data displayed in the vCenter performance chart.

-  : Upper Value of Normal Range after Suppression
-  : Lower Value of Normal Range after Suppression
-  : Upper Value of Normal Range
-  : Lower Value of Normal Range
-  : Measured Value
-  : Location of Anomaly Detection

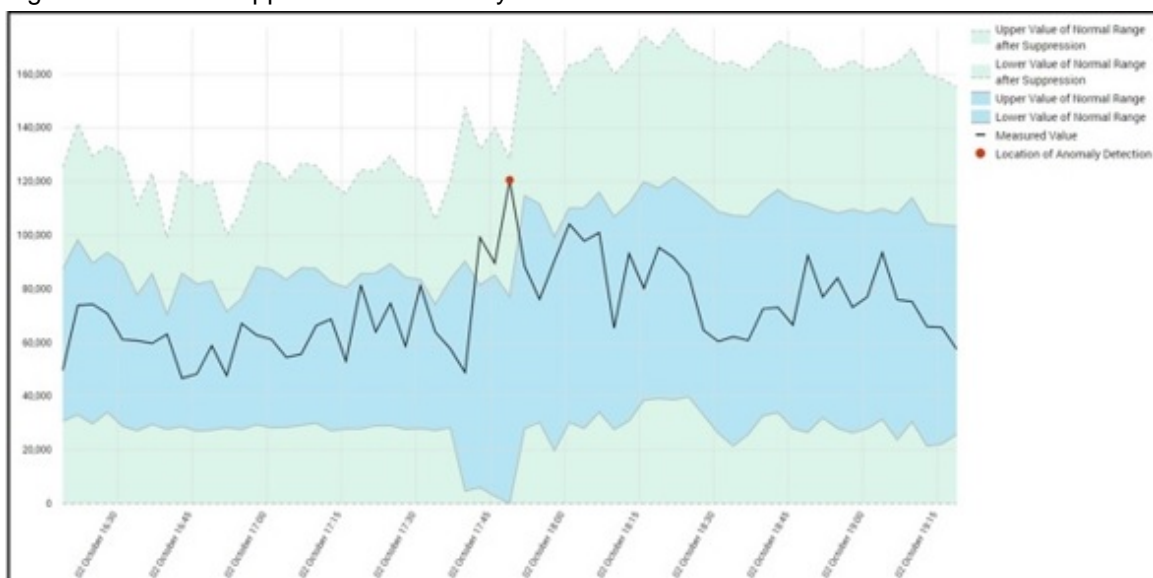
Criteria for determining whether suppression of Anomaly Detection is effective

Use the graph display to check the measured value at the time of detecting the anomalies. The determination is based on whether the “Location of Anomaly Detection (red circle)” displayed in the graph is inside or outside the normal range (green range of upper and lower limit values) after suppression. Note that the upper and lower limit values of the normal range after suppression cannot be set arbitrarily.

When suppression of Anomaly Detection is determined to be effective

When the “Location of Anomaly Detection (red circle)” is inside the normal range after suppression (green range of upper and lower limit values) ([Figure below](#)), suppression of Anomaly Detection works effectively.

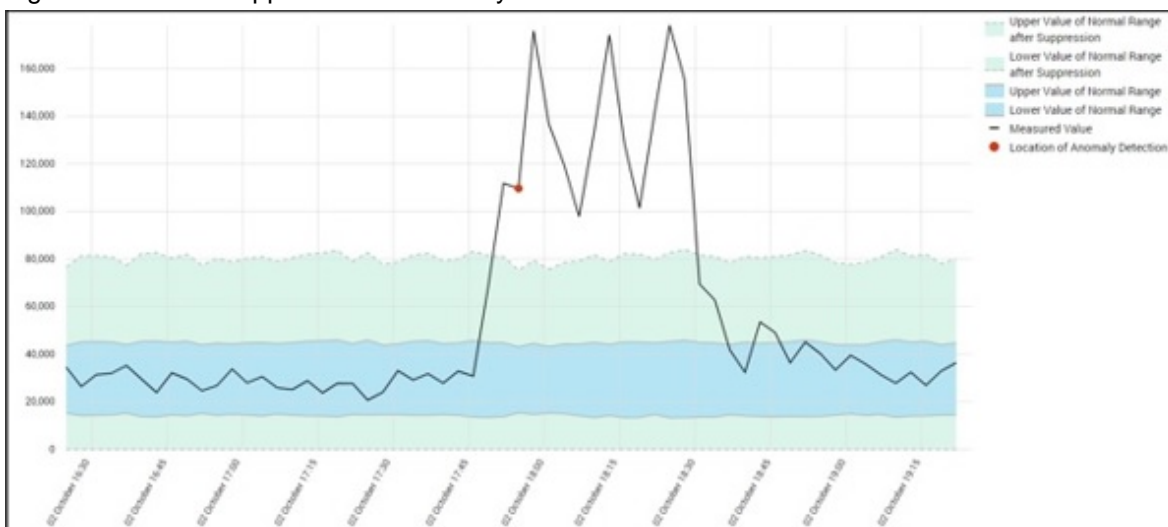
Figure 2.10 When suppression of Anomaly Detection is determined to be enabled



When suppression of Anomaly Detection is determined to be not effective

When the “Location of Anomaly Detection (red circle)” is outside the normal range after suppression (green range of upper and lower limit values) (Figure below), suppression of Anomaly Detection does not work effectively. In order to determine the anomaly within the normal range after suppression, if the same measured result is retrieved by constant monitoring after suppression, anomaly detection is output.

Figure 2.11 When suppression of Anomaly Detection is determined to be not enabled



Check the target device to be detected the anomalies. If you doubt validity of the result of Anomaly Detection, cancel the Anomaly Detection and recreate the learning data.

Suppression of Anomaly Detection

When you want to suppress the output of Anomaly Detection, select the [Suppress] button for Anomaly Detection. After the suppression, the system learns that the anomaly is within the normal range for the same measured results in the constant monitoring. This prevents the occurrence of events.

Suppresses anomalies for each monitoring target.

Target for Anomaly Detection	
Node	Memory
Storage	Storage
Network Adapter	Physical NIC Packet RX Process Packet TX Process Virtual Switch Port (Send packets dropped)
Virtual Machine	Virtual Machine Virtual Switch Port (Receive packets dropped)

Example: If you have two virtual machines, by suppressing CPU utilization for virtual machine 1 does not suppress CPU utilization for virtual machine 2.

Cancelling Suppression of Anomaly Detection

By canceling the suppression of Anomaly Detection, you can return the status from suppressed anomaly to the unsuppressed status. Cancels suppression for all monitoring items.

To check the occurrence status of the anomalies, refer to “4.11.6.1 Confirm occurrence status of the anomalies” in “Operating Procedures.”

For procedure of the suppression of Anomaly Detection, refer to “4.11.6.2 Suppress Anomaly Detection” in “Operating Procedures.”

For procedure to cancel the suppression of Anomaly Detection, refer to “4.11.6.3 Cancel Suppression of Anomaly Detection” in “Operating Procedures.”

2.3.7 Link with Web Interface of PRIMERGY

The following screens can be displayed on the ISM GUI.

- iRMC web interface screen
- AVR screen: Advanced Video Redirection (video redirection)

In addition, iRMC system information and operating system information can be retrieved and displayed as "Asset Management Info" on the "Node List" screen and Details of Node screen.

For more information on the web interface and video redirection display contents and how to operate them, refer the following documents:

“ServerView Suite iRMC Sx Web Interface” (Sx contains S4 and later versions.)

The iRMC web interface login and AVR access environment uses the iRMC account which specified for the “Communication method” during node registration.

The display of the iRMC web interface is a conventional function, which can be displayed by registering the IP address of iRMC and clicking the URL in “Web IF/URL” in the Details of Node screen. However, this conventional operation requires a login operation every time the screen is displayed.

The new operation is called “iRMC Login” to distinguish it from the old operation.

2.3.7.1 Web interface screen display with iRMC Login



You can display the iRMC web interface directly from the ISM GUI without login operation.

You can view detailed PRIMERGY information (such as system information, OS information, sensor information) from the iRMC web interface screen.

The web interface screens displayed by this function are opened with information browsing privileges. Therefore, the setting operation cannot be executed.

For details on how to display web interface with iRMC login, refer to “3.8 Log in to iRMC directly from ISM” in “Operating Procedures.”

Relay Route Settings

The iRMC login prerequisites that you can access iRMC directly from the management terminal. In a network configuration where the firewall restricts access to iRMC from the management terminal, iRMC login can be executed via relay route. In other words, the relay route is a communication route for configuring a route for relaying within ISM.

It has the following features.

- The relay route is set in correspondence with the management terminal.

Set the IP address of the management terminal for iRMC login via the relay route.

The relay route can be set from any management terminal.

- Up to three relay routes can be set for ISM.

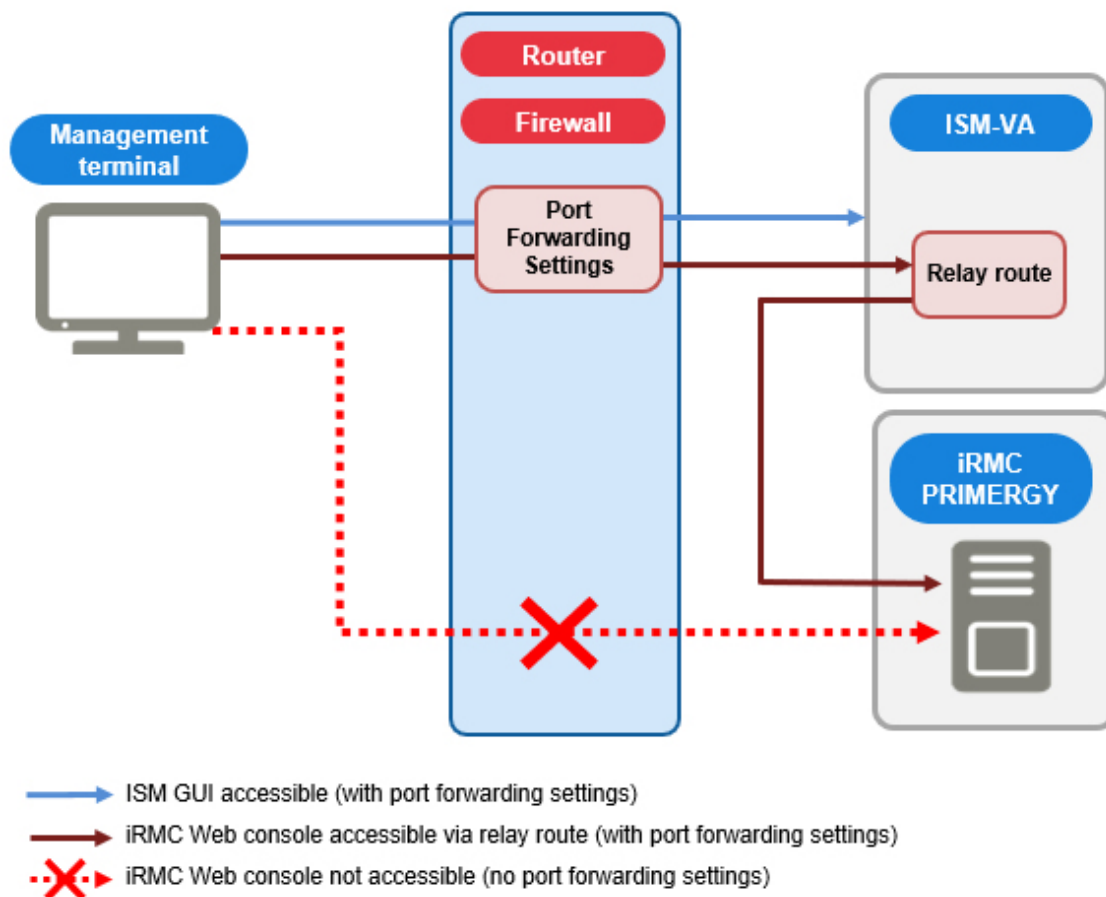
Each of the three relay routes can be assigned to a different management terminal, or all relay routes can be assigned to a single management terminal.

- Only one iRMC connection can be made via one relay route at a time.

The management terminal for which the relay route is set must have a client certificate issued by ISM-VA installed in the browser of the management terminal.

For create the client certificate, refer to “4.28 Creation of Client Certificate for Relay Route.”

Figure 2.12 Relay Route Settings



2.3.7.2 Displaying AVR screen of PRIMERGY



You can start the AVR screen directly from the ISM GUI without login operation.

For details on how to display AVR screen, refer to “6.16 Display iRMC AVR Screen Directly from ISM” in “Operating Procedures.”

For the AVR screen display, setting of the relay route is not supported.

2.3.7.3 Displaying Asset Management Info of iRMC (ISM 3.0.0.010 or later)



You can display the iRMC system information and operating system information as an asset management information on the "Node List" screen and Details of Node screen of the ISM GUI. To display asset management information, select [Asset Management Info] from [Column Display] on the "Node List" screen or the [Asset Management Info] tab on the Details of Node screen.

The following information is displayed:

Item	Description
Node Name	Displays the node names
System Information	Displays the following iRMC system information <ul style="list-style-type: none">- Model Name- Chassis Type- Serial Number- Part Number- Asset Tag- System GUID- BIOS Version
Operating System (OS) Information	Displays the following iRMC operating system (OS) information <ul style="list-style-type: none">- Host Name- Host IP Address(es)- System Description- System Location- System Contact- OS Name- OS Version- OS Up Time- Management Software
Tag	Displays the tag associated to the node Same as the tags in the "Information from OS" screen

For information on the devices that can be displayed asset management information, refer to "Support Matrix."

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

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

Select [DOWNLOADS] and select the target operating system.

The reference procedures are subject to change without notice.

2.4 Profile Management

Profile Management is a function that is mainly used for installation and configuration 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 function groups are displayed below.

Table 2.12 Target nodes and available setting items of Profile Management

Node type	Target node (example)	Function group
Server	PRIMERGY RX PRIMERGY TX PRIMERGY BX PRIMERGY CX	- BIOS settings - iRMC settings - iRMC (User) settings - OS settings - Virtual IO settings - RAID settings
	PRIMEQUEST 2000 series (Partition)	- MMB settings - OS settings
	PRIMEQUEST 2000B	- MMB settings - OS settings
	PRIMEQUEST 3000 series (Partition)	- MMB setup - OS settings - Virtual IO settings (physical partition only)
	PRIMEQUEST 3000B	- BIOS settings - iRMC settings - OS settings
	PRIMEQUEST 4000 series (Partition)	- BIOS settings - iRMC settings - iRMC (User) settings - OS settings - Virtual IO settings
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

Node type	Target node (example)	Function group
		- SNMP, Interface, and NTP settings
Storage	ETERNUS DX	- Creation of RAID groups/volumes - Creation of global hot spares - Host Affinity settings
	ETERNUS NR (Ontap) ETERNUS AX (Ontap) ETERNUS HX (Ontap) ETERNUS AC (Ontap)	- SNMP and NTP settings

Here, the following points are described:

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

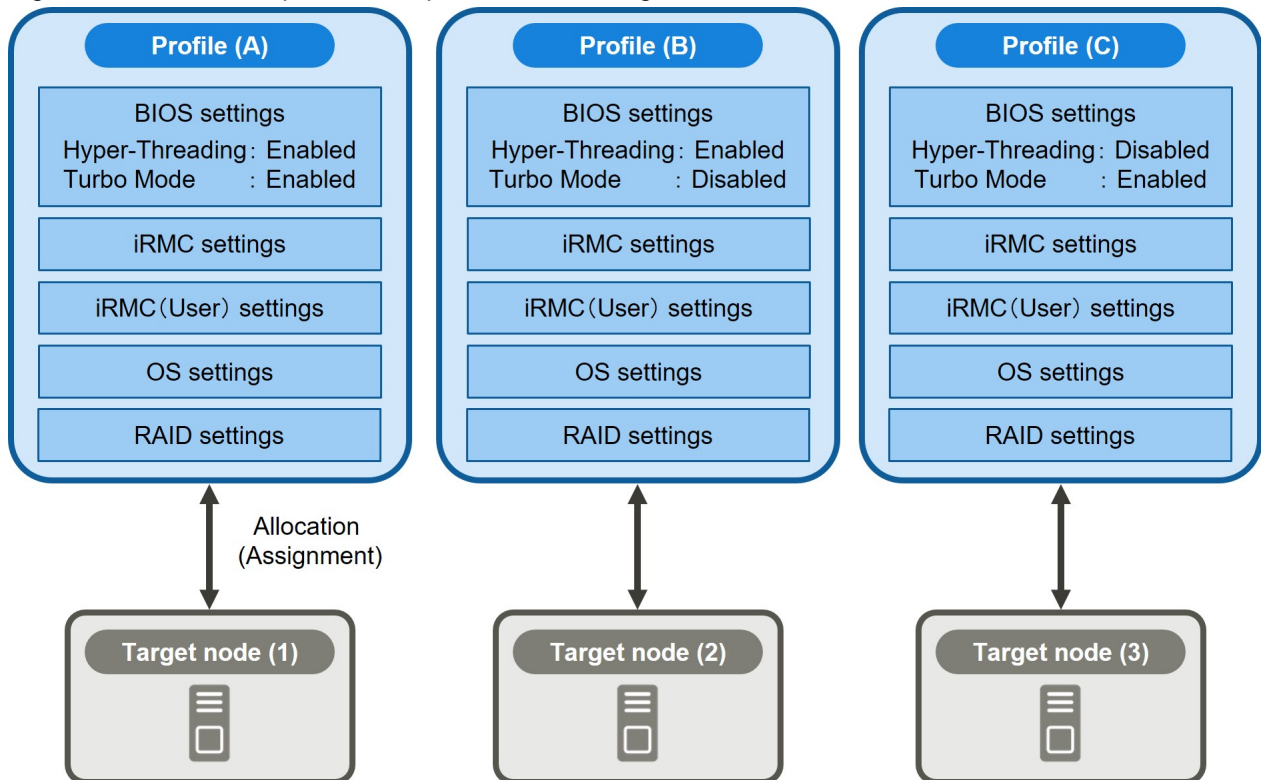
2.4.1 Profile Usage

Before you can use Profile Management to execute node settings, you must record the hardware settings (configuration) of each node and the settings at the time of OS installation in a set of definitions called a “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 one profile is required for each node to be managed by a profile.

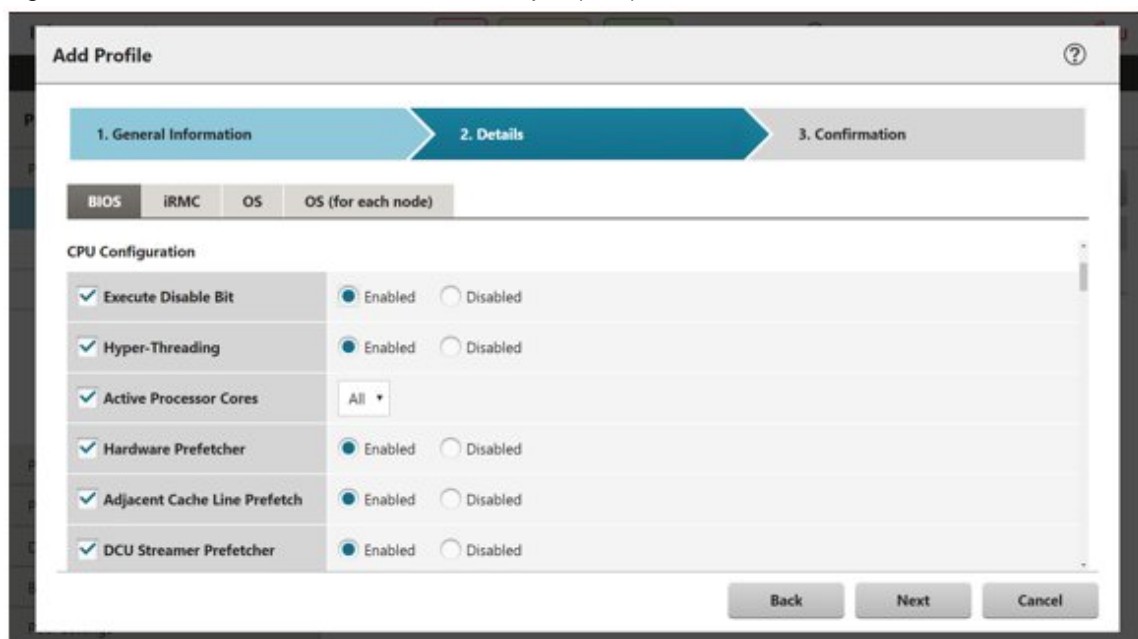
Figure 2.13 Relationships between profiles and managed nodes



Note

When you assign a profile that contains 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 2.14 “Creation of Profile” screen sample (GUI)



2.4.2 Profiles and Policies

Policies are structures that extract those contents to set 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. However, 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.

By retrieving setting items from a node, you can create Profile/Policy for specific model that is specific to the retrieved models. With Profile/Policy for specific model can set more detailed hardware configuration. Profile/Policy for specific model can be assigned to the same model that retrieved the setting items.

The differences between "Profile/Policy" and "Profile/Policy for specific model" are listed below.

Functions of Profile and its required operation	Profile/Policy	Profile/Policy for specific model
Profile assignment range	Assign to the same series such as PRIMERGY RX series	Assign to the specified same models
Creation of profile/policy	Common settings for the same series	Detailed settings for specific model
Operation before creating a profile	Not required	Node registration of the model creating profile is required
Verifying profiles	Supported	Supported
Addition of profiles from Backup	Supported	Not supported
Addition of policies from Backup	Supported	Not supported
Monitoring policy	Supported	Not supported

For Policy, there are existing policy (policies for batch settings: BIOS, iRMC, MMB, OS, RAID) and policy for monitoring. You can create a policy (Monitoring Policy) for monitoring that defines the required settings for monitoring a node regardless of the type of a target server.

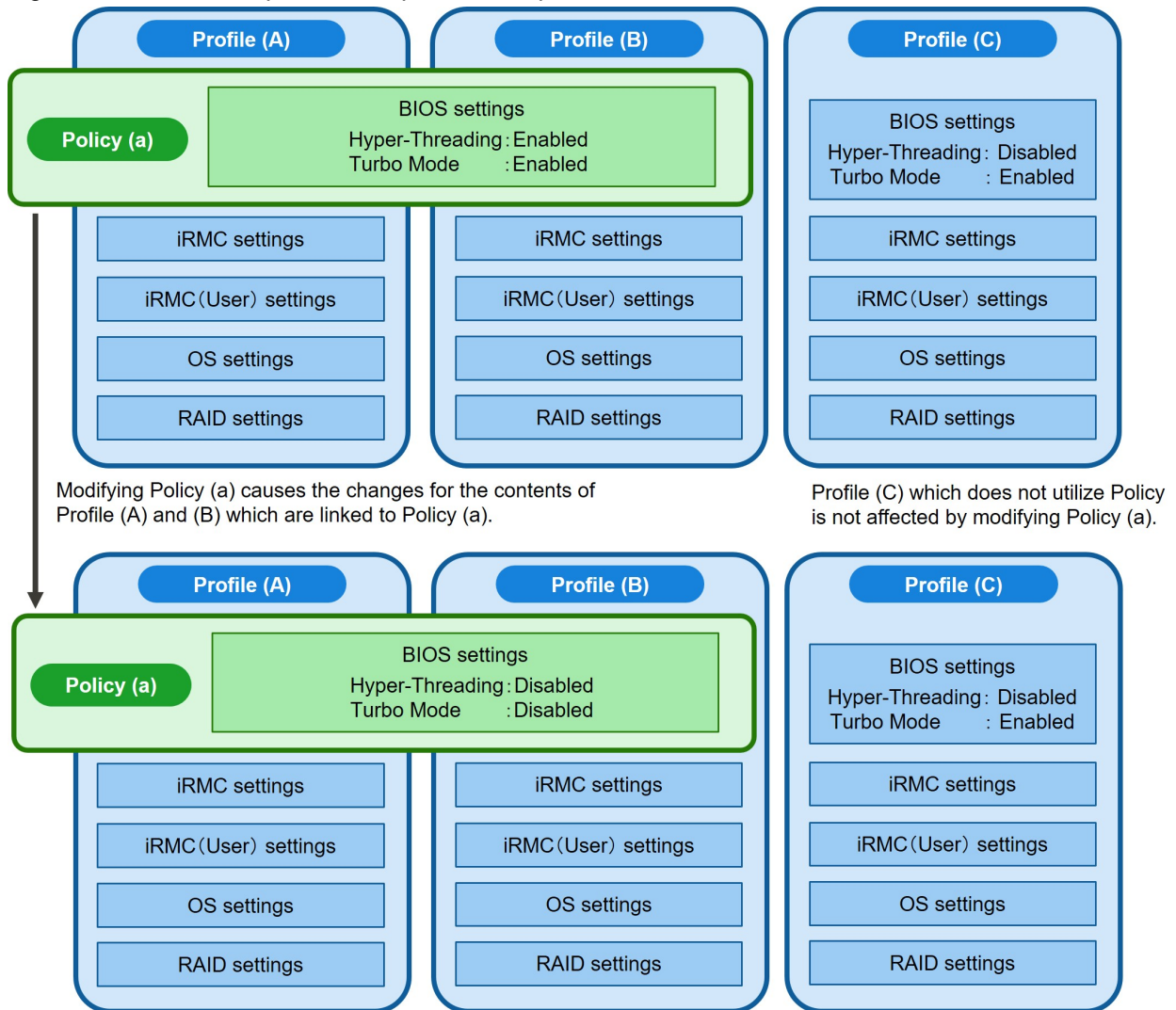
Monitoring policies are similar to existing policies and can be referenced by multiple profiles. A monitoring policy can also be referenced by an existing policy.

If a profile is referencing a monitoring policy, it cannot reference an existing policy that has the same setting items as the monitoring policy. In this case, you must correlate the monitoring policy with the existing policy you want to reference from the profile, and then reference the existing policy from the profile.

One profile is required for each node. For example, in order to set the same contents for the hardware configuration of multiple nodes, you must 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 required number of profiles. This procedure, however, requires that you repeat modifying all profiles, even when you want to change the same settings of all nodes.

In this case, you can use the policy function to create the profiles in advance, and you can then easily change the multiple settings together.

Figure 2.15 Relationships between profiles and policies



Relationships between profiles, existing policies, and monitoring policies

Figure 2.16 Relationships between profiles and an existing policy

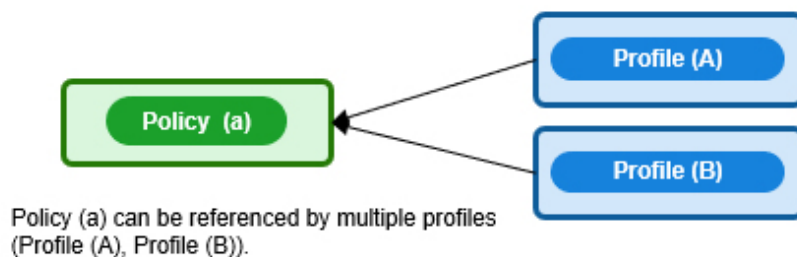


Figure 2.17 Relationships between profiles and a Monitoring Policy

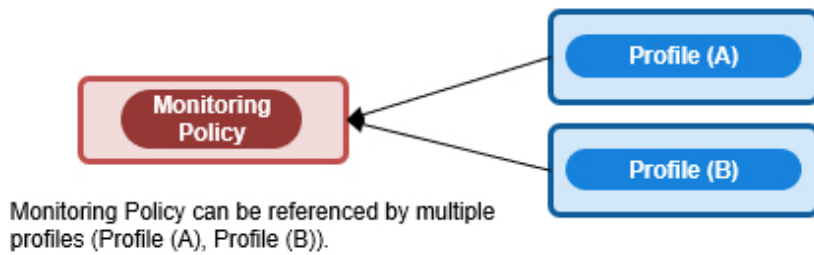
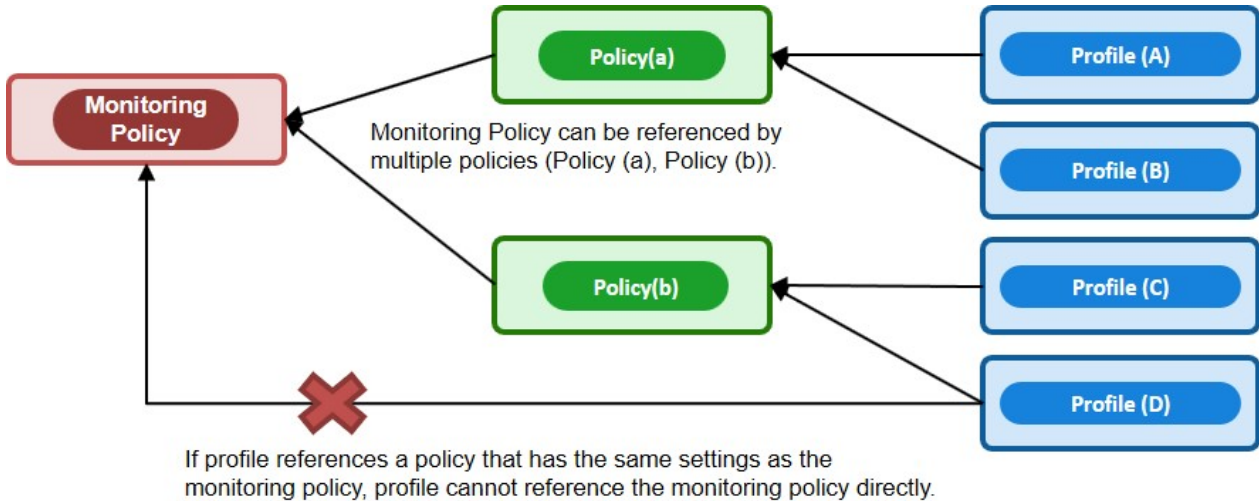


Figure 2.18 Relationships between profiles, existing policies, and a Monitoring Policy



Note

- Profiles and policies contain general setting items that are supported on the target nodes. However, some setting items may not be 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 can install only an OS that is 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, iRMC (User) setting, RAID settings or MMB settings on servers.
- Profile/Policy for specific model can be used for BIOS settings, iRMC settings, and iRMC (User) settings for servers. Profile/Policy for specific model cannot be used at the same time as the existing BIOS settings, iRMC settings, and iRMC (User) settings for the common server types.
- For information on the relationship between Monitoring Policy and profile setting items, refer to “8.1 Monitoring Policy” in “Items for Profile Settings (for Profile Management).”
- If you use a monitoring policy when you create profiles or policies, select the [Enable the monitoring policy] checkbox for Monitoring Policy.

Profile groups and policy groups

Profiles and policies can be managed in groups. 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 ISM GUI, select [Structuring] - [Profiles].
2. From the menu on the left side of the screen, select [Policy Settings].
3. Select the location in which to create a policy group in the tree on the left side of the screen. From the [Actions] button, select [Add Group].

Creating policies

For details, refer to "3.3.4 Create a Policy to Simplify Profile Creation" - "Procedure for creating existing policies" in "Operating Procedures."

Creating monitoring policies

For details, refer to "3.3.4 Create a Policy to Simplify Profile Creation" - "Procedure for creating a monitoring policy" in "Operating Procedures."



Note

- Only users who belong to the Administrator group can create and edit monitoring policies.
- For nodes to which monitoring policy is assigned cannot assign the profile for specific model. To use profile for specific model, do not assign the monitoring policy.

2.4.2.2 Creation of profile groups/profiles



Creating profile groups

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

Creating profiles

For details, refer to Step 1 to Step 5 of "3.3.1 Set BIOS/iRMC/iRMC (User) settings/MMB/Virtual IO/RAID with Profiles" in "Operating Procedures."

2.4.2.3 Assignment of profiles



Note

Executing a profile assignment while you are logged in to the target node with a web operating screen or SSH may result in a profile assignment error.

For details, refer to Step 6 to 9 of "3.3.1 Set BIOS/iRMC/iRMC (User)/MMB/Virtual IO/RAID with Profiles" in "Operating Procedures."

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 "2.14.4 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, changes to the profile do not immediately result in changes to the node settings. ISM handles this status as a mismatch between content of the profile and the node.

Reassign the edited profile to the node when it is convenient. When the reassignment is completed, the node settings change, and it returns to a normal status, where the profile and node settings match.

Reassigning profiles

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Profiles].
2. From the menu on the left side of the screen, select [Profile Settings] - [All Profiles].
The "All Profiles" screen is displayed.
3. Select the profile to be edited.
4. From the [Actions] button, select [Edit] to edit the profile.
5. 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.
6. Select the profile to be assigned.
7. From the [Actions] button, select [Assign/Reassign Profile].
The "Profile Assignment" screen is displayed.
8. Follow the instructions on the screen, and enter the setting items.
For the setting items to be entered, refer to the ISM online help.

Confirming the status of the assigned profile

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

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

The "All Profiles" screen is displayed.

3. Check that the node settings and profiles match.

For the profile that has not been edited, [Assigned] is displayed in [Status].

For the profile whose BIOS/iRMC/Virtual IO/RAID settings have been edited, [Reassignment] is displayed in [Status].

For the profile whose OS settings only have been edited, [Assigned (Differences)] is displayed in [Status].



Note

When [Status] is [Assigned (Differences)], you cannot perform normal re-assignment.

In this case, in the "Profile Assignment" screen, select 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, release any assigned profiles in advance:

- To delete an assigned profile
- To delete a node, which a profile is assigned, from ISM
- To remove a node to which a profile is assigned from its node group, or to modify the node group

For details on node groups, refer to ["2.14.1 User Management."](#)



Point

When replacing a node, you must release the profile. For details, refer to ["5.3 Tasks for Replacing Components."](#)

You do not need to release a profile when resetting iRMC for the device.

Releasing profiles

When a profile is released, the virtual IO settings for the profile are returned to the state they were in before they were assigned. The settings other than the virtual IO settings remain unchanged. In addition, periodic verification of profiles is no longer executed.

1. Power off the server if you want to release a profile that contains Virtual IO settings.
2. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Profiles].
3. From the menu on the left side of the screen, select [Profile Settings] - [All Profiles].
The "All Profiles" screen is displayed.
4. Select the profile to be released.
5. From the [Actions] button, select [Release Profile].

Deleting profiles

The profile definition information on ISM is deleted. This does not affect the node side.

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

2. From the menu on the left side of the screen, select [Profile Settings] - [All Profiles].
The "All Profiles" screen is displayed.
3. Select the profile to be deleted.
4. 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 profiles as text files in JSON format, if, for example, you want to reuse profiles in ISM on another Management server or take out assigned profiles of ISM and store them in another Management terminal.



Point

Policies can also be exported and imported.

Exporting profiles

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Profiles].
2. From the menu on the left side of the screen, select [Profile Settings] - [All Profiles].
The "All Profiles" screen is displayed.
3. Select the profiles to be exported.
4. From the [Actions] button, select [Export].
5. Set an encryption password key (required), and then execute the export with the [Export] button.

Importing profiles

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Profiles].
2. Select the location in which to store the profile in the tree on the left side of the screen. From the [Actions] button, select [Import].
3. Select an option 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 connections and how to transfer to 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 in [Decryption Password Key] when exporting the profiles (required), and then execute the import with the [Import] button.



- The files you transferred to the FTP server of ISM-VA are no longer required after the import has finished. Use an FTP command to delete them.
- Because profiles contain passwords and other security information, you must specify an 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 ISM GUI, 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 ISM GUI, 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 ISM GUI, select [Structuring] - [Profiles].
2. From the menu on the left side of the screen, select [Policy Settings].
3. 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.
4. From the [Actions] button, select [Edit] to edit the policy group.

Deleting policy groups

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Profiles].
2. From the menu on the left side of the screen, select [Policy Settings].
3. 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.
4. From the [Actions] button, select [Delete].

2.4.2.9 Specifying behavior when assigning profiles

You can specify "Assignment Mode" in Profile Assignment by selecting the [Enable Advanced Settings] checkbox when assign/reassign profiles. For servers, you can specify the items to assign for each function group (BIOS settings, iRMC settings, iRMC (User) settings, MMB settings, OS settings, Virtual IO settings, RAID settings).

"Assignment Mode" can be selected from the following.

- "Normal Assignment (Only new and changed portions are applied.)"
This is a default assignment mode. If you are not specifying [Enable Advanced Settings], this mode is used.
- "Assign profile also to unchanged portions"
This setting is executed on a node regardless of whether the node settings match or mismatch the profile settings.
Note, however, that it is not applicable for "OS settings" and "RAID settings." This mode can be specified regardless of the power status of the server (from ISM 3.0.0.010 or later). Note the following:
 - If the setting that includes BIOS settings is specified while the power is on, the settings will be assigned after the next server restart.
 - This mode can be used only on servers with iRMC S4 (version 9.xx or earlier) or iRMC S6 or later.
- "Hot Profile Assignment (with node power remaining on)"
This is the assignment mode for servers. Normally, assigning is executed while the target node is powered off, but you can specify this mode when assigning a profile while the target node is powered on. Note the following:
 - The settings will be assigned after the next server restart.
 - This mode cannot be used on the servers with iRMC S5.
 - This mode cannot be used on the servers with iRMC S4 and iRMC version 9.xxF or later.
- "Handle profile as assigned in ISM without actually assigning it to the node"
When there is a "mismatch" between the profile settings and the node settings, this is used to change the settings on the profile on the ISM side and make them match without assigning the profile. This mode is not displayed unless the profile has been edited.

When you select multiple nodes to assign profiles, you can specify the assignment mode from the "Assignment Mode" pull-down box for batch editing. You can also select the check boxes of applicable function groups to specify.

2.4.2.10 Verifying profiles



If you change the BIOS/iRMC settings for the server directly after assigning a profile, the BIOS/iRMC settings for the server may be different from the settings for the assigned profile. By executing verification of the profile, you can check if the BIOS/iRMC settings for the server match the assigned profile and you can confirm that there are no discrepancies. Verification is executed only on the server.

Execution status or execution results of the verification of profiles are displayed in [Verify Status] of the GUI. If there are discrepancies between the BIOS/iRMC settings for the server and the profile settings, a message is displayed to the event and [Mismatch] is displayed in [Verify Status]. When [Verify Status] is [Mismatch], check the setting items that are different in the applicable profile, and determine that the node settings were intended to change. You must change the status to [Match] in [Verify Status] by reassigning profiles or editing profiles to match the BIOS/iRMC settings for the server and the settings of the profile.

Verification of profiles is available for the following settings:

Server	Functional group to be verified	Functional group not subject to be verified
PRIMERGY	<ul style="list-style-type: none">- BIOS settings- iRMC settings- iRMC (User) settings	<ul style="list-style-type: none">- OS settings- Virtual IO settings- RAID settings
PRIMEQUEST 3000B	<ul style="list-style-type: none">- BIOS settings- iRMC settings	<ul style="list-style-type: none">- OS settings

Server	Functional group to be verified	Functional group not subject to be verified
PRIMEQUEST 4000	<ul style="list-style-type: none"> - BIOS settings - iRMC settings - iRMC (User) settings 	<ul style="list-style-type: none"> - OS settings - Virtual IO settings

Verification of profiles can be executed for the profiles whose status are as follows:

- Assigned
- Reassignment
- Assigned (Differences)

This function enables or disables verification of profiles (automatic execution at approximately every 24 hours and manual execution at any time) by using the enable/disable command for verification of profiles of ISM-VA Management. For details on the commands, refer to "[4.24 Settings for Enabling/Disabling Verification of Profiles](#)."

When it is disabled, [Verify Status] for the target profile is displayed as [- (hyphen)].

Immediately after it is enabled, the [Verify Status] for the target profile is displayed as [Verify Failed]. The appropriate [Verify Status] is set by executing periodic automatic verification of profiles or manual verification at any time.

Here, the following points are described:

- [Procedures to execute verification of profiles at any time](#)
- [Procedures to check the items that do not match when \[Verify Status\] is \[Mismatch\]](#)

Procedures to execute verification of profiles at any time

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

For details, refer to "3.3.5 Compare Assigned Profiles and Hardware Settings" - "Procedures to execute the verification of profiles" in "Operating Procedures."

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

For details, refer to "3.3.5 Compare Assigned Profiles and Hardware Settings" - "Procedures to check the items that do not match when [Verify Status] is [Mismatch]" in "Operating Procedures."



Point

- To confirm the BIOS settings with verification of profiles, the backup files of the BIOS parameters must be saved on the server. Therefore, when you assign a profile, enable [Automatic BIOS Parameter Backup] in the iRMC settings for the profile.
- If the setting for [Automatic BIOS Parameter Backup] is disabled in the iRMC settings for the server or if the server does not have this setting, verification of profiles can not be executed with the latest BIOS settings. In this case, execute the verification of profiles (refer to "[Procedures to execute verification of profiles at any time](#)") after you have backed up the hardware settings for the BIOS (refer to "[2.10.1 Backup of the File of Backup Hardware Settings](#)"). To check the existence of the [Automatic BIOS Parameter Backup] settings in the iRMC settings for the server, refer to the following manuals.
 - "ServerView Suite Remote Management iRMC S2/S3 - integrated Remote Management Controller"
 - "ServerView Suite iRMC Sx Web Interface" (Sx is version S4 or later.)
- If the node is in Maintenance Mode, ISM will not routinely execute verification of profiles. In this case, manually execute verification of profiles.
- There are settings that are not applicable for profile verification. The settings that are not verified are as follows.
 - iRMC settings: [Proxy Server] - [Password]
 - iRMC settings: [LDAP] - [Authentication LDAP Password]

- iRMC settings: [User Management] - [Change Admin Password]
- iRMC (User) settings: [Add User•Edit User] - [User information] - [Password]
- iRMC (User) settings: [Add User•Edit User] - [User information] - [Password (for confirmation)]
- iRMC (User) settings: [Add User•Edit User] - [User information] - [Description]
- If a profile has been assigned with the following settings on the "Profile Assignment" screen, [Verify Status] will be [Verify Failed]. In this case, manually execute verification of profiles.
 - [Assignment Mode]: "Handle profile as assigned in ISM without actually applying it to the node."
[Assignment Mode] is an option that can be selected when the [Enable Advanced Settings] checkbox is selected.
 - [Status]: [Not assigned]



Note

- Verification of profiles may fail in some iRMC firmware versions if LDAP is enabled in the iRMC settings, and HTTP is specified as the protocol in [Web I/F URL] on the Details of Node screen. In this case, edit the node information to set HTTPS in [Web I/F URL] as the protocol. For information on editing nodes, refer to "[2.2.3 Editing of Datacenters/Floors/Racks/Nodes.](#)"
- The server must be restarted in the following cases.
 - When "Assign profile also to unchanged portions" is selected, and assigned the profile while the server is turned on
 - When assigned with "Hot Profile Assignment (with node power remaining on)"

Before restarting the server, the [Verify Status] may be [Match] even though the following settings are different from the actual server status. In this case, there may still be running or pending tasks on the iRMC Task Manager. Restart the server to complete all these tasks. Then execute the verification again.

- [Verify Status]
- Discrepancy between the profile settings and the BIOS/iRMC settings of the server
- When assigning/reassigning profile of BIOS settings (for specific model), the server must be restarted. [Verify Status] will be [Mismatch] before restarting the server (ISM 3.0.0.010 or later). To resolve the mismatch, restart the server and execute the verification of profiles again.

2.4.3 RAID Settings

You can specify the RAID configuration in Profiles

There are two methods to configure RAID. Note, however, that you can specify one or the other. If both "RAID Settings" and "OS Settings" are specified, RAID configuration is executed in "RAID Settings".

- How to specify RAID in "RAID settings"
- How to specify RAID in "OS settings"

This section describes how to specify RAID in "RAID settings" in the function group.

This method is specified in the [RAID] tab in profiles. The RAID configuration is part of the process on the iRMC side. This method requires that RAID has not been configured on the iRMC GUI.

You can specify the RAID level, number of disks, and number of disk groups for the RAID configuration. You can specify number of disk groups when the RAID level is RAID1+0.

If you do not manually set the number of disks in the [RAID] tab, the following rules apply to the number of disks in a RAID configuration. If there are not enough disks, an error occurs. If there are extra disks, they are not used:

RAID level	Number of disks
RAID0	1

RAID level	Number of disks
RAID1	2
RAID1+0	4
RAID1E	4
RAID5	3
RAID6	4



Note

- The RAID array configured with "RAID settings" cannot be deleted (initialized) by releasing profiles. To initialize the RAID array, operate the iRMC of the target device to delete the RAID array.
- If the RAID array has already been configured on the iRMC settings, the RAID configuration with "RAID settings" will fail. Operate the iRMC of the target device to delete the RAID array.
- Note that when the RAID array specified in "RAID Settings" has already been configured, an additional RAID group will be created if there are extra disks connected for the number of disks specified in the settings.

2.4.4 OS Installation Settings

Set a profile for the OS installation.

The following two methods can be used to install an OS.

- Using the PXE boot function

The PXE boot function is used to install an OS on a server by using Profile Management. It is also used to perform Offline Update for servers or mounted PCI cards by using Firmware Management. For details on the settings to use PXE boot function, refer to "[A.1.1 DHCP/PXE Settings in Using Profile Management/Firmware Management](#)."

- Using the ServerView embedded Lifecycle Management function

An installation using ServerView embedded Lifecycle Management (hereafter referred to as "eLCM") uses eLCM of iRMC and embedded Installation Management (hereafter referred to as "eIM") provided by eLCM. This function can be used when the installation target servers are PRIMERGY, PRIMEQUEST 3000B, or PRIMEQUEST 4000 series.

To use eLCM, it is recommended to configure the Repository Server. The downloading time for eIM can be reduced by using Repository Server.



Point

For the procedures to configure and check the Repository Server environment, refer to "ServerView Repository Server - Installation and User Guide" on the following Fujitsu/Fsas Technologies Manual Server site.

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

Reference Procedure

Select "Select a new Product" - [Product Search]. Enter "Repository Server" and select [Continue].

Download from [Documentation] - [Setup Guide].

Reference procedures are subject to change without notice.

Required preparations for OS installation (Common)

- The OS installation media must 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](#)."

Required preparations for OS installation (for using PXE boot function)

- The ServerView Suite DVD must be imported on ISM-VA in advance.

Import the ServerView Suite DVD as a user who belongs to the Administrator group and has an Administrator role or an Operator role. Because the repository is shared by all user groups, you do not need to import the DVD into each user group.



The OS installation may fail when multiple ServerView Suite DVDs are imported.

Import only the ServerView Suite DVDs that are compatible with the server where the OS will be installed.

When multiple ServerView Suite DVDs have been imported, delete all unused ServerView Suite DVDs and restart the ISM-VA.

For details, refer to "[2.14.2 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 that PXE booting is enabled from the management LAN. Also, a separate DHCP server is required within the network. Set the DHCP server so that target nodes can lease the appropriate IPv4 addresses during the PXE boot.

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

Required preparations for OS installation (for using eLCM)

- The following preparations are required:

- Preparing the network connection to the management LAN on the target node

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

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

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

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

- Preparing an eLCM environment on a target server

- Downloading eIM to a bootable SD card on iRMC on the target server

If you use eLCM, the ServerView Suite DVD does not need to be imported on ISM-VA.

You can use an iRMC settings profile to set a Repository Server that is required for downloading eIM.

For details, refer to "Chapter 1. BIOS/iRMC Setting Items of Profiles for PRIMERGY/ PRIMEQUEST3000B/4000E Servers" in "Items for Profile Settings (for Profile Management)."

You can update eIM to the latest version from ISM.

- Manual retrieval of the node information after completing the eLCM environment settings and eIM download

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



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

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

Reference procedure

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

Reference procedures are subject to change without notice.



- Only eIM image version 13.19.07 or later can be used with eLCM.
- If you use a server with iRMC S4, the iRMC firmware version that can use eLCM is 9.xx.F or later.

OS installation on a node where RAID is configured in profiles

Edit additional OS settings to the [Assigned] profile of configured RAID settings and reassign it (refer to [2.4.2.4 Editing and reassigning profiles](#)). The status of the RAID configuration on the server side does not change, ISM is not able to check the RAID settings. If you want to check the configured RAID settings, check the iRMC on the target node.



- Do not edit the configured RAID settings. When you edit the RAID settings, an additional RAID group will be created if there are extra disks connected for the number of disks specified in the settings.

Precautions for OS installation (for using PXE boot function)

If there are errors in the network environment settings or the BIOS settings of the target server, the PXE boot may fail and the OS that is already installed on the target server starts. In this case, the server on which the OS would have been installed cannot be shut down from ISM. When the timeout for processing the profile assignment (Task) elapses, processing ends with an error.

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 (Common)

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

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

2.4.5 Virtual IO Settings

Virtual IO settings virtualize the on-board LAN, on-board CNA (Converged Network Adapter), additional LAN, and additional FC (Fiber Channel) ports. This configuration provides the following benefits.

- You can configure how a LAN port operates by changing its MAC address to a specified MAC address (virtual MAC address) instead of the actual MAC address that the LAN interface has.
- You can configure how an FC port operates by changing its WWN to a specified WWN (virtual WWN) instead of the actual WWN that the LAN interface has.
- You can also configure how an FCoE port operates by changing its actual MAC address or WWN to a virtual MAC address or WWN.

These allow for continued operation even if the system board or PCI card is to be replaced without changing port settings. You can also specify network boot settings for each port in the Virtual IO settings. The Virtual IO settings are applied by assigning a profile.



Point

The virtual MAC address and virtual WWN must be unique across all nodes managed with ISM.



Note

- When software that manages virtual IO, such as ServerView Virtual-IO Manager (VIOM), is running, be careful that it does not 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)."
- In the PRIMERGY BX series, when the MMB firmware version is 5.71 or earlier, do not reset the Virtual IO settings from MMB.
- For the PRIMEQUEST 3000 series (Partition), expansion partitions are not supported. Only physical partitions can be set up.
- For the PRIMEQUEST 3000 series (Partition), you must set the IP address and a user account for the iRMC partition. To confirm and modify the settings, refer to the following site.

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

" PRIMEQUEST 3000 Series Enterprise Model Tool Reference (MMB)"

Select "Select a new Product" - [Product Search]. Enter "PRIMEQUEST" and select [Continue].

Select the appropriate model for PRIMEQUEST and download the manual from [Documentation] - [Manuals].

Reference procedures are subject to change without notice.

- Setting an iRMC IP address

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

- Setting an iRMC user account

" 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 the PRIMEQUEST 3000 series (Partition), disable the CSM settings of the BIOS.
- For the PRIMEQUEST 3000 series (Partition), use UEFI. For the method to set UEFI, refer to "4.2 Port Setting" in "Items for Profile Settings (for Profile Management)."
- For PRIMERGY and PRIMEQUEST 3000 series (Partition), you must set the boot number of the port of the LAN card to more than one in the virtual MAC address settings. If there are multiple ports that are boot targets (ports other than a LAN card port exist), check if the boot order is correct (as you have specified).
- If you release a profile that contains Virtual IO settings that have been assigned to the server to which an ISM IP address is set as an SNMP trap destination, the ISM IP address set as an SNMP trap destination will be deleted.

MAC address and WWN virtualization

You can virtualize MAC addresses and WWNs by managing the server's virtual IO (virtual MAC addresses, virtual WWNs, and so on) settings as a profile or by assigning a profile. When replacing managed servers or PCI cards, using profiles reduces the workload for changing the settings of peripheral devices and makes it easy to re-set network information.

Replacing managed servers or PCI cards that use Virtual IO settings are assumed to be executed according to the following procedure.

Figure 2.19 Replacing a managed server that uses Virtual IO settings

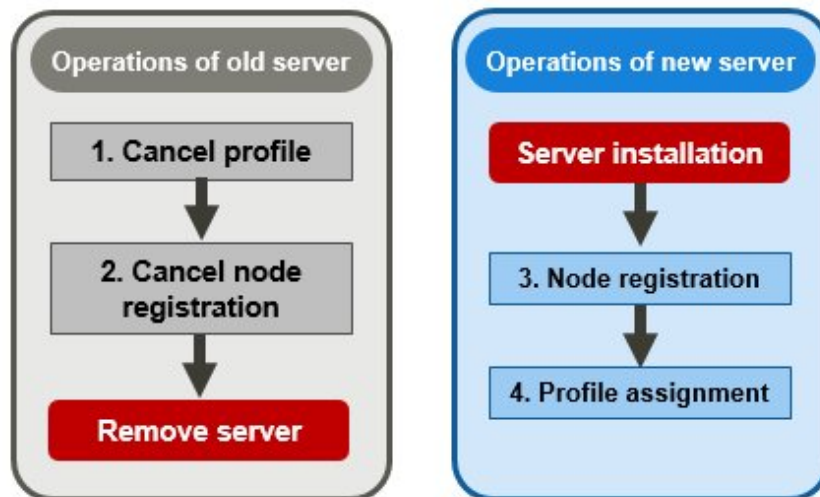
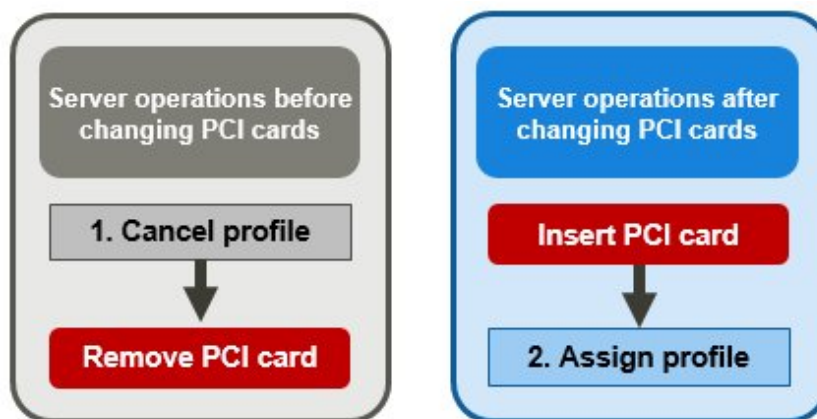


Figure 2.20 Replacing a PCI card that uses Virtual IO settings



Note

Make sure to retrieve the node information after replacing the components of a node such as system boards or PCI cards. Before executing the retrieval of node information, power on PRIMERGY and check that the BIOS screen of the target node is displayed. Retrieving the node information enables ISM to check the status within a node. Retrieve node information before assigning a profile. For retrieval of node information, refer to "2.2.1.3 Management of node information."

2.4.6 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 pools of address ranges that are available to users
- Allocate values from the pool as required
- Return values that are no longer required to the pool

Target resources for pools

The target resources for pools are the following virtual addresses.

- Virtual MAC addresses
- Virtual WWN

The Pool Management function is used when the Virtual IO settings are used 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 also select which values are allocated from the set pool.

If you delete a profile to which the above virtual addresses have been allocated, the deallocated virtual address is returned to the pool.

Here, the following operations are described:

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

Register pool settings

Executable user

Administrator group

Other groups

Admin Operator Monitor

Admin Operator Monitor

1. From the Global Navigation Menu on the ISM GUI, 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 end address of the pool range.
 - Authorized user group
Select a user group that can allocate values from the pool range.
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

Admin Operator Monitor

Admin Operator Monitor

From the Global Navigation Menu on the ISM GUI, 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 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

Admin Operator Monitor

Admin Operator 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 ISM GUI, select [Structuring] - [Profiles] - [Pool Settings].

2. Select the pool you want to edit. From the [Actions] button, select [Edit].
3. Set the required information in the "Edit Pool" screen, and then select [Register].



Note

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

Delete pool settings

	Administrator group	Other groups
Executable user	<div>Admin</div> <div>Operator</div> <div>Monitor</div>	<div>Admin</div> <div>Operator</div> <div>Monitor</div>

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

2.4.7 Confirmation of Boot Information

	Administrator group	Other groups
Executable user	<div>Admin</div> <div>Operator</div> <div>Monitor</div>	<div>Admin</div> <div>Operator</div> <div>Monitor</div>

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

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

2.4.8 iRMC (User) Settings

The iRMC (user) settings allows you to edit user information for local user accounts on iRMC. The main features are as follows.

- Add/Edit

You can add users or edit user information by specifying user information. When applying the profile, the system checks whether the target user exists on iRMC, and then you can either add or edit.

You may access iRMC from ISM using the local user account of iRMC that you added or changed.

- If the user exists, the user information will be edited.
- If the user does not exist, the user will be added.

- Delete

You can delete users by specifying their username. When applying the profile, the system checks whether the target user exists on iRMC, and then deletion is executed.

- If the user exists, the user will be deleted.
- If the user does not exist, no operation is executed on iRMC.



Note

Note the following when its operating on a user of the node that has already been registered in ISM:

- If you specify deletion, profile assignment will result in an error.

- If you change the password, the password of the node that registered in ISM will also be changed.

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 "Types of logs to be collected" and the "Collection schedule" separately for each node.

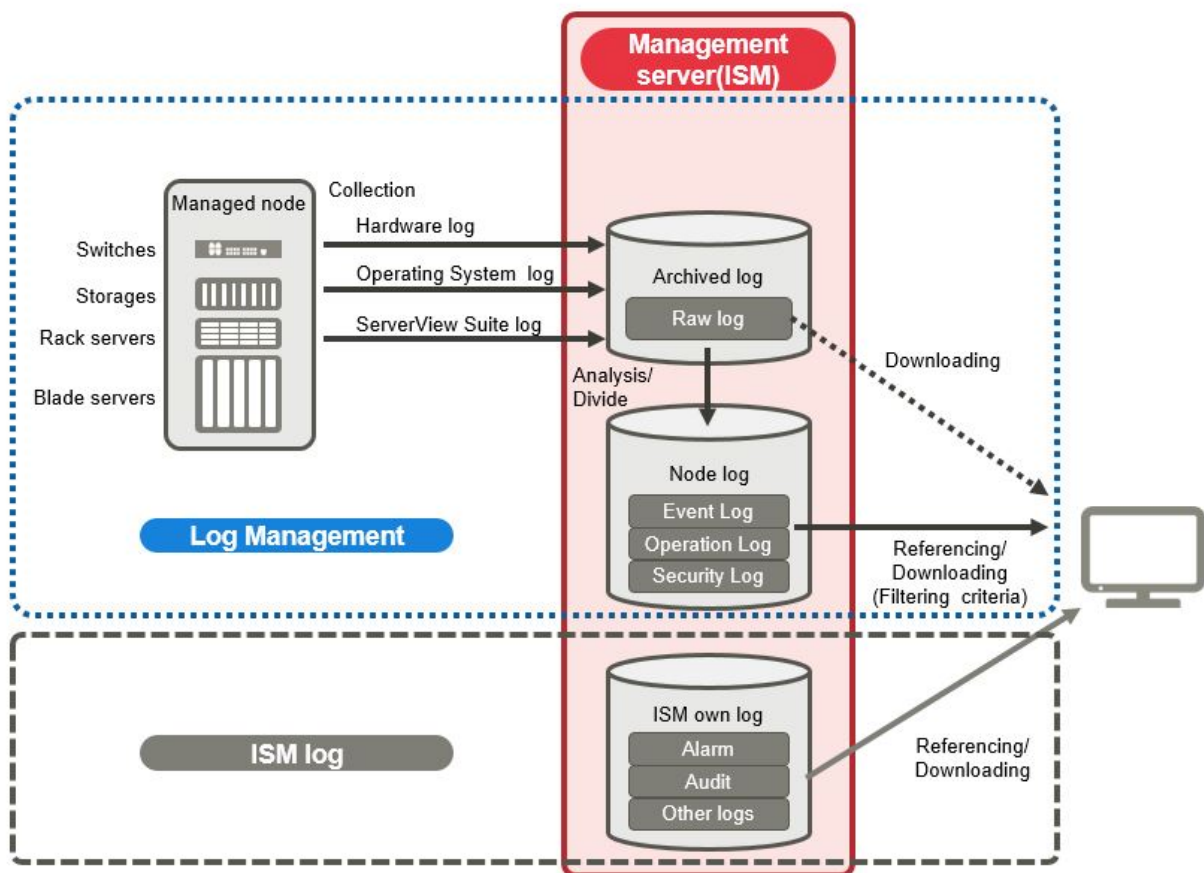
A batch of logs that are collected from nodes according to these settings are called "Archived Logs."

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

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 display in a list or for searching 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. You can filter the display by specifying conditions such as their classification; "Event Logs," "Operation Logs," and "Security Logs," as well as the date and time of occurrence. In addition, you can download the filtered log list as a CSV file or zip files, to the management terminal.

Figure 2.21 Image of Log Management





Note

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, cannot create a 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 logs: hardware logs, operating system logs, and ServerView Suite logs. For supported hardware, OSes, and other details, refer to "Support Matrix."

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

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

Select [DOWNLOADS] and select the target operating system.

The reference procedures are subject to change without notice.

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, GX)	SEL System Report (server with iRMC S4 or later)	SEL
	PRIMEQUEST 3000B		
	PRIMEQUEST 4000 series (Partition)		
	PRIMERGY CX1430 M1	SEL (binary)	None
	PRIMERGY GX		
Chassis	PRIMEQUEST 3000 series (Partition)	SEL Exported results for "opelogview" command	SEL

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 "selview" command Exported results for "configview" command	
Storage	ETERNUS DX/AF	Exported results for "export log" command Exported results for "show events" command	Exported results for "show events" command
	ETERNUS NR (NetApp)	Exported result for "event log show" command	Exported result for "event log show" command
	ETERNUS AB/HB	Retrieval result for "GET xxxx/devmgr/v2/storage-systems/1/audit-log" Retrieval result for "GET xxxx/devmgr/v2/storage-systems/1/mel-events"	None
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		
	SR-S		
	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)
	Cisco Nexus		
	Juniper QFX/EX	Exported results for "request support information" command	None
	Brocade FC 7810 Brocade FC G630/ G720	Various files created with the "supportSave" command	None

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)



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 the "PrimeCollect" command
ServerView Agentless Service	Exported results for the "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 by log classification; "Event Logs," "Operation Logs," and "Security Logs." Also, you can set the number of generations to retain for unclassified "Archived Logs."

You can set arbitrary values for the log retention periods.

The retention periods for "Event Logs," "Operation Logs," and "Security Logs" are specified in 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 - 1,830 days (approximately 5 years).

For "Archived Logs," you must set the number of generations for past log collections that are retained. Each collection operation counts as one generation, 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, the past seven generations of logs are retained. The available setting range is 1 - 366 generations.



Point

- The retention periods and the numbers of retained generations for the log classifications; "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 each, and the logs for the past one year have accumulated on the target 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.

- Confirm that the retention periods are set to optimum values for your operation environment 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 being accumulated 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



By setting log collection on the nodes that are registered in ISM, you can collect logs from the nodes.

Set the following items for the nodes:

- Log Collection Target

As the log types to be collected, you can specify any combination 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, logs will not be collected.

- 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 two 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 must set an execution schedule separately for each node.



Note

After retrieving and confirming information from the nodes, ISM judges whether these nodes are valid 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," or "ServerView Suite Log" settings, which should 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. 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. 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 execute log collection periodically, you must 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 methods to specify the collection schedule as follows:

- Specify by Day of the Week

Here, you can specify the time at which to retrieve logs separately for each day of the week. Specify the day of the week and the time to retrieve logs in the format "Every x-day at hh:mm." Alternatively, you can 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 the 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 at which to retrieve logs 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 ISM GUI, 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 execute the same settings to the multiple nodes.
4. From the [Actions] button, select [Edit Log Collection Settings].

Point

You can edit the log collection settings by using the same operations on the screens described in the following procedure.

1. From the Global Navigation Menu on the ISM GUI, 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 then select the [Log Collection Settings] tab.

Note

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

If you set the time in the time zone that is set on the ISM GUI, regular log collection may not be executed at the expected 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

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

Periodical log collection

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

To have log collections executed periodically, you must 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, the collection is skipped. Log collection will be executed at the next scheduled date and time.

Examples of 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.)
- ISM is executing a different operation for the node
- The node is in Maintenance Mode (manual retrieval is possible)
- ISM is stopped

Whenever log collection fails, the failure is recorded as an error event (logs starting with message ID "5014") under [Events] - [Events] - [Operation Log] in ISM. If log collection fails due to the node is in Maintenance Mode, no error events are registered.

- 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 periodical log collection has been started, you cannot cancel it in the middle of the process. Therefore, if maintenance such as firmware/driver updates, profile assignment, etc. for target nodes is planned, and it overlaps with the periodical log collection execution time, maintenance may fail. You should either disable the periodical log collection or change the setting of schedule.
- There is an upper limit to 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, the log collection will be suspended until log deletion has completed. After log deletion has been completed, log collection 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 the amount of disk space used for log storage

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 (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 setting values for monitoring the amount of disk space used (Threshold monitoring) are set in Edit User Group Settings. For details of User Group Settings, refer to "2.3.2 Manage User Groups" in "Operating Procedures."

If the total size of the various log files approaches the upper limit value for the total size, a warning event is recorded under [Events] - [Events] - [Operation Log] tab in the Global Navigation Menu. If the preset value is exceeded the threshold (when an error event was registered), new logs are no longer stored.

To allow new logs to be retrieved after an error event has been registered, you can either manually delete any obsolete logs for the node on which the event occurred or another node that belongs 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
The total size of log files exceeds the size that is specified for monitoring the amount of disk space used. Example: When the specified upper limit value is 10 GB and the specified value for monitoring the	<ul style="list-style-type: none">- Log collection is executed.- A warning event is output under [Events] - [Operation Log]. The contents of the displayed messages are as follows: <ul style="list-style-type: none">- For Archived Logs

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

2.5.5 Searching Node Logs



You can search the accumulated "Node Logs" 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 ISM GUI, 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.

For the operation using the GUI for filtering logs, refer to "4.8 Display Node Logs" in "Operating Procedures."

Point

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

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.

You can also set a password for the zip file.

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

1. From the Global Navigation Menu on the ISM GUI, 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 on the screens displayed in the following procedure.

1. From the Global Navigation Menu on the ISM GUI, 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 then select the [Log Collection Settings] tab.

- The download files are contained in one zip file even when selecting multiple nodes.



- For the date of the period that you specify in the creation of the download file for the Node Log, specify the date in the time zone of the ISM-VA. If you specify a date in 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 a node that is executing log collection. Create a download file after the log collection has 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. You can also set a password for the zip file.

For the operation using the GUI for downloading logs, refer to "4.9 Download Archived Logs" in "Operating Procedures."

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. However, 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 logs.

Data for download and data for log search are deleted simultaneously if they 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 ISM GUI, 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 the deletion process is complete. In this case, on the "Tasks" screen, confirm in the relevant task that the deletion process has 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, in the deletions conditions, select all log types in [Type] and specify the date to perform deletion in [Period], and you can delete in a short time.
- For log deletion executed for nodes where Node Logs are currently being collected, the deletion will be suspended until log collection has been completed. Deletion will be executed after log collection has completed.

2.5.9 Deleting Archived Logs



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

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

1. From the Global Navigation Menu on the ISM GUI, 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 that is displayed when you select [Display Archived Log Files] from the [Actions] button.
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 the deletion process is complete. In this case, on the "Tasks" screen, confirm in the relevant task that the deletion process has completed, and then open this screen again.
- For log deletion executed for nodes where logs are currently being collected, the deletion will be suspended until log collection has been completed. Deletion will be executed after log collection has completed.

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 ISM GUI
- Confirming the documentation that is supplied with the firmware data
- Updating the firmware on managed nodes using firmware data
- Updating the firmware/driver on managed nodes using ServerView embedded Lifecycle Management

Firmware Management is available for the following nodes:

- Servers and any mounted PCI cards
- Storage
- Switches

For details on the target nodes, refer to "Support Matrix."

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

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

Select [DOWNLOADS] and select the target operating system.

The reference procedures are subject to change without notice.

Here, the following points are described.

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

2.6.1 Confirmation of Firmware Versions



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 ISM GUI, select [Management] - [Nodes].
3. In the [Column Display] field, select [Firmware/Driver].
4. Confirm the [Current Version] field.
The [Current Version] field displays the currently running firmware version.

2.6.2 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 for Online Update for the iRMC/BIOS of a server differs from the "Online Update" of the documents supplied with the firmware data. For Online Update for the iRMC/BIOS of a server, 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 confirm the documentation

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Firmware/Driver].
2. From the menu on the left side of the screen, select [Update].
3. Select the [Current Version] field, the [Latest (Online)] field, or [Latest (Offline)] field of the node whose documentation you want to confirm.
The "Firmware Document" 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 from the screens displayed in the following procedure.

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

If selecting the imported firmware data to confirm the documentation

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Firmware/Driver].
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 whose documentation you want to confirm.
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 ISM GUI, select [Structuring] - [Firmware/Driver].
2. Select the checkbox for the node to be updated. From the [Actions] button, select [Update Firmware/Driver].
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.



.....

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

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

The following procedure is the same as the above.

.....

2.6.3 Firmware/Driver Update

2.6.3.1 How to update firmware

Using Firmware Management, five methods for updating the firmware are available.

How to update and requirements

Select the applicable procedure that matches the operational method of the node you are managing and the following usage conditions.

- Online Update
 - For BIOS/iRMC
Firmware update is available regardless of the status of the operating system.
Execute the firmware update to the iRMC.
 - For PCI card
Execute the firmware update while the OS is operating
Execute the self-deploying software package of the target component on the OS to update the firmware.
- Offline Update
PXE boot temporarily starts a dedicated OS and updates the firmware by executing the self-deploying software package of the target component on the OS.
- eLCM Online Update
The eLCM function allows for firmware/driver and software updates to be executed while the OS is operating, in conjunction with ServerView Agents or Agentless Service running on the OS.
You can update the firmware without selecting the target firmware version.
- eLCM Offline Update
The eLCM function temporarily starts a dedicated image on the iRMC and update the firmware by executing the self-deploying software package of the target component.
The eLCM function allows users to update the firmware without selecting the target component and firmware version.
- eLCM Offline Update (SimpleUpdate)
The eLCM function temporarily starts a dedicated image on the iRMC and update the firmware by executing the self-deploying software package of the target component.

How to update	Requirements				
	Firmware data to be used	Optional selection of target components	Power status of the server at runtime	eLCM license on the target server side	Notes
Online Update	Data imported into ISM Data format <ul style="list-style-type: none"> - For BIOS/iRMC: binary data - For PCI cards: ASP [Note] 	Enable	<ul style="list-style-type: none"> - For BIOS/iRMC: Power On or Power Off - For PCI card: Power On 	Not required	For PCI cards, note the following: <ul style="list-style-type: none"> - ISM must be configured to log in to the OS of the target node. - Supported only when the OS of the target node is Windows or Linux. The supported OS varies depending on the card type. - When importing the firmware data individually, obtain the ASP for the target component according to the OS from the Fujitsu/Fsas Technologies website. - The OS of the target node must be rebooted after the update is completed.
Offline Update	Data imported into ISM Data format: ASP [Note]	Enable	Power Off	Not required	<ul style="list-style-type: none"> - The OS on the target node must have a network connection to ISM (not just a connection to iRMC). - The dedicated OS for the PXE boot is contained in the ServerView Suite Update DVD. The applicable DVD must be imported into ISM in advance. - The dedicated OS for PXE boot is a Linux-based OS. When importing the firmware data individually, obtain the ASP for the target component from the Fujitsu/Fsas Technologies website.
eLCM Online Update	Data downloaded by iRMC from the firmware repository server Data format: ASP [Note]	Enable	Power On	Required	<ul style="list-style-type: none"> - Supported only when the OS of the target node is Windows, Red Hat Enterprise Linux, and SUSE Linux Enterprise Server. - ServerView Agents or Agentless Service must be installed on the OS of the target node.

How to update	Requirements				
	Firmware data to be used	Optional selection of target components	Power status of the server at runtime	eLCM license on the target server side	Notes
eLCM Offline Update	Data downloaded by iRMC from the firmware repository server Data format: ASP [Note]	Disable All components in the target node	Power Off	Required	
eLCM Offline Update (SimpleUpdate)	Data imported into ISM Data format: ASP [Note]	Enable	<ul style="list-style-type: none"> - To update at next startup: Power On - For immediate updates: Power Off 	Required	<ul style="list-style-type: none"> - For PCI card, the firmware tool must be imported into ISM in advance. - The dedicated image is a Linux-based OS. To import firmware data individually, obtain the ASP for the component from the Fujitsu/Fsas Technologies web site.

[Note]: ASP (Autonomous Support Packages) is a firmware update program for the self-deploying software package.

For information on the devices supported as update target, refer to "Support Matrix."

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

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

Select [DOWNLOADS] and select the target operating system.

The reference procedures are subject to change without notice.

Required preparations for using Offline Update

When you execute Offline Update on a server (BIOS/iRMC/mounted PCI card), the following preparations are required.

- The ServerView Suite Update DVD must 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.

For details, refer to "[2.14.2 Repository Management](#)."

- Use the PXE boot function on the target node.

The management LAN used for PXE boot can be set from the [Firmware/Driver] tab in the Details of Node screen. You can also execute this setting on the "Node List" screen that is displayed when you select a target node 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. Also, 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](#)."

- Check the boot mode in the BIOS settings.

Select the same boot mode as the BIOS settings for [Boot Mode] in the "Update Firmware/Driver" wizard when you execute Offline Update. If [Boot Mode] is different from the BIOS settings, PXE boot may fail.



Note

The required firmware data may differ between "Online Update" and "Offline Update." Also, the support scope varies depending on the type of device. For details, refer to "Support Matrix."

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

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

Select [DOWNLOADS] and select the target operating system.

The reference procedures are subject to change without notice.

2.6.3.2 Behavior during firmware 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 following tables.

Table 2.13 Online Update

Type	Behavior during and after updates
Server (iRMC)	Updates are executed regardless of whether the server power is on or off.
Server (BIOS)	<p>Updates are executed regardless of whether the server power is on or off.</p> <ul style="list-style-type: none">- If you execute an update with the power 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 convenient. 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 on the power from the Details of Node screen, etc., in ISM. After you turn on the power, check the following:<ul style="list-style-type: none">- The BIOS version of the server has been updated- In the iRMC system event log, no errors have occurred during the update- If you execute an update with the power turned off You must turn on the server power again in order to switch to the new firmware (BIOS). When the firmware update completes, the server power turns on automatically, and then turns off. After the power has turned off, you can switch to the new firmware by turning on the power from the Details of Node screen, etc., in ISM. After you turn on the power, check the following:<ul style="list-style-type: none">- The BIOS version of the server has been updated- In the iRMC system event log, no errors have occurred during the update
Server (PRIMEQUEST firmware, excluding PRIMEQUEST 4000 series) [Note]	Updates are 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 convenient.
Switch (except CFX) Storage	Execute the firmware update with the node power on. After the firmware update, the node may be rebooted.
Switch (CFX)	Execute the firmware update with the node power on. You must reboot the node in order to switch to the new firmware. You can execute the reboot whenever convenient. Depending on the system

Type	Behavior during and after updates
	configuration, network connections may be broken when rebooting. Take your system configuration into account when rebooting.

[Note]: The PRIMEQUEST firmware is an integrated firmware that includes the following firmware.

- For PRIMEQUEST 2000/3000 series: BIOS firmware, iRMC firmware, MMB firmware
- For PRIMEQUEST 4000 series: BIOS firmware, iRMC firmware

The individual firmware included in the integrated firmware cannot be updated individually.

Table 2.14 Offline Update

Type	Behavior during and after updates
Server (iRMC)	Updates are executed with the server power off. During the firmware update, the server may be turned on or restarted, and after the firmware update is complete, the power is turned off. 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. After the firmware update has been completed, the node will automatically be switched over to the new firmware. Some servers do not update their version display after the update is complete. If the following message appears in a subtask, turn on the server, and then obtain the node information from the Details of Node screen of ISM. Action: To check if the firmware update is complete, you must restart the device. Restart the device according to the procedures for the device. Check that the device is powered on, and then check that the firmware is updated to execute [Get Node information] on the [Details of Node] screen.
Server (BIOS)	
Server (with mounted PCI card)	
Server (PRIMEQUEST firmware) [Note]	Updates are executed with the server power off. For the PRIMEQUEST 4000 series, updates are executed with powered off of all partitions. During the firmware update, the server may be turned on or restarted, and after the firmware update is complete, the power is turned off. After the firmware update has been completed, the node will automatically be switched over to the new firmware.

[Note]: The PRIMEQUEST firmware is an integrated firmware that includes the following firmware.

- For PRIMEQUEST 2000/3000 series: BIOS firmware, iRMC firmware, MMB firmware
- For PRIMEQUEST 4000 series: BIOS firmware, iRMC firmware

The individual firmware included in the integrated firmware cannot be updated individually.

2.6.3.3 Execution of a script during updates

You can execute an arbitrary script saved on an external host before or after the update of target nodes.

You can use this feature when you want to shut down target nodes in advance on which you are executing Offline Update, when you want to reboot target nodes after the completion of Online Update, and other cases.

Macro

The macro (automatic variable) functions displayed below can be used to specify parameters when executing scripts. These macros are automatically replaced with the information of the node.

The details for each macro is as follows.

Macro notation	Overview
\$_TRGID	Node ID of a node on which to execute updates
\$_TRG	Node name of a node on which to execute updates
\$_IPA	IP address of a node on which to execute updates
\$_MDL	Model name of a node on which to execute updates
\$_OSIP	IP address of the OS on a node on which to execute updates
\$_OSTYPE	OS type of a node on which to execute updates
\$_PSKIND	Type of a script file



Point

.....

If the OS information is not registered in the node on which to execute updates, "none" is output.

.....

Preparations for executing a remote script

For preparation, refer to "2.3.3 Action Settings" - "Required preparations before using an action" - "Execute Remote Script."

Procedure for registering a script file

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Firmware/Driver].
2. From the menu on the left side of the screen, select [Script].
The "Script List" screen is displayed.
3. From the [Actions] button, select [Add].
4. Register the remote script file according to the instructions on the screen.
5. On the firmware update screen, select the script to execute during the update.



Point

-
- On the "Script Settings" screen of update, you can set Waiting Time in seconds for Pre-script for update and Post-script for update.
 - The waiting time of the pre-script for the update is the time from when the pre-script is executed to the time the update is executed.
 - The waiting time of the post-script for the update is the time from when the update has completed to the time the post-script is executed.

- If you enable "Execute Post-script for Firmware/Driver Update when firmware update is failed." on the "Script Settings" screen of Update Firmware/Driver, the post-script for an update that has been set will be executed.

In the following case, the post-script for an update is not executed even when the setting is enabled.

- The execution of the pre-script for an update has ended abnormally.
 - The update ended abnormally due to an error in the power source status of the target device.
-

Procedure for testing a script

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Firmware/Driver].
2. From the menu on the left side of the screen, select [Script].
The "Script List" screen is displayed.
3. From the "Script List" screen, select a script in which to execute the test.

4. From the [Actions] button on the right side of the screen, select [Test].
The "Script test" screen is displayed.
5. Select the [Test] button on the right side of the screen and execute the test of script.

When executing a test, the macro that is set for the script information will be replaced with the following character string.

Macro	Character string after replacement
\$_TRGID	TEST_TRGID
\$_TRG	TEST_TRG
\$_IPA	TEST_IPA
\$_MDL	TEST_MDL
\$_OSIP	TEST_OSIP
\$_OSTYPE	TEST_OSTYPE
\$_PSKIND	TEST_PSKIND

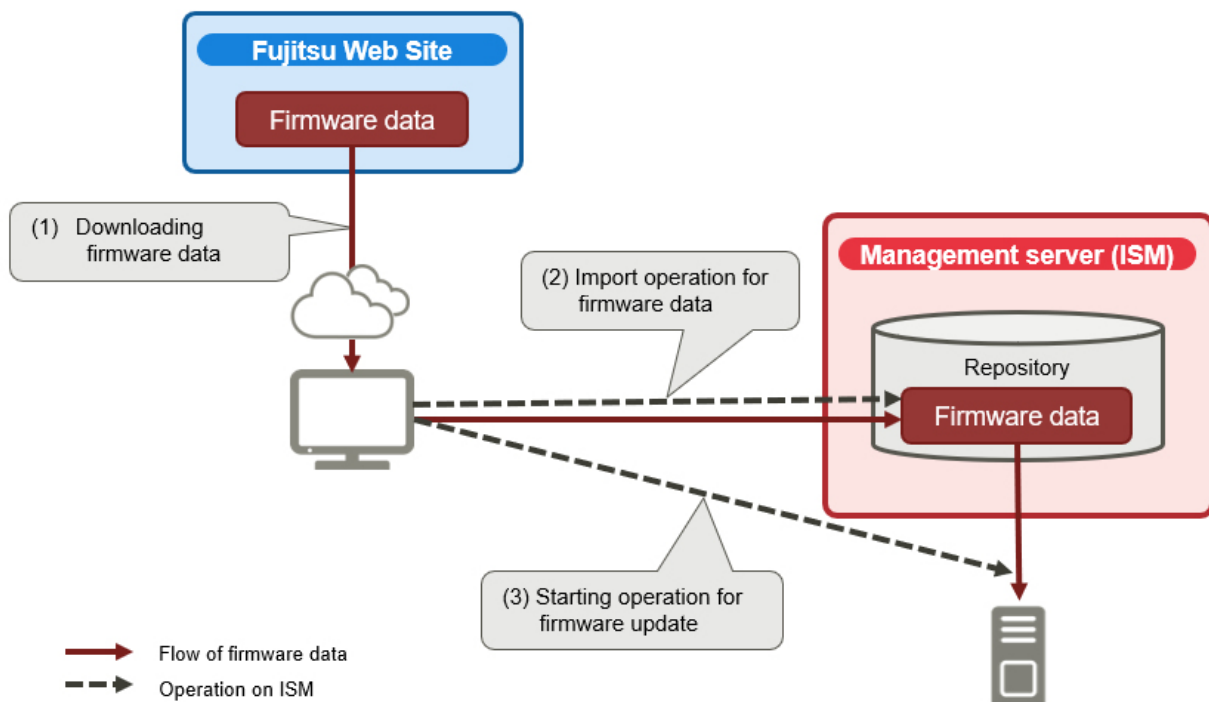
2.6.3.4 Firmware Updates using firmware data

To update firmware using the firmware data, you must import the firmware data into ISM in advance.

Download the firmware data from Fujitsu/Fsas Technologies or another website ((1) in the diagram below) and transfer the 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 ["2.14.2 Repository Management."](#)

Figure 2.22 Workflow for updating firmware using firmware data



Execution of firmware updates





Note

Common Update Notes

- While an update is in progress, observe the following notes:
 - Do not turn the target node on or off.
 - Do not reboot or 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, before any update operations.

For details on how to save the firmware data, refer to "[2.14.2 Repository Management](#)."

- Certain nodes require that firmware updates be executed in stages. Refer to the documentation that is supplied with the firmware data.
- 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 responding while an update is in progress, timeout errors are not discovered. If processing takes significantly longer than the presumed time for the task, confirm the status of the target node directly. If there are any errors, cancel the firmware update task in ISM.

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

- There is an upper limit to the number of nodes that firmware update can be executed simultaneously. This upper limit is 50. If a 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. Then, when the update is complete for the first set of nodes, the update will be executed on the remaining nodes. If a firmware update is executed while the maximum number of firmware updates is already running, the update will be executed after the first firmware updates have completed.

Offline Update Notes

- For Offline Update for the server (BIOS/iRMC/mounted PCI card), use the PXE boot function. In [Boot Mode] in the "Update Firmware/Driver" wizard, "Manufacturing Settings" is selected by default and PXE boot is executed in the following mode by ISM:
 - For a server with iRMC S4 and earlier: LegacyBIOS compatible mode
 - For a server with iRMC S5 or later: UEFI boot mode

If the BIOS settings for the server is different from the above, PXE boot may fail. In this case, select the same boot mode as the BIOS settings for the server in [Boot Mode] on the "Boot Mode" screen.

- For Offline Update, you may not be able to execute firmware updates using the ServerView Suite Update DVD version number that was imported. Refer to "[2.14.2.1 Storing and deleting firmware data](#)" to import the ServerView Suite Update DVD image to ISM.
- Executing Offline Update for the BIOS/BMC on PRIMERGY GX will initialize the firmware settings on the server side. Reconfigure the BIOS/BMC after performing Offline Update for any configuration items and settings that you have changed. You cannot monitor the node until the reconfiguration is complete.

Online Updates Notes

- 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 the update process has finished in ISM. In order to switch operations to the new firmware, execute the following procedure.
 - If you update a PCI card mounted on a server, you must reboot the server in order to switch to the new firmware. You can execute the reboot at any time.
 - If you execute an update for the server BIOS with the power 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 at any time. 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 on the power from the Details of Node screen in ISM.

- If you execute an update for 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 turns on automatically, and then turns off. After the power has turned off, you can switch to the new firmware by turning on the power from the Details of Node screen in ISM.

Network Switch Update Notes

- As network switches other than CFX are reset after they have been updated, data communication will be 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 a firmware update by specifying VCS Fabric (Brocade VCS Fabric). Execute a firmware update for each VDX fabric switch under it.
- Cisco switches (Catalyst or Nexus) do not manage firmware data by models.

The format of the version entered on the firmware data import screen is arbitrary.

If the entered versions are different from the current version, all firmware will be the update target. For [Latest (Online)], the version that is determined as the latest is displayed.

- When performing an Online Update for the Cisco Nexus 9000 series, use the SFTP protocol to transfer firmware data.

The maximum file size for transferring firmware data on Cisco Nexus switches using the TFTP protocol is approximately 1.6 GB.

For the Cisco Nexus 9000 series, the firmware data (Version 9.3 (5)) is approximately 1.9 GB and cannot be transferred via the TFTP protocol. The initial setting is the TFTP protocol, so you must switch to the SFTP protocol.

Refer to "[A.3.3 Changing a Protocol to Be Used for Firmware Updates](#)" for commands to confirm or change the protocol used in Online Update for Cisco Nexus switches.

Storage Update Notes

- When you execute a firmware update on ETERNUS DX/AF, you must specify an ETERNUS DX/AF account with the Maintainer role for the SSH user name and password node information.

PCI Card Update Notes

- When you execute a firmware update for 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 server (node), refer to "[2.2.1.5 Registration of node OS information](#)". Also note that firmware updates for PCI cards are supported only for the following OS types:

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

- 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. Therefore, all these cards will be updated to the same latest firmware version.

- To execute a firmware update for PCI cards (FC/CNA/LAN cards) on Linux, 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 QLogic QConvergeConsole CLI, refer to "[2.14.3 Installation of Emulex OneCommand Manager CLI and QLogic QConvergeConsole CLI](#)".

- For certain nodes and PCI cards, the format of [Current Version] and the format of the version displayed in [Latest (Online)] or [Latest (Offline)] may be different.

For applicable nodes and PCI cards, and for how they are displayed, refer to "Support Matrix."

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

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

Select [DOWNLOADS] and select the target operating system.

The reference procedures are subject to change without notice.

- For some PCI cards, the current version cannot be displayed, therefore, it is displayed as " - ."

In this case, all versions of firmware that have been imported for the applicable PCI card will be targets for updates. The latest version among all firmware versions that are imported for the applicable card will be displayed as the latest version.

- For Intel LAN cards, the identifier eTrack-ID is displayed in the current version.

The eTrack-ID is the firmware version displayed on the iRMC web interface.

Compare the current version with the imported firmware version to determine what to update.

The format of the firmware version to be compared with the current version is as follows.

- When the firmware is imported from the ServerView Suite Update DVD (12.19.07 or later)

In addition to the firmware version, the Intel LAN card firmware contains the eTrack-ID value before it was applied and the eTrack-ID information after it was applied. The version of the imported firmware is displayed in the following format, including the eTrack-ID information.

Format: eTrack-ID before the firmware is applied - eTrack-ID after the firmware is applied (Firmware version of the firmware file)

If the eTrack-ID before the firmware is applied matches the current version, it will be updated.

- When the firmware is downloaded from the public site or when the imported firmware is earlier than ISM 2.6.0.020

Format: (Imported firmware version (The firmware does not contain an eTrack-ID))

It will be updated regardless of the current version.

If the firmware is updated regardless of the current version, the current version will not change for the following cases even if the update succeeds.

- Updated with previously applied firmware.
- The version would be downgraded by the firmware update.

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Firmware/Driver].
2. Set the nodes to be updated to Maintenance Mode.
 - a. Select a node name to display the "Node Information" screen.
 - b. Set the target node to Maintenance Mode with the [Switch Maintenance Mode] button.
3. Confirm the [Current Version] column, the [Latest (Online)] column, and the [Latest (Offline)] column of the nodes to be updated.



Note

If the firmware data is not displayed in the [Latest (Offline)] column, you may not be able to execute firmware update using the ServerView Suite Update DVD version number that was imported. Refer to "2.14.2.1 Storing and deleting firmware data" to import the ServerView Suite Update DVD image to ISM.

4. Select [Online Update] or [Offline Update] in the [Update Mode:] column and select the checkbox for the firmware to be updated.
5. From the [Actions] button, select [Update Firmware/Driver].
6. Proceed by following the instructions on the screen.
 - To specify a date and time for firmware updates

On the "Update Settings" screen, select [Start 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 that is displayed after execution. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Jobs]. A list of jobs is displayed. Identify the job based on its job ID.

- To start firmware updates immediately

On the "Update Settings" screen, select [Start immediately]. After the update is started and 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 you select [Tasks] from the top of the Global Navigation Menu on the ISM GUI, the Task List is displayed. Identify the applicable task by its task ID and task type.

