

FUJITSU Software

ServerView Infrastructure Manager V2.1



User's Manual

CA92344-1716-01
July 2017

Preface

Purpose

This manual describes the installation procedure and the general functions of FUJITSU Software ServerView Infrastructure Manager (hereafter referred to as ISM). ISM is an operation and management software that manages and operates ICT equipment, such as servers and storages, and facility equipment, such as PDUs, in an integrated way.

Related Manuals

| Manual Name | Notation in this Manual | Description |
|--|---|---|
| FUJITSU Software ServerView Infrastructure Manager V2.1 User's Manual | ServerView Infrastructure Manager V2.1 User's Manual | This manual describes the ISM functions, the installation procedure, and methods for operation and troubleshooting. It allows you to quickly grasp all functions and all operations of ISM. |
| FUJITSU Software ServerView Infrastructure Manager V2.1 Start Guide | ServerView Infrastructure Manager V2.1 Start Guide | This manual describes an overview of the functions and a workflow for installing ISM. It allows you to quickly grasp the procedures for installing ISM. |
| FUJITSU Software ServerView Infrastructure Manager V2.1 Operating Procedures | ServerView Infrastructure Manager V2.1 Operating Procedures | This manual describes the operating procedures for the initial setup and daily operation (monitoring of nodes, server setups, installation of OSES on servers, updating of server firmware) of ISM. |
| FUJITSU Software ServerView Infrastructure Manager V2.1 Glossary | ServerView Infrastructure Manager V2.1 Glossary | The glossary describes definitions of the terminology that you require to understand for using ISM. |

Together with the manuals mentioned above, you can also see the latest information about ISM by accessing your local support.

For the respective hardware products for management, see the manuals of the relevant hardware.

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

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

Intended Readers

This manual is intended for system administrators, network administrators, facility administrators, and service technicians who have sufficient knowledge of hardware and software.

Notation in this Manual

Notation

Keyboard

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

Symbols

Items that require your special caution are preceded by the following symbols.



Point

.....
Describes the content of an important subject.
.....



Note

Describes an item that requires your attention.

Variables: <xxx>

Represents variables that require replacement by numerical values or text strings in accordance with the environment you are using.

Example: <IP address>

Abbreviation

You may see the following abbreviations in this manual.

| Official name | Abbreviation | |
|---|-----------------------------------|---|
| Microsoft(R) Windows Server(R) 2016 Datacenter | Windows Server 2016 Datacenter | Windows Server 2016 |
| Microsoft(R) Windows Server(R) 2016 Standard | Windows Server 2016 Standard | |
| Microsoft(R) Windows Server(R) 2016 Essentials | Windows Server 2016 Essentials | |
| Microsoft(R) Windows Server(R) 2012 R2 Datacenter | Windows Server 2012 R2 Datacenter | Windows Server 2012 R2 |
| Microsoft(R) Windows Server(R) 2012 R2 Standard | Windows Server 2012 R2 Standard | |
| Microsoft(R) Windows Server(R) 2012 R2 Essentials | Windows Server 2012 R2 Essentials | |
| Microsoft(R) Windows Server(R) 2012 Datacenter | Windows Server 2012 Datacenter | Windows Server 2012 |
| Microsoft(R) Windows Server(R) 2012 Standard | Windows Server 2012 Standard | |
| Microsoft(R) Windows Server(R) 2012 Essentials | Windows Server 2012 Essentials | |
| Microsoft(R) Windows Server(R) 2008 R2 Datacenter | Windows Server 2008 R2 Datacenter | Windows Server 2008 R2 |
| Microsoft(R) Windows Server(R) 2008 R2 Enterprise | Windows Server 2008 R2 Enterprise | |
| Microsoft(R) Windows Server(R) 2008 R2 Standard | Windows Server 2008 R2 Standard | |
| Red Hat Enterprise Linux 7.3 (for Intel64) | RHEL 7.3 | Red Hat Enterprise Linux Or Linux |
| Red Hat Enterprise Linux 7.2 (for Intel64) | RHEL 7.2 | |
| Red Hat Enterprise Linux 7.1 (for Intel64) | RHEL 7.1 | |
| Red Hat Enterprise Linux 6.8 (for Intel64) | RHEL 6.8(Intel64) | |
| Red Hat Enterprise Linux 6.8 (for x86) | RHEL 6.8(x86) | |
| Red Hat Enterprise Linux 6.7 (for Intel64) | RHEL 6.7(Intel64) | |
| Red Hat Enterprise Linux 6.7 (for x86) | RHEL 6.7(x86) | |
| Red Hat Enterprise Linux 6.6 (for Intel64) | RHEL 6.6(Intel64) | |
| Red Hat Enterprise Linux 6.6 (for x86) | RHEL 6.6(x86) | |

| Official name | Abbreviation | |
|--|--|---|
| SUSE Linux Enterprise Server 12 SP1 (for AMD64 & Intel 64) | SUSE 12 SP1(Intel64) Or SLES 12 SP1(Intel64) | SUSE Linux Enterprise Server Or Linux |
| SUSE Linux Enterprise Server 12 (for AMD64 & Intel 64) | SUSE 12(Intel64) Or SLES 12(Intel64) | |
| SUSE Linux Enterprise Server 11 SP4 (for AMD64 & Intel 64) | SUSE 11 SP4(Intel64) Or SLES 11 SP4(Intel64) | |
| SUSE Linux Enterprise Server 11 SP4 (for x86) | SUSE 11 SP4(x86) Or SLES 11 SP4(x86) | |
| VMware(R) vSphere(TM) ESXi 6.5 | VMware ESXi 6.5 | VMware ESXi |
| VMware(R) vSphere(TM) ESXi 6.0 | VMware ESXi 6.0 | |
| VMware(R) vSphere ESXi 5.5 | VMware ESXi 5.5 | |

Terms

For the major terms and abbreviations used in this manual, see "ServerView Infrastructure Manager V2.1 Glossary."

High Risk Activity

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

To Use This Product Safely

This document contains important information required for using this product safely and correctly. Read this manual carefully before using the product. In addition, to use the product safely, the customer requires to understand the related products (hardware and software) before using the product. Be sure to use the product by following the notes 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 involving decompiling or disassembly.

Disclaimers

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

Trademarks

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

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

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

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

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

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

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

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

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

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

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 Fujitsu Limited 2017 All rights reserved

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

Contents

| | |
|---|----|
| Chapter 1 Overview of ServerView Infrastructure Manager..... | 1 |
| 1.1 Overview..... | 1 |
| 1.2 Overview of Function..... | 2 |
| 1.2.1 Overview of Node Management..... | 2 |
| 1.2.2 Overview of Monitoring..... | 2 |
| 1.2.3 Overview of Profile Management..... | 3 |
| 1.2.4 Overview of Log Management..... | 3 |
| 1.2.5 Overview of Firmware Management..... | 3 |
| 1.2.6 Overview of Network Management..... | 3 |
| 1.2.7 Overview of the Virtual Resource Management Function..... | 4 |
| 1.3 ISM Functions and Scenarios of Infrastructure Operation and Management..... | 4 |
| 1.3.1 Images of ISM Functions for Each Scenario of Infrastructure Operation and Management..... | 4 |
| 1.4 Configuration..... | 7 |
| 1.5 System Requirements..... | 9 |
| 1.5.1 System Requirements for ISM-VA (Virtual Machines)..... | 9 |
| 1.5.2 System Requirements for Management Terminals..... | 9 |
| 1.5.3 Service Requirements Required for ISM Operations..... | 10 |
| 1.5.4 Operation Requirements for Virtual Resources..... | 12 |
| 1.6 Precautions..... | 12 |
| Chapter 2 Functions of ISM..... | 14 |
| 2.1 User Interface..... | 14 |
| 2.1.1 GUI..... | 14 |
| 2.1.2 FTP Access..... | 16 |
| 2.1.3 Console Access..... | 18 |
| 2.2 Functions of ISM..... | 18 |
| 2.2.1 Node Management..... | 19 |
| 2.2.1.1 Registration of Datacenters/Floors/Racks/Nodes..... | 19 |
| 2.2.1.2 Confirmation of Datacenters/Floors/Racks/Nodes..... | 25 |
| 2.2.1.3 Edit of Datacenters/Floors/Racks/Nodes..... | 25 |
| 2.2.1.4 Deletion of Datacenters/Floors/Racks/Nodes..... | 26 |
| 2.2.2 Monitoring..... | 27 |
| 2.2.3 Profile Management..... | 33 |
| 2.2.4 Firmware Management..... | 42 |
| 2.2.4.1 Confirmation of Firmware Versions of Nodes..... | 42 |
| 2.2.4.2 Firmware Update..... | 42 |
| 2.2.4.3 Confirmation of Documentation that Is Supplied with Firmware Data..... | 47 |
| 2.2.5 Log Management..... | 47 |
| 2.2.6 Network Management..... | 59 |
| 2.2.7 Power Capping..... | 66 |
| 2.2.8 Virtual Resource Management Function..... | 67 |
| 2.2.8.1 Supported Virtual Resources..... | 68 |
| 2.2.8.2 Virtual Resource Management GUI..... | 69 |
| 2.2.8.3 Operation of Virtual Resource Management..... | 70 |
| 2.2.9 Virtual IO Management..... | 77 |
| 2.3 Functions of ISM Operating Platform..... | 78 |
| 2.3.1 User Management..... | 79 |
| 2.3.1.1 Managing ISM Users..... | 84 |
| 2.3.1.2 Managing User Groups..... | 85 |
| 2.3.1.3 Operating in Link with Microsoft Active Directory or LDAP..... | 88 |
| 2.3.1.4 Managing node groups..... | 91 |
| 2.3.2 Repository Management..... | 93 |
| 2.3.3 Installing Emulex OneCommand Manager CLI and Qlogic QConvergeConsole CLI..... | 98 |
| 2.3.4 Task Management..... | 99 |
| 2.3.5 ISM-VA Management..... | 99 |

| | |
|---|-----|
| 2.3.5.1 List of Commands in ISM-VA Management..... | 100 |
| 2.3.6 Management of Cloud Management Software..... | 103 |
| 2.4 Operations When Deleting Nodes and When Modifying Groups..... | 105 |
| 2.4.1 When Deleting Nodes..... | 105 |
| 2.4.2 When Modifying or Dissolving Groups..... | 105 |
| 2.4.3 When Deleting User Groups..... | 105 |
| 2.4.4 When Changing User Group Names..... | 106 |
| Chapter 3 Installation of ISM..... | 107 |
| 3.1 Workflow for Installing ISM..... | 107 |
| 3.2 Installation Design for ISM..... | 107 |
| 3.2.1 Estimation of Disk Resources..... | 108 |
| 3.2.1.1 Estimation of Log Storage Capacity..... | 108 |
| 3.2.1.2 Estimation of Required Capacities for Repositories..... | 109 |
| 3.2.2 Repository Settings..... | 109 |
| 3.2.3 Network Design..... | 109 |
| 3.2.4 Setting of Node Names..... | 110 |
| 3.2.5 Setting of Users..... | 110 |
| 3.3 Installation of ISM-VA..... | 110 |
| 3.3.1 Installation on Microsoft Windows Server Hyper-V..... | 111 |
| 3.3.2 Installation on VMware vSphere Hypervisor..... | 113 |
| 3.3.2.1 Installation on VMware ESXi 5.5 or VMware ESXi 6.0..... | 114 |
| 3.3.2.2 Installation on VMware ESXi 6.5 or later..... | 117 |
| 3.3.3 Installation on KVM..... | 120 |
| 3.4 Environment Settings for ISM-VA..... | 122 |
| 3.4.1 First Start of ISM-VA..... | 123 |
| 3.4.1.1 For ISM-VA Running on Microsoft Windows Server Hyper-V (First Time)..... | 123 |
| 3.4.1.2 For ISM-VA Running on VMware vSphere Hypervisor (First Time)..... | 124 |
| 3.4.1.3 For ISM-VA Running on KVM (First Time)..... | 126 |
| 3.4.2 Initial Settings of ISM..... | 127 |
| 3.4.2.1 Initial Settings Using the Basic Setting Menu..... | 127 |
| 3.4.2.2 Initial Settings Using the ismadm Command..... | 128 |
| 3.5 Registration of Licenses..... | 131 |
| 3.6 Registration of Users..... | 132 |
| 3.7 Allocation of Virtual Disks..... | 132 |
| 3.7.1 Allocation of Virtual Disks to Entire ISM-VA..... | 133 |
| 3.7.2 Allocation of Virtual Disks to User Groups..... | 136 |
| 3.8 Pre-Settings for the Virtual Resource Management Function..... | 139 |
| Chapter 4 Operation of ISM..... | 140 |
| 4.1 Start Up and Termination of ISM..... | 140 |
| 4.1.1 Start Up of ISM..... | 140 |
| 4.1.1.1 For ISM-VA Running on Microsoft Windows Server Hyper-V (Second Time and Later)..... | 140 |
| 4.1.1.2 For ISM-VA Running on VMware vSphere Hypervisor (Second Time and Later)..... | 141 |
| 4.1.1.3 For ISM-VA Running on KVM (Second Time and Later)..... | 144 |
| 4.1.2 Termination of ISM-VA..... | 144 |
| 4.1.3 Restart of ISM-VA..... | 145 |
| 4.1.4 Start Up and Stop of ISM Service..... | 145 |
| 4.2 ISM-VA Basic Settings Menu..... | 146 |
| 4.3 Modification of Destination Port Number..... | 148 |
| 4.4 Back Up and Restoration of ISM-VA..... | 148 |
| 4.4.1 Back Up of ISM-VA..... | 148 |
| 4.4.2 Restoration of ISM-VA..... | 150 |
| 4.5 Collection of Maintenance Data..... | 150 |
| 4.6 Management of Virtual Disks..... | 152 |
| 4.6.1 Cancel of Allocations of Virtual Disks..... | 152 |
| 4.6.2 Allocation of Additional Virtual Disks to Entire ISM-VA..... | 153 |
| 4.6.3 Allocation of Additional Virtual Disks to User Groups..... | 153 |

| | |
|---|-----|
| 4.7 Certificate Activation..... | 154 |
| 4.7.1 Deployment of SSL Server Certificates..... | 154 |
| 4.7.2 Display of SSL Server Certificates..... | 155 |
| 4.7.3 Export of SSL server certificates..... | 155 |
| 4.8 License Settings..... | 155 |
| 4.9 Network Settings..... | 155 |
| 4.10 Event Notification Settings..... | 156 |
| 4.10.1 Registration of Certificates for Event Notification Mails..... | 156 |
| 4.10.2 Registration of Action Scripts..... | 156 |
| 4.10.3 Display of Certificates for Event Notification Mails..... | 157 |
| 4.10.4 Display of Action Scripts..... | 157 |
| 4.10.5 Deletion of Certificates for Event Notification Mails..... | 157 |
| 4.10.6 Deletion of Action Scripts..... | 157 |
| 4.11 ISM-VA Service Control..... | 157 |
| 4.12 Display of System Information..... | 158 |
| 4.13 Modification of Host Names..... | 158 |
| 4.14 Application of Patches..... | 159 |
| 4.15 Operation of Plug-in..... | 159 |
| 4.15.1 Application of Plug-in..... | 159 |
| 4.15.2 Display of Plug-in..... | 160 |
| 4.15.3 Deletion of Plug-in..... | 160 |
| 4.16 Switch of Trouble Investigation Logs..... | 160 |
| 4.17 Switch of Levels of Trouble Investigation Logs..... | 161 |
| 4.18 DHCP Server inside ISM-VA..... | 162 |
| 4.18.1 Settings for DHCP Server inside ISM-VA..... | 162 |
| 4.18.2 Operation of DHCP Service inside ISM-VA..... | 163 |
| 4.18.3 Confirmation of DHCP Server Information inside ISM-VA..... | 164 |
| 4.18.4 Switch of DHCP Servers..... | 164 |
| 4.19 MIB File Settings..... | 164 |
| 4.19.1 Registration of MIB Files..... | 165 |
| 4.19.2 Display of MIB Files..... | 165 |
| 4.19.3 Deletion of MIB Files..... | 165 |
| 4.20 Upgrade of ISM-VA..... | 165 |
| Chapter 5 Maintenance of Nodes..... | 166 |
| 5.1 Maintenance Mode..... | 166 |
| 5.2 Investigation of Errors..... | 167 |
| Appendix A Uninstallation of ISM-VA..... | 168 |
| Appendix B Troubleshooting..... | 171 |
| Appendix C Profile Setting Items..... | 175 |
| C.1 BIOS/iRMC Setting Items of Profiles for PRIMERGY Servers..... | 175 |
| C.2 MMB Setting Items of Profiles for PRIMEQUEST2000 Series Partitions..... | 182 |
| C.3 OS Setting Items of Profiles for Servers..... | 184 |
| C.3.1 Profiles for Windows Server..... | 184 |
| C.3.2 Profiles for VMware ESXi..... | 188 |
| C.3.3 Profiles for Red Hat Enterprise Linux..... | 191 |
| C.3.4 Profiles for SUSE Linux Enterprise Server..... | 194 |
| C.4 Virtual IO Setting Items of Profiles for PRIMERGY Servers..... | 198 |
| C.4.1 Card Settings..... | 198 |
| C.4.2 Port Settings..... | 199 |
| C.4.3 Boot Settings..... | 199 |
| C.4.4 CNA Settings..... | 201 |
| C.4.5 Virtual Address Settings..... | 202 |
| C.5 Setting Items of Profiles for Storage..... | 203 |
| C.6 Setting Items of Profiles for Switches..... | 206 |

C.6.1 Profiles for SRX.....206

C.6.2 Profiles for VDXs..... 208

Chapter 1 Overview of ServerView Infrastructure Manager

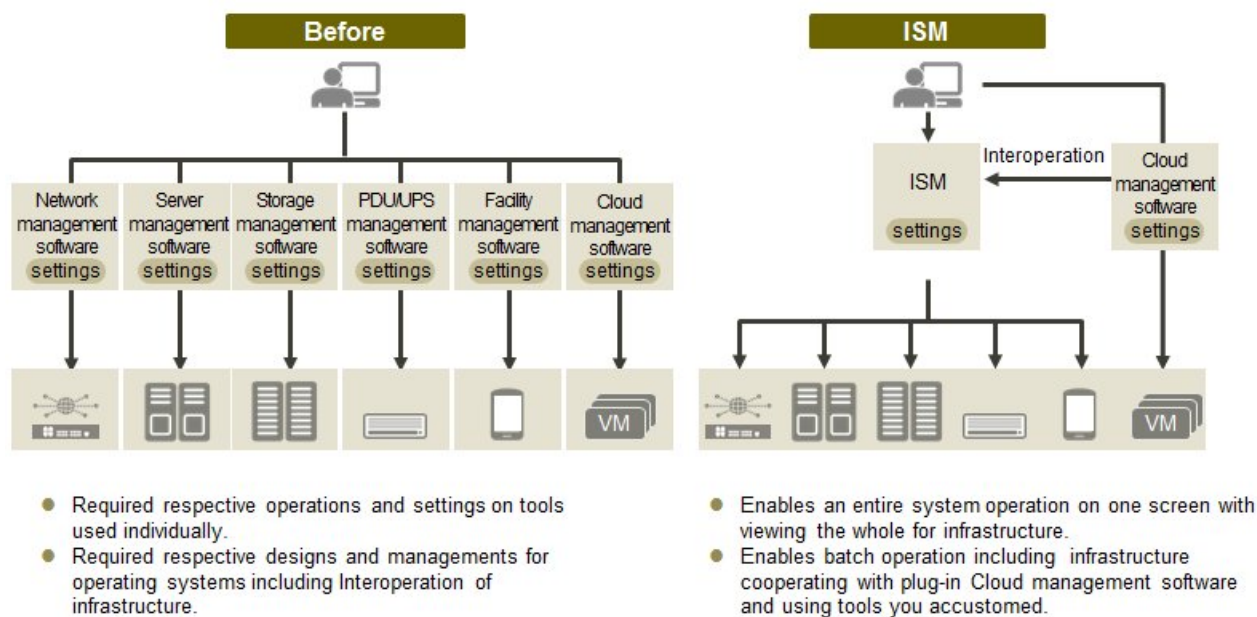
This chapter describes an overview of ServerView Infrastructure Manager.

1.1 Overview

ServerView Infrastructure Manager (hereafter referred to as "ISM") is software for simpler and more efficient operation and management of a multitude of ICT and facility equipment that is running in datacenters and server rooms.

We call ICT and facility equipment that is operated and managed in an ISM environment "nodes."

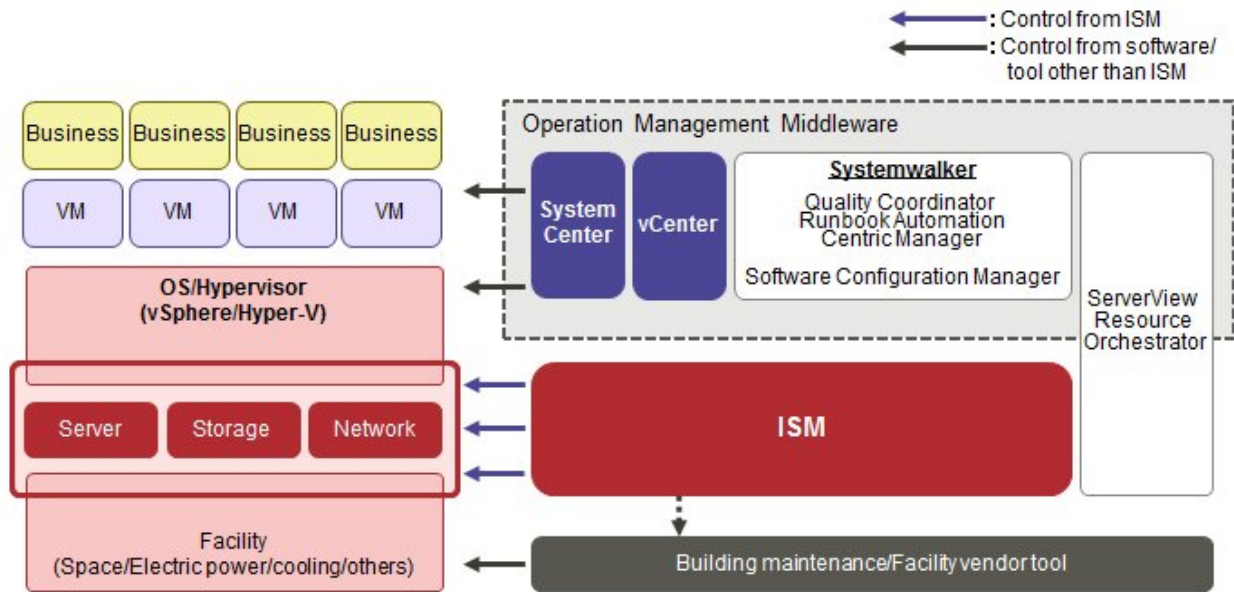
Figure 1.1 Integrated operation and management through installation of ISM



- Optimization of largely integrated operations of physical layers that reach to servers, storages, and networks
 - Hardware Management, Collection/Management of Configuration Information
 - Integration of the management screen
 - Integrated firmware/BIOS update operations for servers, storages, and switches

For the latest information on managed nodes and corresponding functions, access your local support.

Figure 1.2 Working in link with other products



1.2 Overview of Function

This section describes an overview of the ISM functions.

1.2.1 Overview of Node Management

Node Management is a function that carries out the following actions.

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

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

For details on Node Management, see "[2.2.1 Node Management](#)."

1.2.2 Overview of Monitoring

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

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

For these events, you can set up actions such as execution of user-created scripts or transmission of e-mails, and you can monitor nodes according to each user's operating method.

For details on Monitoring, see "[2.2.2 Monitoring](#)."

1.2.3 Overview of Profile Management

Profile Management is a function that carries out the following actions.

- Function for PRIMERGY servers:

This function executes batch settings for the BIOS, iRMC, virtual IO as well as installation of OSes.

- Function for PRIMEQUEST servers:

This function executes batch settings for the BIOS, iRMC, MMB as well as installation of OSes.

- Function for network switches:

This function executes settings for switches, such as switch administrator passwords, SNMP settings, NTP settings, and so on.

- Function for ETERNUS storages:

This function executes configuration of RAID groups, volumes, hot spares as well as Affinity settings.

To make node settings or install an OS, execute the following procedure:

1. Create a settings definition file called "profile" in ISM.
2. Apply the profile to a node.

For effective use of profiles, ISM also provides auxiliary functions such as the "Policy Function", "Group Management", and "Export/Import."

For details on Profile Management, see "[2.2.3 Profile Management](#)."

1.2.4 Overview of Log Management

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

- Periodical collection of logs according to a schedule you set in advance, separately for each node
- Collection of hardware logs and operating system logs from nodes at arbitrary time as required
- Download and utilization of collected logs
- Lookup and keyword search on a GUI screen

For details on Log Management, see "[2.2.5 Log Management](#)."

1.2.5 Overview of Firmware Management

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

- Confirmation of the currently applied firmware versions that are acquired from each node on the screen
- Updating of node firmware to arbitrary version as required (can also be executed simultaneously for multiple nodes)
- Lookup of Readme files attached to firmware data and of update history and similar files on ISM screen

These features allow for an integrated management of firmware versions.

Note that, whenever you are going to update the firmware, you have to download the firmware data to be applied from the web or another source in advance and then import it to ISM-VA.

For details on Firmware Management, see "[2.2.4 Firmware Management](#)."

1.2.6 Overview of Network Management

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

- Confirming information on physical network connections and port information between managed nodes on the Network Map
- Confirming the changes in the information on network connections between managed nodes

- Confirming the virtual connections on the Network Map between the physical ports of the managed nodes and the virtual machines and the virtual switches of the managed node
- Confirming the VLAN and Link Aggregation settings for network switches and changing these settings

For details on Network Management, see "[2.2.6 Network Management](#)."

1.2.7 Overview of the Virtual Resource Management Function

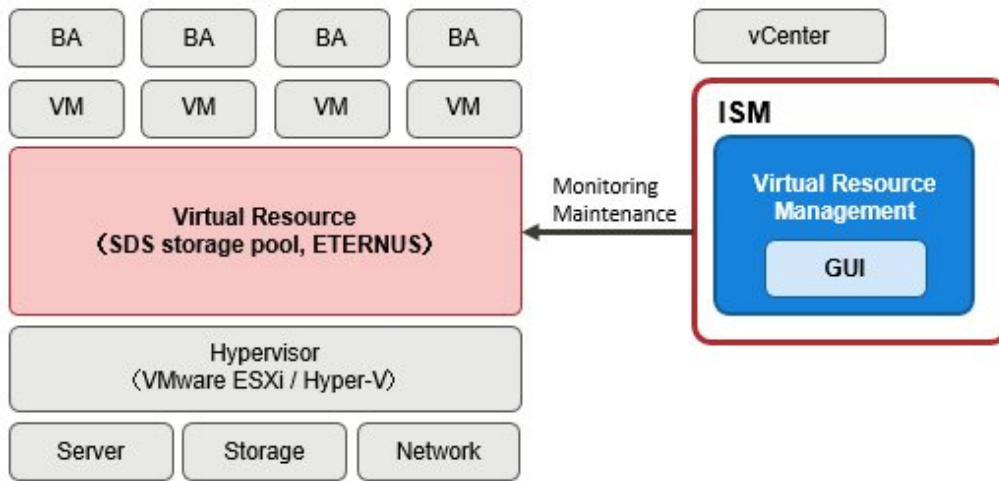
The Virtual Resource Management Function is a function primarily used for the following functions.

- Monitor the usage and status of the virtual resources in connection with the status of the hardware devices (nodes)
- Supports re-deployment and addition(provisioning) of resources by providing an integrated interface for the virtual resources

For details on the Virtual Resource Management Function, see "[2.2.8 Virtual Resource Management Function](#)."

Figure 1.3 Overview of the Virtual Resource Management Function

BA: Business Application
VA: Virtual Machine



1.3 ISM Functions and Scenarios of Infrastructure Operation and Management

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

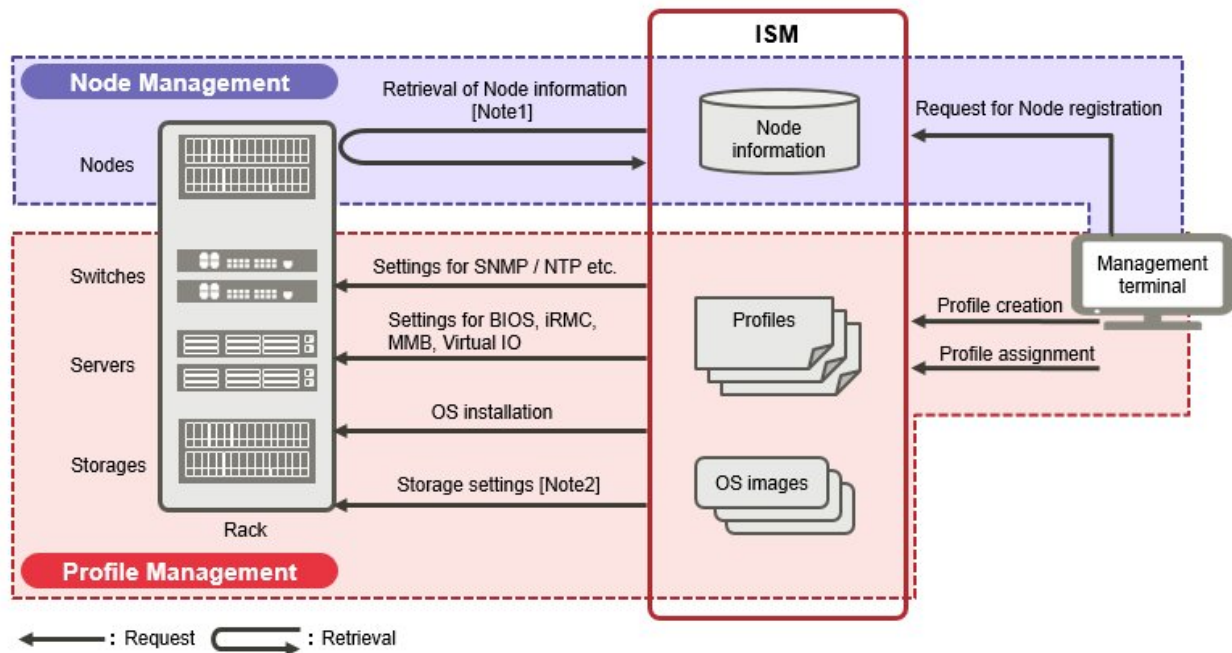
| ISM function | Scenario of operation and management | | |
|---------------------|--------------------------------------|---|------------------------------|
| | System Configuration | Monitoring operations for managed nodes | Maintenance of managed nodes |
| Node Management | Y | Y | - |
| Monitoring | - | Y | - |
| Profile Management | Y | - | - |
| Log Management | - | Y | Y |
| Firmware Management | - | - | Y |
| Network Management | - | - | Y |

1.3.1 Images of ISM Functions for Each Scenario of Infrastructure Operation and Management

(1) System configuration

In the scenario for first-time installation and addition of ICT devices, you can configure systems by effectively using the Node Management and Profile Management functions.

Figure 1.4 Image of functions: system configuration



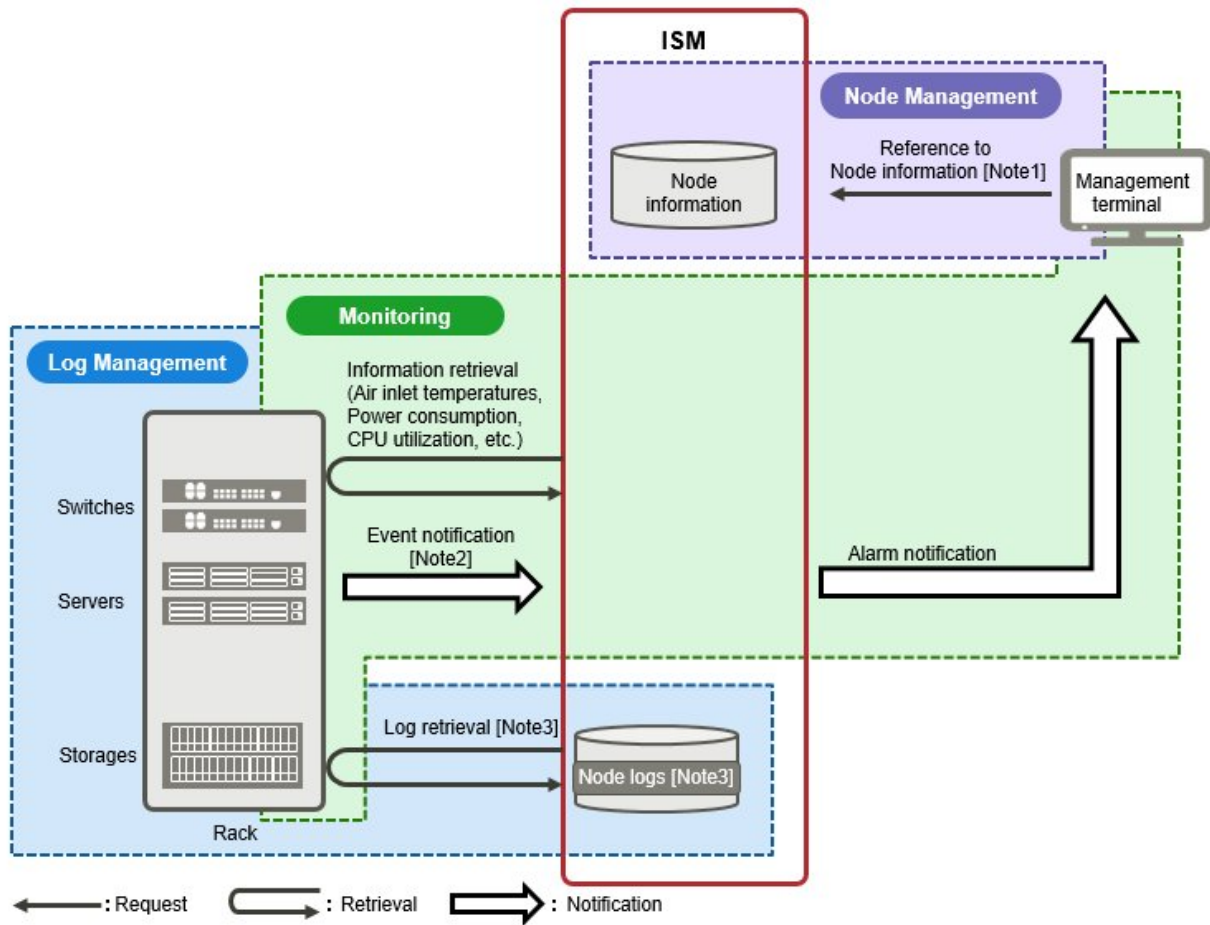
[Note1]: Model names, serial numbers, IP addresses, and similar hardware information

[Note2]: RAID group, volume, hot spare, and Affinity settings

(2) Monitoring operations for managed nodes

In the scenario for monitoring operations for managed nodes, you can carry out monitoring operations for managed nodes by effectively using the Node Management, Monitoring, and Log Management functions.

Figure 1.5 Image of functions: monitoring operations for managed nodes



[Note1]: Model names, serial numbers, IP addresses, installation positions in racks, and similar hardware information

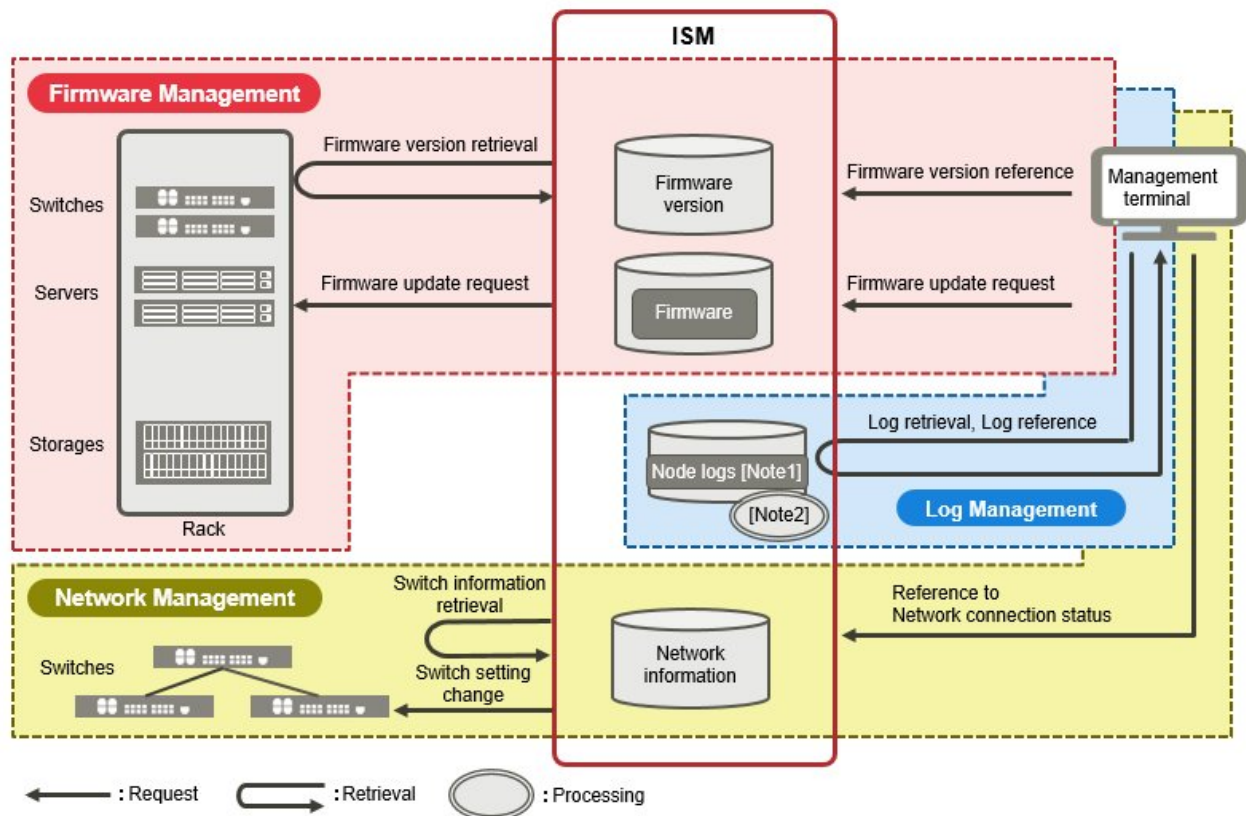
[Note2]: SNMP traps

[Note3]: Hardware logs and operating system logs

(3) Maintenance of managed nodes

In the scenario for maintenance of managed nodes, you can carry out maintenance of managed nodes by using the Log Management, Firmware Management, and Network Management functions.