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

Point

- The firmware update can also be executed using the same operations from the screens displayed in the following procedure.
 1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Nodes].
 2. Execute one of the following.
 - From the [Column Display] field on the "Node List" screen, select [Firmware/Driver].
 - From the "Node List" screen, select the target [Node Name], and then select the [Firmware/Driver] tab.
- If you selected [Switch to the 'Maintenance Mode' when the update.] on "Update Settings" screen in the "Update Firmware/Driver" wizard, Maintenance Mode will be set just before the update, and Maintenance Mode will be released just after the update has been completed. Use this setting when you specify a date and time for updates.

2.6.3.5 Offline Firmware Update using ServerView embedded Lifecycle Management

This firmware update uses ServerView embedded Lifecycle Management (hereafter referred to as "eLCM").

The firmware update procedure involves using firmware data from the Repository Server or the Fujitsu/Fsas Technologies website, or using firmware data that is imported into ISM.

The differences are shown in the table below.

Item	Firmware data to be used		
	Update with Repository Server firmware data	Update with Fujitsu/Fsas Technologies website firmware data	Update with firmware data imported into ISM
Target for the firmware update	All components mounted on the server (BIOS/iRMC/mounted PCI card)		
Select firmware update target (BIOS/iRMC/mounted PCI card)	Disable	Disable	Enable
Structuring Repository Server	Required	Not required	Not required
Operation to import firmware data into ISM	Not required	Not Required	Required

2.6.3.5.1 Update with Repository Server or Fujitsu/Fsas Technologies website firmware data

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

In this procedure, you do not need to import the firmware data mentioned in "[2.6.3.4 Firmware Updates using firmware data](#)" into ISM.

The required firmware data is downloaded from a Repository Server or from the Fujitsu/Fsas Technologies website to the bootable SD card on iRMC of the update target server by eLCM during the firmware update. After downloading the firmware, eLCM creates ISO from the firmware data downloaded on the SD card and updates the firmware of the server with the created ISO.

The following is a list of the update methods that can be selected.

- Prepare the firmware/driver(s)
Download the firmware data from the Repository Server or from the Fujitsu/Fsas Technologies website to the bootable SD card on the iRMC of the server to be updated.
- Execute update
Update using the ISO created from the firmware data downloaded to the bootable SD card on the iRMC.
- Prepare the firmware/driver(s), and then execute update
Execute update as soon as the firmware data is ready.

To use eLCM, it is recommended to structure Repository Server. The processing time can be reduced by using the firmware data.



Point

For the procedures to configure and check each environment, refer to the applicable manuals on the following Fujitsu/Fsas Technologies Manual Server site.

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

- For the procedures to configure and check the eLCM environment, refer to the "ServerView embedded Lifecycle Management (eLCM) x.x for iRMC Sx Overview" (where x is the latest version).

Reference procedure

Select "Select a new Product" - [Browse For Product] and select the server that you want to update.

Download from [Server Management Controller].

- For the procedures to configure and check the Repository Server environment, refer to the "ServerView Repository Server - Installation and User Guide."

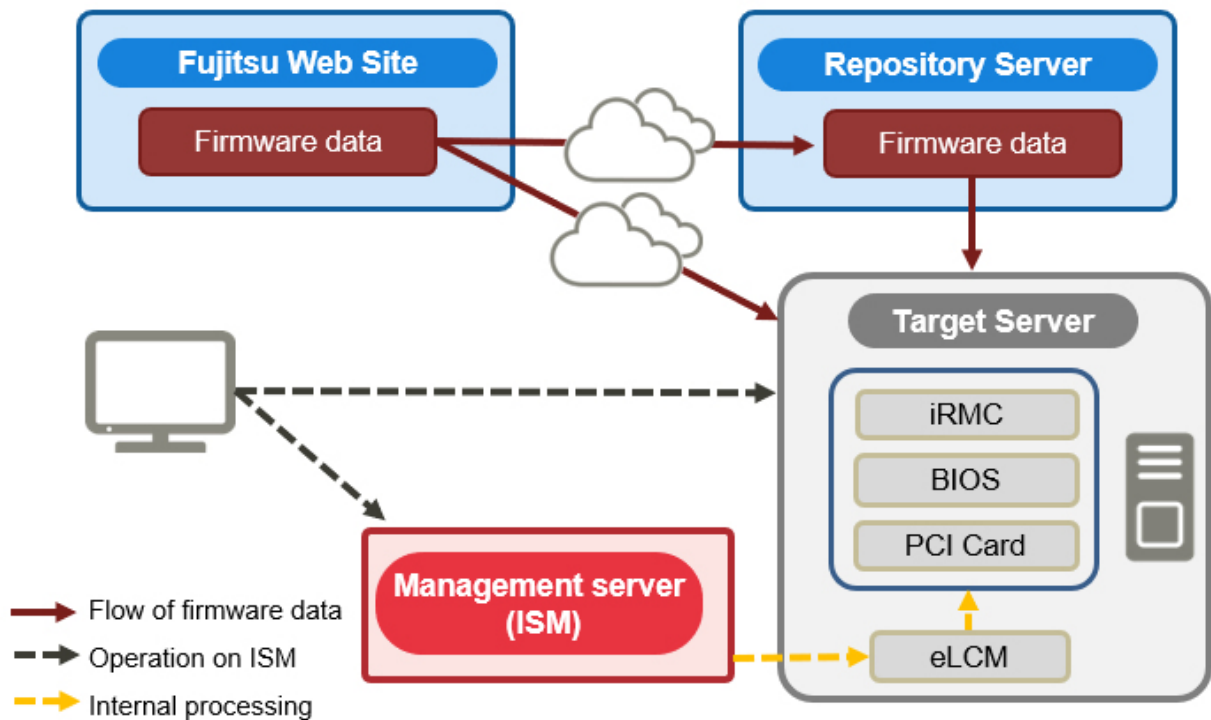
Reference procedure

Select "Select a new Product" - [Product Search]. Enter "Repository Server" and select [Continue].

Download from [Documentation] - [Setup Guide].

Reference procedures are subject to change without notice.

Figure 2.23 Workflow for updating with Repository Server or Fujitsu/Fsas Technologies website firmware data



Required preparations for updating with Repository Server or Fujitsu/Fsas Technologies website firmware data

- Structuring Repository Server (Recommended)
- Setting a firmware update target server to be able to use eLCM
- Turning off the power of the firmware update target server

Execution of firmware updates

	Administrator group	Other groups
Executable user	<div>Admin</div> <div>Operator</div> <div>Monitor</div>	<div>Admin</div> <div>Operator</div> <div>Monitor</div>

For the precautions for firmware updates, refer to "2.6.3.4 Firmware Updates using firmware data."

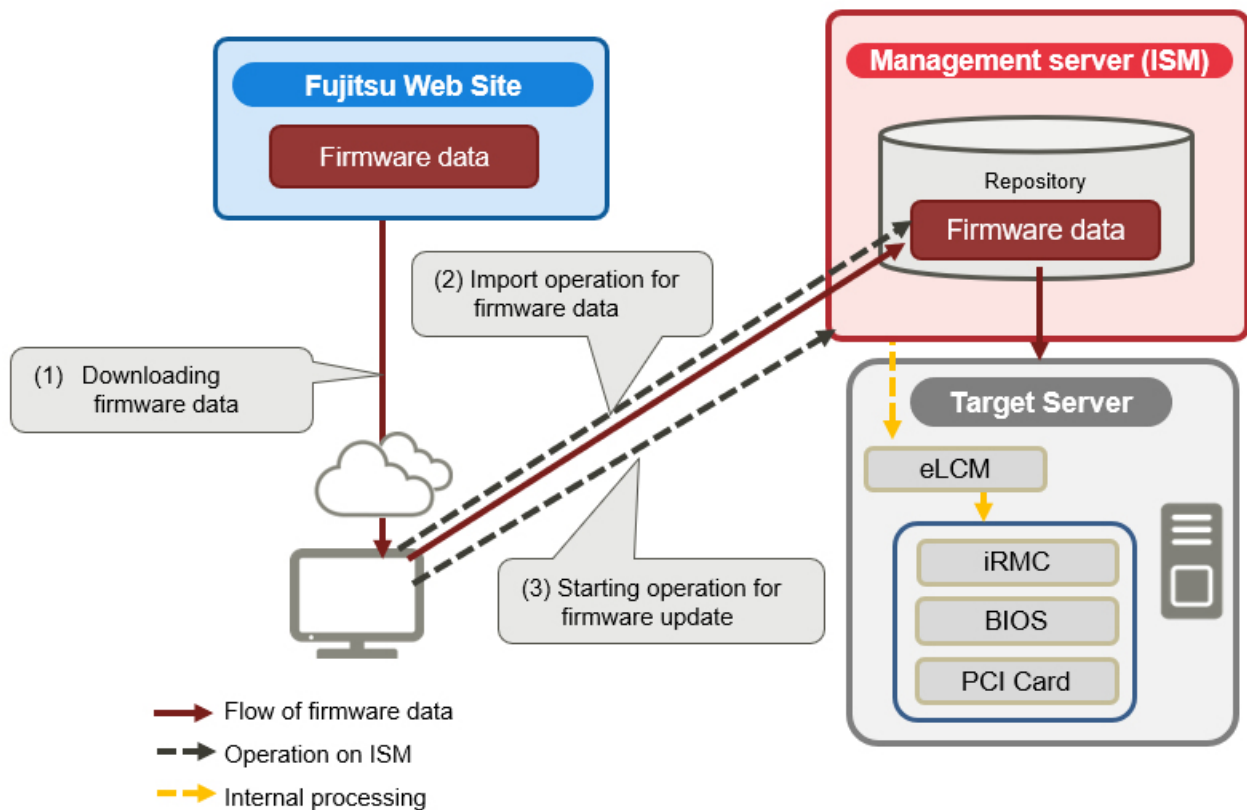
For the detailed procedure, refer to Step 4 to Step 5 of "6.4.2.1 Update using firmware data from a Repository Server" in "Operating Procedures."

2.6.3.5.2 Update with firmware data imported into ISM

This is an update procedure that uses firmware data imported into ISM and eLCM.

In this procedure, you need to import the firmware data mentioned in "2.6.3.4 Firmware Updates using firmware data" into ISM.

Figure 2.24 Workflow for updating with firmware data imported into ISM



Required preparations for updating with firmware data imported into ISM

- Setting a firmware update target server to be able to use eLCM
- Turning off the power of the firmware update target server
- Import eLCM Offline Update (SimpleUpdate) Tool to update PCI

Execution of firmware updates



For the precautions for firmware updates, refer to "2.6.3.4 Firmware Updates using firmware data."

For the detailed procedure, refer to "6.4.2.2 Update using firmware data imported into ISM" - Step 4 to Step 6 of "Update Firmware" in "Operating Procedures."

2.6.3.6 Online Firmware/Driver Update Using eLCM

For details on eLCM and eLCM environment structuring, refer to "2.6.3.5 Offline Firmware Update using ServerView embedded Lifecycle Management."

- eLCM Online Update supports the update depending on the OS type of the target node.
 - You can update the driver package and the software such as ServerView Agents that is provided as a PSP (PrimSupportPack-Win) for Windows.
 - You can update the software such as ServerView Agents for Red Hat Enterprise Linux and SUSE Linux Enterprise Server.
- ServerView Agents or ServerView Agentless Service on the OS of the target node detects available updates and notify the results to iRMC. ISM displays the updatable driver packages based on the information retrieved from iRMC.

- Even if you do not select it as an update target, packages that require updating, such as PrimSupportPack-Win/FSC_SCAN, will be updated automatically.

Workflow for online firmware/driver updates with eLCM

The workflow is the same as offline firmware update using eLCM. Refer to "[2.6.3.5.1 Update with Repository Server or Fujitsu/Fsas Technologies website firmware data.](#)"

Required preparations for online firmware/driver updates with eLCM

For the detailed preparations, refer to "6.10 Export/Import/Delete Cluster Definition Parameters."

2.6.3.6.1 Behavior during updates

- Updates are executed when the server power is on.
- Updates are executed on the server if a supported OS is running.
- During the update, the server may be rebooted.
- After the update, the node does not need to be rebooted.

2.6.3.6.2 Execution of firmware/driver updates



Refer to "[2.6.3.4 Firmware Updates using firmware data](#)" for restrictions.

For the detailed procedure, refer to "6.4.3 Online Update Firmware/Driver Using ServerView embedded Lifecycle Management" in "Operating Procedures."

2.6.4 Job Management

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

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

The following operations are also performed on the "Jobs" screen:

- Canceling an executing process
- Deleting a process before execution
- Deleting a completed process



Note

- The number of jobs has an upper limit. You cannot register more than 100 jobs. Delete unnecessary jobs so as not to exceed the upper limit.
- The job runs every 10 minutes. The job may run longer than the specified time. The longest delay is 9 minutes.

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.

In ISM, you can download a Hardware Compatibility List (hereafter referred to as "HCL") for hardware such as PRIMERGY and create a baseline from the components and firmware versions that are listed in that HCL.

You can determine if the firmware version is compatible with HCL by assigning a created baseline to a node.



HCL is published on the Fujitsu web server (<https://support.ts.fujitsu.com/globalflash/>). HCL is compatible with your OS (VMware ESXi version) and operations are on a list of firmware that is verified.

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, refer to "Support Matrix."

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

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

Select [DOWNLOADS] and select the target operating system.

The reference procedures are subject to change without notice.

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 specific model with Firmware Baseline.

There are three procedures to create a Firmware Baseline definition:

- [Automatically create a Firmware Baseline definition when importing firmware data from the ServerView Suite DVD](#)
- [Create a Firmware Baseline definition manually using the firmware managed in the repository](#)
- [Create a Firmware Baseline definition manually by downloading a Hardware Compatibility List](#)

Automatically create a Firmware Baseline definition when importing firmware data from the ServerView Suite DVD

The following is the procedure to create a Firmware Baseline definition automatically when importing firmware data from the ServerView Suite DVD.

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Firmware/Driver].
2. From the menu on the left side of the screen, select [Import].
3. From the [Actions] button, select [Import DVD].
4. Proceed by following the instructions on the screen.



- 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.
- 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.

Create a Firmware Baseline definition manually using the firmware managed in the repository

The following is the procedure to create a Firmware Baseline definition manually using the firmware managed in the repository.

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Firmware/Driver].
2. From the menu on the left side of the screen, select [Baseline].
3. From the [Actions] button, select [Create].
4. Proceed by following the instructions on the screen.



- 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.
- If you create a Firmware Baseline definition manually, register the firmware in the repository in advance. For details, refer to "[2.14.2.1 Storing and deleting firmware data.](#)"

Create a Firmware Baseline definition manually by downloading a Hardware Compatibility List

The following is the procedure to create a Firmware Baseline definition manually by downloading a Hardware Compatibility List.

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Firmware/Driver].
2. From the menu on the left side of the screen, select [Baseline].
3. From the [Actions] button, select [Import (HCL)].
4. Proceed by following 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.
- The "Web Repository Address" to download HCL is displayed at the following Fujitsu web server URL by default.

<https://support.ts.fujitsu.com/globalflash/>

For the "Web Repository Address," you can also specify the web server address that is configured with ServerView Repository Server (repository server). If you have already configured the repository server in "[2.6.3.5.1 Update with Repository Server or Fujitsu/Fsas Technologies website firmware data](#)," you can use that server. Change the destination of connection according to your environment. You must specify the root address of the repository in which versionTree.text and hclVMWareAll.xml which are accessible from ISM are deployed in "Web Repository Address."

For details, contact your web server administrator.

- To connect to Web Repository Address via proxy, you must set the proxy settings. Use the following procedure to set the proxy.
 1. From the Global Navigation Menu on the ISM GUI, select [Settings] - [General].
 2. From the menu on the left side of the screen, select [Proxy Setting].
 3. From the [Actions] button, select [Add].
 4. Proceed by following the instructions on the screen.

Note

The version for "Firmware type: LAN firmware name: MCXxxxx" is in parentheses. For the version in parentheses, the baseline status always becomes incompatible. If the baseline definition for this firmware is required, edit the baseline definition to correct the version after you create the baseline.

Before editing a baseline definition, download this firmware from the Web Repository Address to which you want to download the HCL and register it in the repository. For details, refer to "[2.14.2.1 Storing and deleting firmware data](#)."

After registering the firmware to the repository, edit the baseline definition. For the detailed procedure to edit baselines, refer to "[2.6.5.5 Editing Firmware Baseline definitions](#)."

If you specify a firmware version number for the firmware defined by the eTrack-ID, the application of the firmware may not result in the version defined in the baseline.

The firmware defined by the eTrack-ID are:

Firmware type	LAN
Firmware name	X550-T2, X710, X722 LOM, or E810

In the above case, the baseline determination is incompatible. Change the eTrack-ID of the version defined in the baseline. For details on the support for eTrack-ID and firmware names, refer to "Intel LAN Controller Firmware Versions" from the following Fujitsu/Fsas Technologies manual site.

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

Reference Procedure

Select "Select a new Product" - [Browse For Product] and select the server with the baseline target model.

Download it from [LAN].

Reference procedures are subject to change without notice.

2.6.5.2 Assigning Firmware Baseline definitions

Executable user

Administrator group: Admin, Operator, Monitor

Other groups: Admin, Operator, Monitor

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 ISM GUI, select [Structuring] - [Firmware/Driver].
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. Proceed by following the instructions on the screen.

Note

- When assigning Firmware Baseline definitions, not only supported nodes for firmware updates with ISM also unsupported nodes are displayed in the "Select applicable node(s)" wizard in [1. Select Node]. Select updating node for firmware updates. Refer to "Support Matrix" for the latest information on models that are supported by "Maintenance Support" - "Management of Firmware Versions" on the "Server, Chassis" sheet.
<https://support.ts.fujitsu.com/index.asp>
Select [Select a new Product] on the above site and enter "Infrastructure Manager" in [Product Search:].
Select [DOWNLOADS] and select the target operating system.
The reference procedures are subject to change without notice.
If you select an unsupported node and execute Assign to Nodes, the assignment will result in an error (Message ID 30113300).
- 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

Executable user

Administrator group: Admin, Operator, Monitor

Other groups: Admin, Operator, Monitor

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 ISM GUI, select [Structuring] - [Firmware/Driver].
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. Proceed by following 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.



Note

Firmware updates are executed using the firmware data that has been imported in advance.

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

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Firmware/Driver].
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/Driver].
5. Proceed by following 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 ISM GUI, select [Structuring] - [Firmware/Driver].
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. Proceed by following the instructions on the screen.

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 ISM GUI, select [Structuring] - [Firmware/Driver].
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. Proceed by following the instructions on the screen.

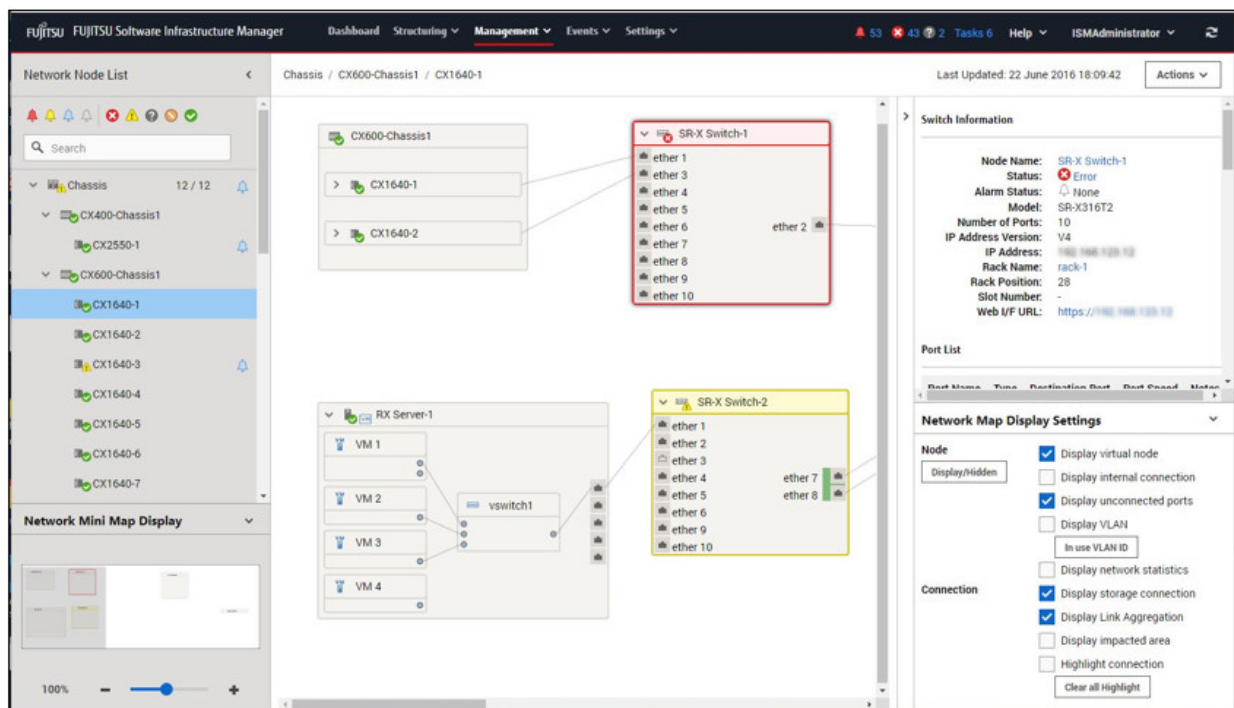
If you delete a Firmware Baseline definition, Firmware Baseline definition assignment is released.

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 a managed node and its virtual machines, virtual switches, and virtual routers
- Confirming the statistical information of the network of the managed nodes on the Network Map
- Confirming the VLAN and Link Aggregation settings for network switches, and changing these settings

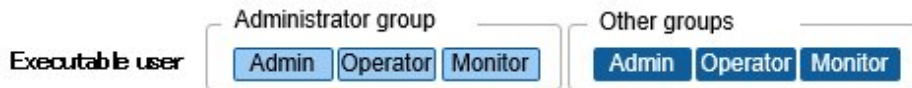
Figure 2.25 Network Map



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 network connections 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.

You can also confirm the virtual connection relationships between the physical ports of a managed node and the virtual ports of its virtual components (virtual switches, virtual machines, and virtual routers).

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

A list of the nodes that can be 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 the Network Node List at the left edge 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.

Switch the Network Map display

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

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 connections 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 area that is affected by an error on the Network Map ON and OFF. For the connections with a node where an error or failure has occurred, the edge of the next connected node as well as the connected port are displayed in yellow. If virtual networks are configured on the connected node, the affected virtual networks will also be displayed in yellow.
Display unconnected ports	Switch the display of ports whose links are down 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 nodes and ports whose VLAN ID setting matches the VLAN ID that is entered in the text box are 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 values that exceed the threshold values are displayed in orange (critical threshold value exceeded) or yellow (warning threshold value exceeded). For the threshold settings, " 2.3.2 Monitoring of Network Statistics Information ." You can select which monitoring item to display from the list in the selection box displayed when you check this item.

Display Setting Name	Description
[Display/Hidden] button	<p>Switch to display/hide nodes displayed on the Network Map.</p> <p>You can also display/hide nodes by selecting the  or  icon that is displayed on the right side of the Network Node List or the node name in the Network Map.</p>

Saving the Network Map display settings

You can save the Network Map display settings. The saved display settings are used to display the Network Map when you display the "Network Map" screen the next time.

You can save the Network Map display settings with the following procedure.

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Network Map].
2. From the [Actions] button, select [Network Information Preserve].

The Network Map display settings are saved.



Point

- You can return the display settings to the initial settings by selecting [Network Information Relocate] from the [Actions] button.
- 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 on the Network Map, the extended display of the ports within the node is displayed.
- The Network Map display settings are saved for each user.



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 connections that actually exist 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 target 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, which is performed by ISM once a day. In order to confirm the most recent status after registering nodes, modifying any connections, or after an error, execute [Update network information] from the [Actions] button.
Also, whenever the hardware configuration of a node has been changed, execute [Get Node Information], and then [Update network information] on the Details of Node screen for the target node. 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. For cloud management software registration, refer to "[2.14.6 Management of Cloud Management Software](#)." For 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 ports with teaming (bonding) settings, and the display of the connections of those ports with virtual switches are supported.

2.7.2 Updates of Network Management Information

Executable user

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

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

1. From the Global Navigation Menu on the ISM GUI, 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, check for an 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 in 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 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 see 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 ISM GUI, select [Management] - [Network Map].

A list of the nodes that can be 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 ISM GUI, select [Management] - [Network Map].

A list of the nodes that can be 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]. The date and time of the latest refresh is the reference point in time that is currently set.

4. Select the [Refresh] button.

A confirmation screen is displayed.

5. 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.

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

A list of the nodes that can be 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 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.

- Select the [Display network statistics] checkbox in the "Network Map Display Settings" pane, and select the monitoring items for 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). For the threshold settings, "[2.3.2 Monitoring of Network Statistics Information](#)."

Point

To check the past statistic information (traffic, and so on), from "Port Information," which is displayed when selecting the port of the network switch, select "Network Statistics Information" - the [Graph] button. The [Graph] button is displayed when the values of each monitoring item for the network statistics information have been retrieved.

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 ISM GUI, select [Management] - [Network Map].

A list of the nodes that can be 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 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

Select the [Display VLAN] checkbox in the "Network Map Display Settings" pane, and 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" pane allows you to check the VLAN information that is already used.
- Use the [Display Link Aggregation] on the "Network Map Display Settings" pane 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 ISM GUI, select [Management] - [Network Map].
2. From the Network Node List, select the node that serves 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. Select the checkboxes for the respective ports for which you want to set the same VLAN ID, and select the [Setting] button on the upper-right of the screen.
5. Enter the VLAN ID you set, edit the contents, and then select the [Confirm] button.
6. Confirm the changed 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, VLAN setting 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 "[2.14.4 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 reserved VLAN IDs depending on the models of network switches. You cannot change the settings of reserved VLAN IDs. Check the specifications of the respective nodes.

2.7.8 Change of Link Aggregation Settings



You can change the Link Aggregation settings of a network switch.

The following is a sample operation of adding link aggregation settings.

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Network Map].
2. From the Network Node List, select the node that serves 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 want to create a Link Aggregation, and select the [Add] button of Link Aggregation Setting.
5. Enter the LAG Name and Mode, select the checkbox for the port to set for Link Aggregation, and then select the [Confirm] button.
6. Confirm the Link Aggregation settings, 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 the respective nodes.
- You cannot set Link Aggregation between 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 create a Multi-Chassis Link Aggregation between different nodes, you must change Link Aggregation settings for the 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 ISM GUI, select [Management] - [Network Map].
A list of the nodes that can be 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, if you want to cancel the settings that 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 (Not available from ISM 3.0.0)

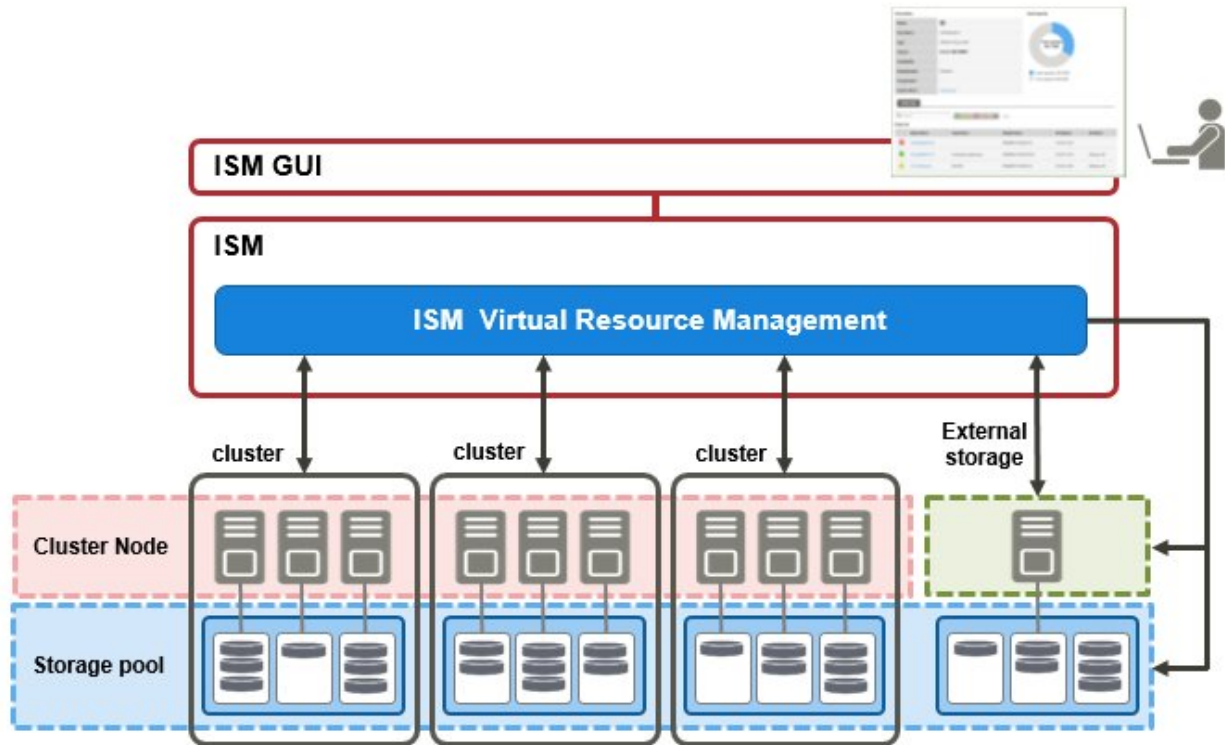
This function is not available from ISM 3.0.0.

2.9 Virtual Resource Management

Virtual Resource Management is a function to manage and monitor the items managed as virtual resources.

The following is the environment configuration for operating this function.

Figure 2.26 Configuration of the operating environment for Virtual Resource Management



Note

For pre-settings for Virtual Resource Management, refer to "3.8 Pre-Settings for Managing Virtual Resources/Clusters."

2.9.1 Supported Virtual Resources

The virtual resources supported with this function are storage pools that configure VMware Virtual SAN and Microsoft Storage Spaces Direct and ETERNUS storage pools.

Software environment

Software environments that can be operated by Virtual Resource Management depend on the type of SDS (Software Defined Storage) and its version. Also, the hypervisor and cloud management software differ depending on the type of SDS.

For information on the software environments in which Virtual Resources Management is available, refer to "Support Matrix."

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

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

Select [DOWNLOADS] and select the target operating system.

The reference procedures are subject to change without notice.



Note

You must enable CredSSP authentication in advance. For pre-settings for Virtual Resource Management, refer to "[3.8 Pre-Settings for Managing Virtual Resources/Clusters](#)."

ETERNUS Storage

ISM GUI attribute information, status, and other information regarding ETERNUS Storage are displayed.

For information on the ETERNUS Storage supported by Virtual Resources Management, refer to "Support Matrix."

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

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

Select [DOWNLOADS] and select the target operating system.

The reference procedures are subject to change without notice.



Note

The display of thin provisioning pool for ETERNUS is not supported.

The volume used by thin provisioning pool is not reflected even when a RAID group is built-in to thin provisioning pool.

For reference and management of thin provisioning pool, use ETERNUS web GUI.

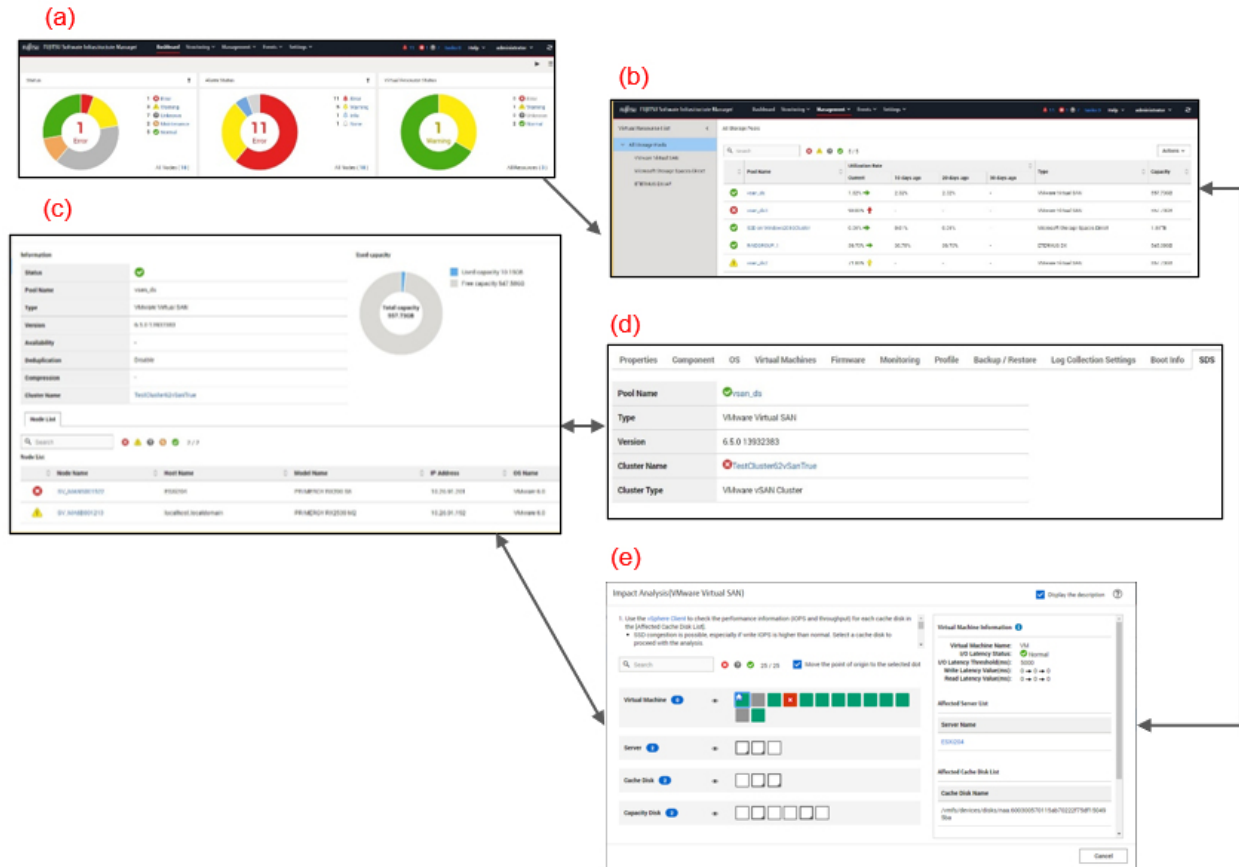
2.9.2 GUI for Virtual Resource Management

From the Global Navigation Menu on the ISM GUI, select [Management] - [Virtual Resource] to display the GUI screen for Virtual Resource Management.

You can use [Add Widget] to add a list of virtual resources to move to that screen.

The following displays the functions of each GUI and the mutual display relationships.

Figure 2.27 GUI for Virtual Resource Management



(a) Display of virtual resources widget

The status for all of the virtual resources managed by ISM is displayed in a widget on the ISM Dashboard.

(b) Display of virtual resources list

Displays a list for the statuses for all of the virtual resources managed by ISM.

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 setting information and utilization rate, is displayed for the selected virtual resource.

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 the information for the virtual resource configured by vSAN or S2D 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>

(e) Display of vSAN disk impact on virtual machines

From the [Actions] button, select [Impact Analysis(VMware Virtual SAN)] to display a list for servers and physical disks (cache disks and capacity disks) that make up vSAN and for virtual machines that use vSAN.

Display of Impact Analysis (VMware Virtual SAN) supports only vSAN OSA.

This screen displays the relationship between the servers and the physical disks and the virtual machines using vSAN physical disks.

You can also check the I/O latency information for the virtual disks used by virtual machines.

It displays the virtual machine I/O latency status in different colors. This makes it easy to be aware of virtual machines with slow I/O.

2.9.3 Operation of Virtual Resource Management

The following describe 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 resource information](#)
- [2.9.3.4 Display of vSAN disk impact on virtual machines](#)



Point

Before monitoring with ISM, you must register the virtual resource environment to ISM. Registration 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 "[2.14.6 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 resource information](#)."

The Storage Pool information is displayed on the GUI for Virtual Resource Management.

2.9.3.1 Monitoring of the utilization status of storage pools



Here the procedure for monitoring the utilization status of storage pools is described.

1. From the Global Navigation Menu on the ISM GUI, select [Dashboard] to display the virtual resource widget "Virtual Resource List."

For how to add the widget, refer to the ISM online help.

- Refer to "Utilization Rate" for the current utilization rate of the storage pools.

Virtual Resource List				
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%

- A more detailed utilization rate status can be checked on the Virtual Resources List screen.

The current utilization rate can be determined from the direction and color of the arrows.

From the Global Navigation Menu on the ISM GUI, 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 Pools						
Search		5 / 5			Actions	
Pool Name	Utilization Rate	10 days ago	20 days ago	30 days ago	Type	Capacity
✓ vsan_ds	1.82% →	2.32%	2.32%	-	VMware Virtual SAN	557.73GB
✗ vsan_ds3	90.00% ↑	-	-	-	VMware Virtual SAN	557.73GB
✓ S2D on Windows2016Cluster	0.01% →	0.01%	0.01%	-	Microsoft Storage Spaces Direct	1.81TB
✓ RAIDGROUP_1	36.70% →	36.70%	36.70%	-	ETERNUS DX	545.00GB
⚠ vsan_ds2	71.00% ↑	-	-	-	VMware Virtual SAN	557.73GB

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.

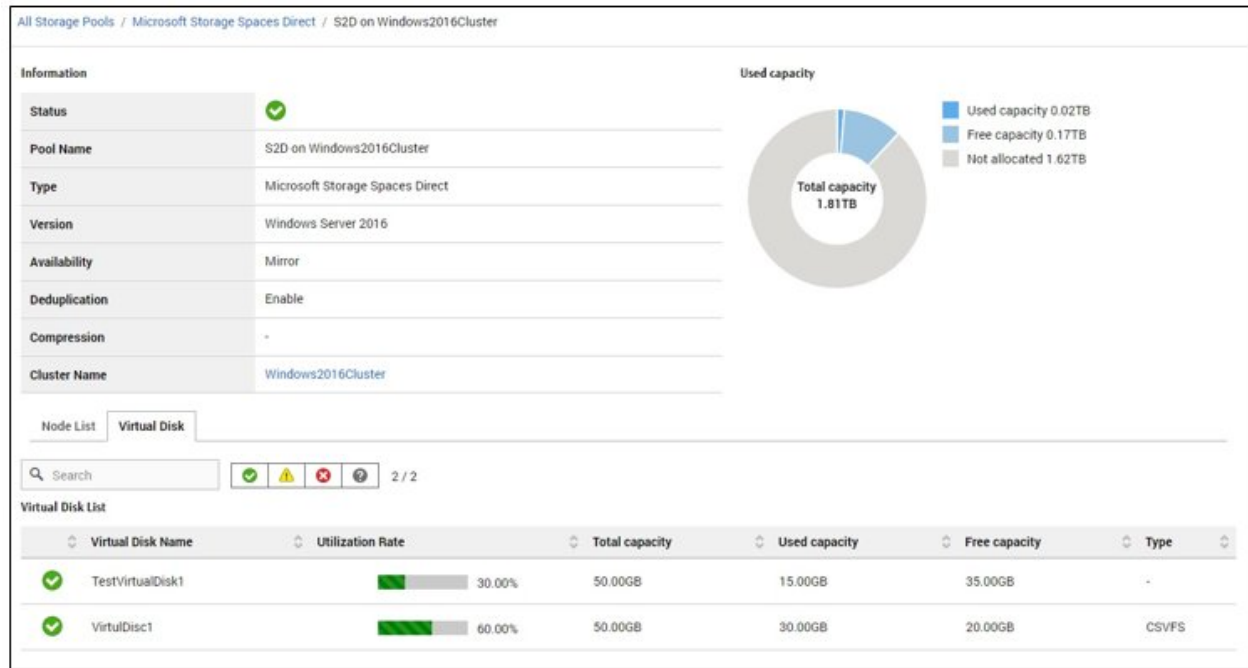
Sideways: The utilization rate is steady, is increasing slightly (the utilization rate is increasing less than 5%) or is decreasing

Diagonal upwards: The utilization rate is increasing (the utilization rate is increasing between 5% - 15%)

Upwards: The utilization rate is increasing sharply (the utilization rate is increasing 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 classification of the capacity information displayed in the pie chart of the utilization rate status for Microsoft 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.



The redundancy settings for the virtual disks is reflected in the capacity information in the [Virtual Disk] tab.

The capacity value displayed in the [Used capacity] pie chart takes the redundancy of the capacity of each virtual disk into account.

- 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 the 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 actions.

2.9.3.2 Identification of the errors in storage pools



The following describes the procedure for discovering errors and identifying their causes 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 resource information.](#)"

The virtual resource information on the GUI is refreshed to the latest. If an error has occurred, the displayed status will change.

Step 2

Discover and identify errors.

Resource errors can be checked from the Virtual Resources List screen. 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 Virtual Resources List screen

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

The Virtual Resources List screen is displayed.

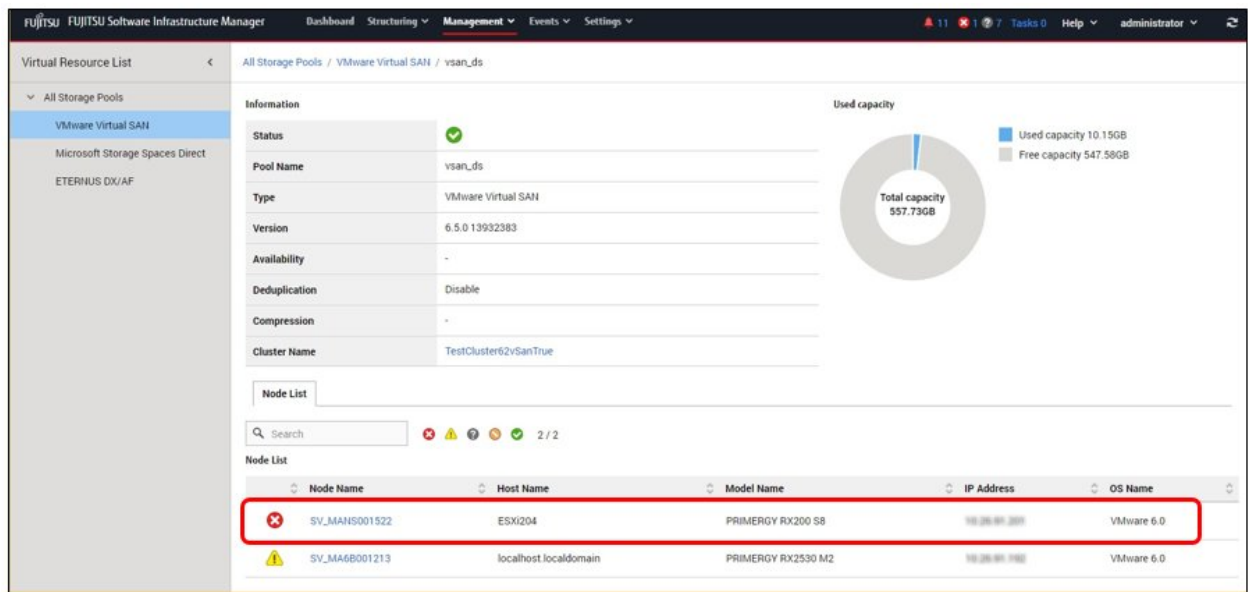
The screenshot shows the 'All Storage Pools' table. At the top, there is a search bar and a status filter icon (a red square with a white 'x') highlighted by a red box. The table has columns for Pool Name, Utilization Rate (Current, 10 days ago, 20 days ago, 30 days ago), Type, and Capacity. The rows show various storage pools with their respective utilization rates and types.

Pool Name	Utilization Rate				Type	Capacity
	Current	10 days ago	20 days ago	30 days ago		
vsan_ds	1.82% →	2.32%	2.32%	-	VMware Virtual SAN	557.73GB
vsan_ds3	90.00% ↑	-	-	-	VMware Virtual SAN	557.73GB
S2D on Windows2016Cluster	0.01% →	0.01%	0.01%	-	Microsoft Storage Spaces Direct	1.81TB
RAIDGROUP_1	36.70% →	36.70%	36.70%	-	ETERNUS DX	545.00GB
vsan_ds2	71.00% ↑	-	-	-	VMware Virtual SAN	557.73GB

Virtual resources with the selected status can be filtered out with the status filter icon at the top of the screen.

2. Select the pool name.

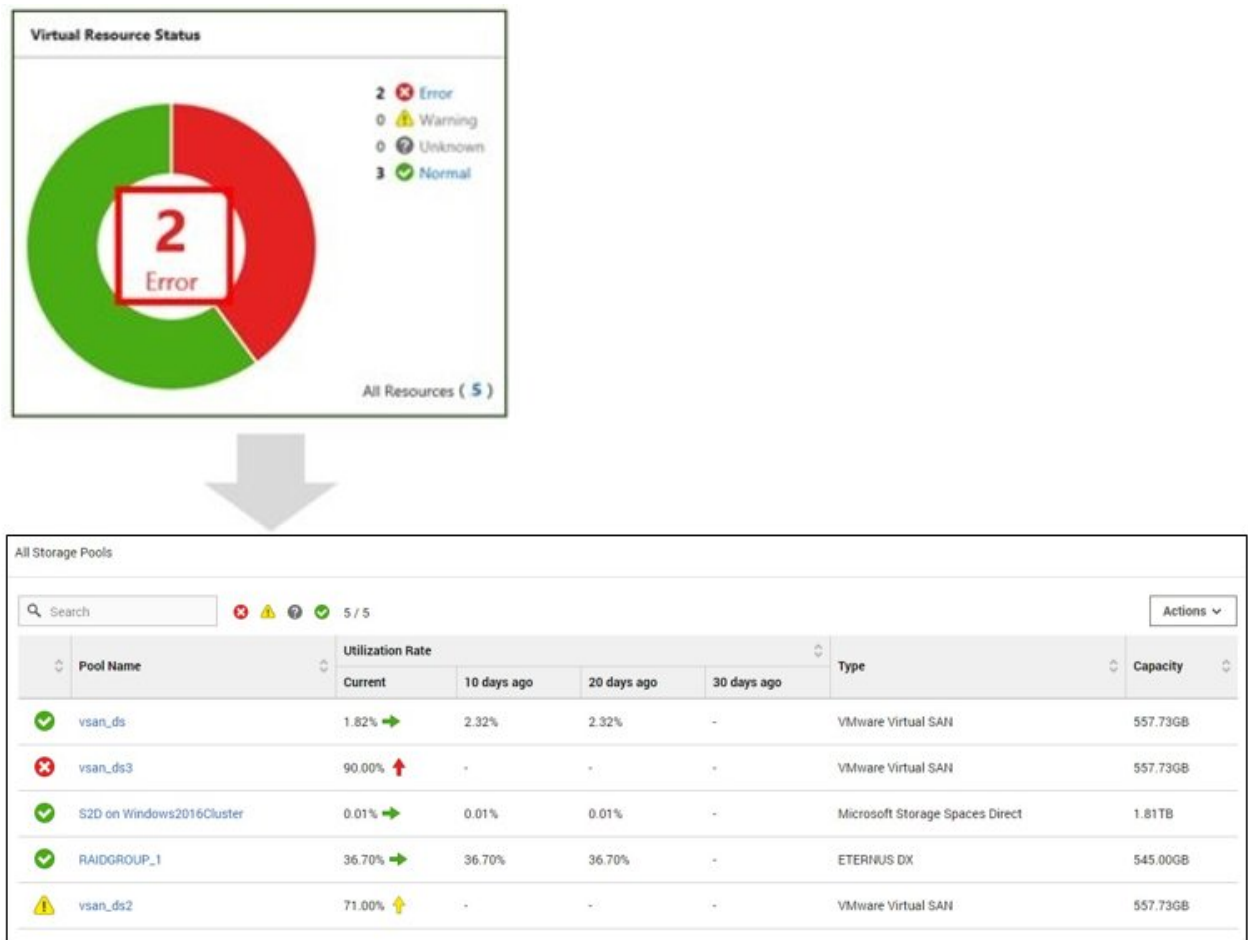
When the virtual resources detailed information screen is displayed, check the node names for which errors are displayed in the "Node List."



(2) When identifying the place of an error from Dashboard

1. Select the number displayed in the middle of the "Virtual Resource Status" widget on the ISM Dashboard.

A resource list of the error statuses will be displayed.



2. Select the pool name.

When the virtual resources detailed information screen is displayed, check the device names for which errors are displayed 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 the error status occurred	Status
Physical layer	<p>An error occurred in the storage pool because of a problem with a physical component (HDD, SSD, or node).</p> <p>Depending on the type of SDS, it will be in one of the following states:</p> <ul style="list-style-type: none"> - If it is vSAN, an error has occurred in the health of vSAN - If it is S2D, an error has occurred on the nodes or physical disks configuring the storage pool - If it is ETERNUS, an error has occurred on the RAID groups, physical disks, or ETERNUS devices
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	Icon displayed in the ISM GUI	Status
Error		An error has occurred in the storage pool, and continued usage is not possible.
Warning		An error has occurred in the storage pool, but continued usage is possible.
Unknown		An error has occurred in the storage pool, and its status cannot be confirmed.
Normal		The storage pool status is normal.

Point

If the capacity of the storage pool is reduced by an error in the physical or virtual layer, whether it can continue to be used as a storage pool can be determined by the "Error" status.

The details of an error and where it occurred can be confirmed as follows.

Point

For details on how to identify the specific error location and its corrective actions, or to recover from an error, execute the procedures by following the manual for the relevant product.

For vSAN

The status of the storage view the vSAN datastore and the "Health" of the vSAN are checked on either the ISM GUI or in the vSphere 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 vSphere 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. Select the node name checked in Step 1 on the [Hosts and Clusters] tab.
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 vSphere Web Client, and select the cluster name in "Hosts and Clusters."
2. From the [Monitor] tab - [Virtual SAN] - [Health], execute [Retest]. Check that the test result that was "Failed" 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. On 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.

For S2D

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 at the top of the screen, and check after refreshing the information.
2. On 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.

For ETERNUS Storage

Open the ETERNUS web GUI with a web browser, check the statuses of RAID groups and physical disks.

You can confirm the URL of the ETERNUS web GUI in the node information that is displayed by selecting the ETERNUS device name in the "Node Lists" on the Virtual Resources details screen.

After recovering from the error, on the Virtual Resource list screen in 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 ISM GUI, 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 resource information



From the virtual resources list screen, execute [Refresh Virtual Resource Information] from the [Actions] button.



Note

You cannot cancel a task whose task type is "Refresh Virtual Resource." Wait until the task completes.

Point

- Since the information displayed on the GUI may be old, make sure to refresh it when checking the latest status.
The refresh process is registered in ISM tasks. Retrieving information is not complete until the task has a status of "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 information displayed on the GUI is periodically and automatically refreshed as follows (tasks are not displayed).
 - All information is automatically refreshed every day at AM 0:00 of local time. This includes information managed by newly registered cloud management software.
 - The statuses are automatically refreshed every three minutes. This is information managed by registered cloud management software.
 - When the cloud management software is set to Event Output Restricted Mode, the information is not automatically updated. It is updated automatically when Event Output Restricted Mode is disabled.

For information about Event Output Restricted Mode for the cloud management software, refer to "[2.14.6.5 Changing Event Output Restricted Mode for the cloud management software.](#)"

2.9.3.4 Display of vSAN disk impact on virtual machines



This section describes the Virtual Machine Resource Impact Analysis (VMware Virtual SAN) screen.

The Virtual Machine Resource Impact Analysis (VMware Virtual SAN) screen displays the physical disks (cache and capacity disks) and the servers that contain them for the virtual machines generated for vSAN storage.

It displays the virtual machines that are affected when a server is down or the performance of physical disks (cache and capacity disks) decline.

Point

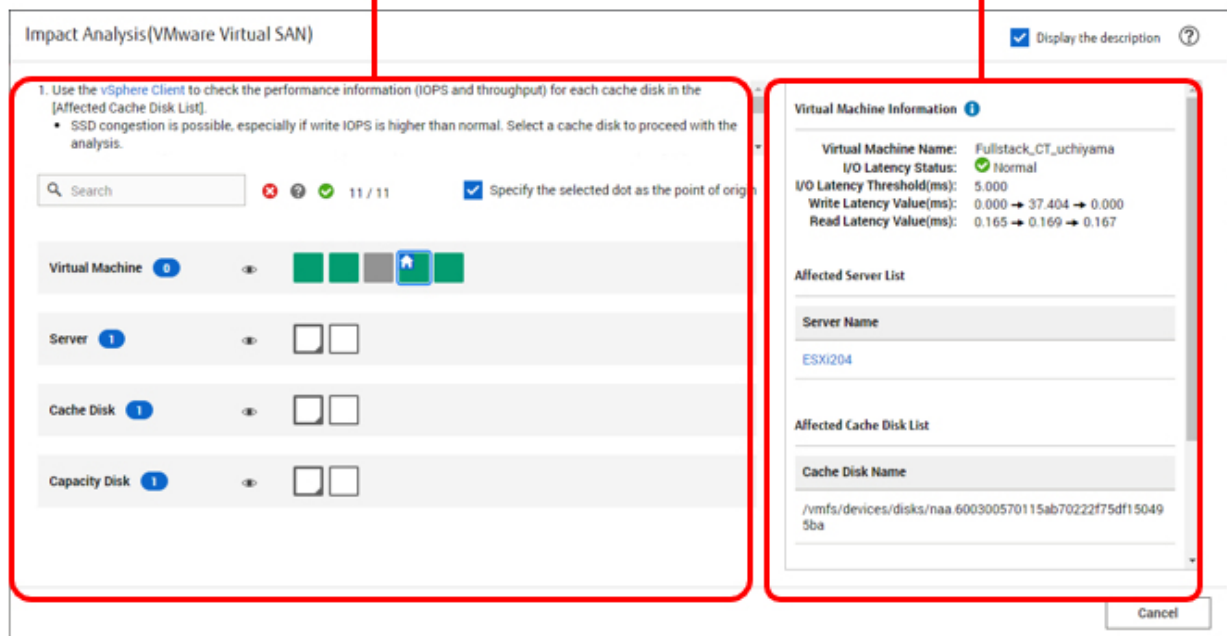
To view the configuration and details for virtual machines, servers, cache disks, and capacity disks, you must register the cloud management software (vCenter Server or vCenter Server Appliance) that manages the vSAN data store or server and the OS information for the node managed in ISM.

Refer to "2.14.6 Management of Cloud Management Software" for registering cloud management software. Refer to "2.2.1.1 Registration of datacenters/floors/racks" for registering OS information.

For the procedures to display the "Impact Analysis (VMware Virtual SAN)" screen, refer to "6.2.4 Confirm the Status of Virtual Machines/ vSAN Storage" in "Operating Procedures."

Virtual machine and vSAN disk configuration view area

Dot detail information display area



The "Impact Analysis (VMware Virtual SAN)" screen consists of the configuration view area on the left side of the screen that displays the configuration of virtual machines, vSAN disks, and servers, and the information display area on the right side of the screen that displays the details for the dot selected in the configuration view area.

Note

- Display of Impact Analysis (VMware Virtual SAN) supports only vSAN OSA. "No Data." is displayed for vSAN ESA.
- The "Impact Analysis (VMware Virtual SAN)" screen shows information for the configuration of the virtual machines and vSAN disks obtained the last time [Refresh Virtual Resource Information] was performed or the information obtained from the hourly update via ISM.

When you update virtual resource management information, you must update it to the latest information.

- If you have registered or deleted cloud management software (vCenter Server or vCenter Server Appliance) from ISM, execute the following procedure.

From the Global Navigation Menu on the ISM GUI, select [Settings] - [General] - [Cloud Management Software]. Select [Get Cloud Management Software Info], and then select [Run].

- If you have added or deleted virtual machines, execute the following procedure.

From the Global Navigation Menu on the ISM GUI, select [Management] - [Virtual Resource]. On the "Virtual Resource List" screen, select [Actions] - [Refresh Virtual Resource Information], and then select [Yes].




The "Impact Analysis (VMware Virtual SAN)" screen may display "No Data." Close the "Impact Analysis (VMware Virtual SAN)" screen, perform the above steps to update the data, and then return to the "Impact Analysis (VMware Virtual SAN)" screen.

- The "Impact Analysis (VMware Virtual SAN)" screen is not automatically updated. If you want the latest information, close the "Impact Analysis (VMware Virtual SAN)" screen and return to the "Impact Analysis (VMware Virtual SAN)" screen.



Configuration view area

Virtual machines, servers, cache disks, and capacity disks are represented as dots in the configuration view area.

Virtual machines are represented as the following dots.

Status	Dot on the ISM GUI	Description
Error	 (Red)	Virtual machine disk latency has occurred (I/O latency threshold exceeded). Possible causes include degraded disk performance or data congestion.
Unknown	 (Gray)	Disk latency information for the virtual machine cannot be obtained.
Normal	 (Green)	The virtual machine is operating normally.

Virtual machines, servers, cache disks, and capacity disks are represented as the following dots.

Dot meaning	Dot on the ISM GUI	Description
Impact dot	 (Triangle in bottom right corner)	The selected dot indicates the item is affected. It has a triangle in the bottom right corner.
No impact dot	 (Frame around dot)	The selected dot indicates the item is not affected.

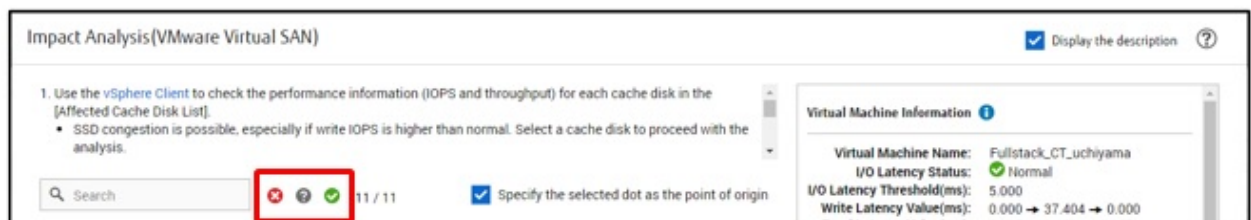
The first time it is displayed, it shows a selected dot to the left of the virtual machine.



In a selected dot, the  icon is displayed in the top left corner with a blue frame.

You can filter dots that are displayed.

You can filter the content that is displayed by entering the conditions into the "Filter." Dots that do not fit the conditions of the entered text turn gray and cannot be selected.

You can also filter for dots by a specified status using the status filter icons to the right of the "Filter."



You can show or hide dots by selecting the  /  icons to the right of the virtual machine, server, cache disk, or capacity disk.

Impact display

- Select the [Move the point of origin to the selected dot] checkbox to update the display of affected objects for selected dots.
- Clear the [Move the point of origin to the selected dot] checkbox to not update the display of affected objects even if you change your selection.
- If you select a virtual machine, a dot is displayed for the affected cache disks and capacity disks that make up the virtual disks of the virtual machine and the servers that make up these disks.
- If you select a server, a dot is displayed for the affected cache disks, capacity disks, and virtual machines that make up the server.

- If you select a cache disk or capacity disk, a dot is displayed for the affected servers that make up the selected disk and the virtual machines that make up the selected disk.

Detail information display area

This area displays detailed information about the dot selected in the configuration area for virtual machines and vSAN disks.

It also lists the affected virtual machine names, server names, cache disk names, and capacity disk names.




Selecting a virtual machine (selecting the dot for a virtual machine only)

This displays the virtual machine name, I/O latency status, I/O latency threshold (ms), write latency value (ms), and read latency value (ms).

It displays the affected server name, a list of cache disks, and a list of capacity disks.

Select the affected server name in [Server Name] to display the properties for that server.

The following statuses are displayed for the I/O latency status for virtual machine.

Status	Icon on the ISM GUI	Description
Error	 (Red)	Disk I/O latency has occurred and disk performance is declining.
Unknown	 (Gray)	Unable to get disk I/O latency information.
Normal	 (Green)	There is no disk I/O latency and disk performance is normal.

Select a virtual machine with the I/O latency status of "Error" to display the servers, cache disks, and capacity disks that are affecting the operation of the virtual machine.

The write latency value (ms) and read latency value (ms) are displayed in the following order: the latency value from 10 to 15 minutes ago → the latency value from 5 to 10 minutes ago → the latency value for the last 5 minutes.

Selecting a server (selecting the dot for a server only)

This displays the server name and OS type.

Select the server name in [Server Name] to display the properties for that server.

It displays a list of affected virtual machine names, a list of cache disks, and a list of capacity disks.

Selecting a cache disk (selecting the dot for a cache disk only)

This displays the cache disk name, disk type, and affected server name.

Select the affected server name in [Server Name] to display the properties for that server.

It displays a list of affected virtual machine names and a list of capacity disks.

Selecting a capacity disk (selecting the dot for a capacity disk only)

This displays the cache disk name, disk type, and affected server name.

Select the affected server name in [Server Name] to display the properties for that server.

It displays a list of affected virtual machine names and a list of capacity disks.

Analyze information about the affected servers, cache disks, and capacity disks to determine the cause of disk performance degradation.

I/O latency status

The I/O latency threshold (ms) is fixed at 5.000.

The default status for I/O latency is "Normal."

The conditions for determining that the I/O latency status is "Error" are as follows.

- All three read latency values are greater than or equal to the I/O latency threshold.
- All three write latency values are greater than or equal to the I/O latency threshold.

The conditions for determining that the I/O latency status is "Normal" are as follows.

- All six values, three read latency values and three write latency values, are below the I/O latency threshold.

The I/O latency status is not updated except for the above conditions.

2.10 Backup/Restore Hardware Settings

This function saves the hardware settings as a file, and can then export the saved file. The target hardware settings are the following:

- BIOS/iRMC settings of PRIMERGY, PRIMEQUEST 3000B, and PRIMEQUEST 4000 series
- Switch settings of VDX

After importing the exported files to a separate ISM, you can apply them to the target device. You can apply the imported BIOS/iRMC settings files to PRIMERGY, PRIMEQUEST 3000B, and PRIMEQUEST 4000 series. You can apply the imported switch settings files to VDX.

Figure 2.28 "Backup/Restore Hardware Settings" screen sample (GUI)

Status	Node Name	IP Address	Model Name	Last Backup	Type	Saved time	Description
Backup completed	server_rx2540s5	192.168.1.101	PRIMERGY RX2540 S5	Server (BIOS)	2020/04/02 12:37:33		
Backup completed	server_rx2530s5	192.168.1.102	PRIMERGY RX2530 S5	Server (iRMC)	2020/04/02 12:37:32		
Backup completed	server_rx2530s5	192.168.1.102	PRIMERGY RX2530 S5	Server (BIOS)	2020/04/02 12:38:28		
Backup completed	server_rx2530s5	192.168.1.102	PRIMERGY RX2530 S5	Server (iRMC)	2020/04/02 12:38:30		
Backup canceled	server_rx200s8	192.168.1.103	PRIMERGY RX200 S8	Server (BIOS)	2020/04/02 12:53:48		
Backup error	switch_vdx6740	192.168.1.104	VDX6740	Switch (iRMC)	-		
Export	storage_dx600s3	192.168.1.105	ETERNAUS DX600 S3	-	-		

Point

- The files for hardware settings are saved separately for BIOS and iRMC.
- When backing up the BIOS hardware settings, turn off the power of the server in advance.
- When backing up the switch settings, turn on the power of the hardware in advance.

2.10.1 Backup of the File of Backup Hardware Settings

Executable user

Administrator group	Other groups
Admin Operator Monitor	Admin Operator Monitor

Retrieve the hardware settings backup from the specified node.

For details, refer to "7.1.1 Backup Server Settings" or "7.2.1 Backup Settings of Switches and Storages" in "Operating Procedures."

2.10.2 Export of the File of Backup Hardware Settings

Executable user

Administrator group	Other groups
Admin Operator Monitor	Admin Operator Monitor

Export the specified already registered backup file.

For details, refer to "7.1.1 Backup Server Settings" or "7.2.1 Backup Settings of Switches and Storages" in "Operating Procedures."

2.10.3 Addition of Profiles from the File of Backup Hardware Settings

Executable user

Administrator group

Other groups

Admin Operator Monitor

Admin Operator Monitor

Convert the specified already registered backup to a profile and then add it.

For details, refer to "7.1.2 Create Profile from Backup Files" in "Operating Procedures."

2.10.4 Addition of Policies from the File of Backup Hardware Settings

Executable user

Administrator group

Other groups

Admin Operator Monitor

Admin Operator Monitor

Convert the specified already registered backup to a policy and then add it.

For details, refer to "7.1.3 Create Policy from Backup Files" in "Operating Procedures."

2.10.5 Import of the File of Backup Hardware Settings

Executable user

Administrator group

Other groups

Admin Operator Monitor

Admin Operator Monitor

Import an exported backup file.

For details, refer to "7.1.4 Import Server Settings" in "Operating Procedures."

2.10.6 Restoration of the File of Backup Hardware Settings

Executable user

Administrator group

Other groups

Admin Operator Monitor

Admin Operator Monitor

Apply the hardware settings of the specified already registered backup on the node.

For details, refer to "7.1.5 Restore Server Settings" in "Operating Procedures."

2.10.7 Deletion of the File of Backup Hardware Settings

Executable user

Administrator group

Other groups

Admin Operator Monitor

Admin Operator Monitor

Delete the specified already registered backup.

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Profiles].
2. From the menu on the left side of the screen, select [Backup / Restore Hardware Settings].
3. Select the link in the [Last Backup] field of the node you want to delete.
4. Select the hardware settings to be deleted. From the [Actions] button, select [Delete].



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 and performance information 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.

The following functions are provided:

- Display information for performance statistics retrieved from the monitored host
- Threshold monitoring for the Send/Receive Error rate and Drop rate
- Display packet analysis results showing information on the traffic rate and quality of communication [Note]
- Bottleneck Analysis to help identify and improve network degradation [Note]

[Note]: Deploy the Analysis VM to the hypervisor of the monitored host.



A virtual machine that analyzes traffic in a virtual environment is called an "Analysis VM."

2.11.1 Support Targets

For information on the supported software environments with this function, refer to "Support Matrix."

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

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

Select [DOWNLOADS] and select the target operating system.

The reference procedures are subject to change without notice.



To monitor virtual network adapters, some settings may be required for hypervisor or cloud management software to be used in advance.

2.11.2 Confirmation of Analysis VM

This function supports the following Analysis VM versions.

- Infrastructure Manager Analysis VM for VMware V2.0.0.

To use this function, the following resources must be added to the hypervisor on the host on which Analysis VM is running.

Additional number of CPU cores	Additional memory capacity	Additional disk capacity
2 cores	16 GB	40 GB

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 2.15 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]	Displays the CPU utilization rate per virtual network adapter.
Traffic information of virtual network adapter [Note]	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]: The upper limit of the number of virtual adapters that can be monitored by the function is 1000.

Table 2.16 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 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 functions supported for Packet Analysis of Virtual Network. an

Functions supported	Display item
Information of performance statistics retrieved from the monitored host	CPU usage [Note 1]
	CPU usage of VM vCPU
	CPU usage of virtual network adapter [Note 2]
	Traffic information of virtual network adapter [Note 3]
Packet analysis results showing information on details and quality of communication	Port traffic information
	Network traffic information
	Host traffic information
	Host quality information

[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.



Note

Xen cannot be used.

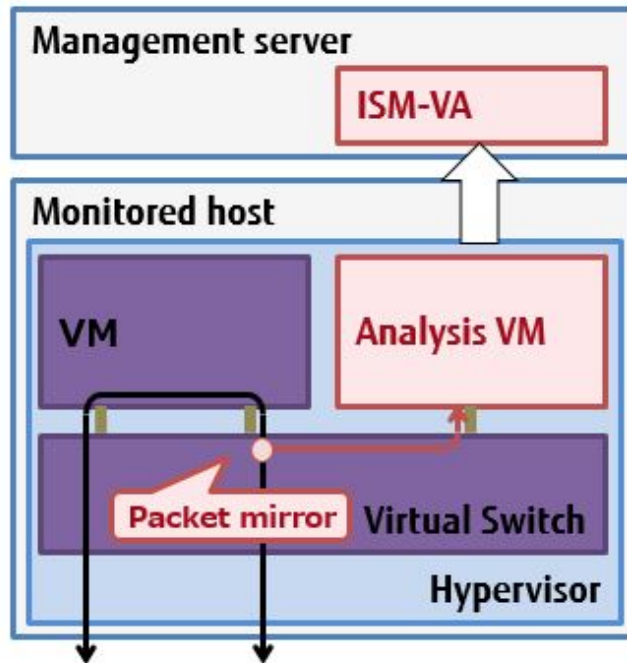
2.11.5 Operation of Packet Analysis of Virtual Network

To use Packet Analysis of Virtual Network, deploy Analysis VM to the hypervisor on the monitoring target host. Analysis VM analyzes actual packets on the virtual switch in order to retrieve the information that is required to specify the cause of a decrease in the communication performance. The targets for retrieval are as follows.

- 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 2.29 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.

2.11.6 Display Items of Bottleneck Analysis for Virtual Networks

Bottleneck Analysis for virtual networks analyzes the causes of performance degradation based on the information retrieved by Packet Analysis of Virtual Network and displays the results of the analysis.

Items that are displayed as potential causes are as follows.

Table 2.17 Potential causes that are displayed by Bottleneck Analysis

Cause	Description
Transmit thread overload	Packet loss in communication with an analysis target VM may have been caused by a high utilization rate of CPU by transmitting threads.
VM overload	Packet loss in communication with an analysis target VM may have been caused by a high utilization rate of CPU of an analysis target VM.
Transmit thread resource conflict	Packet loss in communication with an analysis target VM may have been caused by the effects of other processes.
VM resource conflict	Packet loss in communication with an analysis target VM may have been caused by the effects of other processes.

Cause	Description
Insufficient transmission buffer size of virtual NIC	Packet loss in communication with an analysis target VM may have been caused by insufficiency of the transmission buffer size of the virtual NIC.
Insufficient receive buffer size of virtual NIC	Packet loss in communication with an analysis target VM may have been caused by insufficiency of the receiving buffer size of the virtual NIC.

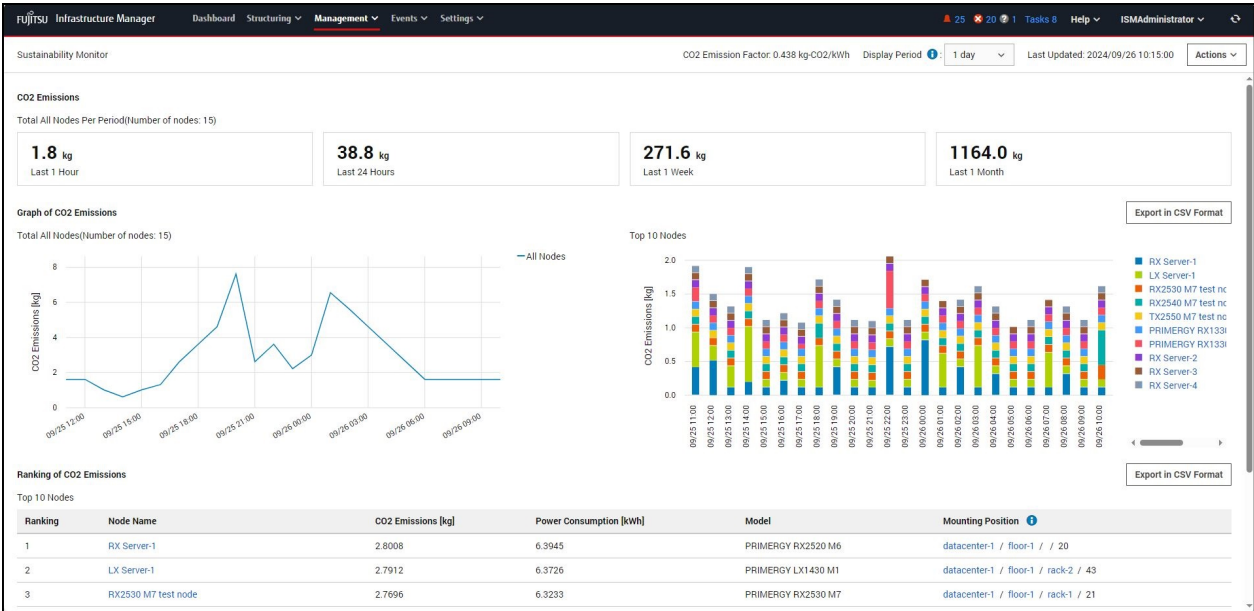
2.12 Sustainability Monitor

Sustainability Monitor is a function that monitors the power consumption of nodes and visualizes and provides the data converted to CO2 emissions per hour.

For example, you can use it for:

- Checking CO2 emissions up to one month in the past
- Analyzing CO2 emission trends and implementing power control settings for servers
- Aggregating total annual CO2 emissions to measure the effect of annual CO2 reductions

Figure 2.30 Sustainability Monitor



2.12.1 Support Targets

For information on the supported software environments with this function, refer to "Support Matrix."

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

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

Select [DOWNLOADS] and select the target operating system.

The reference procedures are subject to change without notice.



- If you have deleted the power consumption of the monitoring items of the node, this function is not applicable.

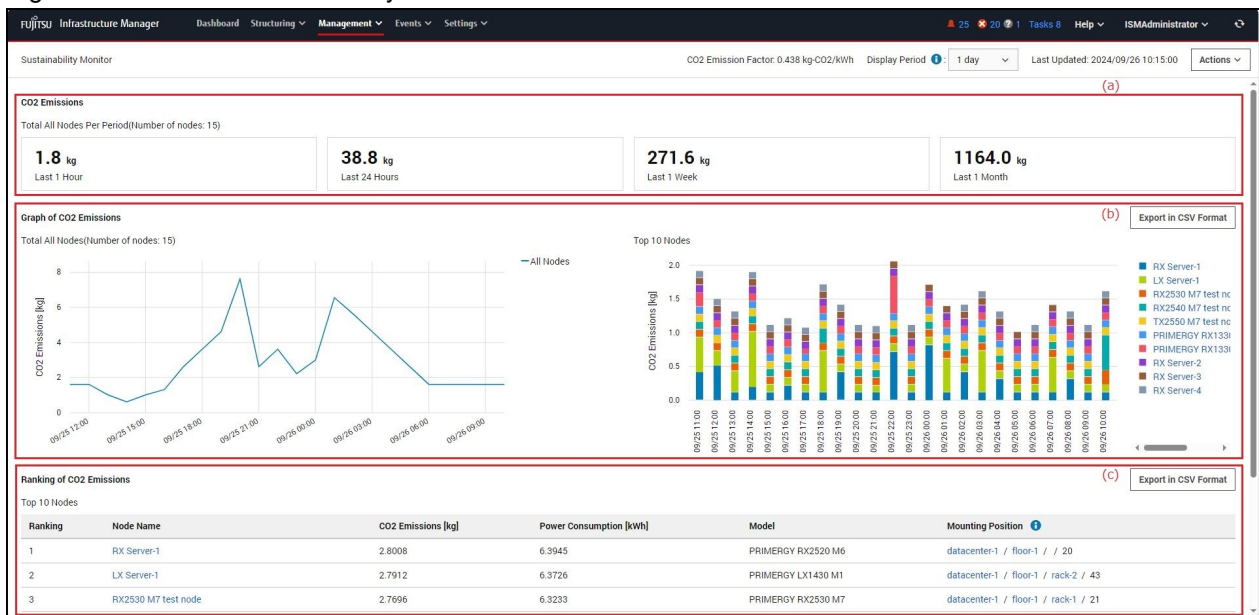
- In the following cases, the data cannot be retrieved. The data for the corresponding period will be 0.
 - the node is in maintenance mode
 - ISM service is stopped

2.12.2 GUI for Sustainability Monitor

From the Global Navigation Menu on the ISM GUI, select [Management] - [Sustainability Monitor] to display the "Sustainability Monitor" screen.

The contents of the GUI screen are as follows:

Figure 2.31 GUI for Sustainability Monitor



(a) CO2 Emissions

The total CO2 emissions of all nodes are displayed for each period. There are four types of total values: last one hour, last 24 hours, last one week, and last one month.

You can easily identify the latest CO2 emissions.

(b) Graph of CO2 Emissions

CO2 emissions for the period selected in the [Display Period] pull-down box are displayed in graph form.

You can check the transition of CO2 emissions for the selected period.

The following two types of graph are displayed.

- Total of All Nodes

The total CO2 emissions of all nodes are displayed in a line graph.

- Top 10 Nodes

The CO2 emissions of the top 10 nodes with the highest CO2 emissions are displayed in a stacked bar graph. Selecting a node name in the graph or in the legend of each node displays the Details of Node screen, where you can check detailed information about the selected node.

The [Display Period] pull-down box changes the display unit of the graph.

- 1 day: displays the data for the last 24 hours in hourly basis
- 1 week: displays the data for the last 7 days daily basis.
- 1 month: displays the data for the last 30 days in daily basis.

(c) Ranking of CO2 Emissions

The top 10 nodes with the highest CO2 emissions for the period selected in the [Display Period] pull-down box are displayed in a ranking.

You can easily identify which nodes have the highest CO2 emissions for the selected period.

Selecting a node name displays the Details of Node screen, where you can check detailed information about the selected node. Selecting a mounting position displays the "Details of Datacenter" screen, "Details of Floor" screen, and "Details of Rack" screen, respectively.

2.12.3 Settings of CO2 Emission Factor

Executable user

Administrator group

Admin

Operator

Monitor

Other groups

Admin

Operator

Monitor

The user can set the CO2 emission factor to be used for calculating CO2 emissions. Since the CO2 emission factor differs for each electricity provider, the user needs to check and set the appropriate factor. Check the information published by the relevant government agencies and electricity providers in each country. The initial value is 0.438.

For detailed procedures, refer to "4.12.1 Set CO2 Emission Factor" in the "Operating Procedures."

2.12.4 Export in CSV Format

Executable user

Administrator group

Admin

Operator

Monitor

Other groups

Admin

Operator

Monitor

You can export the data displayed in Sustainability Monitor in CSV format.

The examples for the settings of CSV file is displayed below.

Table 2.18 Transition of CO2 emissions and power consumption for each node

Item Name	Description
Node Name	Node name
CO2 Emissions	CO2 emissions of the node
Power Consumption	Power consumption of the node
Model Name	Model name of the node
Mounting Position	Node mounting position
Date and Time	Aggregation date and time Outputs in the date and time of the ISM GUI time zone

The contents of the CSV file are CO2 emissions and power consumption data for each node on an hourly basis. Calculating the total CO2 emissions on an hourly basis or daily basis, you can recreate Graph of CO2 Emissions - Total All Nodes in a line graph.

Table 2.19 Data examples for transition of CO2 emissions and power consumption per node

Node Name	CO2 Emissions [kg]	Power Consumption [kWh]	Model Name	Mounting Position	Date and Time
Server001	1.2345	2.3456	PRIMERGY RX2530 M7	DC1 / Floor1 / Rack1 / 30-31	2024-08-01 12:00:00
Server002	1.2345	2.3456	PRIMERGY RX2530 M7	DC1 / Floor1 / Rack1 / 32-33	2024-08-01 12:00:00

Node Name	CO2 Emissions [kg]	Power Consumption [kWh]	Model Name	Mounting Position	Date and Time
Server003	1.2345	2.3456	PRIMERGY RX2530 M7	DC1 / Floor1 / Rack1 / 34-35	2024-08-01 12:00:00
Server001	1.2345	2.3456	PRIMERGY RX2530 M7	DC1 / Floor1 / Rack1 / 30-31	2024-08-01 11:00:00
Server002	1.2345	2.3456	PRIMERGY RX2530 M7	DC1 / Floor1 / Rack1 / 32-33	2024-08-01 11:00:00
Server003	1.2345	2.3456	PRIMERGY RX2530 M7	DC1 / Floor1 / Rack1 / 34-35	2024-08-01 11:00:00
...

Table 2.20 Ranking of CO2 Emissions

Item Name	Description
Collection Period	Aggregation period Settings: one day, one week, or one month
Ranking	Ranking of CO2 emissions for the aggregation period
Node Name	Node name
CO2 Emissions	CO2 emissions of the node
Power Consumption	Power consumption of the node
Model Name	Model name of the node
Mounting Position	Node mounting position

This is the ranking data displayed in Ranking of CO2 Emissions.
It includes data for one day, one week, and one month.

Table 2.21 Data examples for Ranking of CO2 Emissions

Collection Period	Ranking	Node Name	CO2 Emissions [kg]	Power Consumption [kWh]	Model Name	Mounting Position
one day	1	Server001	1.2345	2.3456	PRIMERGY RX2530 M7	DC1 / Floor1 / Rack1 / 30-31
one day	2	Server002	1.2345	2.3456	PRIMERGY RX2530 M7	DC1 / Floor1 / Rack1 / 32-33
one day	3	Server003	1.2345	2.3456	PRIMERGY RX2530 M7	DC1 / Floor1 / Rack1 / 34-35
...
one day	10	Server010	1.2345	2.3456	PRIMERGY RX2530 M7	DC1 / Floor1 / Rack1 / 30-31
one week	1	Server001	1.2345	2.3456	PRIMERGY RX2530 M7	DC1 / Floor1 / Rack1 / 32-33
one week	2	Server002	1.2345	2.3456	PRIMERGY RX2530 M7	DC1 / Floor1 / Rack1 / 34-35
...

For detailed procedures, refer to "4.12.2 Export CO2 Emissions and Power Consumption" in "Operating Procedures."

For information on how to estimate the disk space required for export, refer to "[3.2.1.7 Estimation of required disk space for CSV export of Sustainability Monitor](#)."

2.13 Functions of ISM for PRIMEFLEX

The ISM for PRIMEFLEX function is the ISM with the Virtualized Platform Expansion function added. In addition to the functions of ISM, the following functions are provided. These functions can be used when the ISM operation mode is "Advanced for PRIMEFLEX." "Cluster Management" is also available when the ISM operation mode is "Advanced."

- [2.13.1 Cluster Management](#)
- [2.13.2 Cluster Creation](#)
- [2.13.3 Cluster Expansion](#)
- [2.13.4 Rolling Update](#)
- [2.13.5 Node Disconnection/Reintegration](#)
- [2.13.6 Backup](#)
- [2.13.7 Restore](#)
- [2.13.8 Cluster Stop](#)
- [2.13.9 Batch Collection of vSAN Logs for a VMware vSAN Cluster](#)
- [2.13.10 Generation Switching](#)

To use ISM for PRIMEFLEX functions, refer to the "PRIMEFLEX Design Guide," "PRIMEFLEX Operation & Maintenance Guide," and "PRIMEFLEX Server Expansion Guide" in advance.

If you need these manuals, contact your local Fujitsu customer service partner.

2.13.1 Cluster Management

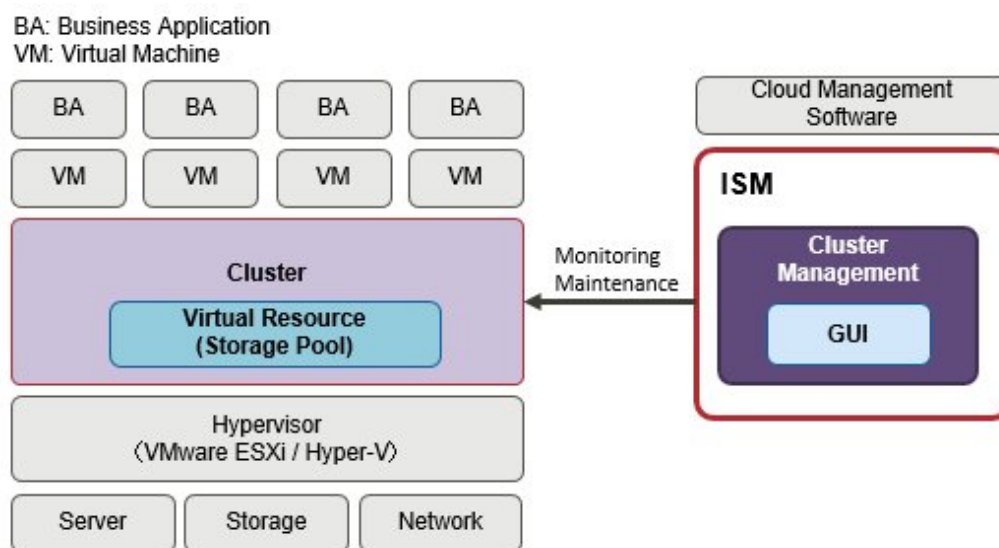
Cluster Management provides functions to display the cluster status.

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 for the smooth maintenance of clusters and determining the addition (provisioning) of resources.

For the types of clusters that can be managed and their requirements, refer to "[2.13.1.2 Environments supported by Cluster Management](#)."

This function can be used when the ISM operation mode is "Advanced."

Figure 2.32 Overview of the Cluster Management operation



Cluster Management provides various GUIs for cluster management that are linked with the ISM GUI and features the following functions:

- List of clusters and summary display, including cluster statuses

- Display of detailed cluster information

For the cluster configuration information, information such as the following is displayed.

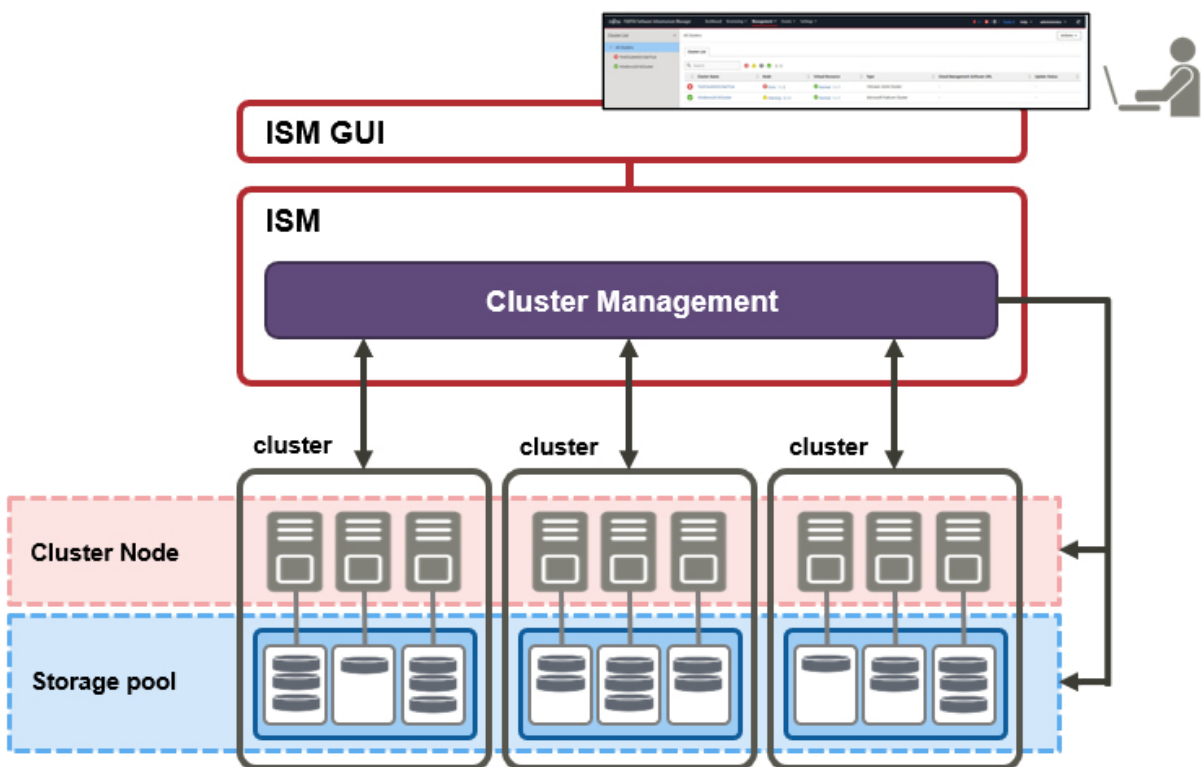
- Information of the nodes configuring the cluster
- Information of the virtual resources in the cluster
- Parameter setting information of Cluster Creation and Cluster Expansion (not available with Advanced mode)
- A widget that is available to monitor the clusters from Dashboard

2.13.1.1 GUI for Cluster Management

Cluster monitoring and management can be used from the ISM GUI.

The following is the environment configuration for operating Cluster Management.

Figure 2.33 Configuration of the operating environment for Cluster Management



The following displays the functions of each screen and their mutual display relationships.

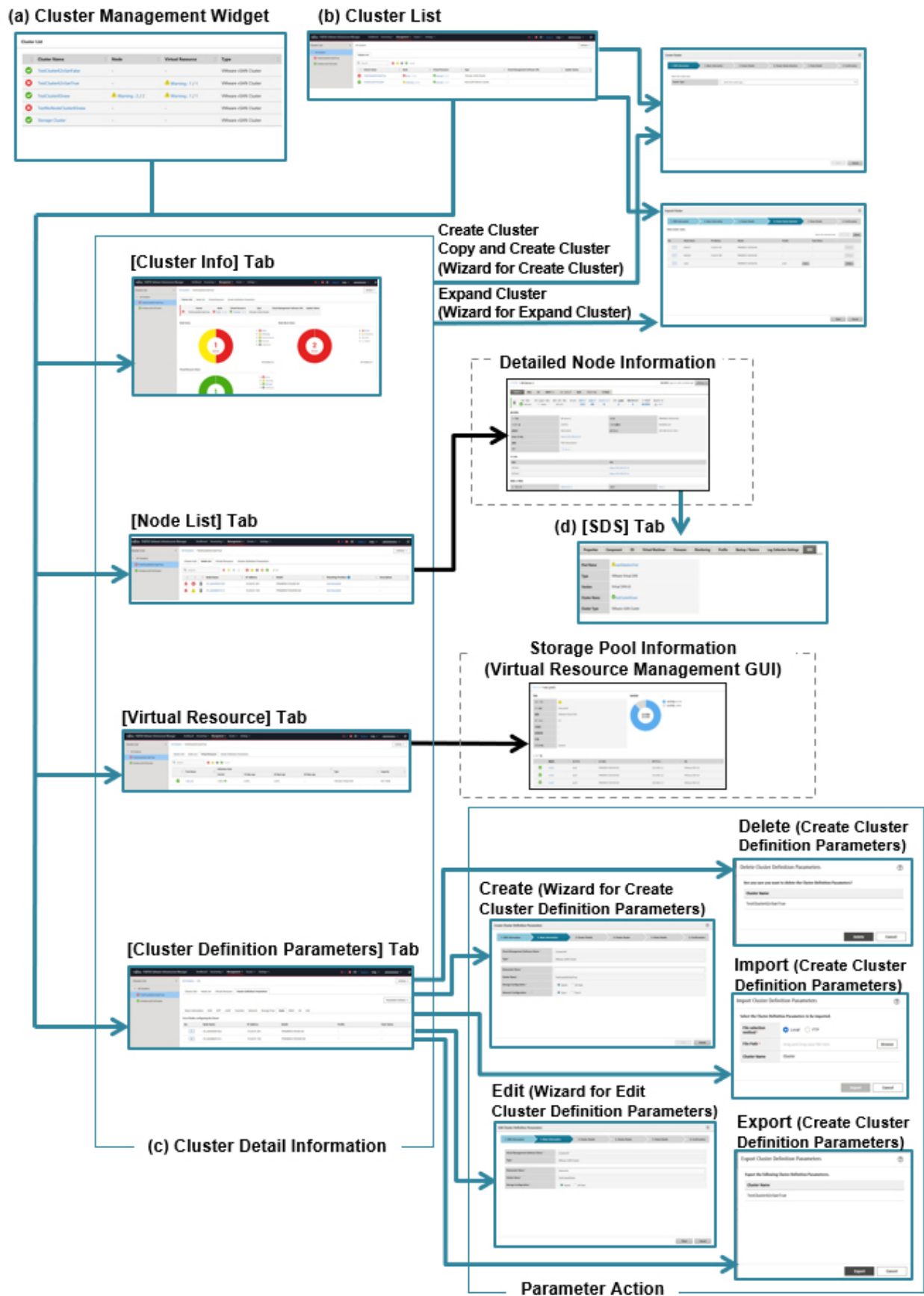
The GUI for Cluster Management ((a) - (d) in the [Figure 2.34 GUI for Cluster Management](#)) displays various kinds of information on the clusters.

More detailed information can be checked, linked with node information (the "Node List" screen) and virtual resource information (GUI for Virtual Resource Management).

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 2.34 GUI for Cluster Management



(a) Cluster Management Widget

On the ISM Dashboard, the 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 "(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 the GUI for Cluster Management.

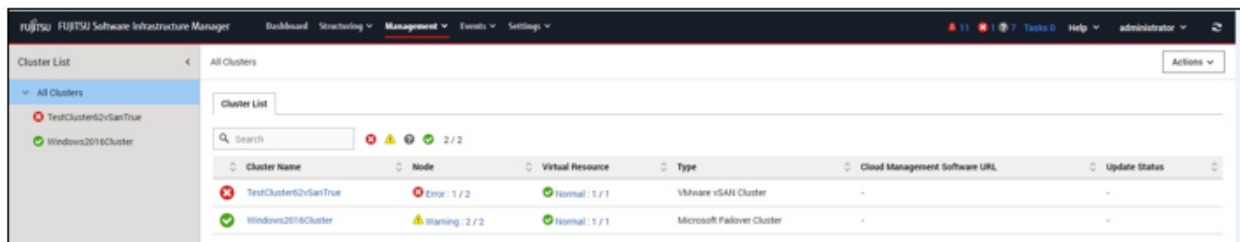
Cluster List screen

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 2.35 Cluster List screen



Details of Cluster screen (tab display screen)

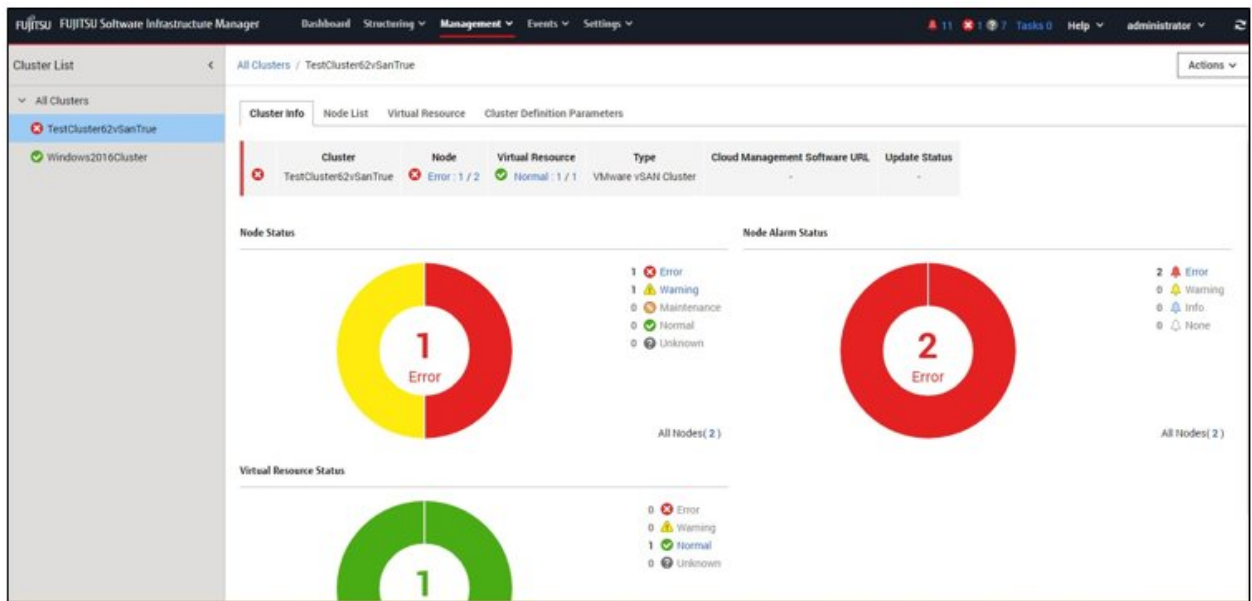
Selecting a cluster name on the cluster list screen opens the Details of Cluster screen for the selected cluster, allowing you to check the information on the nodes and the components that configure the cluster.

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 states (statuses, alarms), and the states of virtual resources.



[Node List] tab

A list of the information of the nodes configuring the cluster is displayed. A status of the node, its position and other information is displayed.

If you select a 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.

Node Name	IP Address	Model	Mounting Position	Description
SV_MAN001522	10.00.01.201	PRIMERGY RX200 S8	Not Mounted	-
SV_MA0001213	10.00.01.102	PRIMERGY RX2530 M2	Not Mounted	-

[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 on the virtual resource detailed information screen.

For the GUI for Virtual Resource Management, refer to ["2.9.2 GUI for Virtual Resource Management"](#) or to the ISM online help.

Pool Name	Utilization Rate	Type	Capacity
vsan_001	1.62%	VMware Virtual SAN	957.73GB

[Resource Planning] tab

Select the [Resource Planning Actions] button and then select the action menu to execute the prediction according to the wizard you just started.

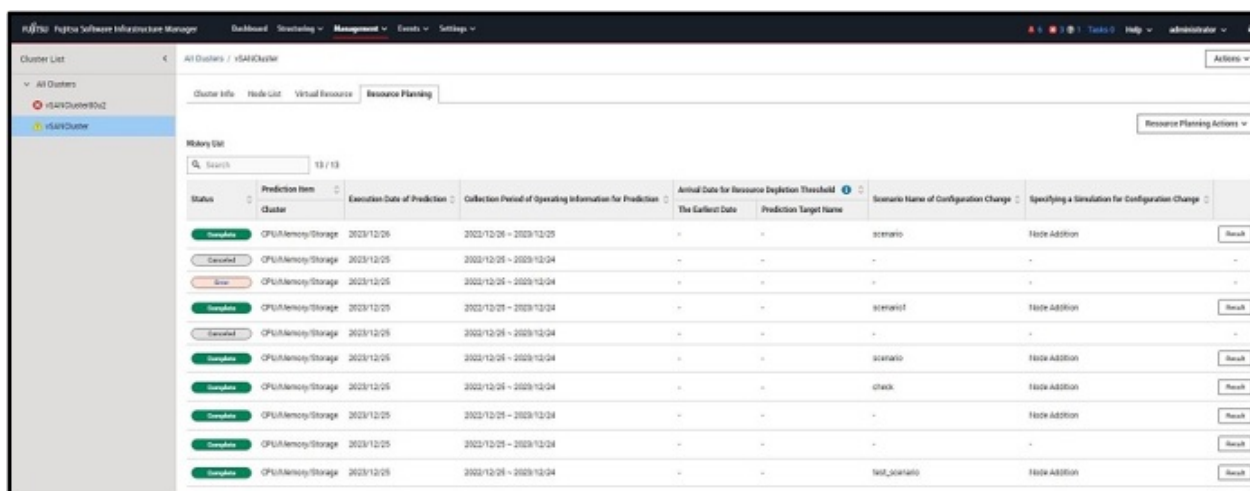
You can also use Simulated Configuration Change to plan future resources.

Simulated Configuration Change is a function that outputs the estimated results of utilization and usage based on the amount of resources at the time of configuration change from the predicted results based on periodicity and trend changes for resources.

The results of Resource Planning executed are displayed on the history list.

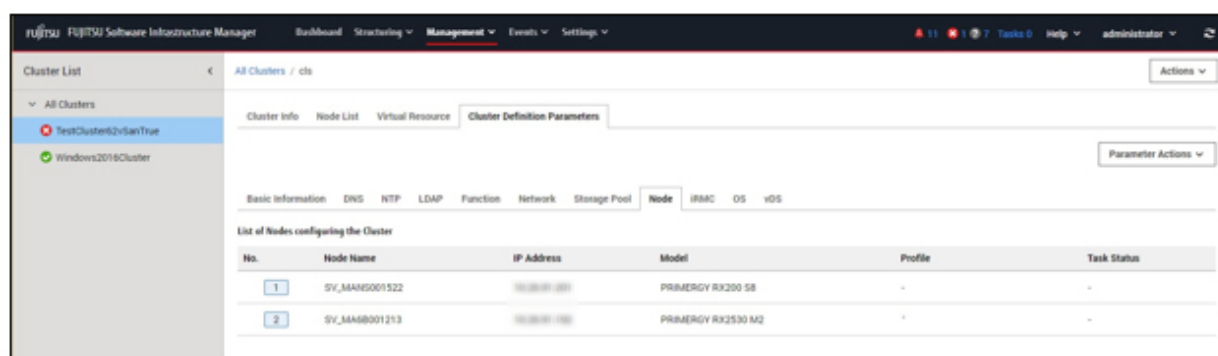
Selecting the [Result] button to display the prediction in a graph.

For description of the Resource Planning screen, refer to the ISM online help.



[Cluster Definition Parameters] tab (not available with Advanced mode)

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.

Tab name	Description
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" or "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 a menu item, 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 upper-right of the screen displays the following menu and allows you to execute operations for the cluster.

- Refresh Cluster Information

Selecting this menu item retrieves the cluster information and refreshes the information.

Refer to "[2.13.1.3 Refreshing cluster information](#)" for details on how to execute the operations.

- Create Cluster (not available with Advanced mode)

Selecting this menu item opens the "Create Cluster" wizard. Follow the wizard to create a cluster.

For details, refer to "[2.13.2 Cluster Creation](#)." For the procedure, refer to "Operating Procedures."

- Copy and Create Cluster (not available with Advanced mode)

Selecting this menu item opens the "Create Cluster" wizard. Follow the wizard to create a cluster reference.

For details, refer to "[2.13.2 Cluster Creation](#)." For the procedure, refer to "Operating Procedures."

- Expand Cluster (not available with Advanced mode)

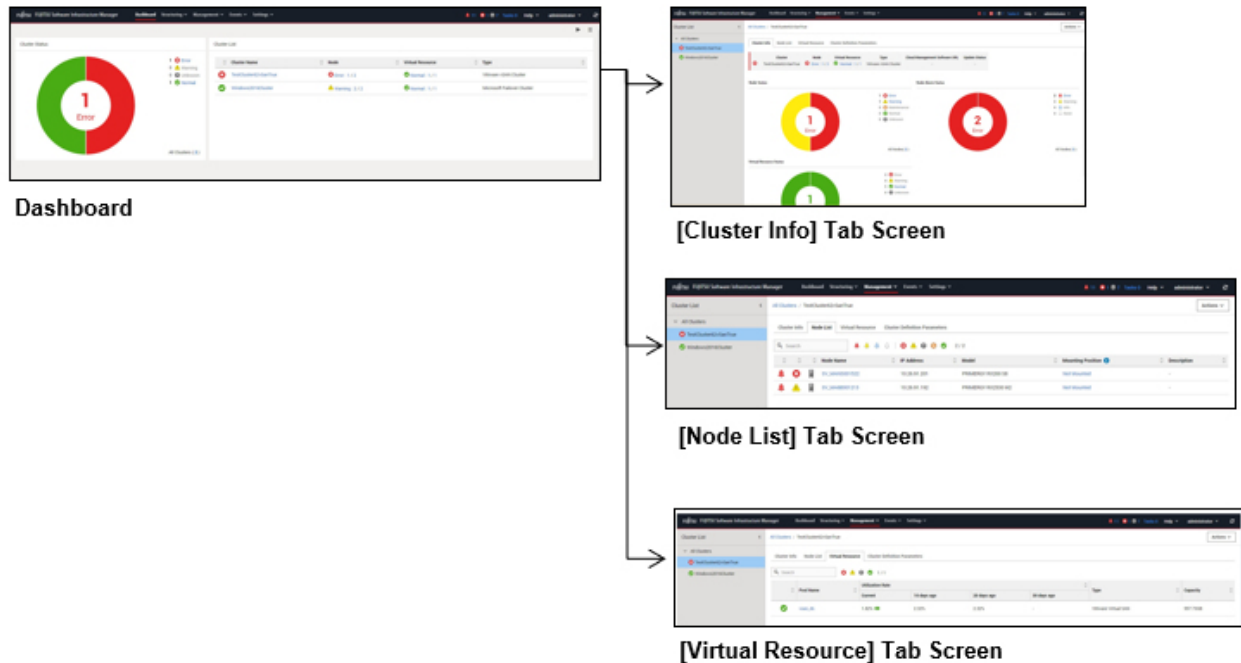
Selecting this menu item opens the "Expand Cluster" wizard. Follow the wizard to add servers to the cluster.

For details, refer to "[2.13.3 Cluster Expansion](#)." For the procedure, refer to "Operating Procedures."

Operation in link with Dashboard

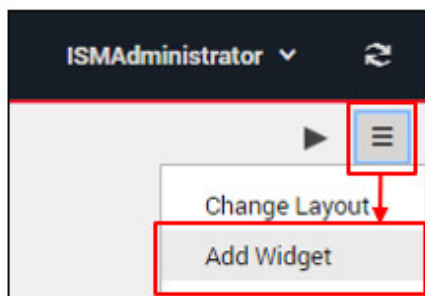
By adding the information display screen (widget) related to Cluster Management to the ISM Dashboard, you can, with just one click on the Dashboard, display the information on clusters and components that configure each cluster (nodes and storage pools) for which you want to check the details.

Figure 2.36 Operation in link with Dashboard



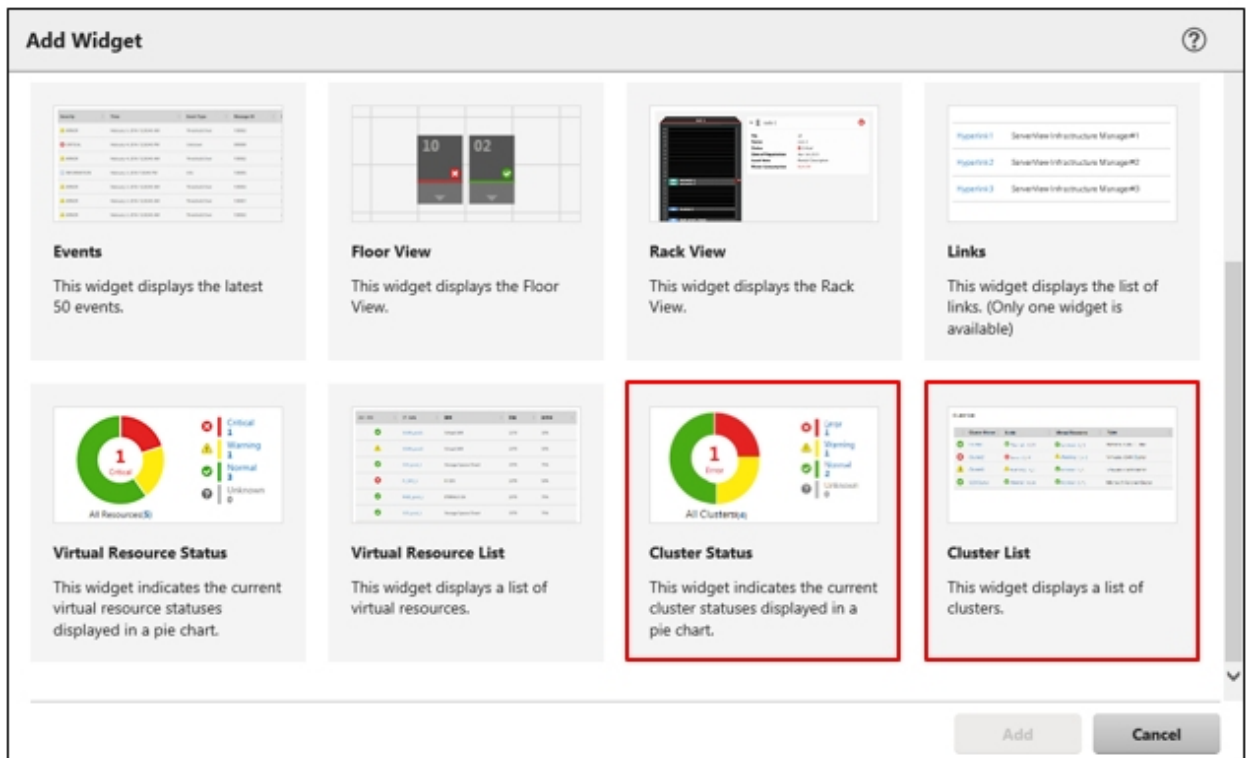
The procedure for adding widgets to the ISM Dashboard is as follows.

1. From the [≡] at the top of the screen, select [Add Widget].

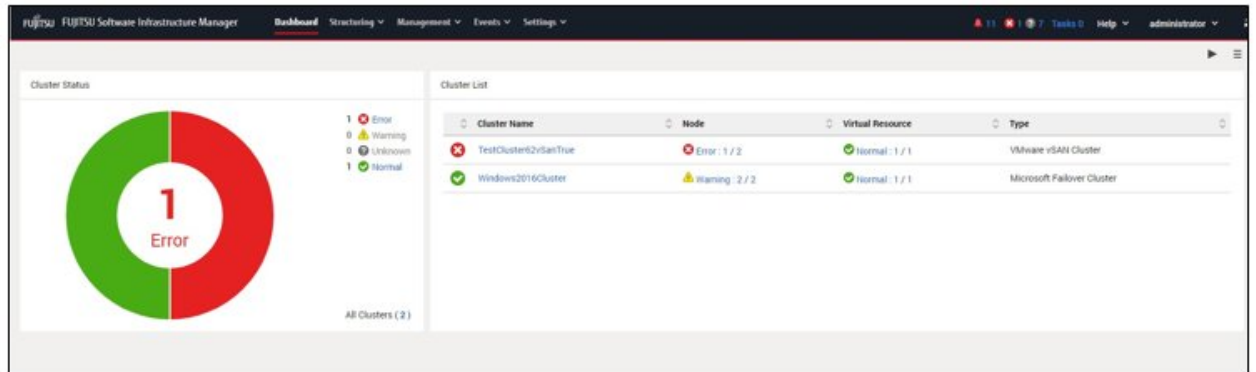


A menu for adding widgets is displayed.

- "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 ISM GUI, 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.

Properties	Component	OS	Virtual Machines	Firmware	Monitoring	Profile	Backup / Restore	Log Collection Settings	Boot Info	SDS
Pool Name	✓vsan_ds									
Type	VMware Virtual SAN									
Version	6.5.0 13932383									
Cluster Name	✖TestCluster62vSanTrue									
Cluster Type	VMware vSAN Cluster									

Selecting the cluster name displays the cluster information screen.

Selecting the pool name displays a 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."

2.13.1.2 Environments supported by Cluster Management

Cluster Management supports the following environments.

- VMware Virtual SAN 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.

For information on the vSAN cluster environments supported by Cluster Management, refer to "Support Matrix."

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

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

Select [DOWNLOADS] and select the target operating system.

The reference procedures are subject to change without notice.

2.13.1.3 Refreshing cluster information

To retrieve information on the virtualized platform on the ISM GUI or to refresh the displayed contents, you must refresh the information from the ISM GUI.

If you are checking the virtual resources from the GUI for Cluster Management, 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 "2.13.1.1 GUI for Cluster Management."



You cannot cancel a task whose task type is "Refresh Virtual Resource." Wait until the task completes.

For information about when to refresh cluster information, refer to "[2.9.3.3 Updates of virtual resource information.](#)"

2.13.1.4 Management and monitoring of clusters



Monitoring and operation of clusters can be executed by using Cluster Management.

The following types of monitoring can be executed using the GUI for Cluster Management.

- Monitoring of clusters
- Monitoring of the nodes configuring the cluster
- Monitoring of virtual resources on a cluster

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 configuring the cluster and the storage pool configured in the cluster can be checked.

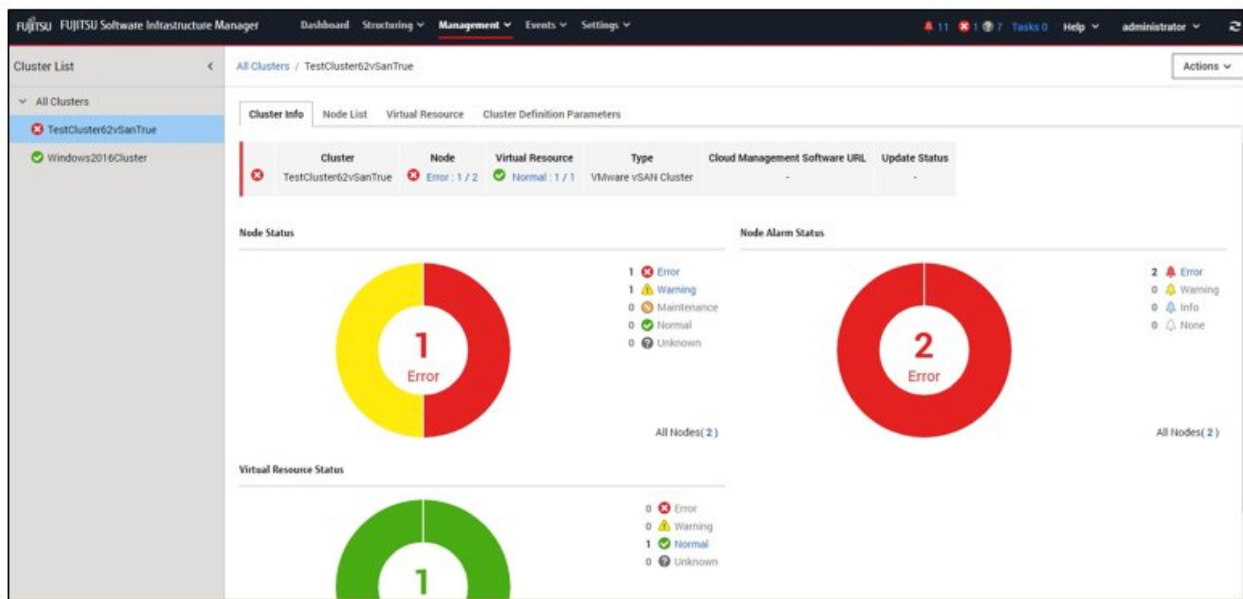


When you select a cluster name, the display moves to the details of cluster screen.

On the details screen, information such as a 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.

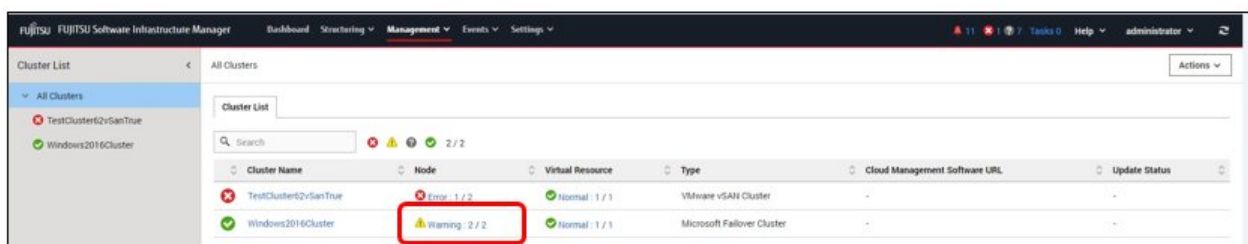
Also, the storage pool configured in the cluster can be checked on the [Virtual Resource] tab screen.



The status (clusters, nodes, and virtual resources) displayed on the "Cluster List" screen has the following severity levels.

Status	Displayed Icon	Severity	Description
Error		High	Fatal errors have occurred in the monitoring targets. This is displayed with the highest priority of all statuses.
Warning		Medium	Errors have occurred 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 "Warning" targets.
Normal		-	This is the normal status with no errors in the monitoring targets.

The number corresponding to the status of the node and virtual resources is displayed in the following format.



[Number of managed nodes that correspond to the status] / [Total number of managed targets]

[Number of managed nodes that correspond to the status] displays the number of targets in the most severe status.

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 on the Details of Cluster screen.

The targets in error statuses are filtered and displayed.

By knowing which components that compose the cluster are in an error status, you can quickly determine whether the cluster operation is robust.

In addition, monitoring from the Cluster Management widget in the ISM Dashboard can be executed.

For the Cluster Management widget, refer to ["2.13.1.1 GUI for Cluster Management"](#) - ["Operation in link with Dashboard."](#)

Monitoring of clusters

When selecting the [Cluster Info] tab, the details of cluster screen is displayed.

For the contents of the screen, refer to "[2.13.1.1 GUI for Cluster Management](#)" - "[Details of Cluster screen \(tab display screen\)](#)." In addition, for detailed information on displayed information, refer to the ISM online help.



Point

For details on how to identify the specific error location and its corrective actions, or to recover from an error, execute the procedures by following the manual for the relevant product.

The details of an error for a cluster and where it occurred can be confirmed as follows.

For VMware Virtual SAN cluster

The "Health" of the vSAN is checked on either the ISM GUI or in the vSphere Web Client.

1. From the cluster list on the ISM GUI, check "Cluster Name."
2. Sign in to vSphere Web Client and in the [Hosts and Clusters] tab, select the cluster name previously checked in Step 1.
If it is operating normally, there is no mark, and any errors are marked in red.
3. From the [Monitor] tab, select [Virtual SAN] - [Health].
4. Refer to the "Test result" and identify the error contents.

Execute the following after recovering from an error.

1. Sign in to the vSphere Web Client, and select the cluster name in "Hosts and Clusters."
2. From the [Monitor] tab - [Virtual SAN] - [Health], execute [Retest]. Check that the test result that was "Failed" has changed to "Passed."
3. On the cluster list screen on the ISM GUI, select [Refresh Cluster Information] from the [Actions] button, and check that the status has returned to normal.

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 "[2.13.1.1 GUI for Cluster Management](#)" - "[\[Node List\] 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 details 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.

The details of an error for node can be confirmed as follows.

1. Select the alarm status of the node indicating the error.
The "Correlated Event" screen is displayed.
2. On the "Correlated Event" screen, sort by the column name "Severity" to check the more severe events.

Monitoring of virtual resources on a cluster

When selecting the [Virtual Resource] tab, the SDS storage pool configured in the cluster is displayed.

Information such as storage pool states, storage utilization is displayed.

For the contents of the screen, refer to "[2.13.1.1 GUI for Cluster Management](#)" - "[\[Virtual Resource\] 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 information screen of the virtual resources and can check the detailed information about the storage pool.

For virtual resource monitoring, refer to "[2.9 Virtual Resource Management](#)."

For the details of an error for virtual resources and where it occurred, refer to "[2.9.3.2 Identification of the errors in storage pools](#)."

2.13.1.5 Resource Planning

Resource Planning collects the historical resource health information of vSAN cluster from the vCenter Server and displays the resource of prediction of resource utilization up to one year later in a graph.

Indicates when resources will run out based on the predicted results considering periodicity and trend changes.

You can also use Simulated Configuration Change to plan future resources.

It supports budgeting and operations related to increasing the resources of virtualized platform. Resource Planning provides transition display of the resource utilization and usage of the following vSAN cluster.

- storage for vSAN cluster
- CPU
- memory



Resource health information is retrieved from vCenter Server. Health information is the resource information used by the virtual machine and available resource information. This may differ from the capacity of CPU, memory, and storage installed on the physical server.

2.13.1.5.1 Execution of Resource Planning



Resource Planning runs on a cluster basis. When executing Resource Planning, ISM retrieves the historical resource health information from the cloud management software to predict the resource usage up to one year later.

The results are added as a result list in "History List" on the [Resource Planning] tab.

Procedure to execute Resource Planning

To execute Resource Planning, select the target cluster from the "Cluster" screen. Execute the function from the [Resource Planning] tab - [Resource Planning Actions] button.

For the procedure to execute Resource Planning, refer to "6.3.1 Execute Resource Planning" in "Operating Procedures."

Point

- It takes about 10 minutes to complete the prediction. You can check the prediction status on the "Tasks" screen. To check the task status of Resource Planning, refer to "[2.14.4 Task Management](#)."
- In order to make a prediction, at least two weeks of health information must be stored in the cloud management software each day from the start of the retrieval period for the health information used for the prediction. Resource Planning uses health information for up to one year each day.
- To check if the health information is enabled in cloud management software, refer to "[3.8.2 Pre-settings for Statistics Collection Intervals in vCenter Server](#)."

Note

- There is an upper limit to the number of clusters that can be predicted simultaneously. This limit is 10 for the entire ISM-VA. If you execute predictions for more than the maximum number of clusters at the same time, the maximum number of predictions are executed first. The remaining clusters are executed after the previous execution of the prediction has finished.
- Prediction cannot be executed concurrently on the same cluster. If you make predictions for the same cluster at the same time, the predictions made later will fail.

2.13.1.5.2 Displaying Resource Planning result



When execution of Resource Planning is completed, the [Result] button is displayed in the result list of "History List." Select the [Results] button to view the results of the execution.

When executing Simulated Configuration Change, the predicted results will show utilization and usage calculated with capacity size that include the added disks, CPUs and memories.

The prediction status displayed in the history list are as follows.

Table 2.22 Status of Prediction

Status	Description
Waiting	Status in which the prediction has not started
Predicting	Status in which the prediction ongoing When a cluster is in this status, another prediction cannot be started on that cluster.
Complete	Status in which the prediction completed By selecting the [Result] button, prediction is displayed in a graph.
Canceling	Status in which the prediction canceling
Canceled	Status in which the prediction cancelled
Error	Status in which abnormality occurred and prediction failed The cause of the error is output to the operation log.

Point

A maximum of 100 lists are recorded for one cluster. If you execute a prediction with a history greater than 100, it will be deleted from the oldest.

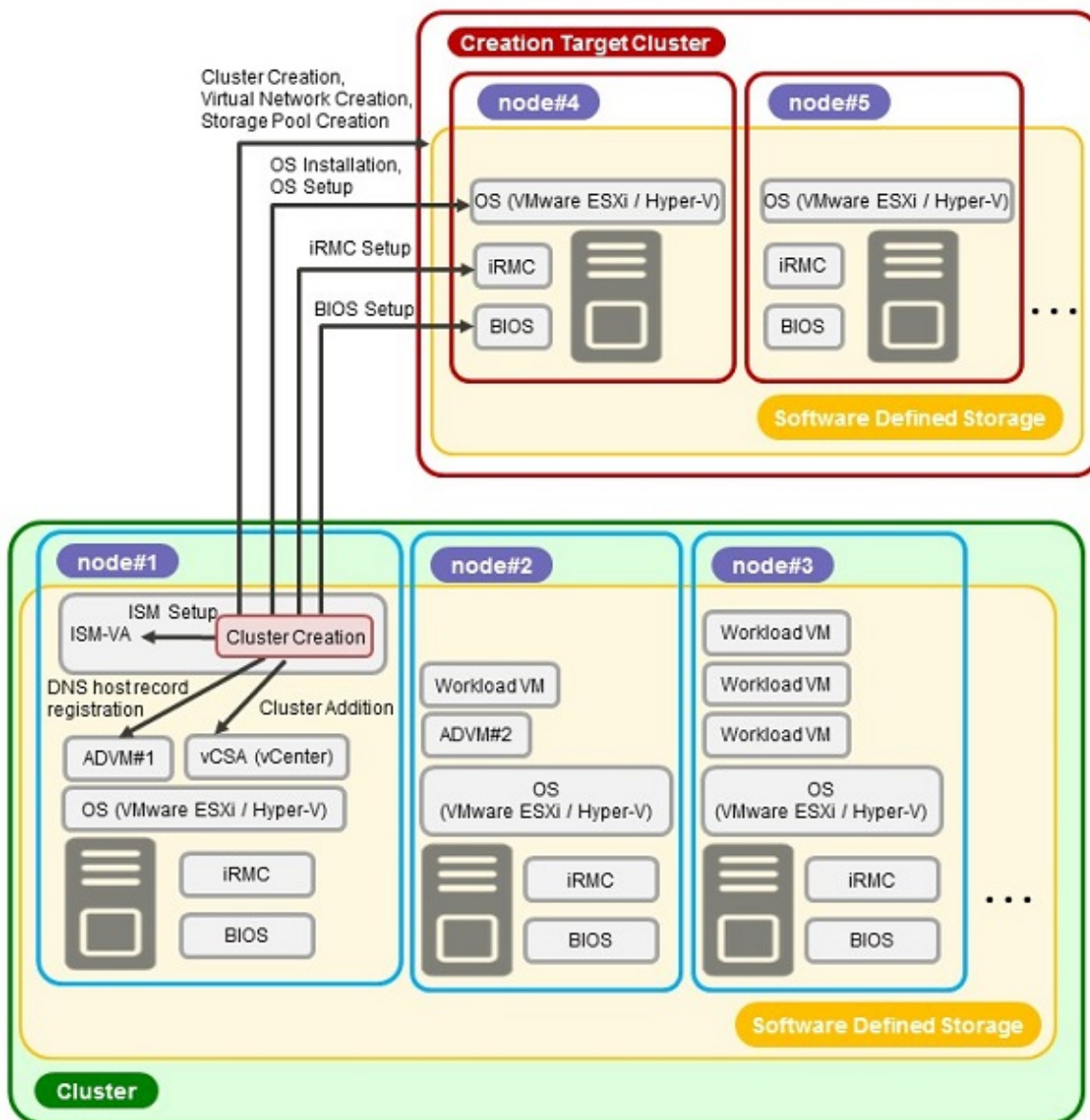
2.13.2 Cluster Creation

Cluster Creation is a function that creates new clusters to expand the resources of the virtualized platform environments of PRIMEFLEX HS/PRIMEFLEX for VMware vSAN. This function links with Profile Management in ISM and reduces the workload of the user by automating the operations for the cluster creation and installing an OS on the target server and adding the server 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 settings of the OS of the servers for creating new clusters
- Addition of servers for creating new clusters to the new cluster environment

Figure 2.37 Overview of Cluster Creation operation



ADV#1, ADV#2: An ADV# dedicated to PRIMEFLEX HS/PRIMEFLEX for VMware vSAN /PRIMEFLEX for Microsoft Storage Spaces Direct/PRIMEFLEX for Microsoft Azure Stack HCI
vCSA(vCenter): vCenter Server Appliance

2.13.2.1 Automatic setting item

By using Cluster Creation, the following items are set automatically.

Table 2.23 PRIMEFLEX for VMware vSAN automatic setting item list

Automatic setting order	Automatic setting item	Description
1	Profile Assignment	<ol style="list-style-type: none"> 1. Set BIOS settings for the servers configuring a new cluster 2. Set iRMC settings for the servers configuring a new cluster 3. Install an OS for the servers configuring a new cluster
2	ESXi patch application	<ol style="list-style-type: none"> 1. Transfer VMware ESXi patch files and scripts to run before and after VMware ESXi patch application 2. Run a script to execute before the VMware ESXi patch application 3. OS Reboot 4. Apply VMware ESXi patches 5. Run a script to execute at the VMware ESXi patch application 6. OS Reboot 7. Delete VMware ESXi patch files 8. Retransfer scripts to run before and after VMware ESXi patch application 9. Run a script to execute after the VMware ESXi patch application 10. OS Reboot 11. Remove scripts to run before and after VMware ESXi patch application
3	DNS host record registration	<ol style="list-style-type: none"> 1. Register DNS for the ESXi servers for creating a new cluster (Do not register when using a configuration that does not use the ADVN of the PRIMEFLEX configuration)
4	OS settings	<ol style="list-style-type: none"> 1. Enable and start the ESXi shell 2. Enable and start the SSH service 3. Apply the VMware SMIS Provider (only set for PRIMERGY M4 series and VMware ESXi 6.5) 4. Enable the ixgben driver (only set for PRIMERGY M4 series, VMware ESXi 6.5 and VMware ESXi 6.5 Update 1) 5. Add local administrator users 6. Set a host name to FQDN 7. Enable SSL v3 (only set for PRIMERGY M4 series / PRIMERGY M5 series) 8. Disable IPv6 9. Set an IP address for secondary DNS servers 10. Set a DNS suffix 11. Set an IP address for the NTP server 12. Set a firewall for the NTP client 13. Execute the NTP client service 14. Set the power management settings of the host to high performance 15. Restart OS

Automatic setting order	Automatic setting item	Description
		16. Add an adapter to the virtual distributed switch (virtual distributed switch for workload/virtual distributed switch for management) 17. Set an NIC to the virtual distributed switch (virtual distributed switch for workload/virtual distributed switch for management) 18. Set an NIC to the Management Network 19. Set Active Directory authentication settings for ESXi of the servers for creating a new cluster (Set only if you are using PRIMEFLEX configuration ADVN or a link with Active Directory using AD server in your environment) 20. Disable and stop the ESXi shell 21. Disable and stop the SSH service
5	iRMC Settings	1. Create local users (pflocaladmin) 2. Change the admin user password 3. Set Active Directory authentication settings for iRMC of the servers for creating a new cluster (Set only if you are using PRIMEFLEX configuration ADVN or a link with Active Directory using AD server in your environment) 4. Reset iRMC for the servers for creating a new cluster
6	Add servers to the cluster	1. Register the servers for creating a new cluster to the virtual distributed switch for management 2. Register the servers for creating a new cluster to the virtual distributed switch for workload 3. Execute the settings for the virtual distributed switch 4. Set up the capacity device of SSD (When using an All Flash environment) 5. Add disk groups 6. Add the servers for creating a new cluster to the cluster
7	ISM settings	1. Change the password of the admin user of iRMC registered in ISM 2. Change the web interface URL of iRMC registered in ISM 3. Set the collection targets and collection date and time for ISM Log Management
8	Cluster Creation	1. Create a cluster
9	Virtual Network creation	1. Create a virtual distributed switch (virtual distributed switch for workload/virtual distributed switch for management) 2. Enable NIOC 3. Create and set port groups 4. Set NIOC of a virtual distributed switch (virtual distributed switch for workload/virtual distributed switch for management)
10	Storage pool creation	1. Enable vSAN 2. Set deduplication and compression
11	Refresh Virtual Resource	1. Refresh cluster information

2.13.2.2 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 a 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.

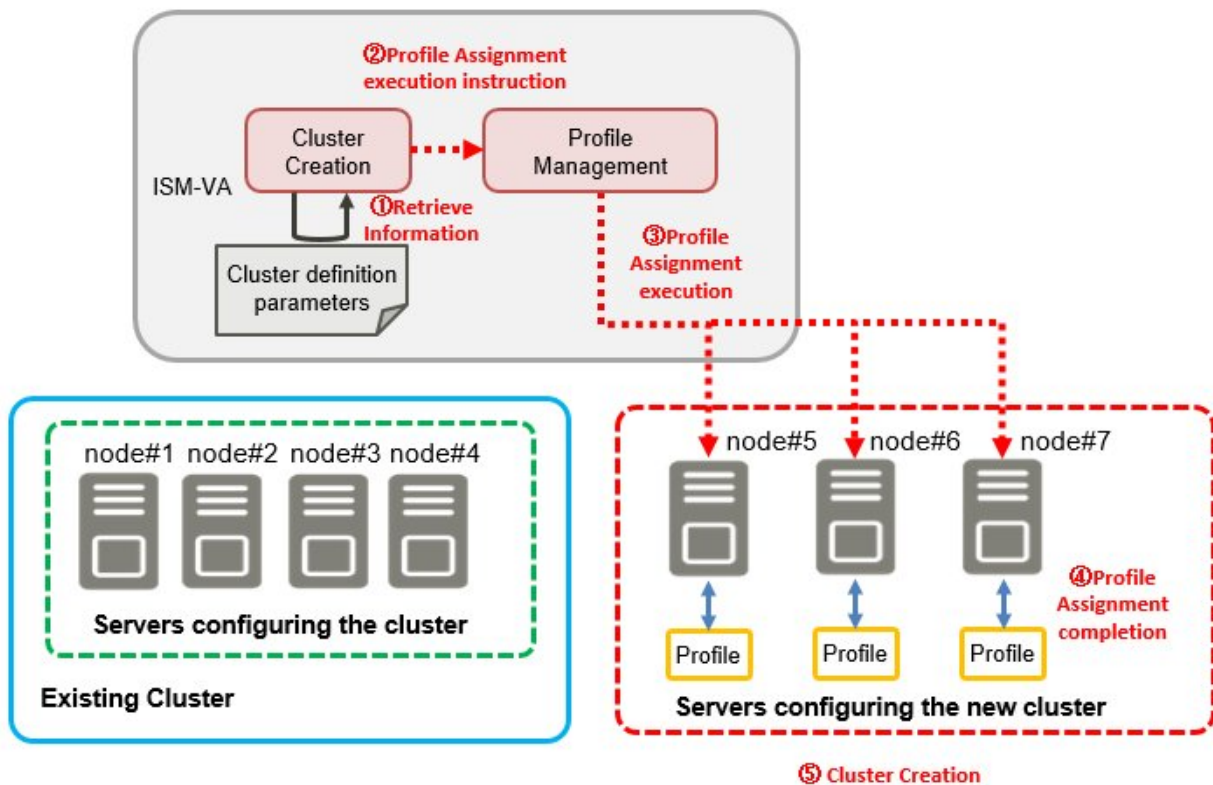
After profile assignment has been completed, the OS settings script is executed by "Executing Script after Installation," which is one of the functions of Profile Management. Afterward, for the target cluster, execute the process for registering the servers for creating a new cluster.

Point

The OS settings 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 process.

A relationship diagram of Cluster Creation and Profile Management is shown below.

Figure 2.38 Relations of Cluster Creation and Profile Management



2.13.2.3 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 "6.9 Export/Import/Delete Cluster Definition Parameters" in "Operating Procedures."

For details of the Cluster Definition Parameters, refer to "ISM for PRIMEFLEX Parameter List."

2.13.2.4 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.

If you select [Tasks] from the top of the Global Navigation Menu on the ISM GUI, the task list will be displayed on the "Tasks" screen. The task name of Cluster Creation is "Cluster Creation." If you select a [Task ID] in the task list whose task type is "Cluster Creation," the task information and subtask list are displayed on the "Tasks" screen. The subtask lists are displayed for each server configuring a new cluster.

Each processing name in the message column of the subtask list is displayed in the following format and the task details are shown below.

`<Processing name>:<Setting item name>`

Table 2.24 PRIMEFLEX for VMware vSAN subtask processing list

Processing name	Task details
PrepCheck Represent TaskItemSet	Register the process in PrepCheck.
Prep Check	Check the execution requirements for creating a new cluster.
OS Installation	Install the OS, apply patches, and run scripts on the servers for creating a new cluster.
DNS Settings	Register the DNS host record on the servers for creating a new cluster.
iRMC Settings	Execute the iRMC settings and the ISM settings for the servers for creating a new cluster.
OS Settings	Execute the OS settings for the servers for creating a new cluster.
Cluster Settings	Execute the cluster settings (first-half settings) for the servers for creating a new cluster.
Ism Settings	Execute the ISM settings for the servers for creating a new cluster.
Cluster Creation	Create a new cluster.
Virtual Network Creation	Create a virtual network for 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 servers for creating a new cluster.

Refer to "[Table 2.23 PRIMEFLEX for VMware vSAN automatic setting item list](#)" for the task details.

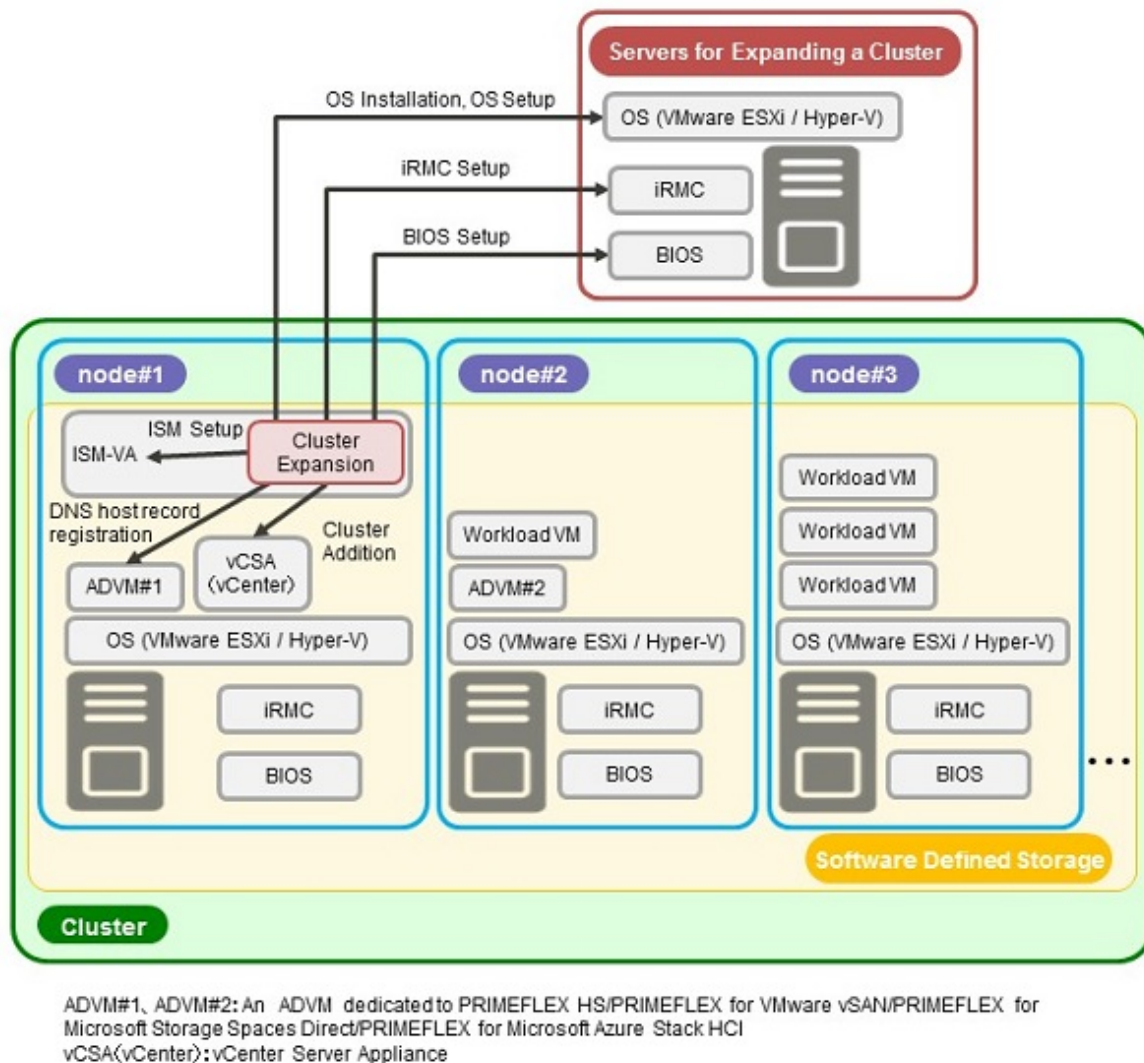
2.13.3 Cluster Expansion

Cluster Expansion is a function that increases resources by adding new servers to the virtualized platforms of PRIMEFLEX HS/ PRIMEFLEX for VMware vSAN when the storage resources of VMware is being depleted. This function links with Profile Management in ISM and reduces the workload of the user by automating the operations from installing an OS on the target server to adding the server to the cluster.

Cluster Expansion is a function that is mainly used for the following purposes:

- Installing and setting an OS on the server for expanding a cluster
- Adding the servers for expanding a cluster to the existing cluster

Figure 2.39 Overview of Cluster Expansion operation



2.13.3.1 Automatic setting item

By using Cluster Expansion, the following items are set automatically.

Table 2.25 PRIMEFLEX HS/PRIMEFLEX for VMware vSAN automatic setting items list

Automatic setting order	Automatic setting item	Description
1	Profile Assignment	<ol style="list-style-type: none"> 1. Set BIOS settings for the servers for expanding a cluster 2. Set iRMC settings for the servers for expanding a cluster 3. Install an OS for the servers for expanding a cluster
2	ESXi patch application	<ol style="list-style-type: none"> 1. Transfer VMware ESXi patch files and scripts to run before and after VMware ESXi patch application 2. Run a script to execute before the VMware ESXi patch application 3. OS Reboot 4. Apply VMware ESXi patches 5. Run a script to execute at the VMware ESXi patch application 6. OS Reboot

Automatic setting order	Automatic setting item	Description
		<ul style="list-style-type: none"> 7. Delete VMware ESXi patch files 8. Retransfer scripts to run before and after VMware ESXi patch application 9. Run a script to execute after the VMware ESXi patch application 10. OS Reboot 11. Remove scripts to run before and after VMware ESXi patch application
3	DNS host record registration	<ul style="list-style-type: none"> 1. Register DNS for the ESXi servers for expanding a cluster (Do not register if the configuration does not use ADVN of PRIMEFLEX configuration)
4	OS settings	<ul style="list-style-type: none"> 1. Enable and start the ESXi shell 2. Enable and start the SSH service 3. Apply the VMware SMIS Provider (only set for PRIMERGY M4 series and VMware ESXi 6.5) 4. Enable the ixgben driver (only set for PRIMERGY M4 series, VMware ESXi 6.5 and VMware ESXi 6.5 Update 1) 5. Add local administrator users 6. Set a host name to FQDN 7. Enable SSL v3 (only set for PRIMERGY M2 series / PRIMERGY M4 series / PRIMERGY M5 series) 8. Disable IPv6 9. Set an IP address for secondary DNS servers 10. Set a DNS suffix 11. Set an IP address for the NTP server 12. Set a firewall for the NTP client 13. Execute the NTP client service 14. Set the power management settings of the host to high performance 15. Restart OS 16. Add an adapter to the virtual distributed switch (virtual distributed switch for workload/virtual distributed switch for management) 17. Set an NIC to the virtual distributed switch (virtual distributed switch for workload/virtual distributed switch for management) 18. Set an NIC to the Management Network 19. Set Active Directory authentication settings for ESXi of the servers for expanding a cluster (Set only if you are using PRIMEFLEX configuration ADVN or a link with Active Directory using AD server in your environment) 20. Disable and stop the ESXi shell 21. Disable and stop the SSH service
5	iRMC Settings	<ul style="list-style-type: none"> 1. Create local users (pflocaladmin) 2. Change the admin user password

Automatic setting order	Automatic setting item	Description
		3. Set Active Directory authentication settings for iRMC of the servers for expanding a cluster (Set only if you are using PRIMEFLEX configuration ADVDM or a link with Active Directory using AD server in your environment) 4. Reset the iRMC settings of the servers for expanding a cluster
6	Add servers to the cluster	1. Register the servers for expanding a cluster to the virtual distributed switch for management 2. Register the servers for expanding a cluster to the virtual distributed switch for workload 3. Execute the settings for the virtual distributed switch 4. Set up the capacity device of SSD (when using an All Flash environment) 5. Add disk groups 6. Add the servers for expanding a cluster to the cluster
7	ISM settings	1. Change the password of the admin user of iRMC registered in ISM 2. Change the web interface URL of iRMC registered in ISM 3. Set the collection targets and collection date and time for ISM Log Management

2.13.3.2 Link with Profile Management

Cluster Expansion links with Profile Management and automates the expansion process.

By selecting a 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 settings script is executed by the "Executing Script after Installation," which is one of the functions of Profile Management. Afterward, for the target cluster, execute the process for registering the servers for expanding the cluster for the target cluster.

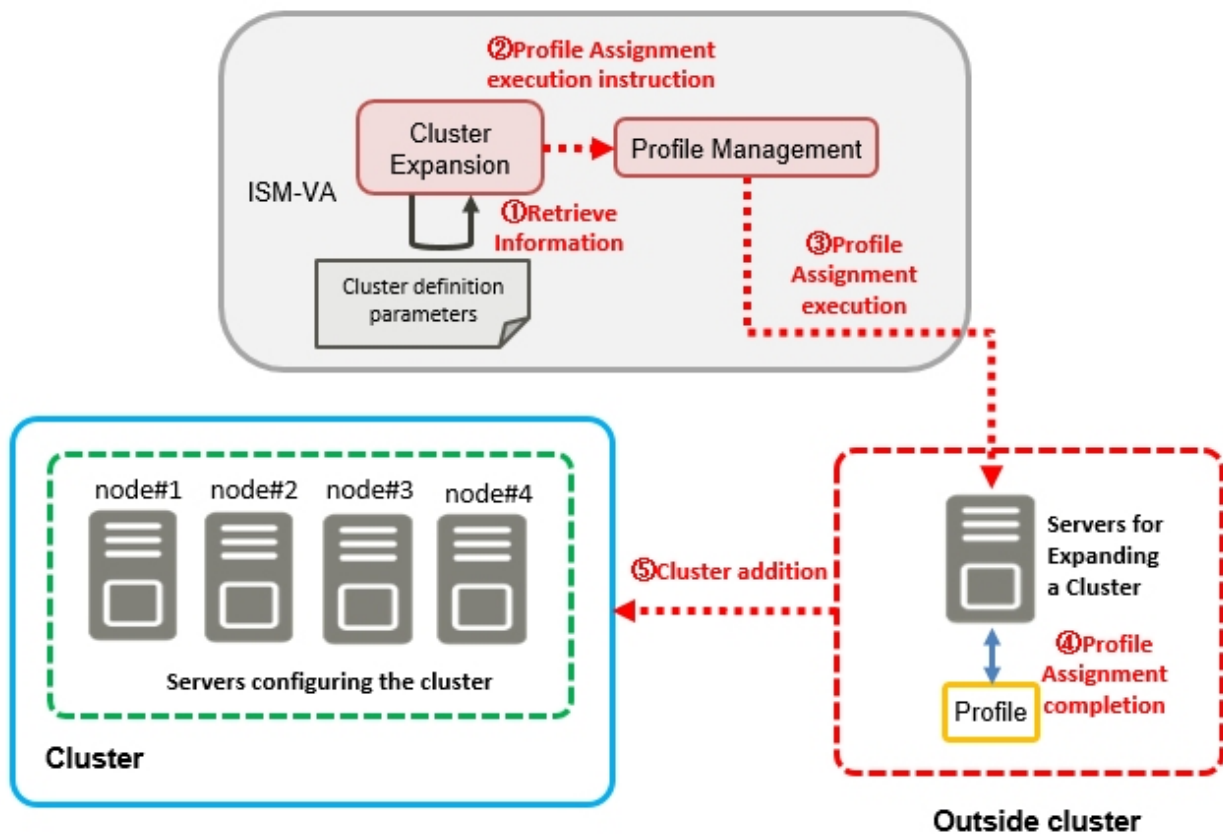


Point

The OS settings 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 process.

A relationship diagram of Cluster Expansion and Profile Management is shown below.

Figure 2.40 Relationship between Cluster Expansion and Profile Management



2.13.3.3 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 can be retained. 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 "6.9 Export/Import/Delete Cluster Definition Parameters" in "Operating Procedures."

For details of the Cluster Definition Parameters, refer to "ISM for PRIMEFLEX Parameter List."

2.13.3.4 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.

If you select [Tasks] from the top of the Global Navigation Menu on the ISM GUI, the task list will be displayed on the "Tasks" screen. The task name of Cluster Expansion is "Cluster Expansion." If you select a [Task ID] in the task list whose task type is "Cluster Expansion," the task information and subtask list are displayed on the "Tasks" screen. The subtask lists are displayed for each server expanding a cluster.

Each processing name in the message column of the subtask list is displayed in the following format and the task details are shown below.

<Processing name>:<Setting item name>

Table 2.26 PRIMEFLEX HS/PRIMEFLEX for VMware vSAN subtask processing list

Processing name	Task details
PrepCheck Represent TaskItemSet	Register the process in PrepCheck.
Prep Check	Check the execution requirements for expanding a cluster.
OS Installation	Install the OS, apply patches, and run scripts on the servers for expanding a cluster.

Processing name	Task details
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 2.25 PRIMEFLEX HS/PRIMEFLEX for VMware vSAN automatic setting items list" for task details.

2.13.4 Rolling Update

Rolling Update is a function that executes the following updates for the clusters structuring the virtualized platform without stopping operations.

Note: Y = Supported, N = Not supported

Processes executed by Rolling Update	PRIMEFLEX HS PRIMEFLEX for VMware vSAN
Firmware updates	Y
Application of ESXi patches	Y
Application of ESXi offline bundle	Y
Application of vCSA patches	Y
vCSA upgrade	Y

This function reduces the workload of the customer by executing the above updates for all servers configuring a cluster automatically. Firmware updates can be automatically executed by linking with Firmware Management of ISM.

The following is the firmware data supported by Rolling Update.

Type	Update method
iRMC firmware (server)	Offline Update
BIOS firmware (server)	Offline Update
LAN/CNA/SAS card firmware (server) [Note]	Offline Update

[Note]: LAN/CNA/SAS cards that are supported on PRIMEFLEX HS/PRIMEFLEX for VMware vSAN is applicable.

For information on the devices (components) that can be used with LAN/CNA/SAS cards, refer to "Support Matrix."

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

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

Select [DOWNLOADS] and select the target operating system.

The reference procedures are subject to change without notice.

The following types are applicable to ESXi with Rolling Update.

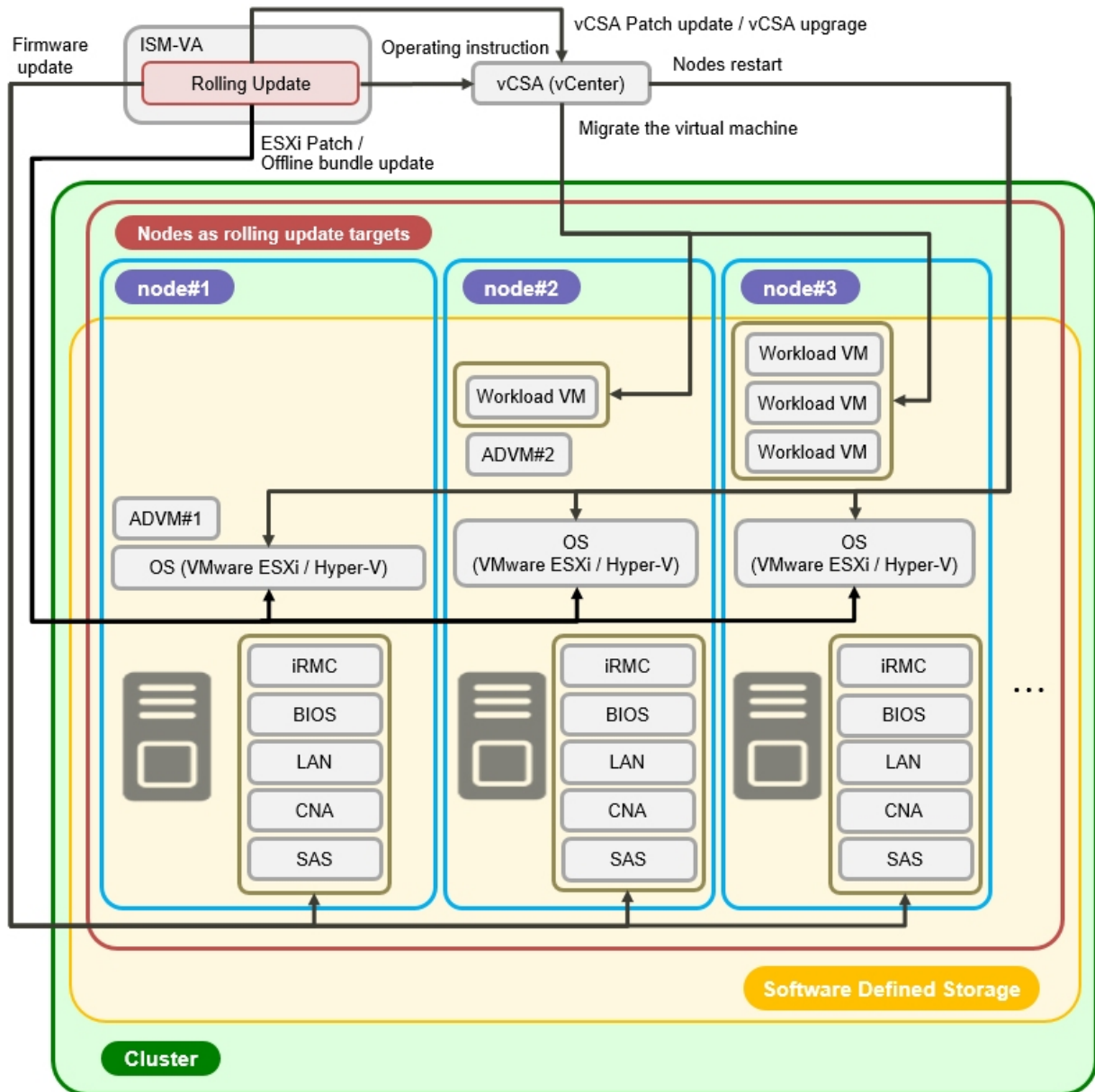
- Patches
- Offline bundle

The following types are applicable to vCSA with Rolling Update.

- Patches

- Upgrade

Figure 2.41 Overview of Rolling Update operation



ADVM#1, ADVM#2: An ADVM dedicated to PRIMEFLEX HS/PRIMEFLEX for VMware vSAN/PRIMEFLEX for Microsoft Storage Spaces Direct/PRIMEFLEX for Microsoft Azure Stack HCI
vCSA(vCenter) : vCenter Server Appliance

2.13.4.1 Operation in link with Firmware Management

Rolling Update operates in link with Firmware Management and automates rolling updates for firmware.

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

The following chart shows the relationship between Rolling Update and Firmware Management.

The diagram illustrates the rolling update process for an Existing Cluster using ISM-VA and the Fujitsu Web Site.

Existing Cluster: Consists of four servers (node#1, node#2, node#3, node#4) configuring the cluster.

ISM-VA (Infrastructure Service Manager - Virtual Agent): Contains the Rolling Update function and the Firmware Management function.

Firmware Management Process:

- Rolling Update:** The Rolling Update function initiates the process.
- Retrieve Information:** The Rolling Update function retrieves information from the Operating Option for Rolling Update.
- Firmware update execution instruction:** The Rolling Update function sends an instruction to the Firmware Management function.
- Firmware update execution:** The Firmware Management function sends an instruction to the Repository.
- Rolling Update:** The Rolling Update function sends an instruction to the Repository.

Repository: A database containing Firmware data.

Fujitsu Web Site: Contains Firmware data.

Flow of firmware data:

- Downloading firmware data:** Firmware data is downloaded from the Fujitsu Web Site to the Repository.
- Import operation for firmware data:** Firmware data is imported from the Repository to the Existing Cluster.

Legend:

- Solid red arrow: Flow of firmware data
- Dotted red arrow: Operation on ISM

Rolling Update is executed from the "Rolling Update" wizard. The processing of the Rolling Update is registered as an ISM task. Confirm the current status of the task on the "Tasks" screen.

Each processing name displayed in the message column of the subtask list in the following format and task details are shown below.

Process name	Setting item name	Setting item details
Rolling Update Prep Check (Confirm preparations for executing Rolling Update)	1. Prep Check	1. Check the conditions for executing Rolling Update
Rolling Update Presetting (Execute the presetting for Rolling Update, vCSA patch application, and vCSA upgrade)	1. Enable Ssh and ESXi shell 2. File transfer to OS 3. Check Dry Run 4. Update vCSA Patch	1. Enable the SSH service and ESXi shell [Note 2] 2. Transfer the following files to the target node [Note 2] <ul style="list-style-type: none"> - ESXi patch file - ESXi offline bundle

Process name	Setting item name	Setting item details
	5. Upgrade vCSA	<ul style="list-style-type: none"> - Scripts to run before and after applying the above files <ol style="list-style-type: none"> 3. Check the ESXi patch or ESXi offline bundle application [Note 2] 4. Apply the vCSA patch [Note 2] 5. Apply the vCSA upgrade [Note 2]
Rolling Update (Execute firmware updates, ESXi patch/ESXi offline bundle application, and restart on the update target nodes)	<ol style="list-style-type: none"> 1. Migrate VM to Another Node & Set Maintenance Mode 2. Migrate VM to Another Node & Set Maintenance Mode 3. Script Execution (Prep) 4. Reboot Node 5. Update ESXi Patch 6. Script Execution (Post1) 7. Shutdown Node 8. Update Firmware (offline) 9. Boot Node 10. File retransfer to OS 11. Script Execution (Post2) 12. Delete File 13. Disable Ssh and ESXishell 14. Reboot Node 15. Unset Maintenance Mode & Migrate VM to Target Node 16. Unset Maintenance Mode & Migrate VM to Target Node 17. Post Check 	<ol style="list-style-type: none"> 1. Migrate the VM that is running on the target node to a temporary node [Note 1] 2. Set the node to Maintenance Mode 3. Execute a script before applying an ESXi patch or ESXi offline bundle [Note 2] 4. Reboot the node [Note 2] 5. Apply the ESXi patch or ESXi offline bundle [Note 2] 6. Execute a script when applying an ESXi patch or ESXi offline bundle [Note 2] 7. Shutdown the node 8. Apply the firmware data Offline 9. Start the node 10. Retransfer the following files to the target node [Note 2] <ul style="list-style-type: none"> - ESXi patch file - ESXi offline bundle - Scripts to run before and after applying the above files 11. Execute a script after applying an ESXi patch or ESXi offline bundle [Note 2] 12. Delete the following files from the target node [Note 2] <ul style="list-style-type: none"> - ESXi patch file - ESXi offline bundle - Scripts to run before and after applying the above files 13. Disable SSH service and ESXi shell settings. [Note 2] 14. Reboot the node [Note 2] 15. Release the Maintenance Mode of the node 16. Return the VM that has been migrated to a temporary node to the target node [Note 1] 17. Check the post-requirements of Rolling Update
Refresh Resource Information (Retrieves cloud management software)	<ol style="list-style-type: none"> 1. Refresh Resource Information 2. Refresh Virtual Inventory 	<ol style="list-style-type: none"> 1. Retrieve the cloud management software information 2. Retrieve the node information

Process name	Setting item name	Setting item details
information and node information)		

[Note 1]: This is not executed when DRS is enabled in a vSAN cluster.

[Note 2]: This is executed for a vSAN cluster.

2.13.5 Node Disconnection/Reintegration

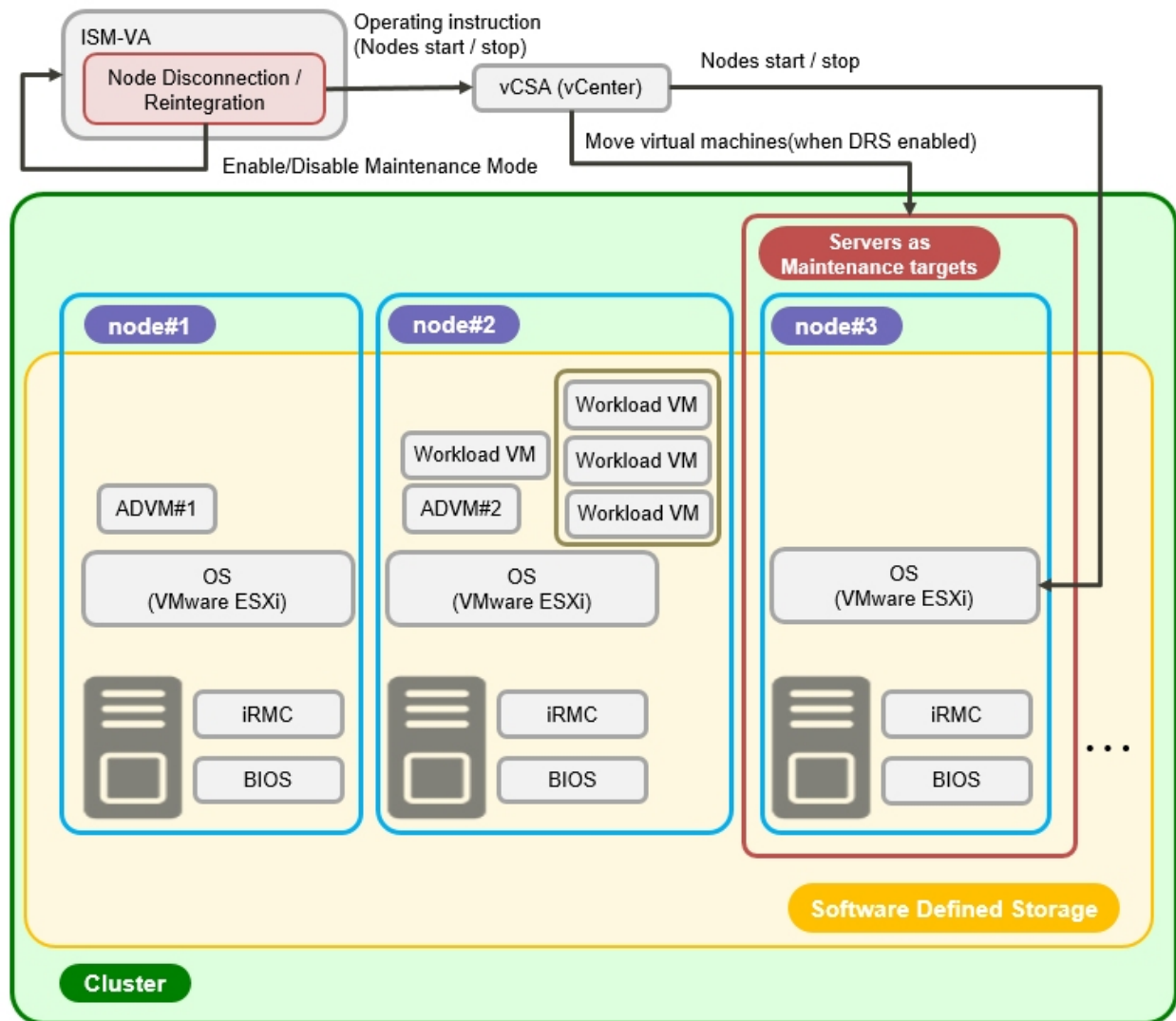
Node Disconnection/Reintegration is a function that disconnects and reintegrates one node at a time without stopping operations even if maintenance requires the servers to be shut down for clusters structuring the virtualized platform of PRIMEFLEX for VMware vSAN.

This function reduces the workload of the user by automating a part of the maintenance tasks that involves restarting servers such as the replacement of an expansion board.

Node Disconnection/Reintegration automates the following series of operations (except for "3. Executing Maintenance").

1. Setting ISM Maintenance mode
2. Stopping maintenance target servers
3. Executing Maintenance (manual operation)
4. Starting maintenance target servers
5. Releasing ISM Maintenance mode

Figure 2.43 Overview of Node Disconnection/Reintegration operation



ADVM#1, ADVM#2: An ADVM dedicated to PRIMEFLEX for VMware vSAN
vCSA (vCenter) : vCenter Server Appliance



Note

In PRIMEFLEX HS, Node Disconnection/Reintegration cannot be used.

2.13.5.1 Task list

Node Disconnection/Reintegration is executed from the GUI for Cluster Management. The process for Node Disconnection/Reintegration is registered as an ISM task. Confirm the current status of the task on the "Tasks" screen.

If you select [Tasks] from the top of the Global Navigation Menu on the ISM GUI, the task list is displayed on the "Tasks" screen. The task name for Node Disconnection/Reintegration is "Node Disconnection" or "Node Reintegration." If you select a [Task ID] in the task list whose task type is "Node Disconnection," or "Node Reintegration," the task information and subtask list are displayed on the "Tasks" screen. The subtask lists are displayed for each cluster to which Node Disconnection/Reintegration is applied.

Each process name displayed in the message column of the subtask list in the following format and the task details are shown below.

```
<Processing name>:<Setting item name>
```

Table 2.28 Node Disconnection subtask process list

Process name	Setting item name	Setting item details
Node Disconnection (Execute the maintenance settings for the node disconnection target server and stop the target server)	<ol style="list-style-type: none"> 1. Target Server VM Existence Check 2. Enabling ISM Maintenance Mode 3. Target Server Turn On LED 4. Enabling Maintenance Mode 5. Stopping Target Server 	<ol style="list-style-type: none"> 1. Make sure there are no VMs on the target server 2. Set the target server to Maintenance Mode 3. Turn on the LED of the target server 4. Set the target server to ESXi Maintenance Mode 5. Stop the target server

Table 2.29 Node Reintegration subtask process list

Process name	Setting item name	Setting item details
Node Reintegration (Start the node reintegration target server and release Maintenance Mode)	<ol style="list-style-type: none"> 1. Starting Target Server 2. Disabling Maintenance Mode 3. Disabling ISM Maintenance Mode 4. Target Server Turn Off LED 5. Reconfigure vSphere HA 	<ol style="list-style-type: none"> 1. Start the target server 2. Release ESXi Maintenance Mode for the target server 3. Release ISM Maintenance Mode for the target server 4. Turn off the LED of the target server 5. Reconfigure vSphere HA for the target server

2.13.6 Backup

Backup is a function that backs up ESXi servers and vCSA for the clusters structuring the virtualized platform of PRIMEFLEX for VMware vSAN.

This function reduces the workload of the user by automating the operations for backing up ESXi servers and vCSA for system recovery from failures.

Backup automates the following operations.

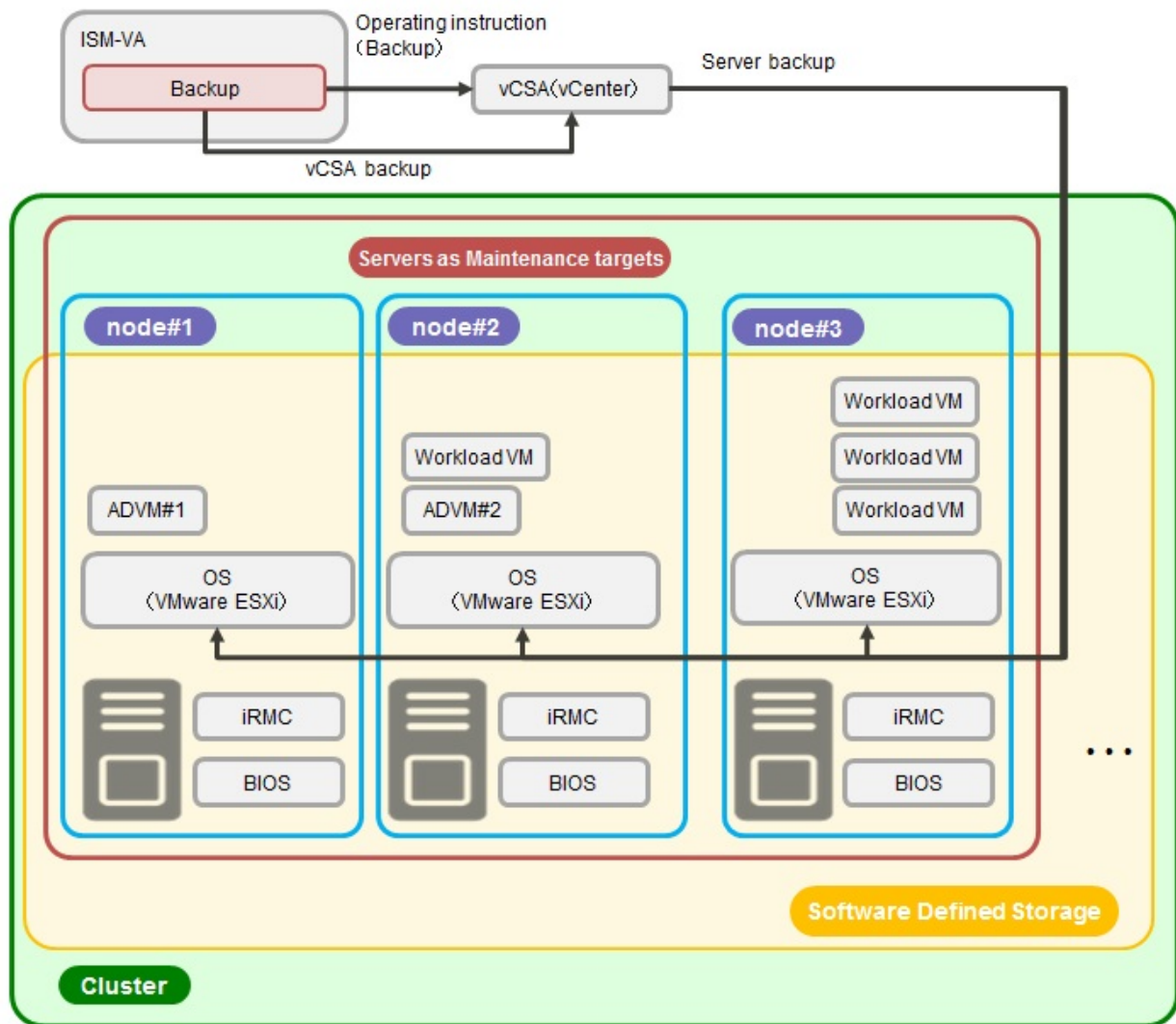
1. Mount of the backup destination
2. Enabling of the SSH service for the target server
3. Backup of the target server
4. Disabling of the SSH service for the target server
5. Backup of the target vCSA
6. Unmount of the backup destination

The following targets can be backed up with Backup.

Note: Y = Supported, N = Not supported

Target	Support
Nodes configuring the cluster	Y
vCSA configuring the cluster	Y

Figure 2.44 Overview of Backup operation



ADVM#1, ADVM#2: An ADVM dedicated to PRIMEFLEX for VMware vSAN
vCSA(vCenter): vCenter Server Appliance

Note

Backup is not available for PRIMEFLEX HS.

2.13.6.1 Task list

Backup can be executed from the GUI for Cluster Management. The backup process is registered as an ISM task. Check the status of the job on the "Tasks" screen.

If you select [Tasks] from the top of the Global Navigation Menu on the ISM GUI, the Task List is displayed. The task name of Backup is "Backup." If you select a [Task ID] in the task list whose task type is "Backup," the task information and subtask list are displayed on the "Tasks" screen. The subtask lists are displayed for each target cluster.

Each process name in the message column of the subtask list displayed in the following format and the task details are shown below.

```
<Process name>: <Setting item name>
```

Table 2.30 Backup subtask process list

Process name	Setting item name	Setting item details
Backup (Back up the backup target server and vCSA)	<ol style="list-style-type: none"> 1. Mount Backup Destination 2. Check Backup Destination 3. Backup Server 4. Backup vCSA 5. Unmount Backup Destination 	<ol style="list-style-type: none"> 1. Mount the backup destination 2. Check the availability of the disk space in the backup destination 3. Back up the server [Note] 4. Back up the vCSA 5. Unmount the backup destination

[Note]: In a server backup, enable the SSH service before the backup, and after the backup, disable the SSH service for the backup target server.

2.13.7 Restore

Restore is a function that restores vCSA for the clusters structuring the virtualized platform of PRIMEFLEX for VMware vSAN.

This function reduces the workload of the user by automating the operations for restoring vCSA for system recovery from failures.

Restore automates the following operations.

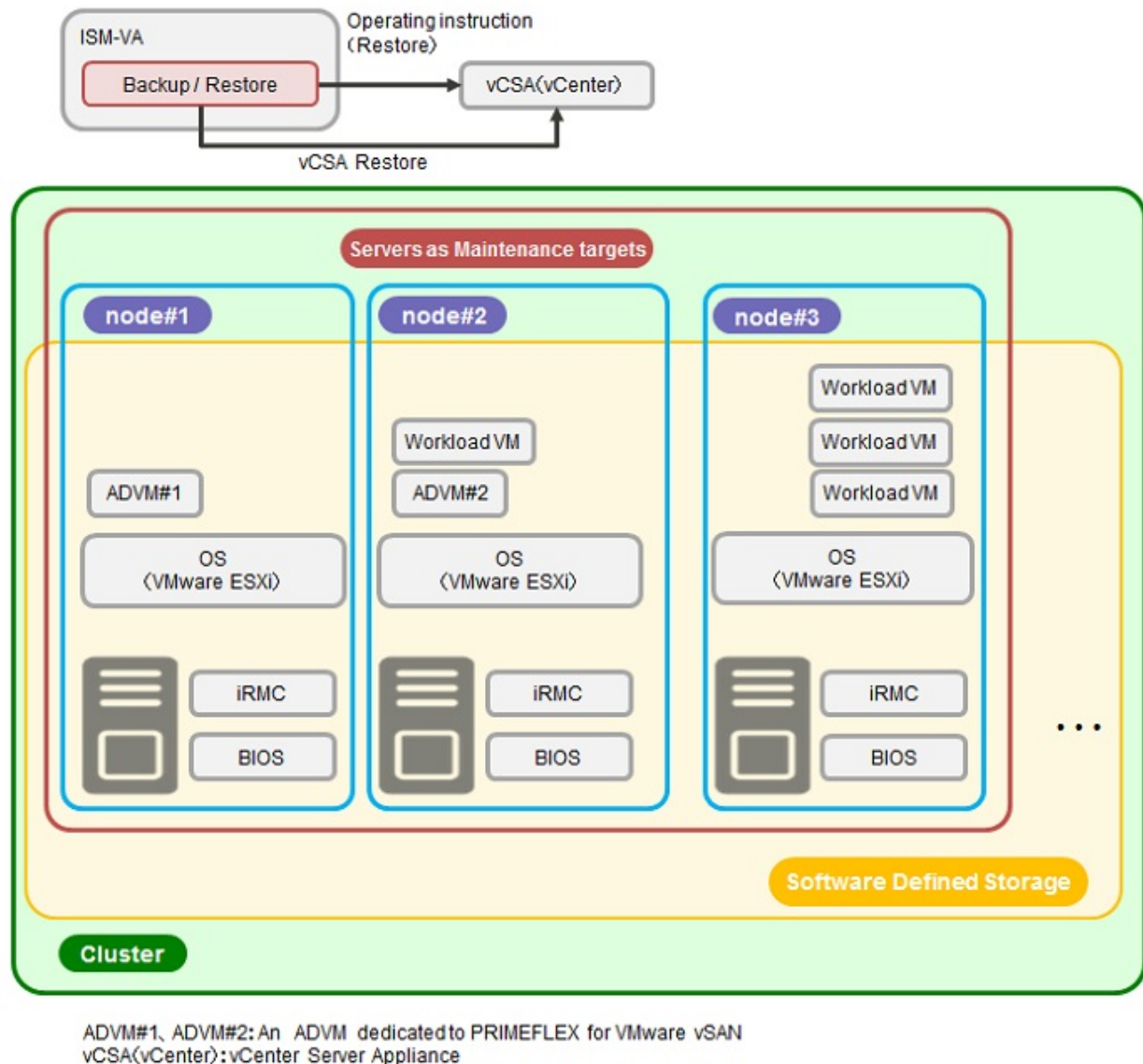
1. Mount of the restore destination
2. Enabling of the SSH service for the server restoring vCSA
3. Restoration of the target vCSA
4. Disabling of the SSH service for the server restoring vCSA
5. Restoration of vDS of the target vCSA
6. Unmount of the restore destination

The following targets can be restored with Restore.

Note: Y = Supported, N = Not supported

Target	Support
Nodes configuring the cluster	N
vCSA configuring the cluster	Y

Figure 2.45 Overview of Restore operation



Note

- Restore is not available for PRIMEFLEX HS.
- Restore cannot be used for ESXi.

2.13.7.1 Task list

Restore can be executed from the GUI for Cluster Management. The restore process is registered as an ISM task. Check the status of the job on the "Tasks" screen.

If you select [Tasks] from the top of the Global Navigation Menu on the ISM GUI, the Task List is displayed. The task name of Restore is "Restore." If you select a [Task ID] in the task list whose task type is "Restore," the task information and subtask list are displayed on the "Tasks" screen. The subtask lists are displayed for each target cluster.

Each process name in the message column of the subtask list displayed in the following format and the task details are shown below.

```
<Process name>: <Setting item name>
```

Table 2.31 Restore subtask process list

Process name	Setting item name	Setting item details
Restore (Restore vCSA)	<ol style="list-style-type: none"> 1. Mount Restore Destination 2. Check Restore Destination 3. Restore vCSA 4. Restore vDS 5. Unmount Restore Destination 	<ol style="list-style-type: none"> 1. Mount the restore destination 2. Check the availability of the disk space in the restore destination 3. Restore vCSA [Note] 4. Restore vDS 5. Unmount the restore destination

[Note]: In a vCSA restoration, enable the SSH service before the restoration, and after the restoration, disable the SSH service for the server in which vCSA is restored.

2.13.8 Cluster Stop

Cluster Stop is a function that stops the clusters structuring the virtualized platform of PRIMEFLEX for VMware vSAN.

Cluster Stop stops all of the nodes in a cluster and turns off the power.

Execute a Cluster Start command to start a cluster that has been stopped with Cluster Stop.

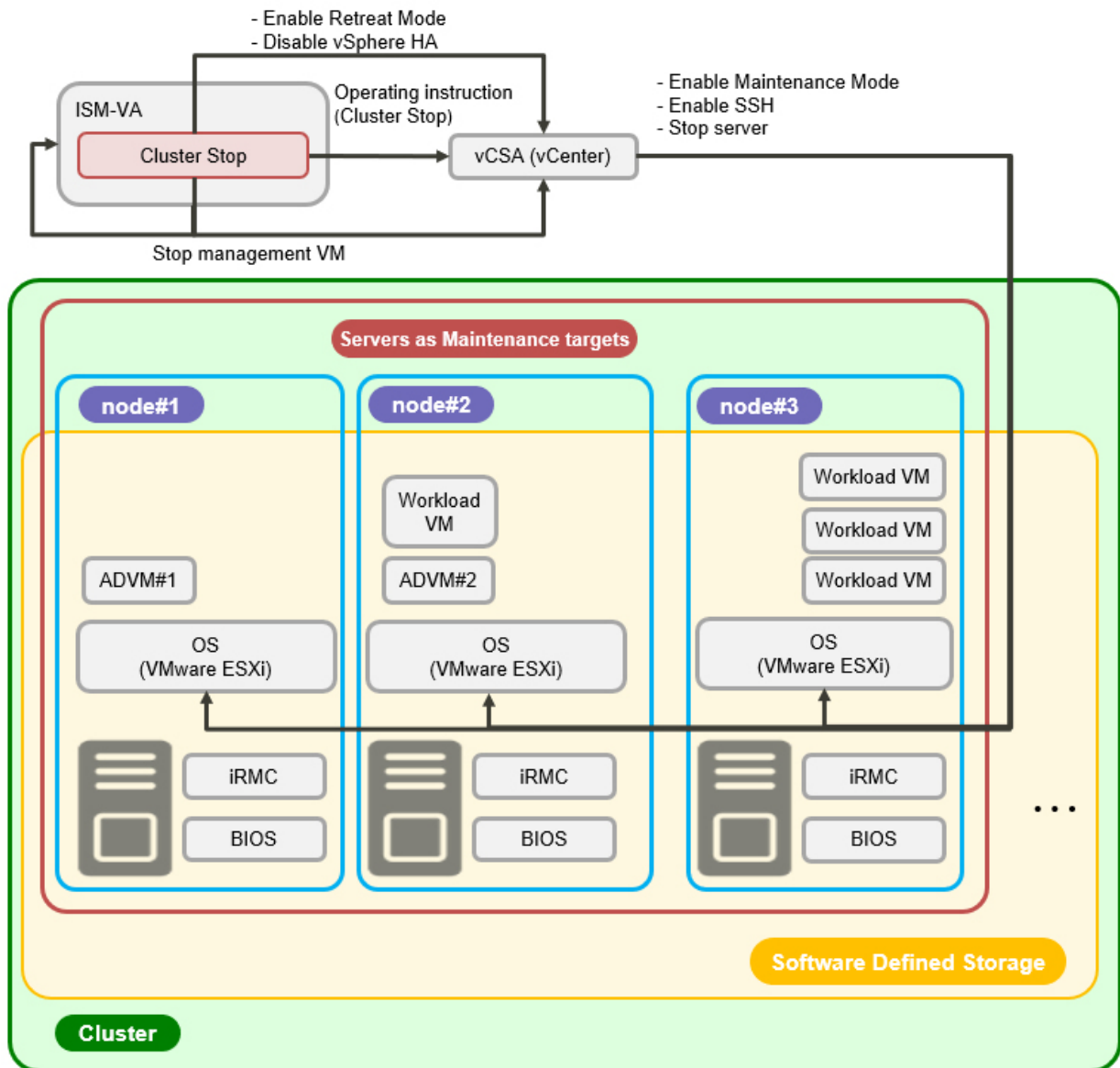
You cannot manually start a cluster as usual if you changed the Cluster Stop settings.