Figure 1.6 Image of functions: maintenance of managed nodes



[Note1]: Hardware logs and operating system logs

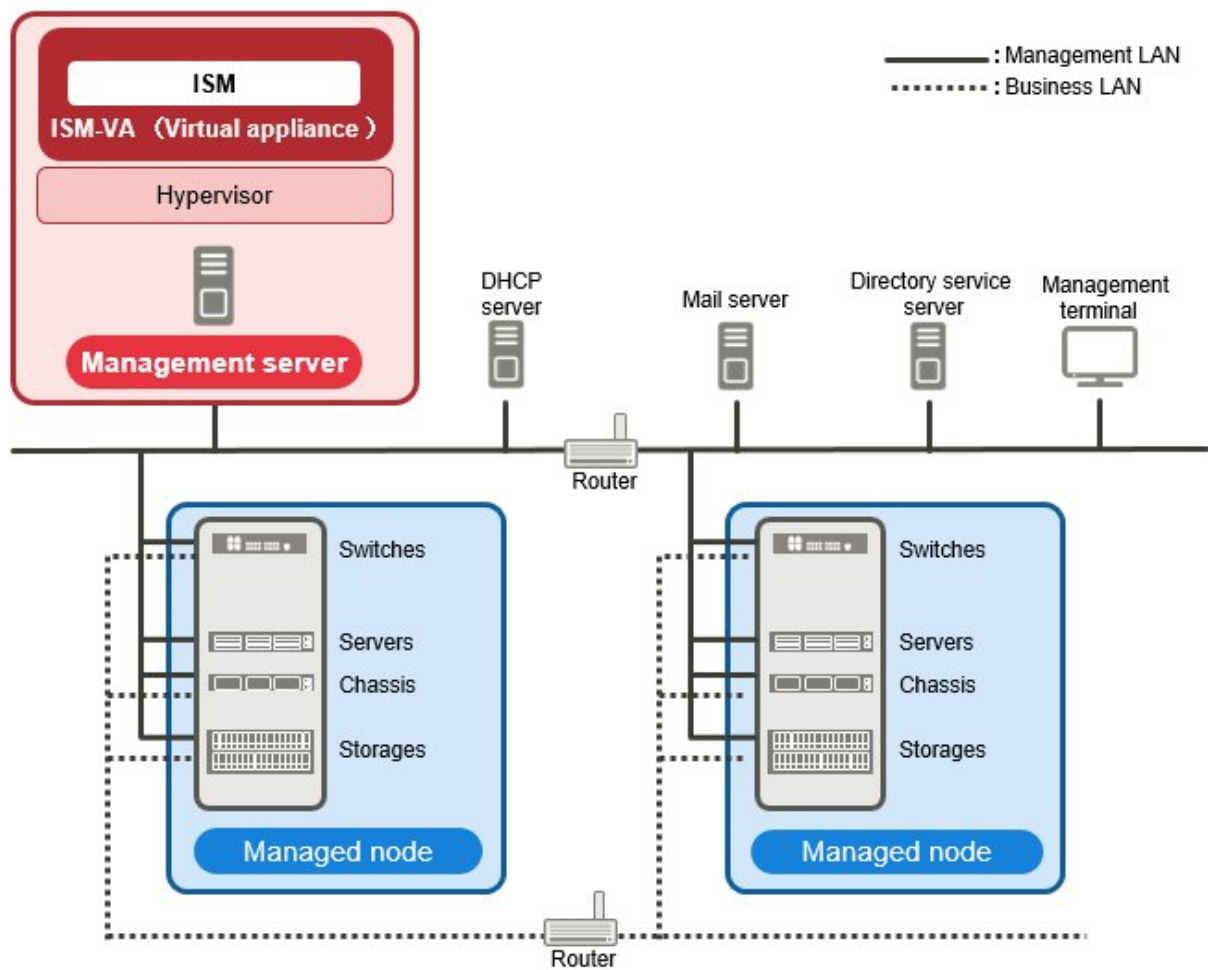
[Note2]: Processing of log searches

1.4 Configuration

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

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

Figure 1.7 Network configuration



Note

For details on the server prepared externally to ISM described in [Figure 1.6](#), see "1.5.3 Service Requirements Required for ISM Operations."

| Device and function | | Description |
|---------------------|--|---|
| Network | Management LAN | LAN used for communicating with the managed nodes so ISM can monitor and control these nodes and transfer data. To ensure security, an isolated connection environment is recommended. Since ISM does not support IPv6, please use it with IPv4. |
| | Service LAN | LAN used for transferring service data between servers and clients. This does not connect to management servers. |
| Management server | ServerView Infrastructure Manager(ISM) | This software. ISM is provided as a virtual appliance into which the software serving as the operating platform is packaged for virtual machines. After installing ISM on a virtual machine, you can control it over a hypervisor console or an SSH client. |
| Management terminal | | PC or tablet that is used for operating ISM through the management LAN. |
| Managed node | Switches | Node that is an object of status monitoring and control by ISM. |
| | Storage | |

| Device and function | | Description |
|---------------------|----------------------------|--|
| | Server (Managed server) | Node that is an object of status monitoring and control by ISM. BMC (iRMC) have to be connected to the management LAN. To use all functions in ISM, the onboard LAN and LAN card both connect to the management LAN. |

For details on designing network configurations and detailed information, access your local support.

1.5 System Requirements

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

1.5.1 System Requirements for ISM-VA (Virtual Machines)

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

| Item | Description |
|---------------------|---|
| Number of CPU cores | 2 cores or more [Note1] |
| Memory capacity | 8 GB or more [Note1] |
| Free disk space | 35 GB or more [Note2] [Note3] [Note4] |
| Network | 1 Gbps or higher |
| Hypervisor | Windows Server 2012/2012 R2/2016 VMware ESXi 5.5/6.0/6.5 Red Hat Enterprise Linux 7.2/7.3 |

[Note1]: The required number of cores and memory capacity depend on the number of nodes to be managed.

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

[Note2]: This is the minimum disk capacity required for monitoring approximately 100 nodes. The disk space requires to be estimated depending on the number of nodes to be managed and the ISM functions to be used. For how to estimate the disk volume, see "[3.2.1 Estimation of Disk Resources](#)."

[Note3]: For backing up ISM-VA, a management server with free disk space equivalent to or larger than that of ISM-VA is required.

[Note4]: This must be fixedly allocated upon installation of ISM-VA.

For the latest information on supported hypervisors, access your local support.

1.5.2 System Requirements for Management Terminals

System requirements for GUI (browser)

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

| Item | Description |
|---------|--|
| Device | PC, server, iPad, Android tablet |
| Display | - PC and server: 1280 x 768 pixels or more |

| Item | Description |
|------------------|--|
| | <p>The window size of your browser for displaying the GUI of ISM must be at least 1280 x 768 pixels.</p> <ul style="list-style-type: none"> - Tablet: display mounted to devices stated above |
| Network | 100 Mbps or higher |
| Web browser | <ul style="list-style-type: none"> - PC and server: <ul style="list-style-type: none"> - Internet Explorer <p>In order to display the "3D View" screen, update version (11.0.15 or higher) must be applied.</p> - Microsoft Edge - Mozilla Firefox - Google Chrome - iPad: Safari8 - Android tablet: Google Chrome |
| Related software | Acrobat Reader (to display the manual) |

For the latest information on devices or Web browsers, access your local support.


System requirements for management terminals for file transfer


The system requirements for management terminals to carry out file transfers with ISM-VA, such as of data required for setting up managed nodes or of ISM logs, are as follows.


| Item | Description |
|-------------------|--------------------------------------|
| Device | PC or server |
| Free disk space | 8 GB or more (equivalent to one DVD) |
| Network | 100 Mbps or higher |
| Required software | FTP client software |
| Related software | SSH client software |

1.5.3 Service Requirements Required for ISM Operations

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

| Item | Description |
|---------------------------|--|
| Mail server (SMTP server) | <p>An email server is required when sending notification mails for errors and changes in the statuses of managed nodes.</p> <p>Set up with [Events] - [Alarms] - [SMTP Server].</p> <p> Note</p> <p>.....</p> <p>In ISM only one mail server can be registered.</p> <p>.....</p> |
| Directory services server | <p>A directory server is required if using the following services.</p> <ol style="list-style-type: none"> 1. When using it in User Management of ISM <p>You can use the following two directory services.</p> <ul style="list-style-type: none"> - OpenLDAP |

| Item | Description |
|--------------|---|
| | <ul style="list-style-type: none"> - Microsoft Active Directory <p>Register the configured server in [Settings] - [Users] - [LDAP Server Setting].</p> <p>2. When using it in OS installation in Profile</p> <p>Settings of 1 as above is not used.</p> <p>The directory service, specified in the setting items in OS installation of Profile, is used. For details, see OS installation of Profile.</p> <p> Note</p> <hr/> <ul style="list-style-type: none"> - In ISM two LDAP servers can be registered, one primary and one secondary. - When a managed node uses a directory service: ISM does not work with the directory service which a managed node belongs to. Individually set up the account capable of accessing the managed node. <hr/> |
| DHCP server | <p>In the following cases it is required to set up a DHCP server.</p> <ul style="list-style-type: none"> - When OS installation is executed using the profile management function - When the Offline Update of the firmware management function is used <p>To enable PXE boot on the managed node (server), set it so that an appropriate IPv4 address can be leased to the node.</p> <p> Point</p> <hr/> <p>The DHCP server function inside ISM-VA can be used instead of preparing a separate DHCP server.</p> <p>For how to use the DHCP function in ISM-VA, see "4.18 DHCP Server inside ISM-VA."</p> <hr/> |
| DNS server | <p>In the following cases it is required to set up a DNS server.</p> <ul style="list-style-type: none"> - Accessing ISM by hostname. - Using FQDN for a variety of sever settings of ISM (such as operations in link with LDAP). <p>For the method of setting up the server, see "Add DNS server" in "4.9 Network Settings."</p> <p> Point</p> <hr/> <ul style="list-style-type: none"> - Manually set up a hostname for ISM-VA if you want to access ISM with the hostname without using a DNS server. For how to set up the hostname manually, see "4.13 Modification of Host Names." - Set up all the settings of ISM (such as operations in link with LDAP) with IP addresses if you do not use the DNS server. <hr/> |
| NTP server | <p>An NTP server is required when setting up time synchronization between ISM and managed nodes and managed clients to avoid out of synchronization between them.</p> <p>Use the ismadm command or the ismsetup command when you set up the NTP server for ISM.</p> <p>For how to set it up, see "Enable/Disable NTP synchronization" and "Add/Remove NTP server" in "3.4.2 Initial Settings of ISM."</p> |
| Proxy server | <p>A Proxy server is required when accessing ISM from a management client via a Proxy server.</p> |

| Item | Description |
|--------|--|
| |  Note <hr/> Monitored nodes and ISM cannot be connected via a Proxy server. <hr/> |
| Router | <p>You can define only one network interface for ISM.</p> <p>If using ISM in an environment with multiple networks, it is required to set up a router to enable communication between the networks.</p> <p>If setting up a gateway in ISM, use the ismadm command or the ismsetup command.</p> <p>For how to set it up, see "Modify network settings" in "4.9 Network Settings."</p> |

1.5.4 Operation Requirements for Virtual Resources

For using the Virtual Resource Management Function, see the following for the requirements.

- Requirements for the Virtual Resource Environment: "[2.2.8 Virtual Resource Management Function](#)"
- Requirements environment for Virtual Resources: "[3.8 Pre-Settings for the Virtual Resource Management Function](#)."

1.6 Precautions

Timing of completing OS installation

The status after completing profile assignment varies with the OS type and the OS settings. Likewise, the timing for executing optional scripts as specified by profiles also varies with the OS type.

| OS type and settings | | Status after completing profile assignment to OS | Timing for executing optional scripts |
|---|---------------------------|--|--|
| Windows | | EULA screen during OS installation | At first login after accepting EULA and completing license input |
| Linux | | Login prompt after OS has completely booted | First login prompt (execution completed) |
| | X Window enabled in RHEL7 | Last setting screen during OS installation | When OS login prompt is displayed after completing last settings |
| VMware ESXi (IP addresses are fix) | | When network communication has become available after OS has completely booted | During OS installation (execution completed) |
| VMware ESXi (IP addresses are set by DHCP) | | After completing OS installation and reboot | During OS installation (execution completed) |

About the RAID configuration when installing an OS on a managed server

For OS installation, you require ServerView Suite DVD.

The number of logical drives configured with an array controller is only one if you perform OS installation using ServerView Suite DVD V11.16.04.

Precautions on using paid support service (SupportDesk Standard) for Red Hat Enterprise Linux (Only for Japanese market)

In order to engage in an agreement for a paid support service and to receive such support, your system configurations are required to fulfill some requirements.

When you use ISM's Profile function to automatically install Red Hat Enterprise Linux, the "Fujitsu Linux Support Package (FJ-LSP)" required for support is not applied, and no memory dump settings are made. Make any required settings manually after installation.

For details on setting contents and methods, refer to the Linux user's manual for SupportDesk service subscribers.

Using automatic data collection by Log Management

ISM can periodically collect logs according to a schedule you set in advance. If you use this feature, however, you should take note of the following points:

- Logs are not collected by merely registering a node. You have to set the type of log to be collected and the schedule separately for each node.
- If there is any mistake in the node settings or in the settings within ISM, logs cannot be properly collected. After making the respective settings, execute a manual log collection to confirm that the log files are accumulated correctly and that there is no log collection error recorded in the [Events] - [Events] - [Operations Log].
- If the volume of the log files reaches the "Warning threshold" set in "Archived Log" and "Node Log" or set for each user group in [Settings] - [Users] - [User Groups], an alert event is registered in ISM events. Delete logs that are no longer required. On reaching the "Maximum Size" set in the same way, no more logs are saved.
- Old logs are automatically deleted when the set period/frequency is exceeded. When you use the log collection function, change this setting to a value that is appropriate for you.

Chapter 2 Functions of ISM

This chapter describes the functions of ISM.

For information on the operating procedures for the main functions, see "ServerView Infrastructure Manager V2.1 Operating Procedures."

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

2.1.1 GUI

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



Point

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

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

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

<https://technet.microsoft.com/en-us/library/security/ms14-051>

- If you are using Google Chrome, depending on the hardware capabilities of your terminal and your graphics driver, the WebGL function (for displaying 3D graphics in browsers) may be disabled. If the WebGL function is disabled, you cannot display the "3D View" screen.

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

1. Open Google Chrome and enter "chrome://gpu" into the address bar.
2. If, under [Graphics Feature Status], [Hardware accelerated] is displayed for [WebGL], the WebGL function is enabled. Otherwise it is disabled.

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

1. Start a browser and enter the following URL:

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

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

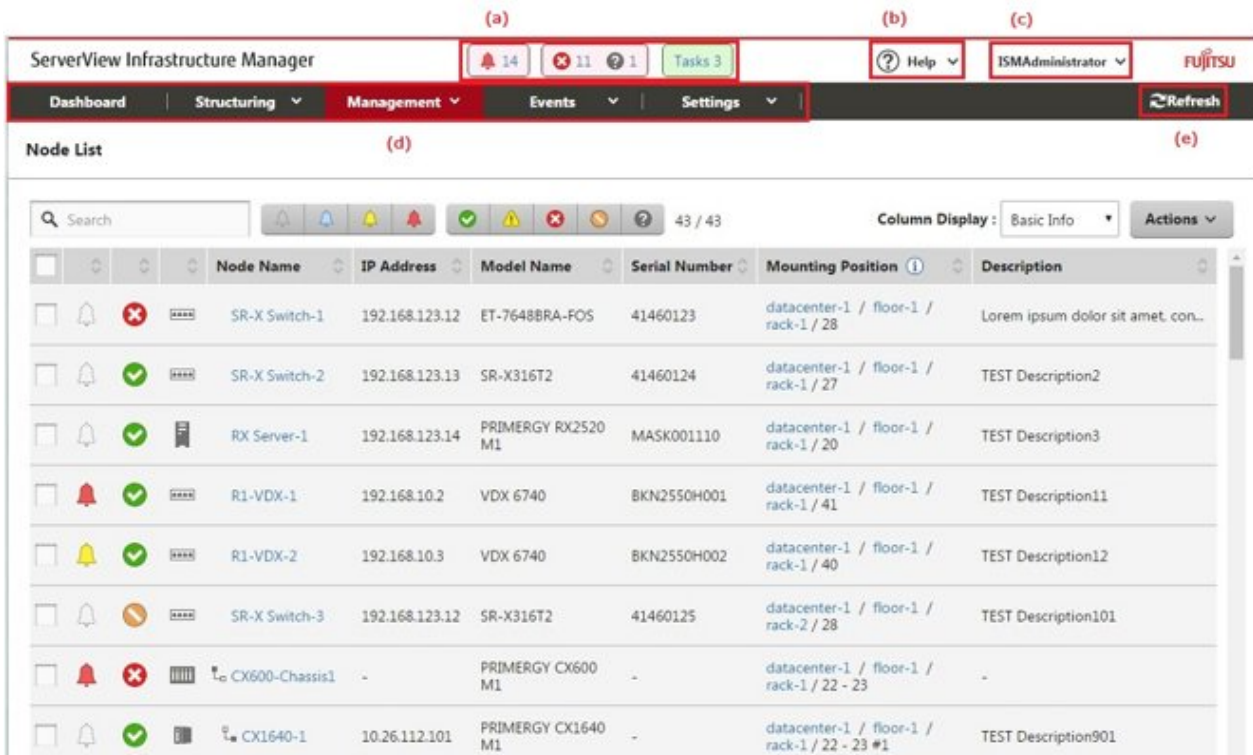
If a warning for the security certificate is displayed, see "4.7 Certificate Activation" and execute the authentication settings.

Point

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

- User Name: administrator
- Password: admin

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



The screenshot shows the ServerView Infrastructure Manager (ISM) GUI. The top navigation bar includes 'Dashboard', 'Structuring', 'Management', 'Events', and 'Settings'. A 'Node List' table is displayed below, showing columns for Node Name, IP Address, Model Name, Serial Number, Mounting Position, and Description. The table contains several rows of node information, including SR-X Switches, RX Servers, and R1-VDX units. The interface also includes a search bar, a 'Column Display' dropdown, and an 'Actions' dropdown.

(a) Alarm status, status, task icon

Alarm status:

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

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

Status:

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

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

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

Task:

Displays the number of currently running tasks.

(b) Help

Displays help and guidance.

(c) User name

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

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

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

(d) Global Navigation Menu

This menu serves to access the various screens of ISM.

(e) Refresh button

Selecting this button refreshes the entire screen.

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

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

If automatic refresh is set up for the following screens, the screens are refreshed automatically.

- "Registration" screen
- "Task" screen

2.1.2 FTP Access

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

Specify the IP address that you set in "[3.4.2 Initial Settings of ISM](#)" to make the connection.

Immediately after login, the files and directories are hidden from the display for security reasons; move to the directory with the group name to which the login user belongs and access the file transfer area from there.

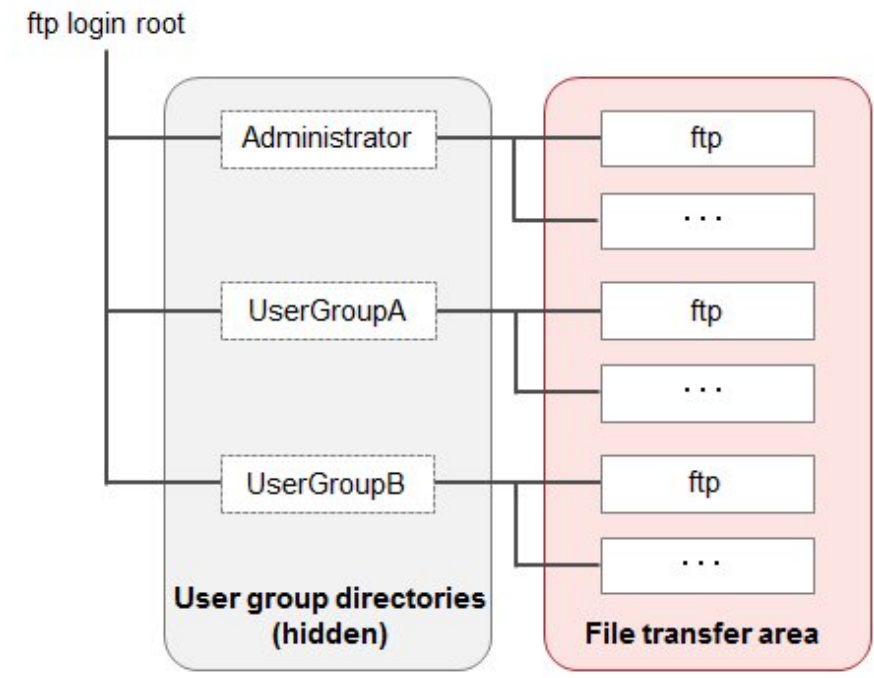
As shown in the figure below, files that are sent or received via FTP are stored under ".<user group name>/ftp."



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, see "[2.3.1.2 Managing User Groups](#)."
- 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 forwarding patch files and other binary data, forward these in binary mode.
- For FTP access as a user operating in link with Microsoft Active Directory or LDAP, do not use the linked password but the one that is registered in ISM.

Figure 2.1 Directory configuration of file transfer area



Example of FTP access

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

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

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

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

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

226 Directory send OK.

*It is possible to access the area used for forwarding files.

2.1.3 Console Access

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

If you connect over an SSH client, specify the IP address that you set in "[3.4.2 Initial Settings of ISM](#)" when you make the connection.

Console access is available only to users who have an Administrator role as described under "Point" in "[2.2 Functions of ISM](#)."

See "[2.3.5.1 List of Commands in ISM-VA Management](#)" for information on commands that can be used.



Note

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

2.2 Functions of ISM

This section describes the functions for configuring, operating, and carrying out maintenance of managed nodes.

It describes the following functions.

- [2.2.1 Node Management](#)
- [2.2.2 Monitoring](#)
- [2.2.3 Profile Management](#)
- [2.2.4 Firmware Management](#)
- [2.2.5 Log Management](#)
- [2.2.6 Network Management](#)
- [2.2.7 Power Capping](#)
- [2.2.8 Virtual Resource Management Function](#)
- [2.2.9 Virtual IO Management](#)



Point

In order to allow users to use the various ISM functions, it is required that privileges (user roles) to access the user group in which each respective user is registered are allocated. For details on Node Management, see "[2.3.1 User Management](#)."

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

| User Group to which user belongs | User Role held by user | Can execute | Cannot execute |
|----------------------------------|------------------------|-------------|----------------|
| Administrator group | Administrator role | | |
| | Operator role | | |
| | Monitor role | | |
| Other than Administrator group | Administrator role | | |
| | Operator role | | |

| User Group to which user belongs | User Role held by user | Can execute | Cannot execute |
|----------------------------------|------------------------|----------------|----------------|
| | Monitor role | Monitor | Monitor |

In the following descriptions, the affiliations of users who can execute operations are indicated as follows.

Example:



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

2.2.1 Node Management

Node Management manages nodes at four levels: datacenters, floors, racks, and nodes. The meanings of datacenters, floors, racks, and nodes are as follows.

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

Node Management has the following functions.

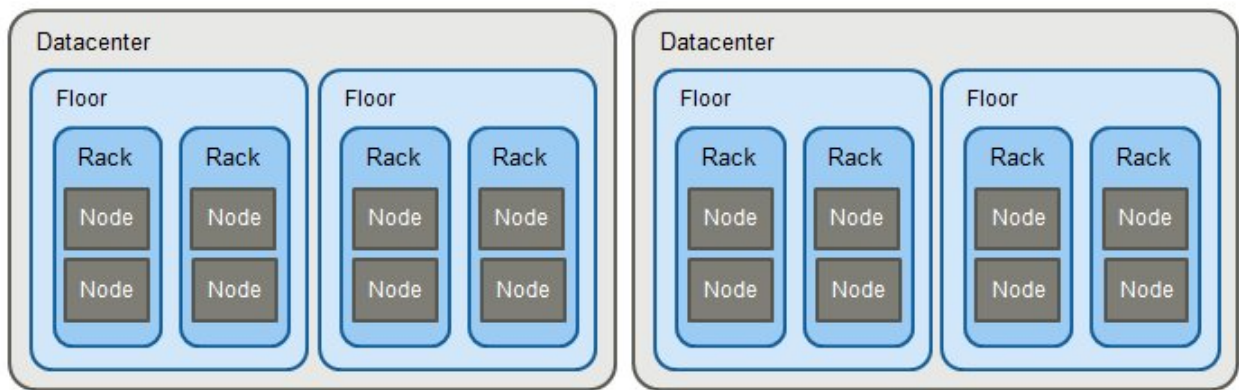
- [2.2.1.1 Registration of Datacenters/Floors/Racks/Nodes](#)
- [2.2.1.2 Confirmation of Datacenters/Floors/Racks/Nodes](#)
- [2.2.1.3 Edit of Datacenters/Floors/Racks/Nodes](#)
- [2.2.1.4 Deletion of Datacenters/Floors/Racks/Nodes](#)

2.2.1.1 Registration of Datacenters/Floors/Racks/Nodes

With ISM, you can manage the physical location information on nodes. The location information is uniquely specified within the level structure "Datacenter > Floor > Rack > Unit Number."

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

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



You can make the following operations:

- [Registration of datacenters/floors/racks](#)
- [Registration of nodes](#)
- [Management of node information](#)
- [Management of information on node installation positions in racks](#)
- [Registration of node OS information](#)
- [Node Discovery](#)
- [Adding tags to nodes](#)

Registration of datacenters/floors/racks

| | Administrator group | | | Other groups | | |
|-----------------|---|---|--|--------------------------------------|---|--|
| Executable user | <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 additionally register information on datacenters, floors, and racks in ISM. The datacenter, floor, and rack names to be registered must be set to unique names in ISM.

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

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

Registration of nodes

| | Administrator group | | | Other groups | | |
|-----------------|---|---|--|--------------------------------------|---|--|
| Executable user | <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"/> |

In order to use ISM for managing nodes, you first have to register the nodes in ISM.

Whenever you register a node, enter all the required information. The requirements for the information to be registered are as follows.

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

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

For the account information that is required for communicating with each type of target node and for the settings that are required before node registration, access your local support.

There are two methods for registration as follows:

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

The following is a sample operation for manual registration in ISM. For the registration method that uses the discovery function, see "[Node Discovery](#)." To register nodes it is required to in advance confirm information such as the model names of devices to be registered and which IP addresses are set.

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

Point

It is not recommended to monitor the same node with multiple instances of ISM or multiple monitoring software. Monitoring may not function correctly, as, depending on each node, there are only a limited number of sessions that can access a node simultaneously.

Management of node information



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

In ISM, the account information that is set for each node is used for collecting node information from the nodes at intervals of approximately 24 hours. Whenever you want to retrieve the latest node information, you can manually execute the command to retrieve it.

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

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

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

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

4. Select the refresh button to update the Details of Node screen.

Management of information on node installation positions in racks



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

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

- Setting of information on installation positions in racks

You can set the information on installation positions in racks when you carry out node registration. Alternatively, you can also make the settings after node registration.

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

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

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

Registration of node OS information



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

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

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

In ISM, the registered OS information is used for retrieving information that is placed under OS management on a node.

For the latest information on supported devices and OS versions, access your local support.



- In order to make a server OS the object of monitoring from ISM, a separate installation procedure is required for each OS.

When you register a domain name as account information and a domain user as an account, you must add the settings for performing the monitoring by another domain user to the OS to be monitored.

For information on installation procedures, access your local support.

- When you monitor the OS by using the domain user, you are required to set up DNS settings and domain environment settings. For how to set up, see "[3.4.2 Initial Settings of ISM.](#)"
- If no OS information is registered or the respective OS has been shut down, a portion of the node information cannot be retrieved. Likewise, the information that is placed under OS management on a node cannot be retrieved.
- Enter the domain name with uppercase letters when you register OS information.

The following is a sample operation.

1. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Nodes] to display the "Node List" screen.
2. Select the node name of the applicable node and select the [OS] tab.
3. From the [OS Actions] button, select [Edit OS Information].
4. Enter and then apply the required information.
5. From the [Actions] button, select [Get Node Information].

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

6. Select the [Refresh] button to refresh the display on the [OS] tab.

Node Discovery



With ISM, you can discover the nodes that are connected to a network. The discovery function supports your node registration work, as you can retrieve the required information for registration from the discovered nodes.

Discovery has to be executed manually. You can execute the following operations:

- Creating settings for manual discovery and executing discovery
- Confirming results of manual discovery
- Registering discovered nodes

Registering settings for manual discovery

Set the required information for manual discovery. Node Discovery is executed for the range of IP addresses that you specify. Moreover, using the set account information, some of the node information required for registration is retrieved.

Before you carry out manual discovery, it is required to set the required account information for connecting to the nodes you want to discover.

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

For the latest information on supported devices and OS versions, access your local support.

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

Confirming results of manual discovery

Refresh the display for [Discovery Progress] tab on the "Node Registration" screen and wait until processing for discovery finishes. When discovery is complete, select the [Discovered Node List] tab and confirm the discovered nodes.

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

Note

- The discovered node information is only enabled during the same session.
- Devices that are not supported may be displayed in the discovery results. Do not register devices that are not supported.
- If it is a Brocade VDX switch, it becomes Brocade VCS Fabric during node discovery and registration. Specify the virtual IP address set in fabric and execute node discovery and node registration. If discovering a physical switch during node discovery, the status becomes "Automatic Registration Only."

Registering discovered nodes

The following is a sample operation for registering manually discovered nodes.

1. Confirm the discovered nodes.
2. From the discovered nodes, select the ones you want to register, then select the [Registration discovered nodes] button.
3. Enter the information that is required for node registration, such as node name, chassis name, Web i/f URL, description.
4. Set the information for the node's installation position in a rack.
5. Set the node group information.
6. Execute the registration.

The account information with which the node was successfully accessed during Node Discovery is registered as account information for the node. The registered accounts are displayed in the [Account] column on the "Discovered Node List" screen.

Adding tags to nodes



In ISM tags can freely be added to nodes. Tag is a function that adds information to allow the user to freely group nodes. For grouping nodes, the node group function also exist, but access rights are controlled for node groups. 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.

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

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

Using tags to execute filtering



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

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

3. Enter the tag name that you want to filter and execute [Filter].

The nodes with the specified tag set up are displayed on the [Node List] screen.

Point

Select the nodes among the filtering results and execute [Apply Profile] or [Firmware Update]. For profile application or software updates, see "[2.2.3 Profile Management](#)" or "[2.2.4 Firmware Management](#)."

2.2.1.2 Confirmation of Datacenters/Floors/Racks/Nodes

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

Confirming datacenters/floors/racks



The screenshot shows a form with two main sections: "Administrator group" and "Other groups". Each section has three buttons: "Admin", "Operator", and "Monitor". The "Executable user" label is on the left.

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

Confirming nodes



The screenshot shows a form with two main sections: "Administrator group" and "Other groups". Each section has three buttons: "Admin", "Operator", and "Monitor". The "Executable user" label is on the left.

Confirm the nodes that are registered in ISM.

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

Confirming node OS information



The screenshot shows a form with two main sections: "Administrator group" and "Other groups". Each section has three buttons: "Admin", "Operator", and "Monitor". The "Executable user" label is on the left.

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

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

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

For details of the settings for the OSes to be monitored, access your local support.

2.2.1.3 Edit of Datacenters/Floors/Racks/Nodes

Edit the information that is registered in ISM.

Editing datacenters, floors, and racks



The screenshot shows a form with two main sections: "Administrator group" and "Other groups". Each section has three buttons: "Admin", "Operator", and "Monitor". The "Executable user" label is on the left.

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

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

Editing nodes

| | Administrator group | Other groups |
|-----------------|--|---|
| Executable user | <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"/> |

The following is the operation method for editing node information.

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

2.2.1.4 Deletion of Datacenters/Floors/Racks/Nodes

Delete any information that is registered in ISM.

Deletion of datacenters

| | Administrator group | Other groups |
|-----------------|--|---|
| Executable user | <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"/> |

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

| | Administrator group | Other groups |
|-----------------|--|---|
| Executable user | <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"/> |

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

| | Administrator group | Other groups |
|-----------------|--|---|
| Executable user | <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"/> |

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, log and other information for the applicable nodes.

Note

If you are logged in from multiple terminals and have deleted any datacenters, floors, racks, and/or nodes, performing an operation for a deleted object from a terminal that was not yet deleted may sometimes cause errors like "The object does not exist" or "The object is already deleted." In such a case, refresh the screen contents by one of the following methods before you resume operation.

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

Point

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

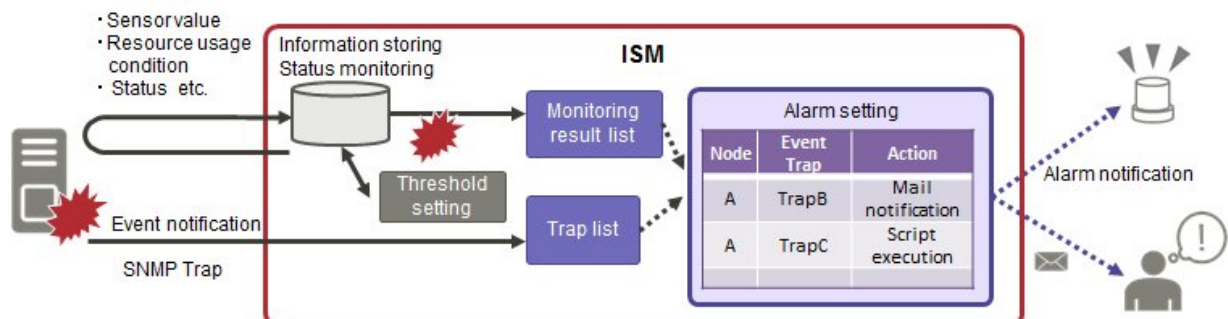
2.2.2 Monitoring

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

- It polls statuses of resource use, such as for sensor values of node temperature or CPU utilization, and accumulates these kinds of information.
- Based on comparing polling results with threshold values you specified in advance as well as on status changes, this function monitors the various statuses.
- It receives incoming event notifications (SNMP traps) from the nodes.
- It issues external alarm notifications on monitoring results and incoming event notifications from the nodes.

You can define the notification method in advance as an action.

Figure 2.3 Image of Monitoring



The following three settings are related to Monitoring.

- [Setting of monitoring items and threshold values](#)
- [Action settings](#)

- [Registration of alarm settings](#)

Setting of monitoring items and threshold values

Executable user

Administrator group

Admin Operator Monitor

Other groups

Admin Operator Monitor

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

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

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

The following items can be additionally specified to be monitored.

| Additional monitoring item | Description |
|--|---|
| Various types of resource information | CPU utilization, memory usage, and other resource statuses are monitored. |
| Fan speed | The speeds of the various fans in managed devices are monitored. |
| Ethernet information | The amounts of incoming and outgoing network data are monitored separately for each port. |
| Average power consumption/Average Intake Temperature | Power consumption and intake temperature are monitored at 3 minute intervals. When the power capping function for the rack is enabled and the only the node with power capping function can be monitored. |

Procedure for adding monitoring items and threshold values

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

Action settings

Executable user

Administrator group

Admin Operator Monitor

Other groups

Admin Operator Monitor

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

| Type of notification method | Description |
|-----------------------------|---|
| Execution of user scripts | Executes any user-defined script. |
| Send E-Mail | Sends e-mails with any user-defined contents. |

| Type of notification method | Description |
|-----------------------------|---|
| Trap Forwarding/Sending | <p>Forward the received SNMP trap to an external SNMP manager, or forward an event discovered inside ISM as an SNMP trap. When forwarding, the following forwarding types can be selected.</p> <ul style="list-style-type: none"> - Forward ISM as the sender <p>The send SNMP trap is processed as if it was sent straight from ISM. Apart from information on the sender, the trap information is sent as it is.</p> <ul style="list-style-type: none"> - Send received trap as it is <p>The received trap is forwarded to the SNMP manager as it is.</p> |

Macro

The macro (automatic integer) functions displayed below can be used in the title or text body of a sent email. These macros are automatically replaced with the information of the node or event.

| Method of notation of macro | Overview |
|-----------------------------|---|
| \$_ISM | ISM host Name |
| \$_TRGTYPE | Event target (System or Node) |
| \$_TRG | Event target name (Node name) |
| \$_IPA | IP address of the node |
| \$_IDN | Serial number of the node. |
| \$_DC | Name of the data center where the node is installed |
| \$_FLR | Name of the floor where the node is installed |
| \$_RACK | Name of the rack where the node is installed |
| \$_SEV | Severity of the event |
| \$_EVT | Event ID |
| \$_MSG | Event message |
| \$_TIM | Time when the event occurred UTC time is displayed in RFC3339 format (Example:2017-01-01T00:00:00.000Z) |

Procedure for adding actions

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

Required preparations before using each action

Execution of user scripts

Any script files to be executed must be imported into ISM-VA in advance.

1. Prepare the user scripts to be used in the action setting.
2. Connect to ISM-VA over FTP and transfer the script files.
3. In ISM-VA Management, execute the command for registering scripts.

For details, see "[4.10.2 Registration of Action Scripts.](#)"

Send E-Mail

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

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

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

1. Prepare the personal certificates to be used in the action setting.
2. Connect to ISM-VA over FTP and forward the certificate files.
These certificates must be in PEM encoding format.
3. In ISM-VA Management, execute the command for registering certificates.

For details, see ["4.10.1 Registration of Certificates for Event Notification Mails."](#)

Trap Forwarding/Sending

When forwarding or sending an SNMP trap it is required to register the SNMP manager to forward or send it to.

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

Registration of alarm settings



Alarm settings are made in advance to define what processing to execute when a given event occurs on a given node.

Procedure for adding alarms

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

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





Event types

There are the following types of events.

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

Alarm statuses

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

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

When you have completed confirming and recovering from the discovered event, carry out the following procedure to deactivate the alarm status.

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

Point

- Alarm statuses are not deactivated automatically. However, if a status with a higher priority is discovered, it is displayed instead.
- Sometimes by design you may require to turn off the power of nodes for performing maintenance on the nodes. ISM is provided with a "Maintenance Mode" function capable of temporarily interrupting its monitoring function so that ISM can avoid detecting alarms, such as power off, resulting from maintenance.

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

For information on Maintenance mode, see "[5.1 Maintenance Mode](#)."

Trap Reception Setting



The following describes how to edit the settings for SNMP trap reception. v1, v2c reception protocols are supported.

Process for adding SNMP Trap Reception Settings

1. From the Global Navigation Menu on the GUI of ISM, select [Settings] - [General].
2. Select [Trap Reception] from the menu on the left side of the screen to display the "Trap Reception Setting List" screen.

3. Select the [Actions] button on the right side of the screen and select [Add] to add trap reception settings.

Note

When changing Add/Edit/Delete to the trap reception settings, the changes are applied immediately. Between when a request is received and reflected all SNMP traps will temporarily not be received. When changing the trap reception settings, first make sure that the matter above will not cause problems.

Registering MIB

It is described the method of registering MIB files on ISM and the methods of confirming and deleting the registered MIB files.

MIB Files

MIB is public information regarding the status of the network devices managed in SNMP, and is standardized as MIB2 prescribed by RFC 1213. The MIB file is a text based file defining this public information. In order to send and receive SNMP traps it is required for the receiver side to save the MIB file provided by the device side.

Add/update the MIB file in the following cases.

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

Note

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

For details of the format for MIB files, access your local support.

Registering MIB Files

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. Connect to ISM-VA via FTP and transfer the MIB file.
3. Execute the MIB registration command from ISM-VA Management.

For details, see "[4.19.1 Registration of MIB Files.](#)"

Point

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

Confirming MIB Files

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

For details, see "[4.19.2 Display of MIB Files.](#)"

Deleting MIB Files

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

For details, see "[4.19.3 Deletion of MIB Files](#)."



Point

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

2.2.3 Profile Management

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

- Making hardware settings for managed nodes
- Installing OSes on servers if the target servers are managed nodes
- Executing virtual IO settings if the target servers are managed nodes

Besides virtual MAC address/virtual WWN allocation, server boot settings are also included in the virtual IO settings of the ISM Profile Management Function.

- Creating RAID/hot spares on storages as managed nodes

Table 2.1 Target nodes (managed nodes) and available setting items of Profile Management

| Node type | Target node (example) | Available setting items |
|----------------|------------------------|--|
| Server | PRIMERGY RX | <ul style="list-style-type: none">- BIOS setup- iRMC setup- OS installation- Virtual IO setup |
| | PRIMERGY CX | <ul style="list-style-type: none">- BIOS setup- iRMC setup- OS installation |
| | PRIMEQUEST 2000 series | <ul style="list-style-type: none">- MMB setup- OS installation |
| Network switch | SR-X | <ul style="list-style-type: none">- Setting of administrator passwords- SNMP, NTP, and STP settings |
| | VDX SDM | <ul style="list-style-type: none">- Setting of administrator passwords- SNMP and NTP settings |
| Storage | ETERNUS DX | <ul style="list-style-type: none">- Creation of RAID groups/volumes- Creation of global hot spares- Host Affinity settings |

Here, the following points are described:

- [Profile usage](#)
- [Profiles and policies](#)
- [Profile groups and policy groups](#)

- Procedure for creating policy groups
- Procedure for creating policies
- Procedure for creating profile groups
- Procedure for creating profiles
- Procedure for assigning profiles
- Procedure for editing and reassigning profiles
- Procedure for releasing and deleting profiles
- Exporting and importing profiles
- Procedure for editing profile groups
- Procedure for deleting profile groups
- Procedure for editing policy groups
- Procedure for deleting policy groups
- Required preparations before OS installation
- Precautions on OS installation
- Procedure for specifying scripts to be executed after OS installation
- Specifying behavior when assigning profiles

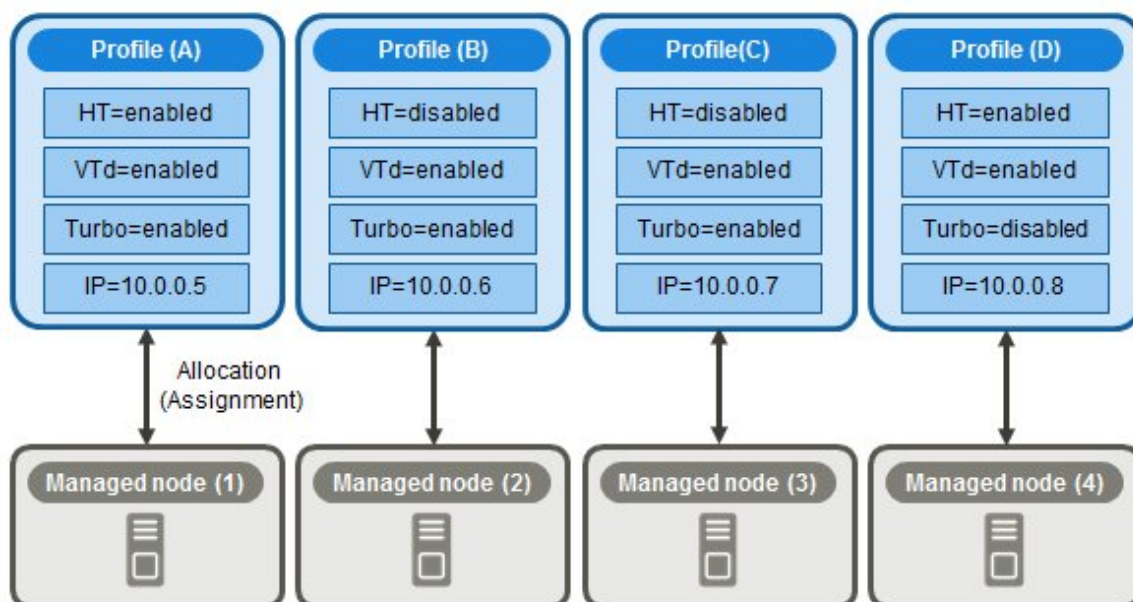
Profile usage

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

By assigning (applying) this profile to nodes, the settings become effective for those nodes.

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

Figure 2.4 Relationships between profiles and managed nodes



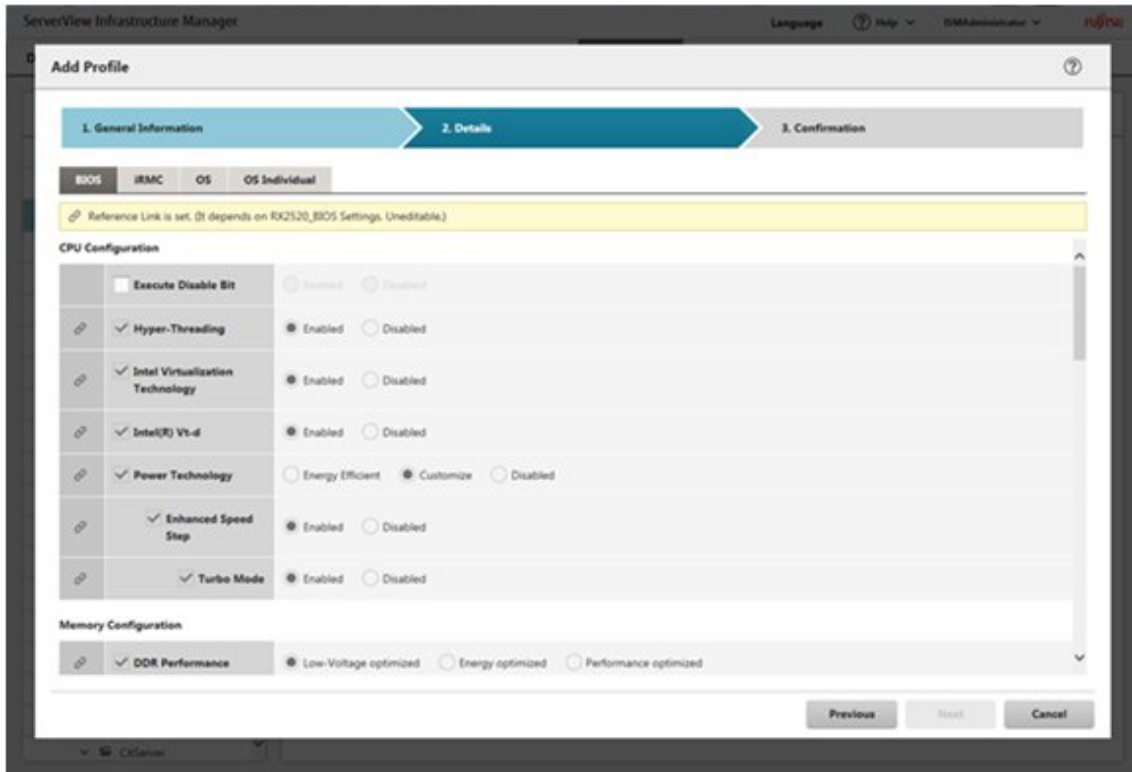


Note

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

Sample profile

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



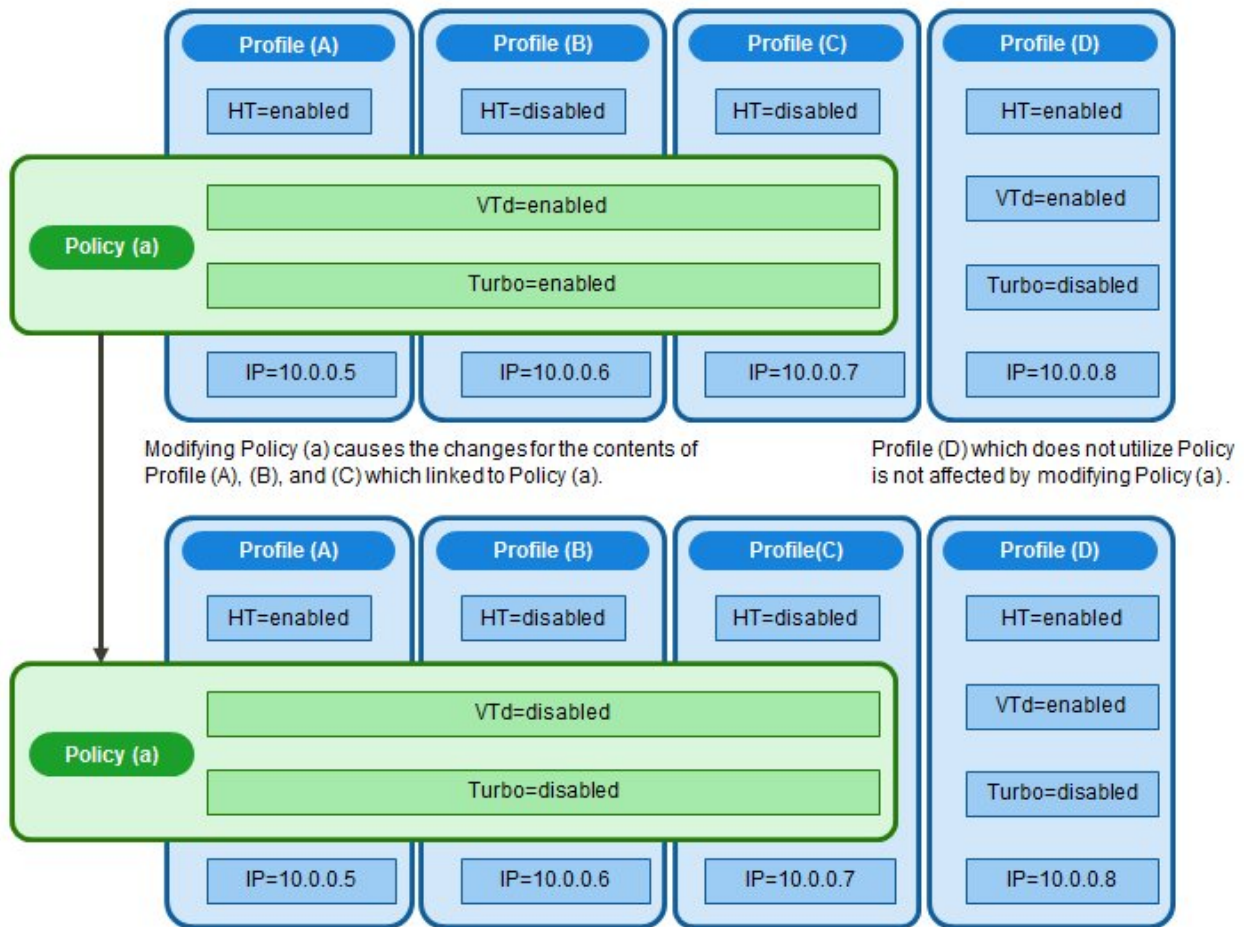
Profiles and policies

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

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

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

Figure 2.6 Relationships between profiles and policies



Note

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

Point

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

Profile groups and policy groups

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

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

Procedure for creating policy groups



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

Procedure for creating policies



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

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

Procedure for creating profile groups



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

Procedure for creating profiles



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

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

Procedure for assigning profiles





- Executing a profile assignment while logged in to the target node over a web operating screen or SSH may sometimes result in a profile assignment error.
- If you are going to install an OS, it is required to prepare the required settings and files in advance. Please see the following:
["Required preparations before OS installation."](#)

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



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, see ["2.3.4 Task Management."](#)

Procedure for editing and reassigning profiles



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

(However, if the node is a server and "Server OS Settings" is set in the profile, these items cannot be revised.)

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

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

Procedure for reassigning profiles

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

Procedure for confirming whether node settings match profiles

1. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Nodes].
2. In the [Column Display] field on the "Node List" screen, select [Profile].
For nodes whose settings do not match the profile, [Reassignment] is displayed under [Status].
For nodes whose settings match the profile, [Assigned] is displayed under [Status].



Note

Modifying any settings directly on a node without using Profile Management causes a mismatch between the contents of the applied profile that are displayed on the ISM screen and the actual node status.

Procedure for releasing and deleting profiles



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

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



Point

For details on Node Groups, see "[2.3.1 User Management](#)."

Procedure for releasing profiles

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

Procedure for deleting profiles

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

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

Exporting and importing profiles



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



Point

Likewise, you can export and import policies.

Procedure for exporting profiles

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Profiles].
2. Select the profiles to be exported.
3. From the [Actions] button, select [Export].

4. Set up an encryption password key (required), and then execute the export by the [Export] button.

Procedure for importing profiles

1. Connect to ISM-VA over FTP and transfer the profiles to be imported.
2. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Profiles].
3. Select the location where the profile is stored in the tree on the left, select the [Actions] button - [Import].
4. Enter the password combined key you set up when exporting the profiles (required), and then execute the import by the [Import] button.



- When the import is complete, deleting the files you transferred to the FTP server in Step 1 does not cause any problem.
- Since profiles contain passwords and other security information, it is required to set up a freely specifiable encryption key when you export profiles.

Procedure for editing profile groups



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

Procedure for deleting profile groups



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

Procedure for editing policy groups



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

Procedure for deleting policy groups



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

Required preparations before OS installation

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

If you are going to import an ISO image of the OS installation media, extend the size of the LVM volume for the user group.

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

For details, see "[2.3.2 Repository Management](#)."

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

For details, access your local support.

Precautions on OS installation

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

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

Procedure for specifying scripts to be executed after OS installation

To execute any specified scripts after installing an OS, it is required to transfer the script files to the ISM-VA via FTP in advance.

1. Prepare the scripts you want to execute after OS installation.
2. Connect to ISM-VA over 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 how to forward FTP, see "[2.1.2 FTP Access](#)."

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

Specifying behavior when assigning profiles

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

The behavior conditions you can specify are as follows.

- Apply to the part without the change.

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

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

- Hot Profile Assignment (with node power remaining on)

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

Note the following points.

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

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

- You cannot select this mode when OSES or virtual IO settings are the target of your profile assignment.
- Not assigned to the node, and it is applied only on ISM.

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

2.2.4 Firmware Management

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

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

Firmware Management is available for the following nodes:

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

For details on the target nodes, access your local support.

Here, the following points are described:

- [2.2.4.1 Confirmation of Firmware Versions of Nodes](#)
- [2.2.4.2 Firmware Update](#)
- [2.2.4.3 Confirmation of Documentation that Is Supplied with Firmware Data](#)

2.2.4.1 Confirmation of Firmware Versions of Nodes



The following is a sample operation using the GUI.

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

For details on retrieving node information, see "[2.2.1.1 Registration of Datacenters/Floors/Racks/Nodes](#)" in "[Management of node information](#)."

2. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Nodes].
3. In the [Column Display] field, select [Firmware].
4. Confirm the [Current Version] field.

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

2.2.4.2 Firmware Update

Here, the following points are described:

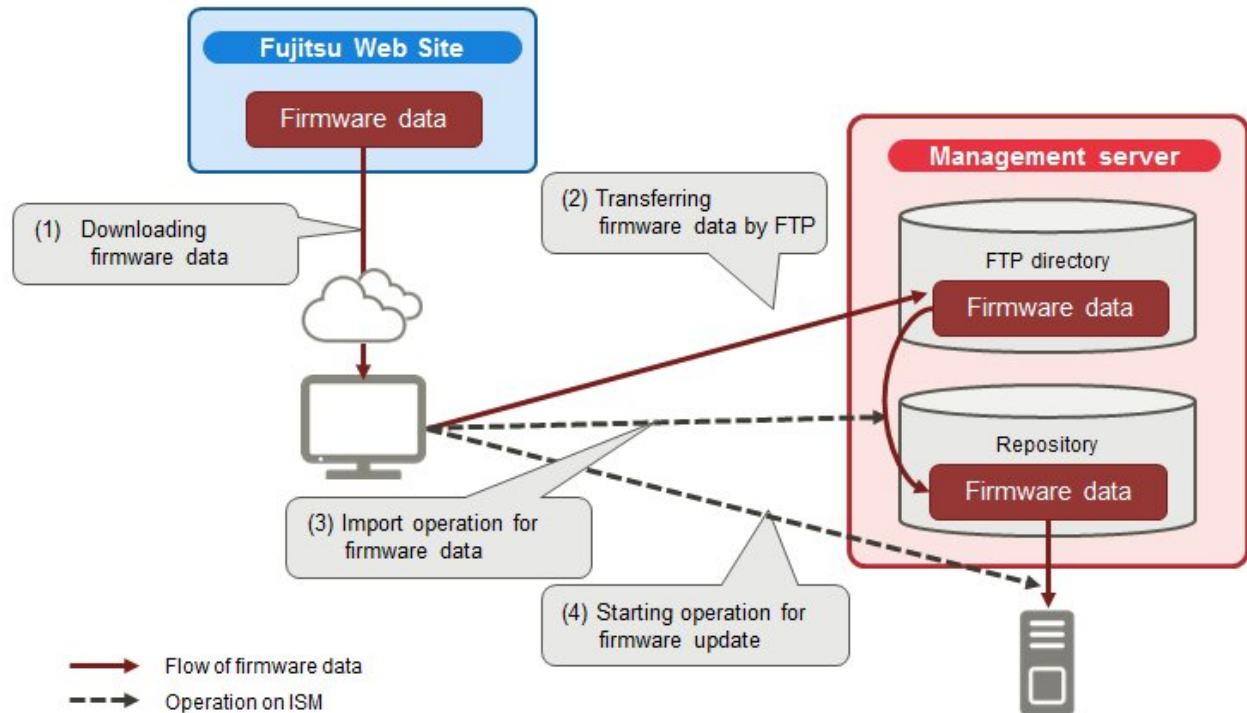
- [Firmware Updates](#)
- [Behavior during updates](#)
- [Executing Firmware Updates](#)

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

Download the firmware data from FUJITSU or another website ((1) in the diagram below), and transfer these data to the repository on ISM-VA ((2) and (3) in the diagram below). ISM uses the firmware data that is deployed in the repository to update the target nodes ((4) in the diagram below).

For details on operations to forwarding firmware data to the repository, see "[2.3.2 Repository Management](#)."

Figure 2.7 Image of Firmware Management



Firmware Updates

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

Online Update

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

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

Offline Update

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

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

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

Required preparations before using Offline Update

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

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

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

For details, see "[2.3.2 Repository Management](#)."

- Use the PXE boot function on the target node.

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

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



Note

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

Behavior during updates

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

Execute any updates according to the table shown below.

Online Update

| Type | Behavior during and after updates |
|---------------------------------|---|
| Server (iRMC) | Updates can be carried out regardless of whether the server power is on or off. |
| Server (BIOS) | <p>Updates can be carried out regardless of whether the server power is on or off.</p> <p>If you execute an update with the power remaining on, it is required to reboot the server and turn the power on again in order to switch to the new firmware (BIOS). You can execute the reboot whenever suits you best. The firmware is automatically applied when you reboot, and then the power of the server turns off. After the power has turned off, you can switch to the new firmware by turning the power on the Details of Node screen in ISM and so on.</p> <p>If you execute an update with the power turned off, it is required to turn the server power on again in order to switch to the new firmware (BIOS). As soon as the firmware update completes, the server power switches on automatically, and then switches off. After the power has turned off, you can switch to the new firmware by turning the power on the Details of Node screen in ISM and so on.</p> |
| Server (Firmware of the server) | Updates can be carried out when the server power is on. |
| Server (with mounted PCI card) | Updates can be executed on the server if a supported OS is running. The new firmware will run only after a reboot. You can execute the reboot whenever suits you best. |
| Switches Storage | Execute the firmware update with the node power remaining on. After the firmware update, you may have to reboot the node. |

Offline Update

| Type | Behavior during and after updates |
|--------------------------------|---|
| Server (iRMC) | Updates can be carried out when the server power is off. |
| Server (BIOS) | <p>During firmware update the server is powered on or restarted, the power is turned off after the firmware update has been completed.</p> <p>After the firmware update has been completed, it will automatically be switched over to the new firmware.</p> |
| Server (with mounted PCI card) | |

Executing Firmware Updates



Note

- While an update is in progress, please observe the following notes.
 - Do not turn the target node on or off.
 - Do not reboot nor reset the target node.
 - Do not interrupt the network connection between ISM and the target node.
 - Do not reboot the management server. Do not power off the management server.
 - Do not delete any import data or firmware data from the repository.
- Before you start any firmware update, confirm the precautions in the documentation that is supplied with the firmware data.
- Firmware data that can be applied on target nodes must be imported in advance, before any update operation.
For details on operations to forwarding firmware data to the repository, see "[2.3.2 Repository Management](#)."
- Firmware cannot be downgraded to an older version.
- As network switches are reset after updating them, data communication is temporarily interrupted. If you are using a redundant network, you should update the sections in the redundancy configuration one after another.
- In case of Brocade VDX switch, you cannot execute firmware update specifying Brocade VCS Fabric. Execute firmware update to each VDX fabric switch under it.
- When you execute a firmware update on ETERNUS DX/AF, account information with a Maintainer role must already be registered in ISM.
- When you execute a firmware update of a PCI card, the OS information of the server on which the PCI card is mounted must already be registered in ISM.
For details on retrieving node OS information, see "[2.2.1.1 Registration of Datacenters/Floors/Racks/Nodes](#)" - "[Registration of node OS information](#)." Also note that firmware updates of PCI cards are supported only for the following OS types:
 - CentOS
 - Red Hat Enterprise Linux
- Firmware updates for PCI cards mounted on servers are executed for all mounted cards of the same type.
If there are multiple cards of the same type, you cannot specify different firmware versions for each card or update only some of the cards. Even if you specify only some cards to be updated, or if you specify different firmware versions for different cards on the ISM screen, the firmware update is executed for all cards of the same type, so all these cards are updated to the same latest firmware version.
- For executing a firmware update for PCI cards (FC/CAN/LAN cards) on Linux, the Qlogic QConvergeConsole CLI must be installed on the OS of the servers on which these PCI cards are mounted.
For details on the installation of Emulex OneCommand Manager CLI or QlogicQConvergeConsole CLI, see "[2.3.3 Installing Emulex OneCommand Manager CLI and Qlogic QConvergeConsole CLI](#)."
- For certain nodes and PCI cards, the format of the version number in the current version column and latest version column might be different.
For applicable nodes and PCI cards, and for how they are displayed, access your local support.
- For certain nodes it is required to execute firmware update in stages. Refer to the document attached to each firmware update.

- After using Online Update to update the server BIOS and the PCI card mounted on a server, the old firmware will continue to run even after update processing has finished in ISM. In order to switch operation to the new firmware, carry out the following procedure.
 - If you update the PCI card mounted on a server, it is required to reboot the server in order to switch to the new firmware. You can execute the reboot whenever suits you best.
 - If you execute an update of the server BIOS with the power remaining on, it is required to reboot the server and turn the power on again in order to switch to the new firmware (BIOS). You can execute the reboot whenever suits you best. The firmware is automatically applied when you reboot, and then the power of the server turns off. After the power has turned off, you can switch to the new firmware by turning the power on the Details of Node screen in ISM and so on.
 - If you execute an update of the server BIOS with the power turned off, it is required to turn the server power on again in order to switch to the new firmware (BIOS). As soon as the firmware update completes, the server power switches on automatically, and then switches off. After the power has turned off, you can switch to the new firmware by turning the power on the Details of Node screen in ISM and so on.
- If processing for the firmware update cannot start normally, or if an update fails, ISM's update processing usually ends with an error. In some cases, however, such as when a target node stops to respond while an update is in progress, timeout errors are not discovered. If processing does not finish for much longer than the presumed time for the task, confirm the status of the target node directly. If there is any error, cancel the firmware update task in ISM.

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

- There is an upper limit for the number of nodes that firmware update can be executed simultaneously. This upper limit is 50 for the entire ISM-VA. If firmware update is executed on a specified number of nodes exceeding the upper limit, the firmware update is first executed on the set maximum number of nodes, and after the preceding firmware update is completed, the update will be executed on the remaining nodes.

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

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Firmware].
2. Set the maintenance mode to a node to be updated.

Select a node name, and set the maintenance mode to the target node with the [Switch Maintenance Mode] button.
3. Confirm the "Current Version" and the "Latest Version" on the node on which you are going to execute the update.
4. Select the checkbox for the node to be updated, then select the [Actions] button - [Update Firmware].
5. Execute the operations according to the instructions on the screen.

When the dialog box for confirmation of the result appears after executing [Apply], this does not mean yet that the assignment itself is complete. Since, after starting the update, the task is registered as a "Task" in ISM, confirm its current status on the "Tasks" screen.

The "Task Details" field in the dialog box for confirmation of the result displays the task ID.

The following tasks types are registered under Firmware Update tasks.

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

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

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

Point

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

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

2. Execute one of the following.
 - From the [Column Display] field in the node list, select [Firmware].
 - From the node list, select the target [Node Name] and select the [Firmware] tab.
-

2.2.4.3 Confirmation of Documentation that Is Supplied with Firmware Data

When you update the firmware, confirm the documentation that came along with the firmware import.

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



Point

.....

- The procedure of checking the document attached to the firmware data can be executed using the same operations as for the screens displayed in the following procedure.
 1. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Nodes].
 2. Execute one of the following.
 - From the [Column Display] field in the node list, select [Firmware].
 - From the node list, select the target [Node Name] and select the [Firmware] tab.
 3. From the [Actions] button, select [Update Firmware].
 4. From the pulldown menu, select the update version and import data, and then select the [Next] button.
 5. In the [Document] field, select the document and confirm the documentation.
 - The update methods in ISM are different from those described in the documentation that is supplied with the firmware data.
 - The method of Online Update for iRMC/BIOS of servers differs from the "Online Update" of the documents attached to the firmware data and the processing corresponding to "Remote update" is performed. The firmware data is transferred from the TFTP server in ISM-VA by using the iRMC Web interface of the target server.
-

2.2.5 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
- Viewing and downloading files on the GUI screen

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

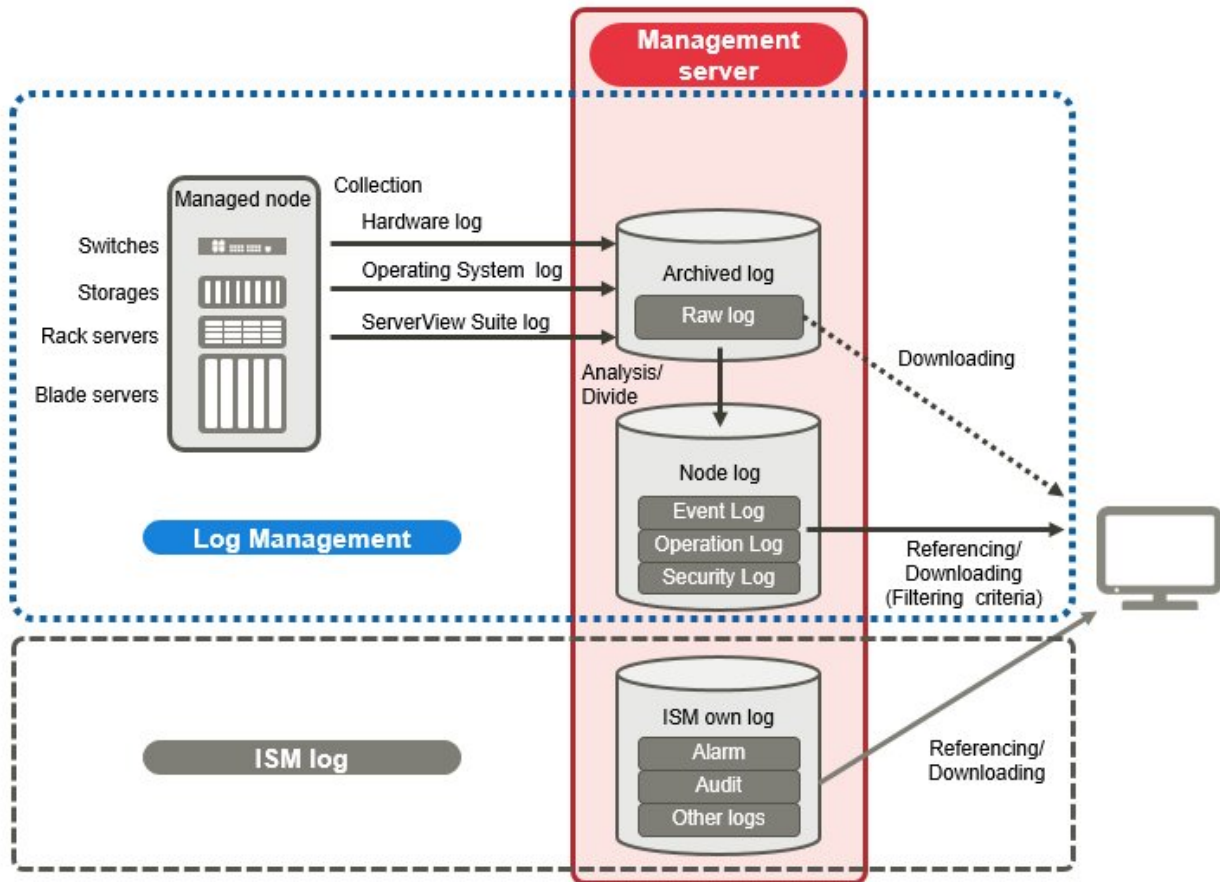
The bulk of log data that are collected from nodes according to these settings are called "Archived Logs."

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

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

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

Figure 2.8 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, generate no correct node log.

Here, the following points are described:

- [Types of collectable logs](#)
- [Setting log retention periods](#)
- [Setting log collection targets, dates and times](#)
- [Operations for log collection](#)
- [Searching node logs](#)
- [Downloading node logs](#)
- [Downloading Archived Logs](#)
- [Deleting node logs](#)
- [Deleting Archived Logs](#)

Types of collectable logs

Log Management can collect three types of log: hardware logs, operating system logs, and ServerView Suite logs. For supported hardware, OSeS, and other details, access your local support.

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 | SEL | SEL |
| | IPCOM VX2 | | |
| Storage | ETERNUS DX/AF | Exported results for "export log" command Exported results for "show events" command | Exported results for "show events" command |
| Switches | SR-X | Exported results for "show tech-support" command | Exported results for "show logging syslog" command (Included in exported results for "show tech-support" command) |
| | 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) |

Operating system logs

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

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



Note

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

ServerView Suite logs

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

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

Note

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

Setting log retention periods

Executable user

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

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

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

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

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

Point

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

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

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

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

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

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

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

Setting log collection targets, dates and times

Executable user

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

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

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

- Log Collection Target

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

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

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

- Retention Period (required for all items)

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

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

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

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

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

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

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



Note

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

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

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

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

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

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

- Specifying by day of the week

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

Example 1: Log retrieval every Sunday at 23:00

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

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

- Specifying by date

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

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

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

The following is a sample setting operation using the GUI.

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Log Collection].
2. From the [Log Collection] menu, select [Log Collection Settings].
3. Select the checkboxes for the nodes for which to make the settings. By selecting the checkboxes for multiple nodes, you can set the same contents in a batch.
4. From the [Actions] button, select [Edit Log Collection Settings].

Point

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

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

Operations for log collection

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

Periodical log collection

Periodical log collection collects and accumulates node logs periodically, according to a specified schedule.

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

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

Note

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

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

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

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

- Depending on the type of node, log collection may take some time to complete. This may cause large differences between the scheduled times for log collection and the time stamps of retained logs.
- After starting periodical log collection, you cannot cancel it in the middle of the process. Therefore, if maintenance such as firmware update, profile application and etc. to target nodes is planning and it overlaps the periodical log collection execution time, maintenance can be failed. It is recommended to either disable the periodical log collection or change the setting of schedule.

- There is an upper limit for the number of nodes from which logs can be collected simultaneously. If the maximum number of log collections is in progress, any log collection you start after that will not be executed immediately but only after the preceding log collections have finished.
- While a log collection is in progress, processing for log deletion is suspended.

Manual log collection

You can collect and accumulate node logs at any suitable time.

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

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Log Collection].
2. From the [Log Collection] menu, select [Log Collection Settings].
3. Select the checkboxes for the nodes from which to collect logs. By selecting the checkboxes for multiple nodes, you can set the same contents in a batch.
4. Select the [Actions] button and select [Collect Logs].

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

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

Under Task Type, [Collecting Node Log] is displayed.

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

Point

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

- From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Log Collection] to execute either of the following.
 - Select [Log Management] on the Log Collection menu.
 - Select [Node Log Search] on the Log Collection menu.
- From the Global Navigation Menu on the GUI of ISM, select [Management] - [Nodes] to execute either of the following.
 - From the [Column Display] field in the node list, select [Log Settings].
 - From the node list, select the node name of the node and select the [Log Settings] tab.

Note

- Although cancel of manual log collection can be executed from the [Tasks] from the top of the Global Navigation Menu, the cancel cannot be completed until the log collection is completed if log collection is being executed.
- Each time you execute a manual log collection, this is added to the number of retained generations for Archived Logs. Note that repeatedly executing this operation several times eventually deletes logs from the past that exceed the setting for the number of retained generations. Moreover, if manual log collection results in an error, it is not added to the number of generations count.
- While a log collection is in progress, processing for log deletion is suspended until the log collection completes.

Monitoring function for disk capacities of log storage locations

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

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

The upper limit for the total size (for example, Size restriction) of various log files (for example, Archived Log, Node Log (for download data), and Node Log (for log search data)) stored in ISM and the specified value for monitoring the disk capacity (Threshold monitoring) are set in Edit User Group Settings. For details of User Group Settings, see "[2.3.1.2 Managing User Groups](#)."

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

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

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

Searching node logs



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

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

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

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

The logs that contain the keyword you entered are displayed.

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

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

The logs that match the condition you entered are displayed.



Point

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

Downloading node logs



You can download accumulated node logs by specified periods and types.

You can also download logs of multiple nodes collectively.

The downloaded files are compressed into a single zip file.

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

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

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

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

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

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

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

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

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

Point

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

Note

ISM can retain only one download file at a time. Therefore, if you execute multiple download operations for logs successively, the previously created download files are deleted.

The downloaded logs are stored with the following file name.

- Name of download file

Log_<specified download interval>.zip

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

Example: If you specified the period from June 1, 2016 through June 7, 2016

Log_20160601-20160607.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."

Downloading Archived Logs



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

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

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Log Collection].
2. From the [Log Collection] menu, select the [Management Logs] - [Archived Log] tab.
3. Select the checkboxes for the Archived Logs to be downloaded.

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



Point

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



Note

ISM can retain only one download file at a time. Therefore, if you execute multiple download operations for logs successively, the previously created download files are deleted.

The downloaded logs are stored with the following file name.