For the Cluster Start command, contact your local Fujitsu customer service partner.

Cluster Stop automates the following operations.

1. Setting Retreat Mode of the target cluster (For vSphere 7.0 Update 1 or later)
2. Disabling of vSphere HA of the target cluster
3. Setting ISM Maintenance Mode for all nodes in the target cluster
4. Enabling of the SSH service for all nodes in the target cluster
5. Deploying ESXi stop/start programs for all nodes in the target cluster
6. Confirming components that are resynchronizing for vSAN storage for the target cluster
7. Shutting down ISM-VA in the target cluster
8. Shutting down vCSA in the target cluster
9. Setting Maintenance Mode for ESXi for all nodes in the target cluster
10. Shutting down all nodes in the target cluster

Figure 2.46 Overview of Cluster Stop operation

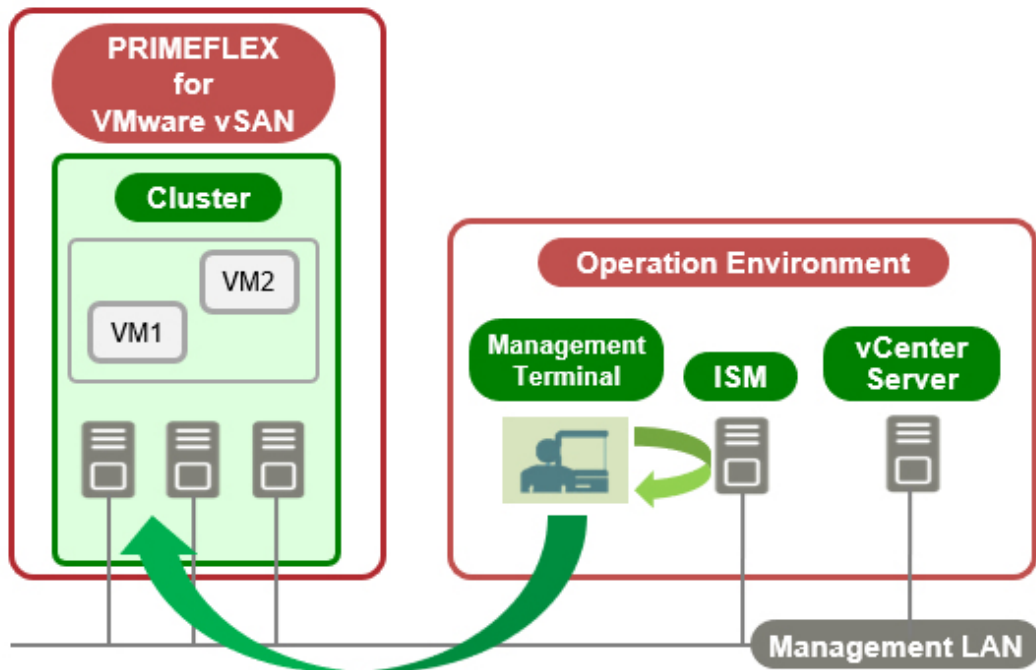


ADVM#1, ADVM#2: An ADVM dedicated to PRIMEFLEX for VMware vSAN
vCSA(vCenter): vCenter Server Appliance

Operation description

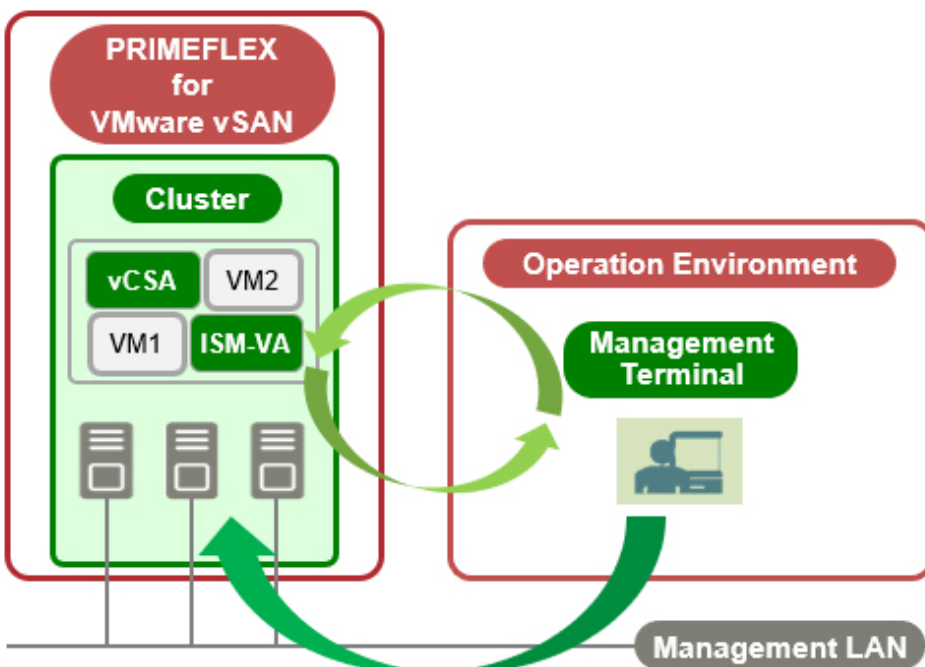
Cluster Stop operates as shown in "Figure 2.47 Operation of Cluster Stop."

Figure 2.47 Operation of Cluster Stop



This function also supports configurations where ISM-VA and vCSA are deployed in the same cluster (["Figure 2.48 Operation in configurations where ISM-VA and vCSA are deployed in the cluster"](#)). This configuration corresponds to the special case mentioned above (["Figure 2.47 Operation of Cluster Stop"](#)).

Figure 2.48 Operation in configurations where ISM-VA and vCSA are deployed in the cluster



You can stop clusters where ISM-VA and vCSA are deployed with Cluster Stop only when it is PRIMEFLEX and the last cluster running. ISM-VA and vCSA are stopped automatically by a process that stops the cluster.

2.13.8.1 Task list

Cluster Stop can be executed from the GUI for Cluster Management. The cluster stop process is registered as an ISM task. Check the status of the job on the "Tasks" screen.

If you select [Tasks] from the top of the Global Navigation Menu on the ISM GUI, the Task List is displayed. The task name of Cluster Stop is "Cluster Stop." If you select a [Task ID] in the task list whose task type is "Cluster Stop," the task information and subtask list are displayed on the "Tasks" screen. The subtask lists are displayed for each cluster that is to be stopped.

Each process name in the message column of the subtask list displayed in the following format and the task details are shown below.

<Process name>: <Setting item name>

Table 2.32 Cluster Stop subtask process list

Process name	Setting item name	Setting item details
Cluster Stop (Execute Cluster Stop preprocessing and stop servers in the target cluster)	1. Check Condition For Stopping Cluster 2. Enable Retreat Mode 3. Preset For Stopping Cluster 4. Disable vSphere HA 5. Enable ISM Maintenance Mode 6. Stop Cluster	1. Precheck for Cluster Stop 2. Set Retreat Mode for the target cluster (For vSphere 7.0 Update 1 or later) 3. Execute the stop preprocess to stop the server in the target cluster [Note] 4. Disable vSphere HA in the target cluster 5. Set the server in the target cluster to ISM Maintenance Mode 6. Stop the target cluster

[Note]: The SSH service is enabled and cluster information is collected in preprocessing.

2.13.9 Batch Collection of vSAN Logs for a VMware vSAN Cluster

If a resource (nodes, cloud management software, hypervisors) that is part of a vSAN cluster fails, retrieve the cluster logs for PRIMEFLEX for VMware vSAN in order to investigate the problem. Using this function can reduce the operation procedure of log collection.

Logs to collect

Collect the following logs for the cluster.

Collection Log	Content
Hardware Log	Hardware logs for the nodes configuring the cluster
Operating system Log	Operating system logs for the nodes configuring the cluster
vm-support	Support logs from ESXi on the nodes configuring the cluster [Note]
vc-support	Support logs retrieved from vCenter [Note]
RVC (VMware Ruby vSphere Console Command) command	Results from running the RVC command "vsan.support_information" on the vCenter Server Appliance

[Note]: For details, refer to the VMware website:

<https://kb.vmware.com/s/article/2032892>



Note

- If ISM operation mode is not in Advanced for PRIMEFLEX, "system License type error." will be displayed during Batch Collection of vSAN Logs. Check the ISM operation mode.

- If the ISM services are not running, "ISM Service is not running." will be output during Batch Collection of vSAN Logs. Execute this after starting the ISM service. Refer to "4.1.4 Start and Stop of ISM Service" for details on starting the ISM service.
- You can perform the log collection even if the cluster is not a VMware vSAN cluster. However, the vm-support, vc-support, and RVC command logs cannot be retrieved (The collection status of the vc-support and RVC commands is Error).
- Logs are not collected for servers that are not running or in Maintenance Mode.
- If the vCenter Server Appliance is not SSH accessible, RVC commands are not collected.

2.13.9.1 Operation of Batch Collection of vSAN Logs

From the console, log in to ISM-VA as administrator group user and execute the following commands.

Specify a combination of the commands in ISM-VA Management and operation options.

Table 2.33 Command for Batch Collection of vSAN Logs

Function	Command
Batch Collection of vSAN Logs	ismadm cluster logcollect <operation option>

Table 2.34 Operation option for Batch Collection of vSAN Logs

Operation name	Operation option	Content
Checking cluster name	-listcluster	Lists the cluster names
Start collection	-collect	Starts Batch Collection of vSAN Logs
Checking collection status	-status	Displays the status of Batch Collection of vSAN Logs

The following describes the operation option.

Checking cluster name (-listcluster)

This command is used to check the cluster name of the cluster that is being logged. Displays a list of clusters registered with ISM (cluster name, cluster type).

For VMware vSAN clusters, the cluster type displays "VMware".

```
# ismadm cluster logcollect -listcluster
```

Example: Results for checking the cluster name (If there were three clusters configured)

```
# ismadm cluster logcollect -listcluster
Cluster List:
TestCluster62vSanTrue      VMware
Cluster-1                  VMware
S2DCluster                 Hyper-V
```

Under "Cluster List:", <Cluster Name> and <Cluster Type> are displayed on separate lines.

Start collection (-collect)

Starts Batch Collection of vSAN Logs.

```
# ismadm cluster logcollect -collect -dir <directory> -file <file name> -port <port number>
```

Parameter	Required	Description	Note
-dir <directory>	Y	Directory to log	Specifies the directory under/Administrator/ftp.
-file <file name>	Y	File name	Log file name to output Example: Cluster62vSanLog.zip

Parameter	Required	Description	Note
			(If the ".zip" extension is not present, the ".zip" is appended to the log file name.)
-port <port number>		Port number	Specifies if the ssh port number in vCenter is set to something other than 22.

Specify the following in the command prompt that is displayed after the command is executed.

Prompt	Required	Description	Note
ClusterName:	Y	Cluster name	Specifies the cluster name to log.
Password:		zip password	Specifies to set a password for the collection log file. If omitted, no password is used.

After "Cluster Name 'Collect Start? (Y/N)" is displayed at the end, enter "Y" if you are satisfied with the input. "Cluster log collection started. Please wait for completion." is output when collection is started.

If you want to correct what you entered, enter "N" and execute the command again.



Note

- Once you start log collection for vSAN, you cannot stop it until it is complete.
- If you are working with a cluster, wait for the cluster operation to complete before starting log collection for vSAN.
- If the specified cluster name does not exist, "The specified cluster name does not exist." is output. Check the cluster name.
- The log collection for vSAN cannot be started on a cluster that is in progress. If so, "Already running on the same cluster." is output.
- If there is not enough free space on the virtual disk of the Administrator user group, "capacity directory error." is output. In this case, expand the free space on the virtual disk. The required free space is about 6 Gbytes in a cluster with a four-node configuration. More space may be required depending on the log size of vm-support and vc-support.
- If the log destination directory specified by "-dir" does not exist, "Target directory does not exist." is output. Specify the directory that exists.
- If the RVC command fails to collect, check that the ssh port on the vCenter Server Appliance matches the port number specified in "-port" (22 if not specified).
- If ISM-VA is restarted or stopped while Batch Collection of vSAN Logs is in progress, the collection operation will be stopped. If a collection status check was performed after ISM-VA was started, the collection status at the time it was stopped is displayed. However, you can start a new collection.



Point

Batch Collection of vSAN Logs can be executed on multiple clusters simultaneously. Execute the start collection command on each cluster. However, the collection time is the sum of the time for each cluster.

Collection time

The estimated collection time is approximately 60 minutes for a four-node cluster.

Batch Collection of vSAN Logs collects logs from each node or cloud management software that is part of the vSAN cluster. Therefore, the collection time varies depending on the cluster configuration and log size. It also takes more time to collect logs on multiple clusters simultaneously.

For the status of the collection, refer to "[Checking collection status \(-status\)](#)."

Checking collection status (-status)

Check the operating status of Batch Collection of vSAN Logs.

```
# ismadm cluster logcollect -status
```

Prompt	Required	Description	Note
ClusterName:		Cluster name	If omitted, the collection state is displayed for all clusters registered with ISM.

Collection status output contents

The output is for each cluster as follows:

Item	Description
ClusterName	Cluster name
Directory	Directory name specified in start collection (-collect)
FileName	File name specified in start collection (-collect)
Status	vSAN log collection status <ul style="list-style-type: none">- Wait: Waiting for collection- Collecting: Collecting- Complete: Collection complete- Error: An error occurred
CollectStartTime	Collection start time (Time zone set for ISM-VA)
CollectEndTime	Collection end time (Time zone set for ISM-VA. Empty character until collection is complete)
Checksum	Hash value for checksum (SHA-256 hash value)
[CmsStatus]	Collection status of vc-support and RVC commands The values displayed (Wait/Collecting/Complete/Error) are the same as those described in "Status".
[NodeStatus]	Log collection status for each node (node count display) The values displayed (Wait/Collecting/Complete/Error) are the same as those described in "Status".

Clusters without Batch Collection of vSAN Logs will be output as "Cluster name 'is not collecting.".

2.13.9.2 Output file

If the collection status check indicates that the vSAN log collection status is "Complete", a log file and an information file of the collection results are created in the directory specified at the start of collection. If "Error", no log file is created.

File	File name	Content
Log file	<specified file name>.zip [Note]	Zipped file of collected logs If a password is specified, it is encrypted with the specified password.
Collection results information file	<specified file name>.Result	File containing textual information about the collection results

[Note]: If ".zip" is appended to the end of the specified file name, ".zip" is not appended a second time.

Contents of collected log files

The log file contains the following files.

File	Content
Storagelog.zip	Hardware logs, operating system logs, vm-support logs

File	Content
Cmslog.zip	vc-support logs, RVC command logs

Contents of the collection results information file

The following items are in the information file of the collection results.

Item	Description
ClusterName	Cluster name
Directory	Directory name specified in start collection (-collect)
FileName	File name specified in start collection (-collect)
Status	vSAN log collection status <ul style="list-style-type: none"> - Complete: Collection complete - Error: End with an error
Checksum	Hash value for checksum (SHA-256 hash value)
CollectStartTime	Collection start time (Time zone set for ISM-VA)
CollectEndTime	Collection end time (Time zone set for ISM-VA)
[CmsStatus]	Result of collecting vc-support and RVC commands <ul style="list-style-type: none"> - Complete: Successful collection - Error: Collection error
[NodeStatus]	Log collection status for each node (node count display) <ul style="list-style-type: none"> - Complete: Successful collection - Error: Collection error

2.13.10 Generation Switching

Generation Switching is a function that updates the management information of generations of the current PRIMEFLEX to the management information of generation of the successor model.

Management information of generation indicates that the following information maintained in ISM.

- Generation of PRIMEFLEX configured with Cluster Creation or Virtualized Platform Structure of PRIMEFLEX (Registered Generation)
- When the node is registered to PRIMEFLEX (Registered Trigger)
- Generation where after Generation Switching of ISM is executed (Switched Generation)

By switching generations, you can replace the server with a successor model while continuing to use the system.

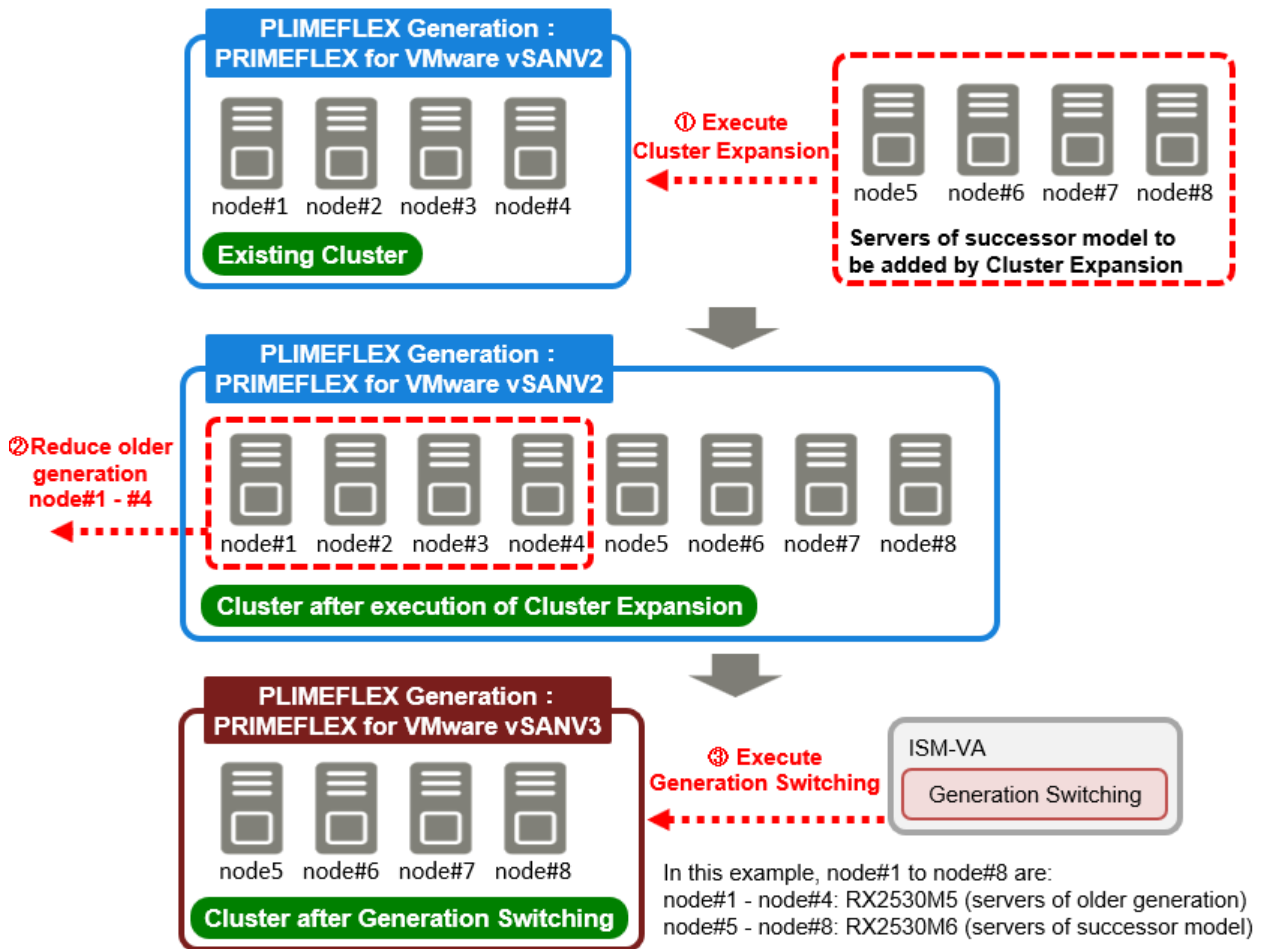
To execute Generation Switching, you must reduce all servers older than the PRIMEFLEX generation that you want to switch to.

If multiple generations of servers are coexisting, the generation is associated with the oldest generation of servers (example: for a coexisting M4/M5 server system without executing Generation Switching, the generation is PRIMEFLEX for VMware vSAN V1.)

A dedicated PRIMEFLEX SupportDesk contract is required for Generation Switching. For more information, refer to "Server Expansion/Generation Switching Guide" of PRIMEFLEX for VMware vSAN.

When you switched the generation of the PRIMEFLEX dedicated SupportDesk without a contract, you can initialize the management information of generation.

Figure 2.49 Overall view of the generation switching function



To update the management information of the generation of PRIMEFLEX with Generation Switching, you must add successor servers to the existing cluster and reduce all older generations.

2.14 Functions of ISM Operating Platform

This section describes the functions configuring the ISM operating platform.

- 2.14.1 User Management
- 2.14.2 Repository Management
- 2.14.3 Installation of Emulex OneCommand Manager CLI and QLogic QConvergeConsole CLI
- 2.14.4 Task Management
- 2.14.5 ISM-VA Management
- 2.14.6 Management of Cloud Management Software
- 2.14.7 Shared Directory Management
- 2.14.8 Link with ISM
- 2.14.9 Linking with Other Software

2.14.1 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," the methods for accessing nodes and execution of the various functions may be restricted.
- By grouping users (hereafter referred to as "user groups"), you can restrict the scope of access to each function separately by user group.
- By grouping nodes (hereafter referred to as "node groups") and associating 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 is displayed in "Figure 2.50 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
- Operations under User Management
- Operating in Link with Microsoft Active Directory or OpenLDAP
- Multi-Factor Authentication

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 associating 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 is to manage all the nodes in ISM.
Group 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 is to manage all the nodes in 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 associated.
	No managed nodes	There are not any nodes or node-related resources (such as logs).

Point

In the subsequent descriptions, consider user groups for which "Manage all nodes" is specified as the managed nodes to be Administrator group.

Note

If "Manage all nodes" is set as the managed nodes, the setting cannot be changed. Also, if "Nodes in the selected node group" or "No managed nodes" is set as the managed nodes, the setting cannot be changed to "Manage all nodes."

Types of user roles and operations executable by users having these roles

The types of operations that can be executed by users on nodes within their access scope are defined by their user roles as follows.

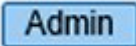
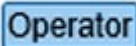
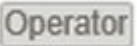








User role	Type of access
Administrator role	Administrators can add, modify, delete, and view nodes, users, and all kinds of settings.

User role	Type of access
Operator role	Operators can modify and view nodes and all kinds of settings. They are not able to manage users.
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 information (icon indications) in the various functions that are provided in this manual. For information on the icon indications, refer to the description below.
- In the subsequent descriptions, users belonging to an Administrator group and having an Administrator role will be referred to as an "ISM administrator."

In order to describe the access rights of users, the user group to which a user belongs and the user role they have within the group are classified and indicated with icons as follows.

User group to which the user belongs	User role held by user	Can execute	Cannot execute
Administrator group	Administrator role		
	Operator role		
	Monitor role		
Other groups (groups other than Administrator group)	Administrator role		
	Operator role		
	Monitor role		

The attributes of users who can execute operations are shown as follows.

Example:



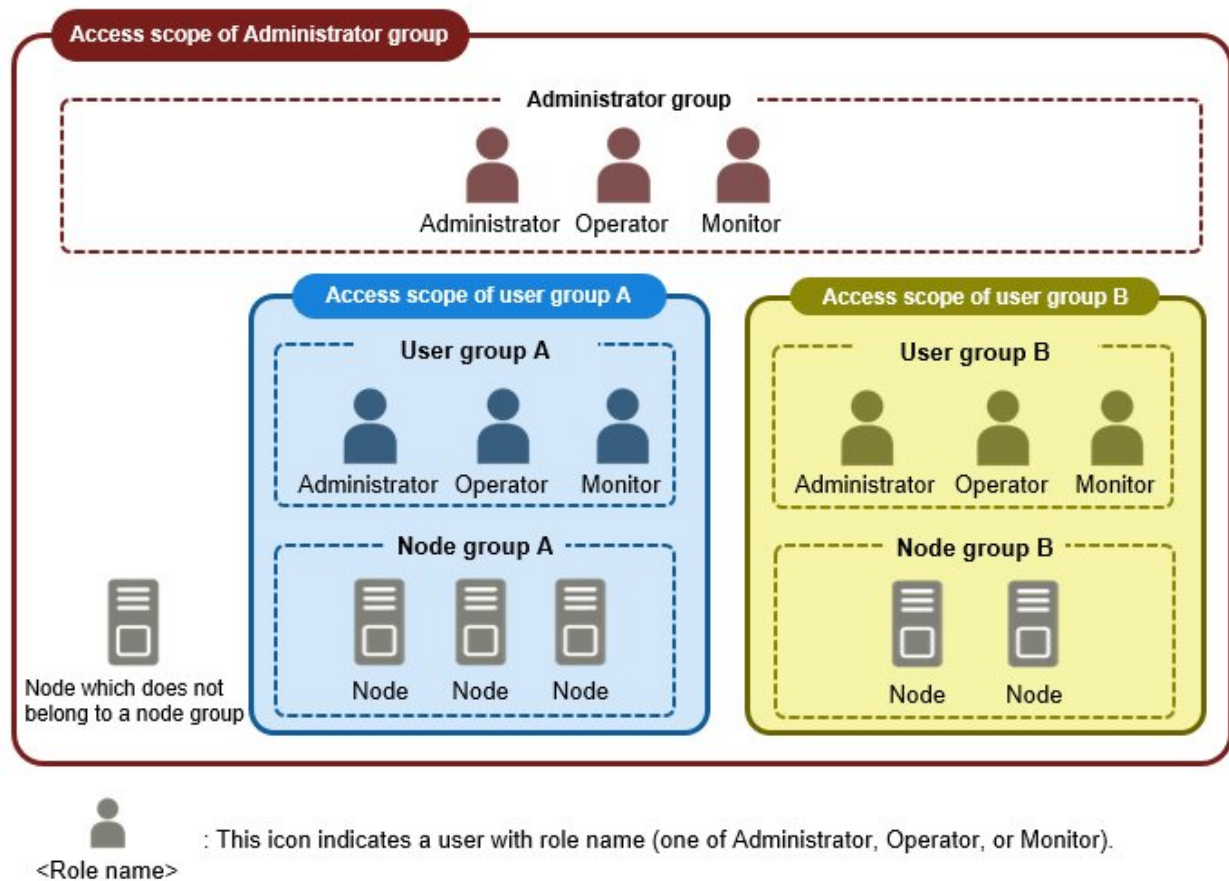
- In the example above, users with the following combinations of groups and roles can execute operations:
 - Users who belong to the Administrator group and have an Administrator role or Operator role
 - Users who belong to a group other than an Administrator group and have an Administrator role or Operator role
- Users with a Monitor role cannot execute the respective functions, as indicated by the gray icons.

Note

Users who belong to an Administrator group and have an Administrator role are special users (ISM administrator) who can perform all the operations.

Users who belong to an Administrator group and have an Operator or Monitor role have a different access scope than users who have the same roles in a non-Administrator group. However, the types of operations they can execute are the same.

Figure 2.50 Relationships between user groups, node groups, and roles



Security policy settings

Executable user

Administrator group

Other groups

Execute the security policy settings with the following procedure.

1. From the Global Navigation Menu on the ISM GUI, select [Settings] - [Users].
2. From the menu on the left side of the screen, select [Security Policy].
3. Select the [Edit] button to set the security policy.

For the security policy, there is the user password policy and the login policy.

You can set passwords handled in User Management and login restrictions.

You can set one security policy for ISM. Setting a firm security policy allows for more secure operation. The setting items are described below.

User Password Policy

Item	Parameter	Operations after settings
Use Past Password	<ul style="list-style-type: none"> - Allowed (recommended) - Past n passwords prohibited (1 ~ n 24) 	These items are checked when a password is set on the "Add User" screen and "Edit User Settings" screen.
Password Length	1 - 80 (byte) (recommended: 8 (bytes))	

Item	Parameter	Operations after settings
Password Character Type	<ul style="list-style-type: none"> - No restrictions (recommended) - Use at least n character classes from among number, lowercase letter, uppercase letter, and special character [Note 2] (2 ≤ n ≤ 4) 	
Same Password as User Name	<ul style="list-style-type: none"> - Allowed - Prohibited (recommended) 	
Prohibited Strings [Note 1]	Up to a maximum of 256 can be specified	
Period of Validity	<ul style="list-style-type: none"> - Indefinitely - 1 - 365 (days) (recommended: 90 (days)) 	<p>If logging in with a setting other than "Indefinitely," operation is as follows:</p> <ul style="list-style-type: none"> - When the expiration date is reached The Action after Expiration is executed. - When the expiration date is within two weeks away Warning messages are output. - Administrator A warning message will be output if the initial password has not been changed.
Action after Expiration	<ul style="list-style-type: none"> - Show warning message - Account lockout indefinitely (recommended) 	

[Note 1]: Set a password that cannot be used. Passwords that match the set character string are forbidden.

[Note 2]: The characters can be used as a special character (!"#\$%&'()*+,-./:;<=>?@[\\]^_`{|}~).



Point

If you select the [Default] button, the recommended values in the table above will be set.



Note

- 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 login restrictions are limited to logging in to ISM. Be careful, since log in to FTP or ISM-VA is not restricted.
 - The first login to ISM succeeds after the password expiry date has passed. Change the password at this time. If the password is not changed, the login will be locked indefinitely.
 - When login has been locked indefinitely, if the password is reset by the ISM administrator, the lock is removed.
 - ISM administrators cannot be locked-out indefinitely. Only warning messages are output.

Login Policy

Item	Parameter	Description
Session Time	2 - 60 (minutes)	The length of time after which the session will time out if there is no activity.

Item	Parameter	Description
	2 - 1440 (minutes) (ISM 3.0.0.010 or later) (Default: 30 minutes)	
Account Lockout Threshold	6 - 256 (times) (Default: 6 times)	Specifies the number of failed operations that lock the account and the length of time that the account is locked. The following are the operations that lock the account. <ul style="list-style-type: none"> - Consecutive failed logins - Consecutive failed input of the current password that is required when changing the password If the account is locked, login will be prohibited.
Account Lockout Time	1 - 1440 (minutes) (Default: 30 minutes)	

Note

- The number of consecutive failed logins will be reset in the following condition:
 - If login succeeded
 - If the lock-out time since the last failed login has passed
- The number of consecutive failed input of the current password, which is required when the password is changed will be reset in the following condition:
 - When the current password specification succeeded
 - If the lock-out time since the last failed input has passed
- With ISM 3.0.0.010 or later, when you set the user session time, the user session time takes precedence.
- If Auto Refresh of the screen is set for a particular screen when the session time is set, the session will be refreshed after each automatic refresh. Therefore, if the interval between Auto Refresh of the screen is shorter than the session time, the session will not time out after the session time. Since the settings for Auto Refresh of the screen are independent for each screen, the setting must be disabled for each screen. Auto Refresh of the screen can be disabled by setting the following.

Screen	To display screen	Operation
"Dashboard" screen	Select [Dashboard]	Select the pause mark
"Node Registration" screen	Select [Structuring] - [Node Registration]	Select the [Stop] button for Auto Refresh
"Jobs" screen	Select [Structuring] - [Jobs]	
"Tasks" screen	Select [Tasks] at the top of the screen	

Custom Login Message

Item	Parameter	Description
Show Message on Login Screen	Enable or Disable	Settings for enable or disable to display a message.
Message	0 to 1024 characters	Settings for message to display. Register any character.

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 OpenLDAP
- Managing node groups
- Setting enable/disable administrator users

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.



Note

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 following operations:

- 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 this case, the profile must 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 delete the logs.

Deleting User Groups

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 this case, modify the settings as a user belonging to an Administrator group.

Before you delete a user group, complete the following operations:

- 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, ServerView Suite DVD data from the repository.
- Delete any schedules for log collection.
- Delete any saved logs.

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:

- Import operations of firmware data
- Firmware update operations
- Import operations of OS installation file
- Assignment of profiles
- Manual log collection

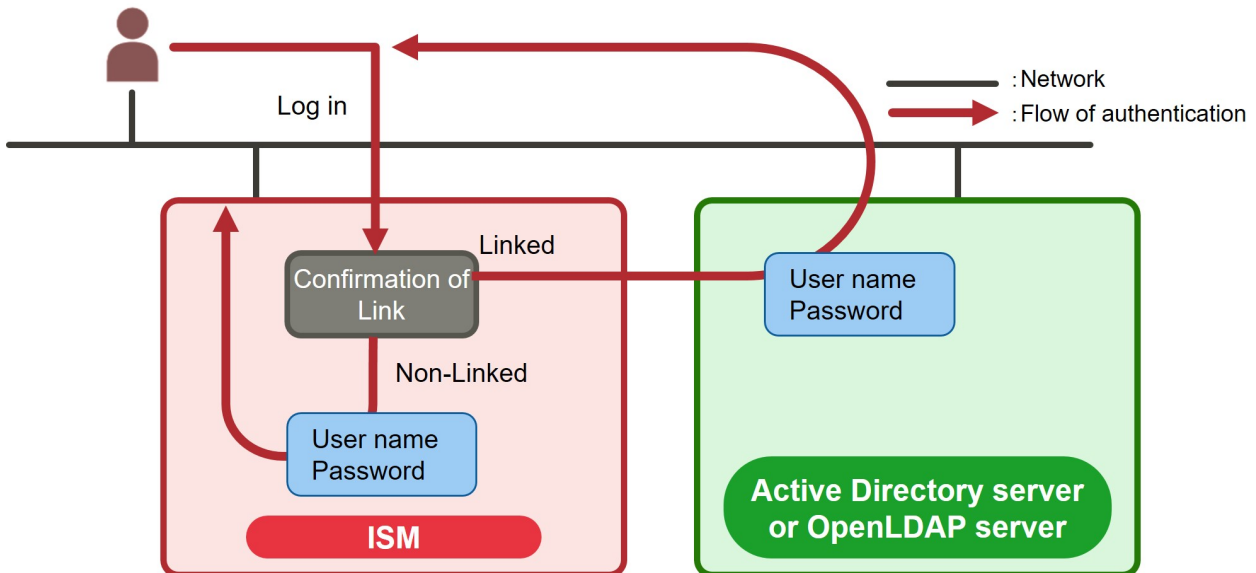
- Periodical log collection

Operating in Link with Microsoft Active Directory or OpenLDAP

By linking ISM with Microsoft Active Directory or OpenLDAP, you can integrate the management of users and passwords of multiple services.

The following diagram gives an overview of a linked configuration.

Figure 2.51 Image of ISM in link with Microsoft Active Directory/OpenLDAP



- If the user is a target of linked operations:

Authentication is executed with Microsoft Active Directory or OpenLDAP.

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

- Link with users

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

- Links with Microsoft Active Directory group or OpenLDAP group

Manage users and passwords on a directory server.

- If the user is not a target of linked operations:

Authentication is executed with ISM.

Point

- The following is the number of directory servers you can register for link with users and Link with groups.
 - A primary and a secondary server can be specified as directory servers for link with users.
 - Up to five domains can be specified for Link with groups.
- When there is no response from the active directory server, a standby directory server becomes active.

Note

- The administrator user cannot operate in link with Microsoft Active Directory or OpenLDAP.

- Users whose user authentication method is "Infrastructure Manager(ISM)" cannot operate in link with Microsoft Active Directory or OpenLDAP.
- You must set up a DNS server in ISM in advance if setting an FQDN name as the Microsoft Active Directory name or OpenLDAP 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.
- Precautions for setting an SSL certificate are as follows:
 - 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 set in the SSL certificate for the LDAP server name.
- The precautions for using SSL to connect to the directory server are as follows:
 - Specify the LDAP user name starting with ldaps://.
 - For the port number, specify the port number for SSL communication (for example 636).
 - Install an 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 in the LDAP server settings on ISM.

Multi-Factor Authentication

Multi-Factor Authentication is a function that enhances the user authentication. In addition to the user name and password, the authentication code is used for authentication. User interfaces for Multi-Factor Authentication are GUI, REST API, and SSH. FTP and hypervisor consoles are exempt from Multi-Factor Authentication.

To use Multi-Factor Authentication, the following operating requirements must be met:

- Install a multi-factor authentication client application on any mobile device.
ISM Multi-Factor Authentication comply with RFC 6238. For the multi-factor authentication client applications, Google Authenticator (iOS, Android) is recommended.
- The ISM-VA and the mobile device on which the multi-factor authentication client application is installed have the same time.
The ISM-VA and the mobile device can be up to six minutes apart in time for successful authentication.
- SSH keyboard interactive authentication of ISM is enabled.

For the procedures to enable SSH keyboard interactive authentication, refer to "4.26.1 SSH Security Settings."

When the user with Multi-Factor Authentication enabled logs into ISM, QR code is displayed. By scanning the QR code with the multi-factor authentication client application, the authentication code is displayed. After that, the user can log in using the authentication code in addition to the user name and password.



Point

- When using Multi-Factor Authentication, there is no communication between ISM and the mobile device with the multi-factor authentication client application installed, and other external servers. ISM generates Authentication Code from the string, called the "Setup Key", and the time shared between ISM and the mobile device, and performs authentication based on the matching of Authentication Code. Setup Key is included in the QR code that is displayed when the user with Multi-Factor Authentication enabled logs into ISM.
- Setup Key is different for each user.
- Setup Key stored in ISM is deleted when Multi-Factor Authentication is disabled. Manually delete Setup Key set on the mobile device.



Note

- Authorization Code is updated once every 30 seconds. Authentication Code that has been successfully authenticated cannot be reused.
- Authentication failures caused by Authentication Code are not affected by login policy settings. Failure to authenticate with an authorization code is not counted as a failure in an operation that locks the account.
- If authentication with Authorization Code fails three times in 30 seconds, you cannot log in for the next 30 seconds.
- Users whose authentication method is "Open LDAP/Microsoft Active Directory (LDAP)" can enable Multi-Factor Authentication.

In case of Multi-Factor Authentication when mobile device malfunction or loss

If a device used for Multi-Factor Authentication at the time of malfunction or loss of the mobile device, you can log into ISM by entering Emergency Codes instead of Authentication Code (Emergency Codes you used cannot be reused).

If Emergency Codes are unknown, or if you replace or lose the mobile device, disable Multi-Factor Authentication for the applicable user. The user's Setup Key is disabled. When your new mobile device is ready, re-enable Multi-Factor Authentication. The new QR Code is displayed when you log in to ISM.

If all users can no longer log in, log in to the ISM-VA as administrator from the hypervisor console and regenerate Setup Key by execute the following command:

```
# ismadm account mfa-reconf -user <user name>
```

A new QR Code is displayed when the user who regenerated the Setup Key logs into ISM.

By scanning the QR code with the multi-factor authentication client application, the authentication code is displayed.

User Session Time (ISM 3.0.0.010 or later)

You can set a session time for each user.

The session time set for each user takes precedence over the session time in the login policy.

2.14.2 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 and the ServerView Suite Update DVD that are used for firmware updates
Used in "[2.6.3 Firmware/Driver Update](#)."
- Storing of OS installation media that are used for installing OSes
Used in "[2.4 Profile Management](#)."
- Storing of ServerView Suite DVD data that is used for installing OSes and Offline Update
Used in "[2.4 Profile Management](#)" and "[2.6.3 Firmware/Driver Update](#)."



Note

If the disk space in a repository is not enough, saving the data for Repository Management will be failed. Refer to the following and allocate a sufficient disk space to the repository.

- [3.2.1.2 Estimation of the required disk space for repositories](#)
- [3.7 Allocation of Virtual Disks](#)
- "2.3.2 Manage User Groups" in "Operating Procedures."

2.14.2.1 Storing and deleting firmware data



Storing firmware data

There are two procedures to save the firmware that are applied to the managed nodes in the repository:

- Importing ISO image files of firmware data that is provided on DVD into the repository
- Importing firmware data that is released on the Fujitsu/Fsas Technologies website for each node into the repository

The firmware data to be used varies with the type of firmware update target. Prepare the DVD or firmware data shown in the following table. If the data is in DVD format, prepare the respective ISO image files.

Target firmware	Firmware type	Firmware data to be used/Location from which to retrieve
iRMC of PRIMERGY	iRMC	ServerView Suite Update DVD [Note 1] Or the firmware data that can be downloaded from the following website: https://support.ts.fujitsu.com/ [Note 2] ISM supports the versions from 11 (11.15.09 or later) to 16 (except 14.21.09) of the ServerView Suite Update DVD.
BMC of PRIMERGY	BMC	
BIOS of PRIMERGY	BIOS	
PCI Card	FC	ServerView Suite Update DVD [Note 1] Or the firmware data that can be downloaded from the following website: https://support.ts.fujitsu.com/ ISM supports the versions from 11 (11.15.09 or later) to 16 (except 14.21.09) of the ServerView Suite Update DVD.
	CNA	
	SAS	
	RAID	
	LAN	
PRIMEQUEST	Server firmware	The firmware data that can be downloaded from the following website: https://support.ts.fujitsu.com/ [Note 2]
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: https://support.ts.fujitsu.com/
	LAN Switch (X440/460-G2 model)	
	LAN Switch (CFX model)	Contact your local Fujitsu customer service partner.
	LAN Switch (Cisco Systems Nexus series, Cisco Systems Catalyst series)	Contact your local Fujitsu customer service partner.
Storage Controller	ETERNUS DX/AF	The firmware data that can be downloaded from the following website: https://support.ts.fujitsu.com/

[Note 1]: To obtain the ServerView Suite Update DVD image, refer to the following website:

<https://support.ts.fujitsu.com/IndexDownload.asp?lng=com&SoftwareGUID=>

[Note 2]: Download Flash File.

For importing the firmware data from DVD

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Firmware/Driver].
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 an option 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 to 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 "[2.14.7 Shared Directory Management](#)."
5. Specify the ISO image in [File Path].
6. Import the ISO image to select the [Apply] button.

The DVD import may take some time to complete. After starting the import, the operation is registered as an ISM task. Confirm the current status of the task on the "Tasks" screen.

When you select [Tasks] from the top of the Global Navigation Menu on the ISM GUI, the Task List is displayed.



Point

- The files you transferred to 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 select the [Delete source file] checkbox, the import source file on the FTP server will be deleted after the import has been completed.
- When you select "Shared Directory" in [File selection method], if you select the [Unmount shared directory] checkbox, the shared directory is unmounted after the import has been completed.

For importing the firmware data downloaded from the Fujitsu/Fsas Technologies web site

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Firmware/Driver].
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 an option in [File selection method].
 - Local
Import firmware data stored 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 connections and how to transfer to 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 the version of the firmware in [Version], and 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 name
iRMC	<ul style="list-style-type: none"> - PRIMERGY (server with iRMC S4 or later) - PRIMEQUEST 3800B
BIOS	<ul style="list-style-type: none"> - PRIMERGY (server with iRMC S3 or later) - PRIMEQUEST 3800B [Note]

[Note]: Only items that are in Offline mode are imported.

- Enter manually

Enter the firmware version manually when importing.

Use the table below to enter the versions.

For information on the version, refer to the release notes.

Type	Model name	Version
PRIMEQUEST	PRIMEQUEST 2400L3 etc.	Version of the firmware of PRIMEQUEST
FC	LPe1250, LPe12002, MC-FC82E	BIOS and FW versions
	LPe16000 or later, MC-FC162E	Firmware version
	QLE2560, QLE2562	BIOS version
	QLE2670, QLE2672, QLE2690, QLE2692, QLE2740, QLE2742	BIOS and FW versions
	QLE2770 and QLE2772 or later	FW versions
CNA	OCe10102, OCe14102 or MC-CNA112E etc.	Firmware version
SAS	PSAS CP200i, PSAS CP400i, PSAS CP400e etc.	
RAID	PRAID CP400i, PRAID EP420e, PY SAS RAID Mezz Card 6Gb etc.	
LAN	MCX415, MCX416 etc.	
LAN Switch	SR-X model	Version of basic software
	VDX model	Firmware version
	CFX model	
	PY CB Eth Switch/IBP 1Gb 36/12	
	PY CB Eth Switch/IBP 10Gb 18/8	
	PY CB Eth Switch 10/40 Gb 18/8+2	
	Cisco Systems Nexus series	Version of NX-OS
	Cisco Systems Catalyst series	Version of IOS

Type	Model name	Version
ETERNUS DX/AF	ETERNUS DX/AF model	Firmware version

Point

- If you select "Local" in [File selection method], specify the zip file where the firmware data and documents are saved in [File Path] to import.
If the firmware is provided in a self-extracting format (exe), decompress the file once. Then, compress the files that were decompressed again in zip format, and import them.
- If you select "FTP" in [File selection method], transfer the folder where the firmware data and documents are saved to the FTP server of ISM-VA, and then specify the transferred folder in [File Path] to import it.
If the firmware is provided in a self-extracting format (exe), decompress the file. Transfer the folder that was decompressed 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 (such as ffftp or WinSCP) to transfer them. In this case, set it so that the character encoding is converted with UTF-8. Do not use Windows Explorer, because the character encoding 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 encoding conversion settings.
 3. Execute the import again.
- The files you transferred to 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.
In this case, you must check which type of firmware data the node whose firmware you are updating 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.
You can check what type of firmware data a node registered in ISM is using.
 1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Nodes].
 2. In the [Column Display] field on the "Node List" screen, select [Firmware/Driver].
 3. Check the [FW/Driver Name] column.

Deleting firmware data from repository

The following is a sample operation using the GUI.

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Firmware/Driver].
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 the repository.
 - a. Select the [Import Data List] tab.
 - b. Select the checkboxes for the data to be deleted, and then select [Delete] from the [Actions] button.
 - c. Proceed by following the instructions on the screen.

- If firmware data downloaded from the Fujitsu/Fsas Technologies website was stored in the repository.
 - a. Select the [Firmware Data] tab.
 - b. Select the checkboxes for the data to be deleted, and then select [Delete] from the [Actions] button.
 - c. Proceed by following the instructions on the screen.

2.14.2.2 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 Fsas Technologies custom image.
2. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Profiles].
3. From the menu on the left side of the screen, select [DVD Import].
4. From the [Actions] button, select [Import DVD].
5. Select an option 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 to FTP, refer to "[2.1.2 FTP Access](#)."
 - Shared Directory

Import an 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 "[2.14.7 Shared Directory Management](#)."
6. Specify the ISO image in [File Path].
7. Select the appropriate OS type in [Media Type], and then execute import with the [Apply] button.

Point

- The files you transferred to 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 select the [Delete source file] checkbox, the import source file on the FTP server will be deleted after the import has been completed.
- When you select "Shared Directory" in [File selection method], if you select the [Unmount shared directory] checkbox, the shared directory is unmounted after the import has been completed.

Deleting OS installation files from the repository

The procedure for deletion is as follows.

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Profiles].
2. From the menu on the left side of the screen, select [DVD Import].
3. Select the checkboxes for the data to be deleted, and then select [Delete] from the [Actions] button.
4. Proceed by following the instructions on the screen.

2.14.2.3 Storing and deleting ServerView Suite DVD



Storing 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 ISM GUI, 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 an option 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 to FTP, refer to "[2.1.2 FTP Access](#)."
 - Shared Directory
Import an 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 "[2.14.7 Shared Directory Management](#)."
6. Specify the ISO image in [File Path].
7. Select [ServerView Suite DVD] in [Media Type], and then execute import with the [Apply] button.



Point

- The files you transferred to 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 select the [Delete source file] checkbox, the import source file on the FTP server will be deleted after the import has been completed.

- When you select "Shared Directory" in [File selection method], if you select the [Unmount shared directory] checkbox, the shared directory is unmounted after the import has been completed.

Deleting ServerView Suite DVD data from the repository

The procedure for deletion is as follows.

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Profiles].
2. From the menu on the left side of the screen, select [DVD Import].
3. Select the checkboxes for the data to be deleted, and then select [Delete] from the [Actions] button.
4. Proceed by following the instructions on the screen.

2.14.3 Installation of Emulex OneCommand Manager CLI and QLogic QConvergeConsole CLI



- To update the firmware 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 OneCommand Manager CLI and for QLogic QConvergeConsole CLI.

For PCI cards that require installation of Emulex OneCommand Manager CLI and QLogic QConvergeConsole CLI, refer to "Support Matrix."

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

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

Select [DOWNLOADS] and select the target operating system.

The reference procedures are subject to change without notice.

- 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.

2.14.4 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, 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 updates
Profile Management	Import of OS installation media Assignment of profiles Reassignment of profiles Release of profiles Update eIM to the latest version
Log Management	Collection of logs Deletion of logs Creation of download file

Function	Type of processing
Network Management	Change of VLAN settings
Virtual Resource Management	Refreshing of virtual resource information
Cluster Management	Resource Planning

Note

If the process of updating eIM to the latest version started (the progress of the subtask is 1% or more), the process of updating eIM to the latest version will continue even if you cancel from ISM. After the process of updating eIM to the latest version is completed, the status of the task is displayed as "Cancellation completed."

If you want to cancel the process of updating eIM to the latest version, refer to the following documents for the target server and delete the executing task from "Task Manager."

"ServerView Suite iRMC Sx Web Interface" (Sx contains the number of editions S4 or later)

Refer the following Fujitsu/Fsas Technologies manual site.

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

Select [Select a new Product] - [Browse for product] and select a target server.

Download the file from [Server Management Controller].

The reference procedures are subject to change without notice.

Procedure to display the "Tasks" screen

Executable user

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

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

2.14.5 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 "[2.14.5.1 List of commands in ISM-VA Management.](#)"

Functions for use when installing ISM

Function name	Overview of function
Initial Setup	<p>This function is for the basic setup from a hypervisor console after installing ISM-VA.</p> <ul style="list-style-type: none"> - 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 from a web browser.

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 can modify the settings for ISM-VA after installation. <ul style="list-style-type: none">- Network settings- Time settings- Locale setting- Virtual disk settings- Modification of host names
Maintenance	This function can execute maintenance. <ul style="list-style-type: none">- Confirmation of versions- Application of Patches- Collection of Archived Logs- Switching of debug flags

2.14.5.1 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
Confirmation of network connectivity	ismadm network ping

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
Keymap setting	ismadm locale set-keymap

License settings

Function	Command
Display of licenses	ismadm license show
Registration of licenses	ismadm license set
Deletion of licenses	ismadm license delete

Certificate activation

Function	Command
Deployment of SSL certificates	ismadm sslcert set
Display of SSL certificates	ismadm sslcert show
Export of SSL certificates	ismadm sslcert export
Creation of self-signed 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 services individually	ismadm service start
Stop of internal services individually	ismadm service stop
Restart of internal services individually	ismadm service restart
Display of status of internal services individually	ismadm service status
Enabling of internal services individually	ismadm service enable
Disabling of internal services 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
Cancellation of allocation of LVM volume to user group	ismadm volume umount
Display of volume settings	ismadm volume show

Function	Command
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
Migrate of ISM-VA	ismadm system migrate
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 of certificate for alarm notification mails	ismadm event import
Display of certificate for alarm notification mails	ismadm event show
Deletion of 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 (GUI/REST)	ismadm security show-tls

Function	Command
SSL/TLS enable status display (FTPS)	ismadm security show-tls-ftp
SSL/TLS enable setting (GUI/REST)	ismadm security enable-tls
SSL/TLS enable setting (FTPS)	ismadm security enable-tls-ftp
Encryption suite settings display (GUI/REST)	ismadm security show-sslcipher
Encryption suite settings (GUI/REST)	ismadm security set-sslcipher
Confirmation of SSH security settings	ismadm security show-ssh-conf
Setting of SSH security	ismadm security set-ssh-conf
Display of SSH logins	ismadm security show-ssh-loginfail
Disabling of user lock for failed SSH logins	ismadm security reset-ssh-userlock
Adding of SSH source of connection IP address	ismadm security add-ssh-clientip
Deletion of SSH source of connection IP address	ismadm security delete-ssh-clientip
Registration of SSH public key	ismadm security set-ssh-pubkey
Display of SSH public key	ismadm security show-ssh-pubkey
Deletion of SSH public key	ismadm security delete-ssh-pubkey
Display of console auto logout settings	ismadm security show-console-timeout
Setting for console auto logout	ismadm security set-console-timeout
Confirmation of source of connection IP address restriction (GUI/REST)	ismadm security show-gui-conf
Confirmation of source of connection IP address restriction (Samba)	ismadm security show-smb-conf
Confirmation of source of connection IP address restriction (FTP)	ismadm security show-ftp-conf
Confirmation of source of connection IP address restriction (TFTP)	ismadm security show-tftp-conf
Confirmation of source of connection IP address restriction (9213 port)	ismadm security show-svs-conf
Confirmation of source of connection IP address restriction (SNMP Trap)	ismadm security show-snmp-conf
Confirmation of source of connection IP address restriction (HTTPS data)	ismadm security show-https-data-conf
Confirmation of source of connection IP address restriction (SSDP)	ismadm security show-ssdp-conf
Settings of source of connection IP address restriction (GUI/REST)	ismadm security set-gui-conf
Setting of source of connection IP address restriction (Samba)	ismadm security set-smb-conf
Setting of source of connection IP address restriction (FTP)	ismadm security set-ftp-conf
Setting of source of connection IP address restriction (TFTP)	ismadm security set-tftp-conf
Setting of source of connection IP address restriction (9213 port)	ismadm security set-svs-conf
Setting of source of connection IP address restriction (SNMP Trap)	ismadm security set-snmp-conf
Setting of source of connection IP address restriction (HTTPS data)	ismadm security set-https-data-conf
Setting of source of connection IP address restriction (SSDP)	ismadm security set-ssdp-conf
Adding of source of connection IP address (GUI/REST)	ismadm security add-gui-clientip
Adding of source of connection IP address (Samba)	ismadm security add-smb-clientip
Adding of source of connection IP address (FTP)	ismadm security add-ftp-clientip
Adding of source of connection IP address (TFTP)	ismadm security add-tftp-clientip
Adding of source of connection IP address (9213 port)	ismadm security add-svs-clientip
Adding of source of connection IP address (SNMP Trap)	ismadm security add-snmp-clientip
Adding of source of connection IP address (HTTPS data)	ismadm security add-https-data-clientip

Function	Command
Adding of source of connection IP address (SSDP)	ismadm security add-ssdp-clientip
Deletion of source of connection IP address (GUI/REST)	ismadm security delete-gui-clientip
Deletion of source of connection IP address (Samba)	ismadm security delete-smb-clientip
Deletion of source of connection IP address (FTP)	ismadm security delete-ftp-clientip
Deletion of source of connection IP address (TFTP)	ismadm security delete-tftp-clientip
Deletion of source of connection IP address (9213 port)	ismadm security delete-svs-clientip
Deletion of source of connection IP address (SNMP Trap)	ismadm security delete-snmp-clientip
Deletion of source of connection IP address (HTTPS data)	ismadm security delete-https-data-clientip
Deletion of source of connection IP address (SSDP)	ismadm security delete-ssdp-clientip
Confirmation of IP address restriction settings for ISM session authentication	ismadm security show-ismauth-conf
Changing of IP address restriction settings for ISM session authentication	ismadm security set-ismauth-conf

Settings for linking with other software

Function	Command
Registration of certificate for link with other software	ismadm security import-software-cert
Display of certificate for link with other software	ismadm security show-software-cert
Deletion of certificate for link with other software	ismadm security delete-software-cert

Profile related settings

Function	Command
Setting to enable/disable the verification of profiles	ismadm system set-profile-verify
Display of the enabled/disabled status for verification of profiles	ismadm system show-profile-verify

Account related settings

Function	Command
Resetting of Multi-Factor Authentication	ismadm account mfa-reconf -user

Settings for relay route port

Function	Command
Setting for relay route port	ismadm relayroute port-change
Display of relay route port	ismadm relayroute port-show

Creation of client certificate for relay route

Function	Command
Certation of client certificate for relay route	ismadm relayroute clientcert-create
Display of client certificate for relay route	ismadm relayroute clientcert-show



Note

ISM-VA must be restarted if the time interval settings were returned to a past time.

2.14.6 Management of Cloud Management Software

To use the functions that link with cloud management software, register cloud management software with ISM.

The following cloud management software is supported:

- VMware vCenter Server 7.0
- VMware vCenter Server 8.0
- Microsoft System Center 2012
- Microsoft System Center 2012R2
- Microsoft System Center 2016
- Microsoft System Center 2019
- Microsoft System Center 2022
- Microsoft System Center 2025
- Microsoft Failover Cluster (Windows Server 2012) [Note]
- Microsoft Failover Cluster (Windows Server 2012R2) [Note]
- Microsoft Failover Cluster (Windows Server 2016) [Note]
- Microsoft Failover Cluster (Windows Server 2019) [Note]
- Microsoft Failover Cluster (Windows Server 2022) [Note]
- Microsoft Failover Cluster (Windows Server 2025) [Note]
- Microsoft Failover Cluster (Azure Stack HCI) [Note]
- KVM (Red Hat Enterprise Linux)
- KVM (SUSE Linux Enterprise)
- OpenStack (Red Hat Enterprise Linux)

[Note]: For Microsoft Failover Cluster, only virtual machines registered for cluster roles are displayed.

2.14.6.1 Registering cloud management software

	Administrator group	Other groups
Executable user	<div>Admin Operator Monitor</div>	<div>Admin Operator Monitor</div>

For details, refer to "6.2.1 Register a Cloud Management Software" in "Operating Procedures."

2.14.6.2 Retrieving information from cloud management software

	Administrator group	Other groups
Executable user	<div>Admin Operator Monitor</div>	<div>Admin Operator Monitor</div>

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.

This information can be retrieved if the type of cloud management software is 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.

This information can be retrieved if the type of cloud management software is OpenStack. VMware vCenter Server, System Center, Microsoft Failover Cluster, and KVM are not supported.



Note

ISM manages information of virtual machines, virtual switches, and virtual routers by linking information of the registered cloud management software and OS information of the nodes. 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.

For the procedure to manually retrieve the information at any time, refer to Step 1 to Step 6 of "6.2.2 Confirm Information for Virtual Machines on Managed Servers" in "Operating Procedures."

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, and then confirm the information of the virtual machine, virtual switch, or virtual router.



Note

- If both System Center and the Microsoft Failover Cluster registered in System Center is registered 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 you delete a virtual machine from the Hyper-V manager, also delete this virtual machine from the failover cluster manager role.

2.14.6.3 Editing cloud management software

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

For the procedure to edit the cloud management software information registered in ISM, refer to "6.2.1.1 Edit cloud management software information" in "Operating Procedures."

2.14.6.4 Deleting cloud management software

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

The following is the operation procedure for deleting cloud management software registered in ISM.

1. From the Global Navigation Menu on the ISM GUI, select [Settings] - [General] - [Cloud Management Software], and then select the target cloud management software on the "Cloud Management Software List" screen.
2. From the [Actions] button, select [Delete].
3. Execute [Delete] to delete the cloud management software.



After deleting the cloud management software, the message ID "50170511" may be displayed. If this message is displayed, execute ["2.9.3.3 Updates of virtual resource information."](#)

2.14.6.5 Changing Event Output Restricted Mode for the cloud management software



Event Output Restricted Mode for the cloud management software is configured to prevent ISM from detecting events (Alarm) that occur due to operations performed during the maintenance on cloud management software (host configuration changes, password changes, etc.) or influences such as status changes.

If you need to execute maintenance for cloud management software, it is recommended to enable Event Output Restricted Mode on the target cloud management software registered in ISM.

Enabling Event Output Restricted Mode for the cloud management software stops ISM from periodically retrieving information from cloud management software. Therefore, the following ISM information is no longer automatically updated.

- Virtual Resource Information
For details, refer to ["2.9.3.3 Updates of virtual resource information"](#) and ["2.9.3.4 Display of vSAN disk impact on virtual machines."](#)
- Cluster Information
For details, refer to ["2.13.1.3 Refreshing cluster information."](#)
- Information from cloud management software
For details, refer to ["2.14.6.2 Retrieving information from cloud management software."](#)

There is no effect on ISM functions other than the above information retrieval when enabling Event Output Restricted Mode for the cloud management software. The following functions do not stop retrieving information from the cloud management software regardless of whether Event Output Restricted Mode for the cloud management software is enabled.

- Anomaly Detection
For details on Anomaly Detection, refer to ["2.3.6 Anomaly Detection."](#)
- Packet Analysis of Virtual Network
For details on Packet Analysis of Virtual Network, refer to ["2.11 Packet Analysis of Virtual Network."](#)

Therefore, the above functions may cause events (Alarm) due to information retrieval from the cloud management software.

Enabling Event Output Restricted Mode for the cloud management software registered with ISM

1. From the Global Navigation Menu on the ISM GUI, select [Settings] - [General] - [Cloud Management Software], and then select the target cloud management software on the "Cloud Management Software List" screen.
2. From the [Actions] button, select [Enable Event Output Restricted Mode].
When the screen for confirmation is displayed, confirm the target cloud management software name and select the [Yes] button.
3. If Anomaly Detection is started on the node managed by the cloud management software, enable Maintenance Mode for the node.
For details, refer to "Setting procedure for enabling Maintenance Mode" in ["5.1 Maintenance Mode."](#)

4. If threshold monitoring is enabled for the virtual network adapter on the node that the cloud management software is managing, set threshold monitoring to disable the virtual network adapter.

For details, refer to "6.6.1 Set Virtual Adapter Threshold" in "Operating Procedures."

Disabling Event Output Restricted Mode for the cloud management software registered with ISM

1. From the Global Navigation Menu on the ISM GUI, select [Settings] - [General] - [Cloud Management Software], and then select the target cloud management software on the "Cloud Management Software List" screen.

If Event Output Restricted Mode is enabled, "Cloud Management Software Name" is preceded by "🔒".

2. From the [Actions] button, select [Disable Event Output Restricted Mode].

When the screen for confirmation is displayed, confirm the target cloud management software name and select the [Yes] button.

3. If required, disable Maintenance Mode for the node.

For details, refer to "Procedure for disabling Maintenance Mode" in "5.1 Maintenance Mode."

4. If required, enable threshold monitoring for the virtual network adapter.

For details, refer to "6.6.1 Set Virtual Adapter Threshold" in "Operating Procedures."

2.14.7 Shared Directory Management

Add a shared directory for use when importing a DVD.

2.14.7.1 Adding shared directories



The following displays the procedure for adding a new shared directory.

1. From the Global Navigation Menu on the ISM GUI, select [Settings] - [General] - [Shared Directory].
2. From the [Actions] button, select [Register].
3. Enter the required 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.
User Group Name	Select the user group that the shared directory information belongs to.

4. 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.

2.14.7.2 Editing shared directories



Executable user

Administrator group: Admin, Operator, Monitor

Other groups: Admin, Operator, Monitor

The following is the operation procedure for editing shared directory information registered in ISM.

1. From the Global Navigation Menu on the ISM GUI, select [Settings] - [General] - [Shared Directory].
2. Execute one of the following:
 - Select the checkbox for the shared directory you want to edit, and then select [Edit] from the [Actions] button.
 - Select the shared directory you want to edit, and select [Edit] from the [Actions] button on the displayed information screen.
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. Select [Apply] to apply the changes.



Shared directories that are mounted cannot be edited.

2.14.7.3 Deleting shared directories



Executable user

Administrator group: Admin, Operator, Monitor

Other groups: Admin, Operator, Monitor

The following is the operation procedure to delete shared directories registered in ISM.

1. From the Global Navigation Menu on the ISM GUI, select [Settings] - [General] - [Shared Directory].
2. Execute one of the following:
 - Select the checkboxes for the shared directories you want to delete, and then select [Delete] from the [Actions] button.
 - Select the shared directories you want to delete, and then select [Delete] from the [Actions] button on the displayed information screen.
3. Select [Delete].



Shared directories that are mounted cannot be deleted.

2.14.7.4 Mounting shared directories

	Administrator group	Other groups
Executable user	<div>Admin Operator Monitor</div>	<div>Admin Operator Monitor</div>

The following is the operating procedure for mounting shared directory information registered in ISM.

1. From the Global Navigation Menu on the ISM GUI, select [Settings] - [General] - [Shared Directory].
2. Execute one of the following:
 - Select the checkboxes for the shared directories you want to mount, and then select [Mount] from the [Actions] button.
 - Select the shared directories you want to mount, and then select [Mount] from the [Actions] button on the displayed information screen.



- The following displays the privileges 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, the directory is unmounted:
 - ISM-VA was restarted or stopped
 - The ISM service was stopped
- The following operations cannot be executed for a user group that has mounted shared directory information:
 - Changing the user group name
 - Deleting the user group

2.14.7.5 Unmounting shared directories

	Administrator group	Other groups
Executable user	<div>Admin Operator Monitor</div>	<div>Admin Operator Monitor</div>


The following is the operating procedure for unmounting shared directory information registered in ISM.

1. From the Global Navigation Menu on the ISM GUI, select [Settings] - [General] - [Shared Directory].
2. Execute one of the following:
 - Select the checkboxes for the shared directories you want to unmount, and then select [Unmount] from the [Actions] button.
 - Select the directories you want to unmount, and then select [Unmount] from the [Actions] button on the displayed information screen.

2.14.8 Link with ISM

2.14.8.1 Link display for the status information of other ISM installations

In ISM, the status information (Alarm Status/Status) of other ISM installations can be displayed on the Dashboard.

Links				Y
Tokyo DC	 4	 1	 2	Tokyo
Kawasaki DC	 2	 2		Kawasaki

For details on status (Alarm Status/Status), refer to "2.1.1 GUI."

The following describes the operating procedure to display the status of other ISM installations on the Dashboard.

1. Set a user who wants to display the status of other ISM installation on the Dashboard.

This user must also be registered in the other ISM installations 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 on whose Dashboard you want to display the status of other ISM installations by making the following settings:
 - In [Link with ISM], select [Set this user as a link user]
 - Password

2. Register the CA certificates of the other ISM installations to display.

For details, refer to "Registration of certificates" in "2.14.8.2 Certificate management for links to other ISM installations."

3. Add [Links] to the Dashboard on the GUI.

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

If [Links] is displayed, proceed to Step f.

If [Links] is not displayed, use the following steps to add the link.

- b. From [☰] at the top of the screen, select [Add Widget].
- c. From the displayed [Add Widget], select [Links], and then select the [Add] button.
- d. From [☰], select [Change Layout].
- e. Select [Save] on [Edit Mode].
- f. Select [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.

For the procedure to add widgets, and details on the widget contents, refer to the ISM online help.

2.14.8.2 Certificate management for links to other ISM installations

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

CA certificates used to access other ISM installations are added in the link function of the widget.

Registration of certificates

The following describes the procedure for adding new certificates.

1. From the Global Navigation Menu on the ISM GUI, select [Settings] - [General] - [CA Certificate].
2. From the [Actions] button, select [Register].
3. Enter the required information:
 - Action after completion
Select whether to delete the source file.
 - File Path
Upload the CA certificate of the other ISM installation that you want to access, and set the uploaded file.
 - Host Name/IP Address
Set the host name or IP address of the other ISM installation that you want to access.
4. Select the [Register] button.

The results screen is displayed, and the registered certificate is displayed in the "CA Certificate List" screen.



Note

- The certificate to register is the CA certificate. Regarding CA certificates, refer to "[4.7.5 Download of CA Certificates](#)."
- ISM does not check the availability of access to the other ISM installations with the registered certificate.

Deleting certificates

The following is the operation procedure for deleting certificates registered in ISM.

1. From the Global Navigation Menu on the ISM GUI, select [Settings] - [General] - [CA Certificate].
2. Execute one of the following.
 - Select the checkboxes for the certificates you want to delete, and then select [Delete] from the [Actions] button.
 - Select the certificates you want to delete, and then select [Delete] from the [Actions] button on the displayed information screen.
3. Execute [Delete] to delete the certificates.



Note

Certificates can be deleted also if you are using the link function of the widget.

2.14.9 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.

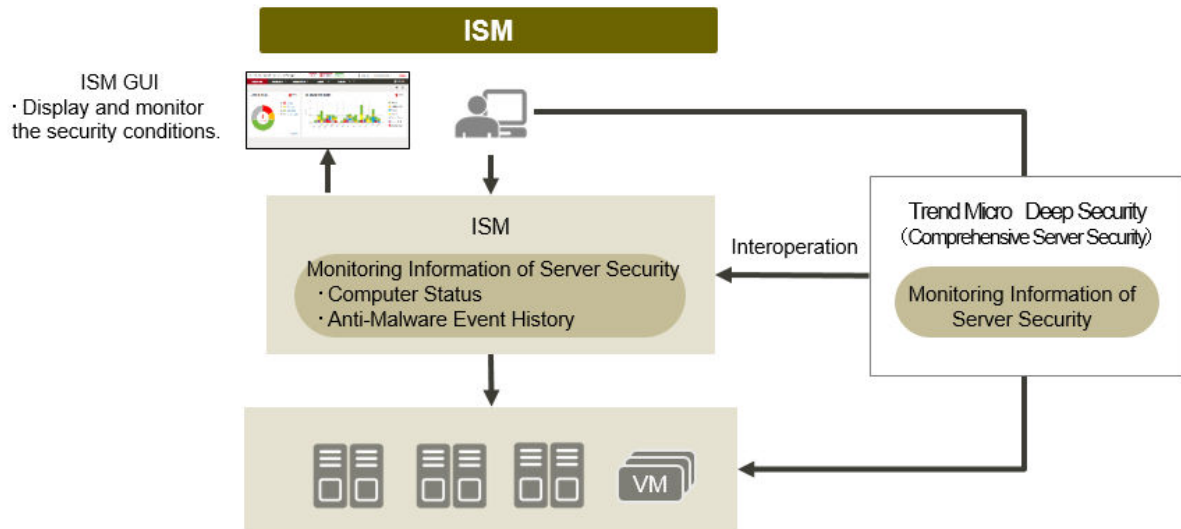
The following is the software that can be linked:

- 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 2.52 Image of link with Trend Micro Deep Security



The following are the widgets that can be displayed on the Dashboard on the ISM GUI:

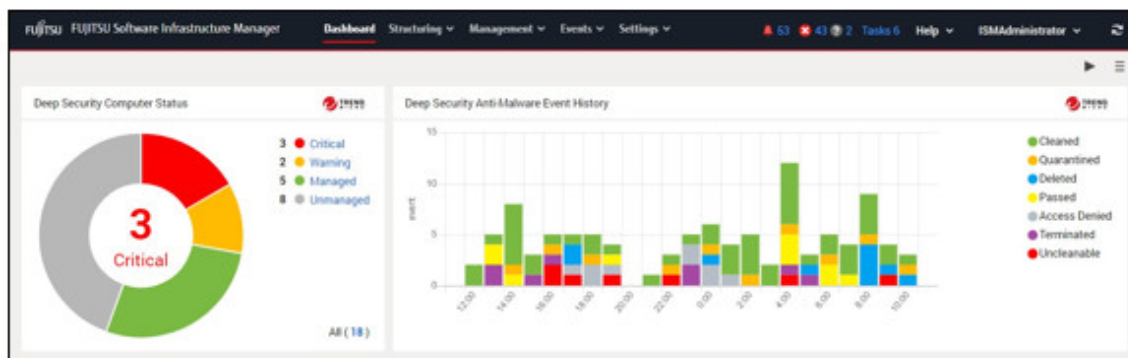
- Computer Status widget

Displays graphs of the security status of the computers managed by Deep Security Manager. If you select a graph, the GUI of Deep Security Manager 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 GUI of Deep Security Manager opens and you can check detailed information.

Figure 2.53 Deep Security link widget



2.14.9.1 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 GUI of Deep Security Manager.

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.



The following is the export procedures for each web browser. Display the GUI of Deep Security Manager in a web browser, and then use the following procedures 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



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 the certificate file to ISM-VA.

For details on upload procedures, refer to "1.4.1 Upload Files to ISM-VA" in "Operating Procedures." When uploading, specify "Certificate for link with other software" for the file type.