- Name of download file

```
Material_<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."

Deleting node logs



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

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

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

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



Note

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

Deleting Archived Logs

| | 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 |

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

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

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Log Collection].
2. From the [Log Collection] menu, select the [Management Logs] - [Archived Log] tab.
3. Select the checkboxes for the target nodes.
Multiple nodes can be selected.
4. Select the [Actions] button and select [Delete Archived Log Files] to execute deletion according to the instructions on the screen.
The "Result" screen is displayed. Take a memo of the detailed task number that is displayed on this screen.
Deletion can also be executed from the screen displayed if you select [Actions] button and select [Show Archived Log Files].
In this case, select the checkboxes for the files to be deleted. By selecting the checkboxes for multiple files, you can delete them in a batch.
5. From the top of the Global Navigation Menu, select [Tasks] and check the processing status.
Under Task Type, [Deleting Log files] is displayed.
For the Task ID, confirm the detailed task number of which you took a memo on the "Result" screen.



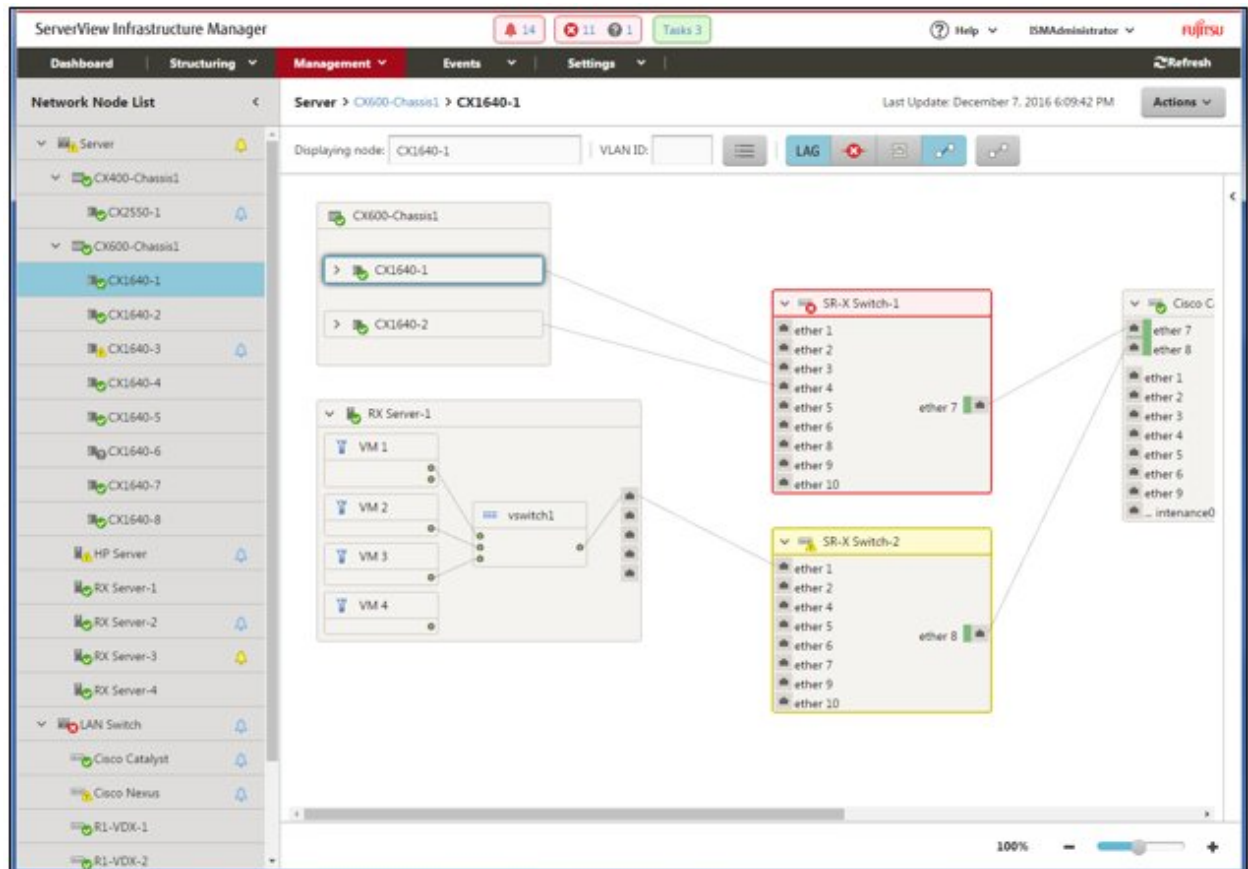
Note

- Deleting Archived Logs may take some time to complete. Therefore, the information of an Archived Log that you set to be deleted may be displayed on the GUI until deletion processing for node logs is completed. In such a case, confirm under the corresponding task on the "Tasks" screen that processing for Archived Log deletion is completed, and then open this screen again.
- Until deletion of Archived Logs completes, processing for log collection is suspended.

2.2.6 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 of the physical ports, the virtual switches and the virtual machines of the managed node
- Confirming the VLAN and Link Aggregation settings for network switches and changing these settings



Here, the following points are described:

- Network Information Display
- Updating network management information
- Confirming information on changes in network connections
- Setting reference information for changes in network connections
- Confirming VLAN and Link Aggregation settings
- Changing VLAN Settings

- [Changing Link Aggregation settings](#)
- [Setting network connection information manually](#)

Network Information Display



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

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

Operating procedure

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

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

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






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

The node at the top of the Network Node List is selected by default when Network Map is displayed.

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 Switch Display Information buttons.

| Button | Description |
|---|--|
|  | Switch the display of Link Aggregation settings on the Network Map ON and OFF. |
|  | Switch the display the scope of influence of an error on the Network Map ON and OFF. If there is a connection with a node where an error or fault has occurred, the edge of the next node connected to as well as the port connected to are displayed in yellow. If virtual networks are constructed on the node connected to, the affected virtual networks will also be displayed in yellow. |
|  | Switch the display of the link down port on the Network Map ON and OFF. |
|  | Switch the display highlights function on the Network Map ON and OFF. When the display highlights function is ON, if you select the managed nodes or its ports the connections it has are highlighted. |
|  | Turn off all of the highlight displays on the Network Map. |

Point

The Network Map displays the nodes that have a connection relationship with the nodes you selected in the Network Node List. By selecting the [>] icon of a node on the Network Map, you can extend the display of the ports within the node.



- LLDP (Link Layer Discovery Protocol) is used for retrieving information on physical network connections. If your nodes do not support LLDP or if LLDP is disabled, the information for actually existing connections cannot be retrieved. For information on whether a node supports LLDP and on how to confirm whether the LLDP settings of the node are enabled or disabled, confirm the technical specifications of each respective node.
- The displayed Network Map shows either the status retrieved when you last executed [Refresh network information] or the status at the point of the periodical update of network management information once a day by ISM. In order to confirm the most recent status after registering nodes, modifying any connections, or after an error, select the [Actions] button and execute [Refresh network information]. Likewise, whenever the hardware configuration of a node was changed, on the Details of Node screen for the respective node, execute [Get Node Information] and then [Refresh network information]. The periodical update of network management information starts at 4:00 AM.
- To display the connection relationships between the virtual switches and the virtual machines, it is required to register the OS information of the Cloud Management Software and of the managed target nodes to ISM. For details on registering the Cloud Management Software, see "[2.3.6 Management of Cloud Management Software](#)", and for registering OS information see "[2.2.1.1 Registration of Datacenters/Floors/Racks/Nodes](#)."
- In managed nodes, if the port is set as teaming (bonding), displaying the port status and connection relationships between the port and the virtual switch is not supported. It is required to access the nodes directly to check it.

Updating network management information



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

Operating procedure

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



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.



- Update the node information for each managed node before updating the network management information. See "[2.2.1.1 Registration of Datacenters/Floors/Racks/Nodes](#)" in "[Management of node information](#)" for how to retrieve node information.
- Depending on the number of managed nodes, updating the network management information may take some time to complete. To confirm that the information update is complete, confirm the event in the Operation Log under Tasks that indicates completion of the information update.
- The latest update time of the network management information is displayed on the upper right part of the Network Map. This last update time specifies the last time information update was completed.
- A periodical update of the network management information is executed once a day at 4:00 AM.

- You can maintain updates of the latest network management information by executing the command after updating the information for each node.

Confirming information on changes in network connections



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

- Added

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

- Deleted

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

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

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

Operating procedure

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

A list of the nodes that are supported on the Network Management 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.

The node at the top of the Network Node List is selected by default when Network Map is displayed.

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

3. From the [Actions] button, select [Confirm connection state 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 "Connection state change List."



Note

Selecting the [Refresh] button under [Confirm connection state change] updates the reference point and deletes the information on changes.

Setting 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.

Operating procedure

1. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Network Map].
A list of the nodes that are supported on the Network Management 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.
The node at the top of the Network Node List is selected by default when Network Map is displayed.
The Network Map is displayed at the center of the screen.
3. From the [Actions] button, select [Confirm connection state 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.

Confirming VLAN and Link Aggregation settings





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

Operating procedure

1. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Network Map].
A list of the nodes that are supported on the Network Management 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.
The node at the top of the Network Node List is selected by default when Network Map is displayed.
The Network Map is displayed at the center of the screen.
3. Execute the following procedure for the item you want to confirm.
 - VLAN
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 [>] icon of a node on the Network Map.
The ports inside the node are opened and the Link Aggregation settings are displayed.

Point

- The currently set "Setting VLAN ID Information" can be confirmed in  button.
- Switch ON and OFF to display the Link Aggregation settings on the network using  button.

- 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.

Changing VLAN Settings

| | Administrator group | Other groups |
|-----------------|---|---|
| Executable user | <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"/> |

You can change the VLAN settings of a network switch.

Operating procedure

1. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Network Map].
2. From the Network Node List, select the node, serving as the point of the network connection that you want to set up.
The node at the top of the Network Node List is selected by default when Network Map is displayed.
The Network Map is displayed at the center of the screen.
3. From the [Actions] button, select [Multiple VLANs settings].
4. Check to select the respective ports for which you want to set the same VLAN ID, and select the [Setting] button on the top right side.
5. Enter the VLAN ID you set and edit the contents, and then select the [Confirm] button.
6. Confirm the changed contents of the setting, and then select the [Register] button.
The VLAN settings are changed.

Point

VLAN settings can be changed also on a node basis. From the [Actions] button, select [VLAN setting].

Note

- Depending on the VLAN settings contents, VLAN settings assignment may take some time to complete. Refresh the screen after you have completed VLAN settings. You can confirm the current progress of VLAN settings assignment on the "Tasks" screen. For details, see "2.3.4 Task Management."
- VLAN settings have their own specifications and therefore may differ depending on the models of network switches. Make settings after confirming the device specifications.
- The number of VLAN IDs that can be set for a port is up to one hundred (100).
- There exists a reserved VLAN IDs depending on the models of network switches. You cannot change the settings of reserved VLAN ID. See the specifications of respective nodes.

Changing Link Aggregation settings

| | Administrator group | Other groups |
|-----------------|---|---|
| Executable user | <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"/> |

You can change the settings of Link Aggregation of a network switch.

Operating procedure (example for addition)

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

2. From the Network Node List, select the node, serving as the point of the network connection that you want to set up.
The node at the top of the Network Node List is selected by default when Network Map is displayed.
The Network Map is displayed at the center of the screen.
3. From [Actions] button, select [Link Aggregation setting].
4. Select the name of the target node for which you set up a Link Aggregation and select the [Add] button of Link Aggregation Setting.
5. Enter the LAG Name and Mode, confirm the port for which you set the Link Aggregation, and then select the [Confirm] button.
6. Confirm the setting contents of the Link Aggregation and select the [Register] button.

Note

- Link Aggregation settings have their own specifications and therefore may differ depending on the models of network switches. Make 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, see the specifications of respective nodes.
- You cannot set up a Link Aggregation between the ports having different VLAN IDs. Be sure to confirm that these ports have the same VLAN settings to change the Link Aggregation settings.
- Whenever you set up a Multi-Chassis Link Aggregation between different nodes, it is required to change Link Aggregation settings for respective switches. To set Multi-Chassis Link Aggregation, it is required to first execute the settings for the peer link connection between nodes and the settings for the managed nodes.
- 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. Make settings after confirming the device specifications.

Setting network connection information manually

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"/> |

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.

Operating procedure

1. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Network Map].
A list of the nodes that are supported on the Network Management 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.
The node at the top of the Network Node List is selected by default when Network Map is displayed.
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 make the settings, and then select the [Add] button.

Note

After selecting the [Add] button and if you want to cancel the settings you executed manually, select the [Clear] button.

5. After adding all the connection information you want to set, select the [Save] button.
6. Confirm that the edited contents are correct and then select the [Save] button.

2.2.7 Power Capping

For the devices mounted in racks, power capping is used to keep it from exceeding the set upper limit value for power consumption.

Beforehand, register the control information and power consumption control policy for each node in the rack and start power capping operations by enabling the power capping policy.



There are the following four types of power capping policies.

- Custom 1, Custom 2

Power capping policy for normal operations. Two types can be operated and switched between.

- Schedule

Policy that is only enabled on the specified day/time.

- Minimum

Control where power capping is kept to a minimum.

Add/Edit power capping policies

| | 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 |

Node power settings

Set the power information and operation priority for each node.

Adjust what power consumption level should be set for what device based on the set information.

The current power consumption value can be confirmed if it is a device that power consumption value can be retrieved for, and if the power capping status is [Stopped Power Capping] or [Power Capping].

If the node cannot execute power capping, maximum power consumption value is alternated as a fixed value.

Power capping policy

Set the upper limit value for power consumption for each policy.

Set operation schedule for schedule policy.

Enable/Disable power capping

| | 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 |

Switch the power capping policy between enabled and disabled.



Each power capping policy can be enabled independently, but if minimum is set, minimum is prioritized and used. If multiple policies other than minimum are enabled, the policy with the lowest upper limit value for power consumption is used.

Note

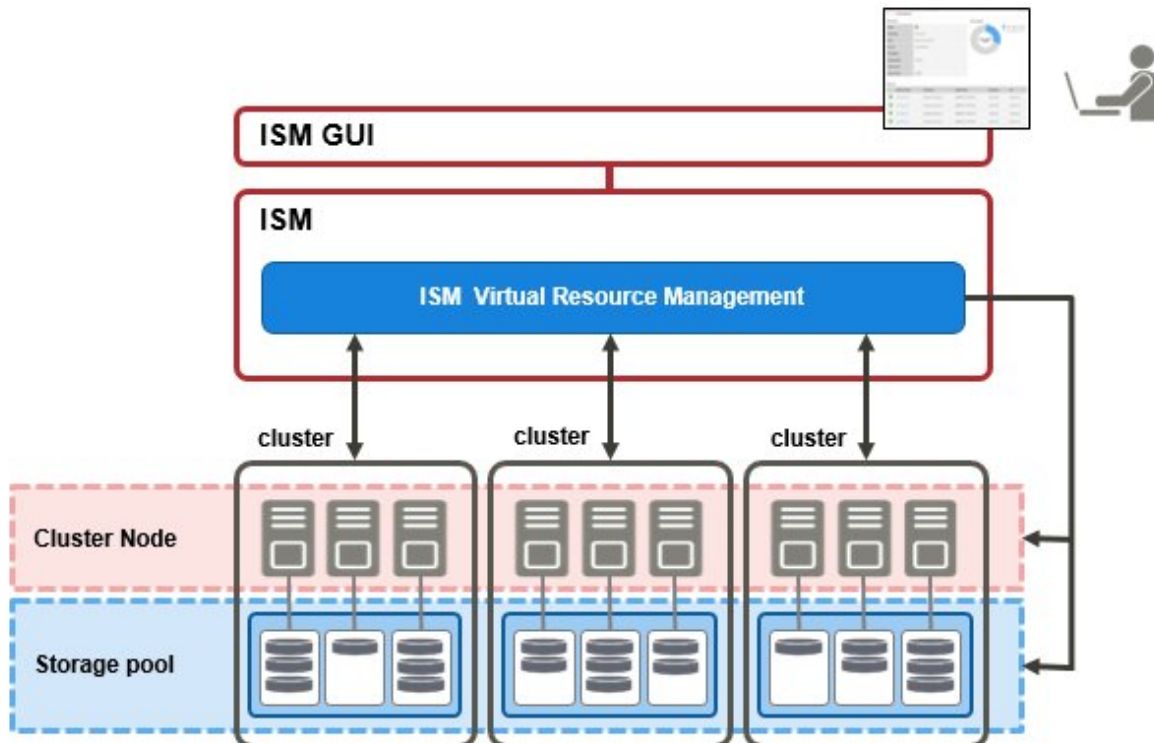
- For racks with an already executed power capping policy, it is required to change the power capping settings if a node was added. If the settings are not changed the power consumption for the rack will be greater than the set upper limit value.
It is recommended that you review the upper limit value in the rack power capping settings even for nodes that have been deleted.
When migrating nodes, it is required to take measures accordingly to each rack before and after migration.
- The upper limit value is the target value of the power capping. Normally the upper limit is set with some margin so that the actual power consumption is below, but if the upper limit value is set low the power consumption might exceed it.
- If the PRIMERGY CX chassis or the ETERNUS DX connected to Drive Enclosure was deleted or moved to a different rack, the power capping policy of the server node for the mounted PRIMERGY CX or the connected Drive Enclosure will also be deleted.
- If using the PRIMERGY RX S7 series, set a numerical value higher than the sum total of the minimum power consumption value of the PRIMERGY RX S7 series.
The minimum power consumption value of the devices can be checked in the [Power Capping] - [Current Power Consumption] - [Current Total Power Consumption] column in the iRMC Web interface.
- If changing the date and time of ISM-VA to past dates or times the power consumption value displayed in [Rack Information] in the [Rack Details] screen and the average power consumption value and average intake air temperature value in the [Monitoring] tab in the Details of Node screen will not be displayed correctly.
When the date and time set in ISM-VA passes it will be displayed correctly again.

2.2.8 Virtual Resource Management Function

The virtual management function is a function to manage and monitor the items managed as virtual resource in ISM GUI.

The following is the environment configuration operating this function.

Figure 2.9 Configuration of the operating environment for the Virtual Resource Management Function





Note

For pre-settings for virtual resource management, please access your local support.

2.2.8.1 Supported Virtual Resources

The following is the virtual resource to be supported by this function.

VMware Virtual SAN

ISM GUI attribute information and status and other information regarding VMware Virtual SAN (hereafter, "VSAN") VSAN data stores are displayed.

The following are the requirements for VSAN environments supported by the Virtual Resources Management Function.

| Item | Requirement |
|----------------------|--|
| Hypervisor | <ul style="list-style-type: none">- VMware ESXi 6.0 Update 2- VMware ESXi 6.5 |
| VSAN Version | <ul style="list-style-type: none">- 6.2- 6.5 |
| Management Appliance | <ul style="list-style-type: none">- vCenter Server Appliance v6.0 Update 2- vCenter Server Appliance v6.5 |

Microsoft Storage Spaces Direct

Attribute information and status and other information regarding Microsoft Storage Spaces Direct memory pools are displayed.

The following are the requirements for Microsoft Storage Spaces Direct environments supported by the Virtual Resources Management Function.

| Item | Requirement |
|-------------------|---|
| OS | Windows Server 2016 |
| Role and function | <p>The following roles and functions are installed</p> <ul style="list-style-type: none">- Hyper-V- Microsoft Failover Cluster |



Note

It is required to enable CredSSP authentication in advance. For pre-settings for virtual resource management, please access your local support.

ETERNUS Storage

ISM GUI attribute information and status and other information regarding ETERNUS Storage are displayed.

The following are the requirements for ETERNUS Storage supported by the Virtual Resources Management Function.

| Item | Requirement |
|--------------------------------------|--|
| ETERNUS device type and storage type | <p>RAID Group of the following ETERNUS DX series</p> <ul style="list-style-type: none">- ETERNUS DX60 S3- ETERNUS DX80 S2 |

| Item | Requirement |
|------|---|
| | <ul style="list-style-type: none"> - ETERNUS DX90 S2 - ETERNUS DX100 S3 - ETERNUS DX200 S3 |

Note

The display of thin provisioning pool for ETERNUS is not supported.

The volume used by thin provisioning pool is not reflected even when RAID group is built into thin provisioning pool.

For reference and management of thin provisioning pool, use ETERNUS Web GUI.

For applicable ETERNUS device types, access your local support.

2.2.8.2 Virtual Resource Management GUI

The virtual resource management is equipped with the management GUI.

The following displays the functions of each GUI screen and the mutual display relationships.

See the ISM online help for items displayed on the GUI and descriptions. For how to add widgets, see "ServerView Infrastructure Manager V2.1 Operating Procedures."

Figure 2.10 Virtual Resource Management GUI



(a) Virtual resources widget display

The status of the virtual resources is displayed in a widget on the ISM dashboard.

(b) Virtual resources list display

Displays a list for the statuses of the virtual resources.

The resource use status is also displayed by the color and direction of the arrows.

(c) Virtual resources detailed information display

Detailed information, such as virtual resource settings information and utilization, is displayed.

The physical nodes making up the virtual resources are displayed and related screens can be displayed.

(d) Virtual resource information on node information ([SDS] tab)

The [SDS] tab that displays virtual resource information on the Details of Node screen is displayed.

If you select the [SDS] tab, the virtual resource information related to nodes on VSAN or Microsoft Storage Spaces Direct is displayed.

2.2.8.3 Operation of Virtual Resource Management

The following describes how to operate the virtual resource management.

- [Monitoring for the Use Status of Storage Pools](#)
- [Identifying the Error in Storage Pools](#)
- [Refresh for Virtual Resource Information](#)



Point

Before monitoring by ISM, it is required to register virtual resource environment to ISM. It is executed with the following procedures.

1. Confirm that nodes configuring the storage pool (cluster) are already registered in ISM.

For how to register nodes and to confirm the information, see "[2.2.1 Node Management](#)."

2. Confirm that virtual management software is already registered in ISM.

For how to register virtual management software and to confirm the information, see [2.3.6 Management of Cloud Management Software](#)."

3. Update the virtual resource information.

For how to update the information, "[Refresh for Virtual Resource Information](#)."

The storage pool information is displayed on the virtual recourse GUI.

Monitoring for the Use Status of Storage Pools



Here the method for monitoring use status of storage pools is described.

1. From the Global Navigation Menu on the GUI of ISM, select [Dashboard] to display the virtual resource widget "Resource List."

For how to add widgets, see "ServerView Infrastructure Manager V2.1 Operating Procedures."

- Refer to "Utilization" for the current utilization of the storage pools.

| Resource List | | | | |
|---------------|------------|--------------------|----------|-------------|
| Status | Pool Name | Type | Capacity | Utilization |
| ✓ | VSAN_pool1 | VMware Virtual SAN | 10TB | 30% |
| ⚠ | VSAN_pool2 | VMware Virtual SAN | 10TB | 50% |
| ✓ | VSAN_pool3 | VMware Virtual SAN | 20TB | 75% |
| ✗ | VSAN_pool4 | VMware Virtual SAN | 10TB | 50% |
| ✓ | VSAN_pool5 | VMware Virtual SAN | 20TB | 75% |

- More detailed utilization information can be found in the Virtual Resources list display screen.

The current utilization can be determined from the direction and color of the arrows.

From the Global Navigation Menu on the GUI of ISM, select [Management] - [Virtual Resource]. The list of virtual resources that can be managed by ISM displays the various types of resources in a tree and list form.

| Pool List | | | | | | | |
|-------------------------------------|------------|---|-------------|---------------------|-------------|--------------------|----------|
| <input type="text" value="Search"/> | | ✓ ⚠ ✗ ? 5 / 5 | | Action | | | |
| | Pool Name | Utilization | | | | Type | Capacity |
| | | Current | 10 Days Ago | 20 Days Ago | 30 Days Ago | | |
| ✓ | VSAN_pool1 | 30% → | 38% | 35% | 30% | VMware Virtual SAN | 10TB |
| ⚠ | VSAN_pool2 | 50% ↗ | 38% | 35% | 30% | VMware Virtual SAN | 10TB |
| ✓ | VSAN_pool3 | 75% ↑ | 38% | 35% | 30% | VMware Virtual SAN | 20TB |
| ✗ | VSAN_pool4 | 50% ↗ | 38% | 35% | 30% | VMware Virtual SAN | 10TB |
| ✓ | VSAN_pool5 | 75% ↑ | 38% | 35% | 30% | VMware Virtual SAN | 20TB |

The utilization is interpreted in the following way.

- Color of the arrow

Displays the current total utilization.

Green: Less than 70% is used.

Yellow: Between 70% and 90% is used

Red: More than 90% is used

- Direction of the arrow

The utilization displays an increase rate compared to the utilization 10 days earlier.

Sideways: The utilization is moving sideways, is increasing slightly (The utilization is increasing with less than 5%) or is decreasing

Diagonal upwards: The utilization is increasing (The utilization is increasing with between 5% - 15%)

Upwards: The utilization is increasing sharply (The utilization is increasing with more than 15%)

If you select the target pool name, the Resource Details screen is displayed, and in "Utilization" you can check the currently used capacity and the available capacity.

2. Execute the following procedure if there is not sufficient capacity available.

- Add storage.

The nodes making up the storage pool are displayed in the node list. If there is not sufficient available capacity there is a risk this limits the available space in the storage made up by the nodes.

The insufficient available capacity can be mitigated by adding nodes to the disk, or by adding new nodes.

- Execute the required maintenance operations if an error is found in the nodes.

If the statuses shown in then node list shows any errors, the storage capacity of this node cannot be used and capacity might become insufficient.

Check the incident for the node in the event log and take appropriate measures.

Identifying the Error in Storage Pools



The following describes the procedure for discovering error and identifying cause in storage pools.

Step 1

Refresh the information of the virtual resources.

From the [Actions] menu, select [Refresh Virtual Resource Information]. For detail, refer to "[Refresh for Virtual Resource Information](#)."

The virtual resource information on the GUI is refreshed to the latest. If an error occurs, the displayed status will change.

Step 2

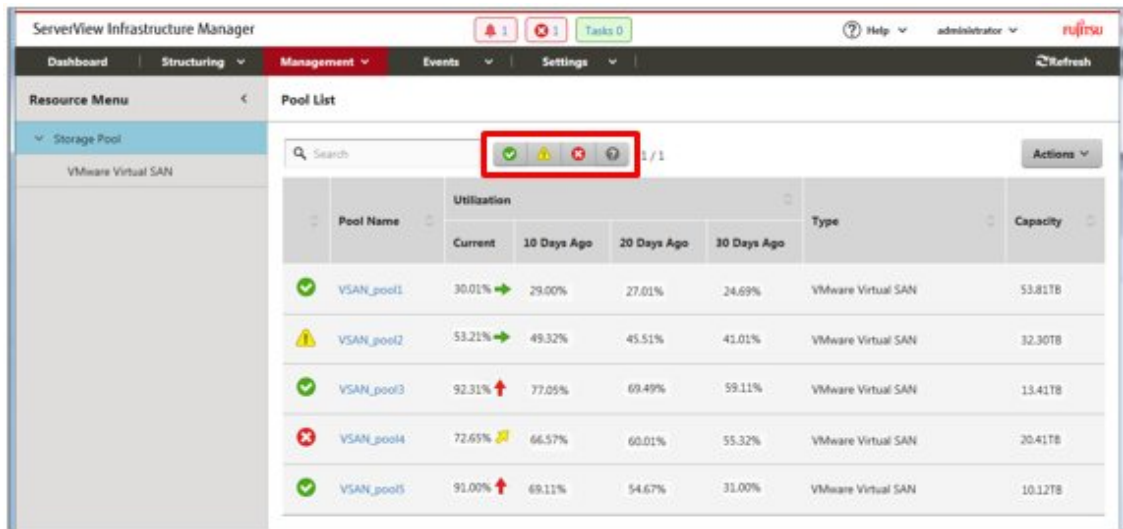
Discover and identify errors.

Resource errors can be checked from the virtual resource list screen. If displaying the "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 display screen

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

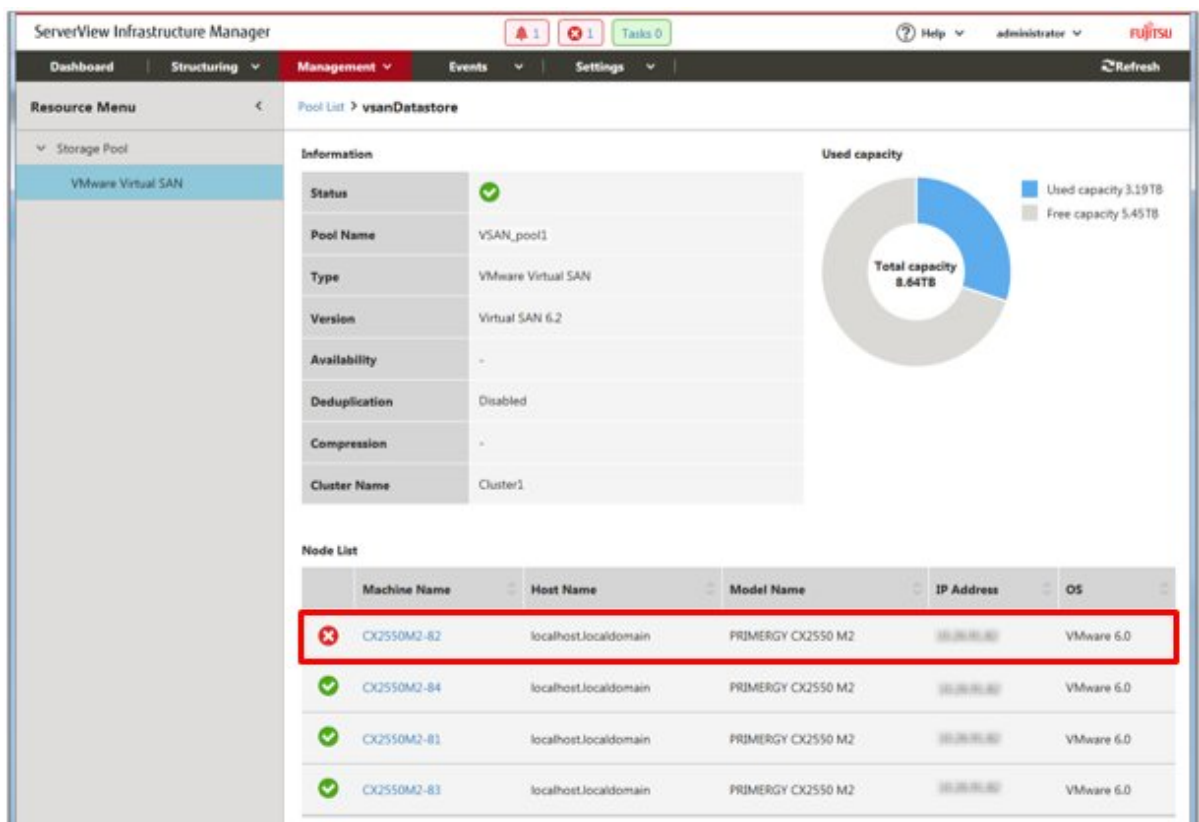
The virtual resources list screen is displayed.



Virtual resources with the selected status can be filtered out from the status filter icon at the top of the screen.

2. Select the pool name.

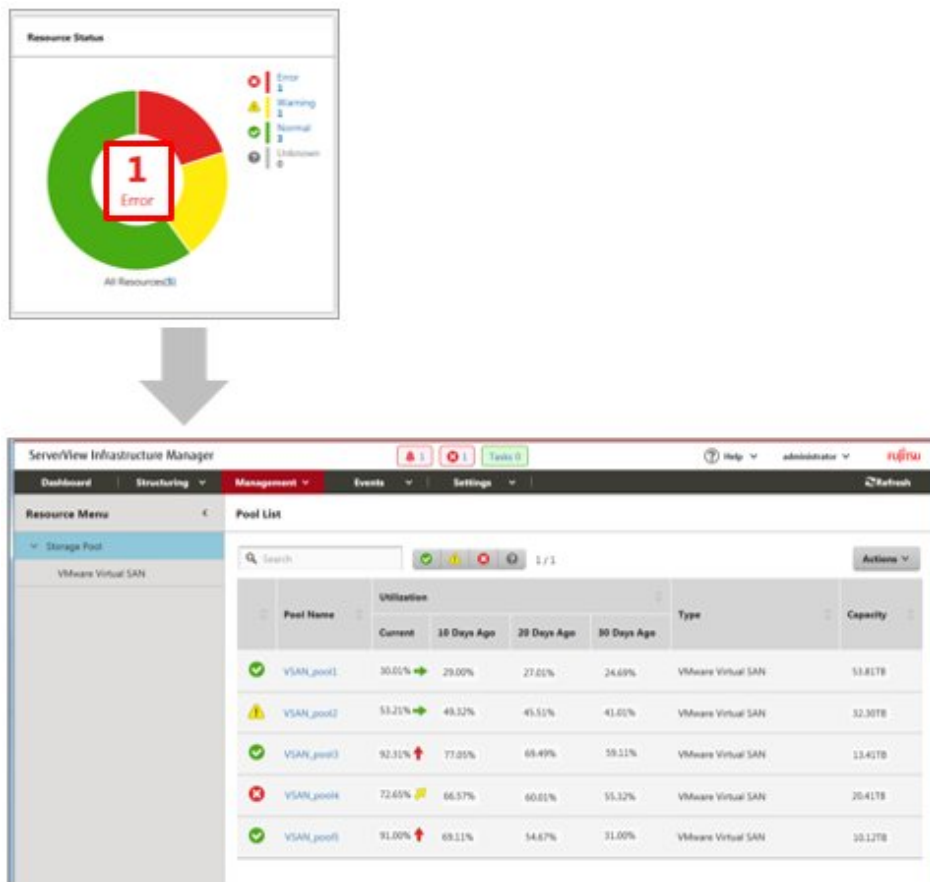
When the virtual resources detailed information screen is displayed, check the device names that error is displayed for in the "Node List."



(2) When identifying the place of an error from the dashboard

1. Select the numbers displayed in the middle of the "Resource Status" widget on the ISM dashboard.

A list of the error status resources will be displayed.



2. Select the pool name.

When the virtual resources detailed information screen is displayed, check the device names that error is displayed for in the "Node List."

Step 3

Check the details of the error that occurred.





- (1) If an error is displayed for the virtual resource

If the storage pool status displays an error, the following situations are probable.

| Layer where error status occurred | Status |
|-----------------------------------|--|
| Physical layer | <p>An error occurred in the storage pool because of a problem with a physical component (HDD, SSD, node).</p> <p>Depending on the type of SDS, it will be one of the following states.</p> <ul style="list-style-type: none"> - If it is a VSAN, errors occur in the health of VSAN - If it is Microsoft Storage Spaces Direct, errors occur on the nodes or physical disks making up the memory pool - If it is ETERNUS, errors occur on RAID groups, physical disks, or ETERNUS devices |

| Layer where error status occurred | Status |
|-----------------------------------|---|
| Virtual layer | An error has occurred in the virtual resource layer (data store). |

The following are statuses of storage pools according to each status.

| Status | In ISM GUI displayed by icons | Status |
|---------|---|---|
| Error |  | A problem has occurred in the storage pool and it is not possible to continue to use. |
| Note |  | A problem has occurred in the storage pool but it is possible to continue to use. |
| Unknown |  | A problem has occurred in the storage pool and its status cannot be confirmed. |
| Normal |  | The storage pool is in a normal status. |

Point

If the capacity of the storage pool is reduced by an error in the physical or virtualized layer, whether it can continue to be used as a storage pool can be determined by the "Error" status.

The error details and place where it occurred are checked in the following way.

Point

For how to identify detailed error location and its corrective actions, or to restore the error, execute procedures according to each storage pool manuals.

VSAN

The status of the storage view VSAN datastore and the "Health" of the VSAN are checked on either the ISM GUI or in the VMware vCenter Web Client.

1. From the virtual resources list on the ISM GUI or from the details screen, check "Pool Name" and "Cluster Name."
2. Sign in to VMware vCenter Server Web Client and in the [Storage View] tab, check the status of the displayed pool name previously checked in step 1.

If it is operating normally there is no mark, and any errors are marked in red.

3. In "Hosts and Clusters", select the node name checked in step 1.
4. From the [Monitoring] tab, select [Virtual SAN] - [Health].

Refer to the "Test result" of the VSAN health and identify the error contents.

Execute the following after recovering from an error.

1. Sign in to the VMware vCenter Server Web Client and select the cluster name in "Hosts and Clusters."
2. From the [Monitoring] tab - [Virtual SAN] - [Health], select [Test again] in the displayed Virtual SAN health screen and then check that the test result that was "Failed" now has changed to "Passed."
3. Select the [Storage View] and from the displayed datastore list, check that the status of the VSAN datastore is normal.
4. From the Virtual Resource list screen on the ISM GUI, select the [Actions] button - [Refresh Virtual Resource Information] and check that the status has returned to normal.

Microsoft Storage Spaces Direct

From the ISM GUI or the server manager on the management server, check the status of the memory 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 services and memory services] - [Memory pool] and check the status of the 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 services and memory services] - [Memory pool] and check that the memory pool and the physical disk are operating normally.

Since the displayed information might be old, select the [Refresh] button on the screen and check after refreshing the information.

2. From the Virtual Resource list screen on the ISM GUI, select the [Actions] button - [Refresh Virtual Resource Information] and check that the status has returned to normal.

ETERNUS Storage

Open ETERNUS Web GUI with Web browser, check the statuses of RAID groups and physical disks.

For URL of ETERNUS Web GUI, move to "Node Lists" on the details of the virtual resource screen, then you can confirm it by the node information when selecting the device name of ETERNUS.

After recovering the error, from the Virtual Resource list screen on the ISM GUI, select [Refresh Virtual Resource Information] from the [Actions] button and check that the status has returned to normal.

(2) If the node error is displayed in the "Node list"

Check the details of the error in the ISM Event Log.

1. From the Global Navigation Menu on the GUI of ISM, select [Events] - [Events].
The "Event List" screen is displayed.
2. Check the error contents by entering "Node name" into the search box and search for events for the entered node.

Refresh for Virtual Resource Information

Executable user

| Administrator group | Other groups |
|---|---|
| Admin Operator Monitor | Admin Operator Monitor |

From the virtual resources list screen, execute [Refresh Virtual Resource Information] from the [Actions] button.

| Pool List | | | | | | | |
|-------------------------------------|------------|---|-------------|------------------------|-------------|--------------------|----------|
| <input type="text" value="Search"/> | | ✓ ⚠ ✗ ? 5 / 5 | | Actions ▼ | | | |
| | Pool Name | Utilization | | | | Type | Capacity |
| | | Current | 10 Days Ago | 20 Days Ago | 30 Days Ago | | |
| ✓ | VSAN_pool1 | 30.01% → | 29.00% | 27.01% | 24.69% | VMware Virtual SAN | 53.81TB |

Point

- Since the information displayed on the GUI might be old, make sure to refresh it when checking the status of the virtual resources.

The refresh process is registered in ISM tasks.

If the displayed information remains old, check if the task of task type of "Refresh Virtual Resource" on the "Tasks" screen on ISM GUI is "Completed."

| Status | Progress | Result | Task ID | Task Type | Operator | Start Time | Completion Time |
|-----------|----------|---------|---------|--------------------------|---------------|------------------------|------------------------|
| Completed | 1 / 1 | Success | 1 | Refresh Virtual Resource | administrator | May 9, 2017 1:32:46 AM | May 9, 2017 1:32:50 AM |

- The virtual resource information is periodically and automatically refreshed as follows (Tasks are not displayed).
 - All virtual resource information is automatically refreshed every day at 0:00.
 - The virtual resource statuses are automatically refreshed every three minutes.

2.2.9 Virtual IO Management

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

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

Point

It is required that the virtual MAC address and virtual WWN address is unique across all nodes managed by ISM as well as in the node group. Because of this, profiles where virtual IO such as virtual MAC address and virtual WWN address has been set cannot be applied to multiple nodes.

MAC address and WWN virtualization

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

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

Figure 2.11 Replacing a managed server that used the Virtual IO Management Functions

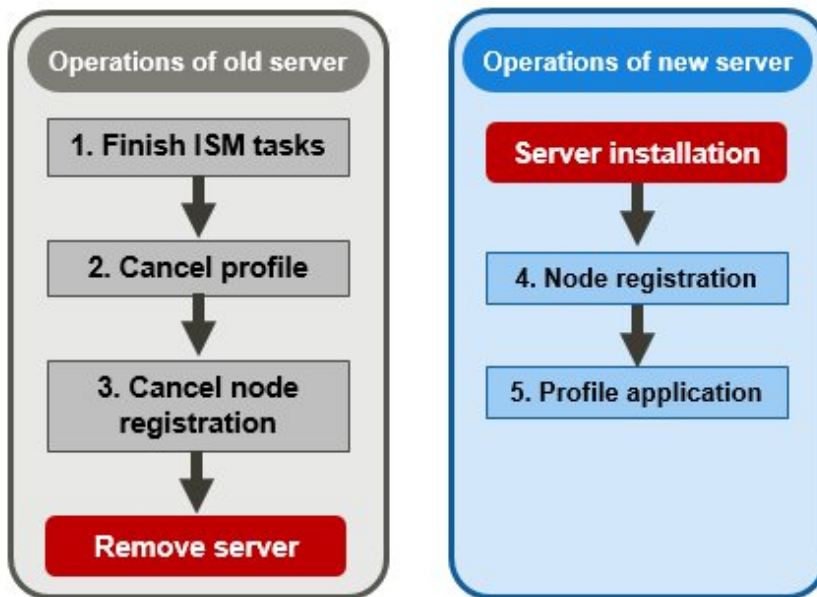
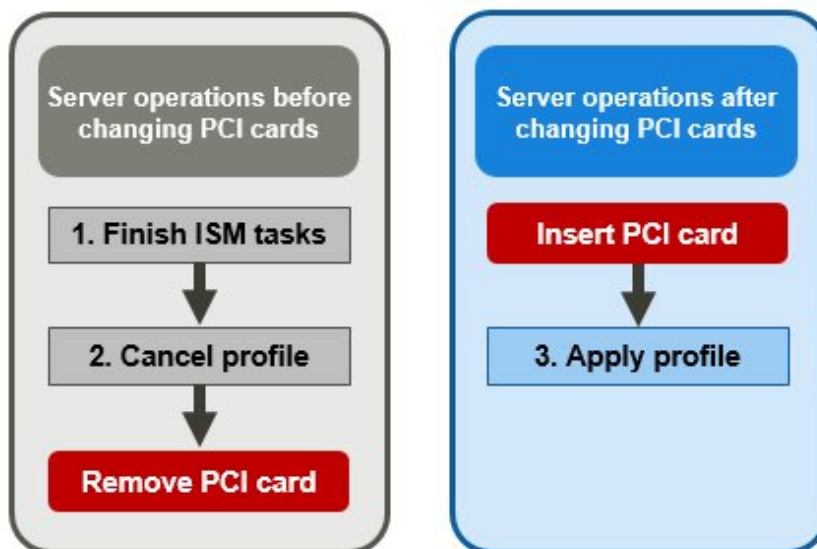


Figure 2.12 Replacing a PCI card that used the Virtual IO Management Function



2.3 Functions of ISM Operating Platform

This section describes the User Management, Repository Management, Task Management, and ISM-VA Management functions in ISM. It describes the following functions.

- [2.3.1 User Management](#)
- [2.3.2 Repository Management](#)
- [2.3.3 Installing Emulex OneCommand Manager CLI and Qlogic QConvergeConsole CLI](#)
- [2.3.4 Task Management](#)
- [2.3.5 ISM-VA Management](#)
- [2.3.6 Management of Cloud Management Software](#)

2.3.1 User Management

ISM users are managed as follows.

- A unique login name and password is assigned to each user.
- Depending on the privileges called "user roles", access methods to nodes and execution of the various functions are restricted.
- By grouping users (hereafter referred to as "user groups"), you can restrict the scope of access to each function separately for each user group.
- By grouping nodes (hereafter referred to as "node groups") and correlating them with user groups, you can restrict the range of nodes that can be accessed by users.

The relationships between user groups and node groups are shown in "[Figure 2.13 Relationships between user groups, node groups, and roles.](#)"

Here, the following points are described:

- [Types of user groups and access scope of users belonging to each group](#)
- [Types of user roles and operations executable by users having these roles](#)
- [Security Policy Settings](#)
- [Creating required users after initial setup of ISM](#)
- [Operations under User Management](#)
- [2.3.1.1 Managing ISM Users](#)
- [2.3.1.2 Managing User Groups](#)
- [2.3.1.3 Operating in Link with Microsoft Active Directory or LDAP](#)
- [2.3.1.4 Managing node groups](#)

Types of user groups and access scope of users belonging to each group

You can define the access scope of users belonging to a user group by correlating user groups with node groups.

| User group name | Access scope |
|--------------------------------|--|
| Administrator group | The administrator group has access to all nodes and node-related resources (such as logs). This user group serves the overall management of ISM. |
| Other than Administrator group | Groups other than the administrator group have access to only those nodes and node-related resources (such as logs) that are within the node groups with which their own user group is correlated. |

Types of user roles and operations executable by users having these roles


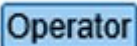
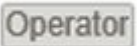



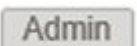




The types of operation that can be executed by users on nodes within their access scope are defined by their user roles as follows.

| User role | Type of access |
|---------------|---|
| Administrator | Administrators can add, modify, delete, and view nodes, users, and all kinds of settings. |
| Operator | Operators can modify and view nodes and all kinds of settings. They are not able to manage users. |
| Monitor | 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, see the contents (indicated by icons) on the various functions that are provided in this manual. For information on the icon indications, see the description below.
- In the description below, users belonging to the Administrator group and carrying administrator roles will be described as "ISM Administrator."

In order to describe the access rights of users, the User Group to which a user belongs and the User Type according to the User Role they hold is indicated by the following icons.

| User Group to which user belongs | User Role held by user | Can execute | Cannot execute |
|----------------------------------|------------------------|---|--|
| Administrator group | Administrator role |  | |
| | Operator role |  |  |
| | Monitor role |  |  |
| Other than Administrator group | Administrator role |  |  |
| | Operator role |  |  |
| | Monitor role |  |  |

The affiliations of users who can execute operations are indicated as follows.

Example:



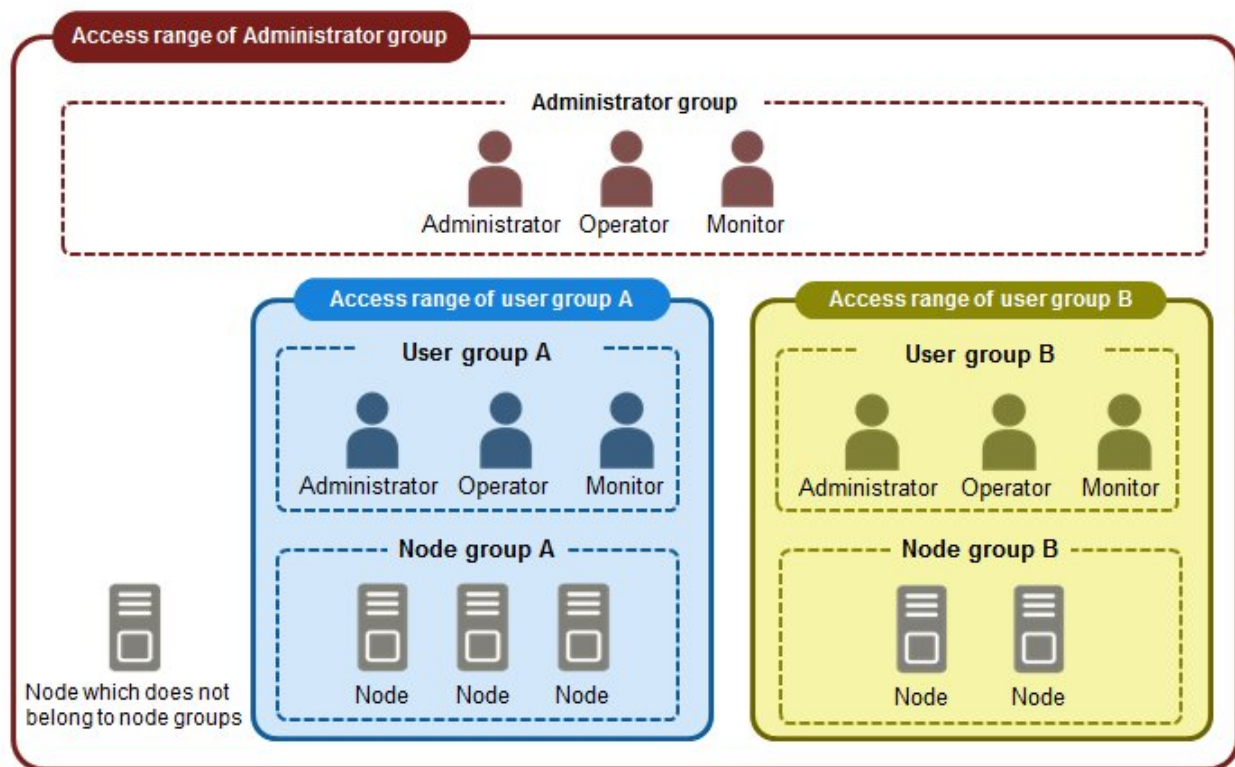
- When the display is as shown above, users with the following user affiliations can execute operations:
 - Users who belong to an Administrator group and have an Administrator or Operator role
 - Users who belong to a group other than an Administrator group and have an Administrator or Operator role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

Note

Users who belong to an Administrator group and have an Administrator role are special users (ISM administrator) who can manage ISM in its entirety.

Users who belong to an Administrator group and have an Operator or Monitor role merely have different access scope, but otherwise the operations they can execute are the same as for users who have an Operator or Monitor role in a non-Administrator group.

Figure 2.13 Relationships between user groups, node groups, and roles



Security Policy Settings

You can set passwords handled in user management and log in restrictions.

You can set one security policy for the entire ISM. Safer operations become possible by setting a firm security policy. The setting items are described below.

User password policy

| Item | Parameter | Operations after settings |
|--|---|---|
| Use former passwords | <ul style="list-style-type: none"> - Possible to use (Recommended) - Use of n times former passwords is not allowed (1 ≤ n ≤ 24) | It is confirmed when setting a password in the add/edit user screen. |
| Password length | 1 - 32 (byte) (Recommended: 8 (bytes)) | |
| Type of characters used | <ul style="list-style-type: none"> - Do not limit (Recommended) - Use at least n types of letters from numbers, small letters, capital letters and special characters (2 ≤ n ≤ 4) | |
| A password that is the same as the user name | <ul style="list-style-type: none"> - Allowed - Not allowed (Recommended) | |
| Example of forbidden character strings [Note1] | Up to a maximum of 256 can be specified | |
| Expires | <ul style="list-style-type: none"> - Indefinite | If logging in with another setting than "Indefinite", execute the following operations. |

| Item | Parameter | Operations after settings |
|-------------------------|--|--|
| | <ul style="list-style-type: none"> - 1 - 365 (days) (Recommended: 90 (days)) | <ul style="list-style-type: none"> - When the expiration date is reached The next action after expiration is executed. - When the expiration date has reached two weeks 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"> - Only warning messages are output - Lock log-in indefinitely (Recommended) | |

[Note1]: Set a password that cannot be used. Passwords that match the set character string are forbidden.

Remark) If you select the [Default] button the recommended values in the chart above will be set.



Note

- The things to be careful about for already created users, when updating ISM 2.1 from a patch earlier than the ISM V2.0.0.d patch are displayed below.
 - When you applied the patch, the expiration date for the passwords will be calculated from the time of the update.
 - The user password policy is set as follows.
 - Password length: 1 (byte)
 - Characters that can be used: No restrictions
 - Passwords that are the same as the user name: Permitted
 - Expiration: Indefinite
 - Action after expiration: Only warning messages are output
- The precautions for when the password expiration date is set to other than "Indefinite" and the action after expiration is set to "Lock log-in indefinitely" are shown below.
 - The log in restrictions are limited to ISM log in. Note that log in is not restricted for FTP and ISM-VA.
 - The first log in to ISM succeeds after the password expiry date has passed. Change the password at this time. If the password is not changed the log in will be locked indefinitely.
 - When log-in has been locked indefinitely, if the password is reset by the ISM administrator the lock is removed.
 - The ISM administrator cannot be locked-out indefinitely. Only warning messages are output.

Log in policy

| Item | Parameter | Description |
|---------------------------------|---|--|
| Session termination time | 2 - 60 (minutes) (Default: 30 minutes) | The time after which the session will time out if there is no activity. |
| Value that should not be locked | 6 - 256 (times) (Default 6 times) | The threshold number of consecutive failed logins after which log in will be temporarily prohibited. |
| Lock time | 1 - 1440 (minutes) (Default: 30 minutes) | The time of temporary log in prohibition after consecutive failed log ins. |

Note

- The number of consecutive failed log-ins will be reset in the following circumstances.
 - If log in succeeded
 - If the lock-out time since the last failed log in has passed.
- The lock-out time is the time threshold after the initial lock-out.

Creating required users after initial setup of ISM

Point

In the default settings of ISM, only users with an [Administrator Role] in [Administrator Groups] are registered.

| User Name | Password | User Group affiliation | User role | Usage |
|---------------|--------------|------------------------|---------------|---------------------------|
| administrator | admin [Note] | Administrator group | Administrator | Overall management of ISM |

[Note]: Change the password before operation.

Use the above user role as an administrator to create the required users.

The procedure is as follows:

1. Log in to ISM as a user who belongs to an Administrator group and has an Administrator role.
2. Create one or more node groups.
See "[2.3.1.4 Managing node groups](#)" in "[Adding node groups](#)" for details.
3. Register the nodes that belong to each node group. (You can also register more nodes later.)
See "[2.3.1.4 Managing node groups](#)" in "[Editing node groups](#)" for details.
4. Create one or more user groups.
See "[2.3.1.2 Managing User Groups](#)" in "[Adding user groups](#)" for details.
5. Create correlations between user groups and node groups as required.
See "[2.3.1.2 Managing User Groups](#)" in "[Editing user groups](#)" for details.
6. Register the users that belong to each user group.
See "[2.3.1.1 Managing ISM Users](#)" in "[Adding users](#)" for details.

Operations under User Management

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

- Managing ISM users
- Managing user groups
- Authenticating ISM users
- Operating in link with Microsoft Active Directory or LDAP
- Managing node groups

The objects of operation in User Management vary with the operating user.

| Operating user | Object of operation |
|---|---|
| Users who belong to an Administrator group and have an Administrator role | Operations can be made for all existing user groups. |
| Users who belong to groups other than Administrator groups and have an Administrator role | Operations can be made only for the user group to which the operating user belongs. |

2.3.1.1 Managing ISM Users

The following three types of user management are available:

- [Adding users](#)
- [Editing users](#)
- [Deleting users](#)

Adding users

Newly add any users by the following method:

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

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

- User Name
Specify a user name that is unique across the entire ISM system.
- Password
- User role
For user roles, see "[Types of user roles and operations executable by users having these roles.](#)"
- Description
Freely enter a description of the user (comment) as required.
- Language
Specify either Japanese or English. If you do not specify the language, English is used.
- Date Format
- Time Zone
- Select the user group.

Editing users

Modify the user information by the following method.

1. From the Global Navigation Menu on the GUI of ISM, select [Settings] - [Users] and in the tree on the left side select [Users].
2. Execute one of the following.
 - Select the checkbox for the user you want to edit, then select the [Actions] button and select [Edit].

- Select the name of the user you want to edit and, when the information screen is displayed, select the [Actions] button and select [Edit].

The information that can be modified is as follows.

| User information | Administrator group | | Group other than administrator group | |
|------------------|---------------------|-------------------------------|--------------------------------------|-------------------------------|
| | Administrator role | Operator role Monitor role | Administrator role | Operator role Monitor role |
| User Name | Y | Y | Y | Y |
| Password | Y | Y | Y | Y |
| User role | Y | N | Y | N |
| Description | Y | N | Y | N |
| Language | Y | Y | Y | Y |
| Date Format | Y | Y | Y | Y |
| Time Zone | Y | Y | Y | Y |
| User Group | Y | N | N | N |

Y: Changeable; N: Not changeable



Note

- If the current password is set it will not be recognized as updated, therefore it is required to be careful when settings the password expiration date.
- If your system works in link with LDAP, changing any passwords does not change the passwords on the LDAP server.

Deleting users



Delete any users as required by the following method.

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

2.3.1.2 Managing User Groups

The following types of user group management are available:

- [Adding user groups](#)
- [Editing user groups](#)
- [Deleting user groups](#)

Adding user groups

Executable user

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

ISM administrators can newly add user groups by the following method:

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

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

- User group name

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

- Authentication Method

Specify one of the following methods for authenticating users who belong to the user group:

- ISM authentication
- Authentication in link with Microsoft Active Directory or LDAP

- Description

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

- Directory size

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

| Usage | Size Restriction | Threshold Monitoring |
|-------------------|--|---|
| Across user group | <p>Specify the total size of the files used by the user group to [Maximum Size] in units of MB.</p> <p>The total size of the files is the total of the following files.</p> <ul style="list-style-type: none"> - Repository - Archived logs - Node logs - Files handled by ISM-VA in FTP <p>If the actual usage size exceeds the specified [Maximum Size], an error message is exported to the Operation Log. Even when the [Maximum Size] value is exceeded, this does not affect the operations of Repository, Archived Log, and Node Log.</p> | <p>Specify the threshold value exporting an alert message to the Operation Log to [Warning threshold] in units of %.</p> <p>A warning message is exported to the Operation Log.</p> |
| Repository | <p>Specify the total size of the files imported to Repository to [Maximum Size] in units of MB.</p> <p>If the total usage size of the imported files exceeds the value of the specified [Maximum Size], the currently executed import to the Repository results in error and an error message is exported to the Operation Log.</p> | You cannot specify the value. |
| Archived logs | <p>Specify the total size of Archived Log to [Maximum Size] in units of MB.</p> <p>If the total size of the Archived Log exceeds the specified [Maximum Size], newly created logs are not stored in Archived Log and an error message is exported to the Operation Log.</p> | <p>Specify the threshold value exporting an alert message to the Operation Log to [Warning threshold] in units of %.</p> <p>A warning message is exported to the Operation Log.</p> |

| Usage | Size Restriction | Threshold Monitoring |
|-----------|--|---|
| | <p>Note that if [Maximum Size] is set to the [0] default value, the occurred logs will not be archived and every time an error message will be exported to the Operation Log.</p> <p>The logs stored before exceeding the [Maximum Size] remains stored.</p> | |
| Node logs | <p>You can specify the total size of download data and log search data to [Maximum Size] in units of MB.</p> <p>The log search data can only be specified to the Administrator user group.</p> <p>If either of the total size of download data or the log search data exceeds the value specified in [Maximum Size], neither download data nor log search data are exported and an error message will be exported to the Operation Log.</p> <p>If the [Maximum Size] of either download data, log search data or both is set to the default [0], neither data will be exported nor an error message will be exported to the Operation Log.</p> | <p>You can specify the threshold value that exports an alert message to the size of download data and the size of log search data, to [Warning threshold] in units of %.</p> <p>A warning message is exported to the Operation Log.</p> |

For information on how to estimate the total size of files imported to Repository, the size of Archived Log, and the size of Node Log (data for downloads, log search data), see "[3.2.1 Estimation of Disk Resources](#)."

- Node group

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



Note

- Only one node group can be correlated with a user group.
- Every user who belongs to the user group can carry out operations only on the nodes belonging to the node group that is correlated with that user group. They cannot access any nodes in node groups that are not correlated with their user group.
- Soon after creating a user group, execute the operations in "[3.7.2 Allocation of Virtual Disks to User Groups](#)."

Editing user groups



Edit the user group information by the following method.

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

The information that can be edited is as follows.

- User group name
- Authentication Method
- Description

- Directory size

For the edited contents, see "Directory size" in "[Adding user groups.](#)"

- Node group

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



Note

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

Newly linking another node group to a user group to which a node group is already linked disables the correlation with the older node group.

Deleting user groups



Delete any user groups as required by the following method.

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



Note

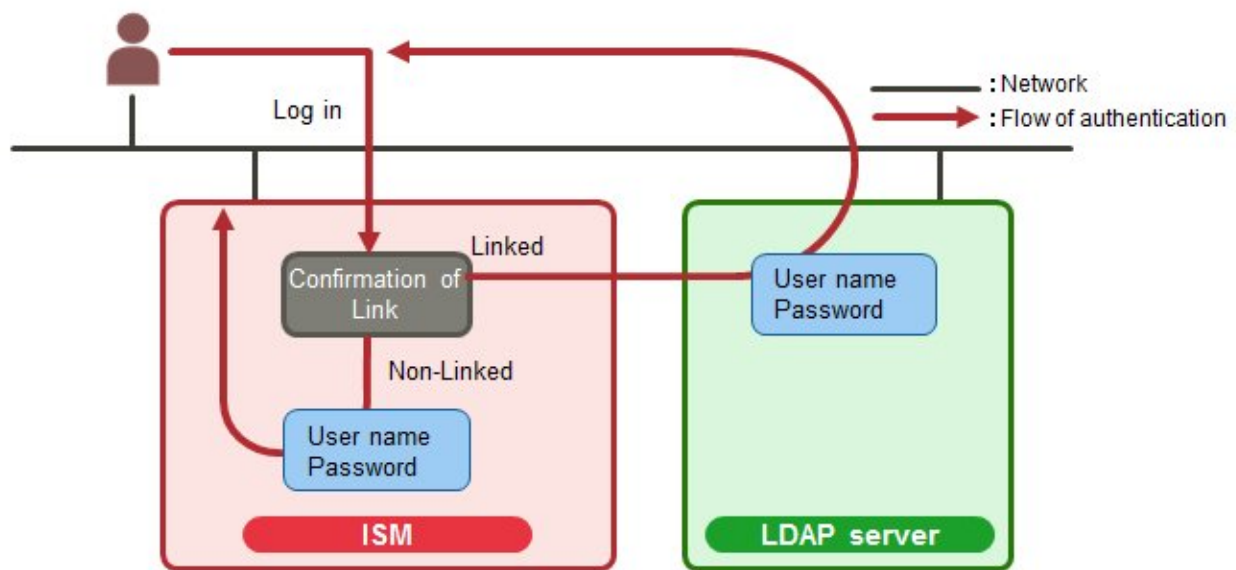
- You cannot delete Administrator groups.
- You cannot delete user groups that have members.
Before you delete a user group, delete all users who belong to the user group, or change the affiliations of all users to other user groups.
- Even if you delete user groups that are correlated with node groups,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

2.3.1.3 Operating in Link with Microsoft Active Directory or LDAP

By linking ISM with Microsoft Active Directory or LDAP, you can integrate the management of users and passwords of multiple services.

The following diagram gives an overview of a linked configuration.

Figure 2.14 Image of ISM in link with LDAP



1. Log in as a user.

- If the user is an object of linked operation:

Authentication is carried out by LDAP (or Microsoft Active Directory, respectively).

- If the user is not an object of linked operation:

Authentication is carried out by ISM.

To enable operations in link with Microsoft Active Directory or LDAP, follow the procedure below.

Setup procedure

1. Register users for operation in link with Microsoft Active Directory or LDAP (hereafter referred to as "directory servers") on these directory servers.
2. Log in to ISM as a user who belongs to an Administrator group and has an Administrator role.
3. If the settings contain no information on the directory server, set up the following information in the LDAP server settings of ISM.
For information on the setting contents, ask the administrator of the directory server about the setting contents you registered in Step 1.

| Item | Setting contents |
|------------------|--|
| LDAP Server Name | Specify the name of the directory server. Specify one of the following: <ul style="list-style-type: none"> - URL or IP address - ldap://<url> or ldap://<IP address> - ldaps://<url> or ldaps://<IP address> |
| Port Number | Specify the port number of the directory server. |
| Base DN | Specify the base DN for searching accounts. This information depends on the registered contents on the directory server. Example: <ul style="list-style-type: none"> - For LDAP: ou=Users,ou=system - For Microsoft Active Directory: DC=company,DC=com |
| Search Attribute | Specify the account attribute for searching accounts. Specify one of the following fixed character strings: |

| Item | Setting contents |
|--------------------|---|
| | <ul style="list-style-type: none"> - For LDAP: uid - For Microsoft Active Directory: sAMAccountName |
| Bind DN | <p>Specify the accounts that can be searched on the directory server. This information depends on the registered contents on the directory server.</p> <p>Example:</p> <ul style="list-style-type: none"> - For LDAP: uid=ldap_search,ou=system - For Microsoft Active Directory: CN=ldap_search,OU=user_group,DC=company,DC=com <p>"anonymous" is not supported.</p> |
| Password | Specify the password for the account you specified under Bind DN. |
| SSL Authentication | If you want to use SSL for the connection to the directory server, set up SSL authentication. |

4. Prepare the user groups for which you set Microsoft Active Directory or LDAP as the authentication method.
5. From the Global Navigation Menu on the GUI of ISM, select [Settings] - [Users] and in the tree on the left side select [Users] and add the user registered in Step 1.

The information to be registered is as follows.

| Item | Setting contents |
|-----------------|--|
| User Name | Specify the names of the users you registered in Step 1. |
| Password | <p>For situations when operation in link is disabled, specify a password different from that in Step 1.</p> <p>Note that the password you specify here is also used when you log in via FTP.</p> |
| User role | Specify the user role in ISM. |
| Description | Freely specify any values as required. |
| Language | Specify the language that is used by the user to be added. |
| Date Format | Specify the date format that is used by the user to be added. |
| Time Zone | Specify the time zone that is used by the user to be added. |
| User group name | Specify the name of the user group you prepared in Step 4. |

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

If they cannot log in, go back to Step 3.



Note

- The administrator user cannot operate in link with Microsoft Active Directory or LDAP.
- It is required to set up a DNS server in ISM in advance if setting FQDN name as LDAP server name.
- If you cannot connect to the directory server with the content specified in [Settings] - [Users] - [LDAP Server Setting], an error will occur in the directory server information and setting will not be possible.
- A primary and two secondary servers can be specified. If two servers are specified, if the currently used server cannot respond, the other server will be used.
- The following are the precautions for setting up a SSL certificate.
 - For the SSL certificate, set it after uploading it to the Administrator\ftp directory in FTP in advance.
 - After setup, delete the uploaded SSL certificate, since it is no longer required.
 - Specify the URL in the SSL certificate for the LDAP server name.

- The following are the precautions if you want to use SSL for the connection to the directory server.
 - Specify the LDAP user name from ldaps://.
 - For the port number, specify the port number for SSL transfer (for example 636).
 - Set the SSL certificate.

Setting Release Procedure

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

- Changing users
Change the user group to which the relevant user belongs to a user group that is not linked. Edit the user information to make this change.
- Changing user groups
Edit the user group to change the authentication method to "ISM Authentication."

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

2.3.1.4 Managing node groups

The following types of node group management are available:

- [Adding node groups](#)
- [Editing node groups](#)
- [Deleting node groups](#)

Adding node groups



ISM administrators can newly add node groups by the following method:

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

Or

1. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Node Groups].
2. Select the [+] button on the node group list screen.

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

- Node Group Name
Specify a user name that is unique across the entire ISM system.
- Selection of Nodes to be Assigned
Select multiple nodes for which the node group affiliation is [Unassigned].
Note that, if you do not assign any nodes here, you can also assign them at a later stage by editing the node group.



Note

Each node can belong to only one node group.

Editing node groups



ISM administrators can edit node groups by the following method:

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

Or

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

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

- Node Group Name
Specify a user name that is unique across the entire ISM system.
- Selection of Nodes to be Newly Assigned
Select multiple nodes for which the node group affiliation is [Unassigned].

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

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

Deleting node groups



ISM administrators can delete node groups by the following method:

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

Or

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

Note

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

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

2.3.2 Repository Management

The repository is a location used by ISM to store various kinds of resources. The resources are related to the user groups. The repository is mainly used for the following purposes:

- Storing of firmware data as well as the ServerView Suite Update DVD that are used for firmware updates
These are used by the "[Firmware Management](#)" function.
- Storing of OS installation media that are used for installing OSes
These are used by the "[Profile Management](#)" function.
- Storing of ServerView Suite DVD data that are used for installing OSes and Offline Update
These are used by the "[Profile Management](#)" and "[Firmware Management](#)" functions.

Note

If the disk area in a repository is not enough, this results in a failure to store the various data for repository management. Refer to the following and allocate a sufficiently large disk area to the repository.

- [3.2.1.2 Estimation of Required Capacities for Repositories](#)
- [3.7 Allocation of Virtual Disks](#)
- [2.3.1.2 Managing User Groups](#)

Storing firmware data



The following two methods are available for storing firmware data to be applied on managed nodes in the repository:

- Importing ISO image files of the firmware data that are provided on DVD into the repository
- Importing the firmware data that are published on the FUJITSU website for each node into the repository

The firmware data to be used vary with the type of managed node. Prepare the data shown in the following table. If the data are in DVD format, prepare the respective ISO image files.

| Managed node | Target firmware | Firmware data to be used |
|--------------|--|---|
| Server | BIOS of PRIMERGY unit iRMC of PRIMERGY unit | <ul style="list-style-type: none"> - Online Update BIOS/iRMC data as published on the FUJITSU PRIMERGY website - Offline Update |

| Managed node | Target firmware | Firmware data to be used |
|----------------|--------------------------------|--|
| | | ServerView Suite Update DVD or BIOS/iRMC data as published on the FUJITSU PRIMERGY website |
| | Cards mounted in PRIMERGY unit | ServerView Suite Update DVD or Firmware data as published on the FUJITSU PRIMERGY website |
| | Firmware of PRIMEQUEST unit | Firmware data as published on FUJITSU website |
| Network switch | Basic software | Firmware data as published on FUJITSU website |
| Storage | Controller | |

Locations for obtaining firmware data images

Download the firmware data for each respective model from the following websites.

| Target firmware | Firmware Type (sort) | Location from which to obtain |
|----------------------------------|-------------------------|--|
| iRMC of PRIMERGY unit | iRMC | http://support.ts.fujitsu.com/ [Note1] http://support.ts.fujitsu.com/globalflash/ManagementController/ |
| BIOS of PRIMERGY unit | BIOS | http://support.ts.fujitsu.com/ [Note1] http://support.ts.fujitsu.com/globalflash/SystemBoard/ |
| Cards mounted in PRIMERGY unit | FC | http://support.ts.fujitsu.com/globalflash/FibreChannelController/ |
| | CNA | http://support.ts.fujitsu.com/globalflash/LanController/ |
| PRIMEQUEST unit | Firmware of the server | http://support.ts.fujitsu.com/ [Note1] |
| Network Switch Basic software | LAN Switch (SR-X model) | http://support.ts.fujitsu.com/ |
| | LAN Switch (VDX model) | http://support.ts.fujitsu.com/ |
| Storage Controller | ETERNUS DX/AF | http://support.ts.fujitsu.com/ |

[Note1]: Download Flash File

Location from which to obtain ServerView Suite Update DVD images

ServerView Update DVD is available for downloading at the following site:

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



Note

Out of the firmware data included on the Update DVD, you can only use firmware types FC and CNA for Online Update.

The following is a sample operation.

1. Use FTP to forward the firmware data you prepared to ISM-VA. Forward the folder in which you deployed the ISO images or compressed ZIP files of the firmware data to the management server.

For how to forward FTP, see "2.1.2 FTP Access."

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

4. Execute one of the following.

- For storing the firmware data in the repository from DVD, select the [Actions] button on the [Import Data List] tab and select [Import DVD].
- For storing the firmware data downloaded from the FUJITSU website in the repository, select the [Actions] button on the [Import Data List] tab and select [Import Firmware].

5. Execute the operations according to the instructions on the screen.

Importing to the repository may take some time to complete. After starting the import, the task is registered as a "Task" in ISM. Confirm the current status of the task on the "Task" screen.

When selecting [Tasks] from the top of the Global Navigation Menu on the GUI of ISM, the Task List is displayed.

Point

The files you deployed on the FTP server of ISM are no longer required after the import has finished. Use an FTP command to delete them.

Deleting firmware data from repository

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

The following is a sample operation using the GUI.

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Firmware].
2. From the menu on the left side of the screen, select [Import].
3. Execute one of the following.
 - If firmware data was stored in repository from DVD:
 - a. Select [Import Data List] tab.
 - b. Select the checkboxes for the data to be deleted, then select the [Actions] button and select [Delete].
 - c. Execute the operations according to the instructions on the screen.
 - If firmware data downloaded from the FUJITSU website was stored in repository:
 - a. Select [Firmware Data] tab.
 - b. Select the checkboxes for the data to be deleted, then select the [Actions] button and select [Delete].
 - c. Execute the operations according to the instructions on the screen.

Importing firmware data

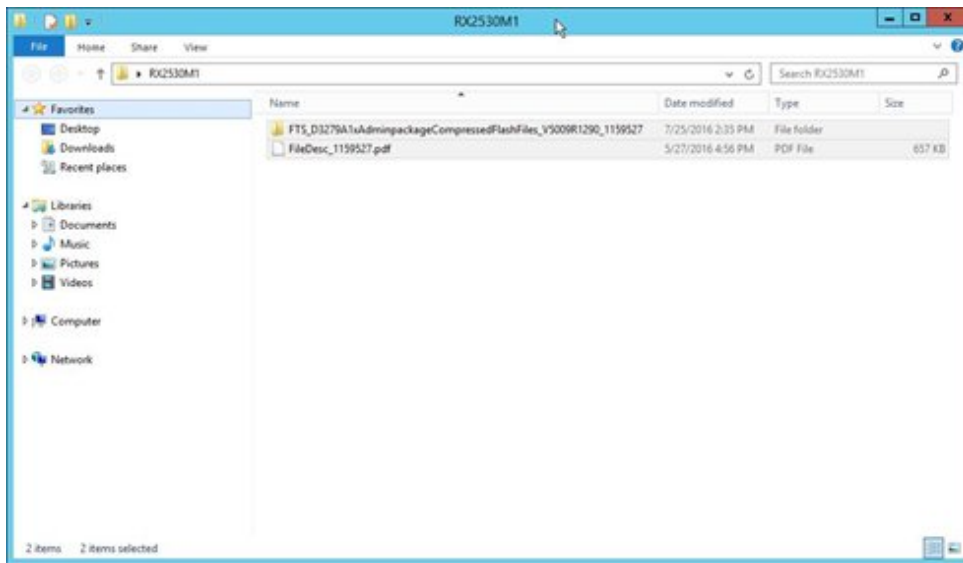
| | Administrator group | Other groups |
|-----------------|-----------------------------------|-----------------------------------|
| Executable user | <div>Admin Operator Monitor</div> | <div>Admin Operator Monitor</div> |

Below example shows the operations for importing firmware data by an administrator user who belongs to an Administrator group.

1. Get a firmware data from a location for obtaining firmware data.

2. If you are not going to use an ISO image file, you can store the downloaded file in any folder that suits you best.

If the downloaded file is a compressed file, decompress it within the folder.



3. Use FTP to forward the data to ISM-VA.

- Use FTP commands or FTP client software (such as FFFTP or WinSCP) to forward the data. In that case, set the character encoding to convert to UTF-8. Do not use Windows Explorer, as it cannot correctly handle the character encoding.
- After logging in to ISM-VA with the FTP client software, move from the root directory to the "<user group name>/ftp" directory and forward the data into this directory.
- If you are not going to use an ISO image file, be sure to forward it without changing the folder structure.

4. Import the firmware data.

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

- b. From the menu on the left side of the screen, select [Import].

- c. Execute one of the following.

- For importing an ISO image file into the repository, select the [Actions] button under [Import Data List] tab and select [Import DVD].

Following the on-screen instructions, select the file location and the media type, and then select [Apply].

- For importing firmware data other than ISO image file into the repository, select the [Actions] button under [Import Data List] tab and select [Import Firmware].

Following the on-screen instructions, enter the file location, type, model, and version, and then select [Apply].

Enter the version according to the following table.

| Type | Model | Version |
|------------|--|--------------------------------------|
| iRMC | RX100 S8, CX2550 M1 etc. | iRMC and SDR versions [Note1] |
| BIOS | RX100 S8, CX2550 M1 etc. | BIOS version [Note1] |
| PRIMEQUEST | PRIMEQUEST 2400S3 etc. | Version of the unit firmware [Note1] |
| FC | LPe1250, LPe12002 | BIOS and FW versions [Note2] |
| | LPeXXX except for LPe1250 and LPe12002 | Firmware version [Note2] |
| | QLEXXX | BIOS version [Note2] |
| CNA | Oce10102 etc. | Firmware version [Note1] |

| Type | Model | Version |
|---------------|---------------------|-----------------------------------|
| LAN Switch | SR-X model | Version of basic software [Note1] |
| | VDX model | Firmware version [Note1] |
| ETERNUS DX/AF | ETERNUS DX/AF model | Firmware version [Note1] |

[Note1]: For information on the version, see the release notes.

[Note2]: For information on the version, see the release notes or the file name.

Importing to the repository may take some time to complete. After starting the import, the task is registered as a "Task" in ISM. Confirm the current status of the task on the "Task" screen.

When selecting [Tasks] from the top of the Global Navigation Menu on the GUI of ISM, the Task List is displayed.

Point

- The files you deployed on the FTP server of ISM are no longer required after the import has finished. Use an FTP command to delete them.
- If you are using FTP client software for forwarding the files, set the character encoding to convert to UTF-8. If the character encoding is not correctly converted, the files cause garbled text in ISM-VA, which may result in the import not being executed correctly. If the import is not carried out correctly or the imported documents are not displayed, delete the already imported firmware data and the files you forwarded via FTP to ISM-VA, and then review the settings for conversion of character encoding before you retry the import.