4. Register the 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
```

2.14.9.2 Procedure to link with Deep Security

1. Log in to the ISM GUI and open the Dashboard screen.
2. Select [Language] from the user name displayed on the upper-right of the screen.
3. Set the same time zone as is set for Deep Security Manager.
4. From the [≡] in the upper-right corner of the screen, select [Add Widget].
5. From the "Add Widget" screen, select the [Other widgets] pane.
[Link widgets with Trend Micro Deep Security] is displayed on the "Other Widgets" screen.
6. Select the [Deep Security Computer Status] pane or the [Deep Security Anti-Malware Event History] pane, 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.

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.

Message	Action
	Execute the procedures in " 2.14.9.1 Preparations in advance for Deep Security link " 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 " 2.14.9.1 Preparations in advance for Deep Security link " 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 " 2.14.9.1 Preparations in advance for Deep Security link " 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"> - There is an error in the Deep Security user name or password entered on the ISM GUI. - 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. - There is an error in the communication with Deep Security. - The number of Deep Security sessions exceeds the number allowed. For details on the cause, check the Deep Security system event.

If the error is not resolved, 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 ISM GUI has been displayed.	If you select the [Back] button of the browser, the ISM GUI 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.

.....

Chapter 3 Installation

This chapter describes how to install ISM.



Point

When structuring a virtualized platform system using ISM for PRIMEFLEX, refer to the following references for the procedure to install ISM:

- For structuring PRIMEFLEX for VMware vSAN
"3. Installation of Virtualized Platform System" in "Integrated System PRIMEFLEX for VMware vSAN V1 Installation Guide."
- For structuring PRIMEFLEX for VMware vSAN / PRIMEFLEX for VMware vSAN V2 / PRIMEFLEX for VMware vSAN V3 / PRIMEFLEX for VMware vSAN V4
"Configuring Virtualized Platforms" in "Integrated System PRIMEFLEX for VMware vSAN V1 Installation Guide," or "Integrated System PRIMEFLEX for VMware vSAN V2 Installation Guide," or "Integrated System PRIMEFLEX for VMware vSAN V3 Deployment Guide," or "Integrated System PRIMEFLEX for VMware vSAN V4 Deployment Guide."

3.1 Workflow for Installing ISM

This section describes the workflow for installing ISM.

(1) Installation design

To prepare for installation of ISM, the following tasks must be performed:

- Disk Resource Estimation
- Repository Setup
- Network Design
- Node Name Design
- User Design

For details on the operations, 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 of the installed ISM-VA.

For the environment setting 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 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 to manage the virtual machines and virtual switches of the managed node.

For details on registering the cloud management software, refer to "[2.14.6 Management of Cloud Management Software](#)." In addition, for pre-settings required to use Management of Cloud Management Software, refer to "[Appendix B Settings for Monitoring Target OS and Cloud Management Software](#)."

(8) Pre-Settings for Managing Virtual Resource/Clusters

To use Virtual Resource Management and Cluster Management in ISM for PRIMEFLEX, you must set it up in advance.

Refer to "[3.8 Pre-Settings for Managing Virtual Resources/Clusters](#)."

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 Design](#)
- [3.2.4 User Design](#)

3.2.1 Disk Resource Estimation

Upon using ISM, estimate the usage of the disk space described in the table below and allocate additional disk space beforehand.

Usage	Data to be stored	Calculation procedure for capacity	Type	
			System area	User area
Log archive	Logs collected by Log Management and files archived upon being downloaded "2.5 Log Management"	Calculate according to the number of nodes that collect logs, the types of logs collected, collection frequency, and storage period "3.2.1.1 Estimation of the required disk space for log storage "	Y [Note 1]	Y
Repository (Excludes ServerView Suite DVD)	DVD images and firmware data "2.4 Profile Management" "2.6.3 Firmware/Driver Update"	Calculate according to the number of DVDs to import and the volume of firmware data "3.2.1.2 Estimation of the required disk space for repositories"	Y [Note 1]	Y
Repository (Only ServerView Suite DVD)	DVD image "2.4 Profile Management" "2.6.3 Firmware/Driver Update"	Calculate according to the number of DVDs to import	Y	-

Usage	Data to be stored	Calculation procedure for capacity	Type	
			System area	User area
		"3.2.1.2 Estimation of the required disk space for repositories"		
Node management data	Data utilized by ISM for internal operation	Calculate according to the number of managed nodes "3.2.1.3 Estimation of the required disk space for node management data"	Y	-
ISM RAS Logs	Logs used for investigation when failures occur	Calculate according to the number of managed nodes "3.2.1.4 Estimation of the required disk space for ISM RAS log"	Y	-
Maintenance data	Files taken when archiving ISM RAS logs "4.5 Collection of Maintenance Data"	Calculate according to the generations to store the number of managed nodes and the documents "3.2.1.5 Estimation of required disk space for maintenance data"	Y [Note 1]	Y [Note 2]
ISM Backup/Restore	ISM Backup file "4.4 Backup and Restoration of ISM"	Calculate according to the number of managed nodes "3.2.1.6 Estimation of required disk space for ISM Backup/Restore"	Y [Note 1]	Y [Note 2]
CSV export of Sustainability Monitor	File displaying CO2 emissions and power consumption data in CSV format "2.12.4 Export in CSV Format"	Calculate according to the number of nodes and sessions targeted by the Sustainability Monitoring "3.2.1.7 Estimation of required disk space for CSV export of Sustainability Monitor"	Y [Note 1]	Y [Note 2]

[Note 1]: If a user group is allocated with an area, the allocated area is used in the user group. In user groups not allocated with an area, a system area is used.

[Note 2]: They are exported to the repository area of the Administrator user group.



Note

- Disk capacity cannot be expanded when operating ISM-VA. Therefore, low disk space during operation affects the operation of log collection for Log Management as well as of repositories and backups. Consequently, it is important to estimate the disk capacity beforehand to make sure sufficient space is available.

Create a virtual disk that has the required disk space estimated and allocate it to ISM-VA.

For creating a virtual disk and allocating it to a system area, refer to "3.7.1 Allocation of Virtual Disks to ISM-VA."

For creating a virtual disk and allocating it to a user group, refer to "3.7.2 Allocation of Virtual Disks to User Groups."

- In order to avoid insufficient disk space, operations should be structured to periodically delete repositories, backups, and other unnecessary data.
- Current use of the disk space can be checked with the following procedure.

1. From the console, log in to ISM-VA as an administrator.
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 the required disk space for log storage

The required disk space for logs exported through Log Management depend on the number of managed nodes and on the period or frequency of log retention. You must estimate the disk space for the potential number of future additional node installations.

In addition, when downloading logs, you must estimate in the same way the disk space to be used.

For information on how to estimate the required disk space for logs that are exported with Log Management, refer to "[A.3.2 General Standards for Disk Usage in Using Log Management](#)."

In addition to the logs that are output with Log Management, there are "Operation Log," "Audit Log," and "SNMP Traps."

Their maximum storage capacity is as follows. These capacities do not depend on the number of nodes.

- Operation Log and Audit Log
Maximum storage capacity: 1,000,000 logs each (200 MB each)
- SNMP traps
Maximum storage capacity: 100,000 traps (300 MB)

These capacities are included in the free disk space as in "[1.3.1 Requirements for Hypervisor to Run ISM-VA \(Virtual Machines\)](#)."

3.2.1.2 Estimation of the required disk space for repositories

Repositories must be prepared in ISM-VA in order to operate functions such as Profile Management or Firmware Management. The following data is stored in a repository:

- Firmware data
- OS image files
- Work files

The disk space required for repositories vary according to the type of OS to be installed for the managed nodes and the number of ServerView Suite Update DVDs to be imported. Normally a disk space of 20 GB or more will be used. Refer to the table below to estimate the required disk space.

Usage	Operation	Required disk space
Storage of firmware data	Import ServerView Suite Update DVD	Approximately 14 GB per ServerView Suite Update DVD
	Import of other firmware data	Depends on data to be imported. Up to approximately 100 MB

Usage	Operation	Required disk space
File storage for OS installation media	Import the Windows installation media	Approximately 3 to 8 GB per OS type Only the OS type to be installed with Profile Management must be imported.
	Import the VMware ESXi installation media	Approximately 0.5 GB per OS type Only the OS type to be installed with Profile Management must be imported.
	Import the Linux installation media	Approximately 4 GB per OS type
Storage of ServerView Suite DVD	Import the 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 use this feature, prepare a separate repository for each user group. In this case, you must estimate the required disk space for all items other than Server View Suite DVD for the 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 space on the LVM volume in the system area.

3.2.1.3 Estimation of the required disk space for node management data

Estimate the required disk space for the data area for node management depending on the number of nodes to be managed in ISM-VA.

The following table shows the number of managed nodes and required disk space for the data area for node management.

Number of managed nodes	Required disk capacity
100 nodes or less	20 GB
400 nodes or less	80 GB
1000 nodes or less	200 GB



Note

The table above shows an estimate from the initial monitoring items when a node is registered have not been changed.

In addition to the above, additional disk space is required when using the following. Refer to the following to add the required amount of disk space.

- Anomaly Detection
For details refer to "[2.3.6.1 Operation requirements](#)."
- Network statistic information
Check the following.

When monitoring settings of the network statistic information is enabled

The following additional capacity estimates are required to monitor the network statistic information. The amount of disk space required depends on the network device.

Classification	Disk capacity
Disk space for one port Up to one year of monitoring data is stored.	240 MB
Disk space for each switch that supports the display of network statistics	Number of ports the switch has x 240 MB
Disk space required for ISM as a whole	Total disk space for managed switches



Note

Switch ports are monitored even if they are not used.

For information on switches that support the display of network statistics, refer to "Support Matrix."

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

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

Select [DOWNLOADS] and select the target operating system.

The reference procedures are subject to change without notice.

The following shows an estimation for monitoring the network statistics information.

- Monitoring switch: PSWITCH 2048 T/PSWITCH 2048 P (x 10 switches)
- For one port, 20 MB is required per month and 240 MB is required per year
- Number of ports for one monitoring switch: 54 ports
- Disk space required for ISM as a whole

$\text{<Disk space for each port>} \times \text{<Number of ports on the switch>} \times \text{<Number of switches>}$
--

= 240 x 54 x 10

= 129600 MB

= 129.6 GB

For information on the network statistics information, refer to "2.7 Network Management."

3.2.1.4 Estimation of the required disk space for ISM RAS log

Change the ISM RAS log levels and estimate the required disk space depending on the number of nodes to be managed in ISM-VA.

The following table shows the number of managed nodes and required diskspace for the log area.

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 "4.5.2.2 Switching the ISM RAS Log level."

3.2.1.5 Estimation of required disk space for maintenance data

Change the ISM RAS log levels and estimate the required disk space depending on the number of nodes to be managed in ISM-VA.

The following table shows the number of managed nodes and required diskspace 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 "[4.5.2.2 Switching the ISM RAS Log level.](#)"

3.2.1.6 Estimation of required disk space for ISM Backup/Restore

Estimate the disk space required for ISM Backup/Restore depending on the number of nodes to be managed in ISM-VA.

The following table shows the number of managed nodes and required diskspace 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

When monitoring settings of the network statistic information is enabled

When monitoring the network statistic information, requires additional capacity estimates.

For the information about disk space for network statistics, refer to "[3.2.1.3 Estimation of the required disk space for node management data.](#)"

3.2.1.7 Estimation of required disk space for CSV export of Sustainability Monitor

Estimate the disk space required for CSV export per session depending on the number of monitored nodes for Sustainability Monitor to be managed in ISM-VA.

The following table shows the number of monitored nodes and required disk space (per session) for CSV export for Sustainability Monitor.

Number of monitored nodes	Required disk capacity	Temporary required disk capacity
100 nodes or less	125 MB	205 MB
400 nodes or less	490 MB	810 MB
1000 nodes or less	1.3 GB	2.1 GB



Note

When CSV export is executed for multiple sessions, the disk space is required according to the number of sessions.

3.2.2 Network Design

ISM uses the following two types of management LAN to manage servers.

Connect the network used in ISM to the following 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.

In addition, network connections are required for managing switches and storage devices. These can be either divided into physical and logical connections or used as one single integrated connection.



Note

ISM-VA starts by default while the IP address "192.168.1.101" remains enabled. Make sure not to overlap with the IP addresses of the other devices within the network.

You can avoid overlapping IP addresses by following the procedure below to change an IP address 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. Back up (export) ISM-VA with a hypervisor
4. Restore (import) ISM-VA that was backed up (exported) with the hypervisor in the actual environment.



Point

- It is recommended that you prepare separate networks for service use (production LANs) in addition to 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 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.
- Multiple ISM network interfaces cannot be defined due to physical network interface redundancy.

Configure physical network interface redundancy using bonding or teaming on the hypervisor running ISM-VA.

3.2.3 Node Name Design

Determine naming rules for nodes and profiles that will be required for node registration.

When you register a node, give it a unique name.

A maximum of 64 characters can be used to set the node name.

Note, however, that you cannot use the following characters:

slashes (/), backslashes (\), colons (:), asterisks (*), question marks (?), double quotations ("), angle brackets (<>), or pipelines (|)

3.2.4 User Design

Set 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. In this case, create a user with an Administrator role within the user group.

For details on user groups and users, refer to "[2.14.1 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 must 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 Infrastructure Manager.

Install ISM-VA according to the installation destination.



Note

Be sure to back up ISM-VA after the installation of ISM-VA on which you are going to restore backup files of the ISM. ISM-VA backup should be backed up (export) on the hypervisor where ISM is running.

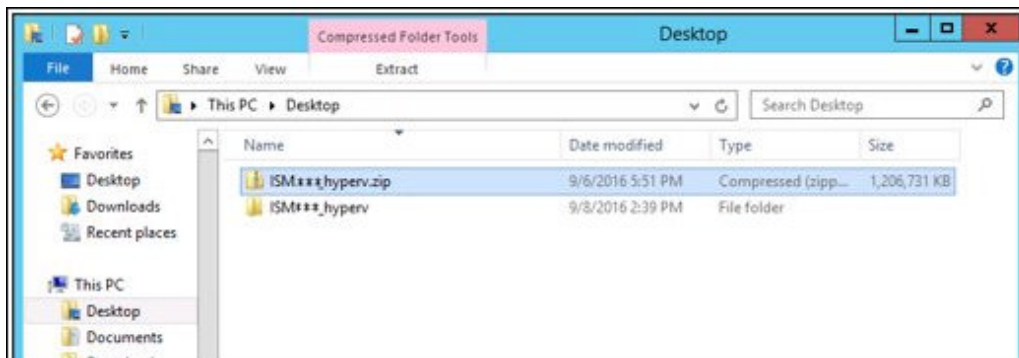
The following procedures describe how to install ISM-VA on Microsoft Windows Server Hyper-V, VMware vSphere Hypervisor, and KVM.

- [3.3.1 Installation on Microsoft Windows Server Hyper-V](#)
- [3.3.2 Installation on VMware vSphere Hypervisor](#)
- [3.3.3 Installation on KVM](#)

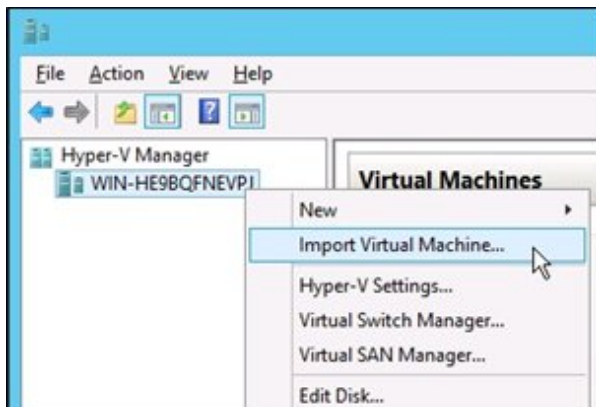
3.3.1 Installation on Microsoft Windows Server Hyper-V

For installation, use the ISM-VA image-compressed file (ISM<Version>_hyperv.zip) that is included on the DVD media. For details on selecting installation destinations and network adapters that are to be specified midway through installation, refer to the Hyper-V manuals.

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

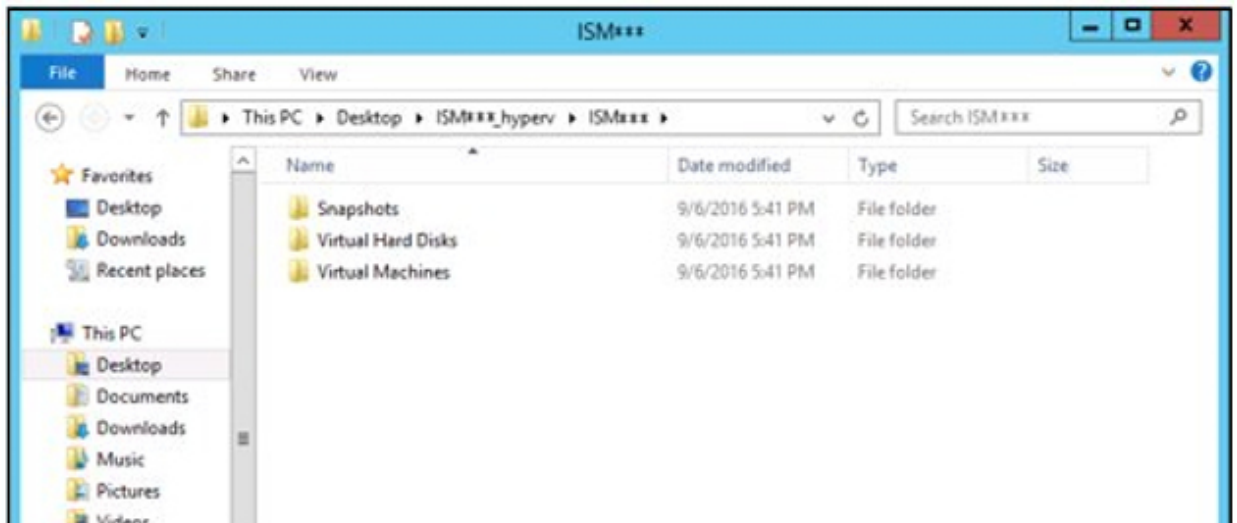


2. Start Hyper-V Manager, right-click on the Windows server to be used as the Hyper-V host, and then select [Import Virtual Machine].

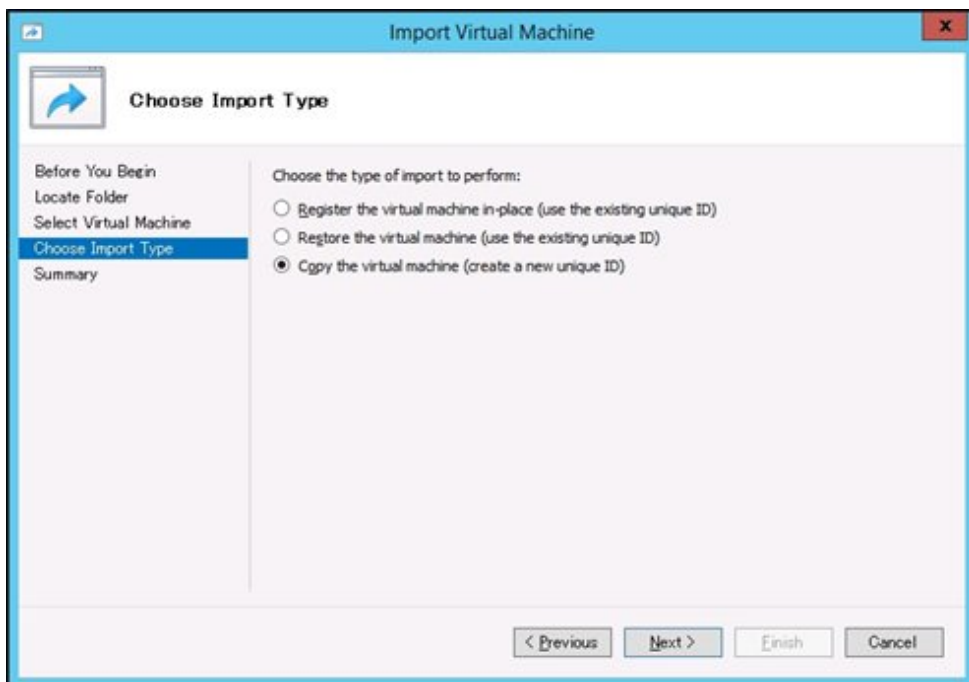


3. On the "Select Folder" screen, select the directory in which you deployed the file in Step 1.

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

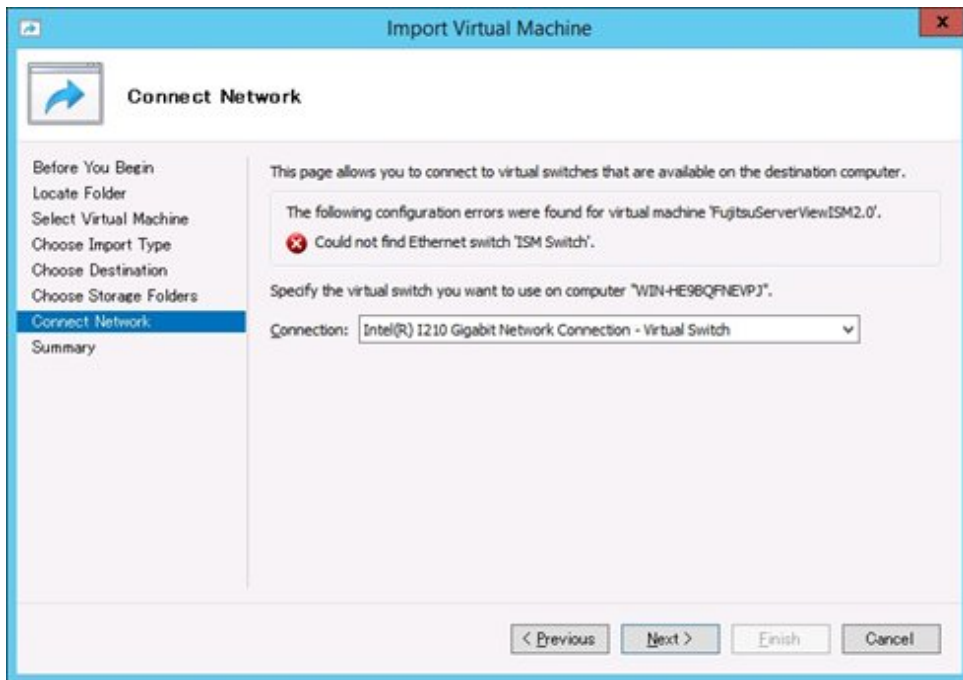


4. On the "Choose Import Type" screen, select [Copy the virtual machine (create a new unique ID)], and then select [Next].



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.
9. Upgrade the ISM-VA virtual machine configuration version to the latest version supported with the imported Windows server. For details on how to upgrade the configuration version, refer the Hyper-V manuals.

3.3.2 Installation on VMware vSphere Hypervisor

For installation, use the ISM-VA definition files (ISM<Version>.ovf) and ISM-VA image files (ISM<Version>-disk1.vmdk) that are included in the DVD media.

The ovf file to be used differs depending on whether you install VMware ESXi directly or install with VMware vCenter.

- Direct installation on VMware ESXi

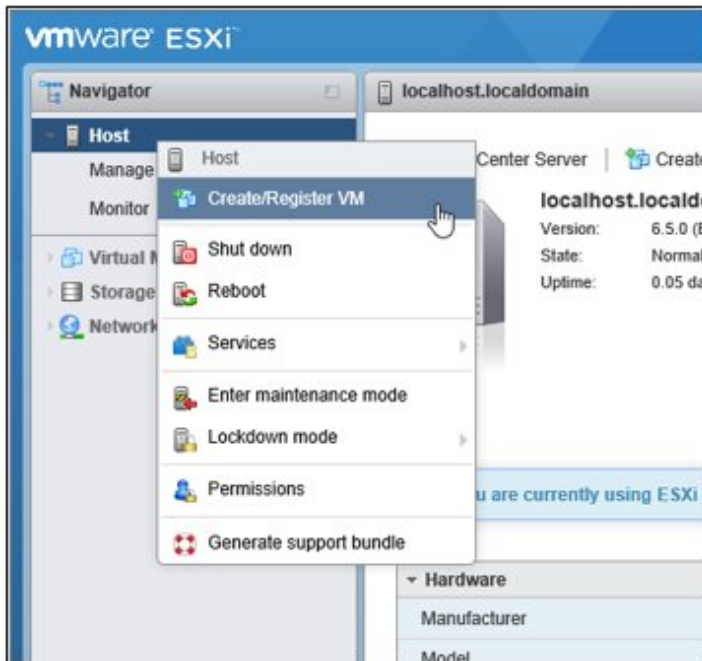
Use ISM<Version>.ovf.

- Installation via VMware vCenter

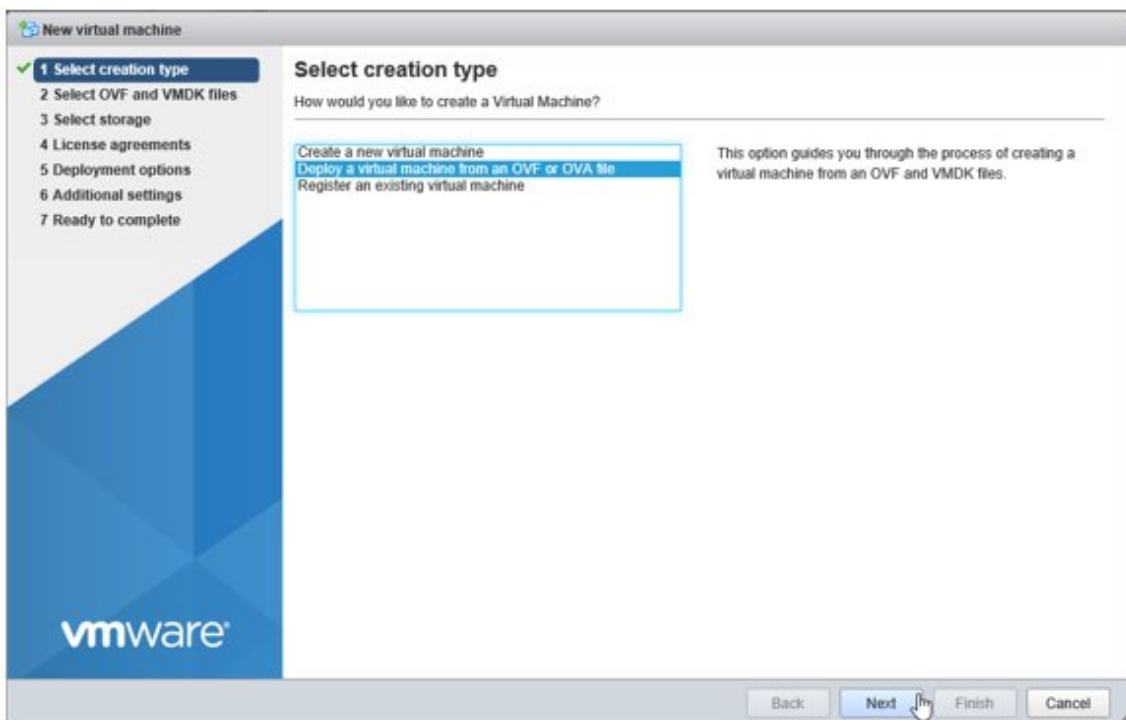
User ISM<Version>_vcenter.ovf.

If you install ISM-VA via VMware vCenter, you can execute network settings for ISM-VA during the installation.

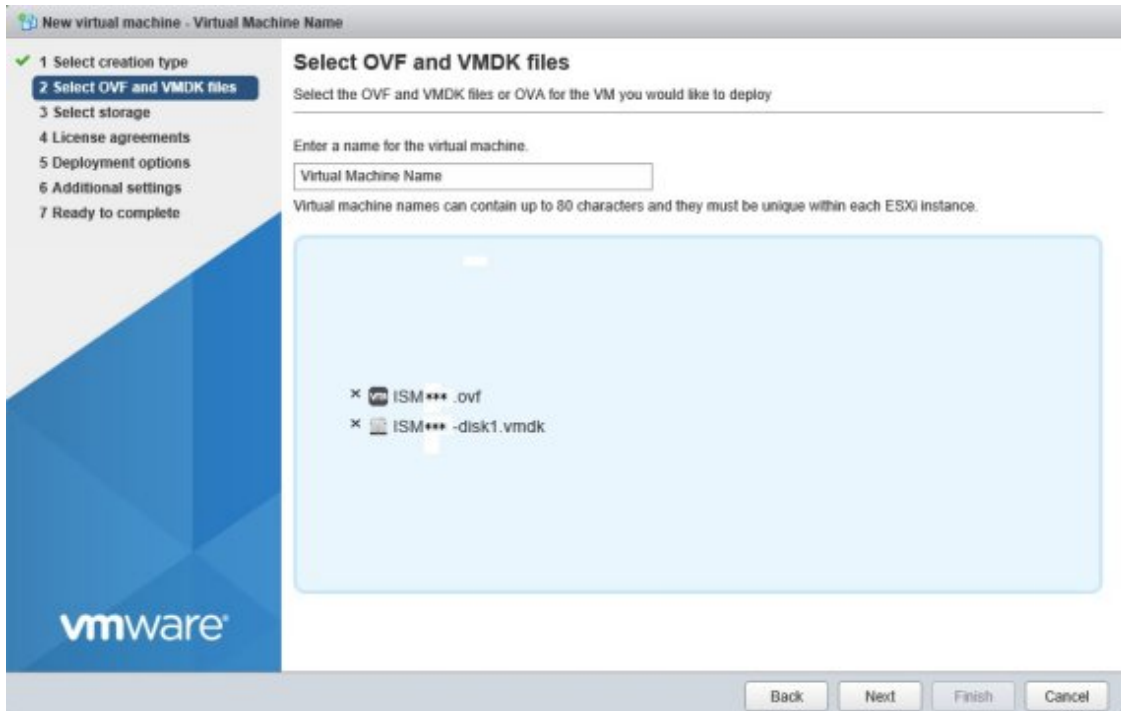
1. Start the vSphere Client (HTML5), right-click on the [Host] of the navigator, and then select [Create/Register VM].



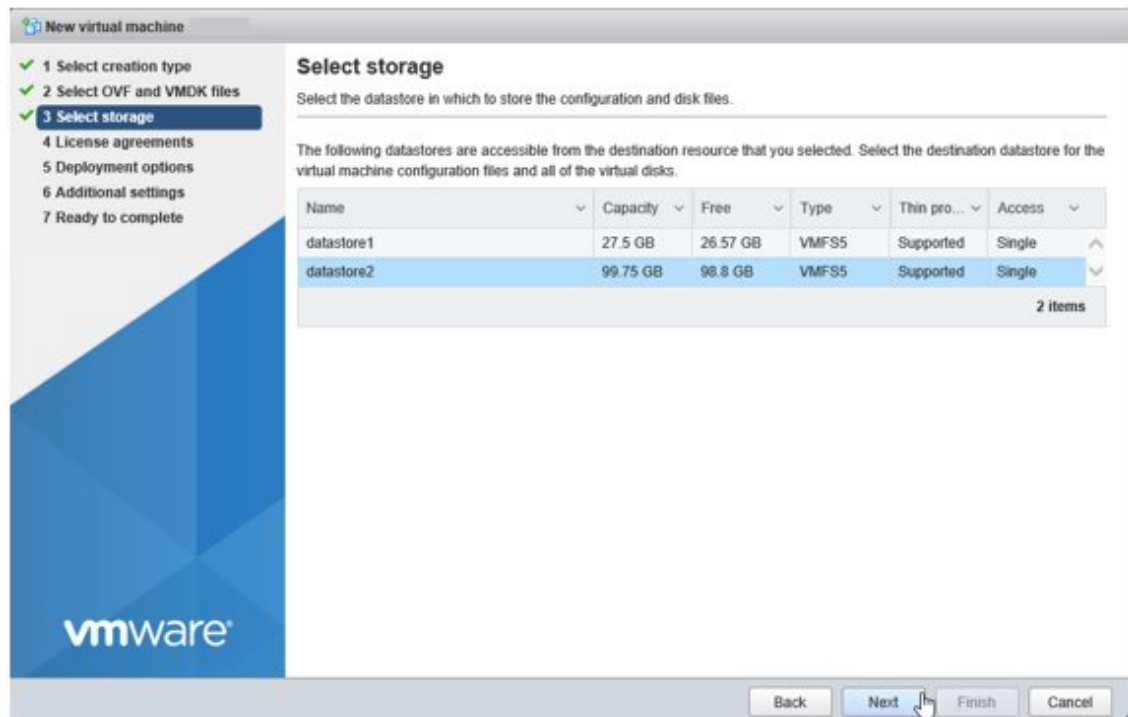
2. On the "Select creation type" screen, select [Deploy a virtual machine from an OVF or OVA file], and then select [Next].



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



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



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

New virtual machine

1 Select creation type
2 Select OVF and VMDK files
3 Select storage
4 Deployment options
5 Ready to complete

Deployment options

Select deployment options

Network mappings	LocalLan VM Network
Disk provisioning	<input type="radio"/> Thin <input checked="" type="radio"/> Thick

Back Next Finish Cancel

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

New virtual machine

1 Select creation type
2 Select OVF and VMDK files
3 Select storage
4 Deployment options
5 Ready to complete

Ready to complete

Review your settings selection before finishing the wizard

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

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

Back Next Finish Cancel

Point

If you set a network item while deploying the OVF file (OVF templates), it will take 10 to 15 minutes for ISM-VA (virtual machine) to start from the initial power on. Check the network items that were set by using the `ismsetup` or `ismadm` command 10 to 15 minutes after the initial power on. If the setting is not correct, wait a few minutes and check again.

Table 3.1 List of network setting items

Item	Description
01 IP Address	An ISM-VA IP address
02 Netmask	Subnet mask or prefix length (Example: 255.255.255.0 or 24)
03 Gateway	Default gateway
04 Hostname	ISM-VA host name (You must specify the FQDN if using DNS)
05 Primary DNS	Primary DNS (optional setting)
06 Secondary DNS	Secondary DNS (optional setting)

3.3.3 Installation on KVM

For installation, use the ISM-VA image-compressed file (ISM<Version>_kvm.tar.gz) that is included in the DVD media.

- [For Red Hat Enterprise Linux or SUSE Linux Enterprise Server](#)
- [For Nutanix AHV](#)

For Red Hat Enterprise Linux or SUSE Linux Enterprise Server

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/RedHat7/ISM<Version>.xml
ISM<Version>_kvm/RedHat8/ISM<Version>.xml
ISM<Version>_kvm/RedHat9/ISM<Version>.xml
ISM<Version>_kvm/SLES12/ISM<Version>.xml
ISM<Version>_kvm/SLES15/ISM<Version>.xml
```

The <Version> part shows the number according to the 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.

Use the xml file that corresponds to the KVM host you are installing.

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



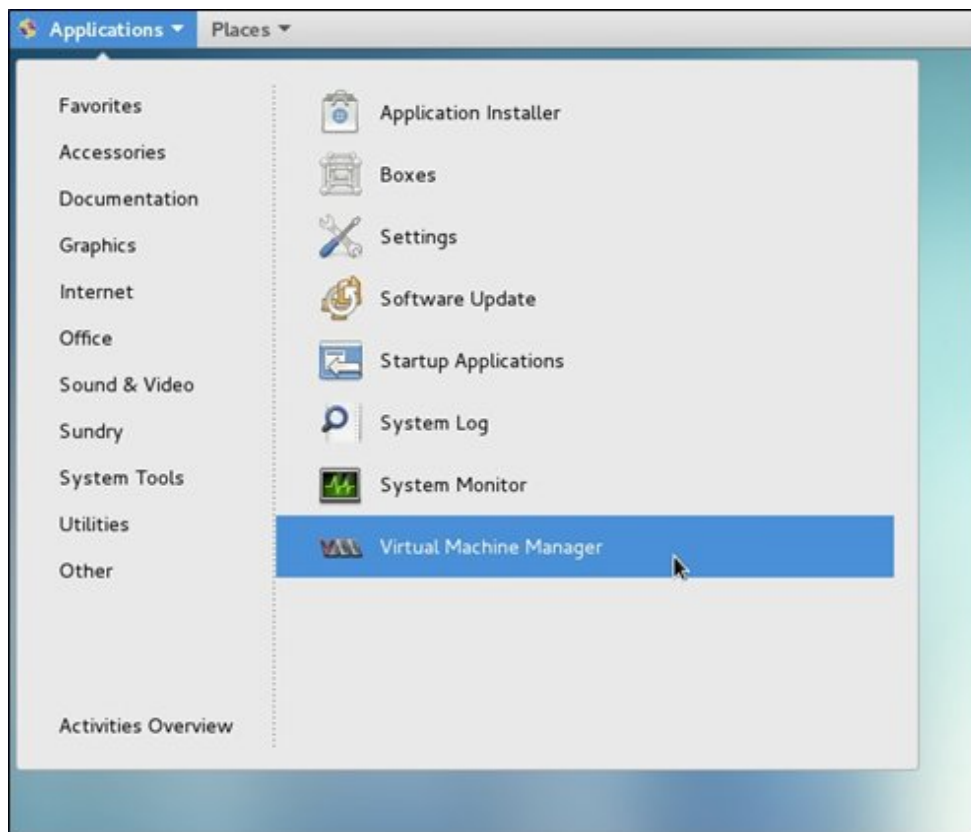
If you use more than one ISM-VA on the same network, use the KVM host virsh command to edit the xml file and change the MAC address.

Refer to the hypervisor documentation for information on changing the MAC address.

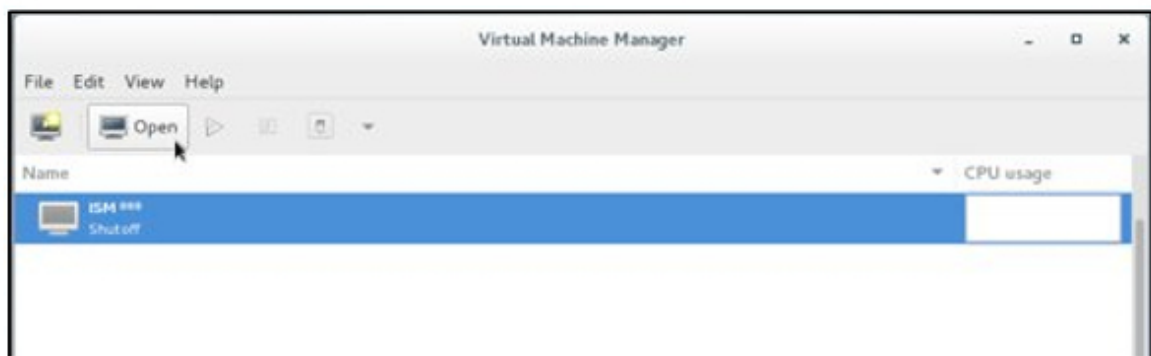
3. Specify the xml file to register ISM-VA.

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

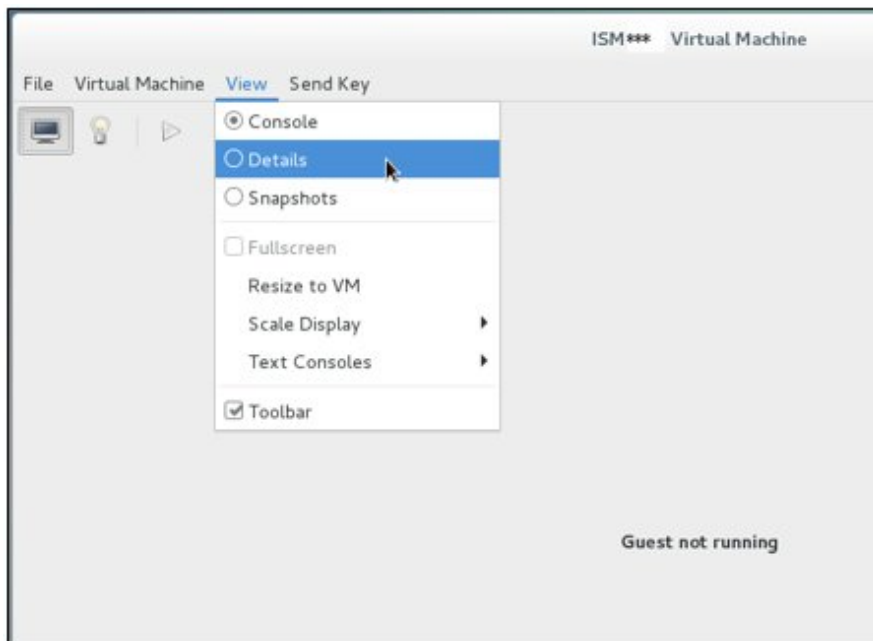
4. Select [Virtual Machine Manager] to open Virtual Machine Manager.



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.



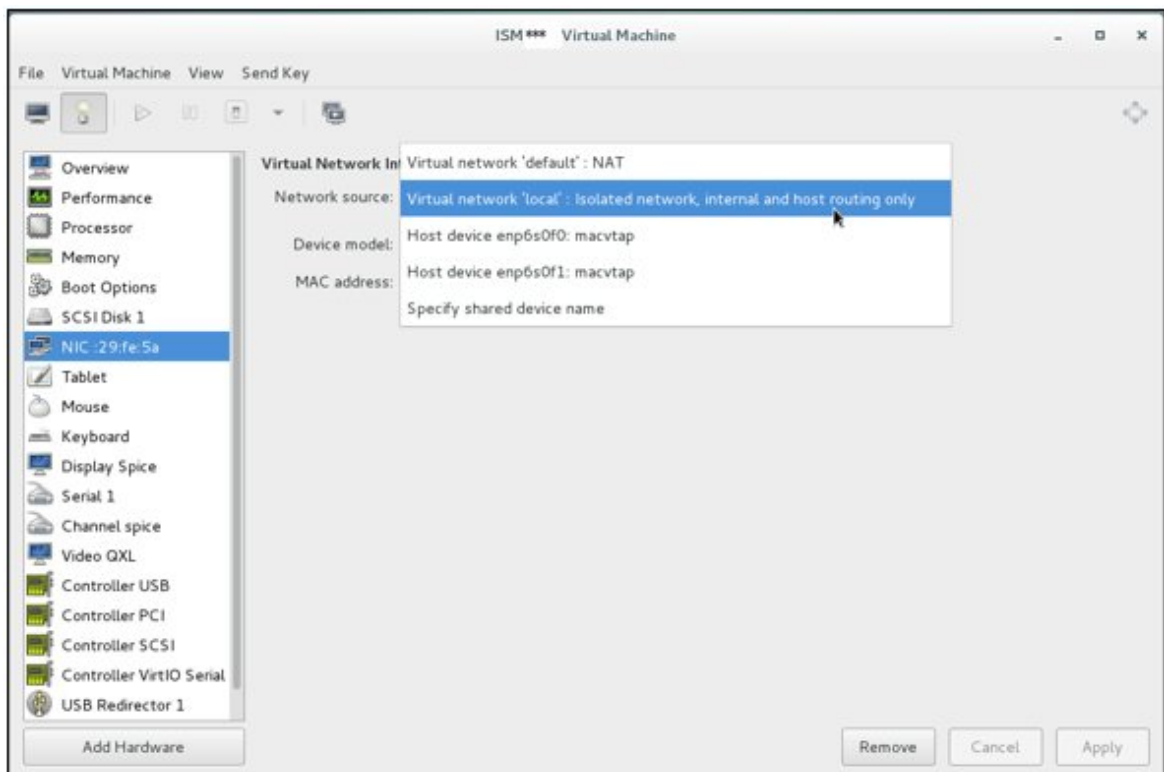
7. On the details screen for ISM-VA Virtual Machine, select [NIC], and select the network source which to connect ISM-VA, and then select [Apply].

Select the network source that can be externally connected to the ISM-VA virtual machine.

On Virtual Machine Manager, the network sources that can be externally connected are displayed as "Bridge Device" and "Macvtap Device". Select one of these to set up the network device.

For details, refer to the documentation for Red Hat Enterprise Server or SUSE Linux Enterprise Server. The name of the network source and how to configure it may differ depending on the version of the OS you are installing.

For the model of virtual network device, select "virtio."



- When using Auto Discovery of Nodes, UDP multicast must reach the ISM-VA virtual machine, so that execute the following command on the OS being installed:

```
# ip link set dev <device name>allmulticast on
```

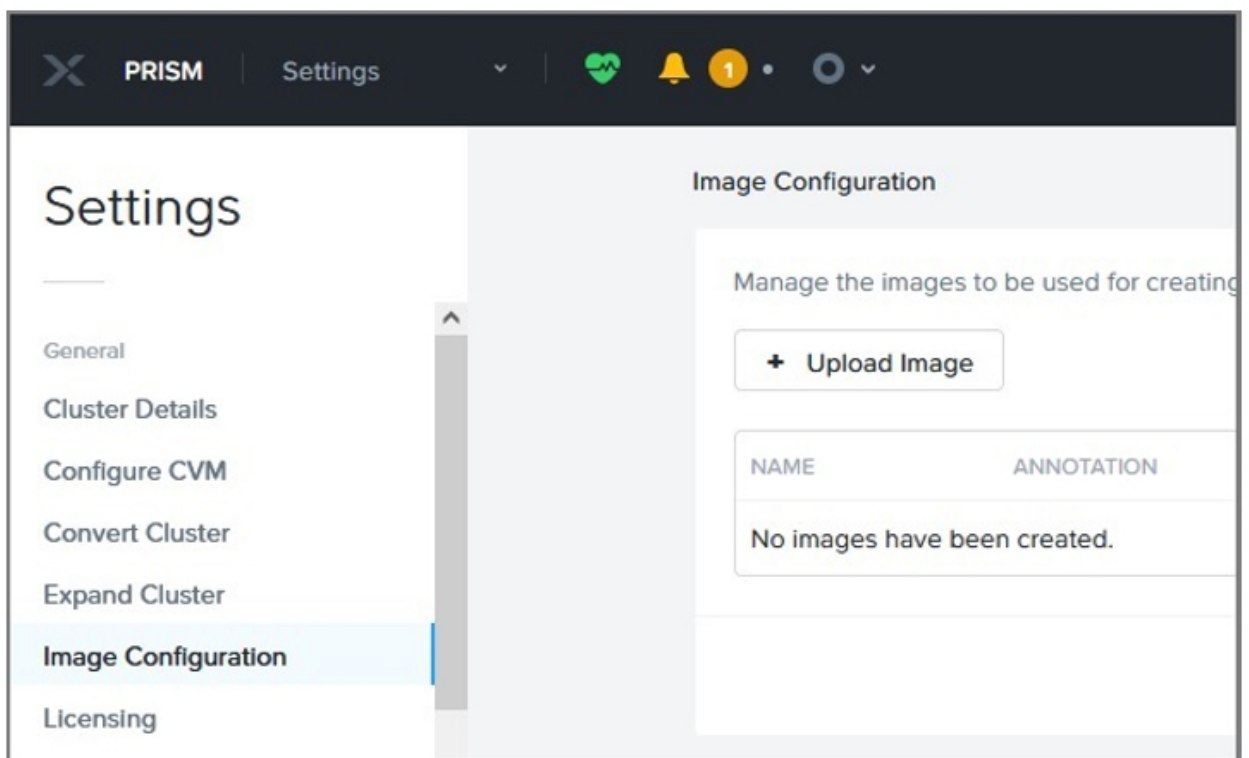
For <device name>, specify the device name specified in Step 7.

Example:

```
# ip link set dev eno1 allmulticast on
```

For Nutanix AHV

- In any directory on the management terminal, decompress the file with the qcow2 extension from the tar.gz file.
You need a tool that can decompress a tar.gz archive on the management terminal.
- In Nutanix PRISM, select the [Settings] menu - [Image Configuration].



3. Select the [Upload Image] button to upload the qcow2 file.

The screenshot shows a web form for uploading an image. It contains the following fields and controls:

- Name:** A text input field containing "ISM-VA Image".
- Annotation:** An empty text input field.
- Image Type:** A dropdown menu with "DISK" selected.
- Storage Container:** An empty dropdown menu.
- Image Source:** Two radio buttons. "From URL" is unselected, and "Upload a file" is selected. To the right of "Upload a file" is a "Choose File" button and the filename "ISM***_kvm.qcow2".
- Navigation:** At the bottom left is a "< Back" button. At the bottom right are "Cancel" and "Save" buttons.

Set the following parameters when uploading. Select the [Save] button.

- Name: Enter a name (Example: ISM-VA Image)
- Annotation: Enter a comment
- Image Type: Select [DISK]
- Storage Container: Select a container to store the ISM-VA virtual disk images
- Image Source: Select [Upload a file] and specify the qcow2 file decompressed in Step 1

4. In Nutanix PRISM, select the [VM] menu - [Create VM] to create a virtual machine for ISM-VA.

Create VM

General Configuration

Name
ISM2xx

Description
Optional

Timezone
(UTC) UTC

☐ Use this VM as an agent VM

Compute Details

vCPU(s)
2

Number Of Cores Per vCPU
1

Cancel Save

The ISM-VA virtual machine is created by setting the following parameters and then selecting the [Save] button.

- General Configuration
 - Name: Enter a virtual machine name (Example: ISM + [ISM version])
 - Description: Enter a comment
 - Timezone: Select a timezone
 - Use this VM as an agent VM: Do not select
- Compute Details
 - vCPU(s): Enter the number of vCPUs according to the number of nodes to be managed and the function to be used (2 vCPU minimum)
 - Number Of Cores Per vCPU: Enter 1

- Memory: Enter the amount of memory according to the number of nodes to be managed and the function to be used (16 GB minimum)
- For information on the values to set for [vCPU (s)] and [Memory], refer to "[1.3.1 Requirements for Hypervisor to Run ISM-VA \(Virtual Machines\)](#)."
- Disks
 - CD-ROM: Select [x] to delete
 - Select [Add New Disk] to add a DISK for use with ISM-VA

When adding parameters, specify the following.

Item	Description
Type	Select [DISK]
Operation	Select [Clone from Image Service]
Bus Type	Select [SCSI]
Image	Specify the ISM-VA image uploaded in Step 3
Size (GiB)	Unchangeable
Index	Select [Next Available]

- Boot Configuration
 - Select [Legacy BIOS]
 - Set Boot Priority: Select [DISK (scsi.0)]
- Network Adapters (NIC)

Select [Add New NIC] to add a Network to connect to ISM-VA.

When adding parameters, specify the following.

Item	Description
Network Name	Specify the name of the network to connect to
Network Connection State	Select [Connected]

- VM Host Affinity

Select [Set Affinity] and select at least one node on which to run ISM-VA.
- Custom Script

Do not select

3.4 Environment Settings for ISM-VA

Execute the initial setup after installing ISM-VA.

3.4.1 First Start of ISM-VA

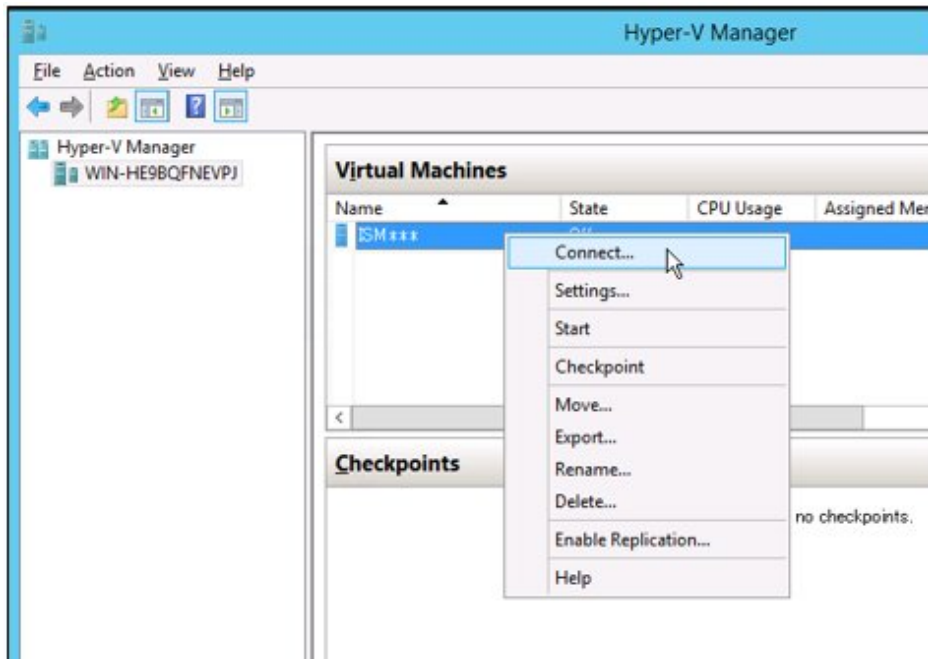
Use the respective function of the hypervisor on the installation destination to start ISM-VA. Start ISM-VA as a host OS user with administrator privileges.

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

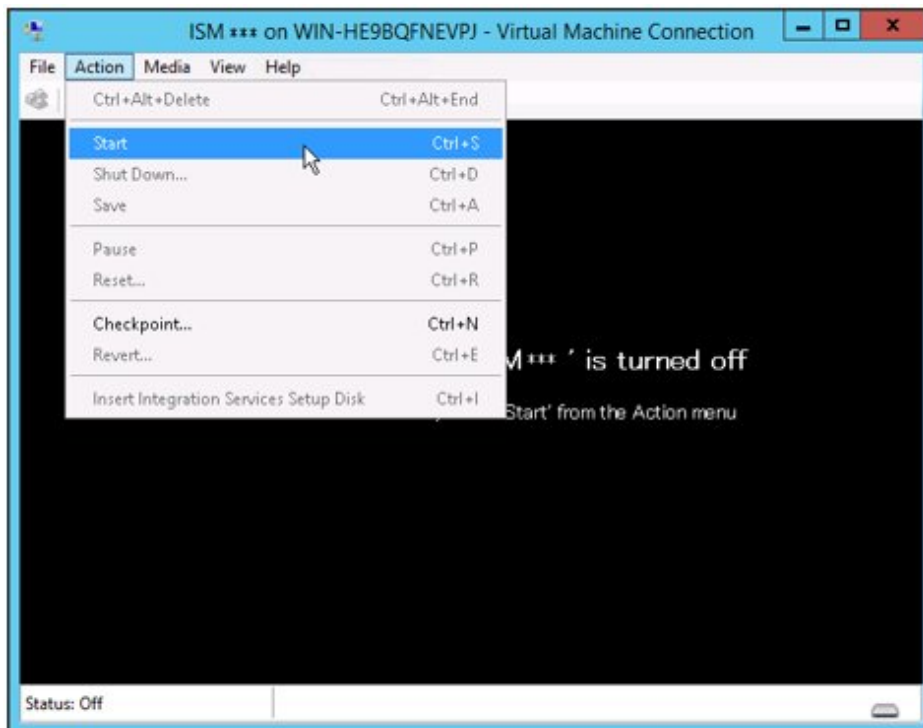
- [3.4.1.1 For ISM-VA running on Microsoft Windows Server Hyper-V \(First Time\)](#)
- [3.4.1.2 For ISM-VA running on VMware vSphere Hypervisor \(First Time\)](#)
- [3.4.1.3 For ISM-VA running on KVM \(First Time\)](#)

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].

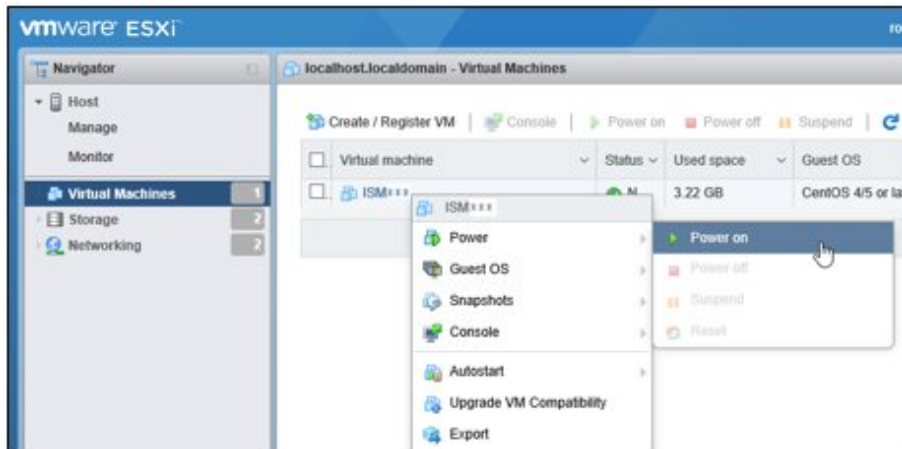


2. On the "Virtual Machine Connection" screen, select [Start] from the [Action] menu to start ISM-VA.

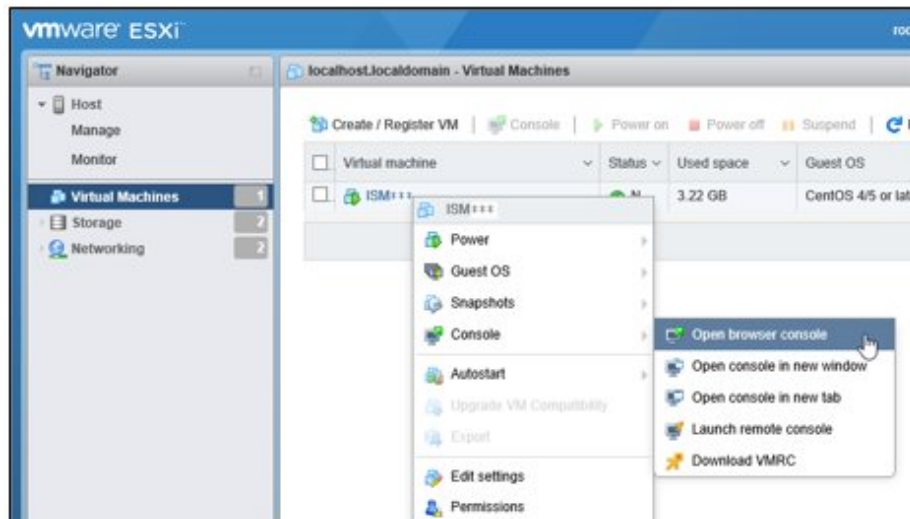


3.4.1.2 For ISM-VA running on VMware vSphere Hypervisor (First Time)

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 another console.



Point

The following message may be displayed when starting ISM-VA, but the ISM-VA settings are optimized to operate on VMware ESXi 6.5/6.7, and so this is not a problem.

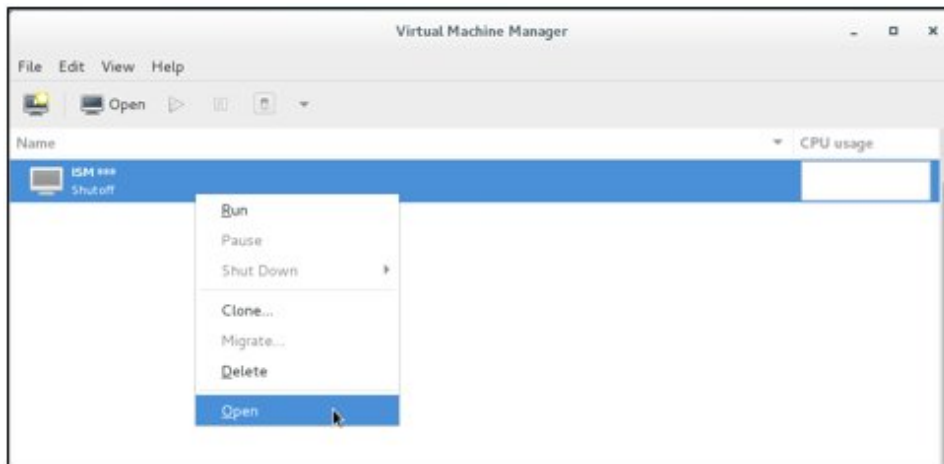
The configured guest OS (CentOS 4/5 or later (64-bit)) for this virtual machine does not match the guest that is currently running (CentOS 7 (64-bit)). You should specify the correct guest OS to allow for guest-specific optimizations.

3.4.1.3 For ISM-VA running on KVM (First Time)

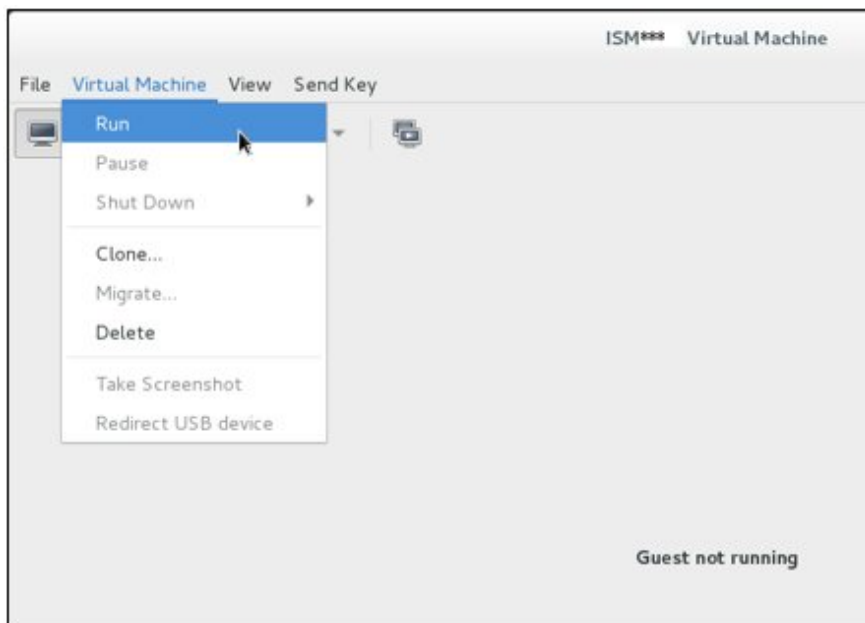
- [For Red Hat Enterprise Linux or SUSE Linux Enterprise Server](#)
- [For Nutanix AHV](#)

For Red Hat Enterprise Linux or SUSE Linux Enterprise Server

1. In Virtual Machine Manager, right-click on the installed ISM-VA, and then select [Open].

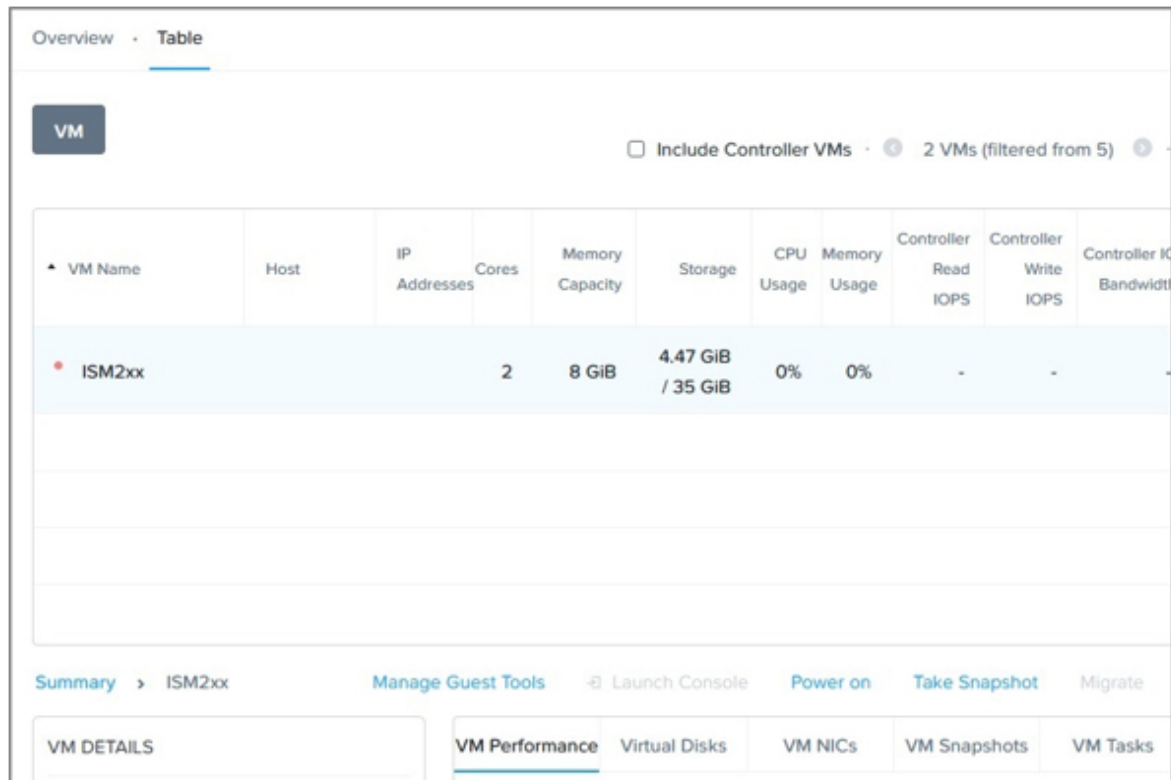


2. On the "ISM-VA Virtual Machine" screen, select [Run] from the [Virtual Machine] menu to start ISM-VA.



For Nutanix AHV

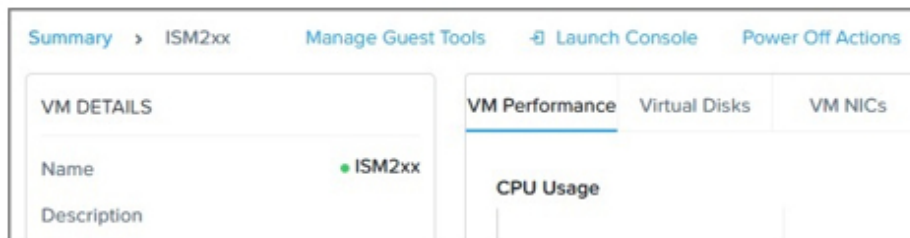
1. In Nutanix PRISM, select the [Table] on the [VM] screen.



The screenshot shows the Nutanix PRISM interface for VM management. At the top, there are tabs for 'Overview' and 'Table', with 'Table' selected. Below the tabs is a 'VM' button and a filter section that includes 'Include Controller VMs' (unchecked) and '2 VMs (filtered from 5)'. The main area contains a table with the following columns: VM Name, Host, IP Addresses, Cores, Memory Capacity, Storage, CPU Usage, Memory Usage, Controller Read IOPS, Controller Write IOPS, and Controller IO Bandwidth. The table has one row for a VM named 'ISM2xx' with 2 Cores, 8 GiB Memory Capacity, 4.47 GiB / 35 GiB Storage, 0% CPU Usage, 0% Memory Usage, and - for both Controller Read and Write IOPS. Below the table, there are buttons for 'Summary', 'Manage Guest Tools', 'Launch Console', 'Power on', 'Take Snapshot', and 'Migrate'. At the bottom, there are tabs for 'VM DETAILS', 'VM Performance', 'Virtual Disks', 'VM NICs', 'VM Snapshots', and 'VM Tasks', with 'VM Performance' selected.

VM Name	Host	IP Addresses	Cores	Memory Capacity	Storage	CPU Usage	Memory Usage	Controller Read IOPS	Controller Write IOPS	Controller IO Bandwidth
ISM2xx			2	8 GiB	4.47 GiB / 35 GiB	0%	0%	-	-	

2. Select the ISM-VA virtual machine and select [Power on].
3. Select [Launch Console] to open the ISM-VA console.



The screenshot shows the Nutanix PRISM interface for VM management. At the top, there are tabs for 'Summary', 'Manage Guest Tools', 'Launch Console', and 'Power Off Actions', with 'Summary' selected. Below the tabs is a 'VM DETAILS' section with a green dot next to 'ISM2xx'. The 'VM DETAILS' section has fields for 'Name' and 'Description'. To the right of the 'VM DETAILS' section are tabs for 'VM Performance', 'Virtual Disks', and 'VM NICs', with 'VM Performance' selected. The 'VM Performance' section has a 'CPU Usage' field.

VM DETAILS	VM Performance	Virtual Disks	VM NICs
Name: ISM2xx	CPU Usage		

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 settings for ISM-VA.

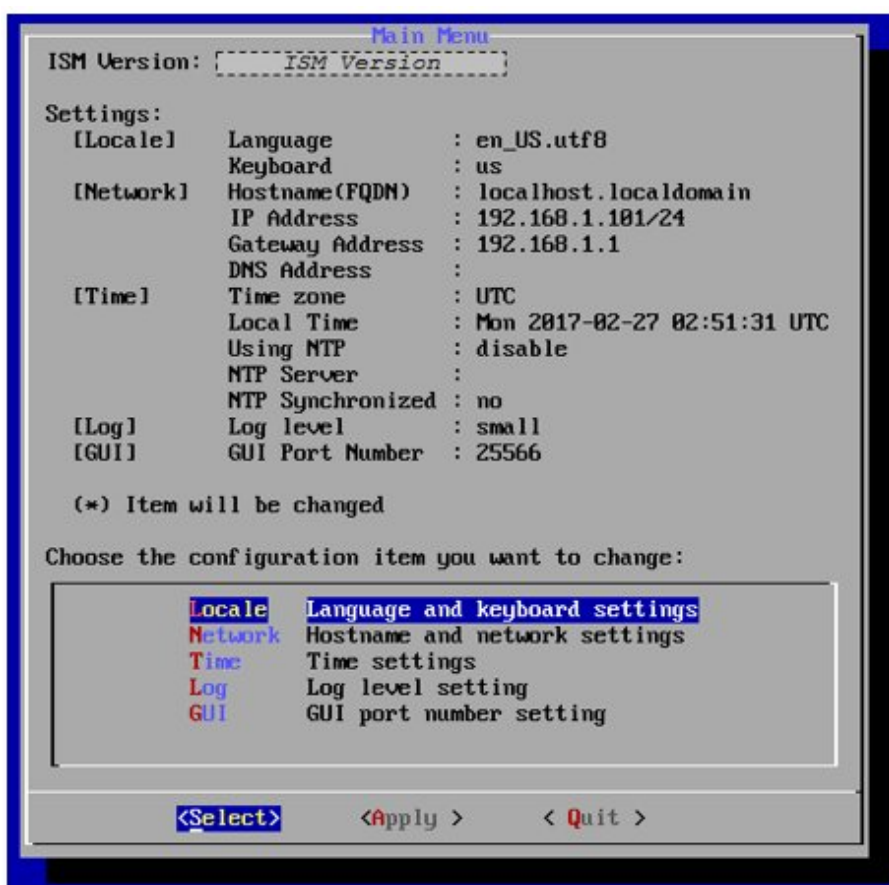
3.4.2.1 Initial setup using the Basic Setting Menu

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 first time you log in from the hypervisor console, the menu is displayed automatically.

The screen below is displayed.



3. Execute the ISM-VA settings.

The following items can be set on the basic setting menu:

- 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 networks and host names

```
# 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.

Operations after executing the network/host name settings can be operated in the same way from both the hypervisor console as well as another console via SSH. However, access via SSH is recommended as it provides good operability.

Point

If you install VMware vSphere Hypervisor version ISM-VA via VMware vCenter, you can omit this network setting by executing the network setting during the installation.

Note

- Characters that can be used as a host name are lowercase letters, numbers, hyphens (-), and periods (.). Hyphens and periods are not allowed as leading or trailing characters in host names. If characters other than those allowed are used, ISM will not work properly.
- IPv4 addresses must be set for the IP address.

IPv6 is not supported. ISM functions such as Profile Management and Firmware Management do not operate if IPv6 addresses are set.

1. 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 3.2 Keymap list

Language	Keymap Name
Japanese	jp
English	us
German	de-nodeadkeys
Chinese	cn
Korean	kr
Filipino	ph

Any modifications to System Locale become effective only after restarting ISM-VA.

2. 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>
```

3. 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
```

- Undoing the latest change to the domain setting information

```
# ismadm kerberos restore
```

You cannot undo two or more changes.

- Initialization of domain setting information

```
# ismadm kerberos init
```

3.5 Registration of Licenses

There are following two types of licenses:

- 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.

ISM requires the registration of both server licenses and node licenses. Register the licenses with ISM-VA Management after installing ISM-VA.

The following two procedures can be used for registering licenses:

- [3.5.1 Procedure to Register Licenses from the Console](#)
- [3.5.2 Procedure to Register Licenses on the ISM GUI](#)

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

3.5.1 Procedure to Register Licenses from the Console

To register licenses, from the console, log in to ISM-VA as an administrator.

1. Register the server licenses.

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

2. Register the node licenses.

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

3. Confirm the results of license registration.

```
# ismadm license show
```

Example of command execution:

```
# ismadm license show
Operation Mode : Advanced
#   [Type]  [Edition] [#Node]  [Reg.Date]  [Exp.Date]  [Status]      [Licensekey]
1   Server  Adv.        -   2024-05-29  2025-05-29  Valid         *****==
2   Node    Adv.        10  2023-08-28  2024-08-27  Expires soon  *****==
3   Node    Adv.        10  2023-05-30  2024-05-29  Expired       *****==

*Reg.Date(RegistrationDate[yyyy-mm-dd])
*Exp.Date(ExpirationDate[yyyy-mm-dd])

You have an expired license.
Delete the expired license and register a new license.
```

For details on the command output, refer to "[4.8 License Settings](#)."

4. Restart ISM-VA.

```
# ismadm power restart
```

3.5.2 Procedure to Register Licenses on the ISM GUI

Implement "[3.4.2 Initial Setup of ISM-VA](#)" in advance.

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

The "Fujitsu End User Software License Agreement" screen is displayed.
4. Check the contents, and then select the [Above contents are correct.] checkbox.
5. Select the [Agree] button.
6. From the Global Navigation Menu on the ISM GUI, select [Settings] - [General].
7. From the menu on the left side of the screen, select [License].
8. From the [Actions] button, select [Register].

The "Register License" screen is displayed.

9. 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 to register all licenses, and then select the [Apply] button.
10. From the [Actions] button, select [Restart ISM-VA] to restart ISM-VA.



- To register additional licenses, repeat Step 6 to 9 above.
- To delete the licenses registered, select the target licenses, and from the [Actions] button, select [Delete].

3.6 Registration of Users

Register the users required in order to operate ISM under "3.2.4 User Design."

For detailed procedures, refer to "2.3 Configure ISM Users" in "Operating Procedures."



In the default settings of ISM, only one user (ISM administrator) with an [Administrator Role] in [Administrator Groups] is registered.

User Name	Password	User Group Name	User Role	Usage
administrator	admin [Note]	Administrator	Administrator	Management of all users/all user groups and the security policy

[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.
 - a. From the Global Navigation Menu on the ISM GUI, select [Settings] - [Users].
 - b. From the menu on the left side of the screen, select [Node Groups].
 - c. From the [Actions] button, select [Add Node Group].
3. Register the nodes that belong to each node group. (You can also register more nodes later.)
 - a. From the Global Navigation Menu on the ISM GUI, select [Management] - [Node Groups].
 - b. Select the node group from the Node Group List on the left side of the screen.
 - c. Select a node on the right side of the screen, then select [Assign to Node Group] from the [Node Actions] button.
 - d. On the "Assign to Node Group" screen, select the [Select] button.
 - e. On the "Select Node Group" screen, select the [<Node group to which to assign a new>], and then select the [Select] button.
 - f. On the "Assign to Node Group" screen, select the [Apply] button.
4. Create one or more user groups.
 - a. From the Global Navigation Menu on the ISM GUI, select [Settings] - [Users].
 - b. From the menu on the left side of the screen, select [User Groups].
 - c. From the [Actions] button, select [Add].

5. Register the users that belong to each user group.
 - a. From the Global Navigation Menu on the ISM GUI, select [Settings] - [Users].
 - b. From the menu on the left side of the screen, select [Users].
 - c. From the [Actions] button, select [Add].

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. In addition, these capacities vary with the respective operating procedures and scales of managed nodes. Allocating large-volume 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 ISM-VA or to user groups.

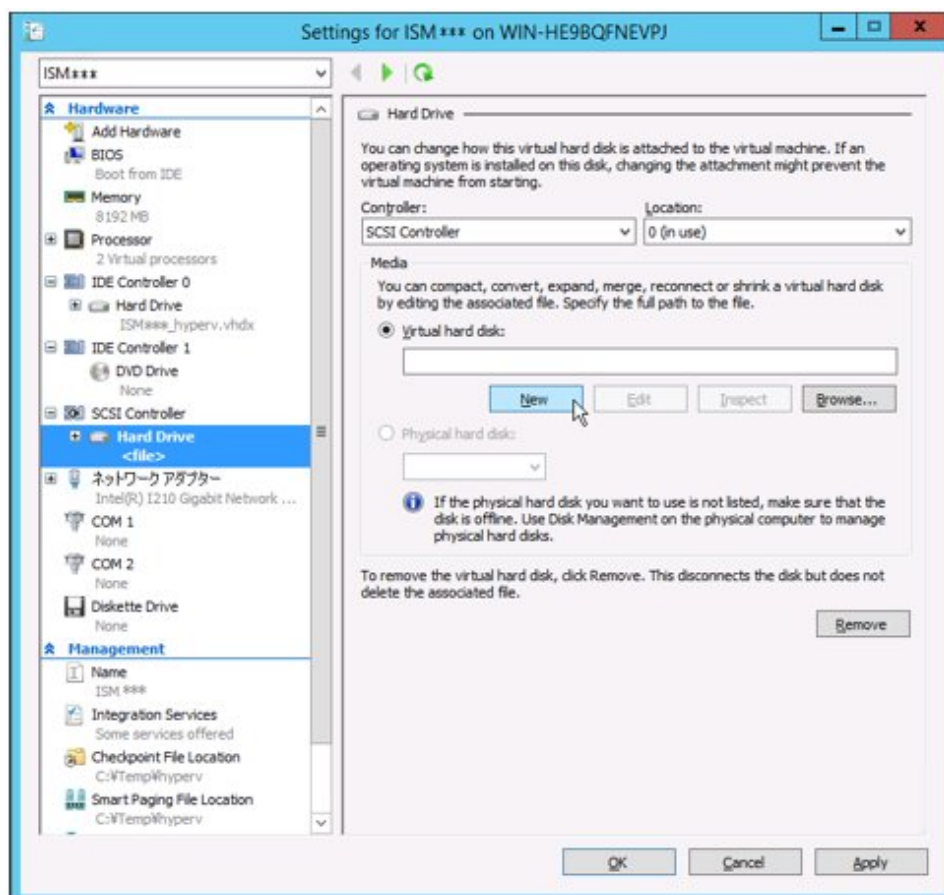
3.7.1 Allocation of Virtual Disks to ISM-VA

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

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

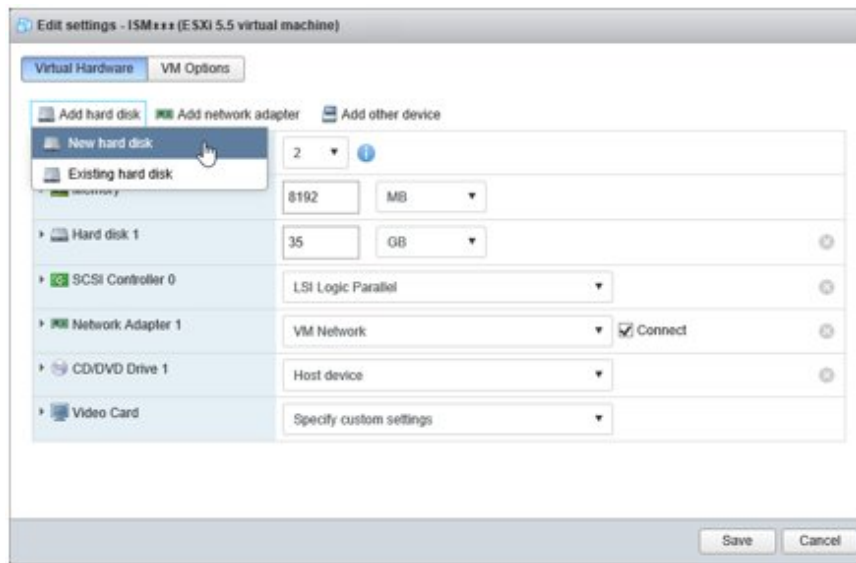
- For Microsoft Windows Server Hyper-V

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



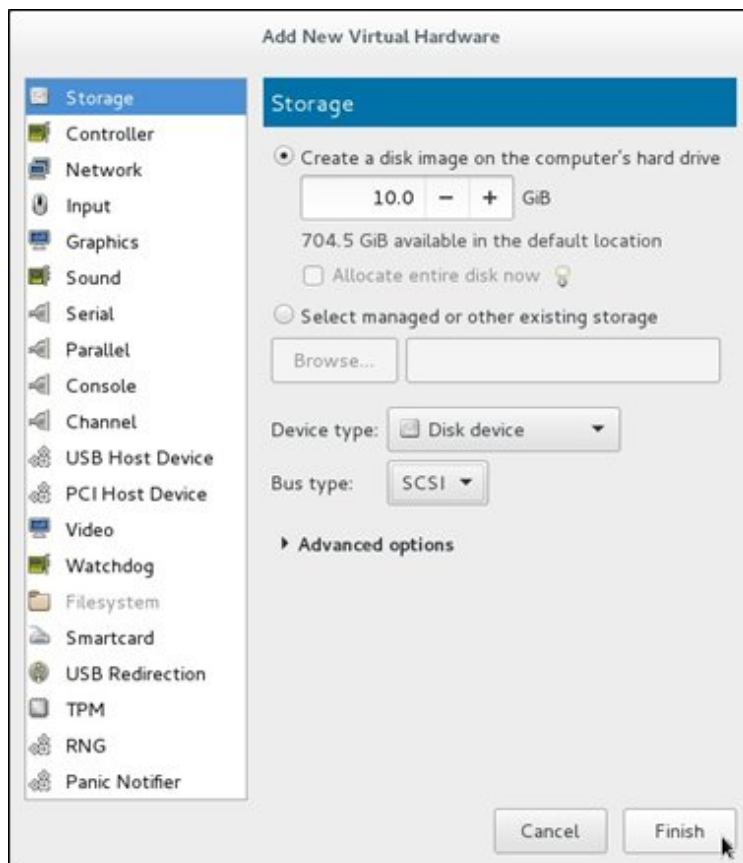
- For VMware vSphere Hypervisor 6.5 or later

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



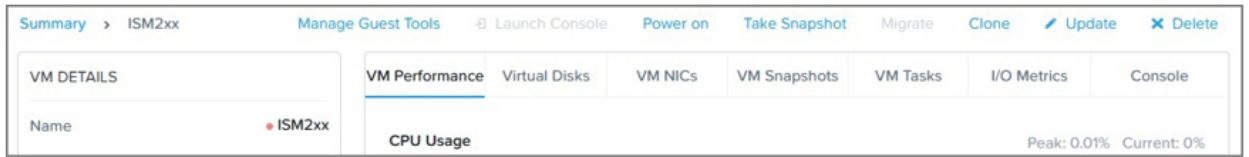
- For KVM (Red Hat Enterprise Linux or SUSE Linux Enterprise Server)

For Bus type, select SCSI.



- For Nutanix AHV

Select [Update] for the virtual machine and add the virtual disk from [Add New Disk].



Add Disk
?
X

Type

DISK

Operation

Allocate on Storage Container

Bus Type

SCSI

Storage Container

NTNX-Container

Size (GiB) ?

10

Index

Next Available

Cancel

Add

For Bus type, select SCSI.

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

```
# 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 10.7 GB)

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 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
```

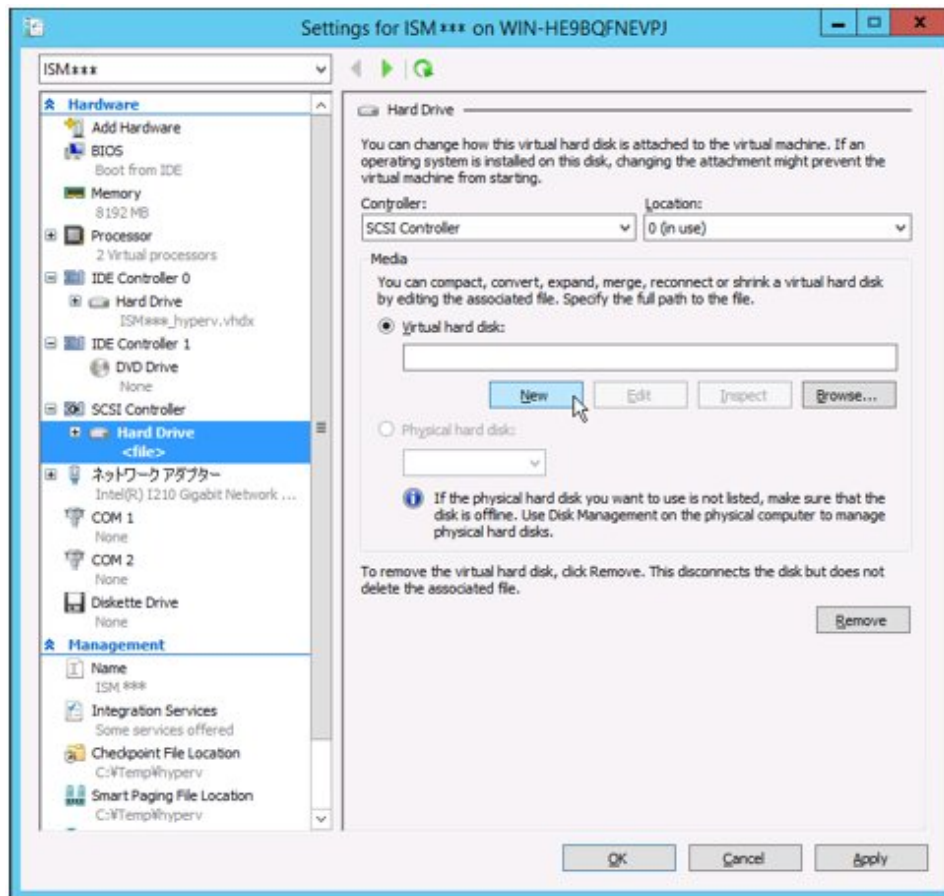
3.7.2 Allocation of Virtual Disks to User Groups

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

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

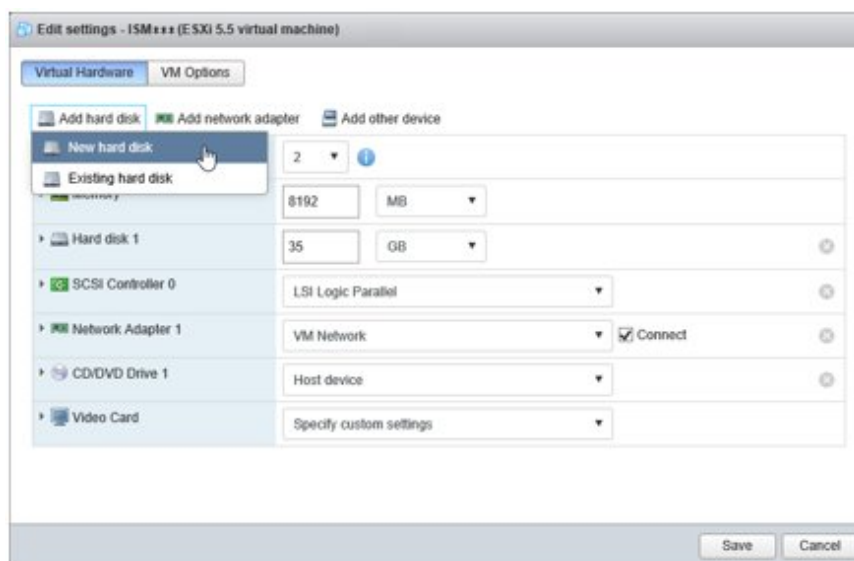
- For Microsoft Windows Server Hyper-V

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

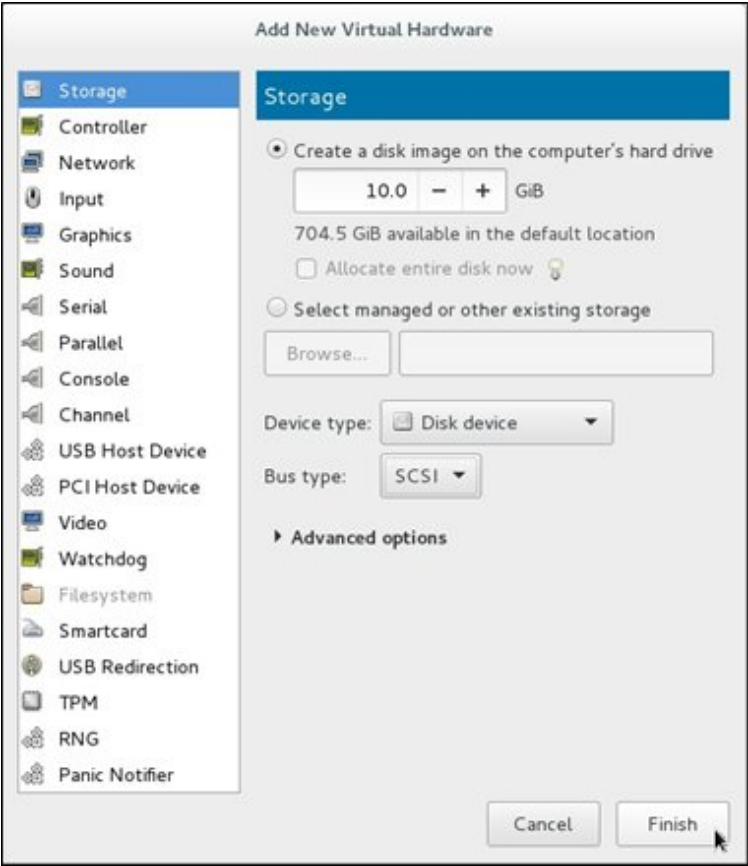


- For VMware vSphere Hypervisor 6.5 or later

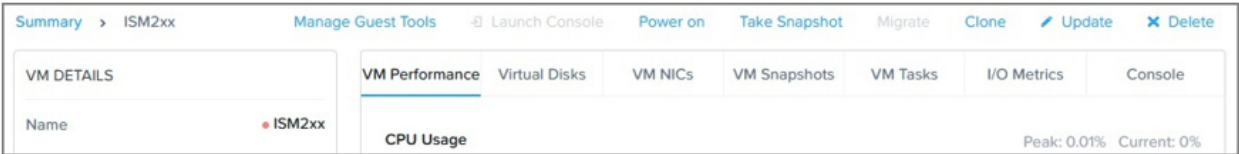
In the virtual device node selection that comes up on the "Detail Option" screen during disk creation, select SCSI.



- For KVM (Red Hat Enterprise Linux or SUSE Linux Enterprise Server)
For Bus type, select SCSI.



- For Nutanix AHV
Select [Update] for the virtual machine and add the virtual disk from [Add New Disk].



Add Disk
?
X

Type
DISK

Operation
Allocate on Storage Container

Bus Type
SCSI

Storage Container
NTNX-Container

Size (GiB) ?
10

Index
Next Available

Cancel
Add

For Bus type, select SCSI.

- After starting ISM-VA, from the console, log in to ISM-VA as an administrator.
- Stop the ISM service temporarily in order to allocate virtual disks.

```
# ismadm service stop ism
```

- 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 8589 MB)
```

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 Managing Virtual Resources/Clusters

This section describes the settings required in advance for operation management of Virtual Resource Management and Cluster Management.

3.8.1 Pre-Settings for vSAN

A vSAN alarm must be specified to detect a datastore error when the network connection between the vSAN hosts become disconnected. In addition, vSAN Monitoring must be enabled to provide latency monitoring for the disks that make up vSAN.

3.8.1.1 Addition of vSAN alarm definitions

The following procedure describes how to add vSAN alarm definitions.

For vCenter Server Appliance 6.5, select "vSphere Client (HTML5) - partial functionality" and log in.

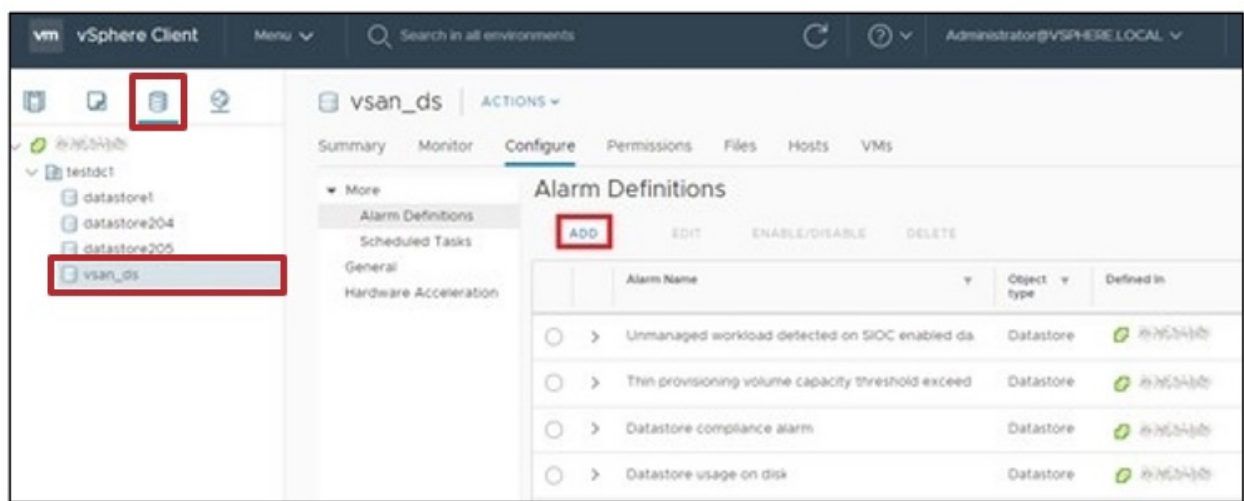
1. Display the vSphere Client screen, select [Storage] from menu, and then select the created vSAN datastore.

The following example is for the settings when a name of the vSAN datastore is "vsan_ds."

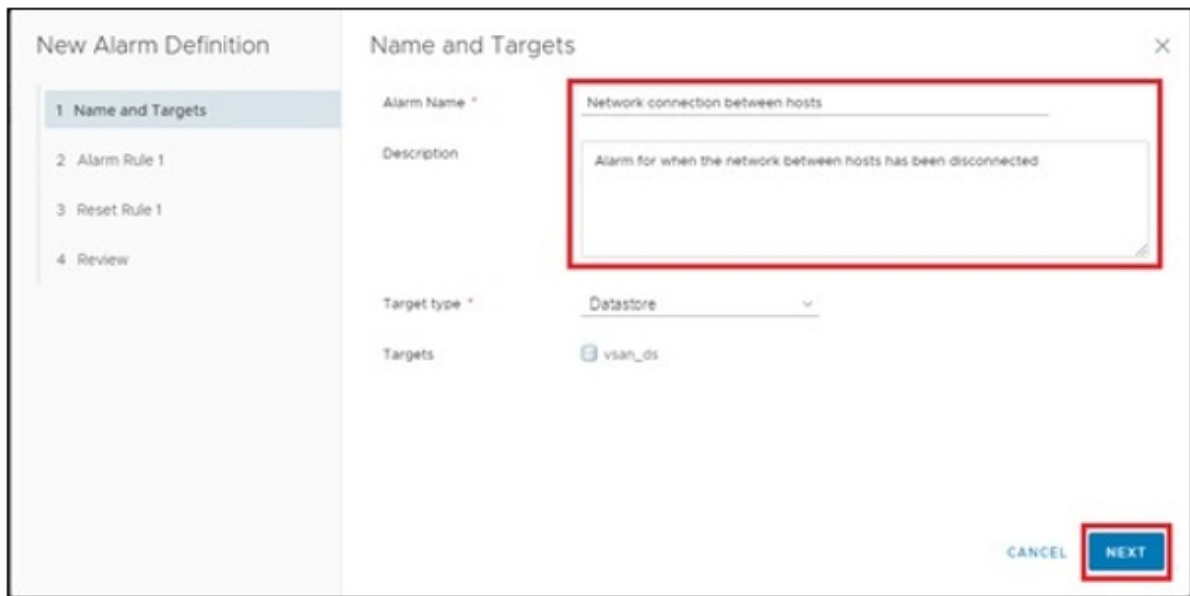
From the [Configure] tab on the right side of the displayed screen, select [More] - [Alarm Definitions].

Confirm "Alarm Name" on the displayed screen. If "Breaking of a network between the host" exists in "Alarm Name", no further steps are required.

Select [ADD] on the displayed screen.



2. When the wizard screen is displayed, enter "Alarm Name" and "Description" according to the following table, and then select the [NEXT] button.



Item	Entered contents
Alarm Name	Network disconnection between hosts
Description	Alarm for when the network between hosts is disconnected

3. Set each item in the following screen as shown in the table below. Then, select the [NEXT] button.

The screenshot shows the 'New Alarm Definition' window with the 'Alarm Rule 1' tab selected. The 'IF' condition is configured as 'Datastore State to All Hosts' is equal to 'Disconnected'. The 'THEN' action is 'Trigger the alarm and *' set to 'Show as Critical'. There are buttons for 'ADD ANOTHER RULE', 'DUPLICATE RULE', and 'REMOVE RULE'. At the bottom are 'CANCEL', 'BACK', and 'NEXT' buttons.

Item	Parameter
Trigger	Datastore State to All Hosts
Operator	is equal to
Option	Disconnected
Severity of the alarm	Show as Critical

4. Reset Rule 1 is not required to be set. Select the [NEXT] button.

The screenshot shows the 'New Alarm Definition' window with the 'Reset Rule 1' tab selected. The 'IF' condition is 'The warning or critical conditions/states are no longer met'. The 'THEN' action is 'Reset the alarm to *' set to 'Normal'. There are buttons for 'SEND EMAIL NOTIFICATIONS', 'SEND SNMP TRAPS', and 'RUN SCRIPT'. At the bottom are 'CANCEL', 'BACK', and 'NEXT' buttons.

5. Select the [CREATE] button on the following screen.

New Alarm Definition

1 Name and Targets
2 Alarm Rule 1
3 Reset Rule 1
4 **Review**

Review

Alarm Name: Network connection between hosts

Description: Alarm for when the network between hosts has been disconnected

Targets: vsan_ds

Alarm Rules: IF Datastore State to All Hosts is equal to Disconnected
THEN Trigger the alarm as Critical

Reset Rules: IF the warning or critical conditions/states are no longer met
THEN Trigger the alarm as Normal

Enable this alarm: ☒

CANCEL BACK **CREATE**

The new definition is added to the alarm definitions when completed.

vsan_ds ACTIONS

Summary Monitor **Configure** Permissions Files Hosts VMs

More

- Alarm Definitions
- Scheduled Tasks
- General
- Hardware Acceleration

Alarm Definitions

ADD EDIT ENABLE/DISABLE DELETE

Alarm Name	Object Type	Defined In
<input checked="" type="radio"/> Network connection between hosts	Datastore	vsan_ds
<input type="radio"/> Unmanaged workload detected on SIOC enabled da	Datastore	vsan_ds
<input type="radio"/> Thin provisioning volume capacity threshold exceed	Datastore	vsan_ds
<input type="radio"/> Datastore compliance alarm	Datastore	vsan_ds
<input type="radio"/> Datastore usage on disk	Datastore	vsan_ds
<input type="radio"/> VASA provider disconnected	Datastore	vsan_ds
<input type="radio"/> VASA provider certificate expiration alarm	Datastore	vsan_ds
<input type="radio"/> Object type storage alarm	Datastore	vsan_ds

3.8.1.2 Procedure to enable vSAN Monitoring

This section describes how to enable vSAN Monitoring. The procedure is different depending on the version of VMware vCenter Server Appliance. Refer to the appropriate version.

- For vCenter Server Appliance 6.5 (Flash) and earlier
- For vCenter Server Appliance 6.7 (HTML 5) or later

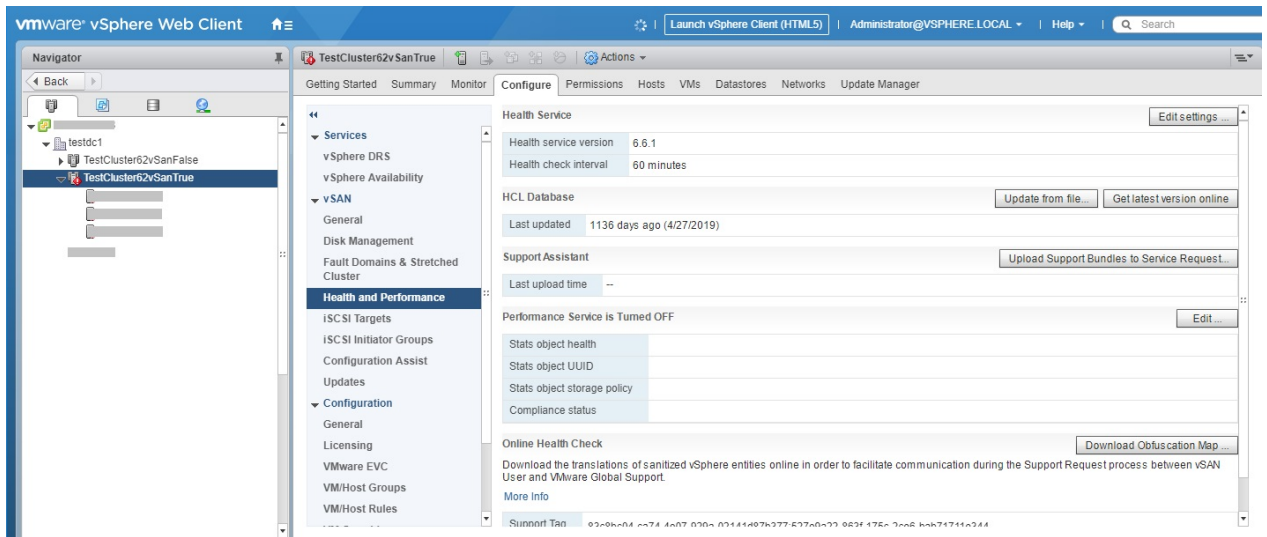
For vCenter Server Appliance 6.5 (Flash) and earlier

1. Display the vSphere Web Client screen, and from the menu select [Host and Clusters], select the created cluster.
2. From the [Configure] tab on the right side of the screen, select [vSAN] - [Health and Performance].

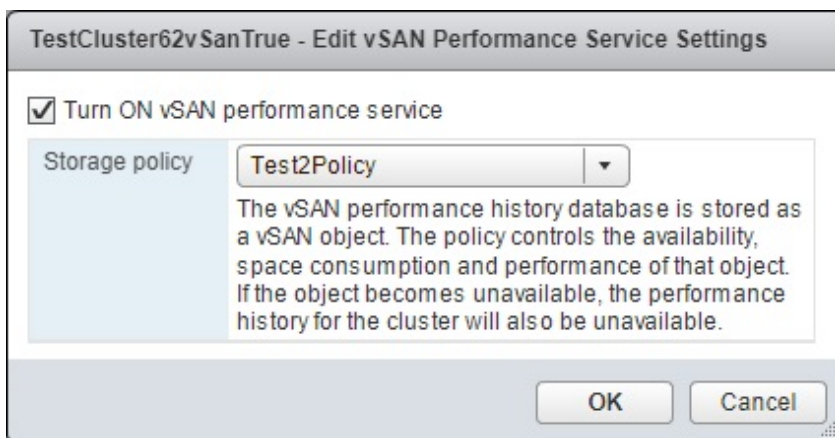
Check "Performance Service." If it is "Performance Service is Turned OFF," perform the following procedures to turn it "ON."

If it is "ON," the following procedures are not required.

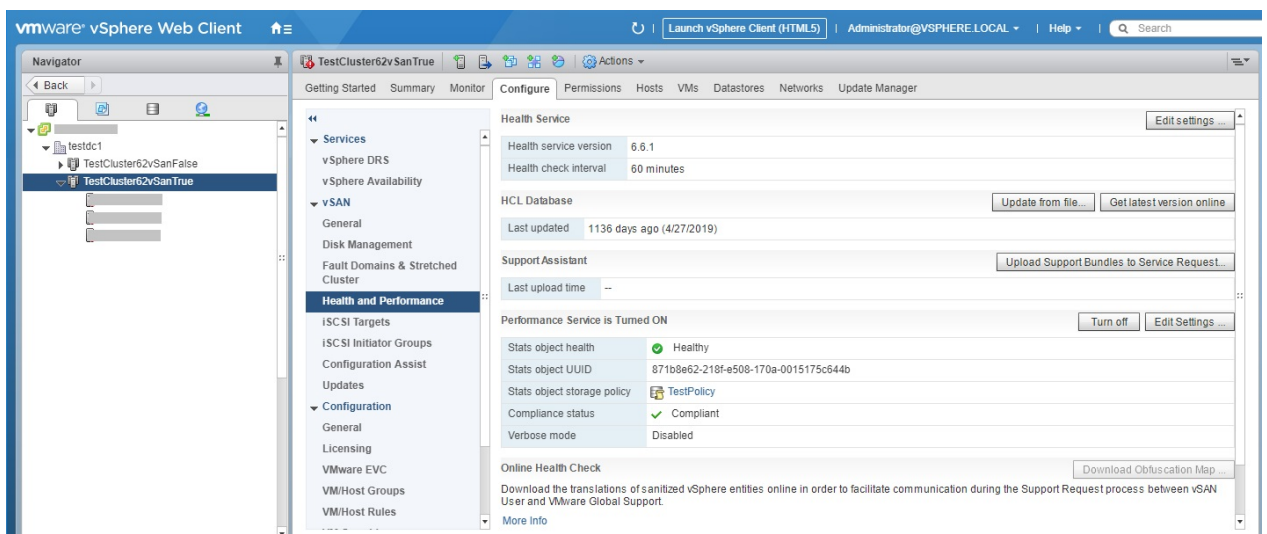
Select [Edit] to the right of the status.



3. Select the "Turn ON vSAN performance service" checkbox, select the storage policy, and then select the [OK] button.



Performance service is "Performance Service is Turned ON" when completed.



4. Apply this similar procedure to all clusters configuring vSAN.

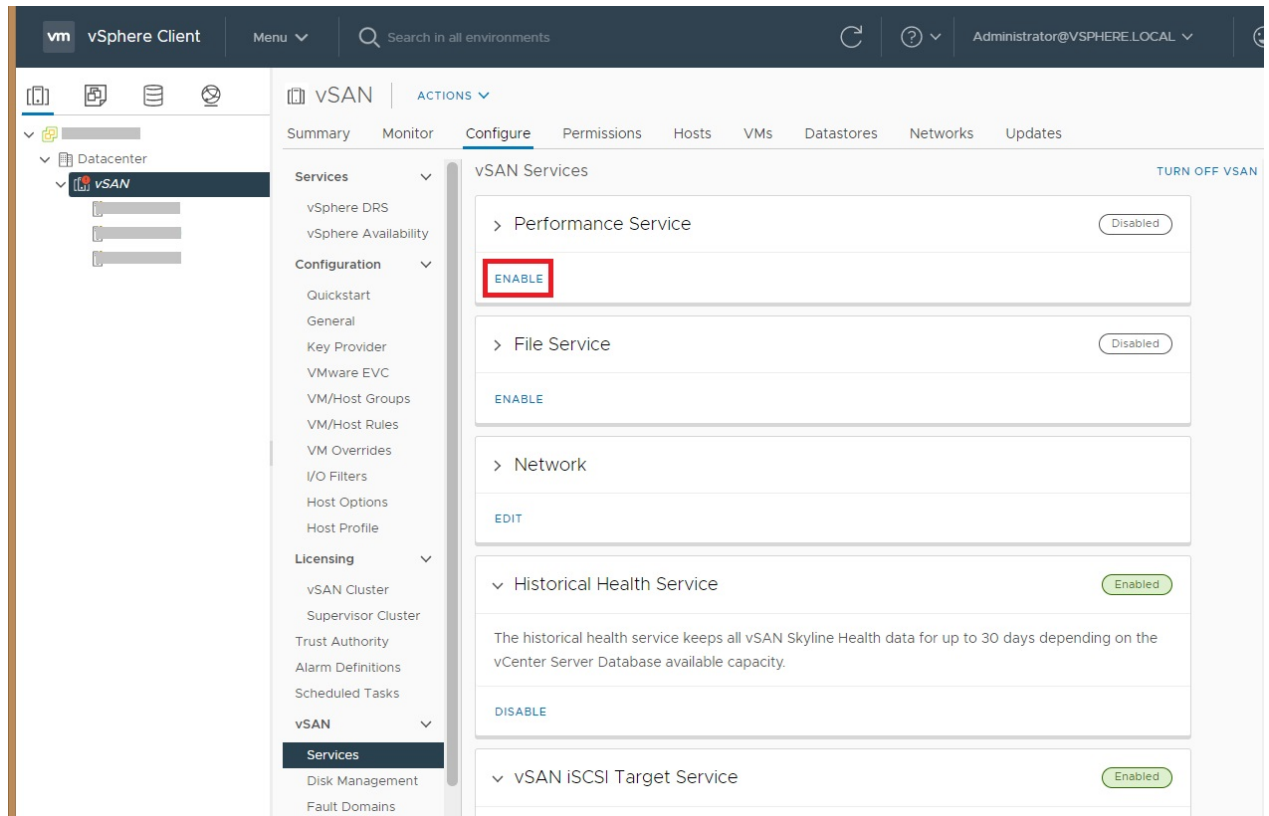
For vCenter Server Appliance 6.7 (HTML 5) or later

1. Display the vSphere Client screen, and from the menu select [Host and Clusters], select the created cluster.
2. From the [Configure] tab on the right side of the screen, select [vSAN] - [Services].

Check [Performance Service]. If it is "Disabled," perform the following procedures to change it to "Enabled."

If it is "Enabled," the following procedures are not required.

Select [ENABLE] in Performance Service.



3. Select "Enable vSAN Performance service," and then select the [APPLY] button.

vSAN Performance Service Settings | vSAN

☒ Enable vSAN Performance service

Storage policy

vSAN Default Storage Policy

The vSAN performance history database is stored as a vSAN object. The policy controls the availability, space consumption, and performance of that object. If the object becomes unavailable, the performance history for the cluster is also unavailable.

Verbose mode

☐ Enable verbose mode

The verbose mode uses additional CPU, Storage IO, and Storage space of vSAN. Use only as directed by VMware Support.

Network diagnostic mode

☐ Enable network diagnostic mode

This allows the vSAN performance service to first create a RAM disk stats object, then collect and save the network metrics to the RAM disk.

CANCEL

APPLY

Performance service is "Enabled" when completed.

vm vSphere Client

Menu

Search in all environments

Administrator@VSPHERE.LOCAL

Datacenter

vSAN

Services

Configuration

Licensing

vSAN

Services

Summary

Monitor

Configure

Permissions

Hosts

VMs

Datastores

Networks

Updates

vSAN Services

TURN OFF VSAN

> Performance Service

Enabled

EDIT

> File Service

Disabled

ENABLE

> Network

EDIT

> Historical Health Service

Enabled

The historical health service keeps all vSAN Skyline Health data for up to 30 days depending on the vCenter Server Database available capacity.

DISABLE

> vSAN iSCSI Target Service

Enabled

4. Apply this similar procedure to all clusters configuring vSAN.

3.8.2 Pre-settings for Statistics Collection Intervals in vCenter Server

To operate Resource Planning, you must enable the statistic information in vCenter Server. The following procedure describes how to enable the statistic information.

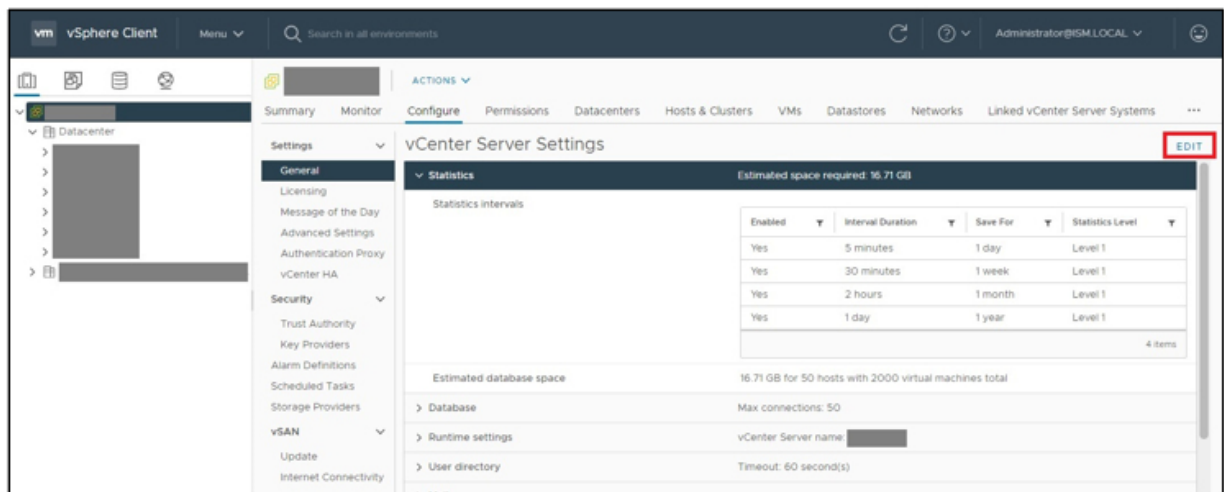
1. Display the vSphere Client screen and select vCenter Server.
2. From the [Settings] tab on the right side of the displayed screen, select [General] - [Statistics].

Confirm that [Enabled] is "Yes" on the displayed screen.

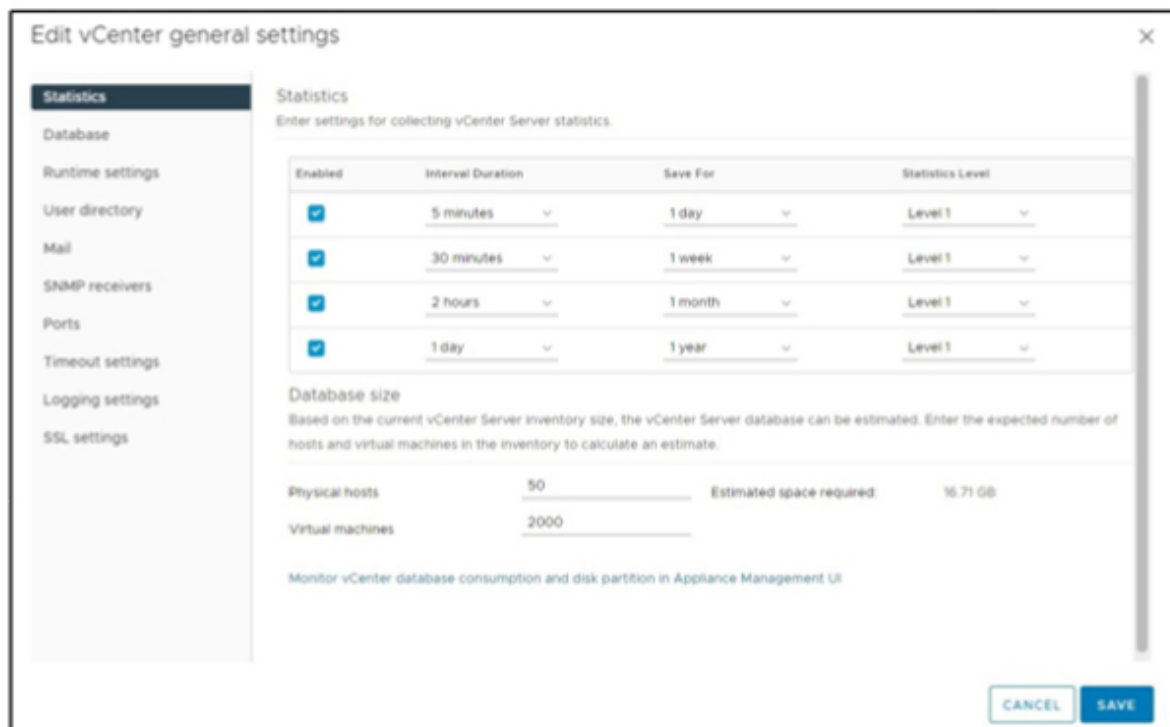
If [Enabled] is not "Yes", follow the next step.

If [Enabled] is "Yes", no further steps are required.

3. Select [EDIT] on vCenter Server Settings.

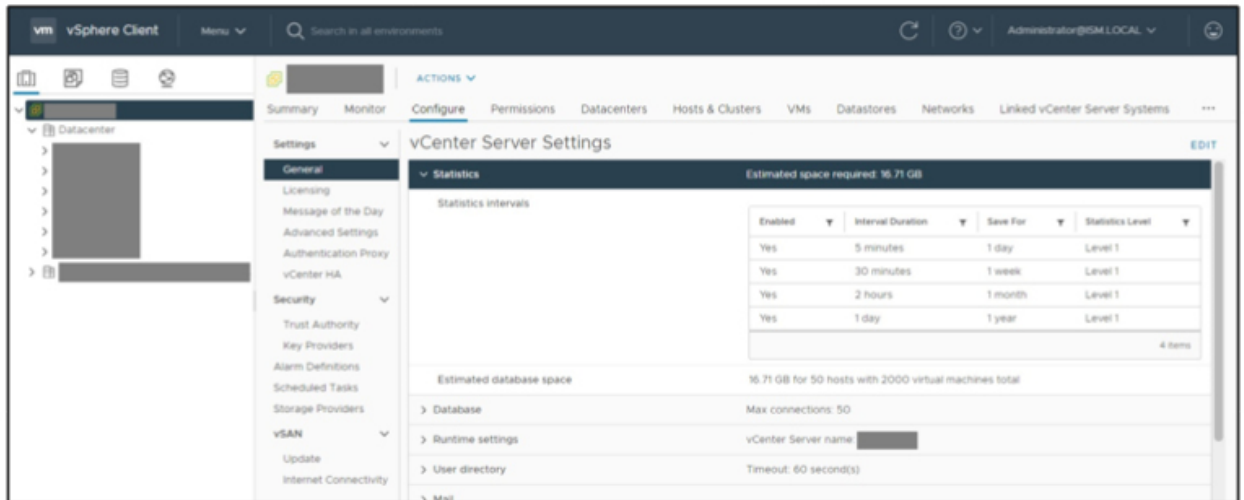


4. Select the [Enabled] checkbox and then select [SAVE] button.



5. Enable status for Statistics displays [Yes].

The [Interval Duration] value of [1 day] must be enabled.



3.8.3 Pre-settings for ISM

Implement the settings required for ISM. The cloud management software and the OS information are registered.

Registering cloud management software

Register the cloud management software in ISM.

For details, refer to "2.14.6 Management of Cloud Management Software."

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



Note

- The tab specifies the following:
 - For vSAN
 - Specify the VMware vCenter Server version that you are using.
 - For S2D/MAS HCI
 - Specify the Microsoft Failover Cluster for the Windows Server version that you are using.
 - 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 the "Cloud Management Software List" screen is displayed.

Registration of OS information

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.

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

The "Node List" screen is displayed.

2. Select the name of the applicable node, and then 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: VMware ESXi version that you are using

- For S2D

OS type: Windows Server

OS version: Windows Server version that you are using

- Enter the 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 the domain name field 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 Basic Operation

This chapter describes how to control ISM.

4.1 Start and Stop of ISM

Sometimes, it may be required to start 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 ISM-VA. Start ISM-VA as a host OS user with administrator privileges.

The following procedures describe how to start 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)

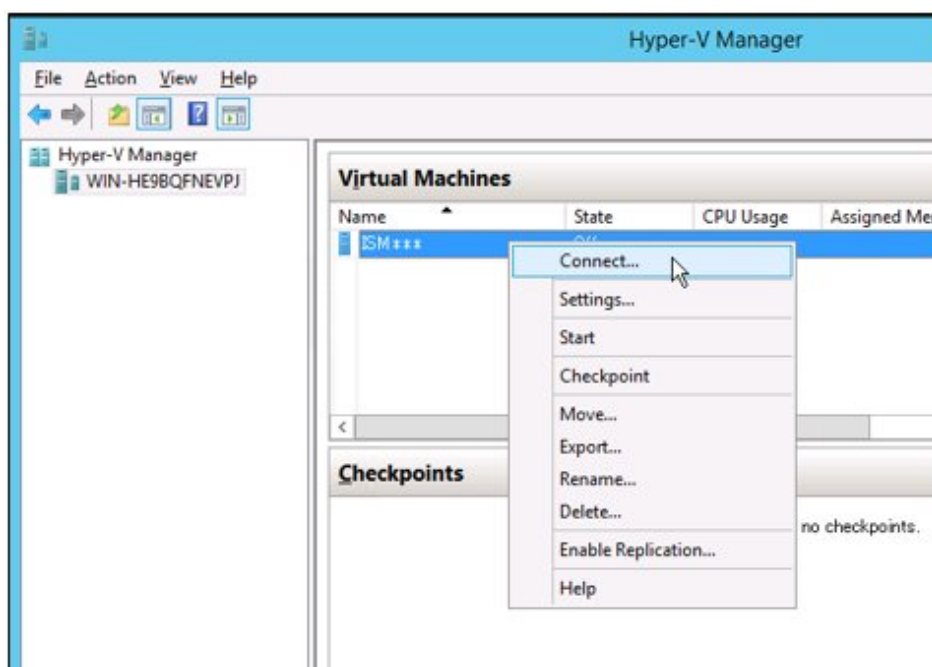


Point

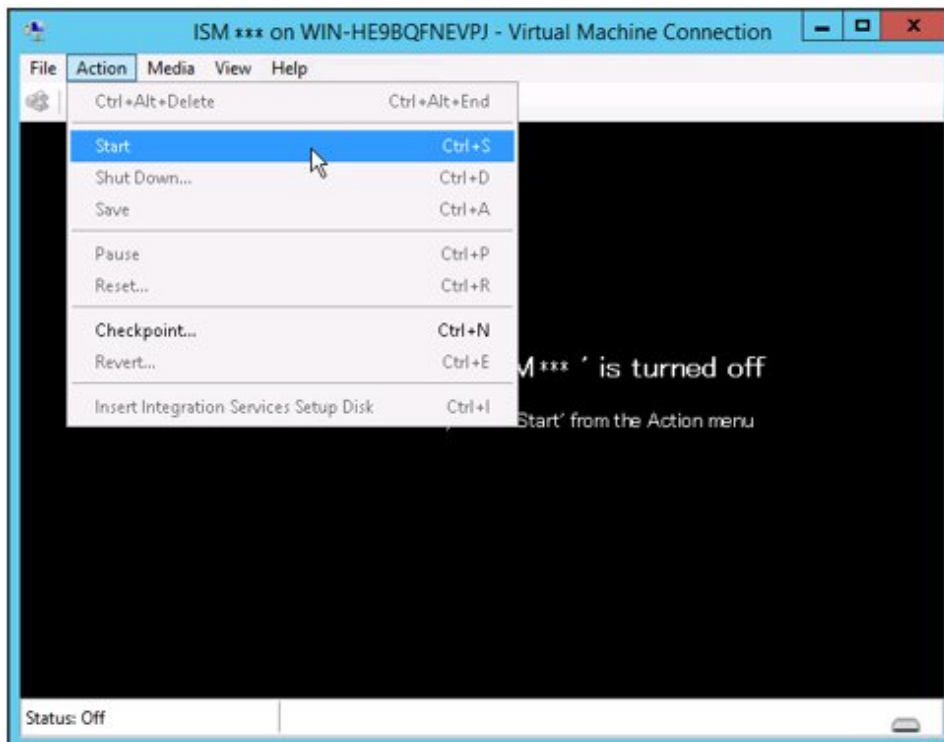
Starting ISM-VA may take several minutes to complete. Wait for a while, and then confirm that you can log in to the GUI.

4.1.1.1 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].

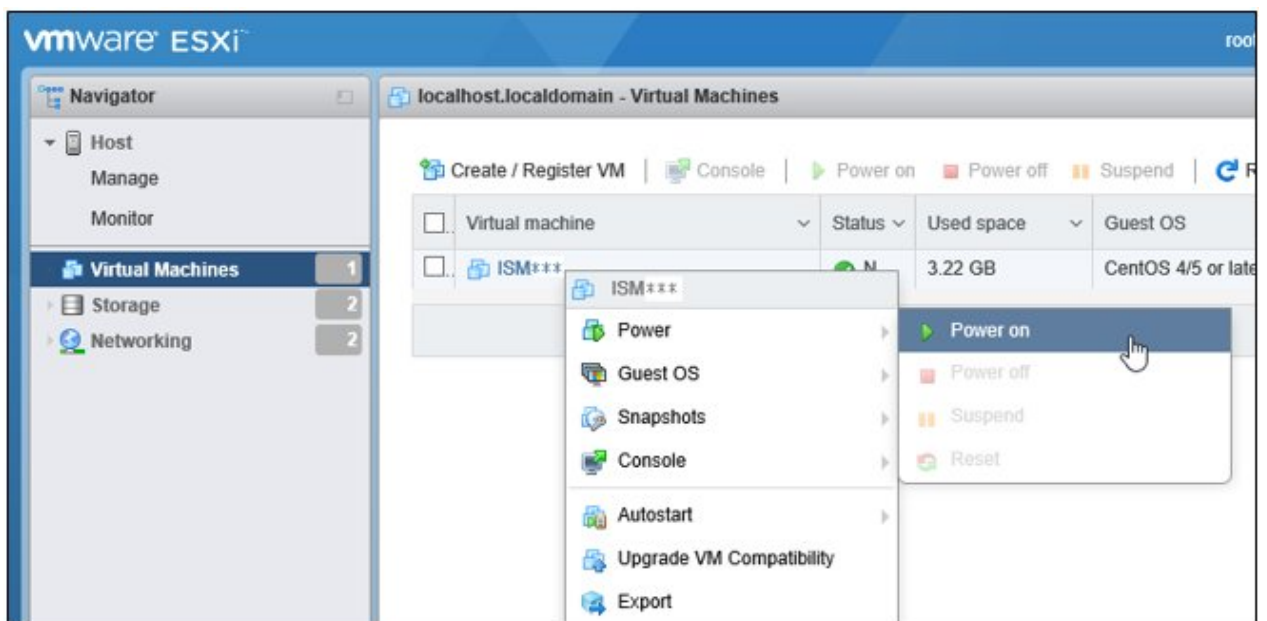


2. On the "Virtual Machine Connection" screen, select [Start] from the [Action] menu to start ISM-VA.

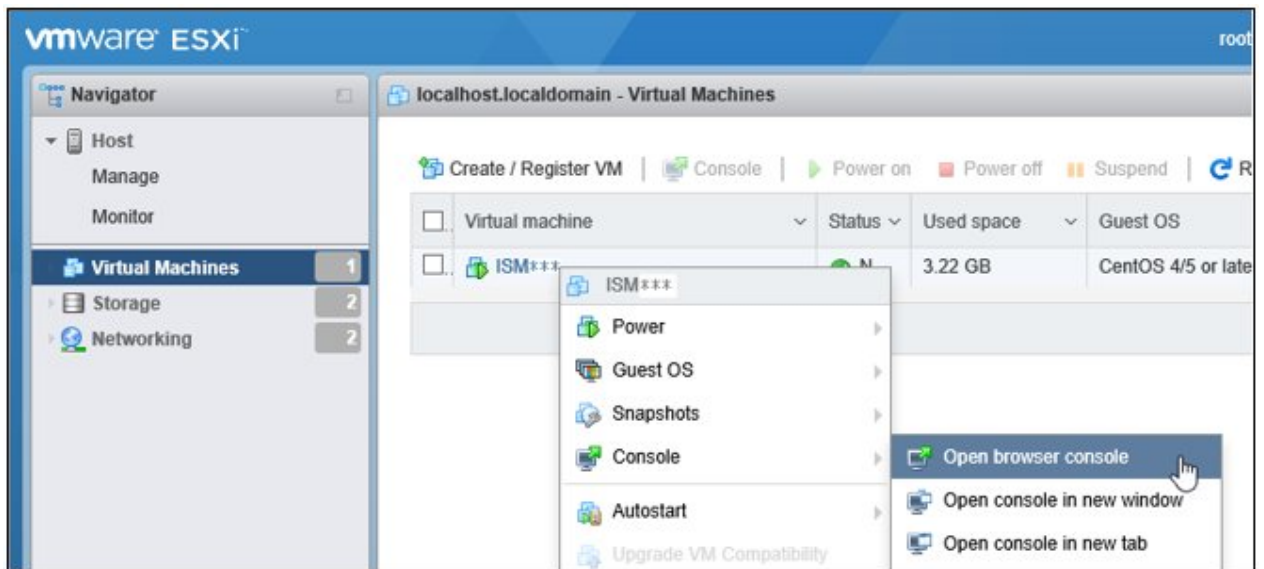


4.1.1.2 For ISM-VA running on VMware vSphere Hypervisor (after installation)

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.

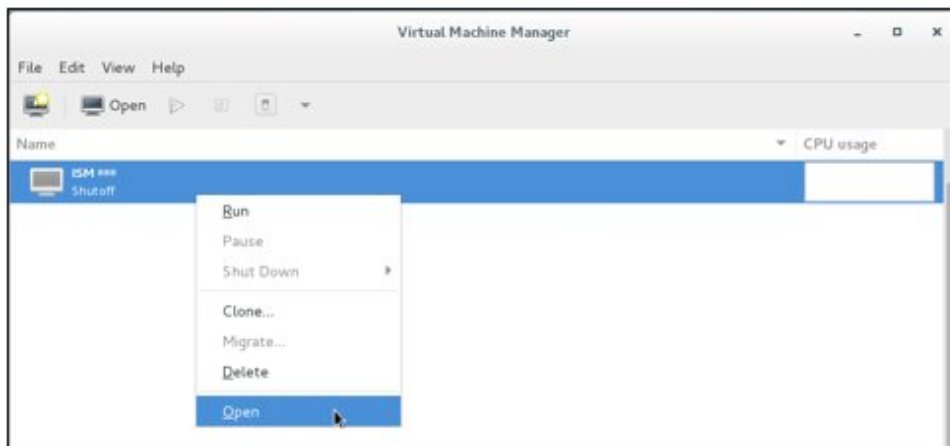


4.1.1.3 For ISM-VA running on KVM (after installation)

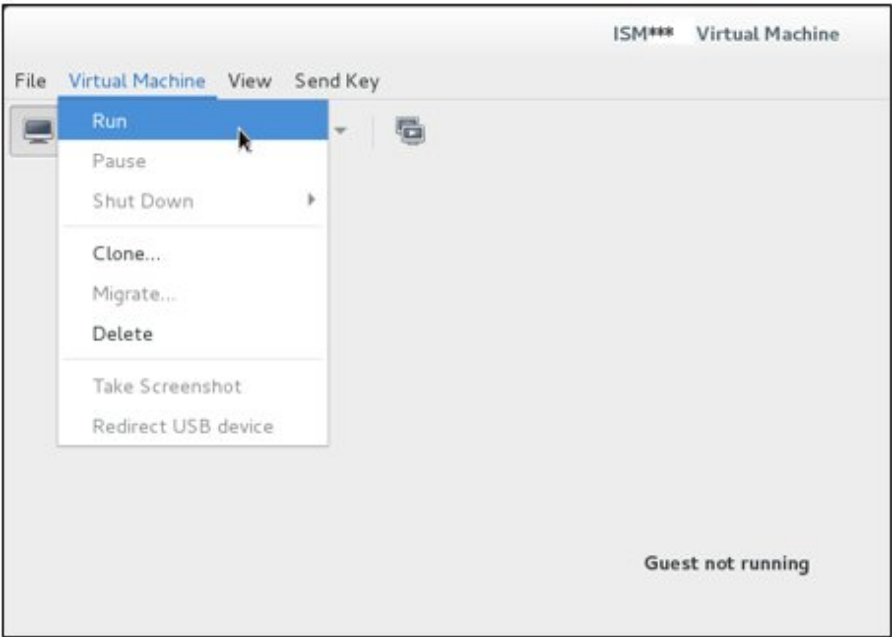
- [For Red Hat Enterprise Linux or SUSE Linux Enterprise Server](#)
- [For Nutanix AHV](#)

For Red Hat Enterprise Linux or SUSE Linux Enterprise Server

1. In Virtual Machine Manager, right-click on the installed ISM-VA, and then select [Open].

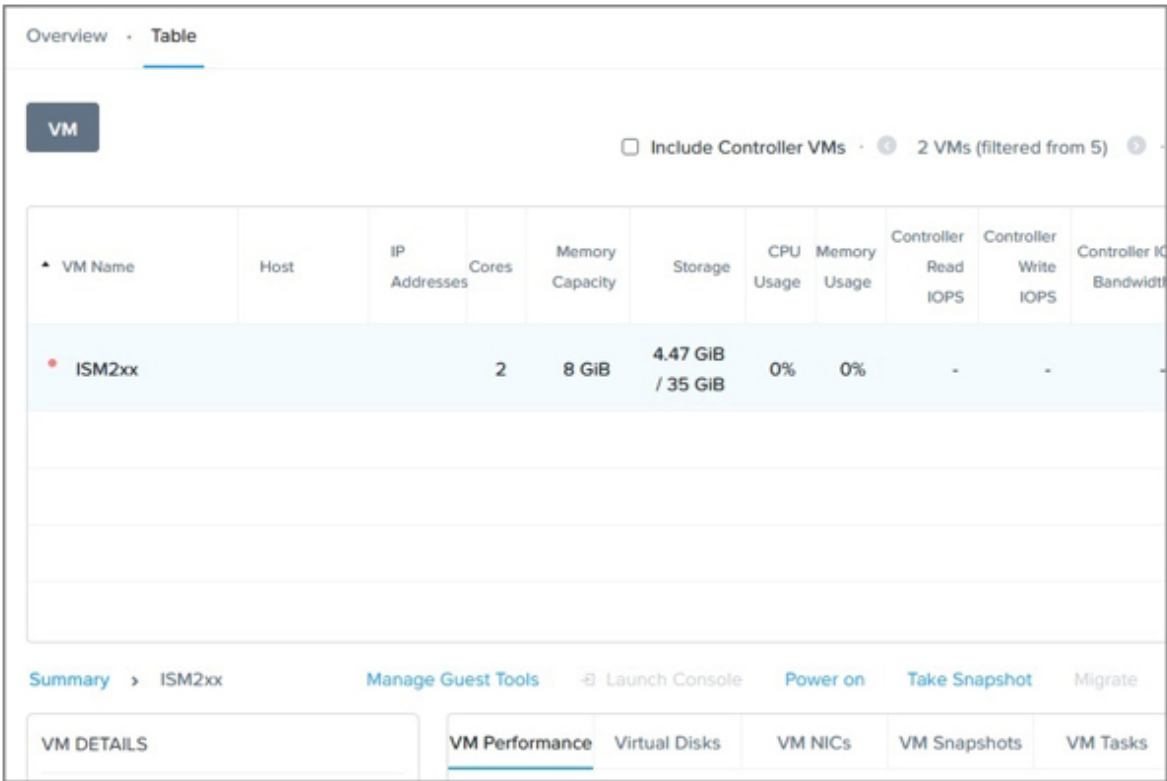


2. On the "ISM-VA Virtual Machine" screen, select [Run] from the [Virtual Machine] menu to start ISM-VA.



For Nutanix AHV

1. In Nutanix PRISM, select the [Table] on the [VM] screen.



2. Select the ISM-VA virtual machine and select [Power on].

4.1.2 Stop of ISM-VA

Use the ISM-VA command to terminate ISM-VA.

1. Start 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 this case, you must 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 ISM GUI, and then close the GUI.
4. Start the console and log in as an ISM administrator.
5. To terminate ISM-VA, execute the termination command of ISM-VA.

```
# ismadm power stop
```



Note

Do not shut down the virtual machine of ISM-VA directly without terminating ISM-VA (executing the ismadm power stop command).

4.1.3 Restart of ISM-

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 ISM-VA, the ISM service starts automatically.

To start and stop the ISM service, 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

For modification of ISM-VA MTU size, refer to "Modification of ISM-VA MTU size" in "[4.9 Network Settings.](#)"

The following is the procedure for using the ISM-VA basic settings menu.

1. From the console, log in to ISM-VA as an administrator.
2. Start using the ISM-VA basic settings menu command.

```
# ismsetup
```

The screen below is displayed.

The screen displays the 'Main Menu' for the ISM Version. It shows current settings for Locale, Network, Time, Log, and GUI. Below the settings, a message states '(*) Item will be changed'. A prompt asks the user to 'Choose the configuration item you want to change:'. A list of items is shown with their corresponding settings: Locale (Language and keyboard settings), Network (Hostname and network settings), Time (Time settings), Log (Log level setting), and GUI (GUI port number setting). At the bottom, there are three buttons: <Select>, <Apply>, and <Quit>.

```
Main Menu
ISM Version: ISM Version

Settings:
[Locale] Language : en_US.utf8
         Keyboard  : us
[Network] Hostname(FQDN) : localhost.localdomain
         IP Address : 192.168.1.101/24
         Gateway Address : 192.168.1.1
         DNS Address  :
[Time]   Time zone   : UTC
         Local Time  : Mon 2017-02-27 02:51:31 UTC
         Using NTP    : disable
         NTP Server   :
         NTP Synchronized : no
[Log]    Log level   : small
[GUI]    GUI Port Number : 25566

(*) Item will be changed

Choose the configuration item you want to change:

Locale Language and keyboard settings
Network Hostname and network settings
Time    Time settings
Log     Log level setting
GUI     GUI port number setting

<Select> <Apply> <Quit>
```

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].

The screen displays the results of the configuration changes. It lists the items that were changed and their new values. At the bottom, there are two buttons: <Execute> and <Cancel>.

```
You made the following changes:

Language: en_US.utf8 -> ja_JP.utf8
Keyboard: us -> jp
Hostname(FQDN): localhost.localdomain ->
localhost2.localdomain
IP Address: 192.168.1.101/24 -> 192.168.1.102/24
Gateway: 192.168.1.1 -> 192.168.1.10
DNS: -> 192.168.1.20
Time zone: UTC -> Asia/Tokyo
Log level: small -> medium

<Execute> <Cancel>
```

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

The purpose of ISM Backup and Restoration is to save and restore the data set with ISM.

You can back up the ISM settings and node registration data and restore them as necessary in case the ISM setting data is damaged due to a problem or the setting data is lost due to an operation error.



Note

- ISM Backup will restore to the same ISM version. It cannot be restored in the different editions.
- ISM Backup backs up some of the ISM settings and registered data. To back up all data, back up the entire ISM-VA using the hypervisor of the cloud management software.

4.4.1 Backup of ISM

The backup operation of ISM is to file the ISM settings set by the user and the information data such as the node registration data registered for monitoring, and retrieve it to the outside. Backup of ISM can be done by the following operations.

The following methods can be used to back up ISM.

- Backup of ISM using the ISM-VA management command
- Backup of ISM using the GUI
- Backup of ISM using the REST API
Refer to "REST API Reference Manual."

The backup file is created in the following directory for the information data collected with the ISM backup.

Directory: /Administrator/ftp

File name: ism2.9.0-backup-202310102723.tar.gz (File name is an example)

The information data of ISM backup targets are as follows.

Note: Y = Backed up, N = Not backed up

Classification	Information data	Target	Remarks
ISM-VA user settings information	Setting item in the ISM-VA basic settings menu	Y	
	Management data of accounts	Y	
	Security policy settings	Y	
	LDAP server settings	Y	
	Log Collection (scheduled settings)	Y	
	Alarm settings	Y	
	License information	Y	
	SSL certificates, CA certificates	Y	
	Client certificate for Relay Route	N	Reconfiguration is required when restoring.
ISM-VA customize information	Dashboard settings	Y	
	Node list customization selection	Y	
	Virtual disk allocation information	Y	
	Plug-in	N	Reinstallation is required.
Node registration information	Node registration data (node list)	Y	
	Node details information (Communication settings, OS information)	Y	
	Node groups, User groups	Y	
	Alarm settings	Y	
Monitoring data	ISM events (Audit logs, Operation logs, SNMP traps, Anomaly Detection logs)	Y	ISM events are backed up.
	Archived logs, Node logs	N	It is deleted when restoring.
	Anomaly Detection learning data	N	
Repository	ServerView Suite DVD	N	Within the repository, all are not applicable. Reconfiguration is required after restoration.
	OS image	N	
	Firmware Update file	N	
Work file	CSV export data	N	All work files are initialized when restoring.
	Event export data	N	

Classification	Information data	Target	Remarks
	Maintenance collection data	N	

4.4.2 Restoration of ISM

Restoration of ISM is an operation that restores ISM settings set by the user and information data such as node registration data registered for monitoring from backup files created in backup of ISM.

Restore from ISM backup file stored in the following directory.

Directory: /Administrator/ftp

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 Required Maintenance Data

The procedure to collect the maintenance data if the failure occurred in ISM and the Virtualized Platform Expansion function is as follows.

Collect the required maintenance data depending on the purpose of investigation for the system operated by ISM.

Target of investigation	Maintenance data	Retrieving method
Investigation of malfunctions in ISM and/or ISM-VA	<ul style="list-style-type: none"> - ISM RAS Logs - ISM-VA Operating System logs - Database information 	<p>You can collect the maintenance data either separately according to the purpose of your investigation or collectively.</p> <p>Maintenance data for ISM can be retrieved from the GUI or by a command.</p> <p>For details, refer to "8.2 Collect Maintenance Data" in "Operating Procedures."</p>
Investigation of common malfunctions in ISM for PRIMEFLEX functions		
Investigation of malfunctions in Virtual Resource Management / Cluster Management	vSAN log	<p>Retrieve the vc-support log from vCenter.</p> <p>Collection procedure for the vc-support log</p>
Investigation of malfunctions in Cluster Creation / Cluster Expansion	Execution log of the OS setting script executed after OS installation	Collection procedure for the execution log of the OS setting script executed after OS installation
	Execution log of the PowerShell script executed on the Windows Server	Collection procedure for the execution log of the PowerShell script executed on the Windows Server

Maintenance data can only be collected by ISM administrators. ISM administrators provide the person in charge (local Fujitsu customer service partner) with the collected maintenance data.



Note

Retrieving database information may take several hours to complete. In addition, this requires large amounts of free disk space in ISM-VA. If you need 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.

Collection procedure for the vc-support log

The vc-support log is collected from vCenter as maintenance documentation for the Virtual Resources Management. For details, refer to "To collect ESX/ESXi and vCenter Server diagnostic data" from the following URL:

<https://kb.vmware.com/s/article/2032892>

In the log collection procedure in the URL above, when selecting the ESXi hosts to export logs to, select all the vSAN cluster ESXi hosts where an error has occurred.



Multiple logs for vSAN cluster can be retrieved. For more information, refer to "[2.13.9 Batch Collection of vSAN Logs for a VMware vSAN Cluster](#)."

Collection procedure for the execution log of the OS setting script executed after OS installation

The log collection procedure depends on the environment. The estimated capacity is about 30 KB.

- PRIMEFLEX HS/PRIMEFLEX for VMware vSAN

Retrieve it from the following location on the ESXi host.

/vmfs/volumes/datastore1_error/post_script.log

Collection procedure for the execution log of the PowerShell script executed on the Windows Server

Collect all of the following files for the target server [Note]:

- C:\FISCRB\Log\<File name of PowerShell script>_yyyymmdd-hhmmssmmm.log
- .log under C:\FISCRB\Log\

[Note]: The target servers are as follows, depending on the environment and function.

- PRIMEFLEX HS/PRIMEFLEX for VMware vSAN

DNS server

4.5.2 Changing Log Output Settings

Output of logs used for failure investigation can be set as follows.

- [4.5.2.1 Switching the ISM RAS Log mode](#)
- [4.5.2.2 Switching the ISM RAS Log level](#)
- [4.5.2.3 Specification of core file collection directory](#)

4.5.2.1 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, log in to ISM-VA as an administrator.
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
```

4.5.2.2 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

Log level	Approximate size of log to be exported	Number of managed 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, log in to ISM-VA as an administrator.
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.](#)"

4.5.2.3 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 "[4.5 Collection of Maintenance Data.](#)"

1. From the console, log in to ISM-VA as an administrator.

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.

4.6 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 ISM-VA as executed according to "[3.7.1 Allocation of Virtual Disks to ISM-VA](#)" cannot be canceled.

The following operating example shows how to cancel the allocation of a virtual disk to a user group named usrgp1.

1. After starting ISM-VA, from the console, log in to ISM-VA 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 usrgp1.

```
# 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`.

- Specify the User Group Name and unmount the virtual disk.

```
# ismadm volume umount -gdir usrgrp1
```

- Specify the Volume Name (`usrgrp1vol`) for `usrgrp1` and delete the virtual disk.

```
# ismadm volume delete -vol usrgrp1vol
Logical volume "usrgrp1vol" successfully removed.
```

- 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 10.7 GB)

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

```

- Restart ISM-VA.

```
# ismadm power restart
```

4.6.2 Allocation of Additional Virtual Disks to ISM-VA

Using the same procedure as in "[3.7.1 Allocation of Virtual Disks to ISM-VA](#)," you can additionally allocate multiple virtual disks to 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 `usrgrp1`.

- Connect to the virtual disk.

Execute the operations in Step 1 of "[3.7.2 Allocation of Virtual Disks to User Groups](#)."

- After starting up ISM-VA, from the console, log in to ISM-VA 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/usrgrplvol-lv  10G   33M   10G    1% 'RepositoryRoot' /usrgrpl
tmpfs            380M    0   380M    0% /run/user/0
/dev/sdc                                     (Free 5368 MB)

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

```
# ismadm volume extend -vol usrgrplvol -disk /dev/sdc
Logical volume "/dev/mapper/usrgrplvol-lv" resized.
```

6. Confirm the virtual disk settings.

Confirm that the newly added volume (/dev/sdc) is set for use by usrgrpl (usrgrplvol).

```
# 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/usrgrplvol-lv  15G   33M   15G    1% 'RepositoryRoot' /usrgrpl
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      usrgrplvol lvm2 a--  10.00g    0
/dev/sdc1      usrgrplvol lvm2 a--   5.00g    0
```

7. Restart ISM-VA.

```
# ismadm power restart
```

4.7 Certificate Activation

You can manage an SSL certificate that is set in the web browser when you use the ISM GUI.

4.7.1 Deployment of SSL Certificates

When using an SSL certificate issued by an authentication authority for security reasons, follow the procedure below to set it.

There is no upper limit on RSA public key length for SSL certificates.

1. Transfer the SSL certificate to ISM-VA.

Transfer destination: /Administrator/ftp

For information on how to transfer files using the GUI, refer to "[4.23 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. Deploy the SSL certificate.

Execute the following command, specifying the "key" and "crt" files you transferred.

```
# ismadm sslcert set -key /Administrator/ftp/server.key -crt /Administrator/ftp/server.crt
```

4. Restart ISM-VA.

```
# ismadm power restart
```



Point

You can create the unique SSL 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 Certificates

You can have the SSL certificates displayed that are enabled in ISM-VA.

1. From the console, log in to ISM-VA as an administrator.
2. Execute the command for displaying the SSL certificates.

```
# ismadm sslcert show
```

4.7.3 Export of SSL Certificates

You can export the SSL certificates that are enabled in ISM-VA.

1. From the console, log in to ISM-VA as an administrator.
2. Execute the command for exporting the SSL certificates.

```
# ismadm sslcert export -dir /Administrator/ftp
```

You can download the exported files via FTP.

4.7.4 Creation of Self-signed Certificates

Create a self-signed certificate based on the IP address specified in ISM-VA or FQDN.

1. From the console, log in to ISM-VA as an administrator.

2. Execute the command for creating the self-signed 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 certificates are created.

<https://<IP address of ISM-VA>:25566/ca.crt>

If you are using Google Chrome, execute [Save as] and change the file name to "ca.crt" for the displayed contents. When saving, select [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, log in to ISM-VA as an administrator.
2. Execute a command for the license settings.

- Registration of licenses

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

- Display of licenses

```
# ismadm license show
```

Example of command execution:

```
# ismadm license show
Operation Mode : Advanced
#   [Type]  [Edition] [#Node]  [Reg.Date]  [Exp.Date]  [Status]      [Licensekey]
1   Server  Adv.         -   2024-05-29  2025-05-29  Valid         *****==
2   Node    Adv.         10  2023-08-28  2024-08-27  Expires soon  *****==
3   Node    Adv.         10  2023-05-30  2024-05-29  Expired       *****==

*Reg.Date(RegistrationDate[yyyy-mm-dd])
*Exp.Date(ExpirationDate[yyyy-mm-dd])

You have an expired license.
Delete the expired license and register a new license.
```

Table 4.1 Description on the command output

Item	Description
[Operation Mode]	Displays one of the following ISM Operation Modes: <ul style="list-style-type: none">- Essential

Item	Description
	<ul style="list-style-type: none"> - Advanced - Advanced for PRIMEFLEX
[Type]	Displays "Server" for a server license and "Node" for a node license.
[Edition]	Displays one of the following types of the license: <ul style="list-style-type: none"> - 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."
[Reg.Date]	Displays the date when the license was registered.
[Exp.Date]	Displays the date when the license expires. Always displays "-" if it is unlimited.
[Status]	Displays the status of the license. <ul style="list-style-type: none"> - Valid: valid - Expires soon: expiring within 30 days - Expired: already expired
[Licensekey]	Displays the character string of the registered license key.

- Deletion of licenses

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



- You can register licenses, check the displayed contents including license types, and delete licenses by selecting [Settings] - [General] - [License] from the Global Navigation Menu on the ISM GUI.
- If registration/deletion of licenses does not change the operating mode, restart of the ISM-VA is not required.

4.9 Network Settings

You can set and display the network settings, and confirm network connectivity.

Setting/Display of Networks

1. From the console, log in to ISM-VA as an administrator.
2. Execute the commands 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>
```



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
```

- Modification of ISM-VA MTU size

```
# ismadm network modify <LAN device name> 802-3-ethernet.mtu <MTU size>
```

The configured MTU size is displayed in the "802-3-ethernet.mtu" entry in the output of the display of network settings command.

After the command is executed, the output of the configuration display command is displayed immediately, but ISM-VA must be restarted to enable the new MTU size.

The MTU size defaults to 1500. "auto" is displayed in the output of the display of network settings command.

You can change the MTU size from 1280 to 65535.

Note

Configuring an MTU size that does not match the network used by ISM can cause loss of communication or slow down the network. Change the MTU size only if you need to.

Example of command execution:

```
# ismadm network modify eth0 802-3-ethernet.mtu 1460
```

- Display of network settings

```
# ismadm network show <LAN device name>
```

Example of command execution:

```
# ismadm network show eth0
```

Point

You can also execute the network setting with "4.2 ISM-VA Basic Settings Menu."

Confirmation of network connectivity

Confirm connectivity between the ISM-VA and the management LAN.

1. From the console, log in to ISM-VA as administrator.

2. Execute the command for confirmation of network connectivity.

```
# ismadm network ping -host <IP address or FQDN>
```

If the DNS server is set to ISM-VA, you can specify the FQDN instead of the IP address.

Example of command execution: when connectivity is succeeded

```
#ismadm network ping -host 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.056 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.038 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=0.066 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=0.039 ms

--- 192.168.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.038/0.049/0.066/0.014 ms
```

Example of command execution: when connectivity is failed

```
# ismadm network ping -host 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
From 192.168.1.101 icmp_seq=1 Destination Host Unreachable
From 192.168.1.101 icmp_seq=2 Destination Host Unreachable
From 192.168.1.101 icmp_seq=3 Destination Host Unreachable
From 192.168.1.101 icmp_seq=4 Destination Host Unreachable
```

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 ["4.23 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 the command for registering certificates for alarm notification mails.

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



Point

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, log in to ISM-VA as an administrator.
2. Execute the commands for controlling the ISM-VA service.

- Restart of ISM-VA

```
ismadm power restart
```

- Stop of ISM-VA

```
ismadm power stop
```

- Display of list of internal services

```
ismadm service show
```

- Start of internal services individually

```
ismadm service start <Service name>
```

Example of command execution: Start FTP server individually

```
# ismadm service start vsftpd
```

- Stop of internal services individually

```
ismadm service stop <Service name>
```

Example of command execution: Stop FTP server individually

```
# ismadm service stop vsftpd
```

- Restart of internal services individually

```
ismadm service restart <Service name>
```

Example of command execution: Restart FTP server individually

```
# ismadm service restart vsftpd
```

- Display of status of internal services individually

```
ismadm service status <Service name>
```

Example of command execution: Display FTP server status individually

```
# ismadm service status vsftpd
```

- Enabling internal services individually

```
ismadm service enable <Service name>
```

Example of command execution: Enable FTP server individually

```
# ismadm service enable vsftpd
```

- Disabling internal services 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, log in to ISM-VA as an administrator.
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, log in to ISM-VA as an administrator.
2. Execute the command for modification of host names.

```
# 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

- Characters that can be used as a host name are lowercase letters, numbers, hyphens (-), and periods (.). Hyphens and periods are not allowed as leading or trailing characters in host names. If characters other than those allowed are used, ISM will not work properly.
- After executing the command, restart is required.
- To modify the default host name "localhost," you need 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 "[4.23 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, log in to ISM-VA as an administrator.
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
```

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 confirmation screen to uninstall the plug-in is displayed.

2. Enter [y] to finalize the uninstallation.

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 (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.



Note

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 you execute the command, a message to confirm 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 "[4.23 File Upload Using the GUI](#)."

For information on how to transfer files via FTP, refer to "[2.1.2 FTP Access](#)."

```
# ismadm dhcpd set -file <conf file>
```

Example of command execution:

```
# ismadm dhcpd 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 (The sentences after the * are not actually displayed on the screen.)

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 start of DHCP services

```
# ismadm service start dhcpd
```



- 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 start of ISM-VA

```
# ismadm service enable dhcpd
```

- Setup not to enable DHCP services upon start 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 dhcpdsvr show-conf
```

- Display of the DHCP server message

```
# ismadm dhcpdsvr 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 dhcpdsvr show-msg -line 50
```

- Export of the current settings (conf file) to the location where ftp access is possible

```
# ismadm dhcpdsvr export-conf -dir /Administrator/ftp
```

- Export a sample of the settings (conf file) to the location where ftp access is possible

```
# ismadm dhcpdsvr 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 dhcpdsvr show-mode
```

Command output (The sentences after the * are not actually displayed on the screen.)

```
DHCP mode: local      *ISM-VA internal DHCP server is used in Profile Management.
DHCP mode: remote    *The external DHCP server is used in Profile Management.
```

- Switching of the settings

- Setting up so that a profile is assigned with use of the ISM-VA internal DHCP server

```
# ismadm dhcpdsvr set-mode local
```

- Setting up so that a profile is assigned with use of the external DHCP server

```
# ismadm dhcpdsvr 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 "[4.23 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 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 on the hypervisor where ISM is running before applying patches.
- ISM-VA disk space is used for system updates. For disk space requirements, refer to the following.

"[System updates after applying a patch or upgrade](#)" in "[1.3.1 Requirements for Hypervisor to Run ISM-VA \(Virtual Machines\)](#)"

"[9.1 Apply Patches and Upgrade Programs to ISM](#)" in "[Operating Procedures](#)"

Apply patch files using the ismadm command

1. Transfer the patch files to ISM-VA.

Transfer destination: /Administrator/ftp

Patch files (tar.gz format) are included in the released files (zip format).

Decompress the released files to obtain the patch files.

For information on how to transfer files using the GUI, refer to "[4.23 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, log in to ISM-VA as an administrator.
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 path>
```

Example of command execution:

```
# ismadm system patch-add -file /Administrator/ftp/ISM240x_S20190901-01.tar.gz
```

If the command execution is successful, the following message is displayed.

```
-----  
Update finished successfully.  
Please restart ISM-VA.  
-----
```

5. After applying patches, restart ISM-VA.

```
# ismadm power restart
```

6. From the console, log in to ISM-VA as an administrator and execute the following command.

Confirm that the patch has been applied and the version of the applied patch is displayed.

```
# ismadm system show
```

Apply patch files using the GUI

For details, refer to "9.1 Apply Patches and Upgrade Programs to ISM" in "Operating Procedures."

4.18 Upgrade of ISM-VA

4.18.1 Migrating with Backup File

Upgrade using the backup file created in V2.9.0 and importing the backup file into the newly installed V3.0.0. This operation is hereafter referred to as "migrate".

For procedure on upgrading from V2.9.0 to V3.0.0, refer to "9.2 Upgrade from V2.x.0 to V3.0.0" in "Operating Procedure."



Note

- Back up ISM-VA on the hypervisor where ISM is running before upgrading.
- ISM-VA disk space is used for system updates. For disk space requirements, refer to the following.

"System updates after applying a patch or upgrade" in "1.3.1 Requirements for Hypervisor to Run ISM-VA (Virtual Machines)"

4.18.2 Applying Upgrade File

Upgrade from V3.0.0 to V3.1.0 or later.

Upgrade files will be provided when V3.1.0 or later is released. Obtain the upgrade file and apply it as follows:

Apply upgrades using the ismadm command

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 "4.23 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. 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.

```
# ismadm system upgrade -file <Upgrade file path>
```

Example of command execution:

```
# ismadm system upgrade -file /Administrator/ftp/ISM240x_S20190901-01.tar.gz
```

If the command execution is successful, the following message is displayed.

```
-----  
Update finished successfully.  
Please restart ISM-VA.  
-----
```

5. After executing the upgrade, restart ISM-VA.

```
# ismadm power restart
```

6. From the console, log in to ISM-VA as an administrator and execute the following command.

Confirm that the upgrade has been applied and the selected version is displayed.

```
# ismadm system show
```

Apply upgrades using the GUI

1. From the Global Navigation Menu on the ISM GUI, select [Settings] - [General].
2. From the menu on the left side of the screen, select [ISM patch / upgrade program].
The current version of ISM is displayed.
3. Select the [Update ISM] button.
4. Follow the instructions on the "ISM Patch / Upgrade Program" screen and input the setting items. Select the [Confirm] button.
5. Confirm the contents, and then select the [Yes] button.
6. Wait for the upgrade to complete.

After the upgrade is completed, clear the cache, and go to the login screen.

7. After a logging into ISM, confirm that the program is upgraded.

From the Global Navigation Menu on the ISM GUI, select [Help] - [About ISM].

Confirm that the selected version is displayed.



Note

- Back up ISM-VA on the hypervisor where ISM is running before upgrading.
- ISM-VA disk space is used for system updates. For disk space requirements, refer to the following.

"[System updates after applying a patch or upgrade](#)" in "[1.3.1 Requirements for Hypervisor to Run ISM-VA \(Virtual Machines\)](#)"

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
HOURL	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      HOURL    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	HOURL	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	HOURL	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. Connections that can be used to change the protocol version are GUI/REST and FTPS connections used for node logging.

By default, the SSL/TLS versions that can be used are as follows.

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

Connection method	ISM environment	SSL/TLS versions that can be used			
		SSLv3	TLSv1	TLSv1.1	TLSv1.2
GUI/REST connection	Before ISM 2.3.0	Y	Y	Y	Y
	ISM 2.3.0 or later	- [Note 1] [Note 2]	- [Note 1] [Note 2]	- [Note 1] [Note 2]	Y
FTPS connection	ISM 2.7.0.020 - ISM 2.9.0.021	- [Note 2]	Y	- [Note 2]	Y
	ISM 2.9.0.030 or later	- [Note 2]	-	- [Note 2]	Y

[Note 1]: If you upgrade ISM, the SSL/TLS version that is available with the version of ISM that you are upgrading to is used.

Example: The SSL/TLS versions available if you update or upgraded from an ISM version before ISM 2.3.0 to ISM 2.7.0.020
SSLv3, TLSv1, TLSv1.1, and TLSv1.2

[Note 2]: You can enable SSL/TLS by specifying the <Versions that are permitted to be used> when executing the command to set SSL/TLS to be enabled.

1. From the console, log in to ISM-VA as an administrator.
2. Execute the command to set SSL/TLS to be enabled.
 - To change the SSL/TLS protocol version for a GUI/REST connection

```
# ismadm security enable-tls <Versions that are permitted to be used>
```

- To change the SSL/TLS protocol version for FTPS connections used for collecting node logs

```
# ismadm security enable-tls-ftp <Versions that are permitted to be used>
```

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, and TLSv1.2

Note that except TLSv1 for FTPS connections for ISM 2.9.0.030 or later.



Note

.....
TLSv1.2 must be enabled when collecting logs or using Online Update on Windows OSes.
.....

Example: Configure TLSv 1.1 and TLSv 1.2 for versions that allow GUI/REST connections

```
# 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 is enabled. Versions not specified are disabled.

4.21 Changing Encryption Suite Settings

You can set the encryption suite type for GUI/REST and FTPS connections.

For the encryption suite type, you can set the following values.

Value	Equivalent encryption suite settings in OpenSSL [Note]	Note
1	HIGH, MEDIUM (Except for aNULL and MD5)	
2	HIGH (Except for SHA1 and aNULL)	
3	HIGH	Default value

[Note]: The equivalent encryption suite settings in OpenSSL are as follows:

- HIGH: Uses an encryption with a key length of 128 bits or more
- MEDIUM: Uses 128 bits key length encryption.
- aNULL: An encryption setting that does not allow authentication for anonymity.

For details, refer to "CIPHER STRINGS List" in "OpenSSL Manual."

1. From the console, log in to ISM-VA as an administrator.
2. Execute the encryption suite setting command.
 - To change the encryption suite for GUI/REST connections

```
# ismadm security set-sslcipher 1
```

- To change the encryption suite for FTPS connections

```
# ismadm security set-sslcipher-ftp 1
```

Note that the encryption suite for FTPS connections cannot be changed with ISM 2.9.0.030 or later.



Note

The HTTP server will reboot automatically after the command is complete. Therefore, the communication with the GUI may be disconnected.

4.22 Settings for Links with Other Software

You can register certificates used when linking to other software.

1. Transfer the certificates.

Transfer destination: /Administrator/ftp/software/cert

For information on how to transfer files using the GUI, refer to ["4.23 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 the 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 of certificate for link with other software

```
# ismadm security show-software-cert -software <Software name>
```

- Deletion of 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>
```

4.23 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 "1.4.1 Upload Files to ISM-VA" in "Operating Procedures."

Point

The following operations are not available when you use the GUI. To perform them, use FTP.

- Downloading of the files in the file storages
- New creation, renaming, and deletion of the file storage directory

Note

If the file name or directory name to be uploaded contains any of the following characters, upload the file via FTP. If the file name or directory name does not contain any of the following characters, you can upload using the GUI.

[Unavailable Characters]

- % (percent, single-byte character)

- & (ampersand, single-byte character)
- ' (single quote, single-byte character)
- ` (grave accent, single-byte character)
- " (double quote, single-byte character)

If the file name or directory name contains any of the above characters, file upload using the GUI will result in an error (Message ID: 50990004 or 50190263).

4.24 Settings for Enabling/Disabling Verification of Profiles

You can enable or disable verification of profiles.

- When verification is disabled
 - Periodic automatic execution and manual execution of verification of profiles are disabled.
 - [Verify Status] for the target profile is displayed as [- (hyphen)].
- When verification is enabled
 - Periodic automatic execution and manual execution of verification of profiles are enabled.
 - [Verify Status] for the target profile is displayed as [Verify Failed]. The appropriate [Verify Status] is set by executing the periodic automatic verification of profiles, or manual verification.

1. From the console, log in to ISM-VA as an administrator.
2. Stop ISM services. For details, refer to "[4.1.4 Start and Stop of ISM Service](#)."
3. Execute the command to enable/disable verification of profiles.

- To enable verification of profiles

```
# ismadm system set-profile-verify enable
```

- To disable verification of profiles

```
# ismadm system set-profile-verify disable
```

4. Start ISM services. For details, refer to "[4.1.4 Start and Stop of ISM Service](#)."

4.25 Display of Verify Status

You can display the enabled/disabled status of verification of profiles.

1. From the console, log in to ISM-VA as an administrator.
2. Execute the command to display the status of verification of profiles.

```
# ismadm system show-profile-verify
```

Command output (The sentences after the * are not actually displayed on the screen.)

```
Profile verify status: enable          * Verification of profiles is enabled.
Profile verify status: disable        * Verification of profiles is disabled.
```

4.26 Security Settings for the Network Connection

You can strengthen the security for the network connection.

4.26.1 SSH Security Settings

You can modify the following settings and display the statuses.

- Lock settings for failed SSH logins

Users who have failed to login five times within a certain period will be locked and SSH connection will be disabled. Logins to the GUI and ftp are not affected by this setting

- Restrict the IP address for the SSH source of connection

Restrict external connections to the ISM-VA 22/TCP port.

To use Multi-Factor Authentication, the setting must be enabled

- Set SSH keyboard interactive authentication

Modify the default password authentication method to a more secure keyboard interactive authentication method.

- Connection settings for SSH public keys

Configure these settings to use a public key-based SSH authentication method. After configuring these settings, you can still log in using your user ID and password.

- Console automatic logout settings

Configure the time (in minutes) to be automatically logged out after a certain period of inactivity when logged in via SSH connection or from the hypervisor console.

Confirming SSH security settings

You can confirm restrictions for the IP address for the SSH source of connection, the lock for failed SSH logins, and settings for SSH keyboard interactive authentication. Each setting is applied to the users who log in after changing the settings.

```
# ismadm security show-ssh-conf
```

Example of command execution:

```
# ismadm security show-ssh-conf
client ip address limitation : enable
client ip address to use : 192.168.2.20,192.168.1.0/24
userlock at login failure : enable
keyboard-interactive authentication : enable
```

If you fail to login five times within 15 minutes, you will be locked and SSH connection will be disabled. To release the lock, use the "Disabling the user lock for failed SSH logins" command.

SSH security settings

You can enable or disable the settings for the lock for failed SSH logins, restrictions for the IP address for the SSH source of connection, and SSH keyboard interactive authentication.

- Set restrictions for the IP address for the SSH source of connection

```
# ismadm security set-ssh-conf -iplimit [enable or disable]
```

- Lock settings for failed SSH logins

```
# ismadm security set-ssh-conf -userlock [enable or disable]
```

- SSH keyboard interactive authentication settings

```
# ismadm security set-ssh-conf -keyboard [enable or disable]
```

Status display for SSH logins

The SSH login history for each user within the certain period is displayed. If you cannot log in with the correct password and your login history is remained, the system is locked. Use the "ismadm security reset-ssh-userlock" command to unlock the system.

```
# ismadm security show-ssh-loginfail
```

The user name and following items are output.

Table 4.5 Description on the command output

Item	Description
When	Login date and time
Type	Connection type ("RHOST" fixed)
Source	Connection source
Valid	Displays "V" or "I" (internal information)

Disabling the user lock for failed SSH logins

You can disable the lock for users that have been locked out due to failed SSH logins.

```
# ismadm security reset-ssh-userlock -user <User name>
```

You can execute this command with a hypervisor console or with a user that is not locked out and has the Administrator group Administrator role.

Adding an SSH source of connection IP address

You can add the IP address or subnet for the source you want to allow a connection for if the restrict IP address for the SSH source of connection function is enabled.

```
# ismadm security add-ssh-clientip -ip <IP address or subnet>
```

IP address example: 192.168.1.250

Subnet example: 192.168.1.0/24 [Subnet mask with bit value included]

Deleting an SSH source of connection IP address

You can delete the IP address or subnet for the source you want to allow a connection for if the restrict IP address for the SSH source of connection function is enabled.

```
# ismadm security delete-ssh-clientip [-ip <IP address or subnet>] [-all]
```

IP address example: 192.168.1.250

Subnet example: 192.168.1.0/24 [Subnet mask with bit value included]

-all specification: Deletes all

Specify either "-ip" or "-all."

Registering an SSH public key

You can register public keys in RFC 4716 or OpenSSH format. Public keys can be created with SSH tools such as Tera Term/PuTTY/OpenSSH. Create a public key for each user connecting to SSH using the following method.

- For Tera Term, use the file output by "Save public key" for the "Key Generator" function.
- For PuTTY, use the file output from the puttygen command "Save public key."
- For OpenSSH, use the "*.pub" file format output by the ssh-keygen command.

For security reasons, public keys created in RSA1 format cannot be used.

1. Rename the SSH public key file to the following file name and transfer it to ISM-VA.

File name: sshkey_<User name connecting to SSH>

Transfer destination: /Administrator/ftp

For information on how to transfer files using the GUI, refer to "[4.23 File Upload Using the GUI.](#)"

For information on how to transfer files via FTP, refer to "[2.1.2 FTP Access.](#)"

2. Log in to the console with the user that you want to register the SSH public key for and execute the command to register the SSH public key.

```
# ismadm security set-ssh-pubkey
```

Example of command execution

```
# ismadm security set-ssh-pubkey
User name      : administrator
Import key file : /Administrator/ftp/sshkey_administrator.pub
Fingerprint    : RSA 2048 SHA256:*****
Import SSH public key? [y/n]: y
Public key import succeeded.
```

Displaying an SSH public key

Log in to the console with the user that you want to display the SSH public key for and execute the command to display the SSH public key.

```
# ismadm security show-ssh-pubkey
```

Example of command execution

```
# ismadm security show-ssh-pubkey
User name      : administrator
Fingerprint    : RSA 2048 SHA256:*****
```

Deleting an SSH public key

Log in to the console with the user that has the SSH public key you want to delete and execute the command to delete the SSH public key.

```
# ismadm security delete-ssh-pubkey
```

Example of command execution

```
# ismadm security delete-ssh-pubkey
User name      : administrator
Fingerprint    : RSA 2048 SHA256:*****
Delete SSH public key? [y/n]: y
Public key delete succeeded.
```

Confirming console automatic logout settings

You can check the time (in minutes) to be automatically logged out after a certain period of inactivity, after a user logged in via SSH or hypervisor console.

```
# ismadm security show-console-timeout
```

Example of command execution

```
# ismadm security show-console-timeout
Console login timeout: 30 (minute)
```

Console automatic logout settings

You can set the time (in minutes) to be automatically logged out after a certain period of inactivity, after a user logged in via SSH or hypervisor console. The setting time is applied to the users who log in after changing the settings.

```
# ismadm security set-console-timeout -time <timeout time (minutes)>
```

Default: 30 minutes

Available range: between 2 to 60 minutes

Example of command execution

```
# ismadm security set-console-timeout -time 60
Console login timeout: 60 (minute)
```

4.26.2 Restrict ISM Communication Ports

You can modify the following settings and display the statuses.

- Restrict the IP address for the GUI/REST source of connection

You can restrict external connections to the ISM-VA GUI port (default: 25566/TCP port).

- Restrict the IP address for the Samba source of connection

You can restrict external connections to the ISM-VA 445/TCP port.

- Restrict the IP address for the FTP source of connection

You can restrict external connections to the ISM-VA 21/TCP port.

- Restrict the IP address for the TFTP source of connection

You can restrict external connections to the ISM-VA 69/UDP port.

- Restrict the IP address for the port 9213 source of connection

You can restrict external connections to the ISM-VA 9213/TCP port.

- Restrict the IP address for the SNMP trap source of connection

You can restrict external connections to the ISM-VA 162/UDP port.

- Restrict the IP address for the HTTPS data source of connection

You can restrict external connections to the ISM-VA 25613/TCP port.

- Restrict the IP address for the SSDP source of connection

You can restrict external connections to the ISM-VA 1900/UDP port.

Confirming security settings for ISM communication ports

You can confirm the IP address restriction settings for the source of connection for ISM communication ports.

- Confirm the IP address restriction for the GUI/REST source of connection

```
# ismadm security show-gui-conf
```

- Confirm the IP address restriction for the Samba source of connection

```
# ismadm security show-smb-conf
```

- Confirm the IP address restriction for the FTP source of connection

```
# ismadm security show-ftp-conf
```

- Confirm the IP address restriction for the TFTP source of connection

```
# ismadm security show-tftp-conf
```

- Confirm the IP address restriction for the port 9213 source of connection

```
# ismadm security show-svs-conf
```

- Confirm the IP address restriction for the SNMP trap source of connection

```
# ismadm security show-snmp-conf
```

- Confirm the IP address restriction for the HTTPS data source of connection

```
# ismadm security show-https-data-conf
```

- Confirm the IP address restriction for the SSDP source of connection

```
# ismadm security show-ssdp-conf
```

Example of command execution:

```
# ismadm security show-gui-conf
client ip address limitation : enable
client ip address to use : 192.168.2.20,192.168.1.0/24
```

Setting security settings for ISM communication ports

You can enable or disable the IP address restriction settings for the source of connection for ISM communication ports. If you switch between enable and disable, the setting is applied to the communication where connecting after setting is made.

- Set the IP address restriction for the GUI/REST source of connection

```
# ismadm security set-gui-conf -iplimit [enable or disable]
```

- Set the IP address restriction for the Samba source of connection

```
# ismadm security set-smb-conf -iplimit [enable or disable]
```

- Set the IP address restriction for the FTP source of connection

```
# ismadm security set-ftp-conf -iplimit [enable or disable]
```

- Set the IP address restriction for the TFTP source of connection

```
# ismadm security set-tftp-conf -iplimit [enable or disable]
```

- Set the IP address restriction for the port 9213 source of connection

```
# ismadm security set-svs-conf -iplimit [enable or disable]
```

- Set the IP address restriction for the SNMP trap source of connection

```
# ismadm security set-snmp-conf -iplimit [enable or disable]
```

- Set the IP address restriction for the HTTPS data source of connection

```
# ismadm security set-https-data-conf -iplimit [enable or disable]
```

- Set the IP address restriction for the SSDP source of connection

```
# ismadm security set-ssdp-conf -iplimit [enable or disable]
```

Adding an ISM communication port source of connection IP address

You can add the IP address or subnet for the source you want to allow a connection for if the restrict IP address for the source of connection function is enabled for ISM communication ports. You can specify multiple IP addresses or subnets separated by commas.

If the restriction settings of the IP address for the connection source is enabled (enable) in "[Setting security settings for ISM communication ports](#)" the added IP address or subnet can be connected immediately.

- Add the IP address for the GUI/REST source of connection

```
# ismadm security add-gui-clientip -ip <IP address or subnet>
```

- Add the IP address for the Samba source of connection

```
# ismadm security add-smb-clientip -ip <IP address or subnet>
```

- Add the IP address for the FTP source of connection

```
# ismadm security add-ftp-clientip -ip <IP address or subnet>
```

- Add the IP address for the TFTP source of connection

```
# ismadm security add-tftp-clientip -ip <IP address or subnet>
```

- Add the IP address for the port 9213 source of connection

```
# ismadm security add-svs-clientip -ip <IP address or subnet>
```

- Add the IP address for the SNMP trap source of connection

```
# ismadm security add-snmp-clientip -ip <IP address or subnet>
```

- Add the IP address for the HTTPS data source of connection

```
# ismadm security add-https-data-clientip -ip <IP address or subnet>
```

- Add the IP address for the SSDP source of connection

```
# ismadm security add-ssdp-clientip -ip <IP address or subnet>
```

IP address example: 192.168.1.250

Subnet example: 192.168.1.0/24 [Subnet mask with bit value included]

Deleting an ISM communication port source of connection IP address

You can delete the IP address or subnet for the source you want to allow a connection for if the restrict IP address for the source of connection function is enabled for ISM communication ports.

If the restriction settings of the IP address for the connection source is enabled (enable) in "[Setting security settings for ISM communication ports](#)", the deleted IP address or subnet can be disconnected immediately.

- Delete the IP address for the GUI/REST source of connection

```
# ismadm security delete-gui-clientip [-ip <IP address or subnet>] [-all]
```

- Delete the IP address for the Samba source of connection

```
# ismadm security delete-smb-clientip [-ip <IP address or subnet>] [-all]
```

- Delete the IP address for the FTP source of connection

```
# ismadm security delete-ftp-clientip [-ip <IP address or subnet>] [-all]
```

- Delete the IP address for the TFTP source of connection

```
# ismadm security delete-tftp-clientip [-ip <IP address or subnet>] [-all]
```

- Delete the IP address for the port 9213 source of connection

```
# ismadm security delete-svs-clientip [-ip <IP address or subnet>] [-all]
```

- Delete the IP address for the SNMP trap source of connection

```
# ismadm security delete-snmp-clientip [-ip <IP address or subnet>] [-all]
```

- Delete the IP address for the HTTPS data source of connection

```
# ismadm security delete-https-data-clientip [-ip <IP address or subnet>] [-all]
```

- Delete the IP address for the SSDP source of connection

```
# ismadm security delete-ssdp-clientip [-ip <IP address or subnet>] [-all]
```

IP address example: 192.168.1.250

Subnet example: 192.168.1.0/24 [Subnet mask with bit value included]

-all specification: Deletes all

Specify either "-ip" or "-all."

4.26.3 Settings for ISM Session Authentication

ISM session authentication is the authentications for the GUI login or the API session.

If the IP address restriction settings for ISM session authentication is enabled, access during ISM session authentication can be limited to access from the same IP address used for login.

Confirming the IP address restriction settings for ISM session authentication

You can confirm the IP address restriction settings for ISM session authentication.

```
# ismadm security show-ismauth-conf
```

Example of command execution:

```
# ismadm security show-ismauth-conf
source ip address limitation: enable
```

Changing the IP address restriction settings for ISM session authentication

You can set enable/disable of IP address restriction settings for ISM session authentication.

```
# ismadm security set-ismauth-conf -iplimit [enable or disable]
```

4.27 Port Number of Relay Route

The relay route is a communication route for iRMC login. Ports can be assigned to relay routes.

You can check the port numbers assigned to the relay route and change the assignment.

The following is the default port numbers.

Relay route number (id)	Port number (port) (default setting)
1	63000
2	63001
3	63002

4.27.1 Confirmation of Port Number of Relay Route

You can display the port number of relay route used for the iRMC login.

1. From the console, log in to ISM-VA as an administrator.

2. Execute the following command to display the port number of relay route.

```
# ismadm relayroute port-show
```

Example of command execution:

```
# ismadm relayroute port-show
id    port
1     63000
2     63001
3     63002
```

4.27.2 Change of Port Number of Relay Route

If you need to change the port number of the relay route used for iRMC login, you can change the setting by the following procedure.

The port number of relay route that can be specified is in the range between 50000 to 63999.

1. From the console, log in to ISM-VA as an administrator.
2. Execute the following command to set the relay route port.

```
# ismadm relayroute port-change -id <relay route number> -port <port number>
```

Example of command execution:

```
# ismadm relayroute port-change -id 1 -port 53000
```



Note

When you change the port number of relay route used for the iRMC login, communication with iRMC is cut off. Execute the iRMC login from the GUI again.

4.28 Creation of Client Certificate for Relay Route

The client certificate for the relay route is a certificate for relay route access issued by ISM-VA.

To use a relay route, the client certificate for the relay route must be installed on the management terminal in advance.

4.28.1 Creation of Client Certificate

The procedure for creating a client certificate for a relay route to ISM-VA is as follows.

1. From the console, log in to ISM-VA as an administrator.
2. Execute the following command to create the client certificate.
 - When creating without a password

```
# ismadm relayroute clientcert-create
```

- When creating with password

```
# ismadm relayroute clientcert-create -password
Enter Export Password: <enter password >
Verifying - Enter Export Password: <enter password for confirmation>
```

The client certificate file (PKCS #12 format: ".p12" extension) is output to:

/Administrator/ftp/relayroute/ism_relay_client.p12



Note

- Even if the relay route is configured for multiple management terminals, the client certificate is the same. It is created only once in ISM-VA.
If the client certificate is re-created by ISM-VA, the previous client certificate becomes invalid.
- If you use iPad for your device and Safari for your web browser, make sure to set a password for the client certificate.

4.28.2 Download of Client Certificate for Relay Route

The client certificate for the relay route created by ISM-VA is downloaded to the management terminal via FTP or HTTPS.

Download from FTP

You can download the following client certificate file from FTP.

/Administrator/ftp/relayroute/ism_relay_client.p12

Download from HTTPS (using curl command)

You can download the client certificate file from the following URL.

https://<IP address of ISM-VA>:25566/ism/data/export/Administrator/transfer/ism_relay_client.p12

Example of command execution: when downloading on the Linux sever that curl command is installed

```
# curl -O "https://192.168.10.20:25566/ism/data/export/Administrator/transfer/ism_relay_client.p12"
--cacert /tmp/certificate.crt
-b "X-Ism-Authorization=123456789"
```



Note

- When transferring the client certificate file via FTP, transfer the file in a binary mode.
- When using the curl command to download the client certificate file, authentication is required for HTTPS communication. For authentication operation, refer to "3.1 Authentication" in "REST API Reference Manual".

4.28.3 Installation of Client Certificate for Relay Route

You can install the downloaded client certificate on the management terminal.

The installation procedure is as follows. The procedure varies depending on the using device and web browser.

For the devices: PC, server or Windows tablet, and web browser: Microsoft Edge or Google Chrome

The procedure may vary depending on the version of the Windows OS. The following procedure is for Windows 10.

1. Double-click or double-tap the downloaded client certificate to start the Certificate Import wizard.
Select a location to save the file and select [Next]. The saving location is optional.
2. Confirm that the file name "ism_relay_client.p12" is specified in [File to Import], and select [Next].
3. For [Private key protection], enter a password and select [Next] without changing the import options.
4. In [Certificate Store], select [Automatically select the certificate store based on the type of certificate], and then select [Next].
5. In [Completing the Certificate Import Wizard], select [Finish].

For the devices: PC, server or Windows tablet, and web browser: Mozilla Firefox

The procedure may vary depending on the version of Mozilla Firefox. The following procedure is for the version 113.0 (64-bit).

1. Select [Settings] from the Mozilla Firefox menu.
2. From [Privacy & Security], select [Security] - [Certificates], and [View Certificates].

3. From [Import], select "ism_relay_client.p12" and select [Open].
4. For the client certificate with a password, enter the password in [Password Required], and select [Sign in].
5. In the [Your Certificates] tab, check that the certificate with the certificate name "ISM RELAY ROUTE CLIENT" has been added, and then select [OK].

For the devices: Android tablet, and web browser: Google Chrome

The procedure may vary depending on the Android OS version. The following procedure is for Android OS 11.

1. Tap the [Settings] icon on the Home screen.
2. Tap [Security] - [Encryption & credentials] - [Install a certificate] - [VPN & app user certificate].
3. Tap ism_relay_client.p12.
4. For the client certificate with a password, enter the password in [Extract certificate], and tap [OK].
5. Change the certificate name if necessary and tap [OK].

For the devices: iPad, and web browser: Safari

The procedure may vary depending on the iOS version. The following procedure is for iOS 13.

1. Tap the [Settings] icon on the Home screen.
2. Tap [General]-[Profile].
3. Select [Identity Certificate] and tap [Install].
4. Enter a password in [Enter your passcode], and tap [Done]. (The passcode is the code used to unlock iPad)
5. In [Warning], tap [Install]. On the screen that displays, tap [Install].
6. Enter the password in [Enter Password], and tap [Next].
7. Tap [Done].

4.28.4 Display of Client Certificate for Relay Route

You can display the client certificate created in ISM-VA.

1. From the console, log in to ISM-VA as an administrator.
2. Execute the following command to display the client certificate.

```
# ismadm relayroute clientcert-show
```

Chapter 5 Maintenance of Nodes

This chapter describes the maintenance of nodes.

5.1 Maintenance Mode

If you need 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.
Anomaly Detection	Stops Anomaly Detection.

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

Setting 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

- Execution of Enable/Disable Maintenance Mode for PRIMEQUEST: excluding PRIMEQUEST 4000 series, 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.

- For PRIMERGY CX series and PRIMEQUEST 4000 series, even if you enable/disable Maintenance Mode for the chassis, the Maintenance Mode cannot be enabled/disabled for the nodes under the chassis. Specify a node under the chassis to enable/disable Maintenance Mode.

Note that the chassis of PRIMERGY CX series and PRIMEQUEST 4000 series themselves do not have any functions, so that ISM does not suppress the processing toward the chassis. Therefore, there is no need to enable/disable Maintenance Mode for the chassis.

- Execution of 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. Check the SEL log and component information of the WebUI for each device to identify the cause of the error.

5.3 Tasks for Replacing Components

When replacing a component for a node, the procedures vary depending on the component.

Refer to the following task examples and follow the procedure for the applicable component.

Table 5.1 Replacement method for component

Replacement method	Device status	Component examples
A: Replace the hot plug component	Monitoring for the device is continued	HDD and SSD
B: Replace the component after shutting down the OS	iRMC is not stopped	LAN cards, RAID cards, and software/drivers/BIOS updates
C: Replace the component after turning off the device	iRMC is stopped, but stored in memory	Power units, FAN, and iRMC firmware updates
D: Replace the physical component	iRMC is stopped, but not stored in memory	Server devices and system boards

Work flow for replacing components

Refer to the table above for the replacement method for components (A to D).

Note: Y = Required, - = Perform as necessary

Task sequence	Location	Task for the device	Description	Replacement method			
				A	B	C	D
1	ISM	Backup the hardware settings "2.10 Backup/Restore Hardware Settings"	Get the settings of the BIOS/iRMC from the device and store them on ISM. This is effective when replacing a system board.				Y
2	ISM	Enable Maintenance Mode for the node "5.1 Maintenance Mode"	Stop ISM monitoring operations (periodic collection of node information, log collection, and anomaly detection). SNMP traps are received while Maintenance Mode is enabled, however there are no alarm notifications when they are received. Maintenance Mode settings for the node are on ISM, and the status of the device is not changed.	Y	Y	Y	-

Task sequence	Location	Task for the device	Description	Replacement method			
				A	B	C	D
3	ISM	Release profiles "2.4.2.5 Releasing and deleting profiles"	Releasing the profile resets only the Virtual IO settings for the device setting information (iRMC, BIOS, Virtual IO, and RAID settings) set in the profile. In addition, periodic profile verification is no longer performed. This is required to prevent inconsistencies between node registration information and profiles.				Y
4	ISM	Delete the registered node "2.2.4 Deletion of Datacenters/Floors/Racks/Nodes"	Remove the device from ISM monitoring. You do not need to delete the registered node when replacing a component. The goal is to reset any inconsistencies between the registration and monitoring status of the registered node. If you replace a part on a node for a PRIMERGY server and the following are the same before and after the replacement, you do not need to delete or re-register the node. - PRIMERGY model - iRMC IP address/user/password				-
5	ISM	Delete the profile "2.4.2.5 Releasing and deleting profiles"	Delete created profiles from ISM. Deleting the profile and recreating it are effective when profile settings change drastically. You must delete profiles that remain after deleting a registered node.				-
6	Device	Replace the component Refer to the maintenance manual for details on turning off the device and other operations.	The following tasks are required depending on the type of component replaced. - Shutting down and starting up the OS - Disconnecting and reconnecting the power plug Reassign the profile if the OS must be reinstalled after replacing the component.	Y	Y	Y	Y
7	Device	Set the iRMC IP address	Set the iRMC IP address on the device side. The iRMC IP address is registered on the ISM side via node registration. No setup is required on the ISM side.				Y
8	ISM	Restore the hardware settings "2.10 Backup/Restore Hardware Settings"	Restore the hardware settings from ISM using Restore if you backed up the hardware settings. You do not need to restart iRMC after restoring the hardware settings.				Y

Task sequence	Location	Task for the device	Description	Replacement method			
				A	B	C	D
9	ISM	Register the node again "2.2.1 Registration of Datacenters/ Floors/Racks/Nodes"	You must register the node again if you deleted it. You do not need to register the node again if you did not delete it.				-
10	ISM	Create the profile again "Creating profiles" "2.4.2.4 Editing and reassigning profiles"	Create the profile again or modify the settings. You must recreate any profiles you deleted. You do not need to recreate the profile if you did not delete it. Modify the settings for the profile if necessary.				-
11	ISM	Get the information for the node "2.2.1.3 Management of node information"	You must manually get the node information after replacing the component. Get the status and configuration (CPU, DIMM, OS) information for the registered device. Normally, ISM gets information from iRMC once a day for a registered device.	Y	Y	Y	Y
12	ISM	Reassign the profile "2.4.2.4 Editing and reassigning profiles"	The profile must be reassigned if it was released. Reassign the profile if there are mismatches for verification of profiles even if you did not release a profile.				Y
13	ISM	Disable Maintenance Mode for the node "5.1 Maintenance Mode"	Disable Maintenance Mode for the node if it is enabled.	Y	Y	Y	-

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

This section describes information on environmental settings and notes required to use functions of ISM.

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 Offline Update of a server or an installed PCI card

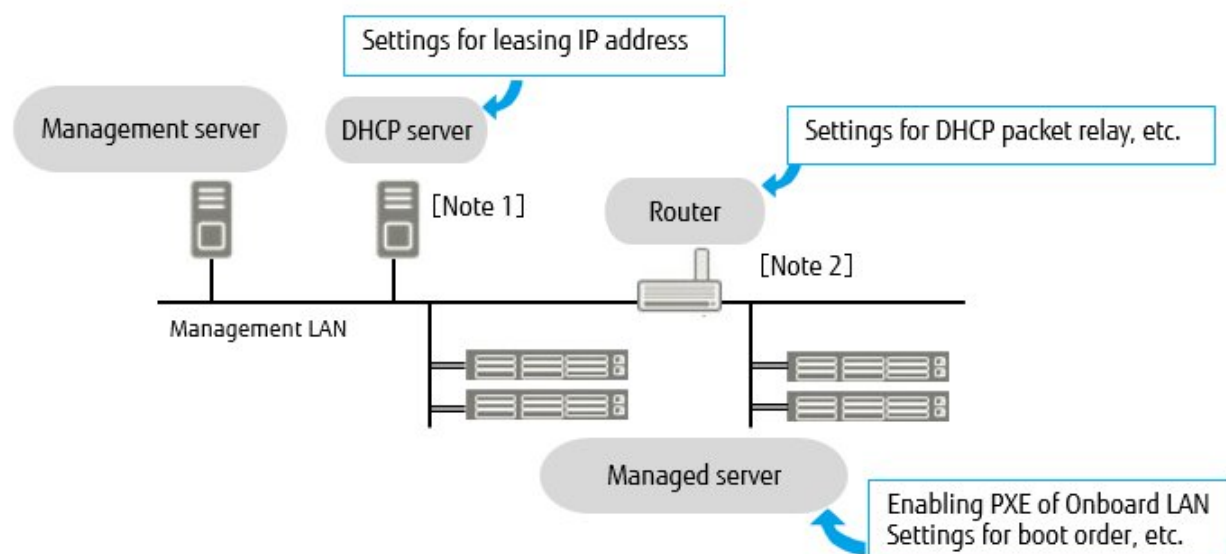
To operate PXE correctly, adequate prior preparation for managed server (node) and network configurations are required. This section provides information on the required operations for PXE boot.

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.



Note

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 specifying the LAN port to be used with "PXE Boot Port" of ISM and the LAN port is not unique in "Select Port" (by specifying a slot number or a port number), specify the LAN port in "Select MAC Address."

DHCP Server/Router

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

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

- Lease range: 192.168.1.128 to 192.168.1.159
- Lease period: eight 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 ISM-VA/allocating virtual disk(s) to user groups
- Importing the OS installation DVD (For OS installation)
- Importing the ServerView Suite Update DVD (For Office update)
- Importing the ServerView Suite DVD
- Registering managed servers in ISM

When registering in ISM, register the iRMC user with "OEM" or "Administrator" authorization.

A.1.2 Display of ETERNUS DX/AF/AB/HB Enclosures

ISM manages the various enclosures contained in ETERNUS DX/AF/AB/HB as nodes.

This section provides the required setting information to manage various enclosures.

The enclosures (child nodes) managed with ISM differ depending on the model, refer to "Table 2.4 Models in which tree structures are set between nodes" in "Operating Procedures."

Registration of enclosures

Various enclosures are automatically registered as nodes in ISM by registering the ETERNUS main unit as nodes and retrieving node information.

Details of node information of enclosures

Detailed node information for various enclosures is displayed in the detailed node information for the controller enclosure.

Status of enclosures

Status of various enclosures is different for ETERNUS AB/HB and ETERNUS DX/AF.

- For ETERNUS AB/HB, the drive enclosure status is always displayed as "Unknown." This is because the various enclosures are collectively managed by a controller enclosure. Refer to the controller enclosure node information.
- For ETERNUS DX/AF, ISM displays the status of each drive enclosure obtained from the controller enclosure. ETERNUS DX/AF must be SMI-S enabled to view the various enclosure status. If SMI-S is not enabled, the display is the same as ETERNUS AB/HB.

Deletion of enclosures

Various enclosures are deleted from a node list in the following cases:

- When a drive enclosure is disconnected from a controller enclosure, the drive enclosure is deleted from the node details after subsequent node information is retrieved.
- When the node of the controller enclosure is deleted from ISM.



Note

If ETERNUS DX900 S5 is registered as a node before ISM 2.9.0.020, you can display various enclosure information by deleting the target node and then registering it again. If this operation is not executed, only the Properties and Monitoring tabs will be displayed, and the various enclosure information of the child nodes will not be displayed.

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
```

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.

Comment	Description
--#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"> - INFORMATIONAL - MINOR - MAJOR - CRITICAL



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 an Unknown trap is 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 an 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.1.4 List of Available Port Numbers in ISM

This section describes port numbers that are used for communication by each ISM function.

Table A.1 Available port numbers for each ISM function

Function	Protocol	Available Port	Direction of Connection
SSH console access	SSH	22/tcp	Management terminal to ISM
Access to file transfer area using FTP	FTP	21/tcp	Management terminal to ISM
	FTP data	64872-65002/tcp	Management terminal to ISM
Time adjustment using an NTP server	NTP	123/udp	ISM to NTP server
Host name resolution using a DNS server	DNS	53/udp	ISM to DNS server
User management using a directory server	LDAP	389/tcp *Can be changed on ISM	ISM to directory server
	LDAPS	636/tcp *Can be changed on ISM	
Executing remote script when ISM detects an event External host OS executing the script: Red Hat Enterprise Linux SUSE Linux Enterprise Server	SSH	22/tcp *Can be changed on ISM	ISM to external host

Function	Protocol	Available Port	Direction of Connection
AlmaLinux			
Executing remote script when ISM detects an event External host OS executing the script: Windows	HTTPS	5986 *Can be changed on ISM	ISM to external host
Sending mail when ISM detects an event	SMTP	25/tcp *Can be changed on ISM	ISM to mail server
		587/tcp	
Sending or forwarding traps when ISM detects an event	SNMPTRAP	162/udp *Can be changed on ISM	ISM to external SNMP manager
Forwarding syslogs when ISM detects an event	syslog	514/udp *Can be changed on ISM	ISM to external Syslog server
Mounting an external shared directory (SMB/CIFS)	SMB/CIFS	445/tcp	ISM to SMB/CIFS server
		445/udp	
	NETBIOS	137/tcp	
		138/udp	
		139/tcp	
Mounting an external shared directory (NFS)	NFS	2049/tcp	ISM to NFS server

A.2 Details of Managed Nodes Settings

This section describes port numbers that are used in ISM and connection information that must be set on the managed nodes.