Storing OS installation files

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 |

As Profile Management uses the OS installation media you imported to the repository for installing OSes, the OS installation media are not directly used after the import.

To import the data, execute the following procedure.

1. Prepare an ISO image of the OS installation media. For ESXi, prepare a FUJITSU custom image.
2. After logging in to ISM-VA over FTP, forward the ISO image you prepared into the "./<user group name>/ftp" directory.
For FTP connection and how to forward FTP, see "[2.1.2 FTP Access](#)."
3. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Firmware].
4. From the menu on the left side of the screen, select [Import].
5. Select the [ServerView Suite] tab, then select the [Actions] button - select [Import DVD].
6. Select the appropriate OS type under [Media Type], specify the ISO file you transferred over FTP, and then execute the import.

Point

The files you deployed on the FTP server of ISM are no longer required after the import has finished. Use an FTP command to delete them.

Deleting OS installation files from repository

Executable user

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

The procedure for deletion is as follows:

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Firmware].
2. From the menu on the left side of the screen, select [Import].
3. Select the [ServerView Suite] tab.
4. Select the checkboxes for the target to be deleted, then select the [Actions] button and select [Delete].
5. Execute the operations according to the instructions on the screen.

Storing of ServerView Suite DVD



When Profile Management installs an OS, it retrieves the programs for controlling the target node as well as the driver, application, and other files to be installed on the target node from the ServerView Suite DVD.

Import the ServerView Suite DVD that supports the target node and the OS to be installed in advance.

To import the data, execute the following procedure:

1. Prepare an ISO image of "ServerView Suite DVD."
2. After logging in to ISM-VA over FTP, forward the ISO image you prepared into the "`./<user group name>/ftp`" directory.
For FTP connection and how to forward FTP, see "[2.1.2 FTP Access](#)."
3. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Firmware].
4. From the menu on the left side of the screen, select [Import].
5. Select the [ServerView Suite] tab, then select the [Actions] button - select [Import DVD].
6. Select [ServerView Suite DVD] under [Media Type], specify the ISO file you transferred over FTP, and then execute the import.

Point

The files you deployed on the FTP server of ISM are no longer required after the import has finished. Use an FTP command to delete them.

Deleting ServerView Suite DVD data from repository



The procedure for deletion is as follows:

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Firmware].
2. From the menu on the left side of the screen, select [Import].
3. Select the [ServerView Suite] tab.
4. Select the checkboxes for the target to be deleted, then select the [Actions] button and select [Delete].
5. Execute the operations according to the instructions on the screen.

2.3.3 Installing Emulex OneCommand Manager CLI and Qlogic QConvergeConsole CLI



Note

- For executing a firmware update of a PCI card on Linux, the Emulex OneCommand Manager CLI or the QLogic QConvergeConsole CLI must be installed in the OS of the target server, and the PCI card information must be retrievable. For information on how to install and operate these CLIs, refer to the manuals for Emulex One Command Manager CLI and for QLogic QConvergeConsole CLI.

For PCI cards that require installation of Emulex OneCommand Manager CLI and QLogic QConvergeConsole CLI, access your local support.

- 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, access your local support.

2.3.4 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.

Likewise, you have to use the "Task" screen to abort (cancel) any ongoing processing.

On the "Task" screen, you can view processing of the tasks shown in the following table.

| Function | Type of processing |
|--------------------------------------|--|
| Firmware Management | Import of firmware data Firmware update |
| Profile Management | Import of OS installation media Assignment of profiles Reassignment of profiles Release of profiles |
| Log Management | Collect Logs Delete Logs Create Download File |
| Network Management | Changing VLAN Settings |
| Virtual Resource Management Function | Updating for Virtual Resource Information |

Method for displaying "Tasks" screen

Executable user

| | |
|---|---|
| Administrator group | Other groups |
| <input type="text" value="Admin"/> <input type="text" value="Operator"/> <input type="text" value="Monitor"/> | <input type="text" value="Admin"/> <input type="text" value="Operator"/> <input type="text" value="Monitor"/> |

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

2.3.5 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 "[2.3.5.1 List of Commands in ISM-VA Management](#)."

Functions for use when installing ISM

| Function name | Overview of Function |
|------------------------|---|
| Initial Setup | This function carries out the basic setup from a hypervisor console after installing ISM-VA. <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 over web browsers. |

Functions for use in maintenance

| Function name | Overview of Function |
|------------------------|---|
| ISM-VA Service Control | This function can stop and restart ISM-VA as well as control the services that run internally. |
| General Settings | This function serves to modify the settings for ISM-VA after installation. <ul style="list-style-type: none">- Network Settings- Time settings- Local settings- Virtual disk settings- Modification of Host Names |
| Maintenance | This function serves to carry out all kinds of maintenance. <ul style="list-style-type: none">- Confirmation of versions- Application of Patches- Collection of archived logs- Switching of debug flags |

2.3.5.1 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 |
|----------------------------------|-----------------------|
| Show of network devices | ismadm network device |
| Modification of network settings | ismadm network modify |
| Show of network settings | ismadm network show |

Time settings

| Function | Command |
|---|----------------------------|
| Show of time settings | ismadm time show |
| Show of available time zones | ismadm time list-timezones |
| Setting of time zone | ismadm time set-timezone |
| Setting of date and time | ismadm time set-time |
| Enabling/Disabling of 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 |
|---------------------------|----------------------------|
| Show of locale and keymap | ismadm locale show |
| Show of available locales | ismadm locale list-locales |
| Locale settings | ismadm locale set-locale |
| Show of available keymaps | ismadm locale list-keymaps |
| Setting of keymap | ismadm locale set-keymap |

License Settings

| Function | Command |
|--------------------------|-----------------------|
| Show of list of licenses | ismadm license show |
| License Settings | ismadm license set |
| Deletion of license | ismadm license delete |

Certificate Activation

| Function | Command |
|---------------------------------------|-----------------------|
| Deployment of SSL Server Certificates | ismadm sslcert set |
| Display of SSL Server Certificates | ismadm sslcert show |
| Export of SSL server certificates | ismadm sslcert export |

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 |
| Show of list of internal services | ismadm service show |
| Start of internal service individually | ismadm service start |
| Stop of internal service individually | ismadm service stop |
| Restart of internal service individually | ismadm service restart |
| Show of status of internal service individually | ismadm service status |
| Enabling of internal service individually | ismadm service enable |

| Function | Command |
|--|------------------------|
| Disabling of internal service individually | ismadm service disable |

Virtual disk settings

| Function | Command |
|--|-----------------------------|
| Adding of LVM volume | ismadm volume add |
| Allocation of LVM volume to user group | ismadm volume mount |
| Cancel of allocation of LVM volume to user group | ismadm volume umount |
| Show of volume settings | ismadm volume show |
| Extension of LVM volume size | ismadm volume extend |
| Extension of size of LVM system volume | ismadm volume sysvol-extend |
| Removal of LVM volume | ismadm volume delete |

Maintenance

| Function | Command |
|--------------------------------------|------------------------------|
| Collection of archived logs | ismadm system snap |
| Display of System Information | ismadm system show |
| Application of Patches | ismadm system patch-add |
| Application of Plug-in | ismadm system plugin-add |
| Upgrade of ISM-VA | ismadm system upgrade |
| Modification of Host Names | ismadm system modify |
| Switch of Trouble Investigation Logs | ismadm system set-debug-flag |

Event Notification Settings

| Function | Command |
|---|---------------------|
| Registration certificate for event notification mails / Registration action script | ismadm event import |
| Show certificate for event notification mails / Show action script | ismadm event show |
| Deletion certificate for event notification mails / Deletion action script | 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 |



Note

ISM-VA must be restarted if the time interval settings were returned to a past time.

2.3.6 Management of Cloud Management Software

When you use the functions in link with Cloud Management Software, register Cloud Management Software with ISM.

Registering Cloud Management Software



The following is the operation method for registering new Cloud Management Software.

1. From the Global Navigation Menu on the GUI of ISM, select [Settings] - [General] - [Cloud Management Software].
2. From the [Actions] button, select [Registration].
3. Enter the information that is required for registration.

- Cloud Management Software Name

Set a name that is unique across the entire ISM system.

- IP Address

Set the IP address of the Cloud Management Software.

Register the cluster virtual IP in the case of Microsoft Failover Cluster.

- Type

Select the type of Cloud Management Software to be registered.

Also specify the version of Windows Server in the case of Microsoft Failover Cluster.



Note

.....
If Microsoft Failover Cluster was specified, it is required to set the domain name in [Account Information].
.....

- Account Information

Set the domain name, account name, and password for the Cloud Management Software.

Enter the domain name by using uppercase letters.

- URL

Set the URL for accessing the web management screen for the Cloud Management Software.

If a Cloud Management Software that provides a web management function was specified in [Type], the URL used to access the web management screen must be set.

- User Group

Select the name of the user group to be managed.

4. Select the [Register] button.

The Cloud Management Software registered with Cloud Management Software List screen is displayed.

Retrieving Information from Cloud Management Software



In ISM, information can be retrieved for the virtual machines or virtual switches running on the nodes.

- Virtual Machine Information

The virtual machine information retrieved from the Cloud Management Software can be confirmed on the [Virtual Machines] tab of the Details of Node screen.

- Virtual Switch Information

The virtual switch information retrieved from the Cloud Management Software can be confirmed on the [Network Map] screen.

It can be retrieved if the Cloud Management Software is a VMware vCenter Server or System Center type. Microsoft Failover Cluster is not supported.



Note

ISM manages information for the registered Cloud Management Software, OS information of nodes and information for the virtual machines and virtual switches connected to it. Execute the settings respectively to retrieve virtual machine and virtual switch information.

ISM retrieves virtual machine and virtual switch information in 24 hour cycles. Follow the procedure below to retrieve the information at any time.

1. Retrieve node information for nodes that are managed by the Cloud Management Software.
Execute procedure 2 after the information has been retrieved.
2. From the Global Navigation Menu on the GUI of ISM, select [Settings] - [General] - [Cloud Management Software].
3. Retrieve information using one of the following methods.
 - If retrieving information from all Cloud Management Software, select [Get Cloud Management Software Info] and then select [Run].
 - If limiting the items to be retrieved, select the Cloud Management Software to be retrieved and select [Run] from the [Actions] button - [Get Info].

As soon as retrieval of the information is complete, a log with the Message ID "10021503" is exported to the [Events] - [Events] - [Operation Log]. If there is Cloud Management Software where information could not be retrieved, a log will additionally be exported in [Events] - [Events] - [Operation Log]. Confirm that an error has not been exported, then confirm the information of the virtual machine or virtual switch.



Note

- If registering both System Center and the Microsoft Failover Cluster registered in System Center in ISM, ISM will retrieve information from System Center, but information will not be retrieved from Microsoft Failover Cluster.
- In an environment using Microsoft Failover Cluster, if deleting a virtual machine from the Hyper-V manager, also delete this virtual machine from the failover cluster management role.

Editing Cloud Management Software



The following is the operation method for editing Cloud Management Software information registered with ISM.

1. From the Global Navigation Menu on the GUI of ISM, select [Settings] - [General] - [Cloud Management Software], and then select the target Cloud Management Software on the displayed [Cloud Management Software List] screen.
2. From the [Actions] button, select [Edit].
3. Edit the information.
4. Execute [Registration] to make the contents of the information effective.

Deleting Cloud Management Software



The following is the operation method for deleting Cloud Management Software registered with ISM.

1. From the Global Navigation Menu on the GUI of ISM, select [Settings] - [General] - [Cloud Management Software], and then select the target Cloud Management Software on the displayed [Cloud Management Software List] screen.
2. Select the [Actions] button and select [Delete].
3. Execute [Delete] to delete the Cloud Management Software.

2.4 Operations When Deleting Nodes and When Modifying Groups

When you are going to delete a node or modify a group, perform the operations described below.

2.4.1 When Deleting Nodes

Before you delete a node, complete the operations described below.

- If any tasks are being executed, wait until they have completed.
- Release any profiles assignments you have made.



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

2.4.2 When Modifying or Dissolving Groups

Before you change the affiliation of a node from one node group to another or release a node from a node group, complete the operations described below.

- If any tasks are being executed on the relevant node, wait until they have completed.
- If any profile was applied to the relevant node, release the profile.
- Delete any schedules for log collection from the relevant node.
- Delete any saved logs that were retrieved from the relevant node.
- Delete any alarm settings of the relevant node.



-
- For profiles that were set by users who belong to a user group, these users will no longer be able to view and modify the profile settings. In such a case, the profile has to be deleted by a user belonging to an Administrator group.
 - If you forgot to delete any saved logs, revert the node temporarily to the former user group in order to be able delete the logs.
-

2.4.3 When Deleting User Groups

Before you delete a user group, complete the operations described below.

- Release any profiles assignments you have made.

- Delete all profiles, profile groups, policies, and policy groups that are included in the user group.
- Delete all imported OS media, SVS DVD data from the repository.
- Delete any schedules for log collection.
- Delete any saved logs.



Point

.....

For profiles and log-related operations that were set by users who belong to a user group, these users will no longer be able to view and modify the settings for profiles and log-related operations. In such cases, the settings have to be corrected by a user belonging to an Administrator group.

.....

2.4.4 When Changing User Group Names

Before you change the name of a user group, make sure that none of the following tasks are currently being executed.

- Firmware data import operations
- Firmware update operations

Chapter 3 Installation of ISM

This chapter describes how to install ISM.

3.1 Workflow for Installing ISM

Set up the operating environment for ISM itself.

(1) Installation Design

When you are going to install ISM, you have to perform the following tasks in preparation.

- Estimation of disk resources
- Repository settings
- Network design
- Setting node names
- Setting of Users

For information on the contents of these tasks, see "[3.2 Installation Design for ISM.](#)"

(2) Installation of ISM-VA

Install ISM-VA on a management server.

For information on the installation procedure, see "[3.3 Installation of ISM-VA.](#)"

(3) Setup of ISM-VA Environment

Set up the operating environment in which you installed ISM-VA.

For information on the contents of the environment setup procedure, see "[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, see "[3.5 Registration of Licenses.](#)"

(5) Registration of Users

Register the ISM users.

For information on the tasks required to register users, see "[3.6 Registration of Users.](#)"

(6) Allocation of Virtual Disks

Allocate virtual disks in order to extend the disk capacities of ISM-VA.

See "[3.7 Allocation of Virtual Disks](#)" to allocate virtual disks to the entire ISM-VA and Administrator user groups.



Note

After installation of ISM-VA, immediately perform virtual disk allocation for Administrator groups according to the procedure described in "[3.7.2 Allocation of Virtual Disks to User Groups.](#)"

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 Estimation of Disk Resources](#)

- [3.2.2 Repository Settings](#)
- [3.2.3 Network Design](#)
- [3.2.4 Setting of Node Names](#)
- [3.2.5 Setting of Users](#)

3.2.1 Estimation of Disk Resources

Operation of the following items requires an estimate calculation of disk capacities:

- Logs
- Repository
- Backups

Disk capacities cannot be extended dynamically during the operation of ISM-VA. Therefore, if disk space runs low during operation, this has an effect on the operation of log collection for Log Management as well as of repositories and backups. Consequently, it is important to estimate the disk capacity in advance to make sure it will not run low.

Create a virtual disk with the estimated capacity and allocate it to ISM-VA. For information on how to create and allocate virtual disks, see "[3.7 Allocation of Virtual Disks](#)."

In order to avoid insufficient disk space, you should also design operations to include periodical deletion of repository, backup, and other data that are no longer required.

3.2.1.1 Estimation of Log Storage Capacity

ISM exports logs through the following functions.

- Log Management

The disk capacities for logs exported through Log Management depend on the number of managed nodes and on the period or frequency of log retention. In estimating the capacities, you should also take the possible number of additional node installations in the future into account.

For information on how to estimate disk capacities for logs that are exported by Log Management, access your local support.

- Trouble investigation logs

The log disk space requires to be extended depending on the number of nodes to be managed by ISM-VA.

The following chart shows approximate values for the required disk capacities for various numbers of managed nodes and the corresponding log areas.

| Number of managed nodes | Disk capacity required for log area |
|-------------------------|-------------------------------------|
| 100 nodes | 10 GB (default) |
| 400 nodes | 40 GB |
| 1000 nodes | 100 GB |

The procedure for extending a log area is as follows:

1. Allocate an additional virtual disk.

For details, see "[3.7.1 Allocation of Virtual Disks to Entire ISM-VA](#)."

2. Switch the log level.

For details, see "[4.17 Switch of Levels of Trouble Investigation Logs](#)."

3.2.1.2 Estimation of Required Capacities for Repositories

In order to operate functions such as Profile Management or Firmware Management, it is required to prepare repositories in ISM-VA. In a repository, the following data are stored.

- Firmware data
- OS image files
- Work files

The disk capacities required for repositories vary with the types of OS to be installed on the managed nodes and the numbers of Update DVDs to be imported, but it is normal for them to use 10 GB and more. Please refer to the table below when you estimate the required capacities.

| Usage | Operation | Required capacity |
|--|--|---|
| Storage of firmware data | Import from Update DVD | Approximately 7 GB per Update DVD |
| | Import of other firmware data | Depends on data to be imported. |
| File storage for OS installation media | Import from Windows installation media | Approximately 3 to 8 GB per OS type Import of only the OS types to be installed by Profile Management is required. |
| | Import from VMware ESXi installation media | Approximately 0.5 GB per OS type Import of only the OS types to be installed by Profile Management is required. |
| | Import from Linux installation media | Approximately 4GB per OS type |
| Storage of ServerView Suite DVD | Import from ServerView Suite DVD | Approximately 8 GB per ServerView Suite DVD |
| Creation and storage of files for work | None | Approximately 0.5 GB |



- By correlating user groups and node groups, you can operate ISM separately for each node group. To do so, you have to prepare a separate repository for each user group. In this case, it is required to estimate the required disk capacities (excluding the one for the Server View Suite DVD) for repositories only for the number of user groups.
- The ServerView Suite DVDs are stored in the system area. Depending on the number of ServerView Suite DVDs to be used, it is required to estimate the required disk capacity on the LVM volume in the system area.

3.2.2 Repository Settings

Repositories store large amounts of data. If you operate repositories separately for each user group, the amounts of stored data are going to be even larger. This is why you should create the repositories on virtual disks that allow you to extend the disk capacities. For information on how to create and allocate virtual disks, see "[3.7 Allocation of Virtual Disks](#)."

3.2.3 Network Design

ISM uses the following two types of management LAN to manage servers:

- Networks connected to iRMC Management LAN

This type of network is mainly used for controlling servers or making BIOS, iRMC, MMB or virtual IO settings.

- Networks connected to the onboard LAN or LAN card

This type of network is mainly used for OS installation and for establishing connections after OS installation.

Moreover, network connections are required for managing switches and storages. These can be either divided into physical and logical connections or used as one single integrated connection.



Note

ISM-VA starts by default while the IP address "192.168.1.101" remains enabled. Be careful about overlapping with IP addresses of the other devices within the network.

You can avoid such IP address overlap by changing the IP address in the following procedure if an overlapped IP address is found.

1. Install ISM-VA on a hypervisor other than the one in the actual environment.
2. Change the IP address of ISM-VA.
3. Back it up according to the procedure described in "4.4.1 Back Up of ISM-VA."
4. Restore the ISM-VA that was backed up with hypervisor in the actual environment, according to the procedure described in "4.4.2 Restoration of ISM-VA."



Point

- It is recommended that you prepare separate networks for service use (service LANs) besides these management LANs.
- By correlating user groups and node groups, you can operate ISM separately for each node group. To do so, design separate networks for each node group. You can also set up firewalls around the network of each node group in order to separate data communication between groups and thereby prevent viewing and manipulation of nodes that belong to other node groups.
- You can define only one network interface for ISM. If you are going to configure multiple networks, configure the router to enable communication between the networks.

3.2.4 Setting of Node Names

Determine naming rules for nodes and profiles that will be required for node registration.

When you register a node, give it a unique name.

You can set up a maximum of 64 characters.

Note, however, that you cannot use the following characters.

Slash (/), Backslash (\), colon (:), Asterisk (*), Question mark (?), Double quotation ("), Angle brackets (<>), or Pipeline (|)

3.2.5 Setting of Users

Set up appropriate user roles and user groups according to the actual tasks and functions of each user. It is recommended that you execute the user settings according to the actual tasks and functions of each user within the framework, setting up user roles according to such tasks as installation, monitoring, or maintenance of nodes, and setting up user groups organization-wise for only the actual users of each node resource.

If you are going to operate nodes separately for each user group, you should define a node that is operated and managed by a given user group as a node group and then correlate the user group with the node group. When you do so, you have to create a user with an Administrator role within the user group.

In order to ensure security in node management, it is also recommended that you design operations so that users are removed as soon as they have become obsolete, that passwords have to be changed at regular intervals, and so on.

For information on how to make settings for user roles and user groups and on how to change passwords, see the ISM online help.

3.3 Installation of ISM-VA

The ISM software is supplied with the "FUJITSU Software ServerView Infrastructure Manager 2.1 Media Pack."

Install ISM-VA according to the installation destination.

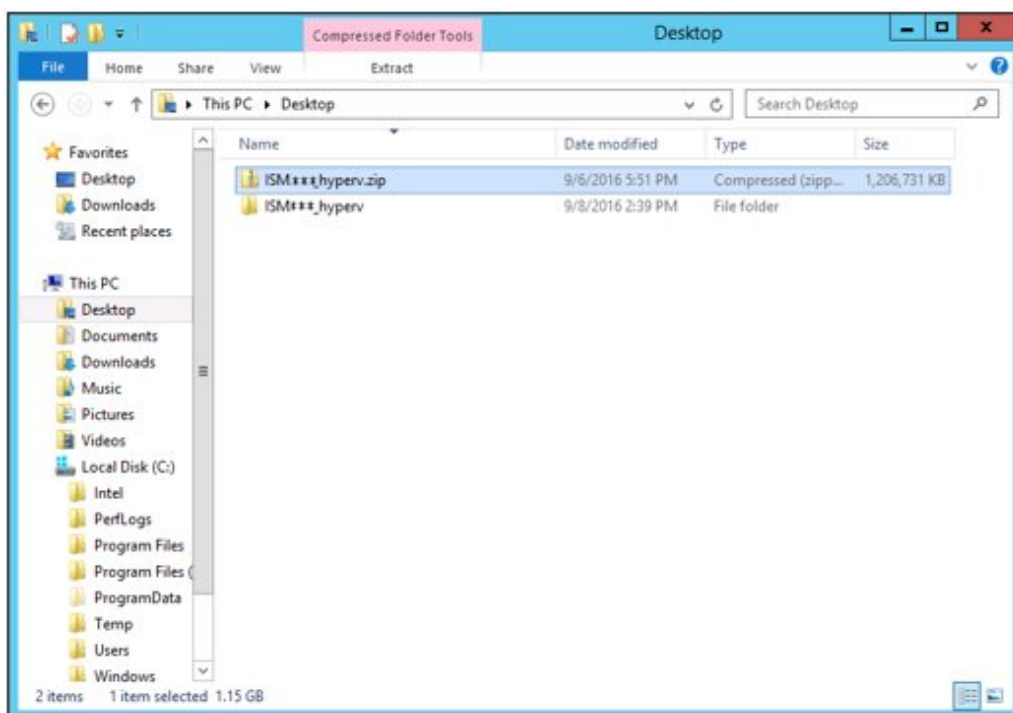
The following procedures describe how to install ISM-VA on Microsoft Windows Server Hyper-V, VMware vSphere Hypervisor, and KVM.

- [3.3.1 Installation on Microsoft Windows Server Hyper-V](#)
- [3.3.2 Installation on VMware vSphere Hypervisor](#)
- [3.3.3 Installation on KVM](#)

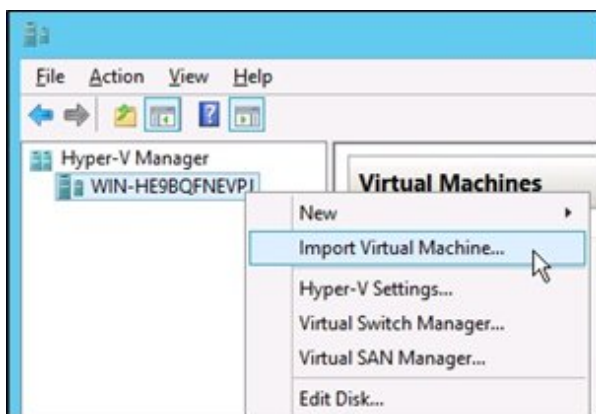
3.3.1 Installation on Microsoft Windows Server Hyper-V

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

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

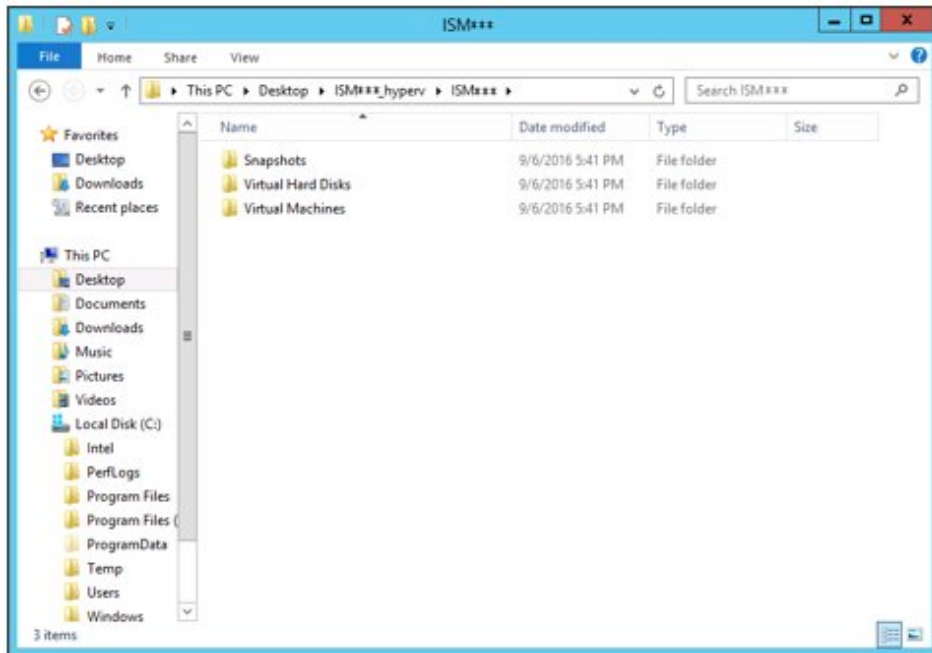


2. Start Hyper-V Manager, right-click on the Windows server to be used as the Hyper-V host, and then select [Import Virtual Machine].

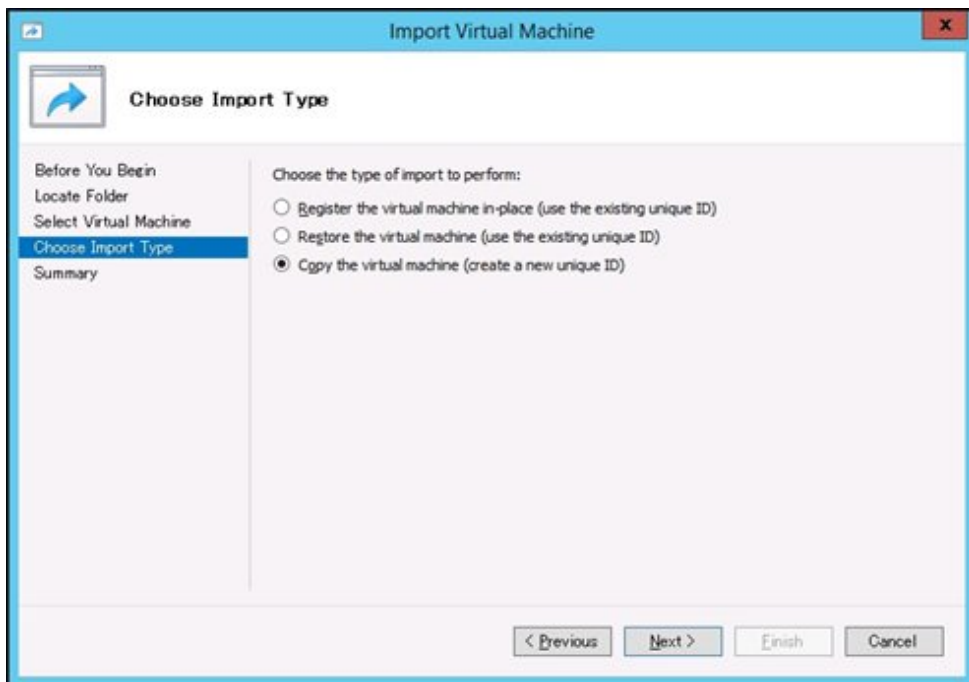


3. On the "Select Folder" screen, select the directory in which you deployed the file in Step 1.

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

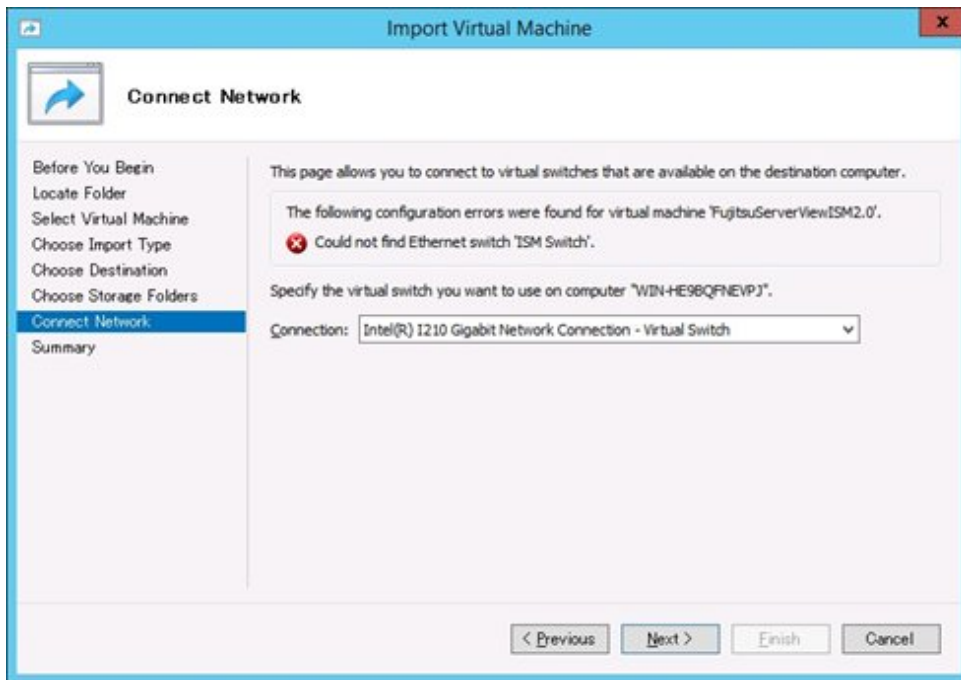


4. On the "Choose Import Type" screen, select [Copy the virtual machine (create a new unique ID)], and then select [Next].



5. On the "Choose Folders for Virtual Machine Files" and "Choose Folders to Store Virtual Hard Disks" 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 constant capacity. For details on how to convert, refer to the Hyper-V manual.

3.3.2 Installation on VMware vSphere Hypervisor

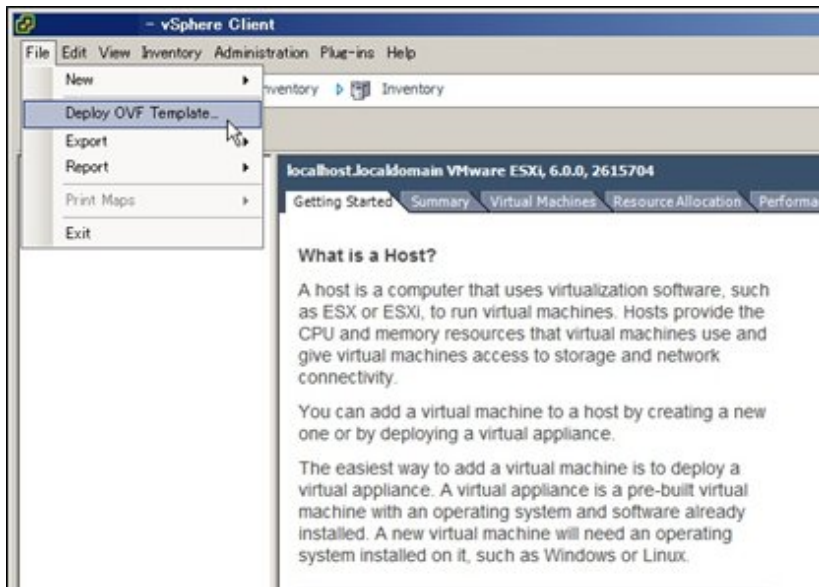
For installation, use the ova file that is included in the DVD media.

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

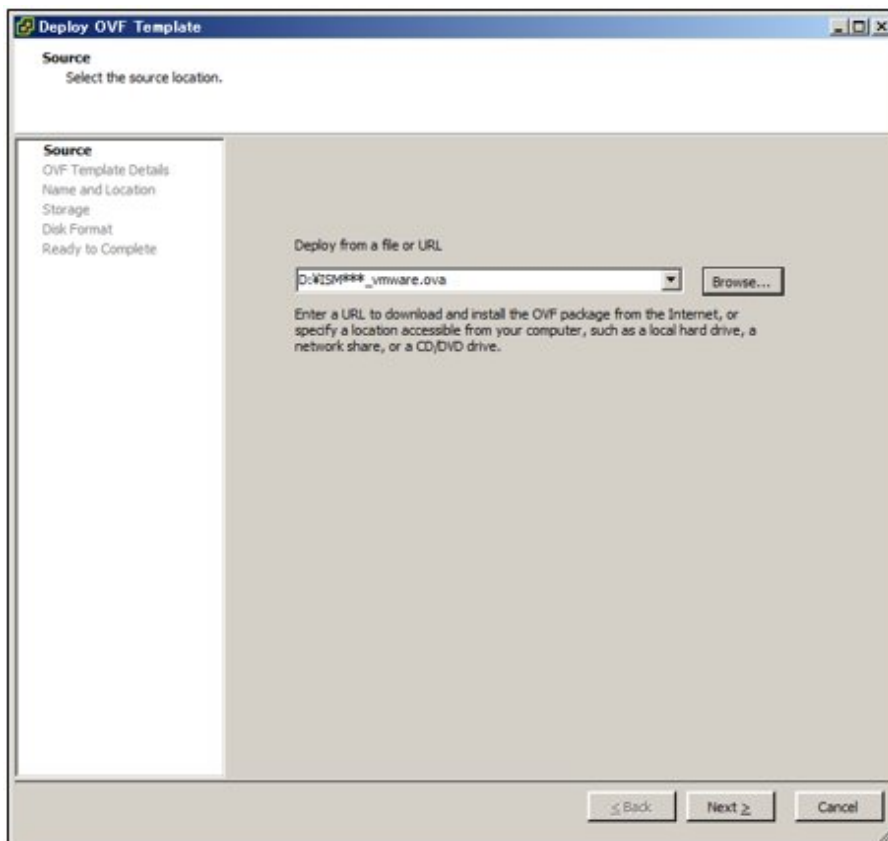
- [3.3.2.1 Installation on VMware ESXi 5.5 or VMware ESXi 6.0](#)
- [3.3.2.2 Installation on VMware ESXi 6.5 or later](#)

3.3.2.1 Installation on VMware ESXi 5.5 or VMware ESXi 6.0

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



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



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

Deploy OVF Template

Storage
Where do you want to store the virtual machine files?

[Source](#)
[OVF Template Details](#)
[Name and Location](#)
Storage
Disk Format
Network Mapping
Ready to Complete

Select a destination storage for the virtual machine files:

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

☐ Disable Storage DRS for this virtual machine.

Select a datastore:

| Name | Drive Type | Capacity | Provisioned | Free | Type | Thin Provi |
|------|------------|----------|-------------|------|------|------------|
|------|------------|----------|-------------|------|------|------------|

[< Back](#) [Next >](#) [Cancel](#)

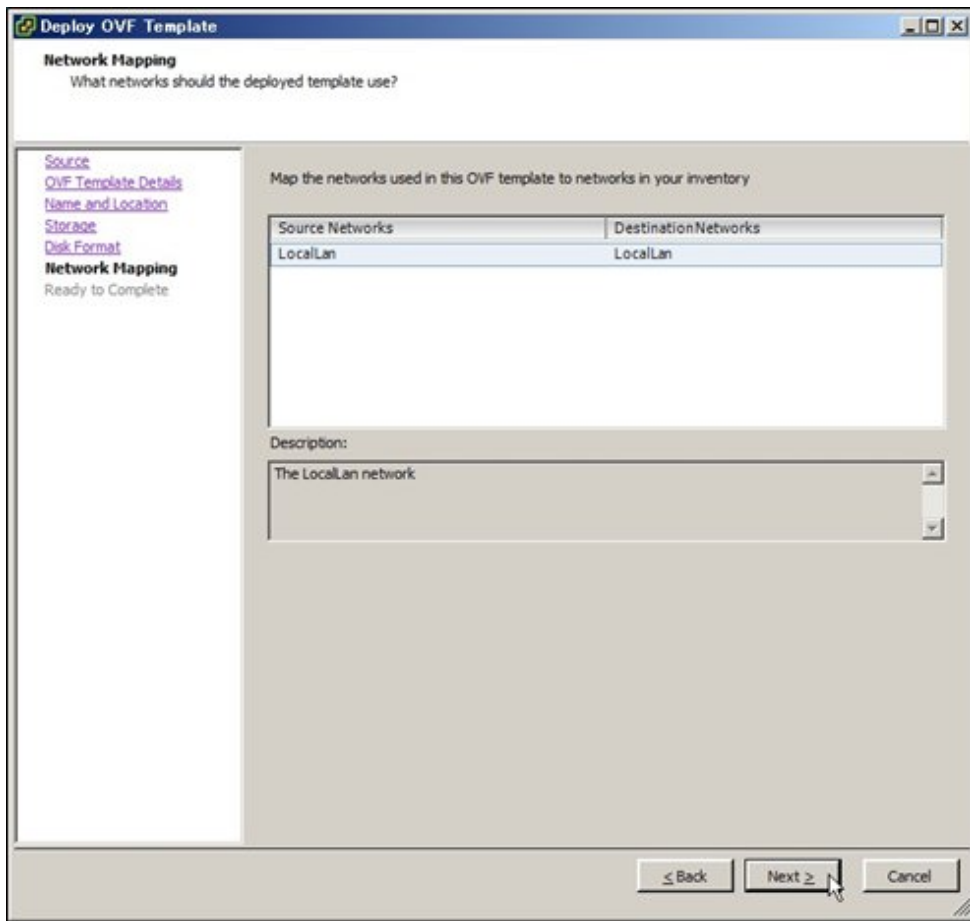
4. On the "Disk Format" screen, select [Thick Provision Lazy Zeroed] or [Thick Provision Eager Zeroed], and then select [Next].

The screenshot shows the 'Deploy OVF Template' wizard window. The title bar reads 'Deploy OVF Template'. The main heading is 'Disk Format' with the subtitle 'In which format do you want to store the virtual disks?'. On the left, a navigation pane lists the steps: 'Source', 'OVF Template Details', 'Name and Location', 'Storage', 'Disk Format' (which is highlighted), 'Network Mapping', and 'Ready to Complete'. The main area contains the following fields and options:

- Datastore:** A text box containing 'datastore1'.
- Available space (GB):** A text box containing '59.3'.
- Provisioning Method:** Three radio button options:
 - ☒ Thick Provision Lazy Zeroed
 - ☐ Thick Provision Eager Zeroed
 - ☐ Thin Provision

At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. A mouse cursor is pointing at the 'Next >' button.

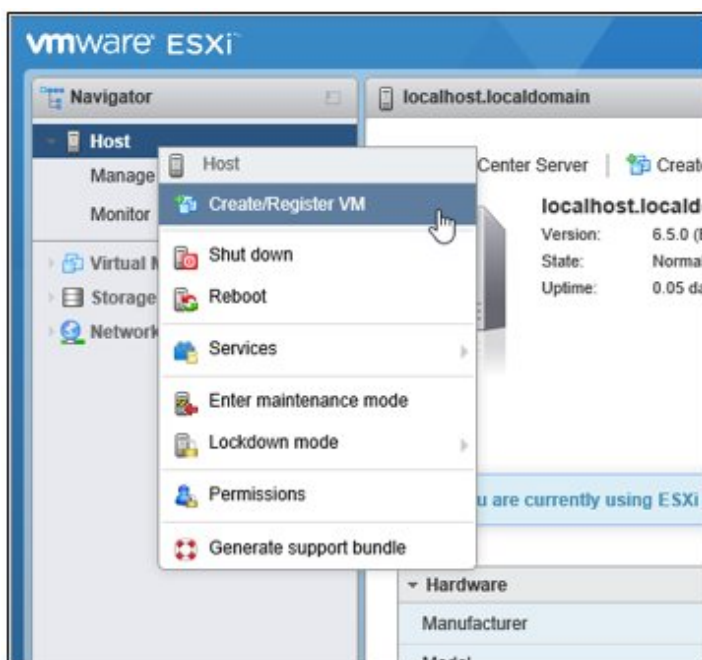
5. On the "Network Mapping" screen, select the network to be used by ISM, and then select [Next].



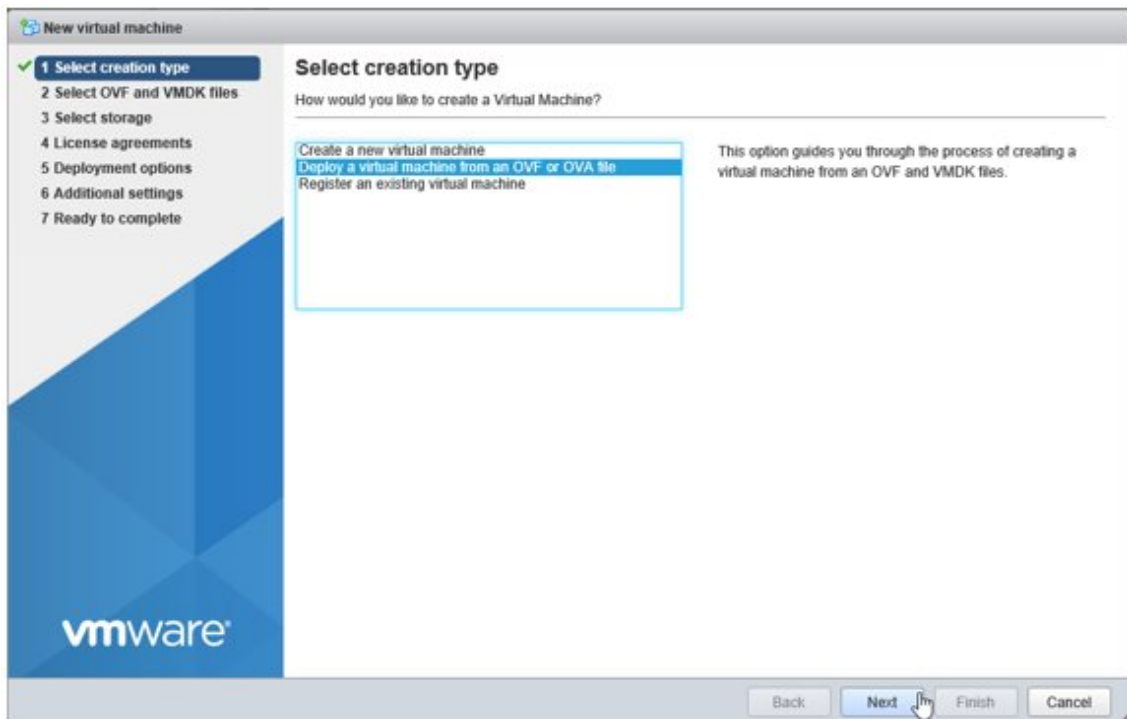
6. Select [Finish] to finish deployment of OVF templates.

3.3.2.2 Installation on VMware ESXi 6.5 or later

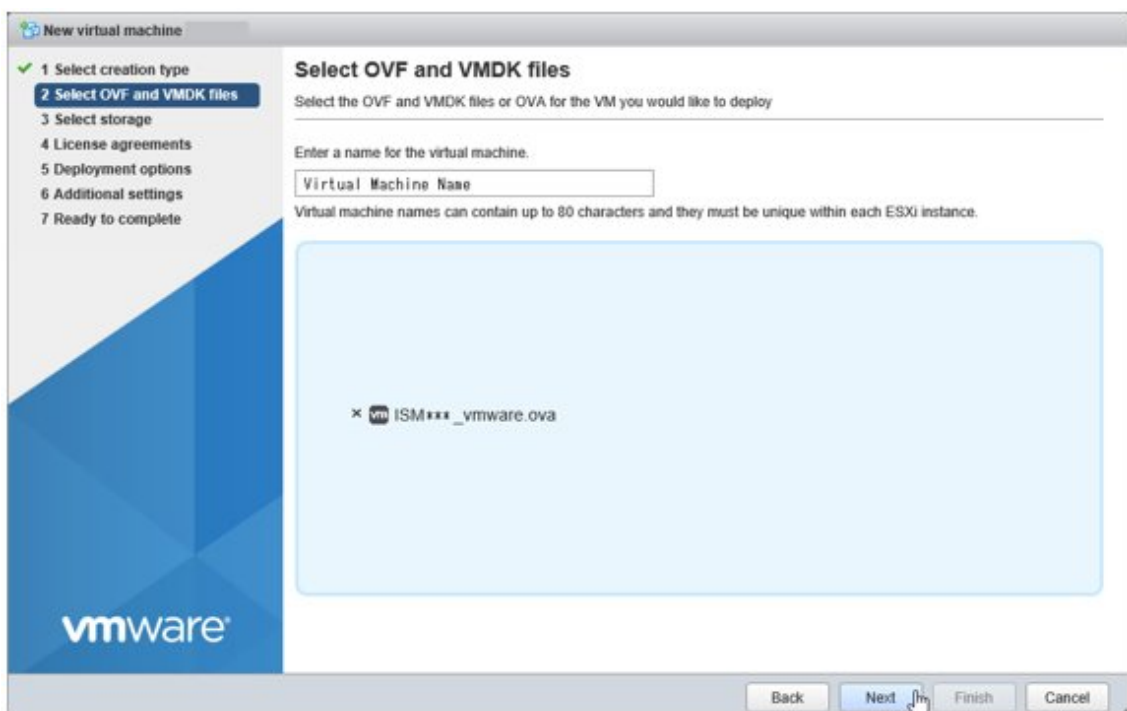
1. Start the vSphere Client (HTML5), right-click on the [Host] of the navigator, and then select [Create/Register VM].



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



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



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

New virtual machine

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- 4 License agreements
- 5 Deployment options
- 6 Additional settings
- 7 Ready to complete

Select storage

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

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

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

2 items

Back Next Finish Cancel

5. In 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

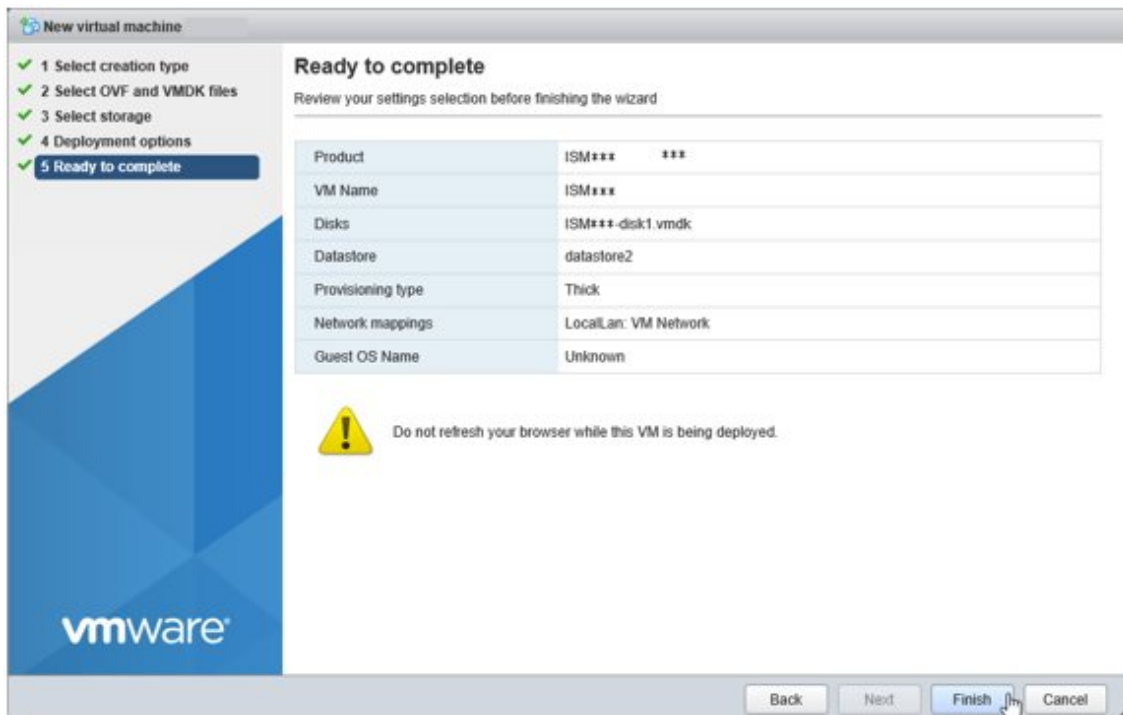
Select deployment options

Network mappings: LocalLan VM Network

Disk provisioning: ☐ Thin ☒ Thick

Back Next Finish Cancel

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



3.3.3 Installation on KVM

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

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

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

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

2. Copy the files in the decompressed directory to their respective designated locations.
 - a. Copy the qcow2 file to /var/lib/libvirt/images.

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

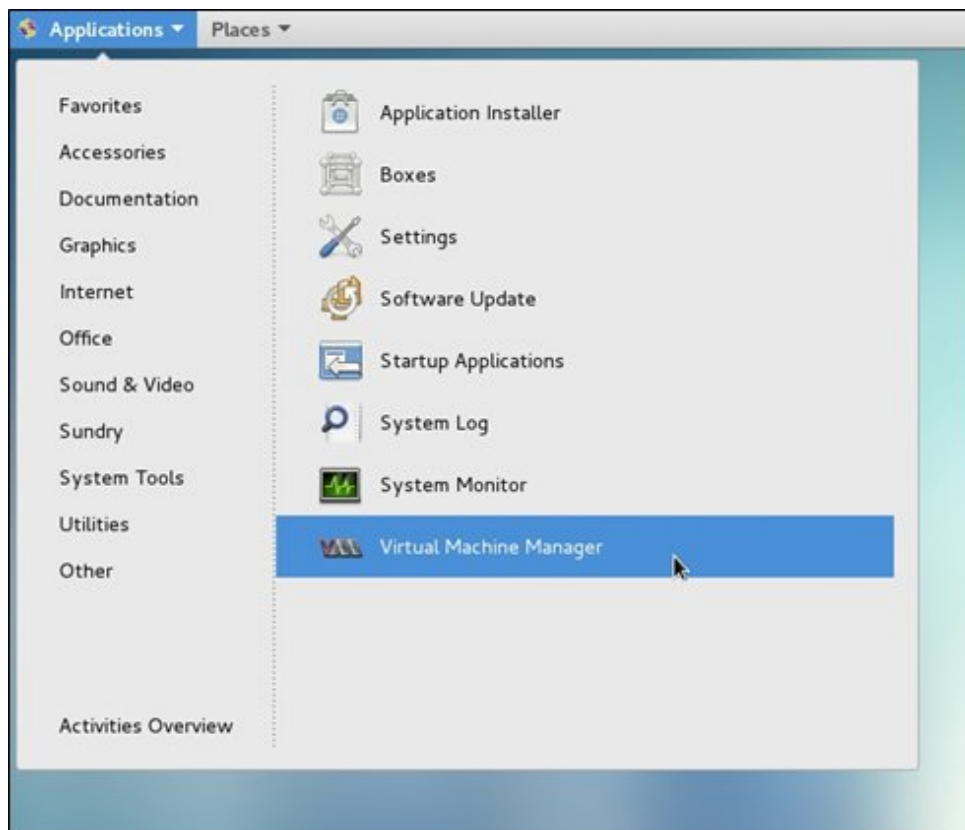
- b. Copy the xml file to /etc/libvirt/qemu.

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

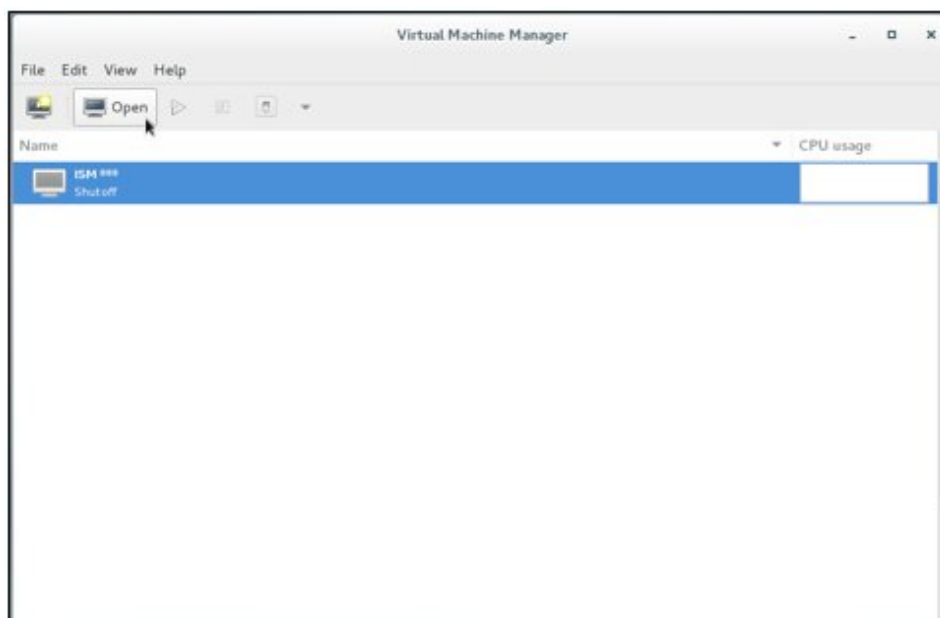
3. Specify the xml file to register ISM-VA.

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

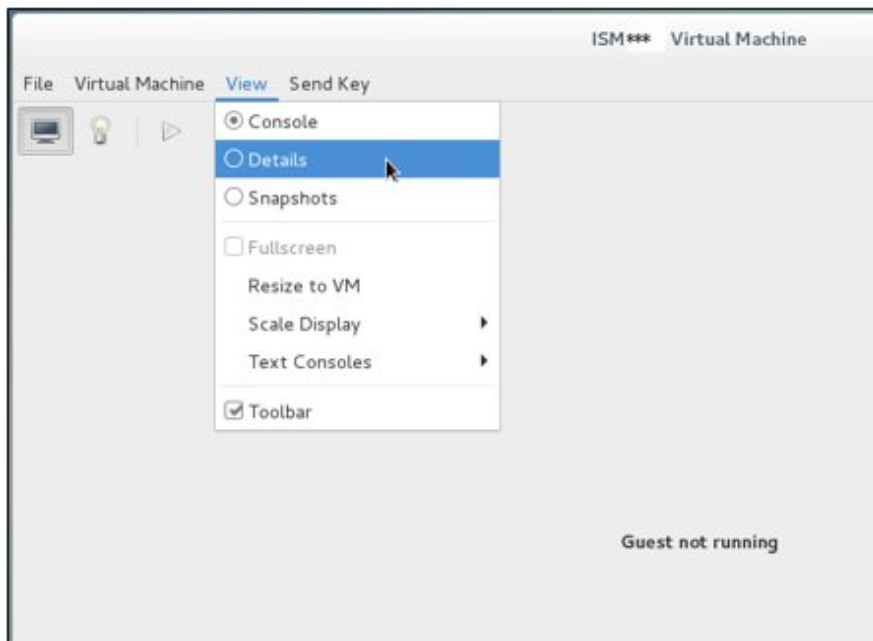
4. Select [Virtual Machine Manager] to open Virtual Machine Manager.



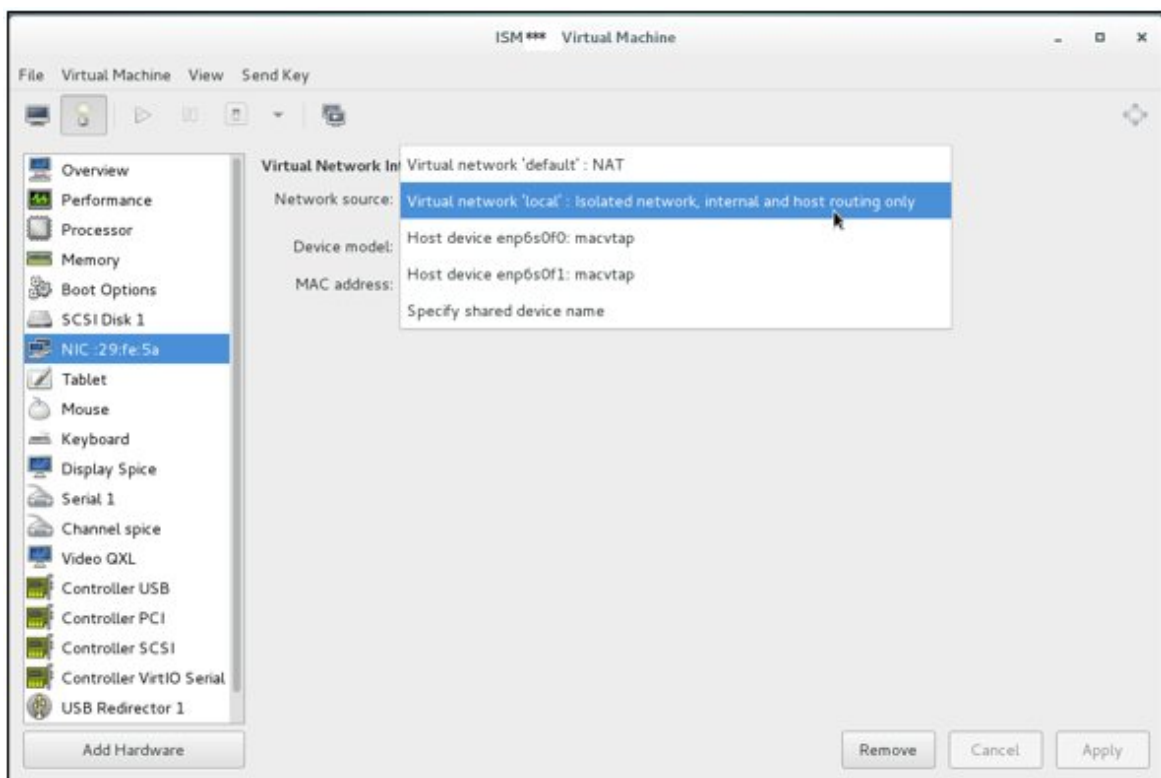
5. In Virtual Machine Manager, select ISM-VA, and then select [Open].



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



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



3.4 Environment Settings for ISM-VA

Make the initial settings after installing ISM.

3.4.1 First Start of ISM-VA

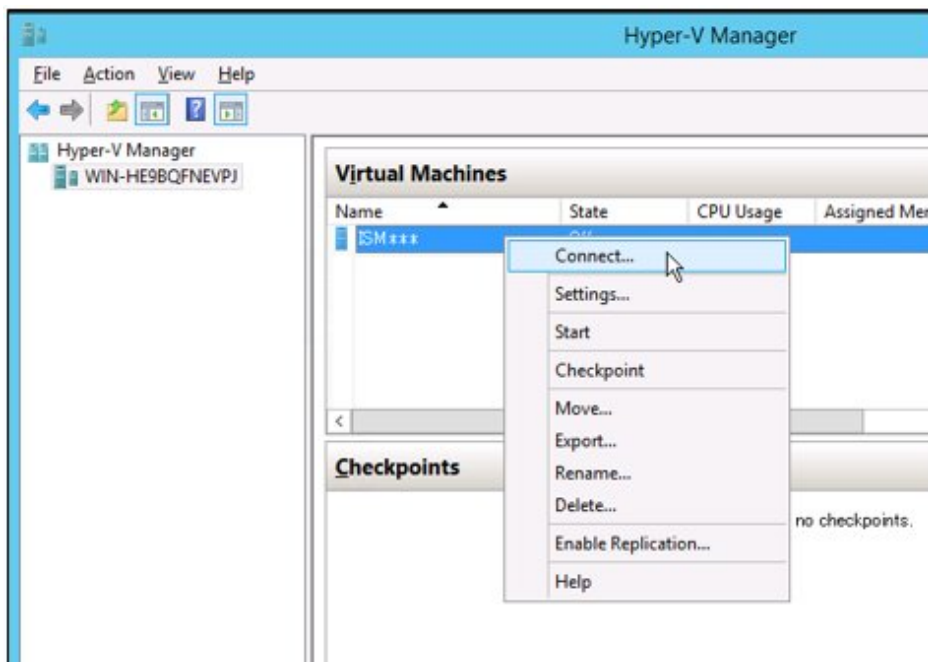
Use the respective function of the hypervisor on the installation destination to start up ISM-VA. Start up ISM-VA as a host OS user with administrator privileges.

The following procedures describe how to start up ISM-VA from Microsoft Windows Server Hyper-V, VMware vSphere Hypervisor, and KVM.

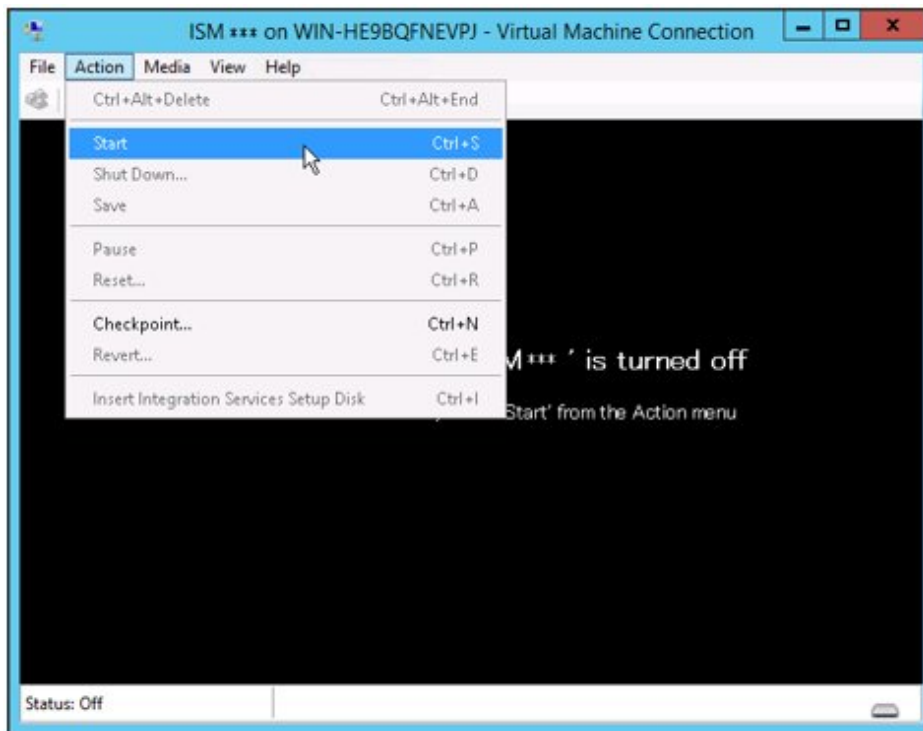
- [3.4.1.1 For ISM-VA Running on Microsoft Windows Server Hyper-V \(First Time\)](#)
- [3.4.1.2 For ISM-VA Running on VMware vSphere Hypervisor \(First Time\)](#)
- [3.4.1.3 For ISM-VA Running on KVM \(First Time\)](#)

3.4.1.1 For ISM-VA Running on Microsoft Windows Server Hyper-V (First Time)

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



2. On the "Virtual Machine Connection" screen, select [Start] from the [Action] menu to start ISM-VA.



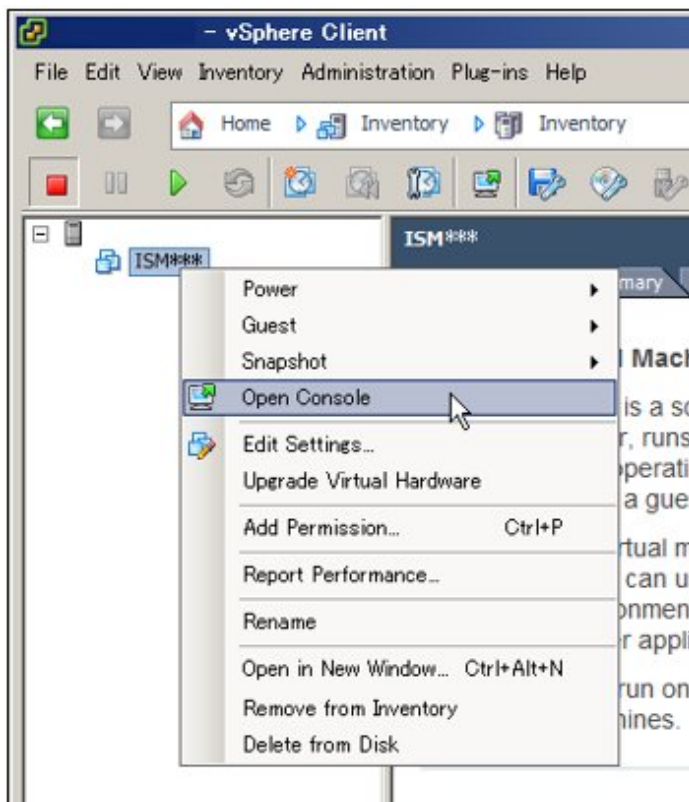
3.4.1.2 For ISM-VA Running on VMware vSphere Hypervisor (First Time)

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

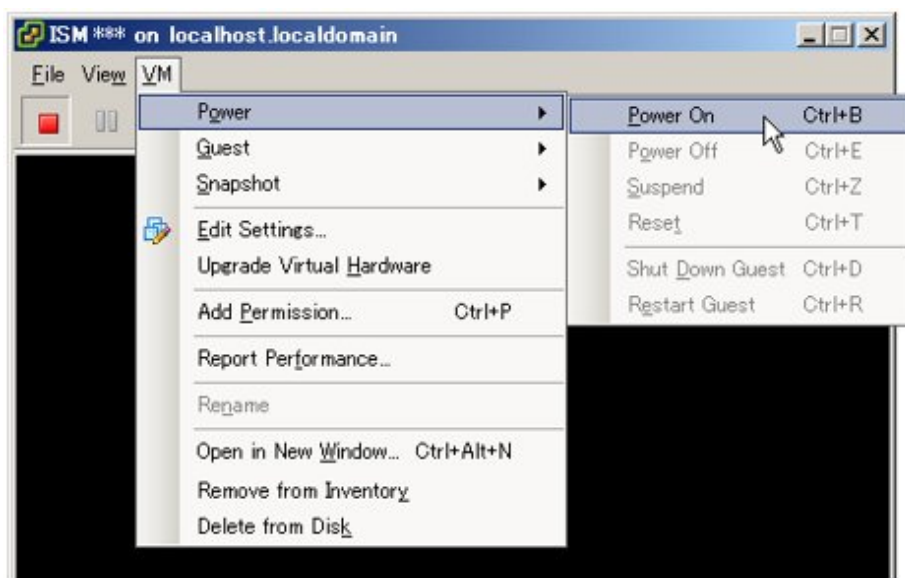
- [VMware ESXi 5.5 or VMware ESXi 6.0](#)
- [VMware ESXi 6.5 or later](#)

VMware ESXi 5.5 or VMware ESXi 6.0

1. In vSphere Client, right-click on the installed ISM-VA, and then select [Open Console].

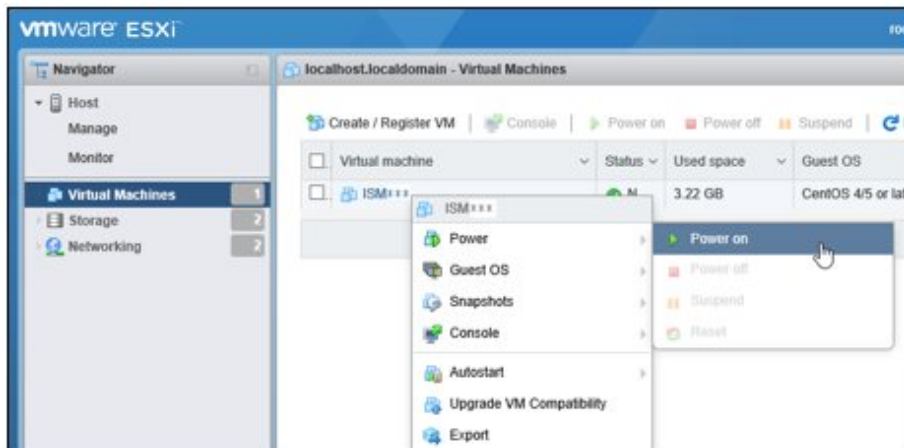


2. On the "Console" screen, select [Power] - [Power On] from the [VM] menu to start ISM-VA.

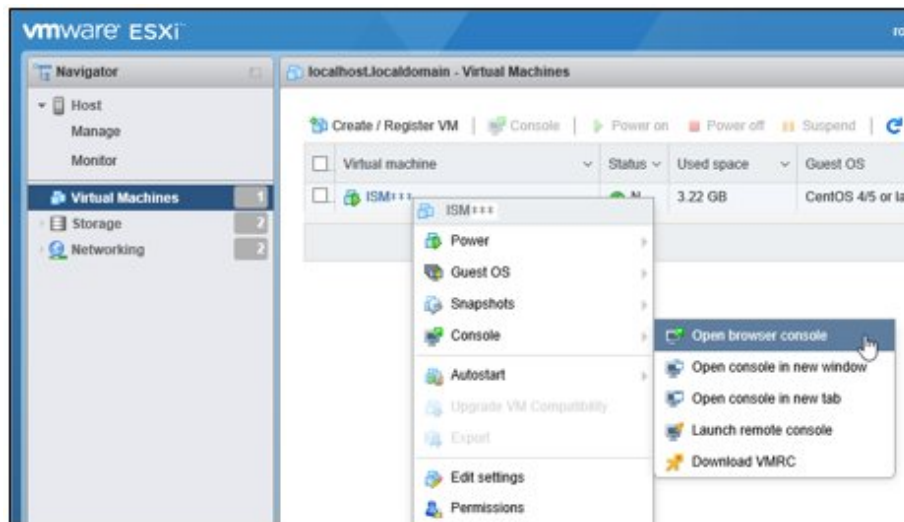


VMware ESXi 6.5 or later

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

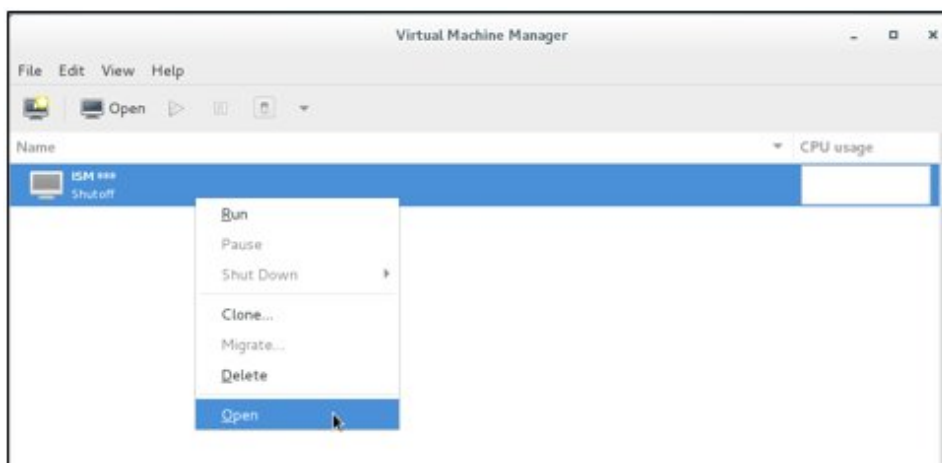


2. Right-click on the installed ISM-VA, and then select [Open browser console] or other console.

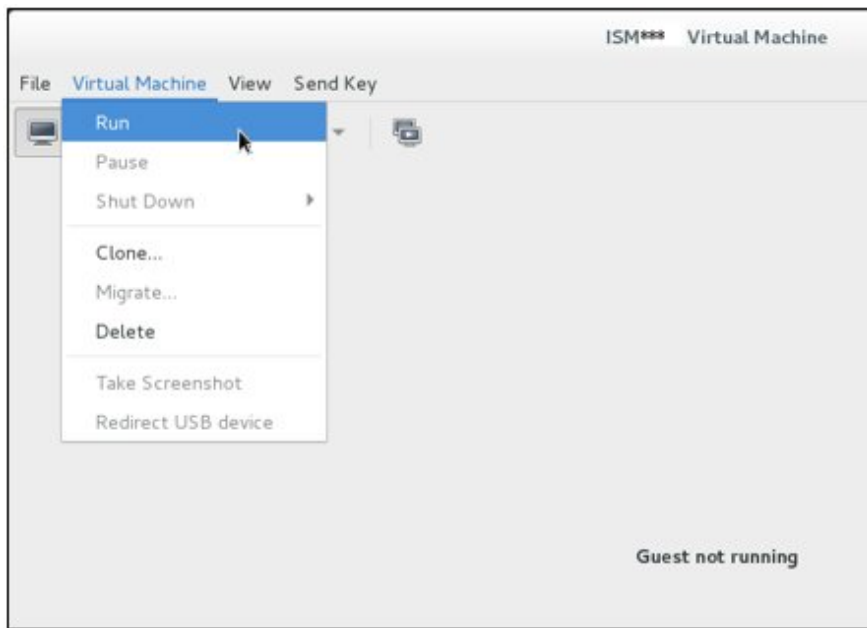


3.4.1.3 For ISM-VA Running on KVM (First Time)

1. In Virtual Machine Manager, right-click on the installed ISM-VA, and then select [Open].



2. On the "ISM-VA Virtual Machine" screen, select [Run] from the [Virtual Machine] menu to start ISM-VA.



3.4.2 Initial Settings of ISM

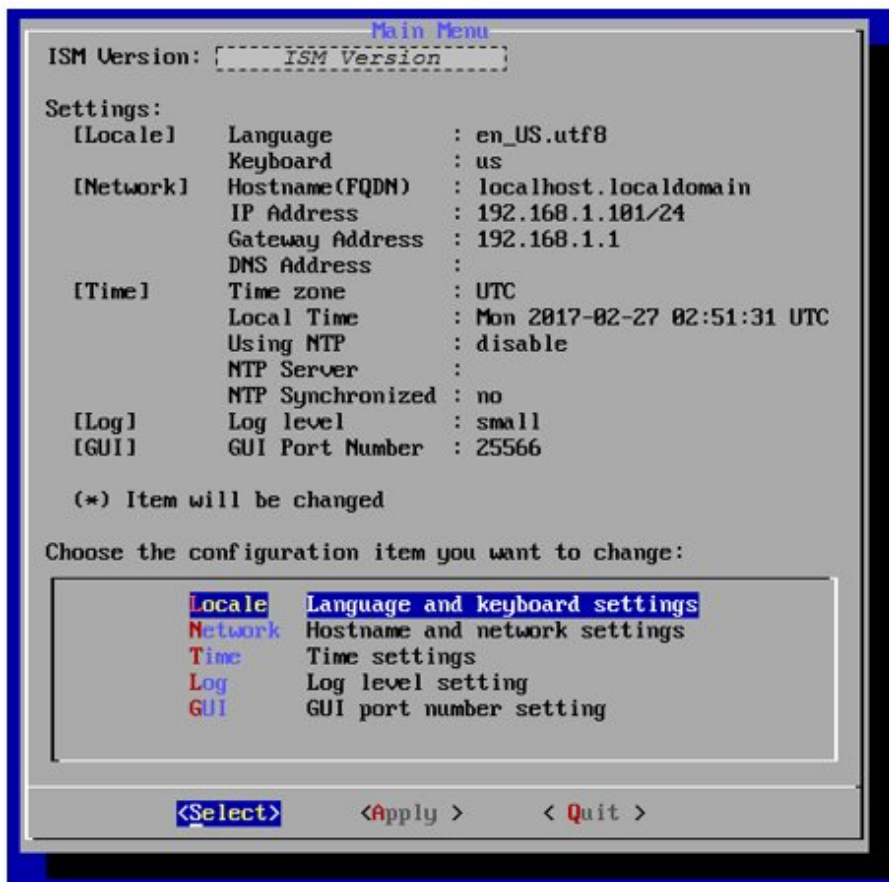
After starting ISM-VA, use the console basic setting menu or the ismadm commands to execute the basic setting menu for ISM.

3.4.2.1 Initial Settings Using the Basic Setting Menu

1. Use the administrator account and the default password to log in to the console.
 - Administrator account: administrator
 - Default password: admin
2. Execute the following command to start the basic setting menu.

```
# ismsetup
```


The screen below is displayed.



3. Execute the ISM settings.

In the basic setting menu, the following items can be set.

- Locale
- Network
- NTP server
- Log level
- Web GUI port number

When domain environment settings are required, execute Step 5 in "[3.4.2.2 Initial Settings Using the ismadm Command](#)."

3.4.2.2 Initial Settings 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, make the network settings.

- Confirm the LAN device names

```
# ismadm network device
DEVICE  TYPE      STATE      CONNECTION
eth0    ethernet  connected  eth0
lo      loopback   unmanaged  --
```

- Setup of network

```
# ismadm network modify <LAN device name> ipv4.method manual ipv4.addresses <IP address>/
<Maskbit> ipv4.gateway <Gateway IP address>
```

Example of command execution

```
# ismadm network modify eth0 ipv4.method manual ipv4.addresses 192.168.1.101/24 ipv4.gateway
192.168.1.1
```

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.

The operations after making the network settings can be carried out from both the hypervisor console as well as another console via SSH in the same ways. However, we recommend access via SSH for its good operability.

3. From the console, set the System Locale and the Keymap.

Use the following method 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.

- Setting of System Locale

```
# ismadm locale set-locale LANG=<Locale name>
```

Example of command execution

```
# ismadm locale set-locale LANG=en_US.utf8
```

- Display of available <Locale names>

```
# ismadm locale list-locales
```

- Setting of Keymap

```
# ismadm locale set-keymap <Keymap name>
```

Example of command execution

```
# ismadm locale set-keymap us
```

- Display of available <Keymap names>

```
# ismadm locale list-keymaps
```

Any modifications of System Locale become effective only after rebooting ISM-VA.

4. From the console, set the date and time.

Use the following method to confirm the current settings.

```
# ismadm time show
      Local time: Thu 2016-06-09 16:57:40 JST
      Universal time: Thu 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.

- Setting of time zone

```
# 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 server

```
# ismadm time add-ntpserver <NTP server>
```

Remove server

```
# ismadm time del-ntpserver <NTP server>
```

5. From the console, set the domain environment.

This setting is not required if you do not use the domain environment.

- Adding of domain setting information

```
# ismadm kerberos add -d <Domain Name> -r <Realm> -n <Controller Name>
```

Example of command execution

```
# ismadm kerberos add -d sample.local -r SAMPLE.LOCAL -n adsvr.sample.local
```

- Display of domain setting information

```
# ismadm kerberos show
```

- Going back to previous domain setting information

```
# ismadm kerberos restore
```

Unable to return to more than one previous state.

- Initialization of domain setting information

```
# ismadm kerberos init
```

3.5 Registration of Licenses

There are two types of license as follows. ISM requires registration of both server licenses and node licenses.

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

- Server licenses

These licenses are required for using ISM.

- Node licenses

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

There are two methods to register licenses, the first is to register from the console, and the second is to register from the operating GUI of a Web browser.

Method of registering from the console

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

1. Register the server licenses.

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

2. Register the node licenses.

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

3. Confirm the results of license registration.

```
# ismadm license show
```

4. Restart ISM-VA.