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. Set these according to your device type or environment.

The available port numbers listed are the default port numbers. The available port numbers can be changed from the node settings if the direction of the connection is from ISM to the node.

Table A.2 Available port numbers for ISM for each target device

Target Device	Function	Protocol	Available Port	Direction of Connection
PRIMERGY (RX/ CX/TX) (Except for PRIMERGY CX1430 M1, PRIMERGY RX2450 M1) PRIMEQUEST 3000B PRIMEQUEST 4000 series (Partition)	Retrieval of node information	IPMI	623/udp	ISM to node
		HTTPS	443/tcp	ISM to node
	Auto Discovery	SSDP	1900/udp	Node to ISM
	Monitoring	IPMI	623/udp	ISM to node
		HTTPS	443/tcp	ISM to node
	Trap reception	SNMP (Trap)	162/udp	Node to ISM
	CAS	HTTPS	25593/tcp *Can be changed on ISM	Node to ISM

Target Device	Function	Protocol	Available Port	Direction of Connection
	Firmware update (Online Update) (iRMC S3 not supported)	IPMI	623/udp	ISM to node
		TFTP (iRMC S4)	69/udp	Node to ISM
		TFTP data (iRMC S4)	any/udp	ISM to node
		HTTPS (iRMC S5 or later)	443/tcp	ISM to node
	Firmware update (Offline Update)	SSH	22/tcp	ISM to node
		FTP	21/tcp	Node to ISM
		FTP data	64872-65002/tcp	Node to ISM
		DHCP	67/udp	Node to ISM
		TFTP	69/udp	Node to ISM
		TFTP data	any/udp	ISM to node
		PXE	4011/udp	Node to ISM
		HTTPS	443/tcp	ISM to node
		HTTPS data	25613/tcp	Node to ISM
	Firmware update (eLCM Offline Update (SimpleUpdate)) (iRMC S5 or later)	HTTPS	25566/tcp *Can be changed on ISM	Node to ISM
		HTTPS	443/tcp	ISM to node
	Log collection	IPMI	623/udp	ISM to node
		SSH (iRMC S3 only)	22/tcp	ISM to node
		HTTPS (iRMC S4 or later)	443/tcp	ISM to node
	Profile assignment (general) [Note 1]	IPMI	623/udp	ISM to node
		HTTP	80/tcp	ISM to node
		HTTPS	443/tcp	ISM to node
	Profile assignment (only upon OS installation) [Note 2]	FTP	21/tcp	Node to ISM
		FTP data	64872-65002/tcp	Node to ISM
		DHCP	67/udp	Node to ISM
		TFTP	69/udp	Node to ISM
		TFTP data	any/udp	ISM to node
		SMB	445/tcp	Node to ISM
		PXE	4011/udp	Node to ISM
		HTTPS data	25613/tcp	Node to ISM
		ISM-original	9213/tcp	Node to ISM
		ISM-original	5001/tcp	ISM to node
PRIMERGY CX1430 M1 PRIMERGY GX2460 M1	Retrieval of node information	IPMI	623/udp	ISM to node
		HTTPS	443/tcp	ISM to node

Target Device	Function	Protocol	Available Port	Direction of Connection
PRIMERGY GX2570 M6 PRIMERGY GX2560 M7 PRIMERGY RX2450 M1	Monitoring	IPMI	623/udp	ISM to node
	Log collection	IPMI	623/udp	ISM to node
PRIMERGY GX2570 M5	Retrieval of node information	IPMI	623/udp	ISM to node
		HTTPS	8080/tcp	ISM to node
	Monitoring	IPMI	623/udp	ISM to node
	Log collection	IPMI	623/udp	ISM to node
PRIMERGY LX1430 M1	Retrieval of node information	IPMI	623/udp	ISM to node
	Monitoring	IPMI	623/udp	ISM to node
	Log collection	IPMI	623/udp	ISM to node
PRIMEQUEST 3000 series (Partition)	Retrieval of node information	SNMP	161/udp	ISM to node
		IPMI	623/udp	ISM to node
	Monitoring	SNMP	161/udp	ISM to node
		IPMI	623/udp	ISM to node
	Trap reception	SNMP (Trap)	162/udp	Node to ISM
	Firmware update	SSH	22/tcp	ISM to node
		FTP	21/tcp	Node to ISM
		FTP data	64872-65002/tcp	Node to ISM
	Log collection	SSH	22/tcp	ISM to node
		IPMI	623/udp	ISM to node
PRIMEQUEST 2000 series (Partition) PRIMEQUEST 2000B	Retrieval of node information	SNMP	161/udp	ISM to node
		IPMI	623/udp	ISM to node
	Monitoring	SNMP	161/udp	ISM to node
		IPMI	623/udp	ISM to node
	Trap reception	SNMP (Trap)	162/udp	Node to ISM
	Firmware update	SSH	22/tcp	ISM to node
		FTP	21/tcp	Node to ISM
		FTP data	64872-65002/tcp	Node to ISM
ETERNUS DX/AF (Except for ETERNUS DX900 S5 for node registered before ISM2.9.0.030)	Retrieval of node information	SNMP	161/udp	ISM to node
		SSH	22/tcp	ISM to node
	Monitoring	SNMP	161/udp	ISM to node
		SMI-S [Note 3]	5989/tcp	ISM to node
	Trap reception	SNMP (Trap)	162/udp	Node to ISM
	Firmware update	SSH	22/tcp	ISM to node
		FTP	21/tcp	Node to ISM
		FTP data	64872-65002/tcp	Node to ISM
	Log collection	SSH	22/tcp	ISM to node
		FTP	21/tcp	Node to ISM

Target Device	Function	Protocol	Available Port	Direction of Connection
		FTP data	64872-65002/tcp	Node to ISM
	Profile assignment	SSH	22/tcp	ISM to node
ETERNUS NR (NetApp) ETERNUS HX/AX ETERNUS AC	Retrieval of node information	SNMP	161/udp	ISM to node
		SSH	22/tcp	ISM to node
	Monitoring	SNMP	161/udp	ISM to node
		HTTPS	443/tcp	ISM to node
	Trap reception	SNMP (Trap)	162/udp	Node to ISM
	Log collection	SSH	22/tcp	ISM to node
		HTTPS	80/tcp	ISM to node
ETERNUS AB/HB	Retrieval of node information	SNMP	161/udp	ISM to node
		HTTPS	443/tcp	ISM to node
	Monitoring	HTTPS	443/tcp	ISM to node
	Log collection	HTTPS	443/tcp	ISM to node
ETERNUS CS800 S7 ETERNUS CS800 M1 ETERNUS LT ETERNUS DX900 S5 (for node registered before ISM2.9.0.030)	Retrieval of node information	SNMP	161/udp	ISM to node
	Monitoring	SNMP	161/udp	ISM to node
SR-X	Retrieval of node information	SSH	22/tcp	ISM to node
		SNMP	161/udp	ISM to node
	Monitoring	SNMP	161/udp	ISM to node
	Trap reception	SNMP (Trap)	162/udp	Node to ISM
	Firmware update	FTP	21/tcp	ISM to node
		FTP data	any/tcp	ISM to node
		SSH	22/tcp	ISM to node
	Log collection	SSH	22/tcp	ISM to node
	Profile assignment	SSH	22/tcp	ISM to node
	VLAN/Link Aggregation settings	SSH	22/tcp	ISM to node
SR-S	Retrieval of node information	SSH	22/tcp	ISM to node
		SNMP	161/udp	ISM to node
	Monitoring	SNMP	161/udp	ISM to node
	Trap reception	SNMP (Trap)	162/udp	Node to ISM
	Log collection	SSH	22/tcp	ISM to node
	VLAN/Link Aggregation settings	SSH	22/tcp	ISM to node
PSWITCH 2048 T/PSWITCH 2048 P	Retrieval of node information	SSH	22/tcp	ISM to node
		SNMP	161/udp	ISM to node

Target Device	Function	Protocol	Available Port	Direction of Connection
	Auto Discovery	SSDP	1900/udp	Node to ISM
	Monitoring	SNMP	161/udp	ISM to node
	Trap reception	SNMP (Trap)	162/udp	Node to ISM
	Firmware update	FTP	21/tcp	Node to ISM
		FTP data	64872-65002/tcp	Node to ISM
		SSH	22/tcp	ISM to node
	Log collection	SSH	22/tcp	ISM to node
	Profile assignment	SSH	22/tcp	ISM to node
	VLAN/Link Aggregation settings	SSH	22/tcp	ISM to node
VDX	Retrieval of node information	SSH	22/tcp	ISM to node
		SNMP	161/udp	ISM to node
	Monitoring	SNMP	161/udp	ISM to node
	Trap reception	SNMP (Trap)	162/udp	Node to ISM
	Firmware update	SSH	22/tcp	ISM to node
		FTP	21/tcp	Node to ISM
		FTP data	64872-65002/tcp	Node to ISM
	Log collection	SSH	22/tcp	ISM to node
		FTP	21/tcp	Node to ISM
		FTP data	64872-65002/tcp	Node to ISM
	Profile assignment	SSH	22/tcp	ISM to node
	VLAN/Link Aggregation settings	SSH	22/tcp	ISM to node
Catalyst	Retrieval of node information	SSH	22/tcp	ISM to node
		SNMP	161/udp	ISM to node
	Monitoring	SNMP	161/udp	ISM to node
	Trap reception	SNMP (Trap)	162/udp	Node to ISM
	Firmware update	SSH	22/tcp	ISM to node
		FTP	21/tcp	Node to ISM
		FTP data	64872-65002/tcp	Node to ISM
	Log collection	SSH	22/tcp	ISM to node
Nexus series	Retrieval of node information	SSH	22/tcp	ISM to node
		SNMP	161/udp	ISM to node
	Monitoring	SNMP	161/udp	ISM to node
	Trap reception	SNMP (Trap)	162/udp	Node to ISM
	Firmware update	SSH	22/tcp	ISM to node
		SFTP [Note 1]	22/tcp	ISM to node
		TFTP	69/udp	Node to ISM
		TFTP data	any/udp	ISM to node

Target Device	Function	Protocol	Available Port	Direction of Connection
	Log collection	SSH	22/tcp	ISM to node
Juniper QFX/EX	Retrieval of node information	SSH	22/tcp	ISM to node
	Monitoring	SNMP	161/udp	ISM to node
	Log collection	SSH	22/tcp	ISM to node
	Trap	SNMP (Trap)	162/udp	Node to ISM
Arista 7000 Family	Retrieval of node information	SSH	22/tcp	ISM to node
	Monitoring	SNMP	161/udp	ISM to node
	Trap reception	SNMP (Trap)	162/udp	Node to ISM
CFX2000F/R	Retrieval of node information	SSH	22/tcp	ISM to node
		SNMP	161/udp	ISM to node
	Monitoring	SNMP	161/udp	ISM to node
	Trap reception	SNMP (Trap)	162/udp	Node to ISM
	Firmware update	FTP	21/tcp	ISM to node
		FTP data	any/tcp	ISM to node
		SSH	22/tcp	ISM to node
	Log collection	SSH	22/tcp	ISM to node
	Profile assignment	SSH	22/tcp	ISM to node
	Trap reception	SNMP (Trap)	162/udp	Node to ISM
Brocade FC Switch	Retrieval of node information	SSH	22/tcp	ISM to node
		SNMP	161/udp	ISM to node
	Monitoring	SNMP	161/udp	ISM to node
	Trap reception	SNMP (Trap)	162/udp	Node to ISM
	Log collection	SSH	22/tcp	ISM to node
		SCP	22/tcp	Node to ISM
ExtremeSwitching X440/460-G2	Retrieval of node information	SSH	22/tcp	ISM to node
	Monitoring	SNMP	161/udp	ISM to node
	Trap reception	SNMP (Trap)	162/udp	Node to ISM
	Firmware update	SSH	22/tcp	ISM to node
		TFTP	69/udp	Node to ISM
		TFTP data	any/udp	ISM to node
	VLAN/Link Aggregation settings	SSH	22/tcp	ISM to node
Schneider Electric Switched Rack PDU /Schneider Electric Smart-UPS	Retrieval of node information	SNMP	161/udp	ISM to node
	Monitoring	SNMP	161/udp	ISM to node
	Trap reception	SNMP (Trap)	162/udp	Node to ISM

[Note 1]: Used to communicate with the BMC (iRMC).

[Note 2]: Used to communicate with the onboard LAN or LAN card.

[Note 3]: Used to communicate with the controller enclosure to obtain drive enclosure status.

Table A.3 Available port numbers for ISM for each target OS

Target OS	Function	Protocol	Available Port	Direction of Connection
Windows	Retrieval of OS information	HTTPS	5986/tcp	ISM to node
	Monitoring	HTTPS	5986/tcp	ISM to node
	Firmware update (Online Update)	HTTPS	5986/tcp	ISM to node
		FTPS	21/tcp	Node to ISM
		FTPS data	64872-65002/tcp	Node to ISM
	Log collection	HTTPS	5986/tcp	ISM to node
		FTPS	21/tcp	Node to ISM
		FTPS data	64872-65002/tcp	Node to ISM
Red Hat Enterprise Linux/ SUSE Linux Enterprise Server	Retrieval of OS information	SSH	22/tcp	ISM to node
	Monitoring	SSH	22/tcp	ISM to node
	Firmware update (Online Update)	SSH	22/tcp	ISM to node
	Log collection	SSH	22/tcp	ISM to node
AlmaLinux	Retrieval of OS information	SSH	22/tcp	ISM to node
	Monitoring	SSH	22/tcp	ISM to node
	Log collection	SSH	22/tcp	ISM to node
VMware ESXi	Retrieval of OS information	HTTPS	443/tcp	ISM to node
			5989/tcp	ISM to node
	Monitoring	HTTPS	443/tcp	ISM to node
	Log collection	HTTPS	443	ISM to node

Table A.4 Available port numbers for ISM for target Cloud Management Software

Target Cloud Management Software	Function	Protocol	Available Port	Direction of Connection
vCenter	Retrieval of information	HTTPS	443/tcp	ISM to node
SystemCenter	Retrieval of information	HTTPS	5986/tcp	ISM to node
FailOverCluster	Retrieval of information	HTTPS	5986/tcp	ISM to node
KVM	Retrieval of information	SSH	22/tcp	ISM to node
OpenStack	Retrieval of information	HTTPS	5001/tcp	ISM to node
		SSH	22/tcp	ISM to node

A.2.2 Details of Node Settings

To manage nodes with ISM, you must set the connection information on the node side. This section provides the required connection information for settings.

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.

Table A.5 Available devices and connection information

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) M6 or earlier (Except for PRIMERGY CX1430 M1, PRIMERGY RX 2450 M1, PRIMERGY 1WAY M6, and PRIMERGY RX1440 M2/RX2450 M2)	Y	-	-	- [Note 4]
PRIMERGY(RX/CX/TX) M7 PRIMERGY 1WAY M6 PRIMERGY RX1440 M2 PRIMERGY RX2450 M2	- [Note 6]	-	-	Y
PRIMERGY CX1430 M1 PRIMERGY RX 2450 M1	Y	-	-	Y
PRIMERGY GX	Y	-	-	Y
PRIMERGY LX	Y	-	-	-
PRIMEQUEST 2000 series (Partition)	Y	Y	Y	-
PRIMEQUEST 2000B	Y	Y	Y	-
PRIMEQUEST 3000 series (Partition)	Y	Y	Y	-
PRIMEQUEST 3000B	Y	-	-	- [Note 4]
PRIMEQUEST 4000 series (Partition)	- [Note 6]	-	-	Y
ETERNUS DX/AF (Except for ETERNUS DX900 S5 for node registration before ISM2.9.0.030)	-	Y	Y	- [Note 5]
ETERNUS NR ETERNUS HX/AX ETERNUS AC	-	Y	Y	Y
ETERNUS AB/HB	-	-	Y	Y
ETERNUS CS800 S7 ETERNUS CS800 M1 ETERNUS LT ETERNUS DX900 S5 (for node registration before ISM2.9.0.030)	-	-	Y	-
SR-X	-	Y	Y	-
PSWITCH 2048P/T PSWITCH 4032P	-	Y	Y	-

Node	Connection Information			
	IPMI Account [Note 1]/ Password	SSH Account/ Password	Information Required to Enter for SNMP [Note 2]	HTTPS Account/ Password
VDX	-	Y	Y	-
Brocade FC Switch	-	Y	Y	-
Cisco Catalyst	-	Y	Y	-
Cisco Nexus	-	Y	Y	-
Arista 7000 Family	-	Y	Y	-
Juniper QFX/EX	-	Y	Y	-
CFX2000F/R	-	Y	Y	-
Schneider Electric Switched Rack PDU	-	-	Y	-
SchneiderElectric Smart-UPS	-	-	Y	-
SR-S	-	Y	Y	-
ExtremeSwitching X440/460-G2	-	Y	Y	-

Note: Y = Required, - = Not required

For the models which are confirmed for operation, refer to "Support Matrix."

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

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

Select [DOWNLOADS] and select the target operating system.

The reference procedures are subject to change without notice.

[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.

[Note 5]: The account/password will be the same as its SSH.

[Note 6]: You can only specify IPMI port number. The account/password will be the same as its HTTPS.

Required settings for Manual Discovery

To execute Manual Discovery on the server of PRIMERGY 2/4/8WAY M7 or later, PRIMERGY 1WAY M6 or later, and PRIMERGY RX1440/2450 M2 or later, enable SSDP in the iRMC web UI.

Execute the following step to check the settings.

From [Services] - [SSDP], check that [Enable SSDP] is selected.

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] - select the [Redfish Enabled] checkbox.
2. [User Management] - [iRMC S4 User Management] - [IPMI Privileges/Permissions] - change the box of [Redfish Role] to Administrator.

[PRIMERGY GX2460 M1]

- Change the default password for the BMC fixed user (root), and specify the changed password during the node registration.
- Change the default password for HTTPS fixed user (Administrator), and specify the changed password during the node registration.

[SR-X]

Enable LLDP settings.

[VDX]

- Enable LLDP settings.
- Set the IP address of the management LAN port for each switch.

[Brocade FC switch]

- Disable AG mode.
- Enable SW-MIB settings.

Example of command execution:

```
snmpconfig --enable mibCapability -mib_name SW-MIB
```

[Arista 7000 Family]

Enable LLDP settings.

[ETERNUS DX/AF] (Except for node registration of ETERNUS DX900 S5 before ISM2.9.0.030)

- 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.
- Enable SMI-S

[ETERNUS NR1000]

The cluster management IP and the node management IP should be configured on the same network segment.

[ETERNUS NR/AX/HX/AC]

Add the user account that can log in with HTTPS password authentication.

[PRIMEQUEST 2000/3000 series (Partition), PRIMEQUEST 2000B]

- 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. The access privileges must be administrator or CE.
- 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.

[PRIMEQUEST 4000 series (Partition)]

For ISM HTTPS account settings, use the account set for each PRIMEQUEST partition.

[ExtremeSwitching X440/460-G2]

- Enable LLDP settings.
- Create an SSH account with Admin privileges and set up the account when you register the node.

Required settings for notification

Execute 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.

Supported devices whose Engine ID is automatically input when you select them as a target node in Trap Reception settings are as follows.

Table A.6 Available devices

Node	Availability of Automatic input of Engine ID
PRIMERGY(RX/CX/TX) (except for PRIMERGY CX1430 M1)	Y
PRIMERGY CX1430 M1	-
PRIMERGY GX	
PRIMERGY LX	-
PRIMEQUEST 2000 series (Partition)	-
PRIMEQUEST 2000B	Y
PRIMEQUEST 3000 series (Partition)	Y
PRIMEQUEST 3000B	Y
PRIMEQUEST 4000 series (Partition)	Y
ETERNUS DX/AF	Y
ETERNUS NR ETERNUS HX/AX ETERNUS AC	-
ETERNUS AB/HB	-
SR-X	Y [Note 1]
PSWITCH 2048P/T PSWITCH 4032P	Y
VDX	Y
Brocade FC Switch	Y
Cisco Catalyst	Y
Cisco Nexus	Y
Juniper QFX/EX	Y
CFX2000F/R	Y [Note 1] [Note 2]
Schneider Electric Switched Rack PDU	-
SchneiderElectricSmart-UPS	-

Note: Y = Supported, - = Not supported

[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.

- 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 all fabrics managed with ISM.

A.3 Details of Other Settings for Node Operation

This section describes the details of other settings for managed nodes.

A.3.1 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. In addition, 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.7 General standards for firmware update time

Target of Firmware Update	Standard Time/Unit	Note
iRMC in PRIMERGY Firmware update	Online update 15 to 30 min.	
	Offline update 20 to 40 min.	If the server is set to be turned ON after the firmware is assigned, it takes an additional 15 minutes.
BIOS in PRIMERGY Firmware update	Online update 5 to 10 min.	To assign firmware, you must take into account the extra time for powering the server ON/OFF.
	Offline update 20 to 40 min.	If the server is set to be turned ON after the firmware is assigned, it takes an additional 15 minutes.
BMC of PRIMERGY GX Firmware update	Offline update 15 to 30 min.	After the firmware update, the BMC and BIOS settings are initialized on the server side, so additional time to reconfigure the settings is needed.
BIOS of PRIMERGY GX Firmware update	Offline update 15 to 30 min.	
iRMC in PRIMEQUEST 3800B Firmware update	Online update 10 to 20 min.	
BIOS in PRIMEQUEST 3800B Firmware update	Online update 5 to 15 min.	To assign firmware, you must take into account the extra time for powering the server ON/OFF.
PRIMEQUEST 2000/3000 series (Partition) Firmware update	70 to 130 min.	
PRIMEQUEST 4000 series (Partition) Firmware update	70 to 130 min.	
Network switch SR-X Firmware update	2 to 10 min.	
Fabric switch CFX2000R/F, converged fabric switch blade Firmware update	10 to 20 min.	
Converged switch VDX Firmware update	15 to 30 min.	

Target of Firmware Update	Standard Time/Unit	Note
Converged switch X440/460-G2 Firmware update	10 to 20 min	
PSWITCH 2048P/T, PSWITCH 4032P Firmware update	20 to 30 min.	
Cisco Systems Nexus series Firmware update	30 to 50 min.	
Cisco Systems Catalyst series Firmware update	10 to 20 min.	
PCI card Firmware update	Online update 10 to 20 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 20 to 40 min.	The time noted in the left is the time taken per card.
ETERNUS DX/AF series Firmware update	10 to 60 min.	When a unified environment exists and multiple controller enclosures are installed, the update time will be longer.

A.3.2 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)	
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

Table A.8 Capacity for Archived Logs of general standard for one generation per node

Log Collection Target			Standard Capacity	
Hardware	Server	PRIMERGY	1 KB	
		PRIMEQUEST 3000B	1 KB	
		PRIMEQUEST 4000 series (Partition)	50 KB	
	Chassis	PRIMEQUEST 3000 series (Partition)	50 KB	
	Switch	SR-X	50 KB	
		CFX	100 KB	
		PSWITCH 2048P/T PSWITCH 4032P	350 KB	
		VDX	50 MB	
		Cisco Catalyst	1 MB	
		Cisco Nexus	10 MB	
		Juniper QFX/EX	1 MB	
		SR-S	50 KB	
		Brocade FC 7810 Brocade FC G630/G720	100 MB	
		Storage	ETERNUS DX/AF ETERNUS DX900 S5 (for node registered with ISM2.9.0.030 or later)	10 MB
			ETERNUS NR/AX/HX (Ontap) Cluster ETERNUS AC (Ontap) Cluster	100 KB
	ETERNUS NR (Ontap) Chassis (For some types)		500 MB	
	ETERNUS AB/HB		80 MB	
	Operating system	Windows		5 MB
		Linux		5 MB
		VMware ESXi		3 MB
	ServerView Suite	ServerView Agents		Windows: 10 MB
ServerView Agentless Service		Linux: 80 MB		
ServerView RAID Manager				

Table A.9 Capacity for Node Logs of general standard for 30 days' worth per node

Log Collection Target			Standard Capacity for Node Logs	
			Data for download	Data for log search
Hardware	Server	PRIMERGY (except for CX1430 M1)	50 KB	500 KB

Log Collection Target			Standard Capacity for Node Logs	
			Data for download	Data for log search
		PRIMEQUEST 3000B	50 KB	500 KB
		PRIMEQUEST 4000 series (Partition)	50 KB	500 KB
	Chassis	PRIMEQUEST 3000 series (Partition)	50 KB	500 KB
	Switch	SR-X	100 KB	1 MB
		CFX	100 KB	1 MB
		PSWITCH 2048P/T PSWITCH 4032P	150 KB	1 MB
		VDX	100 KB	1 MB
		Cisco Catalyst	50 KB	500 KB
		Cisco Nexus	50 KB	500 KB
		SR-S	100 KB	1 MB
	Storage	ETERNUS DX/AF ETERNUS DX900 S5 (for node registered with ISM2.9.0.030 or later)	100 KB	1 MB
		ETERNUS NR/AX/HX (Ontap) Cluster	200 KB	2 MB
		ETERNUS AC (Ontap) Cluster		
Operating system	Windows		1 MB	15 MB
	Linux		1 MB	15 MB
	VMware ESXi		4 MB	50 MB

A.3.3 Changing a Protocol to Be Used for Firmware Updates

For Nexus Series, you can change the protocol to be used for firmware updates.

Available protocols for the setting are TFTP and SFTP. The initial setup value is TFTP.

The current setting can be checked with the following command.

```
# ismadm security show-protocol -item nexus-fwup
```

To change the setting, use the following command.

```
# ismadm security set-protocol -item nexus-fwup -value <Protocol to be used>
```

Example for setting SFTP as the protocol to be used for firmware updates:

```
# ismadm security set-protocol -item nexus-fwup -value SFTP
```

Example for setting TFTP as the protocol to be used for firmware updates:

```
# ismadm security set-protocol -item nexus-fwup -value TFTP
```

Appendix B Settings for Monitoring Target OS and Cloud Management Software

To manage OS/Cloud Management Software by using ISM, you must execute settings on the OS/Cloud Management Software side. This chapter provides the required information for the settings.

B.1 List of Settings Required per Monitoring Target OS/Cloud Management Software

To use the display of the virtual machine information, device information (OS information and disk volume), Log Management (OS log collection), and firmware update (Online PCI card) from ISM, you must execute settings for each OS/cloud management software. Change the settings according to the tables shown below.

B.1.1 Required Settings per Monitoring OS

Note: Y = Settings required, N = Settings not required, - = Not applicable

OS	Service		Security		Domain	
	sshd	WinRM	Firewall	PowerShell	SPN	ISM-VA Settings
Windows Server	-	Y	Y	Y	Y	Y
Red Hat Enterprise Linux	Y	-	N	-	-	Y
SUSE Linux Enterprise Server	Y	-	Y	-	-	Y
AlmaLinux	Y	-	N	-	-	Y
VMware ESXi	-	-	-	-	-	Y
Azure Stack HCI	-	Y	Y	Y	Y	Y

For details on the required settings for each OS, refer to the following sections.

- [B.2 Setting Procedure for Monitoring Targets \(OS: Windows\)](#)
- [B.3 Setting Procedure for Monitoring Targets \(OS: Red Hat Enterprise Linux\)](#)
- [B.4 Setting Procedure for Monitoring Targets \(OS: SUSE Linux Enterprise Server\)](#)
- [B.5 Setting Procedure for Monitoring Targets \(OS: AlmaLinux\)](#)
- [B.6 Setting Procedure for Monitoring Targets \(OS: VMware ESXi\)](#)
- [B.7 Setting Procedure for Monitoring Targets \(OS: Azure Stack HCI\)](#)

B.1.2 Required Settings per Monitoring Cloud Management Software

Note: Y = Settings required, N = Settings not required, - = Not applicable

Cloud Management Software		Settings for each host/ virtual machine		Domain		
		sshd	WinRM	SPN	ISM-VA Settings	Kerberos delegation configuration
vCenter Server	5.5 or later	-	-	-	Y	-
Microsoft Failover Cluster	Windows Server 2012 or later	-	Y	Y	Y	Y

Cloud Management Software		Settings for each host/ virtual machine		Domain		
		sshd	WinRM	SPN	ISM-VA Settings	Kerberos delegation configuration
Microsoft Failover Cluster (Azure Stack HCI)	20H2 or later	-	Y	Y	Y	Y
Microsoft System Center	2012 or later	-	Y	Y	Y	Y
KVM Red Hat		Y	-	-	Y	Y
KVM SUSE Linux Enterprise		Y	-	-	Y	Y
OpenStack		Refer to " B.12 Setting Procedure for Monitoring Targets (Cloud Management Software: OpenStack) ."				

For details on required settings for the cloud management software, refer to the following.

- [B.8 Setting Procedure for Monitoring Targets \(Cloud Management Software: vCenter Server\)](#)
- [B.9 Setting Procedure for Monitoring Targets \(Cloud Management Software: Microsoft Failover Cluster\)](#)
- [B.10 Setting Procedure for Monitoring Targets \(Cloud Management Software: Microsoft System Center\)](#)
- [B.11 Setting Procedure for Monitoring Targets \(Cloud Management Software: KVM\)](#)
- [B.12 Setting Procedure for Monitoring Targets \(Cloud Management Software: OpenStack\)](#)
- [B.13 Setting Procedure for Monitoring Targets \(Cloud Management Software: Microsoft Failover Cluster \(Azure Stack HCI\)\)](#)

B.1.3 Precautions When Setting a Monitoring Target OS and Cloud Management Software

- To monitor a target server, you must register the OS information, with a user account that has administrator privileges.
- To manage Emulex LAN/FC/CNA cards mounted on Windows/Linux, Emulex OneCommand Manager CLI must be already installed on the OS of the target server.
- To manage the QLogic FC card mounted on Windows/Linux, QLogic QConvergeConsole CLI must be already installed on the OS of a target server.
- Use the latest Emulex OneCommand Manager CLI or QLogic QConvergeConsole CLI. Apply the latest drivers for LAN/FC/CNA cards.
- To manage LAN/FC/CNA card mounted on Linux, the pciutils and ethtool package must be already installed on the OS of the target server.
- To monitor the performance of the disk speed, network speed, CPU utilization rate per CPU core of Linux, and Anomaly Detection for physical servers, the sysstat package must be already installed on the OS of the target server.
- To collect Linux operating system logs or ServerView Suite logs, a zip package must be already installed on the OS of the target server.
Also, to collect the operating system logs, a syslog demon such as rsyslog package must be already installed on the OS of the target server.
- To manage OS with a general user account of Linux, a sudo package must be already installed on the OS of the target server.
- After having changed the domain user password from Active Directory, change the password in ISM.
- To use the domain user account correctly, the ISM time must be aligned with the target server.

B.2 Setting Procedure for Monitoring Targets (OS: Windows)

ISM uses WS-Management protocol for the monitoring target devices on which Windows Server is installed. For the communication method, Https Protocol + Basic authentication is used. The following are the required settings.

- [B.2.1 Confirmation on Starting WinRM Service](#)
- [B.2.2 Settings for WinRM Service](#)
- [B.2.3 Opening the Firewall Port](#)
- [B.2.4 Execution Policy Change for Windows PowerShell](#)
- [B.2.5 Settings When Using a Domain User Account](#)

B.2.1 Confirmation on Starting WinRM Service

1. Open the command prompt as an administrator and execute the following command to check that WinRM service has started.

```
>sc query winrm
```

2. Check the following results and confirm that the "STATE" is "RUNNING."

```
TYPE                : 20 WIN32_SHARE_PROCESS
STATE               : 4 RUNNING
                   (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
WIN32_EXIT_CODE     : 0 (0x0)
SERVICE_EXIT_CODE : 0 (0x0)
CHECKPOINT          : 0x0
WAIT_HINT           : 0x0
```

3. If the WinRM service has not started, execute the following command to start WinRM service.

```
>sc start winrm
```

4. Set the WinRM service to be delayed-auto-started (delayed-auto).

```
>sc config winrm start=delayed-auto
```

B.2.2 Settings for WinRM Service

Settings for WinRM Service



.....

Since Basic authentication is not allowed in the initial settings, you must set the service to allow Basic authentication.

Execute the following command.

```
>winrm set winrm/config/service/Auth @{Basic="true"}
```

.....

To use https communication, communication with Basic authentication is encrypted.

1. Open the command prompt as an administrator and execute the following command.

```
>winrm quickconfig
```

The settings are already complete if the message "WinRM service is already running on this machine. WinRM is already set up for remote management on this computer." is displayed. In this case, proceed to "[Settings for Https Communication](#)."

2. Enter "y," and then press the [Enter] key.

```
WinRM service is already running on this machine.
WinRM is not set up to allow remote access to this machine for management.
The following changes must be made:
```

```
Configure LocalAccountTokenFilterPolicy to grant administrative rights remotely to local users.
Make these changes [y/n]? y
```

The following message is displayed.

```
WinRM has been updated for remote management.

Configured LocalAccountTokenFilterPolicy to grant administrative rights remotely to local users.
```

3. If the OS of a target server is Windows Server 2008 R2, execute the following command to increase the numerical value of MaxConcurrentOperationsPerUser depending on the type and the number of cards.

```
>winrm set winrm/config/Service @{MaxConcurrentOperationsPerUser="numerical value"}
```

Example: In the case where the above value is set as 1500 (1500 is recommended because 1500 is set by default in Windows Server 2012/2012R2.)

```
>winrm set winrm/config/Service @{MaxConcurrentOperationsPerUser="1500"}
```

Settings for Https Communication

To establish https communication, you must set a certificate.

1. Preparation of required tools

Two tools are required for creating a certificate. You can create the certificate without depending on the execution environment.

- .NET Framework 4.5 or later (Download site)
<https://www.microsoft.com/en-us/download/details.aspx?id=30653>
- Windows Software Development Kit (Download site)
<https://developer.microsoft.com/en-us/windows/downloads/windows-sdk/>



- Check the requirements for the Windows Software Development Kit in the above URL for supported OSes. When installing OS of other than mentioned, install the appropriate Windows Software Development Kit.
- Windows Software Development Kit includes two tools required for creating the certificate.
 - Certificate creation tool (makecert.exe)
[https://msdn.microsoft.com/en-us/library/bfskty3\(v=vs.80\).aspx](https://msdn.microsoft.com/en-us/library/bfskty3(v=vs.80).aspx)
 - Personal information exchange file creation tool (pvk2pfx.exe)
[https://msdn.microsoft.com/en-us/library/windows/hardware/ff550672\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/hardware/ff550672(v=vs.85).aspx)

2. Creating certificates

Use the certificate creation tool and personal information exchange file creation tool to create the following three files:

- CER file (Certificate)
- PVK file (Private key file)
- PFX file (Service certificate)

For more detailed procedure for creating certificates, refer to the following URL.

<https://msdn.microsoft.com/en-us/library/ff699202.aspx>

a. Creating a certificate and private Key files

When creating the certificate and private key files, you must execute commands depending on the environment of a target server.

The following is a command example when the server name of a target server is set as "192.168.10.10" and the effective period of the certificate is set to March 30th, 2017.

```
>makecert.exe -r -pe -n "CN=192.168.10.10" -e 03/30/2017 -eku 1.3.6.1.5.5.7.3.1 -ss My  
-sr localMachine -sky exchange <certificate file name.cer> -sv <private key file name.pvk>
```

For detailed settings on the certificate configuration, refer to the following URL.

[https://technet.microsoft.com/en-us/library/ms186362\(v=sql.105\).aspx](https://technet.microsoft.com/en-us/library/ms186362(v=sql.105).aspx)

b. Creating a service certificate

Execute the following command.

```
>pvk2pfx.exe -pvk <private key file name.pvk> -spc <certificate file name.cer> -pfx <service  
certificate file name.pfx>
```

3. Registering a certificate and a service certificate

Open the Certificate Snap-In and register the certificate created above in Step 2.

- a. Execute mmc.exe on a target server.
- b. From [File], select [Add and Remove Snap-In].
- c. From [Available Snap-in], select "Certificate" to [Add].
- d. Select "Computer Account," and then select [Next] - [Finish].
- e. Select [OK].

4. Registering an SSL certificate

Register <certificate file name.cer> with the Trusted Root Certificate Authority.

- a. From [Console Root] - [Certificates (Local Computer)], right-click on [Trusted Root Certificate Authority].
- b. From [ALL Tasks] - [Import], select <certificate file name.cer> file, and finish the "Certificate Import" wizard.
- c. Select [Console Root] - [Certificate (Local Computer)] - [Trusted Root Certificate Authority] - [Certificate] in sequence, and confirm if "Issued to" and "Issued by" are the server names specified as CN, and "Authentication Purpose" is specified as "Server Authentication."

5. Registering SSL certificate

Register <service certificate file name.pfx> in "personal."

- a. From [Console Root] - [Certificate (Local Computer)], right-click on [Personal].
- b. From [All Tasks] - [Import], select <service certificate file name.pfx>, and finish the "Certificate Import" wizard.
- c. From [Console Root] - [Certificate (Local Computer)], select [Personal] in sequence, and confirm if "Issued to" and "Issued by" are the server name specified as CN, and "Authentication Purpose" is specified as "Server Authentication."

Register the Thumbprint Described on the Certificate to WinRM Service

1. Checking Thumbprint

The following shows how to check if the certificate is saved in LocalMachine\my.

- a. Start PowerShell from a command prompt.
- b. Check the Thumbprint. Execute the following command.

```
>ls cert:LocalMachine\my
```

The following is displayed.

```
PS C:\Windows\system32> ls cert:LocalMachine\my

Directory: Microsoft.PowerShell.Security\Certificate::LocalMachine\my
Thumbprint                                     Subject
-----
1C3E462623BAF91A5459171BD187163D23F10DD9      CN=192.168.10.10
```

2. Registering the Thumbprint described on the certificate with WinRM Listener.

Finish Powershell and execute the following command. A space must be entered between "HTTPS" and "@."

```
>winrm create winrm/config/listener?Address=*&Transport=HTTPS @{Hostname="<CN Name that was
specified above in step (4)Creating a Certificate and Private Key
Files>";CertificateThumbprint="<created certificate thumbprint>"}
```

3. Checking the registration of WinRM Listener

Execute the following command.

```
>winrm get winrm/config/listener?Address=*&Transport=HTTPS
```

If the command result as shown below is returned, WinRM Listener is successfully registered.

```
Listener
  Address = *
  Transport = HTTPS
  Port = 5986
  Hostname = 192.168.10.10
  Enabled = true
  URLPrefix = wsman
  CertificateThumbprint = 1C3E462623BAF91A5459171BD187163D23F10DD9
  ListeningOn = 192.168.10.10, 127.0.0.1, ::1, 2001:258:8402:200:bd8a:1c1:c50d
:8704, fe80::5efe:192.168.10.10%13, fe80::bd8a:1c1:c50d:8704%12
```

B.2.3 Opening the Firewall Port

You must open the port that you have set up in the above WinRM Listener, so that WinRM services can accept requests. The default port number of https communication is 5986.

For Windows Server 2012 / 2012R2 / 2016 / 2019 / 2022

Open Windows PowerShell as an administrator and execute the following command.

```
>New-NetFirewallRule -DisplayName <firewall rule name> -Action Allow -Direction Inbound -Enabled True
-Protocol TCP -LocalPort <port number>
```

Example: Set the name "WinRM" as the rule to open the port number 5986.

```
>New-NetFirewallRule -DisplayName WinRM -Action Allow -Direction Inbound -Enabled True -Protocol TCP
-LocalPort 5986
```



Note

The firewall settings differ depending on the environment of the target servers.

B.2.4 Execution Policy Change for Windows PowerShell

1. Open Windows PowerShell as an administrator and execute the following command.

```
>set-executionpolicy remotesigned
```

2. If the following message is displayed, enter [Y] and press the [Enter] key.

```
Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution
policy might expose you to the security risks described in the about_Execution_Policies help
topic at
https://msdn.microsoft.com/powershell/reference/5.1/Microsoft.PowerShell.Core/about/
about_Execution_Policies. Do you want to change the execution policy?
```

B.2.5 Settings When Using a Domain User Account

Monitoring using a domain user account cannot monitor multiple different domain environments concurrently.

1. Adding an SPN of WinRM service to Active Directory

Execute the following command and check that the SPN of the WinRM service is registered in Active Directory.

```
>setspn -L <monitoring target host name>
```

If WSMAN/<monitoring target host name> and WSMAN/<FQDN name of the monitoring target host> are output, the SPN of the WinRM service is registered.

```
>setspn -L <monitoring target host name>
      WSMAN/<monitoring target host name>
      WSMAN/<FQDN name of the monitoring target host>
```

If WSMAN/<monitoring target host name> and WSMAN/<FQDN name of the monitoring target> are not output, execute the following command on the monitoring target server and start WinRM service again.

```
>net stop winrm
```

```
>net start winrm
```

You must register the correct Service Principal Name (SPN) in Active Directory, even if WSMAN/<monitoring target host name> and WSMAN/<FQDN name of the monitoring target host> are not output after restarting the WinRM service. Execute the following command to register an SPN of the WinRM service.

```
>setspn -S WSMAN/<monitoring target host name> <monitoring target host name>
```

```
>setspn -S WSMAN/<FQDN name of the monitoring target host> <monitoring target host name>
```

2. Adding an SPN of the monitoring target server to Active Directory

To perform monitoring with a domain user account, you must correctly register a Service Principal Name (SPN) of a monitoring target server on Active Directory. Execute the following command to register the Service Principal Name of the monitoring target server.

```
>setspn -S HTTP/<monitoring target IP address> <monitoring target host name>
```



Point

- Command for checking

```
>setspn -L <monitoring target host name>
```

- Command for deleting

```
>setspn -D HTTP/<monitoring target IP address> <monitoring target host name>
```

3. Adding domain information to ISM-VA

To perform monitoring with the domain user account, follow the procedures in "3.4.2 Initial Setup of ISM-VA."

4. Adding DNS information to ISM-VA

To perform monitoring with the domain user account, execute "Add DNS server" in "[4.9 Network Settings](#)" to register the DNS server on ISM-VA.

B.3 Setting Procedure for Monitoring Targets (OS: Red Hat Enterprise Linux)

ISM communicates with the target servers with Red Hat Enterprise Linux installed, by using ssh (Secure Shell service). The following are the required settings.

- [B.3.1 Confirmation on Starting of ssh Service](#)
- [B.3.2 Settings for root user to Enable ssh Connections](#)
- [B.3.3 Settings When Using a Domain User Account](#)
- [B.3.4 Settings When Using a General User Account](#)
- [B.3.5 Common Settings for User Accounts](#)

B.3.1 Confirmation on Starting of ssh Service

Configure so that sshd can be started. The command differs depending on the OS versions.

For Red Hat Enterprise Linux 7/8/9

1. Execute the following command, and confirm if sshd is auto-started.

```
# systemctl is-enabled sshd
```

The auto-start of sshd is disabled if the result is as shown below.

```
disabled
```

2. Execute the following command if the auto-start of sshd is disabled.

```
# systemctl enable sshd
```

From the next starting of the target server, sshd will be auto-started.

3. Start sshd.

```
# systemctl start sshd
```

B.3.2 Settings for root user to Enable ssh Connections

For Red Hat Enterprise Linux 9 or later, logging in as the root user using a password via ssh is disabled by default. When monitoring as the root user, execute the following settings.

1. Execute the following command to open the setting file.

```
# vi /etc/ssh/sshd_config
```

2. Add "PermitRootLogin yes" to the Authentication section in the file.

Example:

```
# Authentication:
#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

3. Restart sshd.

```
# service sshd restart
```

After restarting, you can login as root with the ssh command.

B.3.3 Settings When Using a Domain User Account

Pay attention to the following points when monitoring by using a domain user account.

Adding domain information to ISM-VA

To perform monitoring using the domain user account, follow the procedures in "[3.4.2 Initial Setup of ISM-VA](#)."

Adding DNS information to ISM-VA

To perform monitoring using the domain user account, follow the procedures in "Add DNS server" in "[4.9 Network Settings](#)" to register the DNS server on ISM-VA.

Restriction on a domain user account name

Pay attention to the restriction on the user names of Linux when you use the domain user name that has been registered on Active Directory for Linux.

- Representative examples unavailable for Linux user names

Uppercase letters, numeric characters at the beginning, and symbols, such as dot (.) are not allowed

Restriction when collecting Emulex card information

Use "hbacmd" to collect the card information for the devices on which the card provided by Avago/Emulex is mounted.

When collecting the card information with the domain user account, provide "hbacmdan" with administrator privileges.

For details, refer to "OneCommandManager Command Line Interface User Manual."

Restriction when collecting QLogic card information

You cannot retrieve the information about the devices on which the card provided by QLogic is mounted, by using the domain user account. Register a root user from the "Edit OS Information" screen to retrieve the information.

Restriction when collecting ServerView logs

You cannot collect ServerView logs by using the domain user account. Register a root user from the "Edit OS Information" screen to collect the information.

Restriction when updating firmware

You cannot execute online firmware update by using the domain user account. Register a root user from the "Edit OS Information" screen to execute firmware update.

B.3.4 Settings When Using a General User Account

Pay attention to the following points when monitoring using a general user account other than the root user account.

Settings for sudo command

You must change the monitoring target server settings to enable the applicable user account to execute the sudo command with their login password (a general user account password).

The following is an example of a setting to enable the sudo command with the login password of user 1.

1. Edit /etc/sudoers file.

```
# visudo
:
#Defaults targetpw          . . . Comment out
root    ALL=(ALL)          ALL
user1   ALL=(ALL)          ALL . . . Add user1
:
```

2. Log in to a monitoring target server with ssh using user 1.

If the password for user 1 is asked for when executing the sudo command, the setting is completed.

Settings for environment variables

After logging in to the monitoring target server with ssh using the applicable account, confirm that the prompt strings meet the following conditions. If the following conditions are met, do not change the settings for prompt strings. Prompt strings can be changed by changing the value of environment variable PS1.

- Directed to home directory upon login
- "~" is included in the prompt strings upon login
- "\$" or "#" is included after "~" in the prompt strings upon login

Example: [user1@localhost ~]\$

Example parameter for environment variable PS1:

```
[user1@localhost ~]$ echo $PS1
[\u@\h \W]\$
```

B.3.5 Common Settings for User Accounts

Settings for a login shell

Set "/bin/bash" for the login shell for the user account. If you cannot change the login shell, create a new user account on Linux, and update the OS information registered in ISM.

Log in to the target server for monitoring with an appropriate user account via ssh, and execute the following command to confirm the login shell.

```
# echo $SHELL
```

When the command result is not "/bin/bash," execute the following command.

```
# chsh -s /bin/bash
```

Settings for ".bashrc"

1. Open ".bashrc" file in the home directory of an applicable account.

Create a file if there is no ".bashrc" file.

```
# vi ~/.bashrc
```

2. Add the paths of "/sbin," "/usr/sbin," and "/usr/local/sbin" to ".bashrc" file.

```
PATH=$PATH:/sbin
PATH=$PATH:/usr/sbin
PATH=$PATH:/usr/local/sbin
```

Settings for the environment variable

To execute the Log Collection function of ServerView, you must set the environment variable PS1 of the applicable account. To set the environment variable PS1, refer to "[Settings for environment variables](#)" in "[B.3.4 Settings When Using a General User Account](#)."

B.4 Setting Procedure for Monitoring Targets (OS: SUSE Linux Enterprise Server)

ISM communicates with the target servers with SUSE Linux Enterprise Server installed, by using ssh (Secure Shell service). The following are the required settings.

- [B.4.1 Confirmation on Starting of ssh Service](#)
- [B.4.2 Opening the Firewall Port](#)
- [B.4.3 Settings When Using a Domain User Account](#)
- [B.4.4 Settings When Using a General User Account](#)
- [B.4.5 Common Settings for User Accounts](#)

B.4.1 Confirmation on Starting of ssh Service

The start of sshd is disabled by default in SUSE Linux Enterprise Server.

Set sshd to be started. The command differs depending on OS versions.

SUSE Linux Enterprise Server 12/15

1. Execute the following command, and confirm if sshd is auto-started.

```
# systemctl is-enabled sshd
```

The auto-start of sshd is disabled if the result is as shown below.

```
disabled
```

2. Execute the following command if the auto-start of sshd is disabled.

```
# systemctl enable sshd
```

From the next starting of the target server, sshd will be auto-started.

3. Start sshd.

```
# systemctl start sshd
```

B.4.2 Opening the Firewall Port

If you set the firewall enabled, allow the ssh communication with the settings of the firewall. The firewall of SUSE Linux Enterprise Server closes the ssh port by default.

The firewall settings differ depending on the environment of the target servers.

SUSE Linux Enterprise Server 12

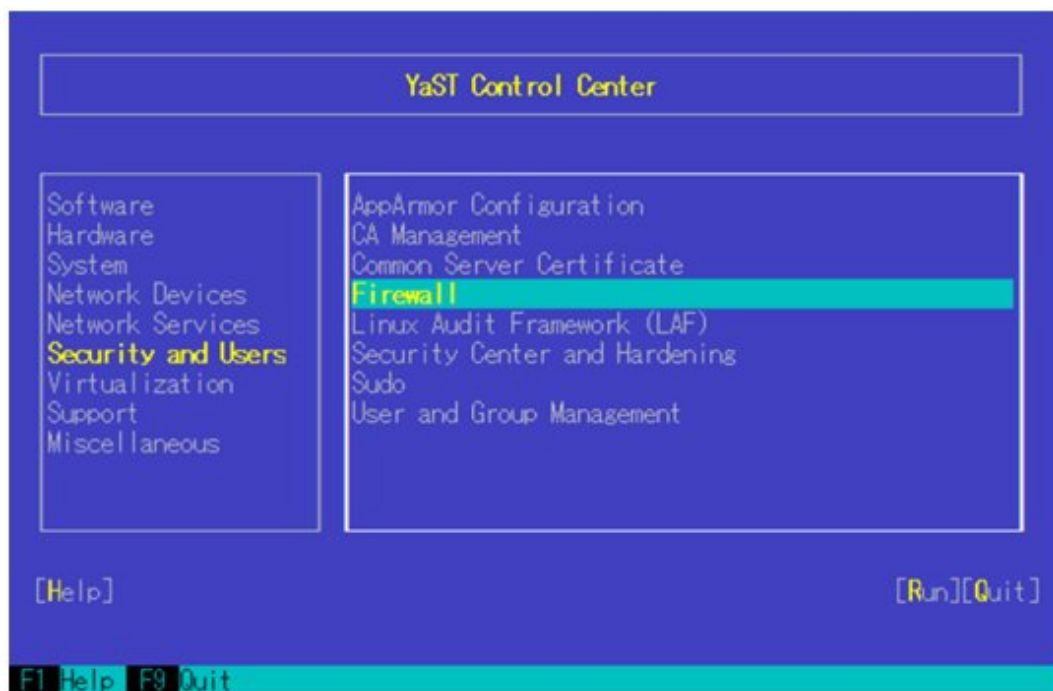
The example as shown below is the firewall settings in which YaST is used.

1. Execute the following command to display YaST Control Center.

```
# yast
```

In "yast," select items by using the arrow key combined with the [Tab] key.

2. Select [Security and Users] - [Firewall], and press the [Enter] key.

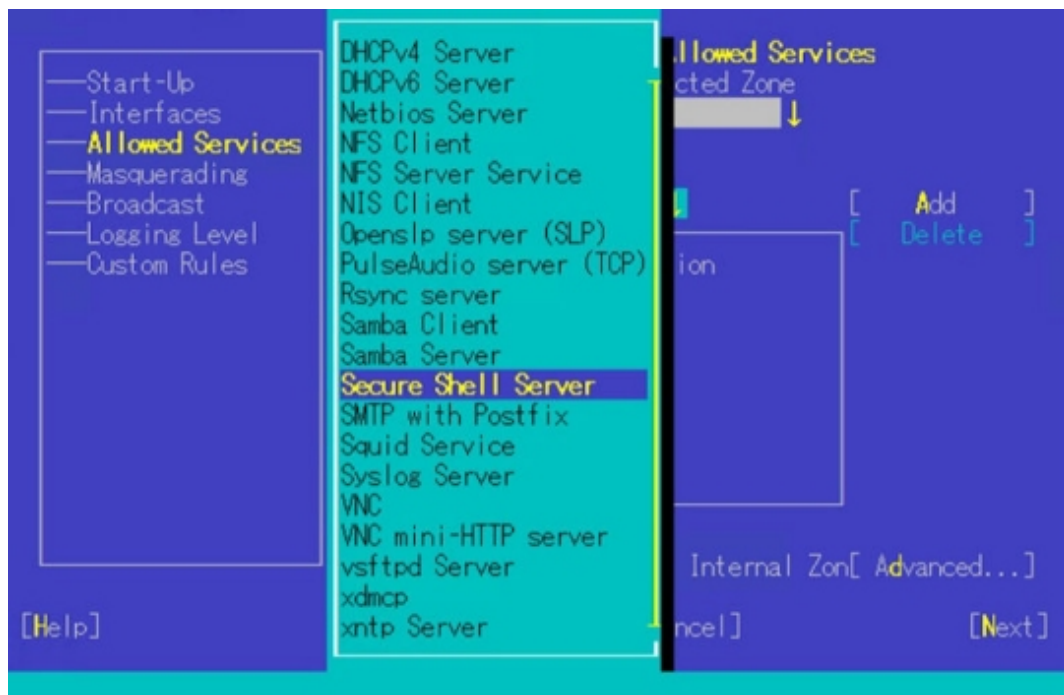


3. From the "Start-Up" screen, change the status of [Service Start] to "Enable Firewall Automatic Starting."

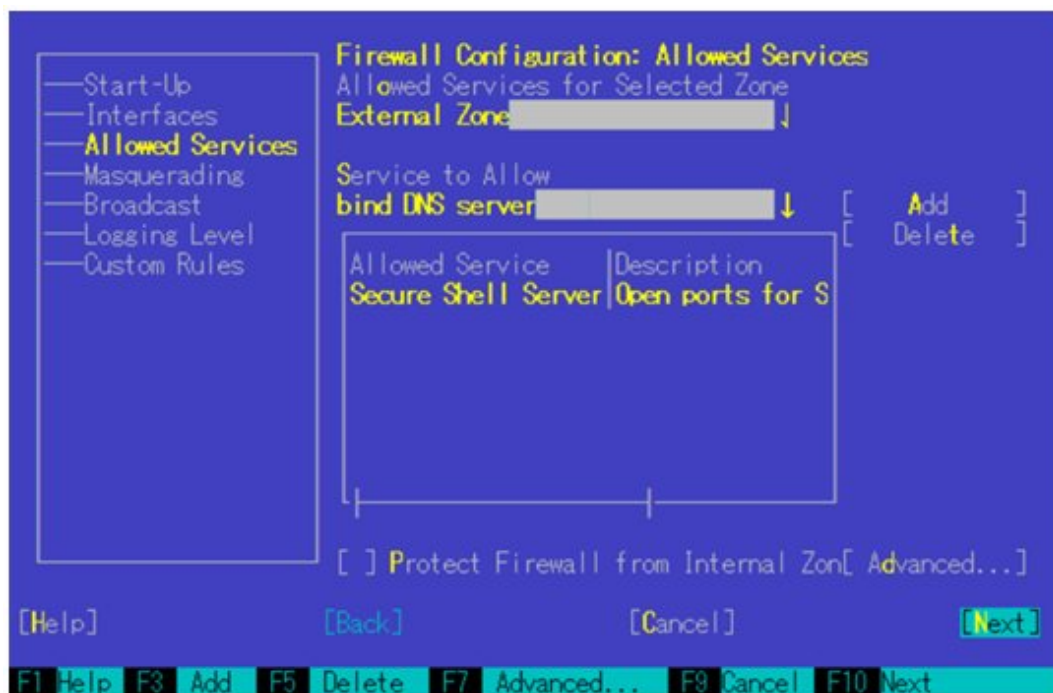


4. From [Allowed Services] - [Service to Allow], press the down-arrow key.

5. Select "Secure Shell Server," and press the [Enter] key.



6. Select [Add] and press the [Enter] key.
7. Confirm if "Secure Shell Server" is added to [Allowed Service], move to [Next], and then, press the [Enter] key.



8. After the "Firewall Configuration: Summary" screen is displayed, select [Finish] and press the [Enter] key to finish the firewall settings.



9. Move to "Quit," press the [Enter] key to finish YaST Control Center.

SUSE Linux Enterprise Server 15

For SUSE Linux Enterprise Server 15, Firewall setting with YaST is not supported. Use "firewall-cmd" to set Firewall.

1. Start firewalld.

```
# systemctl start firewalld
```

2. Execute the following command, and allow the ssh communication.

```
# firewall-cmd --permanent --add-service=ssh
# firewall-cmd --reload
```

B.4.3 Settings When Using a Domain User Account

Pay attention to the following points when monitoring using a domain user account.

Adding domain information to ISM-VA

To perform monitoring with the domain user account, follow the procedures in "[3.4.2 Initial Setup of ISM-VA](#)."

Adding DNS information to ISM-VA

To perform monitoring with the domain user account, follow the procedures in "Add DNS server" in "[4.9 Network Settings](#)" to register the DNS server on ISM-VA.

Restriction when collecting Emulex card information

Use "hbacmd" to collect the card information for the devices on which the card provided by Avago/Emulex is mounted.

When collecting the card information with the domain user account, provide the "hbacmdan" administrator privilege.

For details, refer to "One Command Manager Command Line Interface User Manual."

Restriction when collecting QLogic card information

You cannot retrieve the information about the devices on which the card provided by QLogic is mounted, by using the domain user account. Register a root user from the "Edit OS Information" screen to retrieve the information.

Restriction when collecting ServerView logs

You cannot collect ServerView logs by using the domain user account. Register a root user from the "Edit OS Information" screen to collect the information.

Restriction when updating firmware

You cannot execute Online firmware update by using the domain user account. Register a root user from the "Edit OS Information" screen to execute firmware updates.

B.4.4 Settings When Using a General User Account

Pay attention to the following points when monitoring using a general user account other than the root user account.

Settings for sudo command

You must change the monitoring target server settings to enable the applicable user account to execute the sudo command with their login password (a general user account password).

The following is an example of a setting to enable the sudo command with the login password of user 1.

1. Edit /etc/sudoers file.

```
# visudo
:
#Defaults targetpw          <- Comment out
root    ALL=(ALL)           ALL
user1   ALL=(ALL)           ALL <- Add user1
:
```

2. Log in to a monitoring target server with ssh using user 1.

If the password for user 1 is asked for when executing the sudo command, the setting is completed.

Settings for environment variables

After logging in to the monitoring target server with ssh using the applicable account, confirm that the prompt strings meet the following conditions. If the following conditions are met, do not change the settings for prompt strings. Prompt strings can be changed by changing the value of environment variable PS1.

- Directed to home directory upon login
- "~" is included in the prompt strings upon login
- "\$" or "#" is included after "~" in the prompt strings upon login

Example: [user1@localhost ~]\$

Example parameter of environment variable PS1:

```
[user1@localhost ~]$ echo $PS1
[\u@\h \W]\$
```

B.4.5 Common Settings for User Accounts

Settings for a login shell

Set "/bin/bash" for the login shell for the user account. If you cannot change the login shell, create a new user account on Linux, and update the OS information registered in ISM.

Log in to the target server for monitoring with an appropriate user account via ssh, and execute the following command to confirm the login shell.

```
# echo $SHELL
```

When the command result is not "/bin/bash," execute the following command.

```
# chsh -s /bin/bash
```

Settings for ".bashrc"

1. Open the ".bashrc" file in the home directory of an applicable account.

Create a file if there is no ".bashrc" file.

```
# vi ~/.bashrc
```

2. Add the paths of "/sbin," "/usr/sbin" and "/usr/local/sbin" to ".bashrc" file.

```
PATH=$PATH:/sbin
PATH=$PATH:/usr/sbin
PATH=$PATH:/usr/local/sbin
```

Settings for environment variables

To execute the Log Collection function of ServerView, you must set the environment variable PS1 of applicable account. To set the environment variable PS1, refer to "[Settings for environment variables](#)" in "[B.4.4 Settings When Using a General User Account](#)."

B.5 Setting Procedure for Monitoring Targets (OS: AlmaLinux)

ISM communicates with target servers with AlmaLinux installed, by using ssh (Secure Shell service). For required settings, refer to "[B.3 Setting Procedure for Monitoring Targets \(OS: Red Hat Enterprise Linux\)](#)."

B.6 Setting Procedure for Monitoring Targets (OS: VMware ESXi)

ISM communicates with target servers with VMware ESXi installed, by using vSphere API/CIM protocol. The following are the required settings.

B.6.1 Settings Required When Enabling VMware ESXi Lockdown Mode

ISM-VA cannot monitor when VMware ESXi lockdown mode is enabled.

The symptom is failure to get node information.

The workaround is to add the VMware ESXi login account to the Exception User list so that ISM-VA can monitor it even when lockdown mode is enabled. Registration to the Exception User list is handled by the vSphere Client.

B.6.2 Settings When Using Domain User Account

Pay attention to the following points when monitoring by using a domain user account.

Adding domain information to ISM-VA

To perform monitoring with the domain user account, follow the procedures in "[3.4.2 Initial Setup of ISM-VA](#)."

Adding DNS information to ISM-VA

To perform monitoring with the domain user account, follow the procedures in "Add DNS server" in "[4.9 Network Settings](#)" to register the DNS server on ISM-VA.

B.7 Setting Procedure for Monitoring Targets (OS: Azure Stack HCI)

ISM uses WS-Management protocol for the monitoring target devices on which Azure Stack HCI is installed. For the communication method, Https Protocol + Basic authentication is used. The following are the required settings.

- [B.7.1 Confirmation on Starting WinRM Service](#)
- [B.7.2 Settings for WinRM Service](#)
- [B.7.3 Opening the Firewall Port](#)
- [B.7.4 Execution Policy Change for Windows PowerShell](#)
- [B.7.5 Settings When Using a Domain User Account](#)

B.7.1 Confirmation on Starting WinRM Service

1. Open the command prompt as an administrator and execute the following command to check that WinRM service has started.

```
>sc query winrm
```

2. Check the following results and confirm that the "STATE" is "RUNNING."

```
TYPE                : 20 WIN32_SHARE_PROCESS
STATE                : 4 RUNNING
                    (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
WIN32_EXIT_CODE       : 0 (0x0)
SERVICE_EXIT_CODE   : 0 (0x0)
CHECKPOINT            : 0x0
WAIT_HINT             : 0x0
```

3. If the WinRM service has not started, execute the following command to start WinRM service.

```
>sc start winrm
```

4. Set the WinRM service to be delayed-auto-started (delayed-auto).

```
>sc config winrm start=delayed-auto
```

B.7.2 Settings for WinRM Service

Settings for WinRM Service



.....

Since Basic authentication is not allowed in the initial settings, you must set the service to allow Basic authentication.

Execute the following command.

```
>winrm set winrm/config/service/Auth @{Basic="true"}
```

.....

To use https communication, communication with Basic authentication is encrypted.

1. Open the command prompt as an administrator and execute the following command.

```
>winrm quickconfig
```

The settings are already complete if the message "WinRM service is already running on this machine. WinRM is already set up for remote management on this computer." is displayed. In this case, proceed to ["Settings for Https Communication."](#)

2. Enter "y," and then press the [Enter] key.

```
WinRM service is already running on this machine.
WinRM is not set up to allow remote access to this machine for management.
The following changes must be made:
```

```
Configure LocalAccountTokenFilterPolicy to grant administrative rights remotely to local users.
Make these changes [y/n]? y
```

The following message is displayed.

```
WinRM has been updated for remote management.

Configured LocalAccountTokenFilterPolicy to grant administrative rights remotely to local users.
```

3. Execute the following command to increase the numerical value of MaxConcurrentOperationsPerUser depending on the type and the number of cards.

```
>winrm set winrm/config/Service @{MaxConcurrentOperationsPerUser="numerical value"}
```

Example: In the case where the above value is set as 1500 (1500 is recommended because 1500 is set by default in Azure Stack HCI.)

```
>winrm set winrm/config/Service @{MaxConcurrentOperationsPerUser="1500"}
```

Settings for Https Communication

To establish https communication, you must set a certificate.

1. Create and register a self-signed root certificate

Create a self-signed root certificate to sign the client certificate.

For more detailed procedure for creating certificates, refer to the following URL.

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-certificates-point-to-site>

- a. Start PowerShell from a command prompt.
- b. Creating a self-signed root certificate.

You must execute commands depending on the environment of a target server.

Execute a command similar to the following on the PowerShell.

The following is a command example when the server name of a target server is set as "192.168.10.10" and the effective period of the certificate is set to 10 years.

```
>$cert = New-SelfSignedCertificate `
-Subject "CN=192.168.10.10" -NotAfter $(Get-Date).AddDays(3650) `
-CertStoreLocation cert:\LocalMachine\My `
-KeyUsage CertSign,CRLSign
```

- c. Register as a trusted root certificate.

Execute a command similar to the following on the PowerShell.

```
>Export-Certificate -Cert $cert -FilePath <certificate file name.cer>
```

```
>Import-Certificate -Cert cert:\LocalMachine\Root -FilePath <certificate file name.cer>
```

2. Registering a client certificate

Create a client certificate based on the certificate created above in Step 1.

- a. Create a client certificate.

Execute a command similar to the following on the PowerShell.

The following is a command example when the server name of a target server is set as "192.168.10.10" and the effective period of the certificate is set to 10 years.

```
>$cert = Get-ChildItem `
-Path cert:\LocalMachine\My | where { $_.Subject -eq "CN=192.168.10.10" }
```

```
>$client= New-SelfSignedCertificate `
-Subject "CN=192.168.10.10, C=Japan" `
-NotAfter $(Get-Date).AddDays(3650) `
-CertStoreLocation cert:\LocalMachine\My `
-Signer $cert `
-TextExtension @( `
"2.5.29.37={text}1.3.6.1.5.5.7.3.1" `
)
```

b. Registering the client certificate

Execute a command similar to the following on the PowerShell.

The following is a command example when setting "password" as the password.

```
>$password = ConvertTo-SecureString -String "password" -Force -AsPlainText
```

```
>Export-PfxCertificate -Cert $client -FilePath <certificate file name.pfx> -Password
$password
```

Register the Thumbprint Described on the Certificate to WinRM Service

1. Checking Thumbprint

The following shows how to check if the certificate is saved in LocalMachine\my.

- Start PowerShell from a command prompt.
- Check the Thumbprint. Execute the following command.

```
>ls cert:\LocalMachine\my
```

The following is displayed.

```
PS C:\Windows\system32> ls cert:\LocalMachine\my

Directory: Microsoft.PowerShell.Security\Certificate::LocalMachine\my
Thumbprint                                     Subject
-----
1C3E462623BAF91A5459171BD187163D23F10DD9      CN=192.168.10.10
```

2. Registering the Thumbprint described on the certificate with WinRM Listener.

Finish Powershell and execute the following command. A space must be entered between "HTTPS" and "@."

```
>winrm create winrm/config/listener?Address=*&Transport=HTTPS @{Hostname="<CN Name that was
specified above in step (4)>Creating a Certificate and Private Key
Files";CertificateThumbprint="<created certificate thumbprint>"}
```

3. Checking the registration of WinRM Listener

Execute the following command.

```
>winrm get winrm/config/listener?Address=*&Transport=HTTPS
```

If the command result as shown below is returned, WinRM Listener is successfully registered.

```
Listener
Address = *
Transport = HTTPS
```

```
Port = 5986
Hostname = 192.168.10.10
Enabled = true
URLPrefix = wsman
CertificateThumbprint = 1C3E462623BAF91A5459171BD187163D23F10DD9
ListeningOn = 192.168.10.10, 127.0.0.1, ::1, 2001:258:8402:200:bd8a:1c1:c50d
:8704, fe80::5efe:192.168.10.10%13, fe80::bd8a:1c1:c50d:8704%12
```

B.7.3 Opening the Firewall Port

You must open the port that you have set up in the above WinRM Listener, so that WinRM services can accept requests. The default port number of https communication is 5986.

Open Windows PowerShell as an administrator and execute the following command.

```
>New-NetFirewallRule -DisplayName <firewall rule name> -Action Allow -Direction Inbound -Enabled True
-Protocol TCP -LocalPort <port number>
```

Example: Set the name "WinRM" as the rule to open the port number 5986.

```
>New-NetFirewallRule -DisplayName WinRM -Action Allow -Direction Inbound -Enabled True -Protocol TCP
-LocalPort 5986
```



Note

The firewall settings differ depending on the environment of the target servers.

B.7.4 Execution Policy Change for Windows PowerShell

1. Open Windows PowerShell as an administrator and execute the following command:

```
>set-executionpolicy remotesigned
```

2. If the following message is displayed, enter [Y] and press the [Enter] key.

```
Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution
policy might expose you to the security risks described in the about_Execution_Policies help
topic at
https://msdn.microsoft.com/powershell/reference/5.1/Microsoft.PowerShell.Core/about/
about_Execution_Policies. Do you want to change the execution policy?
```

B.7.5 Settings When Using a Domain User Account

Monitoring using a domain user account cannot monitor multiple different domain environments concurrently.

1. Adding an SPN of WinRM service to Active Directory

Execute the following command and check that the SPN of the WinRM service is registered in Active Directory.

```
>setspn -L <monitoring target host name>
```

If WSMAN/<monitoring target host name> and WSMAN/<FQDN name of the monitoring target host> are output, the SPN of the WinRM service is registered.

```
>setspn -L <monitoring target host name>
WSMAN/<monitoring target host name>
WSMAN/<FQDN name of the monitoring target host>
```

If WSMAN/<monitoring target host name> and WSMAN/<FQDN name of the monitoring target> are not output, execute the following command on the monitoring target server and start WinRM service again.

```
>net stop winrm
```

```
>net start winrm
```

You must register the correct Service Principal Name (SPN) in Active Directory, even if WSMAN/<monitoring target host name> and WSMAN/<FQDN name of the monitoring target host> are not output after restarting the WinRM service. Execute the following command to register an SPN of the WinRM service.

```
>setspn -S WSMAN/<monitoring target host name> <monitoring target host name>
```

```
>setspn -S WSMAN/<FQDN name of the monitoring target host> <monitoring target host name>
```

2. Adding an SPN of the monitoring target server to Active Directory

To perform monitoring with a domain user account, you must correctly register a Service Principal Name (SPN) of a monitoring target server on Active Directory. Execute the following command to register the Service Principal Name of the monitoring target server.

```
>setspn -S HTTP/<monitoring target IP address> <monitoring target host name>
```



- Command for checking

```
>setspn -L <monitoring target host name>
```

- Command for deleting

```
>setspn -D HTTP/<monitoring target IP address> <monitoring target host name>
```

3. Adding domain information to ISM-VA

To perform monitoring with the domain user account, follow the procedures in "[3.4.2 Initial Setup of ISM-VA](#)."

4. Adding DNS information to ISM-VA

To perform monitoring with the domain user account, execute "Add DNS server" in "[4.9 Network Settings](#)" to register the DNS server on ISM-VA.

B.8 Setting Procedure for Monitoring Targets (Cloud Management Software: vCenter Server)

ISM communicates with vCenter Server. The following settings are required for communication.

B.8.1 Adding DNS Information to ISM-VA

When executing Monitoring under the condition where an ESXi host with FQDN is registered on vCenter, execute "Add DNS server" in "[4.9 Network Settings](#)" to register the DNS server on ISM-VA.

B.8.2 Settings When Using Domain User Account

To retrieve the information from vCenter Server, settings for respective hosts must have already been registered on vCenter Server. Refer to "[B.6 Setting Procedure for Monitoring Targets \(OS: VMware ESXi\)](#)" to execute the settings for respective hosts.

B.9 Setting Procedure for Monitoring Targets (Cloud Management Software: Microsoft Failover Cluster)

ISM communicates with Microsoft Failover Cluster. The following settings are required for communication.

B.9.1 Settings When Using a Domain User Account

1. Setting WinRM for respective hosts configuring a cluster

To retrieve the information from Microsoft Failover Cluster, settings for respective hosts that configure a cluster must have already been completed. Refer to "[B.2 Setting Procedure for Monitoring Targets \(OS: Windows\)](#)" to execute the settings for respective hosts.

2. Adding an SPN to Active Directory

You must correctly register a Service Principal Name (SPN) of a monitoring target cluster on Active Directory when monitoring a Windows Server using the domain user account. Execute the following procedure to register the Service Principal Name of the monitoring target cluster.

```
> setspn -S HTTP/<monitoring target cluster IP> <monitoring target cluster name>
```



Command for checking

```
>setspn -L <monitoring target cluster name>
```

If the command result as shown below is output, the registration has succeeded.

```
HTTP/<monitoring target cluster IP>
```

3. Adding domain information to ISM-VA

When executing Monitoring using the domain user account, follow the procedures in "[3.4.2 Initial Setup of ISM-VA.](#)"

4. Adding DNS information to ISM-VA

When executing Monitoring with the domain user account, follow the procedures in "Add DNS server" in "[4.9 Network Settings](#)" to register the DNS server on ISM-VA.

5. Kerberos delegation configuration for Active Directory

- a. Log on to the Active Directory server.
- b. Open Server Manager.
- c. From the [Tool] button, select [Active Directory Users and Computers].
- d. Expand the domain, and then expand the [Computers] folder.
- e. Right-click the cluster node name or cluster name on the right-side window, and then select [Properties].
- f. From the [General] tab, select the [Trust computer for delegation to any service (Kerberos only)] checkbox.
- g. Select [OK] and repeatedly perform the above Step e to f for all the cluster nodes or cluster.

B.10 Setting Procedure for Monitoring Targets (Cloud Management Software: Microsoft System Center)

Refer to "[B.2 Setting Procedure for Monitoring Targets \(OS: Windows\)](#)" to execute the settings for the respective hosts and virtual machines with Microsoft System Center installed.

B.11 Setting Procedure for Monitoring Targets (Cloud Management Software: KVM)



If you use domain users, setting procedures differ depending on the cloud management software that you use. Refer to the applicable procedure below.

- [B.11.1 Setting Procedure for KVM Red Hat Enterprise Linux \(Using Domain User\)](#)
- [B.11.2 Setting Procedure for KVM SUSE Linux Enterprise Server \(Using Domain User\)](#)

B.11.1 Setting Procedure for KVM Red Hat Enterprise Linux (Using Domain User)

To retrieve the KVM information, set the SSSD service for the monitoring target node.

The required packages are shown below:

- krb5-workstation
- samba
- samba-client
- samba-common
- sssd

Set the following items from the terminal as a root user.

1. Editing "/etc/hosts"

- Open the "/etc/hosts" file.

```
# vi /etc/hosts
```

- Add the following.

- An IP address and a host name of the KVM server to be the monitoring target
- An IP address of ISM-VA

Example:

```
192.168.30.222 rhel73.win2016.local rhel73
192.168.30.228
```



Note

This setting is not reflected in the local host name (on the local host). However, without this setting, executing the command to join Active Directory as described further below will result in an error.

2. Editing "/etc/krb5.conf"

- Open the "/etc/krb5.conf" file.

```
# vi /etc/krb5.conf
```

- Set a domain name in uppercase letters in "default_realm" in the [libdefaults] section.

Example:

```
[libdefaults]
dns_lookup_realm = true
dns_lookup_kdc = true
ticket_lifetime = 24h
renew_lifetime = 7d
```

```
forwardable = true
default_realm = WIN2016.LOCAL
```

- c. Execute the settings in the [realms] section.

Example:

```
[realms]
WIN2016.LOCAL = {
    kdc = 192.168.30.69
    admin_server = WIN2016-ADVM.WIN2016.LOCAL
}
```

For kdc, set an IP address of the server that issues Kerberos tickets.

For admin_server, set the FQDN of the Kerberos management server.

Generally, kdc and admin_server are the same servers as the DNS and Active Directory servers.

- d. Execute the settings in the [domain_realm] section.

Example:

```
[domain_realm]
win2016.local = WIN2016.LOCAL
.win2016.local = WIN2016.LOCAL
```



Note

Use uppercase and lowercase letters as in the above example to set the domain name you are actually using.

3. Editing "/etc/samba/smb.conf"

- a. Open the "/etc/samba/smb.conf" file.

```
# vi /etc/samba/smb.conf
```

- b. Delete all sections other than the [global] section, and execute the settings in the [global] section as follows.

Example:

```
[global]
workgroup = WIN2016
client signing = yes
client use spnego = yes
kerberos method = secrets and keytab
log file = /var/log/samba/%m.log
realm = WIN2016.LOCAL
security = ads
```



Note

For workgroup and realm, set the domain name you are actually using.

4. Creation of "/etc/sss/sss.conf"

- a. Open the "/etc/sss/sss.conf" file. Since it does not exist in the default setting, you must create it newly.

```
# vi /etc/sss/sss.conf
```

Example:

```
[sss]
config_file_version = 2
services = pam,nss
```

```
domains = WIN2016.LOCAL

[pam]

[nss]
filter_groups = root
filter_users = root

[domain/WIN2016.LOCAL]
id_provider = ad
auth_provider = ad
enumerate = false
cache_credentials = false
case_sensitive = false
```



Note

For domains in the [sssd] section and for the [domain/WIN2016.LOCAL] section name, set the domain names you are actually using.

- b. To create a home directory automatically when a domain user logs in, add the following to the [domain/Domain name] section in "/etc/sssd/sssd.conf."

```
fallback_homedir = /home/%u
```

5. Modification of permission in "/etc/sssd/sssd.conf"

Modify the permission in "/etc/sssd/sssd.conf" to "600."

```
# chmod 600 /etc/sssd/sssd.conf
```



Note

Any value other than "600" will cause an error at startup of the sssd service.

6. Setting of a local host name (on the local host)

Set the local host name (on the local host) with the following command.

```
# hostnamectl set-hostname <FQDN of host>
```

Example:

```
# hostnamectl set-hostname rhel73.win2016.local
```



Note

This is the host name setting on the local host. It is not reflected to the host name on the network. Make sure that the FQDN of the host matches the one you set in Step 1.

7. IP address setting of DNS server

- a. Use the following command to set the IP address of the DNS server and restart the interface.

```
# nmcli connection modify <Interface name> ipv4.dns <IP address of DNS server>
# systemctl restart NetworkManager
```

- b. Execute the following command to look up the interface name.

```
# ip addr
```

- c. Execute the following command to check the settings.

```
# host <Kerberos management server name>
```

Example:

```
# host WIN2016-ADVM.WIN2016.LOCAL
```

If the output includes the IP address, the settings are correct.

8. Getting permission to retrieve a Kerberos ticket

- a. Execute the following command to get permission to retrieve a Kerberos ticket.

```
# kinit Administrator
```

- b. When you are requested to enter the password, enter the password for the domain administrator user "Administrator."

- c. Execute the following command to check the settings.

```
# klist
```

If the domain information is output, the settings are correct.

If there is any failure, check "/etc/krb5.conf."

9. Joining Active Directory

- a. Use the following command to join Active Directory.

```
# net ads join -U Administrator
```

- b. When you are requested to enter the password, enter the password for the domain administrator user "Administrator."

- c. Execute the following command to check the settings.

```
# net ads info
```

If the server information (shown as "LDAP server") and domain information is output, the settings are correct.

If there is any failure, check the host name setting and the settings in "/etc/samba/smb.conf." Alternatively, refer to Point in Step 13.

10. System authentication settings

Execute the following command to set the system authentication (authorization for a target monitoring server).

This command automatically updates all related setup files.

- To not automatically create a home directory for the domain user

```
# authconfig --enablsssd --enablsssdauth --enablelocauthorize --update
```

- To create a home directory automatically for the domain user

Execute Step b in Step 4 in advance, and then execute the following command.

```
# authconfig --enablsssd --enablsssdauth --enablelocauthorize --enablemkhomedir --update
```



Note

For Red Hat Enterprise Linux 8.0 or later, it is recommended to use "authselect" instead of "authconfig."

To use "authselect," execute the following command.

```
# authselect select sssd with-mkhomedir
```

If the home directory is not created automatically when you log in as a domain user, create the directory manually.

11. Starting SSSD (System Security Services Daemon) service

- a. Execute the following commands to start the SSSD service.

```
# systemctl enable sssd
# systemctl start sssd
```

- b. Execute the following command to check that the service has started.

```
# systemctl status sssd
```

If it is running normally, the settings are correct.

If there is any failure, check the contents of "/etc/sss/sss.conf" and the file permissions.

12. Checking login as a domain user

You can use any of the following commands to check logins with the SSH protocol. For formats of the domain user name, refer to the following Point.

```
# ssh <domain user name>@<IP address of monitored server>
```

```
# ssh -l <domain user name> <IP address of monitored server>
```

Examples:

```
# ssh administrator@192.168.30.222
```

```
# ssh 'administrator@win2016'@192.168.30.222
```

```
# ssh -l 'win2016.local\administrator' 192.168.30.222
```

If you can log in normally with any of these procedures, the settings are correct.

Point

- Name formats for domain users

There are several different formats to write domain user names as follows.

Since "case sensitive" is set to "false" in the [domain/WIN2016.Domain name] section in "/etc/sss/sss.conf," there is no distinction between uppercase and lowercase letters.

Name formats for domain users	Examples
User name	administrator
'Domain prefix\User name'	'win2016\administrator'
'Domain prefix.Domain name suffix\User name'	'win2016.local\administrator'
'User name@Domain prefix'	'administrator@win2016'
'User name@Domain prefix.Domain name suffix'	'administrator@win2016.local'

- Check of domain user existence

You can use any of the following commands to check whether a domain user exists. For the domain user name, you can use any of the name formats for domain users described above.

```
# id <domain user name>
```

```
# getent passwd <domain user name>
```

If the user information is displayed, the settings are correct.

13. Settings for the Domain User

Follow the procedures in "[B.11.3 Settings When Using a General User Account](#)," and set the domain user appropriately.



When login is no longer available after changing a host name

If you changed a host name both on the local host and on the network, execute the following two commands.

```
# net ads join -U Administrator
# systemctl restart sssd
```

If the login still fails, the previous settings may exist in "/etc/krb5.keytab," so you must delete "/etc/krb5.keytab" with the following command first, and then execute the above commands.

```
# rm /etc/krb5.keytab
```

14. Adding domain information to ISM-VA

Execute the settings in "[3.4.2 Initial Setup of ISM-VA](#)."

15. Adding DNS information to ISM-VA

Register DNS servers in ISM-VA by executing "Add DNS server" in "[4.9 Network Settings](#)."

B.11.2 Setting Procedure for KVM SUSE Linux Enterprise Server (Using Domain User)

To retrieve the KVM information, set the SSSD service on the monitoring target node.

Execute the following settings by either using the yast command on the terminal or by using YaST on the GUI menu. The following procedure uses the yast command.

1. Startup of yast command

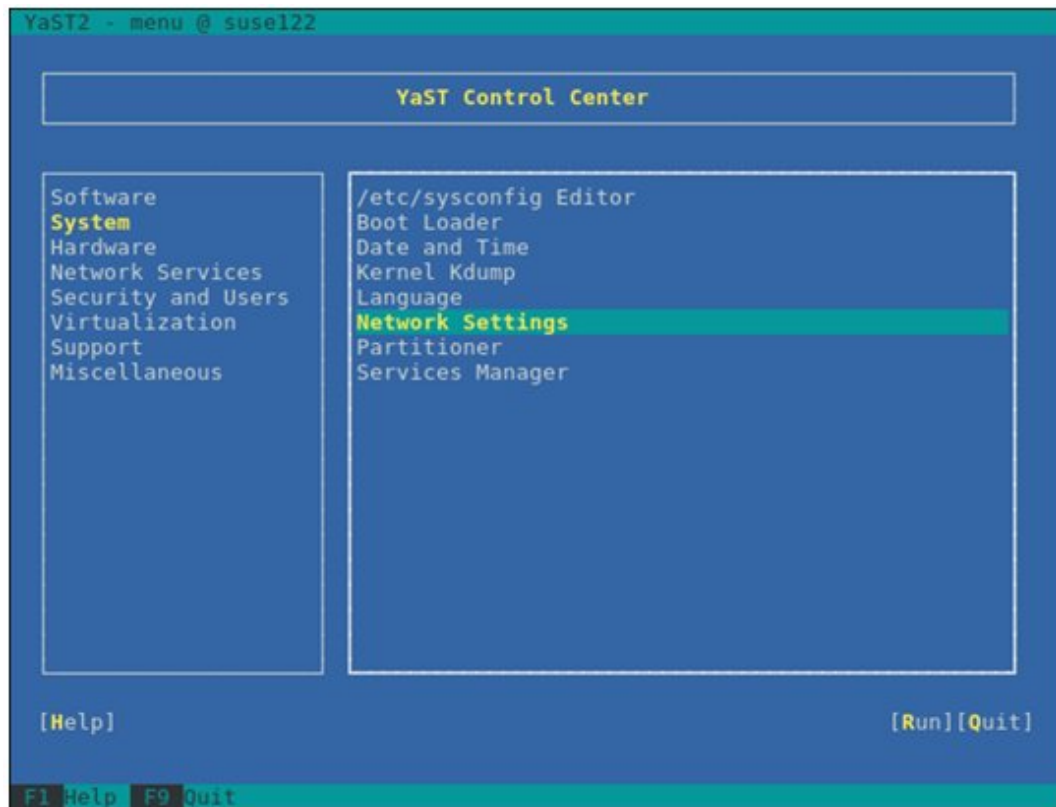
Execute the following command as a root user from your terminal.

```
# yast
```

To select items in yast, use combinations of the arrow keys and the [Tab] key.

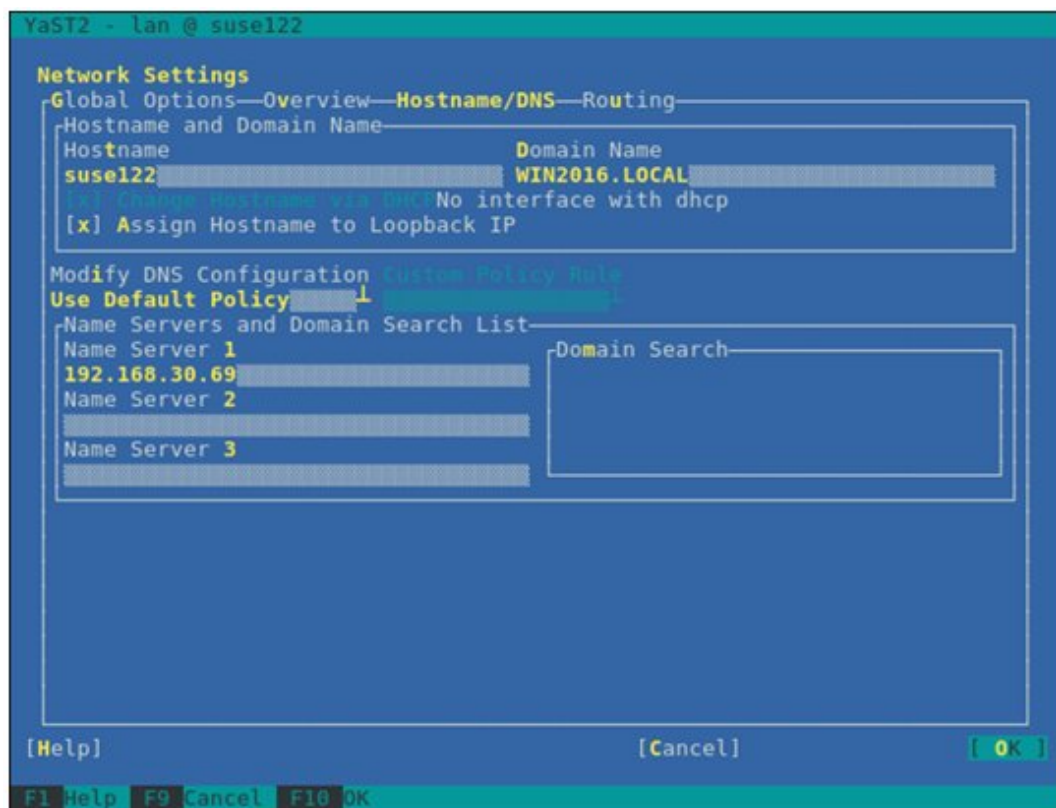
2. Host name and DNS settings

- a. Select [System] - [Network Settings], and then press the [Enter] key.



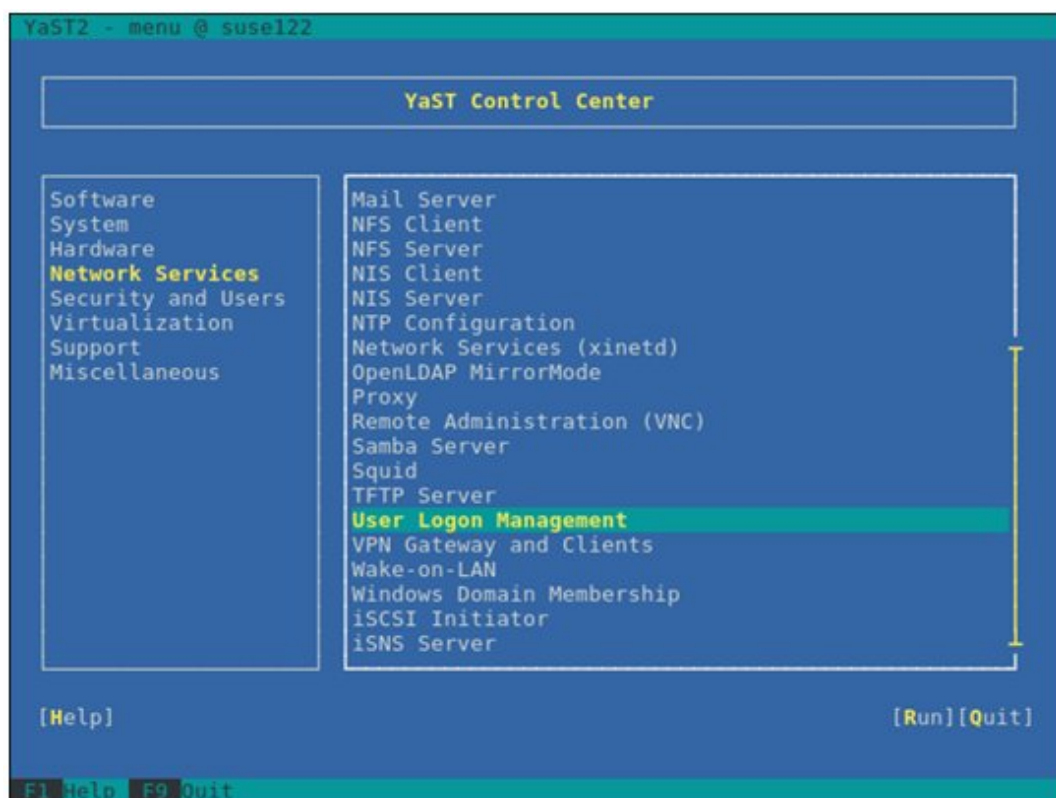
- b. Select [Hostname/DNS], execute the settings for the following items, then select [OK] and press the [Enter] key.
- Hostname
 - Domain Name
 - Assign Hostname to Loopback IP

- Name Server 1

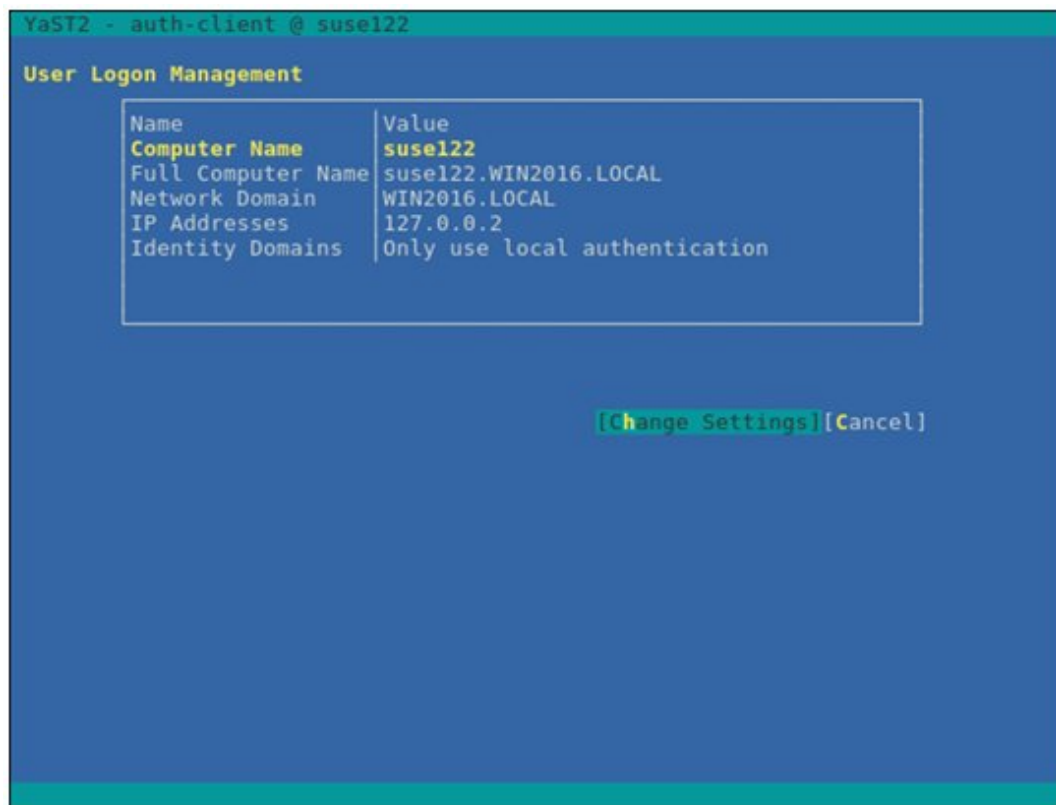


3. SSSD service settings

- Select [Network Services] - [User Logon Management], and then press the [Enter] key.

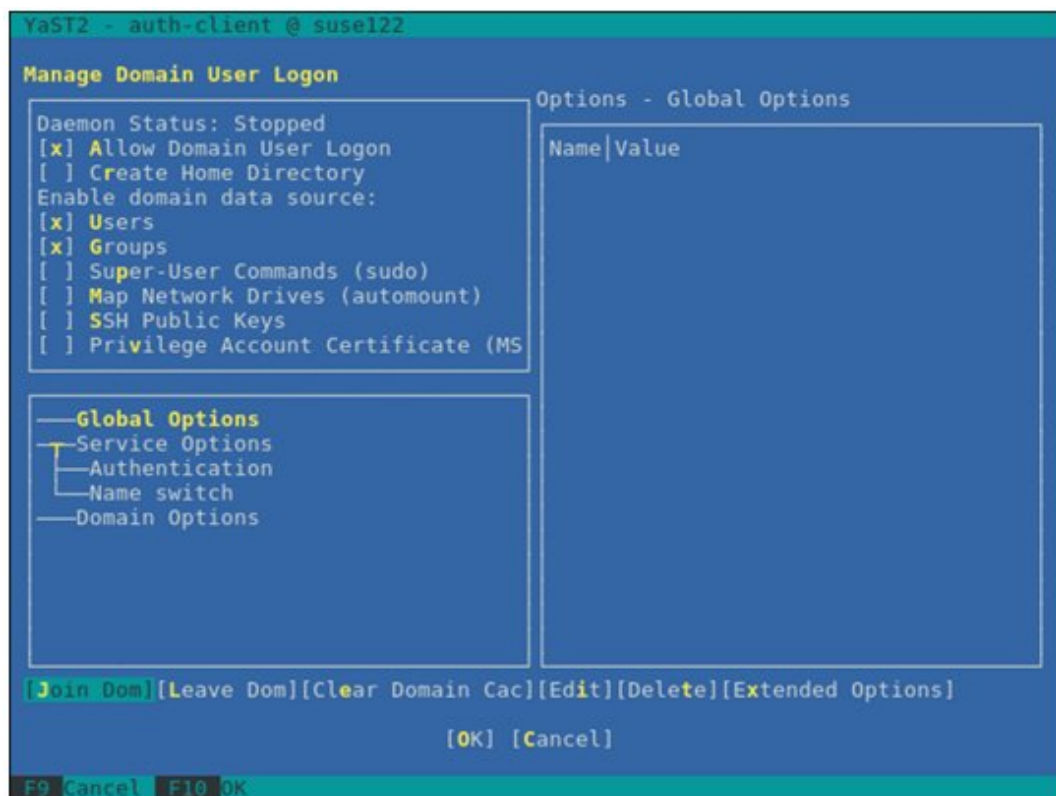


- b. Select [Change Settings], and then press the [Enter] key.



- c. Select the checkboxes for the following items, select [Join Dom], and then press the [Enter] key.
- Allow Domain User Logon
 - Users

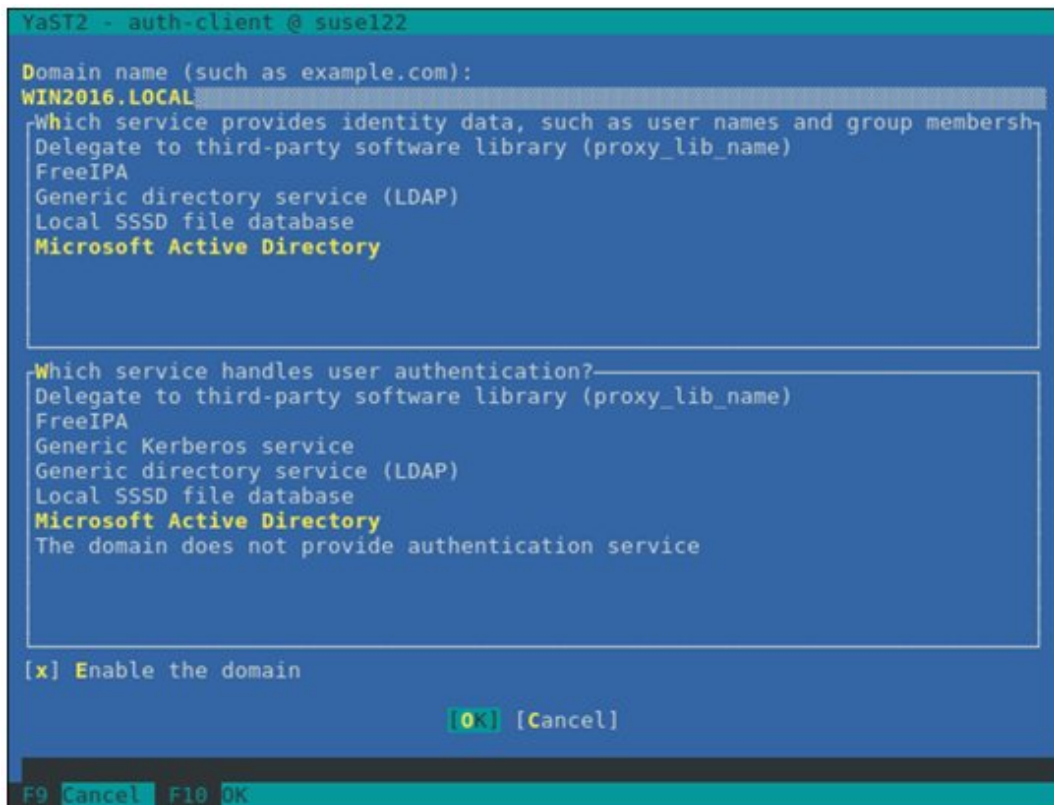
- Groups



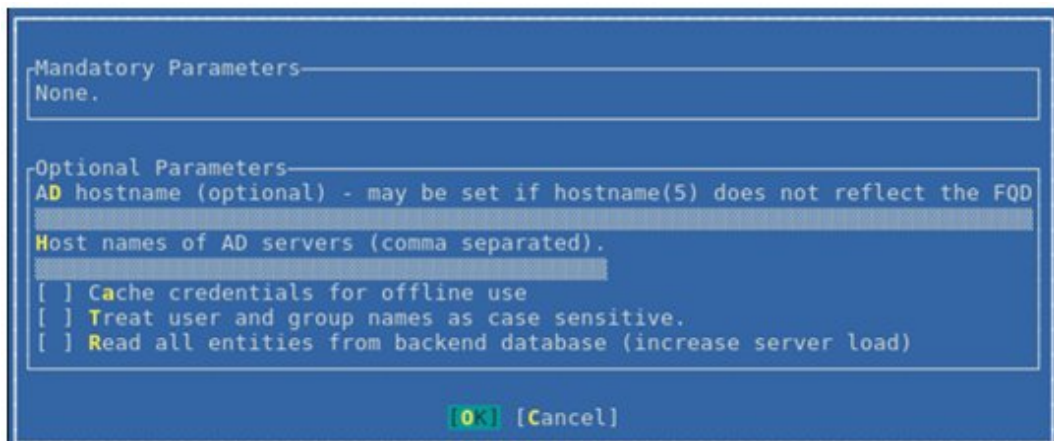
d. Set the following items, then select [OK] and press the [Enter] key.

- Domain name
- Which service provides identity data, such as user names and group members
Microsoft Active Directory
- Which service handles user authentication?
Microsoft Active Directory

- Enable the domain



- e. Leave all items blank and clear the checkboxes, select [OK], and then press the [Enter] key.



- f. Set the following items, then select [OK] and press the [Enter] key.

- Username
- Password

- Update AD's DNS records as well

```
YaST2 - auth-client @ suse122

Active Directory enrollment

Current status:
+-----+
| Name                               | Value                                     |
| Active Directory Server            | WIN2016-ADVM.WIN2016.LOCAL (Auto-discovered via DN) |
| Active Directory Domain            | WIN2016.LOCAL                             |
| Workgroup                          | WIN2016                                   |
| Enrollment Status                  | Not yet enrolled                           |
+-----+

Enter AD user credentials (e.g. Administrator) to enroll or re-enroll this computer
Username: Administrator
Password: *****
[x] Update AD's DNS records as well
Optional Organisation Unit such as "Headquarter/HR/BuildingA"
[ ] Overwrite Samba configuration to work with this AD

[OK]
```

- g. Select [OK], and then press the [Enter] key.

```
Enrollment has completed successfully! Command output:
Using short domain name -- WIN2016 Joined 'SUSE122' to dns
domain 'WIN2016.LOCAL'

[OK]
```

To create a home directory for the domain user, proceed to Step h.

If you do not create a home directory for the domain user, proceed to Step k.

- h. Set [Create Home Directory], then select [Extended Options] and press the [Enter] key.

```
YaST2 - auth-client @ suse122

Manage Domain User Logon

Daemon Status: Stopped
[x] Allow Domain User Logon
[x] Create Home Directory
Enable domain data source:
[x] Users
[x] Groups
[ ] Super-User Commands (sudo)
[ ] Map Network Drives (automount)
[ ] SSH Public Keys
[ ] Privilege Account Certificate (MS

Options - domain/WIN2016.LOCAL
[x] Use this d[Enroll to Active Direct]

Name      Value
id_provider    ad
auth_provider  ad
enumerate      false
cache_credentials false
case_sensitive false

--Global Options
--Service Options
--Authentication
--Name switch
--Domain Options
--WIN2016.LOCAL

[Join Dom][Leave Dom][Clear Domain Cac][Edit][Delete][Extended Options]

[OK] [Cancel]

F9 Cancel F10 OK
```

- i. Select [fallback_homedir], then select [Add] and press the [Enter] key.

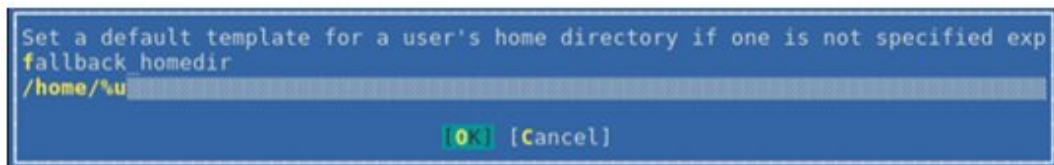
```
YaST2 - auth-client @ suse122

Extended options - domain/WIN2016.LOCAL
Name filter:

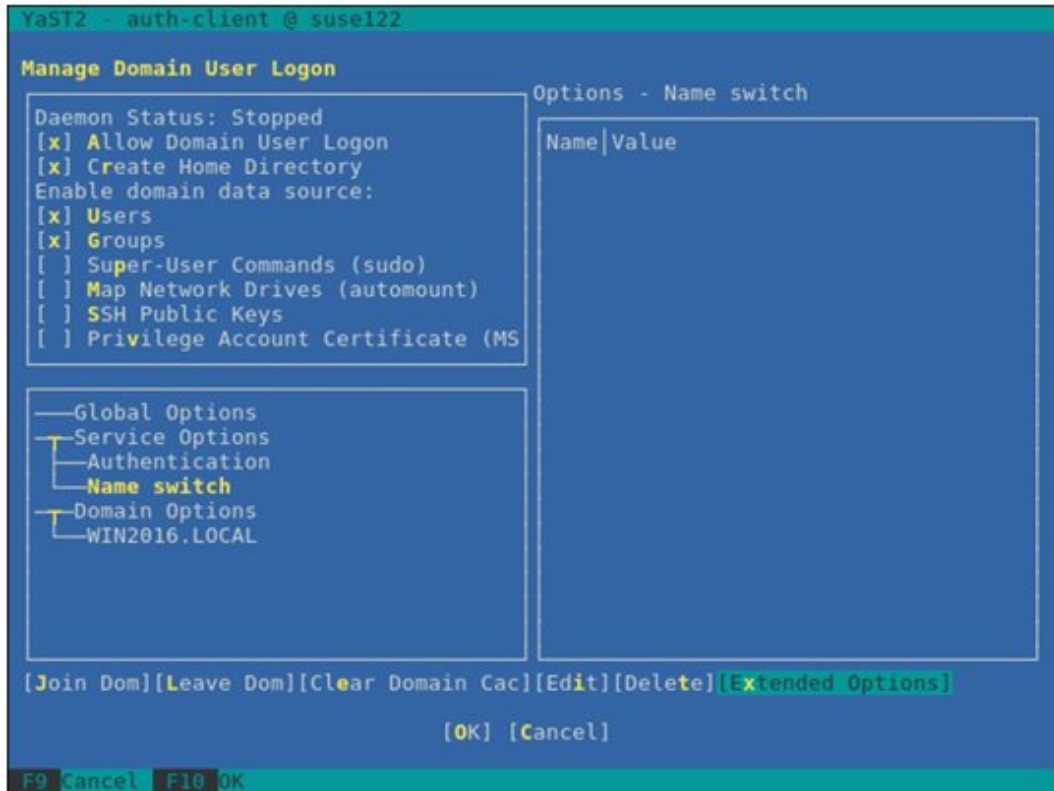
Name      Description
override_homedir Override the user's home director
proxy_fast_alias When a user or group is looked up
subdomain_homedir Use this homedir as default value
simple_allow_users Comma separated list of users who
simple_allow_groups Comma separated list of groups wh
simple_deny_users Comma separated list of groups th
ad_domain Specifies the name of the Active
ad_server Host names of AD servers (comma s
ad_backup_server Host names of backup AD servers (
ad_hostname AD hostname (optional) - may be s
fallback_homedir Set a default template for a user
default_shell The default shell to use if the p
ldap_idmap_range_min Specifies the lower bound of the
ldap_idmap_range_max Specifies the upper bound of the
ldap_idmap_range_size Specifies the number of IDs avail
ldap_idmap_default_domain_sid Specify the domain SID of the def
ldap_idmap_default_domain Specify the name of the default d
ldap_idmap_autorid_compat Changes the behavior of the ID-ma
ldap_use_tokengroups (Active Directory specific) Use t
ldap_uri URIs (ldap://) of LDAP servers (c
ldap_sudo_search_base An optional base DN to restrict L

[Add] [Cancel]
```

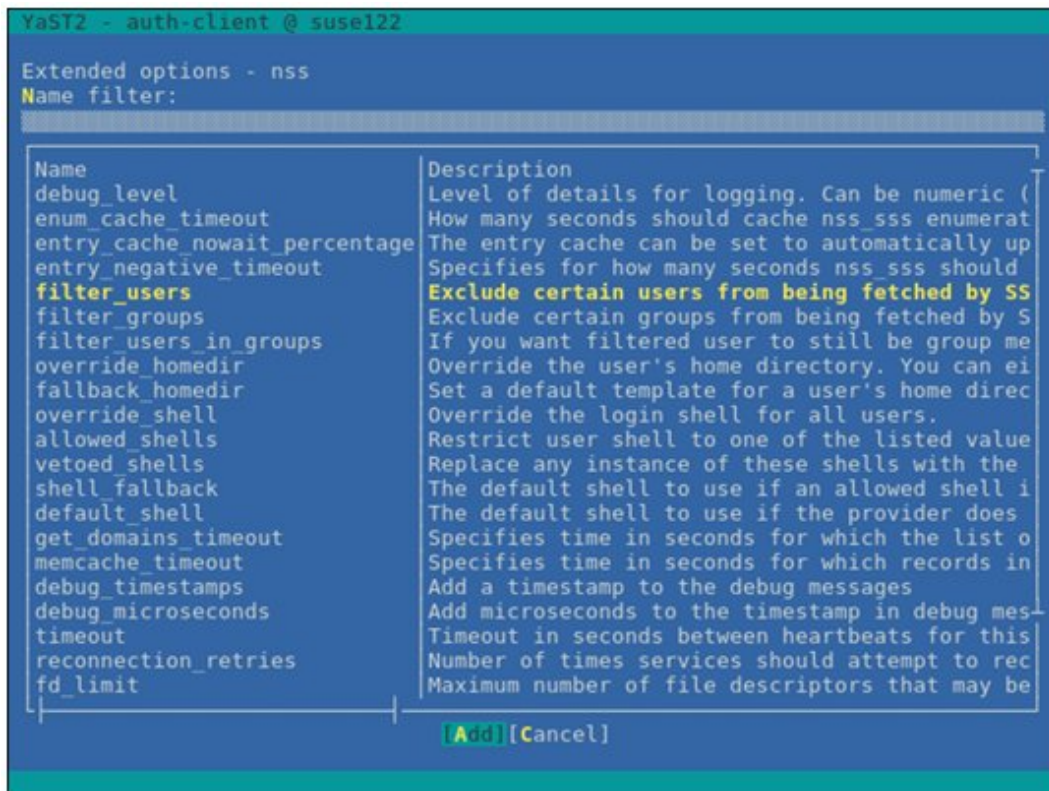
- j. Enter `"/home/%u,"` then select [OK] and press the [Enter] key.



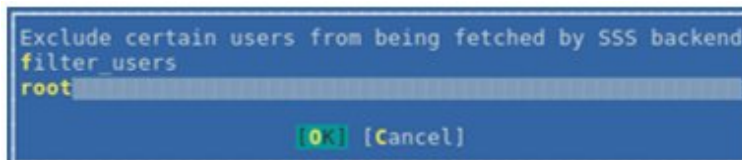
- k. Select [Name switch] - [Extended Options], and then press the [Enter] key.



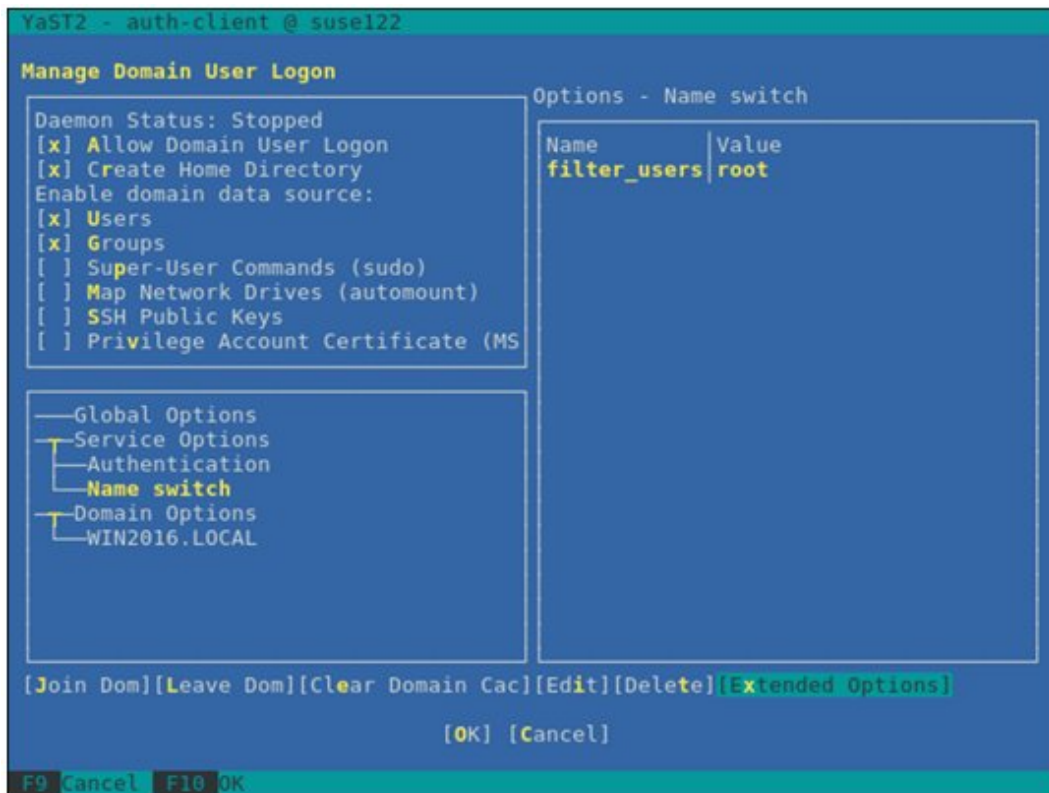
- l. Select [filter_users], then select [Add] and press the [Enter] key.



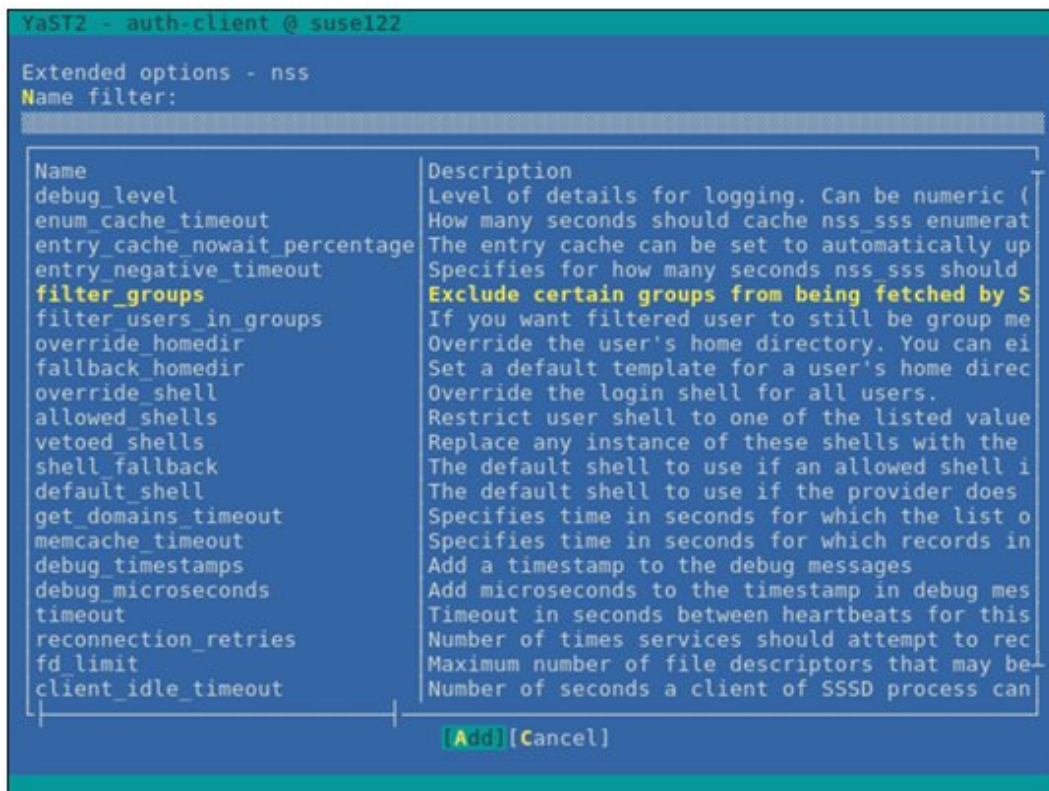
- m. Enter "root," then select [OK] and press the [Enter] key.



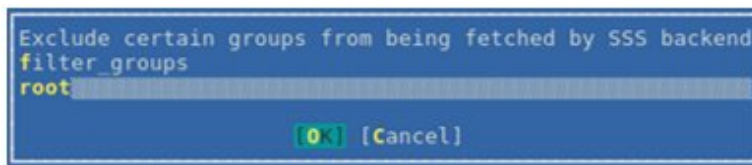
- n. Select [Name switch] - [Extended Options], and then press the [Enter] key.



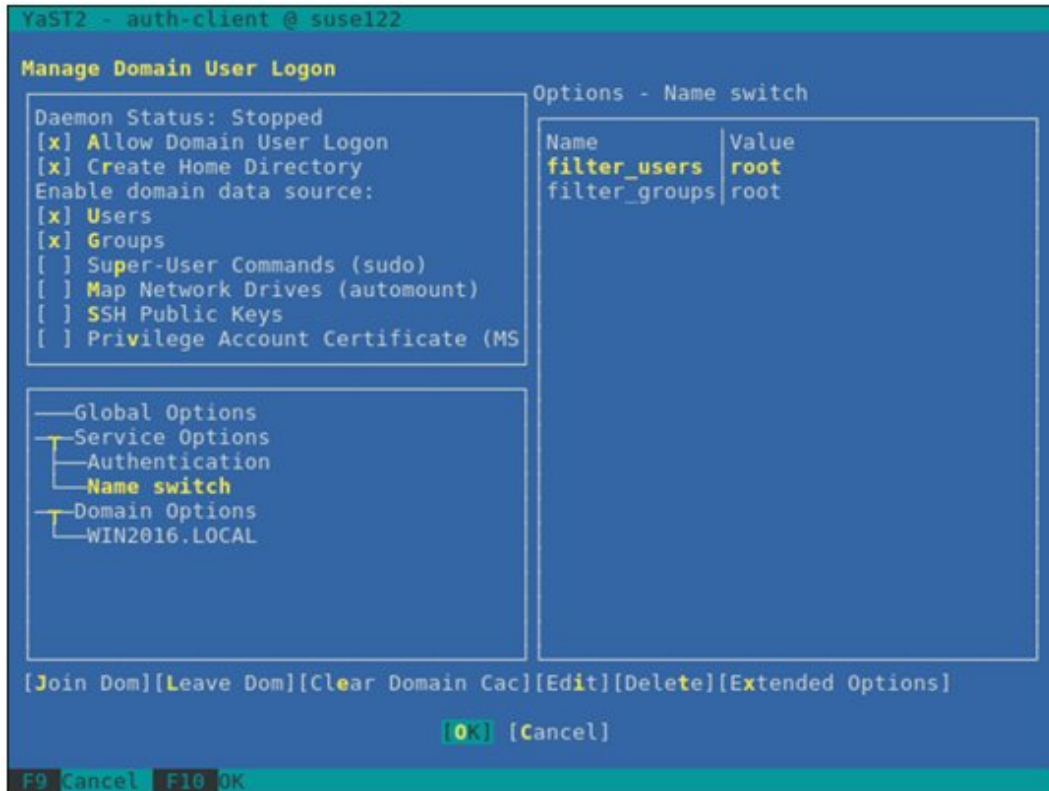
- o. Select [filter_groups], then select [Add] and press the [Enter] key.



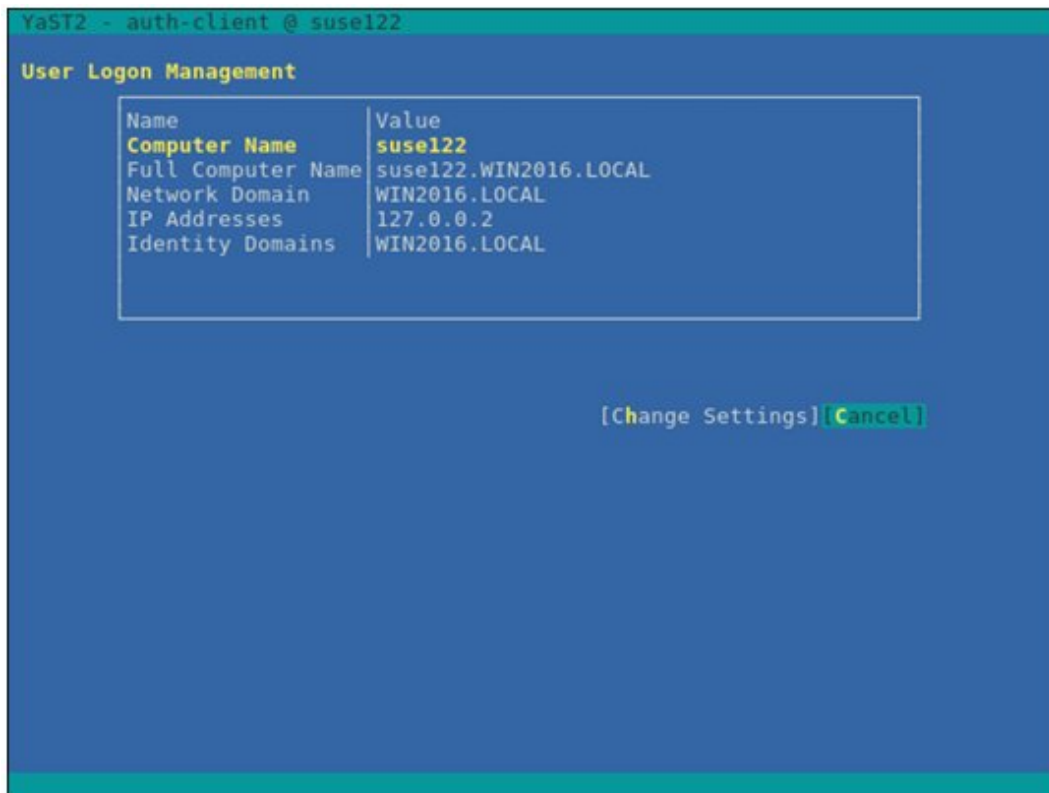
- p. Enter "root," then select [OK] and press the [Enter] key.



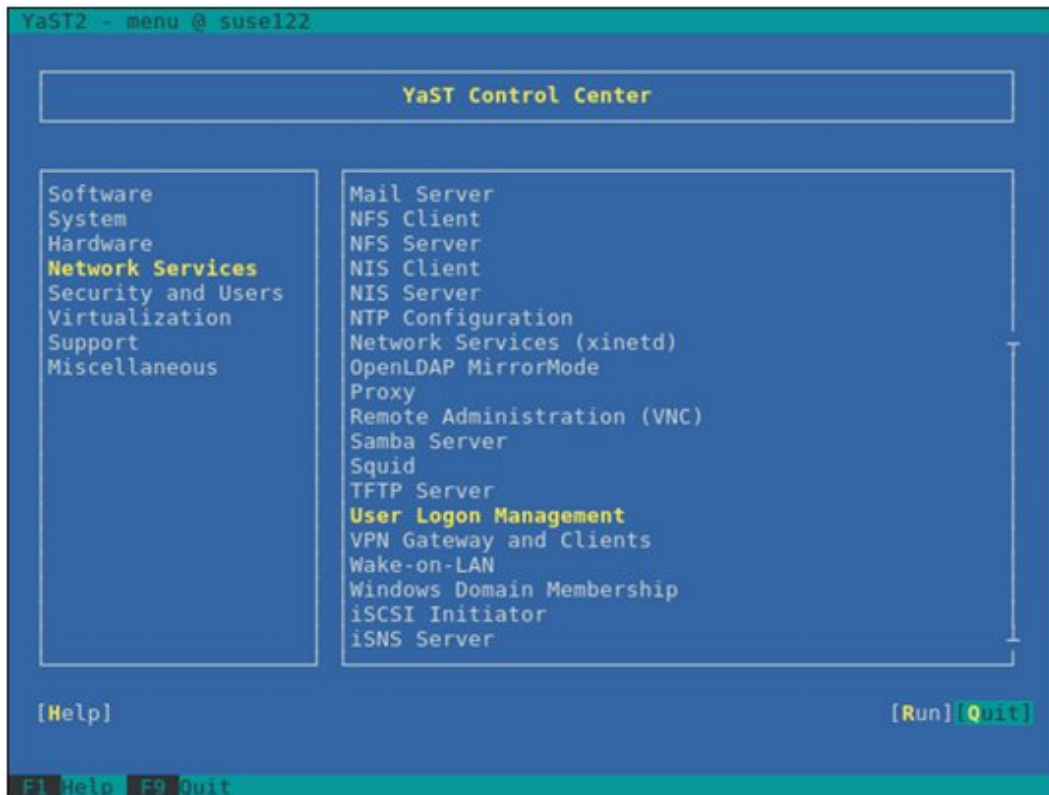
- q. Select [OK], and then press the [Enter] key.



- r. Select [Cancel], and then press the [Enter] key.



- s. Select [Quit], and then press the [Enter] key.



This completes your settings for the SSSD service.

4. Check of login as a domain user

You can use any of the following commands to check logins with the SSH protocol. For formats of the domain user name, refer to the following Point.

```
# ssh <domain user name>@<IP address of monitored server>
```

```
# ssh -l <domain user name> <IP address of monitored server>
```

Examples:

```
# ssh administrator@192.168.30.222
```

```
# ssh 'administrator@win2016'@192.168.30.222
```

```
# ssh -l 'win2016.local\administrator' 192.168.30.222
```

If you can log in normally with any of these procedures, the settings are correct.



Name formats for domain users

There are several different formats to write domain user names as follows. Since "case sensitive" is set to "false" in the optional domain settings, there is no distinction between uppercase and lowercase letters.

Name formats for domain users	Examples
User name	administrator
'Domain prefix\User name'	'win2016\administrator'
'Domain prefix.Domain name suffix\User name'	'win2016.local\administrator'
'User name@Domain prefix'	'administrator@win2016'
'User name@Domain prefix.Domain name suffix'	'administrator@win2016.local'

5. Settings for the Domain User

Follow the procedures in "[B.11.3 Settings When Using a General User Account](#)" and execute the settings for the domain user.

6. Adding domain information to ISM-VA

Execute the settings in "[3.4.2 Initial Setup of ISM-VA](#)."

7. Adding DNS information to ISM-VA

Register DNS servers in ISM-VA by executing "Add DNS server" in "[4.9 Network Settings](#)."

B.11.3 Settings When Using a General User Account

In principle, KVM information can only be retrieved by root users.

When letting users other than the root users (including domain users) retrieve KVM information, you must add those users to the "libvirt" group on the monitoring Linux server.

Execute the following command as a root user.

```
# gpasswd -a <user name> libvirt
```



To remove a user from the "libvirt" group, execute the following command as a root user.

```
# gpasswd -d <user name> libvirt
```



- Set the user name using only lowercase letters.
- You can also use the above commands to add and remove domain users.

B.12 Setting Procedure for Monitoring Targets (Cloud Management Software: OpenStack)

ISM communicates with OpenStack. The following settings are required for communication.

B.12.1 Setting Procedure for a Controller Node

1. Installing an SSL module

If an SSL module is already installed on the controller node, the installation is not required.

The following is an example of an installation using the "yum" command.

```
# yum install mod_ssl
```

2. Preparing SSL certificates

- a. You must prepare SSL certificates and SSL certificate key files for HTTPS communication.

SSL certificates can be prepared in the following three ways:

- Reusing the existing SSL certificates and SSL certificate key files that are already installed
- Issuing by the Certificate Authority
- Creating self-signed certificates



Example of creating a self-signed certificate

```
# 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
```

For "Common Name," enter an IP address, FQDN, or a host name.



- Only SSL certificates whose version is X.509 v3 can be used. You can check the version information with the following command.

```
# openssl x509 -text -noout -in certificate_file_path
```

For "certificate_file_path," enter a full pathname of the certificate file.

- A certificate file may be created automatically when installing OpenStack, but it may be created with a version other than X.509 v3. Be sure to use the certificates created in X.509 v3.

b. Store the obtained SSL certificate in the controller node.

- SSL certificate file: /etc/pki/CA/certs/
- SSL certificate key file: /etc/pki/CA/private/

3. Determining port assignment

Determine the port to assign to the Proxy server.

Select a port that is not used by other services on the controller node.

1-1023 cannot be used.

4. Preparing a setting file for OpenStack environment variables

Download the information according to the following procedure. (The procedure may vary depending on the used version/platform.)

- Log in to "OpenStack Dashboard" as an admin user.
- Select the admin icon on the upper-right of the screen.
- Select "OpenStack RC File v3" to download.

You can also use the file created when installing OpenStack.

5. Retrieving the OpenStack endpoint information

Execute the following command on the controller node to retrieve the following four types of URL information and two types of version information. Retrieve the last "vx" part of the URL for the version information.

- URL and version of the item where "Service Type" is "identity" and "Interface" is "public"
- URL of the item where "Service Type" is "network" and "Interface" is "public"
- URL of the item where "Service Type" is "image" and "Interface" is "public"
- URL and version of the item where "Service Type" is "compute" and "Interface" is "public"

Execute the following command on the controller node.

```
source <OpenStack environment variable settings file>; unset OS_SERVICE_TOKEN; export OS_PASSWORD=<OpenStack_PASSWORD>; openstack endpoint list
```

Example:

```
source keystone_admin; unset OS_SERVICE_TOKEN; export OS_PASSWORD=password; openstack endpoint list
```

Example of output:

```
+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+
| ID | Region | Service Name | Service Type | Enabled | Interface | URL |
+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+
| 01d7dd66d19947d5870acec413876ba2 | RegionOne | keystone | identity | True | public | http://
192.168.30.86:5000/v3 |
| 04005c8d71a544e596b9e40083fa7206 | RegionOne | placement | placement | True | internal | http://
192.168.30.86:8778/placement |
| 0797675ff3c64da58a57a4988ec44a2b | RegionOne | cinderv2 | volumev2 | True | admin
| http://192.168.30.86:8776/v2/?(tenant_id)s |
| 09ae73e20c004030ae04a7f5d8bf048a | RegionOne | placement | placement | True | admin | http://
192.168.30.86:8778/placement |
| 12d9cbc0b1de4bf5a63d6819ec274685 | RegionOne | swift | object-store | True | internal | http://
192.168.30.86:8080/v1/AUTH_?(tenant_id)s |
| 201c7c5ecef54c0691c043eafe6087ae | RegionOne | neutron | network | True | admin
| http://192.168.30.86:9696 |
| 32920d76f674494d9a9dd98e06c9e229 | RegionOne | gnocchi | metric | True | internal
```

http://192.168.30.86:8041	
3ff445febbec434aafc70c964dc3dbdc RegionOne ceilometer metering True internal http://192.168.30.86:8777	
42f8a5c483ef43f18e736b622c2d5cf8 RegionOne cinderv2 volumev2 True internal http://192.168.30.86:8776/v2/(tenant_id)s	
4aba919df7f947bbaf7a19918fadd01e RegionOne swift object-store True admin http://192.168.30.86:8080/v1/AUTH_(tenant_id)s	
4b8c976fe4e742018b0fd4177dcae429 RegionOne cinderv3 volumev3 True admin http://192.168.30.86:8776/v3/(tenant_id)s	
5b61335921c247689906b1bf390a45e7 RegionOne cinderv2 volumev2 True public http://192.168.30.86:8776/v2/(tenant_id)s	
676ec9c2044947fea66b15f6168465de RegionOne gnocchi metric True admin http://192.168.30.86:8041	
6855184db088496baabb85f5a70021f4 RegionOne aodh alarming True internal http://192.168.30.86:8042	
8944c76fb0784089b1f7f56c94388530 RegionOne nova compute True public http://192.168.30.86:8774/v2.1/(tenant_id)s	
930030ede13049439e2933665e91a3b4 RegionOne cinderv3 volumev3 True public http://192.168.30.86:8776/v3/(tenant_id)s	
9503ad1f5e754993838fa53fd5d58690 RegionOne nova compute True admin http://192.168.30.86:8774/v2.1/(tenant_id)s	
9541b01381404c4cb200dcbeea0168c4 RegionOne keystone identity True admin http://192.168.30.86:35357/v3	
98f00b9d75564ba29e92ccd5fdccb376 RegionOne keystone identity True internal http://192.168.30.86:5000/v3	
9ae897c5ae704d9aa142b7b61c728468 RegionOne aodh alarming True admin http://192.168.30.86:8042	
9bdc57b0a32e40148e2a049ba9211e8b RegionOne placement placement True public http://192.168.30.86:8778/placement	
b0ea3c01f909451bafb57ccc2e5a6e32 RegionOne glance image True admin http://192.168.30.86:9292	
b75f5ae0fc8644fc9859ef37d4a4afc5 RegionOne ceilometer metering True public http://192.168.30.86:8777	
b7dellad749b4d0f9b593446794c355c RegionOne swift object-store True public http://192.168.30.86:8080/v1/AUTH_(tenant_id)s	
b82ce3bd754a46289838cdc4ec17fd0f RegionOne cinder volume True public http://192.168.30.86:8776/v1/(tenant_id)s	
be3d757e64a945f8b0cdf784f0167ff8 RegionOne neutron network True internal http://192.168.30.86:9696	
c70161c0b104474f8fld15fee74b222f RegionOne gnocchi metric True public http://192.168.30.86:8041	
c89faf6e8b9d4b3f9823d1a7e490e45b RegionOne cinder volume True internal http://192.168.30.86:8776/v1/(tenant_id)s	
cbd56dff0a5d4fe4b1a705e820115fd6 RegionOne ceilometer metering True admin http://192.168.30.86:8777	
dab0b8fa23c943a787803e0fd5e00450 RegionOne nova compute True internal http://192.168.30.86:8774/v2.1/(tenant_id)s	
dbaf3b9d826d49ec8955623bf57cd7ec RegionOne neutron network True public http://192.168.30.86:9696	
e2fff591156f4176a13aad68c7e0e000 RegionOne glance image True internal http://192.168.30.86:9292	
ecda799534b144e7a48dbe8c4e99836a RegionOne cinderv3 volumev3 True internal http://192.168.30.86:8776/v3/(tenant_id)s	
f9052dd300904e8c80fca87fdb8bc2a1 RegionOne glance image True public http://192.168.30.86:9292	
fa9b861b2e14423baba72aa08bf2953d RegionOne aodh alarming True public http://192.168.30.86:8042	
fd768ee6e3844bd982e27b6cd3501c5b RegionOne cinder volume True admin http://192.168.30.86:8776/v1/(tenant_id)s	
-----+	-----+
-----+	-----+

Example of retrieval:

Service Type	URL	Version
identity	http://192.168.30.86:5000/v3	v3
network	http://192.168.30.86:9696	-
image	http://192.168.30.86:9292	-
compute	http://192.168.30.86:8774/v2.1	v2.1

6. Retrieving the OpenStack endpoint information with version information

Retrieve the URL with the version information and the version of the URL for network and image with the curl command.

Retrieve the last "vx" part of the URL for the version information.

If there are multiple results, use the href key where "status" is "CURRENT."

- For network

Execute the following command.

```
# curl -k <url of network>
```

Example:

```
# curl -k "http://192.168.30.86:9696"
```

Example of output:

```
{ "versions": [ { "status": "CURRENT", "id": "v2.0", "links": [ { "href": "http://192.168.30.86:9696/v2.0/", "rel": "self" } ] } ] }
```

Example of retrieval:

Service Type	URL	Version
network	http://192.168.30.86:9696/v2.0	v2.0

- For image

Execute the following command.

```
# curl -k <url of image>
```

Example:

```
# curl -k "http://192.168.30.86:9292"
```

Example of output:

```
{ "versions": [ { "status": "CURRENT", "id": "v2.5", "links": [ { "href": "http://192.168.30.86:9292/v2/", "rel": "self" } ] }, { "status": "SUPPORTED", "id": "v2.4", "links": [ { "href": "http://192.168.30.86:9292/v2/", "rel": "self" } ] }, { "status": "SUPPORTED", "id": "v2.4", "links": [ { "href": "http://192.168.30.86:9292/v2/", "rel": "self" } ] }, { "status": "SUPPORTED", "id": "v2.2", "links": [ { "href": "http://192.168.30.86:9292/v2/", "rel": "self" } ] }, { "status": "SUPPORTED", "id": "v2.1", "links": [ { "href": "http://192.168.30.86:9292/v2/", "rel": "self" } ] }, { "status": "SUPPORTED", "id": "v2.0", "links": [ { "href": "http://192.168.30.86:9292/v2/", "rel": "self" } ] }, { "status": "DEPRECATED", "id": "v1.1", "links": [ { "href": "http://192.168.30.86:9292/v1/", "rel": "self" } ] }, { "status": "DEPRECATED", "id": "v1.0", "links": [ { "href": "http://192.168.30.86:9292/v1/", "rel": "self" } ] } ] }
```

Example of retrieval:

Service Type	URL	Version
image	http://192.168.30.86: 9292/v2	v2

7. Changing Apache SSL settings

- a. Create a setting file with an arbitrary name by referring to the following example. The file extension must be ".conf."

```
Listen <Port number determined in Step 3>
<VirtualHost *: <Port number determined in Step 3>>
    ServerName <IP address of the controller node, FQDN or host name>
    SSLEngine on
    SSLProtocol all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
    SSLCipherSuite HIGH:MEDIUM:!aNULL:!MD5:!SEED:!IDEA:!3DES:!RC4:!DH
    SSLHonorCipherOrder on
    SSLCertificateFile <Full pathname of SSL certificate>
    SSLCertificateKeyFile <Full pathname of SSL certificate key file>
    LogLevel notice
    ErrorLog /var/log/httpd/ssl_openstack_api_error.log
    ServerSignature Off
    CustomLog /var/log/httpd/ssl_openstack_api_access.log combined
    <Location /identity>
        ProxyPass <URL of "identity" retrieved in Step 5>
        Header set x-openstack-api-version <version of "identity" retrieved in Step 5>
    </Location>
    <Location /network>
        ProxyPass <URL of network retrieved in Step 5>
        Header set x-openstack-api-version <version of "network" retrieved in Step 6>
    </Location>
    <Location /compute>
        ProxyPass <URL of "compute" retrieved in Step 5>
        Header set x-openstack-api-version <version of "compute" retrieved in Step 6>
    </Location>
    <Location /image>
        ProxyPass <URL of "image" retrieved in Step 5>
        Header set x-openstack-api-version <version of "image" retrieved in Step 6>
    </Location>
</Virtualhost>
```

Example:

```
Listen 5001
<VirtualHost *:5001>
    ServerName 192.168.30.86
    SSLEngine on
    SSLProtocol all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
    SSLCipherSuite HIGH:MEDIUM:!aNULL:!MD5:!SEED:!IDEA:!3DES:!RC4:!DH
    SSLHonorCipherOrder on
    SSLCertificateFile /etc/pki/CA/certs/server.crt
    SSLCertificateKeyFile /etc/pki/CA/private/server.key
    LogLevel notice
    ErrorLog /var/log/httpd/ssl_openstack_api_error.log
    ServerSignature Off
    CustomLog /var/log/httpd/ssl_openstack_api_access.log combined
    <Location /identity>
        ProxyPass http://localhost:5000/v3
        Header set x-openstack-api-version v3
    </Location>
    <Location /network>
        ProxyPass http://localhost:9696/v2.0
        Header set x-openstack-api-version v2.0
    </Location>
    <Location /compute>
        ProxyPass http://localhost:8774/v2.1
        Header set x-openstack-api-version v2.1
    </Location>
```

```
</Location>
<Location /image>
    ProxyPass http://localhost:9292/v2
    Header set x-openstack-api-version v2
</Location>
</Virtualhost>
```

- b. Store an Apache SSL settings file.

Store in the following path.

```
/etc/httpd/conf.d/
```

- c. Reload the Apache settings.

Execute the following command from the terminal as a root user.

```
systemctl reload httpd
```

8. Setting a Firewall

Use the following command to allow the specified port.

- Command to confirm the port allowance status

```
iptables -nL --line-numbers
```

- Command to open a port

```
iptables -I INPUT 1 -p tcp --dport <port> -s <IP address of ISM> -j ACCEPT
```

Example of a command to open a port.

```
iptables -I INPUT 1 -p tcp --dport 5001 -s 192.168.0.101 -j ACCEPT
```

- Command to save settings

```
/sbin/service iptables save
```

- Command to close a port

```
iptables -D INPUT <No>
```

Example of a command to close a port

```
iptables -D INPUT 1
```

B.12.2 Settings when using Virtualized Network Analysis

1. Editing "/etc/nova/nova.conf"

- a. Open the "/etc/nova/nova.conf" file.

```
# vi /etc/nova/nova.conf
```

- b. Add the following two items in a separate line for each.

Key	Value
scheduler_available_filters	arbitrary
scheduler_default_filters	SameHostFilter

Example:

```
scheduler_available_filters = nova.scheduler.filters.all_filters
scheduler_default_filters =
SameHostFilter,RetryFilter,AvailabilityZoneFilter,RamFilter,DiskFilter,ComputeFilter,Comput
eCapabilitiesFilter,ImagePropertiesFilter,ServerGroupAntiAffinityFilter,ServerGroupAffinity
Filter
```

2. Restarting the nova service

Execute the following command on the controller node.

Enter the command in a line.

```
for service in api consoleauth conductor scheduler novncproxy; do systemctl restart openstack-
nova-$service; done
```

B.13 Setting Procedure for Monitoring Targets (Cloud Management Software: Microsoft Failover Cluster (Azure Stack HCI))

ISM communicates with Microsoft Failover Cluster (Azure Stack HCI). The following settings are required for communication.

B.13.1 Settings When Using a Domain User Account

1. Setting WinRM for respective hosts configuring a cluster

To retrieve the information from Microsoft Failover Cluster (Azure Stack HCI), settings for respective hosts that configure a cluster must have already been completed. Refer to "[B.7 Setting Procedure for Monitoring Targets \(OS: Azure Stack HCI\)](#)" to execute the settings for respective hosts.

2. Adding an SPN to Active Directory

You must correctly register a Service Principal Name (SPN) of a monitoring target cluster on Active Directory when monitoring an Azure Stack HCI using the domain user account. Execute the following procedure to register the Service Principal Name of the monitoring target cluster.

```
> setspn -S HTTP/<monitoring target cluster IP> <monitoring target cluster name>
```



Command for checking

```
>setspn -L <monitoring target cluster name>
```

If the command result as shown below is output, the registration has succeeded.

```
HTTP/<monitoring target cluster IP>
```

3. Adding domain information to ISM-VA

When executing Monitoring using the domain user account, follow the procedures in "[3.4.2 Initial Setup of ISM-VA.](#)"

4. Adding DNS information to ISM-VA

When executing Monitoring with the domain user account, follow the procedures in "Add DNS server" in "[4.9 Network Settings](#)" to register the DNS server on ISM-VA.

5. Kerberos delegation configuration for Active Directory

- a. Log on to the Active Directory server.
- b. Open Server Manager.
- c. From the [Tool] button, select [Active Directory Users and Computers].

- d. Expand the domain, and then expand the [Computers] folder.
- e. Right-click the cluster node name or cluster name on the right-side window, and then select [Properties].
- f. From the [General] tab, select the [Trust computer for delegation to any service (Kerberos only)] checkbox.
- g. Select [OK] and repeatedly perform the above Step e to f for all the cluster nodes or cluster.

Appendix C Uninstallation of ISM-VA

Uninstall ISM-VA according to the installation destination.

Each uninstall procedure is described below.

- [Uninstalling from Microsoft Windows Server Hyper-V](#)
- [Uninstalling from VMware vSphere Hypervisor 6.5 or later](#)
- [Uninstalling from KVM](#)
- [Uninstall from Nutanix AHV](#)

Uninstalling from Microsoft Windows Server Hyper-V

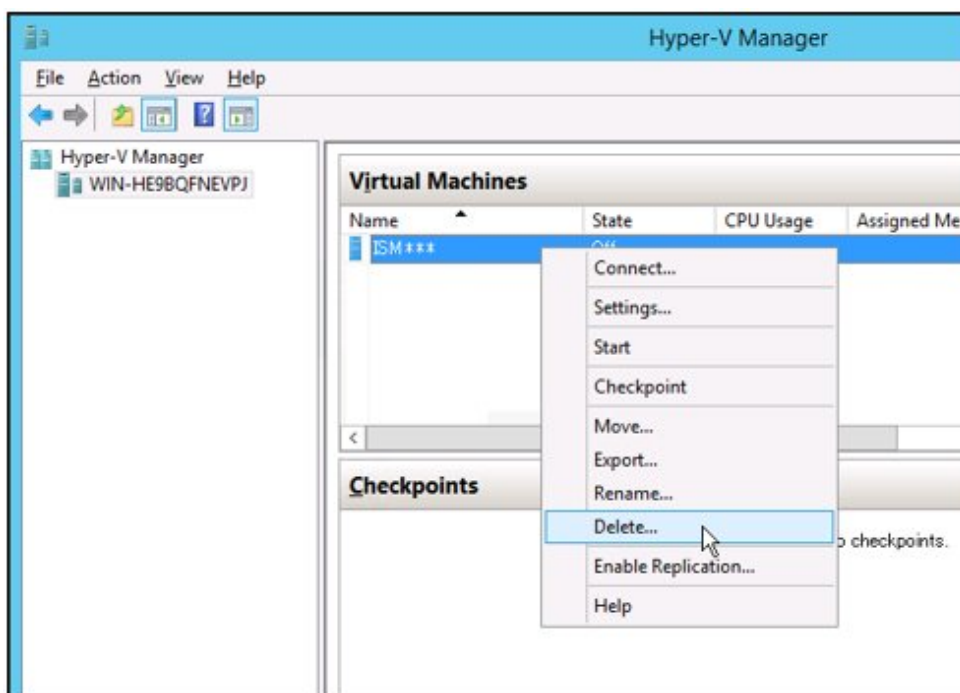
1. Stop ISM-VA.

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].



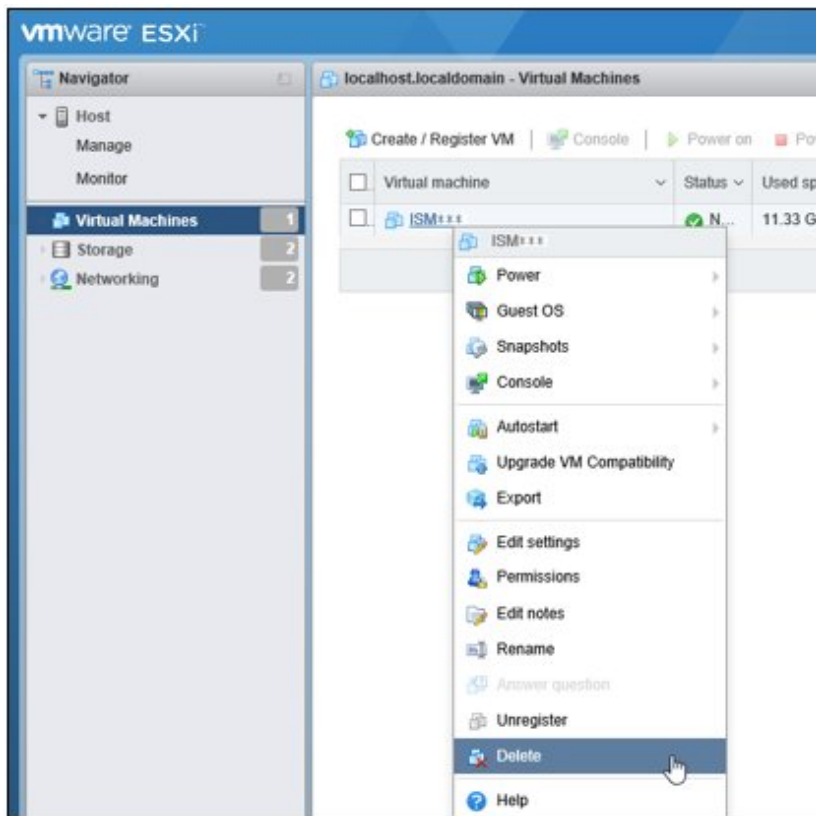
4. Use Explorer to remove the virtual hard disk for which you took the memo in Step 2.

Uninstalling from VMware vSphere Hypervisor 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].

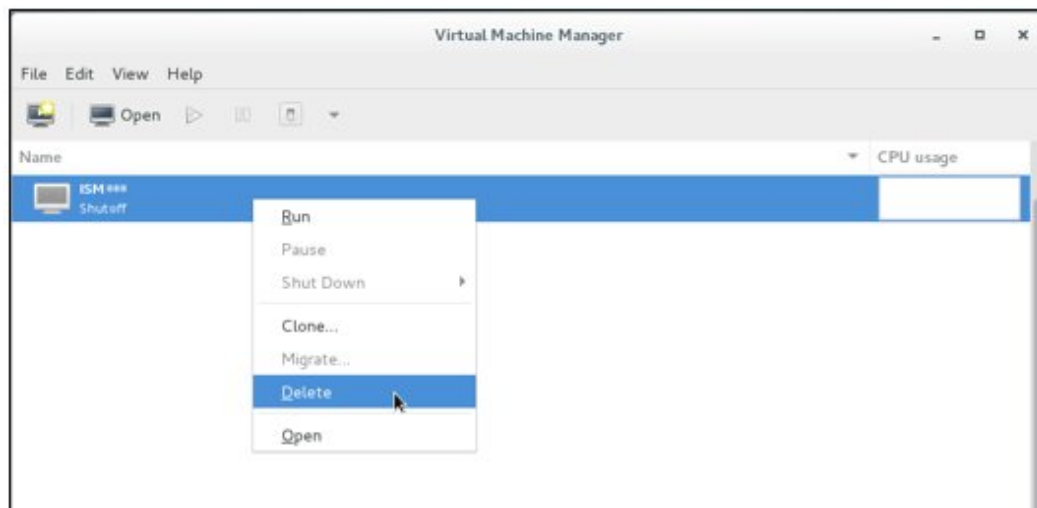


Uninstalling from KVM

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].

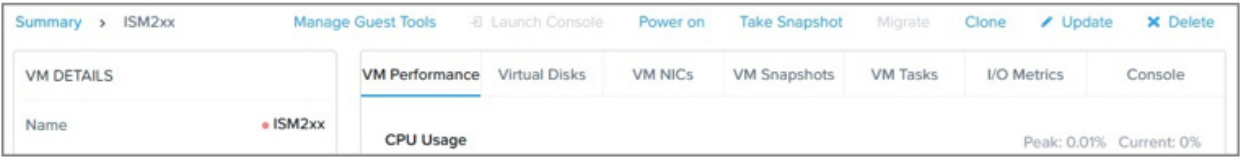


Uninstall from Nutanix AHV

1. Stop ISM-VA.

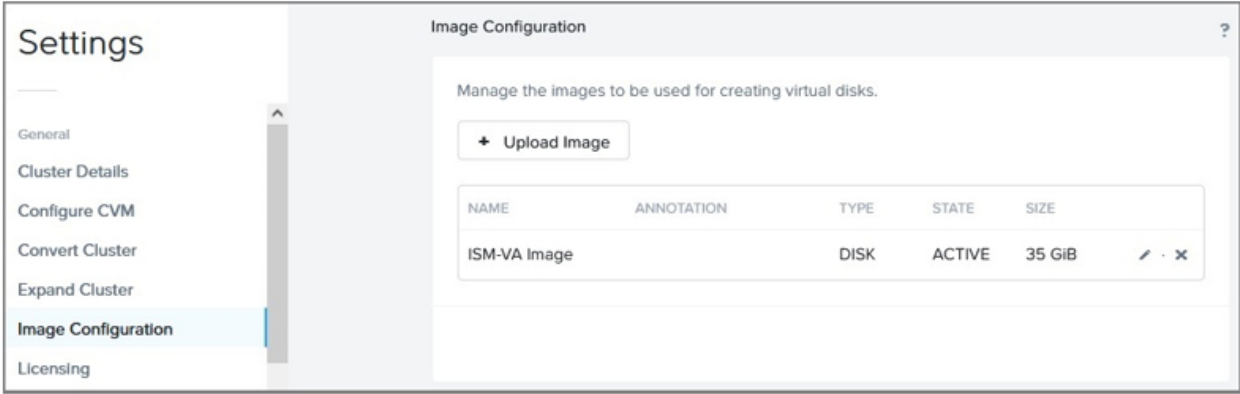
For details, refer to "[4.1.2 Stop of ISM-VA.](#)"

2. In Nutanix PRISM, select the [Table] on the [VM] screen.



3. Select the ISM-VA virtual machine and select [Delete] to remove it.

4. In Nutanix PRISM, select the [Settings] menu - [Image Configuration]. Delete the ISM-VA image on the displayed screen.



Appendix D Requirements for Cluster Creation and Cluster Expansion in PRIMEFLEX HS/ PRIMEFLEX for VMware vSAN

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.

D.1 Addable Servers

For a model of addable servers for each type of servers at the time of purchase, refer to "Support Matrix."

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

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

Select [DOWNLOADS] and select the target operating system.

The reference procedures are subject to change without notice.

D.2 Cluster Creation and Cluster Expansion for ADVN Configurations

For configurations running the ADVN of PRIMEFLEX HS or PRIMEFLEX for VMware vSAN, if you want to manage the added server with ADVN, you must use the KB below to apply a version of ESXi/vCSA that supports the functional level of ADVN.

The functional level of PRIMEFLEX HS 1.0 is "Windows Server 2012R." The functional level of PRIMEFLEX HS 1.1 and PRIMEFLEX for VMware vSAN is "Windows Server 2016."

- vCenter Server

<https://kb.vmware.com/s/article/2071592>

- ESXi

<https://kb.vmware.com/s/article/2113023>

User management with ESXi/vCSA Active Directory may not be supported in the future.

If you execute Cluster Expansion using an ESXi/vCSA version that does not support user management with Active Directory, you must change your user management with Active Directory to local account management.

D.3 Network Configuration

When adding a server, match the physical/logical network configuration for the Management LAN/vMotion LAN/vSAN LAN to the configuration for the server at the time of purchase.

For the network interface of the existing servers and servers for expanding a cluster (10GBase/10GBase-T, 25GBase/25GBase-T), select the same port.

The physical network configuration for the existing servers and servers for expanding a cluster is as follows. The additionally installed LAN cards that are not used by Management LAN, vMotion LAN, and vSAN LAN are not included.

Table D.1 Network configuration for PRIMEFLEX HS

Item	Existing server and Network configuration		Servers for expanding a cluster and Network configuration	
Server	PRIMERGY RX2530 M2 PRIMERGY RX2540 M2	PRIMERGY CX2550 M2	PRIMERGY RX2530 M2 PRIMERGY RX2540 M2 PRIMERGY RX2530 M4 PRIMERGY RX2540 M4	PRIMERGY CX2550 M2 PRIMERGY CX2560 M4 PRIMERGY CX2560 M5

Item	Existing server and Network configuration		Servers for expanding a cluster and Network configuration	
			PRIMERGY RX2530 M5 PRIMERGY RX2540 M5	
Network Configuration	- Port expansion option: 10G x2 ports - PCI: 10G x2 ports	- Port expansion option: 1G x2 ports - PCI: 10G x2 ports	- Port expansion option: 10G x2 ports - PCI: 10G x2 ports	- Port expansion option: 10G x2 ports - PCI: 1G x2 ports

Table D.2 Network configuration for PRIMEFLEX for VMware vSAN

Item	Existing server and Network configuration	Servers for expanding a cluster and Network configuration
Server	PRIMERGY RX2530 M4 PRIMERGY RX2540 M4 PRIMERGY CX2560 M4	PRIMERGY RX2530 M4 PRIMERGY RX2540 M4 PRIMERGY CX2560 M4 PRIMERGY RX2530 M5 PRIMERGY RX2540 M5 PRIMERGY CX2560 M5 PRIMERGY RX2530 M6 PRIMERGY RX2540 M6
	PRIMERGY RX2530 M5 PRIMERGY RX2540 M5 PRIMERGY CX2560 M5 PRIMERGY RX4770 M5	PRIMERGY RX2530 M5 PRIMERGY RX2540 M5 PRIMERGY CX2560 M5 PRIMERGY RX4770 M5 PRIMERGY RX2530 M6 PRIMERGY RX2540 M6 PRIMERGY RX2530 M7 PRIMERGY RX2540 M7
	PRIMERGY RX2530 M6 PRIMERGY RX2540 M6	PRIMERGY RX2530 M6 PRIMERGY RX2540 M6 PRIMERGY RX2530 M7 PRIMERGY RX2540 M7
	PRIMERGY RX2530 M7 PRIMERGY RX2540 M7	PRIMERGY RX2530 M7 PRIMERGY RX2540 M7
Network Configuration	- Port expansion option: 10G/25G x 2 ports - PCI: 10G/25G x 2 ports	- Port expansion option: 10G/25G x 2 ports - PCI: 10G/25G x 2 ports

Figure D.1 Network configuration when adding PRIMERGY RX2530 M4/PRIMERGY RX2530 M5 in a PRIMERGY RX2530 M2 environment of PRIMEFLEX HS

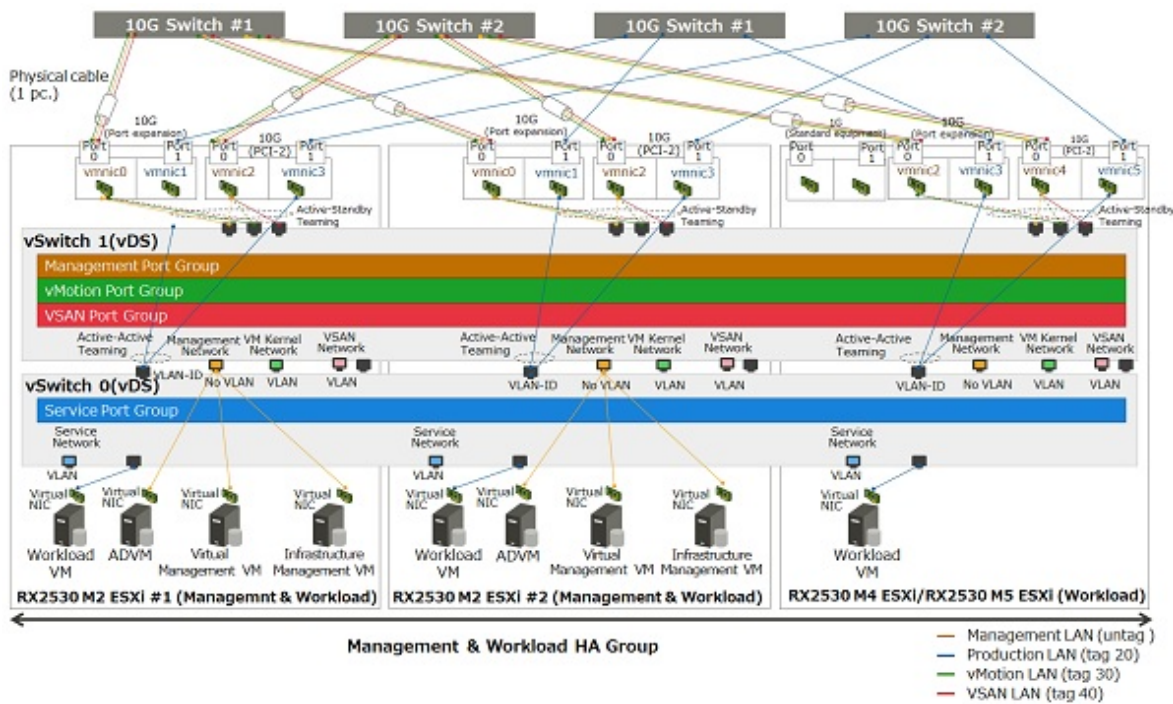
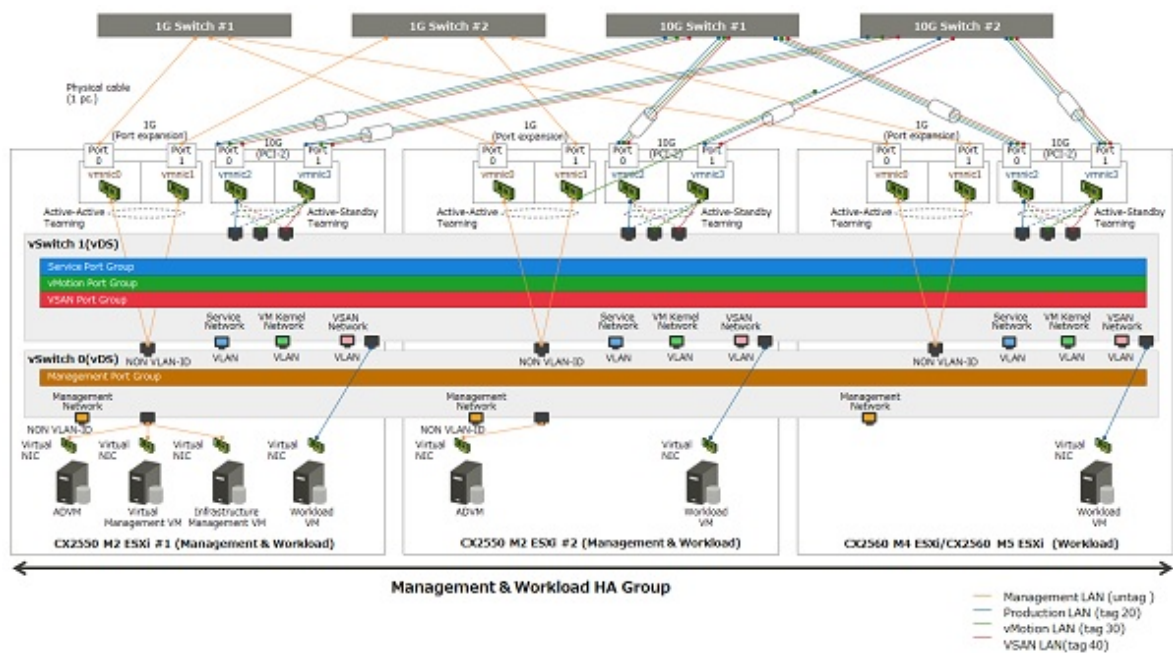


Figure D.2 Network configuration when adding PRIMERGY CX2560 M4/PRIMERGY CX2560 M5 in a PRIMERGY CX2550 M2 environment of PRIMEFLEX HS



D.4 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.

The following are the options that are relevant for the existing servers and the servers for expanding a cluster. The following options are also for the servers for creating a new cluster:

- Base unit
- CPU
- Memory
- HDD
- SSD
- Onboard LAN (Flexible LOM, etc.)
- 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.

D.4.1 Base unit

The server types listed in "[D.1 Addable Servers](#)" can be added.

D.4.2 CPU

Since the CPU generations that can be installed on existing servers and servers for expanding a cluster are different, it is recommend that CPUs installed in the servers for expanding a cluster are equal to or higher than those installed in existing servers.

"CPUs equal to or higher than" means that the both number of cores and clocks are equal to or higher than the CPU installed in the existing server.

The number of CPUs is to be the same as that of existing servers.

Depending on the CPU installed in the existing server, there may be cases in which there are no CPUs equal to or higher than the CPUs that can be installed 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.

D.4.3 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 one 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.

D.4.4 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. Also, use the same model name for all the HDDs mounted on the servers configuring a new cluster.

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 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).

D.4.5 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. Also, use the same model name for all the SSDs mounted on the servers configuring a new cluster.

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)	

D.4.6 Onboard LAN (Flexible LOM, etc.)

Select the option with the communication speed/number of ports described in "[D.3 Network Configuration](#)."

D.4.7 SAS Controller Card

Select the SAS controller card for the vSAN connection available for each generation of servers.

SAS controller cards must have firmware that supports the ESXi/vSAN version being deployed.

Update the SAS controller card firmware if necessary.

For the relationship between the vSAN version and firmware version, contact your local Fujitsu customer service partner.

Since a combination of SAS controller card firmware and driver versions are used for vSAN Ready Node authentication, you must update the driver when you update the firmware.

The firmware/driver versions can be inconsistent between nodes. However, updating to the latest version is recommended due to performance impact, troubleshooting, etc.

D.4.8 Option Card (LAN card that is required to be mounted)

As described in "D.3 Network Configuration," this is 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.

The network interface (10GBase/10GBase-T, 25GBase/25GBase-T) must be the same as the existing server.

D.4.9 Other Options

For options other than the above, you can select them according to the requirements for each PRIMEFLEX or your environment because they are not related to servers for expanding a cluster.

D.5 Software Requirements

D.5.1 Software Version

You must install the same version of software for both existing servers and servers for expanding a cluster.

If the software installed on the existing server is not supported by the servers for expanding a cluster, update the software of the existing servers before adding a server. Also, update the software on the existing servers when creating a new cluster.

The update policy for the software installed on each PRIMEFLEX are as follows.

Software name	Where to install	Version
ESXi	<ul style="list-style-type: none">- Server for expanding a cluster- Existing servers	<p>Install a version that is supported by both the servers for expanding a cluster and the existing servers.</p> <p>Select the same version for both the servers for expanding a cluster and the existing servers (including build numbers).</p>
vSAN	<ul style="list-style-type: none">- Server for expanding a cluster- Existing servers	<p>Install a version that is supported by both the servers for expanding a cluster and the existing servers.</p> <p>Select the same version for both the servers for expanding a cluster and the existing servers (including build numbers).</p>
vCenter Server (vCSA)	Virtual Management VM	Install the same version as ESXi or a later version.
Windows Server (ADVM)	ADVM	Install the version at the time of purchase.
ISM for PRIMEFLEX	Infrastructure Management VM	Install a version which supports ESXi/vSAN of both the server for expanding a cluster and the existing servers.
ServerView RAID Manager	ADVM	Install a version which supports ESXi of both the server for expanding a cluster and the existing servers.
ServerView Suite DVD	Infrastructure Management VM	<p>Import the ServerView Suite DVD into ISM for PRIMEFLEX.</p> <p>Confirm that the ServerView Installation Manager on the ServerView Suite DVD to be imported meets the following requirement.</p> <ul style="list-style-type: none">- Supports the versions of custom images to be installed on the servers for expanding a cluster

D.5.2 Confirmation of Software Version

Check the version of ESXi that is installed on the ESXi host of the vSAN cluster, which is the destination for cluster expansion.

For the supported version, contact your local Fujitsu customer service partner.

If your ESXi version is not supported, you must update the software. Check the ESXi versions that are supported on the servers for expanding a cluster and determine the ESXi version for the updates.

After determining the ESXi version for servers for expanding a cluster, check the version of the following software for which the ESXi version is supported. Also, check the software on the existing servers when creating a new cluster.

- PRIMERGY firmware version
- vCSA version
- ISM for PRIMEFLEX version
- RAID Manager version
- ServerView Installation version and the version of the ServerView Suite DVD that contains ServerView Installation

D.5.3 Confirmation of SAS Controller Card Firmware Version

Check that the SAS controller card firmware version supports the ESXi version that is determined in "D.5.2 Confirmation of Software Version."

For the supported versions, contact your local Fujitsu customer service partner.

The relationship between the ESXi version and vSAN version can be checked on the following website.

<https://kb.vmware.com/s/article/2150753>

If you updated your SAS controller card firmware version, a driver for it may need to be updated.

For details, contact your local Fujitsu customer service partner.

D.6 Sizing of Management VM

Resources of Infrastructure Management VM, Virtual Management VM and ADVN may be insufficient according to the number of servers to be added.

If the 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 Management VM at factory settings and the number of registerable nodes in each model are as follows.

Model name	Management VM name/Software name	Resource amount			Number of registerable nodes
		CPU	Memory	Disk	
PRIMEFLEX HS V1.0	Infrastructure Management VM (ISM for PRIMEFLEX)	4vCPU	16 GB	136 GB	400 nodes
	Virtual Management VM (vCenter Server Appliance)	2vCPU	10 GB	120 GB	Host: 10 units Virtual machine: 100 units
PRIMEFLEX HS V1.1	Infrastructure Management VM (ISM for PRIMEFLEX)	4vCPU	16 GB	136 GB	400 nodes
	Virtual Management VM (if Small is selected) (vCenter Server Appliance)	4vCPU	16 GB	290 GB	Host: 100 units Virtual machine: 1000 units
PRIMEFLEX for VMware vSAN	Infrastructure Management VM (ISM for PRIMEFLEX)	4vCPU	16 GB	100 GB	400 nodes
	Virtual Management VM (if Small is selected) (vCenter Server Appliance)	4vCPU	16 GB	290 GB	Host: 100 units Virtual machine: 1000 units

Appendix E Troubleshooting

This appendix describes the major causes and countermeasures for errors and unexpected behavior in ISM operation.

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 may 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 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 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 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 may 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] - [Firmware/Driver], 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] - [Firmware/Driver], 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] - [Firmware/Driver], 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 encoding 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: 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.

Symptom: After applying ISM patch or upgrade program using the GUI, the following message is displayed on the GUI screen and the application fails. Also, you will not be able to log in from the GUI.

```
Applying ISM patch / upgrade program was failed.
ERROR:50980030:Update failed () (Elapsed: xx:xx:xx)
```

Causes and countermeasures

- The patch or upgrade failed to apply due to insufficient disk space.
- Restarting ISM-VA makes it available in its pre-applied state.
- When applying the ISM patch or upgrade program, make sure that the following sizes of disk space are available in the ISM-VA system area.
Patch: 3.5 GB or more
Upgrade program: 5.5 GB or more

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 Update DVD must have been imported. Confirm that the ServerView Suite Update DVD has been imported for the version of ISM you are using.
- 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 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.

ISM-VA Operation on Nutanix AHV

Symptom: When the ISM-VA IP address is changed, Nutanix PRISM shows the IP addresses before and after the change.

Causes and countermeasures

The Nutanix specification allows PRISM to display the old and new IP addresses for approximately 24 hours after the ISM-VA IP address change. To determine the IP address configured for ISM-VA, use the ismadm or ismsetup command. It does not affect ISM operation.

Appendix F Scripts for Rolling Update for PRIMEFLEX HS/PRIMEFLEX for VMware vSAN

ESXi patches and offline bundles may have restrictions and precautions. For details, contact your local Fujitsu customer service partner. Note that actions can be taken Rolling Update is running by creating a script.

Note that actions can be taken by a script while Rolling Update is running. Create a script as needed. Scripts can be executed at three different times.

- Before applying ESXi patch/offline bundle
- When applying ESXi patch/offline bundle
- After applying ESXi patch/offline bundle

Note

- When applying ESXi patch/offline bundle means status of immediately after executing the apply command and before restarting ESXi. After applying ESXi patch/offline bundle means status of after executing the apply command and restarting ESXi.
- If the script cannot finish within the specified time (720 seconds), Rolling Update fails. If an error is displayed on the ISM "Tasks" screen, check the ISM event log. For information about the messages checked in the event log, refer to "ISM for PRIMEFLEX Messages."

The script name to be executed is fixed. The script name differs depending on the each of the following execution timings.

Script name [Note]	Execution timing
pre_script.sh	Execute before applying ESXi patch/offline bundle
post01_script.sh	Execute when applying ESXi patch/offline bundle
post02_script.sh	Execute after applying ESXi patch/offline bundle

[Note]: Only the shell (bash) script format is supported.

Point

- Error can be detected by exiting the scripts with "exit 1".
- Include the process such as outputting a log file to ESXi to check the execution result of the scripts in post-processing.

Example of scripts to execute before applying

Example scripts are created to execute the following operations required to apply ESXi.

- Deleting tools
- Deleting drivers
- Changing driver settings

Script example for "Deleting tools"

```
#!/usr/bin/sh

### Tool removal ###
echo "Tool removal Start" >> /scratch/log/pre_script.log
toolName=`(esxcli software vib list | grep storcli)`
if [ $? = 0 ]; then
    echo ${toolName} >> /scratch/log/pre_script.log
```

```

    toolName=`(echo ${toolName} | cut -f 1 -d ' ')`
    cmd="esxcli software vib remove -n ${toolName}"
    echo ${cmd} >> /scratch/log/pre_script.log
    eval ${cmd}
    if [ $? != 0 ]; then
        exit 1
    fi
fi
echo "Tool removal End" >> /scratch/log/pre_script.log

echo "pre_script End" >> /scratch/log/pre_script.log
exit 0

```

Script example for "Deleting drivers"

```

#!/usr/bin/sh

### Driver removal ###
echo "Driver removal Start" >> /scratch/log/pre_script.log
driver1=`(esxcli software vib list | grep "OEM.500")`
if [ $? = 0 ]; then
    echo ${driver1} >> /scratch/log/pre_script.log
    driver1Name=`(echo ${driver1} | cut -f 1 -d ' ')`
    cmd="esxcli software vib remove -n \"${driverName1}\""
    echo ${cmd} >> /scratch/log/pre_script.log
    eval ${cmd}
    if [ $? != 0 ]; then
        exit 1
    fi
fi
echo "Driver removal End" >> /scratch/log/pre_script.log

echo "pre_script End" >> /scratch/log/pre_script.log
exit 0

```

Script example for "Changing driver settings"

```

#!/usr/bin/sh

### Driver settings ###
echo "Driver settings Start" >> /scratch/log/pre_script.log
driver2=`(esxcli system module list | grep lsi_mr3)`
if [ $? = 0 ]; then
    echo ${driver2} >> /scratch/log/pre_script.log
    cmd="esxcli system module set -e true -m lsi_mr3"
    echo ${cmd} >> /scratch/log/pre_script.log
    eval ${cmd}
    if [ $? != 0 ]; then
        exit 1
    fi
fi
driver3=`(esxcli system module list | grep lsi_msgpt3)`
if [ $? = 0 ]; then
    echo ${driver3} >> /scratch/log/pre_script.log
    cmd="esxcli system module set -e true -m lsi_msgpt3"
    echo ${cmd} >> /scratch/log/pre_script.log
    eval ${cmd}
    if [ $? != 0 ]; then
        exit 1
    fi
fi
echo "Driver settings End" >> /scratch/log/pre_script.log

```

```
echo "pre_script End" >> /scratch/log/pre_script.log
exit 0
```

Example of scripts to execute when applying

Example scripts are created to take actions for precautions for operating and maintenance for ESXi 6.7.

This script is for replacement of the Inbox driver when applying patch "ESXi 670-201905001" or later to ESXi configured with v470-1 custom image.

```
#!/usr/bin/sh

#### parameter settings ####
EffectiveValue='VMware-ESXi-6.7.0-13473784-Fujitsu-v470-1-offline_bundle.zip -n lsi-mr3 -n lsi-
msgpt3'

### Execution command ###
cmd="esxcli software vib install --dry-run -d /var/tmp/RollingUpdatePatch/${EffectiveValue}"
echo ${cmd} >> /scratch/log/post01_script.log
eval ${cmd}
if [ $? != 0 ]; then
    exit 1
fi

cmd="esxcli software vib install -d /var/tmp/RollingUpdatePatch/${EffectiveValue}"
echo ${cmd} >> /scratch/log/post01_script.log
eval ${cmd}
if [ $? != 0 ]; then
    exit 1
fi

echo "post01_script End" >> /scratch/log/post01_script.log
exit 0
```

Example of scripts to execute after applying

Example scripts are created to take the following actions for restrictions/precautions after applying the ESXi patch/offline bundle.

- Precautions for power management settings
- Updating igbn drivers
- Temporary area settings

Script example for "Precautions for power management settings"

```
#!/usr/bin/sh

#### parameter settings ####
PowerValue="High Performance"

### Execution command ###
# Power Policy
echo "Power Policy Start" >> /scratch/log/post02_script.log
CurrentValue=`esxcli system settings advanced list --option=/Power/CpuPolicy | grep '    String
Value: High Performance'`
if [ $? != 0 ]; then
    cmd='esxcli system settings advanced set --option=/Power/CpuPolicy --string-value="High
Performance"'
    echo ${cmd} >> /scratch/log/post02_script.log
    eval ${cmd}
    if [ $? != 0 ]; then
        exit 1
    fi
fi
```

```

echo "Power Policy End" >> /scratch/log/post02_script.log

echo "post02_script End" >> /scratch/log/post02_script.log
exit 0

```

Script example for "Updating igbn drivers"

```

#!/usr/bin/sh

#### parameter settings ####
DriverFile="<applying driver faile name>"

### Execution command ###
# Update Driver
echo "Update Driver Start" >> /scratch/log/post02_script.log
cmd="esxcli software vib install -d /var/tmp/RollingUpdatePatch/${DriverFile}"
echo ${cmd} >> /scratch/log/post02_script.log
eval ${cmd}
if [ $? != 0 ]; then
    exit 1
fi
echo "Update Driver End" >> /scratch/log/post02_script.log

echo "post02_script End" >> /scratch/log/post02_script.log
exit 0

```

Script example for "Temporary area settings"

```

#!/usr/bin/sh

#### parameter settings ####
TemporaryName="scratch"

### Execution command ###
# Temporary
echo "Temporary Start" >> /scratch/log/post02_script.log
TmpSetting=`(vim-cmd hostsvc/advopt/view ScratchConfig.ConfiguredScratchLocation | grep "value")`
TmpDir=`(echo ${TmpSetting} | cut -f 2 -d ' ')`
if [ ${#TmpDir} = 0 ]; then
    cmd="mkdir /var/tmp/${TemporaryName}"
    echo ${cmd} >> /scratch/log/post02_script.log
    eval ${cmd}
    if [ $? != 0 ]; then
        exit 1
    fi
    cmd="vim-cmd hostsvc/advopt/update ScratchConfig.ConfiguredScratchLocation string /var/tmp/${TemporaryName}"
    echo ${cmd} >> /scratch/log/post02_script.log
    eval ${cmd}
    if [ $? != 0 ]; then
        exit 1
    fi
fi
echo "Temporary End" >> /scratch/log/post02_script.log

echo "post02_script End" >> /scratch/log/post02_script.log
exit 0

```



The first line of the script must include the following statement.

```
#!/usr/bin/sh
```



Note

Do not include the process of restarting the target node in the script you create. Restart is always needed after the script is executed.