```
# ismadm power restart
```

Register from the operating GUI of a Web browser

When registering a license for the first time

1. Execute "[3.4.2 Initial Settings of ISM.](#)"
2. Restart ISM-VA.
3. Start the GUI operating in a Web browser.
4. From the GUI, log in as an administrator.
5. Follow the procedure below and register a license key.
 - a. Specify the license key in the entry field.
 - b. Select the [Apply] button.
 - c. Select the [Add] button to add entry fields if adding other license keys.
 - d. Repeat Step a - c and register all licenses, then select the [Close] button.



Point

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

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

If registering additional node licenses

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

1. The license screen is displayed under [Settings] - [General] - [License].
2. Select the [Register] button.
3. Specify the license key in the entry field.
4. Select the [Add] button to add entry fields if adding other license keys.
5. Repeat Step 3 - 4 and after specifying all the licenses, select the [Apply] button.



Note

.....
Licenses cannot be deleted from the GUI. Delete licenses from the console. For details, see deleting licenses in "[2.3.5.1 List of Commands in ISM-VA Management](#)."
.....

3.6 Registration of Users

Register the users for whom registration is required in order to operate ISM.

For information on how to register users, see "[2.3.1 User Management](#)."

3.7 Allocation of Virtual Disks

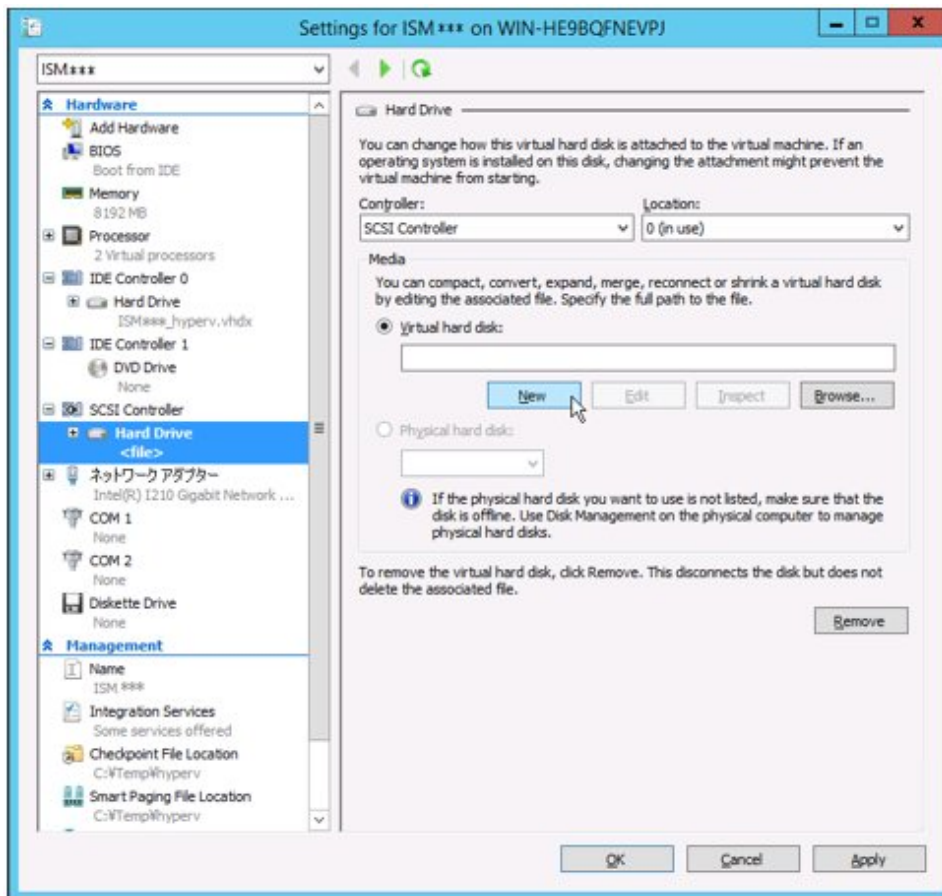
Virtual disks are resources for adding ISM-VA disk capacities. The storage of logs, repositories, and backups requires large capacities of disk resources. Moreover, these capacities vary with the respective operating methods and scales of managed nodes. Allocating voluminous resources to virtual disks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

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

3.7.1 Allocation of Virtual Disks to Entire ISM-VA

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

For Microsoft Windows Server Hyper-V



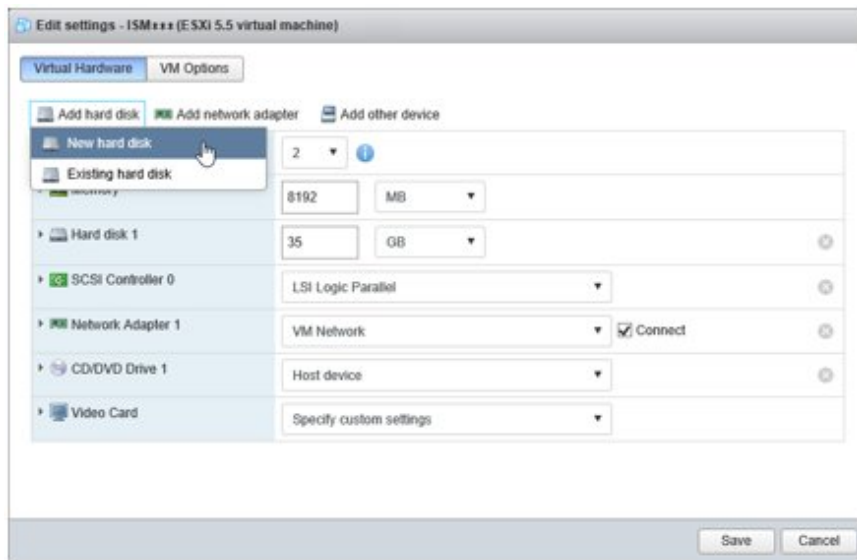
Create the virtual disks so as to be controlled by SCSI controllers.

For VMware vSphere Hypervisor 5.5 or VMware Hypervisor 6.0



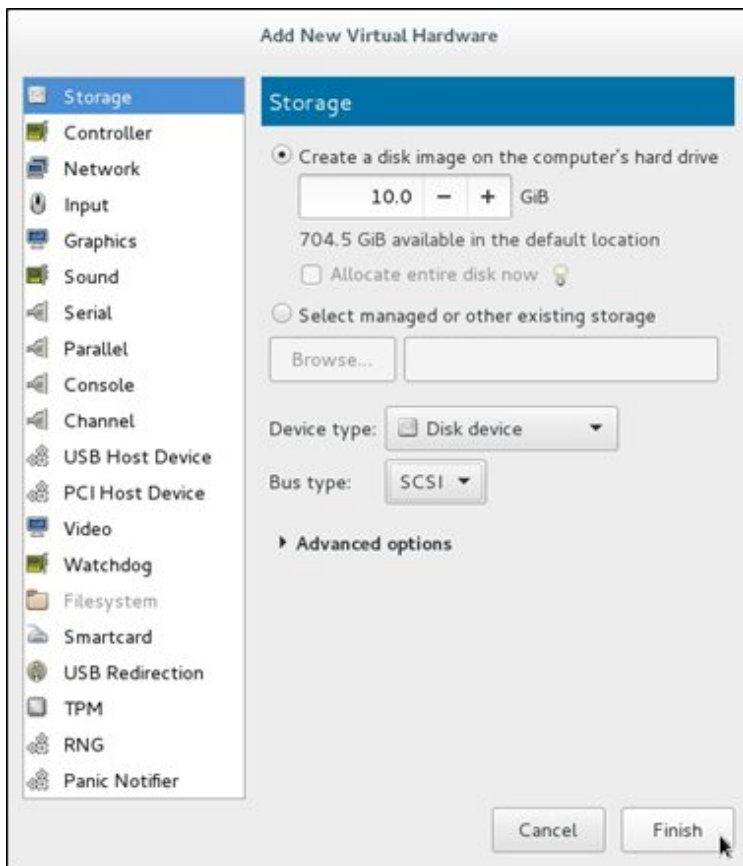
In the virtual device node selection that comes up on the "Detail Option" screen during disk creation, select SCSI.

For VMware vSphere Hypervisor 6.5



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

For KVM



For the bus type, select SCSI.

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

```
# ismadm service stop ism
```

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

Example:

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

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

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

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

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


6. Confirm the virtual disk settings.

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

```
# ismadm volume show -disk
```

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

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

7. Restart ISM-VA.

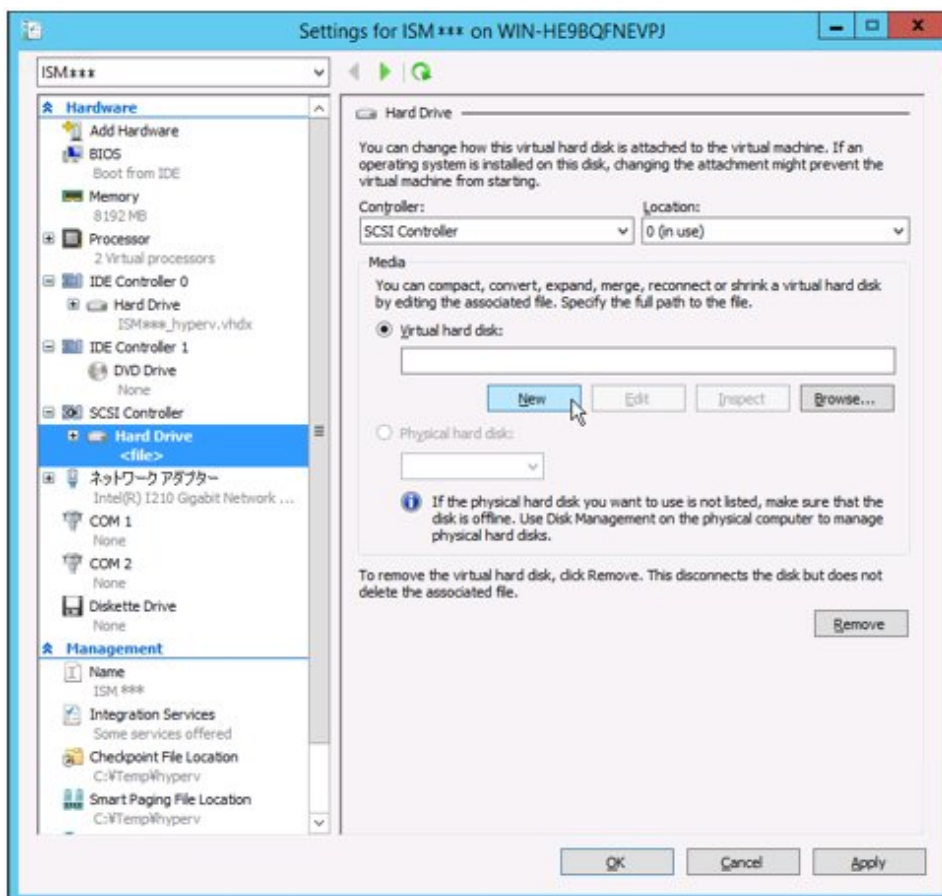
```
# ismadm power restart
```

3.7.2 Allocation of Virtual Disks to User Groups

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

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

For Microsoft Windows Server Hyper-V



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

For VMware vSphere Hypervisor 5.5 or VMware Hypervisor 6.0



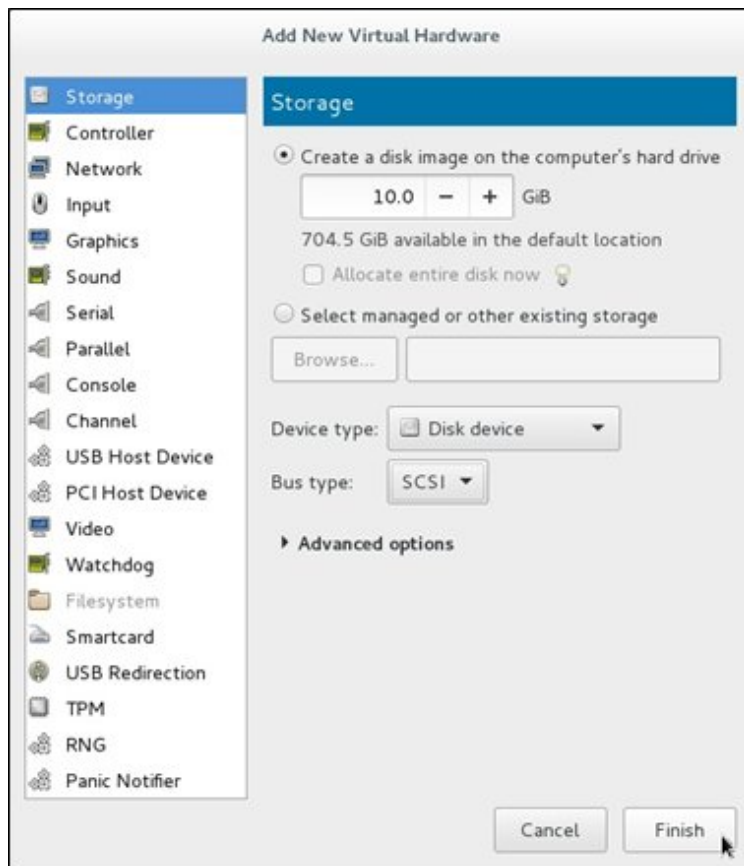
In the virtual device node selection that comes up on the "Detail Option" screen during disk creation, select SCSI.

For VMware vSphere Hypervisor 6.5



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

For KVM



For the bus type, select SCSI.

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

```
# ismadm service stop ism
```

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

Example:

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

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

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

5. Create an additional volume named "adminvol" for the Administrator group 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 (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 the Virtual Resource Management Function

Operation monitoring for the virtualized platform can be executed by using the Virtual Resource Management function.

Management and monitoring for the virtual resource can be executed from the each management screen of the virtual resource on ISM GUI.

For the descriptions for the contents and displayed items of the virtual resource management GUI, see the ISM online help.



Note

For pre-settings for virtual resource management, please access your local support.

Chapter 4 Operation of ISM

This chapter describes how to control ISM.

4.1 Start Up and Termination of ISM

Sometimes, it may be required to start up or terminate ISM manually for maintenance or other reasons.

4.1.1 Start Up of ISM

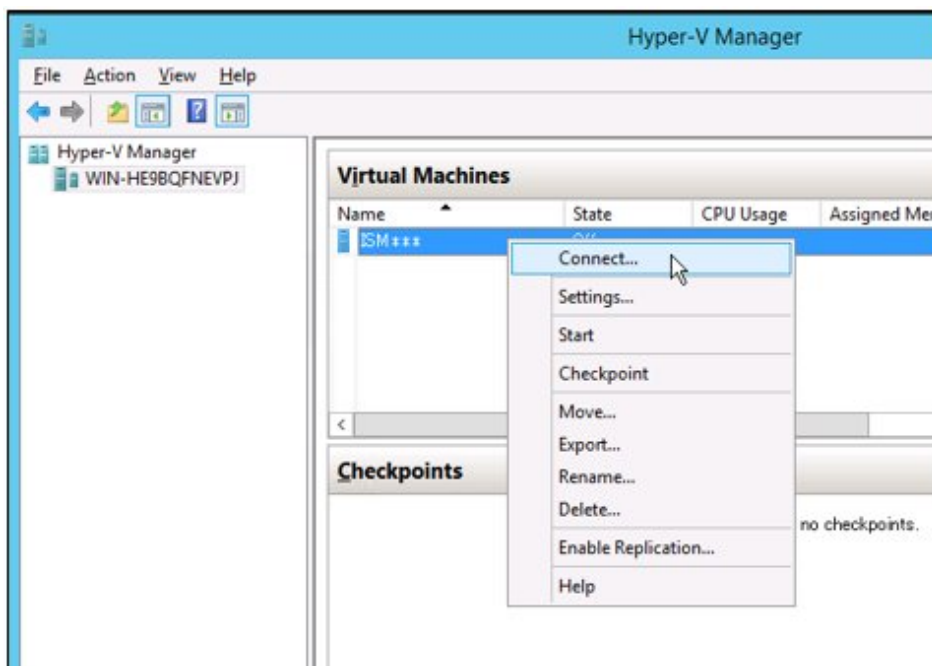
Use the respective function of the hypervisor on the installation destination to start up ISM-VA. Start up ISM-VA as a host OS user with administrator privileges.

The following procedures describe how to start up ISM-VA from Microsoft Windows Server Hyper-V, VMware vSphere Hypervisor, and KVM.

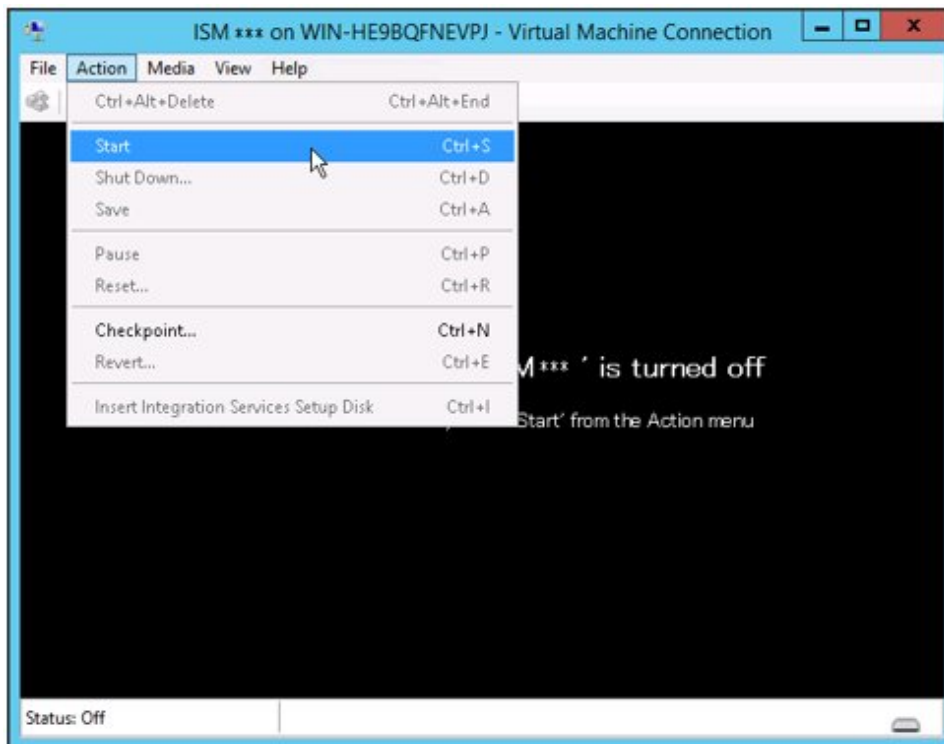
- 4.1.1.1 For ISM-VA Running on Microsoft Windows Server Hyper-V (Second Time and Later)
- 4.1.1.2 For ISM-VA Running on VMware vSphere Hypervisor (Second Time and Later)
- 4.1.1.3 For ISM-VA Running on KVM (Second Time and Later)

4.1.1.1 For ISM-VA Running on Microsoft Windows Server Hyper-V (Second Time and Later)

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.



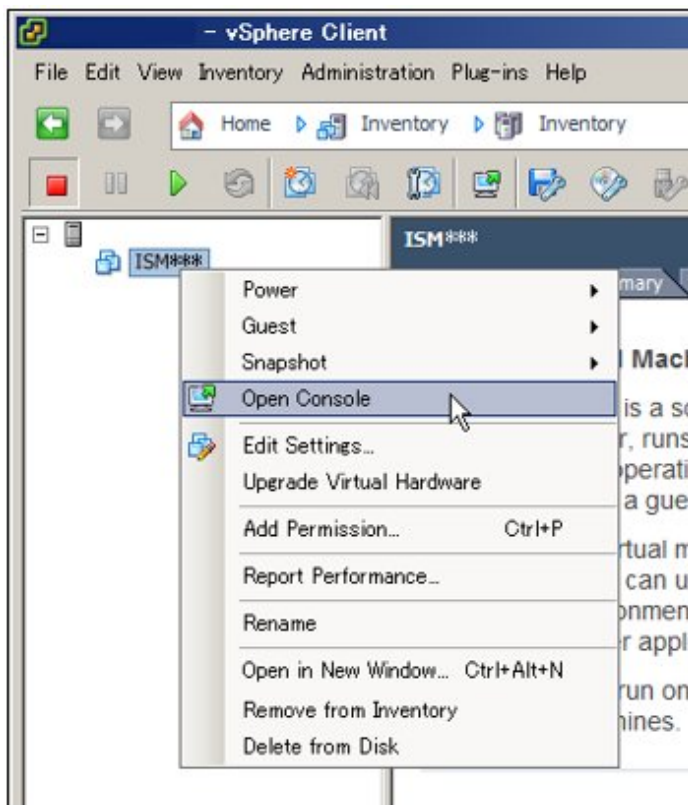
4.1.1.2 For ISM-VA Running on VMware vSphere Hypervisor (Second Time and Later)

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

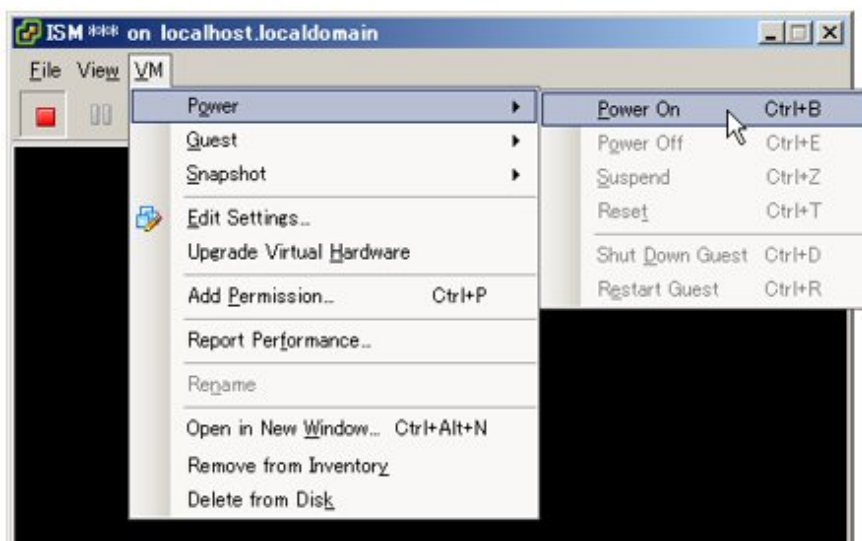
- [VMware ESXi 5.5 or VMware ESXi 6.0](#)
- [VMware ESXi 6.5 or later](#)

VMware ESXi 5.5 or VMware ESXi 6.0

1. In vSphere Client, right-click on the installed ISM-VA, and then select [Open Console].

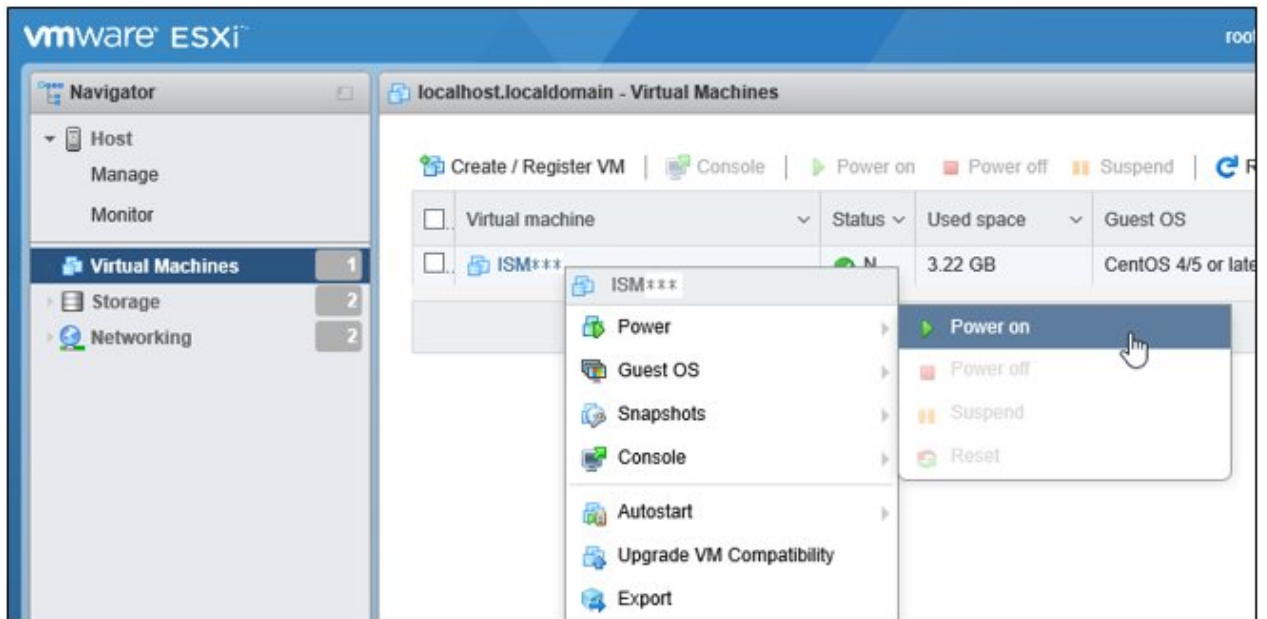


2. On the "Console" screen, select [Power] - [Power On] from the [VM] menu to start ISM-VA.

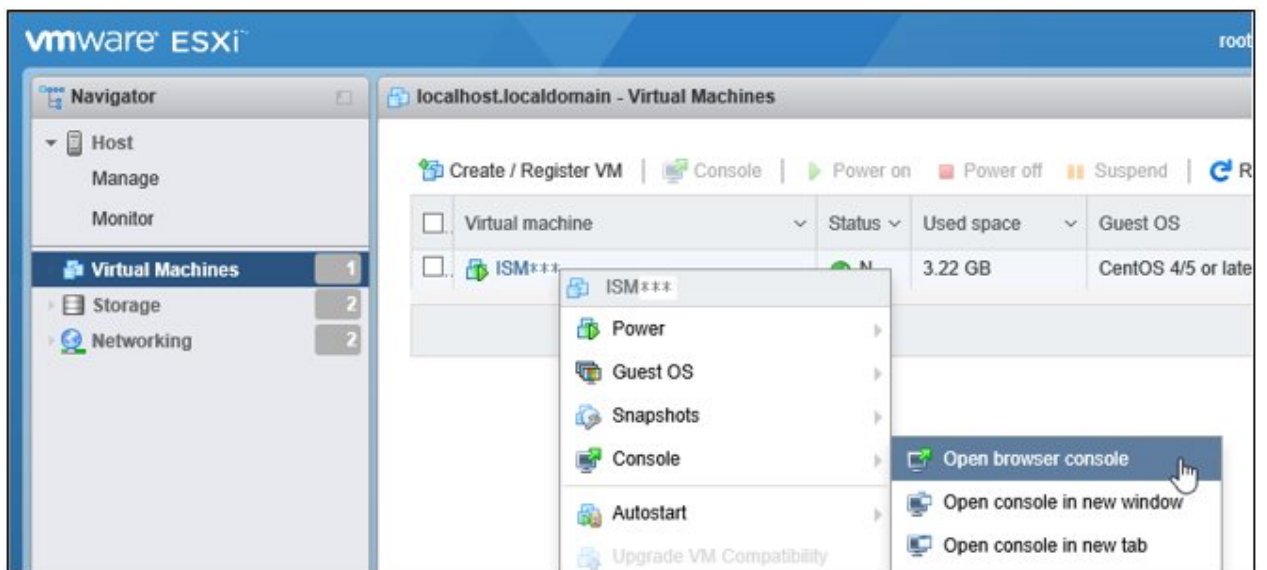


VMware ESXi 6.5 or later

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

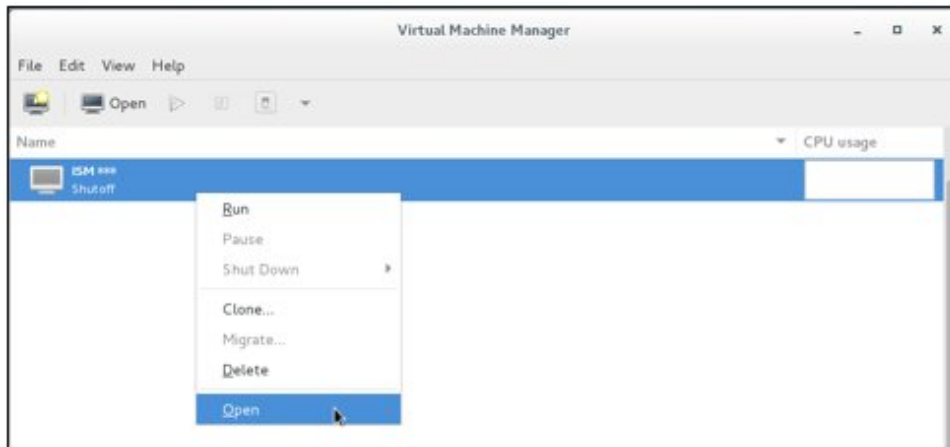


2. Right-click on the installed ISM-VA, and then select [Open browser console] or other console.

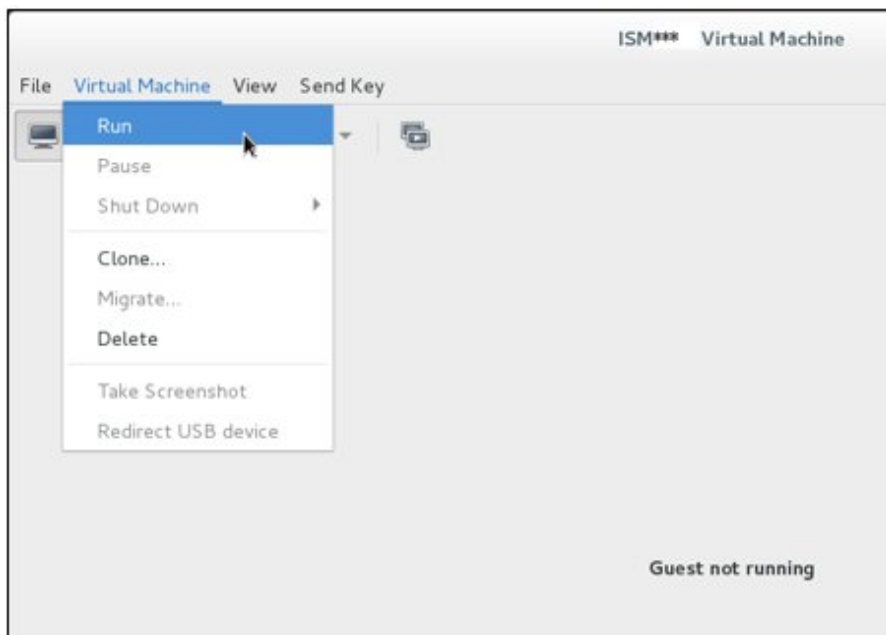


4.1.1.3 For ISM-VA Running on KVM (Second Time and Later)

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.



Starting up ISM-VA may take several minutes to complete. Wait for a while, then confirm that you can log in to the GUI.

4.1.2 Termination of ISM-VA

Use the ISM-VA command to terminate ISM-VA.

1. Start up the GUI.

Log in to the GUI as an ISM administrator.

2. Terminate all operations.

View the "Tasks" screen to confirm that all tasks are terminated.

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

- b. In the [Tasks] screen, check that the status has become "Completed" or "Cancellation completed."
- c. If there are tasks that are not either "Completed" or "Cancellation completed", then either wait for them to finish or cancel these tasks.

If you cancel the tasks, select the tasks running and then select [Cancel] from the [Actions] button. Cancel all tasks that are currently being executed.

Tasks of the "Updating Firmware" (Firmware Update process) type may sometimes not be aborted by canceling. In such a case, you have to wait until processing finishes.



Note

Terminating ISM-VA with any tasks still running may cause task processing to be interrupted with an error and result in incorrect operating behavior in later operations.

Therefore, be sure to either wait until all tasks finish, or cancel them manually and then, only when processing for canceling has finished, terminate ISM-VA.

3. Log out from the GUI of ISM, and then close the GUI.
4. Start up the console and log in as an ISM administrator.
5. To terminate ISM-VA, execute the termination command of ISM-VA.

```
# ismadm power stop
```

4.1.3 Restart of ISM-VA

Restarts of ISM-VA are mainly carried out when applying patches in ISM-VA.

1. Terminate all ISM tasks, close the GUI, and then log in to the console.

For information on how to terminate ISM tasks and close the GUI, see "[4.1.2 Termination of ISM-VA.](#)"

2. Execute the following command to restart ISM-VA.

```
# ismadm power restart
```

4.1.4 Start Up and Stop of ISM Service

As soon as you start up ISM-VA, the ISM service starts automatically.

To start and stop the ISM service, you have to log in to ISM-VA from the console as an administrator and execute the applicable ISM-VA commands.

Start up 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 information on how to terminate ISM tasks and close the GUI, see "[4.1.2 Termination 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 | Timezone | Set time zone | ismadm time set-timezone |
| | Local Time | Display local time | ismadm time show |
| | Using NTP | Enable/Disable NTP | ismadm set-ntp |
| | NTP Server | NTP server setting | ismadm add-ntpserver |
| | | | ismadm del-ntpserver |
| | NTP Synchronized | Display NTP synchronization | ismadm time show |
| Log | Log level | Damage investigation log size setting | ismadm system change-log-level |
| GUI | GUI port number | Web GUI connection port setting | ismadm service modify -port |

The following is the method for using the ISM-VA basic settings menu.

1. From the Console as an administrator, log in to ISM-VA.
2. Start using the ISM-VA basic settings menu command.

```
# ismsetup
```

The screen below is displayed.

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, 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 to from the new destination port number.

4.4 Back Up and Restoration of ISM-VA

This section describes the procedure for backing up and restoring ISM-VA.



Note

Before you back up or restore ISM-VA, be sure to terminate ISM-VA. For information on how to terminate ISM-VA, see "[4.1.2 Termination of ISM-VA](#)."

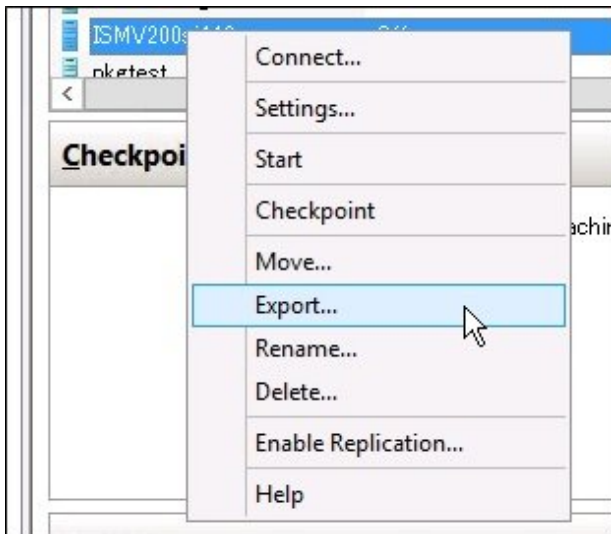
4.4.1 Back Up of ISM-VA

Use the export function of the hypervisor to back up ISM-VA.

The following procedures describe how to back up ISM-VA from Microsoft Windows Server Hyper-V, VMware vSphere Hypervisor, and KVM.

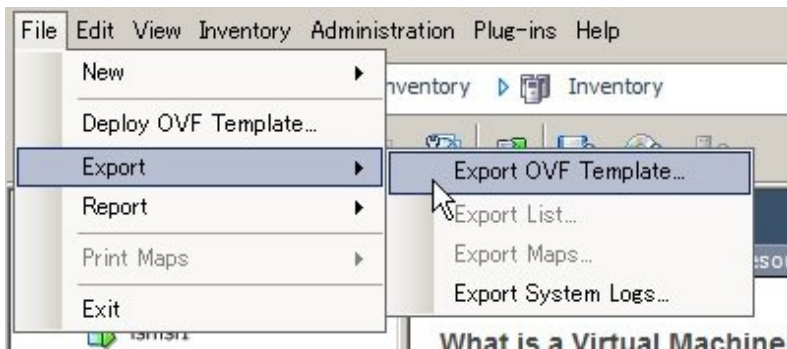
Back Up of ISM-VA Running on Microsoft Windows Server Hyper-V

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



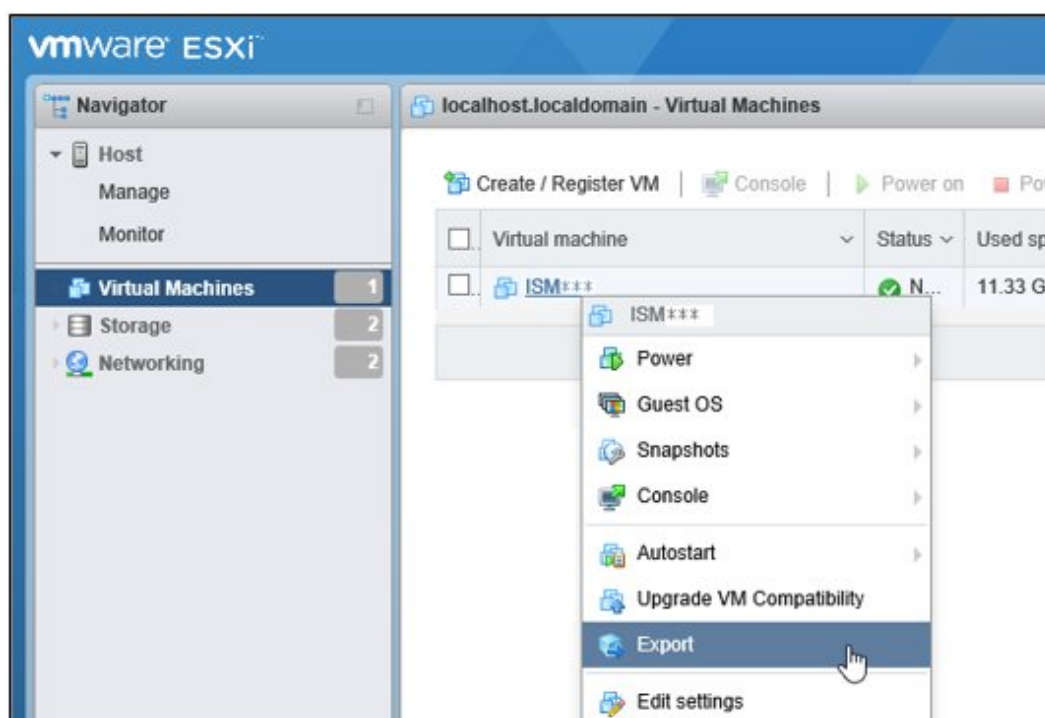
Back Up of ISM-VA running on VMware vSphere Hypervisor 5.5 or VMware vSphere Hypervisor 6.0

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



Back Up of ISM-VA Running on VMware vSphere Hypervisor 6.5

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



Back Up of ISM-VA Running on KVM

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

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

4.4.2 Restoration of ISM-VA

To restore ISM-VA, use the backed up files and execute the procedure described in "[3.3 Installation of ISM-VA.](#)"

4.5 Collection of Maintenance Data

You can collect maintenance data that is required for investigating any trouble that occurred in the system operated by ISM.

Collect the maintenance data according to the objective of your investigation.

| Objective of investigation | Investigating staff | Maintenance data |
|--|---------------------|---|
| Investigation of malfunctions in ISM and/or ISM-VA | Support personnel | ISM RAS logs ISM-VA Operating System logs Archived logs |

You can collect the maintenance data either separately according to the objective of your investigation or collectively in a batch.

Maintenance data can only be collected by ISM administrators. Depending on each inspection objective, ISM administrators provide the investigating staff with the collected maintenance data.

Note

- Collecting archived logs may take several hours to complete. Moreover, this requires large amounts of free disk space in ISM-VA. If you have to collect these kinds of data, or if you are going to collect maintenance data in a batch, follow the instructions of your support personnel.

- When you execute a command, the following message may sometimes be displayed on the hypervisor console, but this does not mean any problem.

```
blk_update_request:I/O error, dev fd0, sector 0
```

Collection Method

Use the ISM-VA commands to collect ISM maintenance data.

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

Sample investigation of malfunctions in ISM and/or ISM-VA

- Collection of ISM RAS logs only

```
# ismadm system snap -dir /Administrator/ftp
snap start
Your snap has been generated and saved in:
/Administrator/ftp/ismsnap-20160618175323.tar.gz
```

- Batch collection of ISM RAS logs, ISM-VA Operating System logs, and archived logs

```
# ismadm system snap -dir /Administrator/ftp -full
snap start
Your snap has been generated and saved in:
/Administrator/ftp/ismsnap-20160618175808.tar.gz
```



Point

"-dir" specifies the output destination path. By specifying a file transfer area as described in "2.1.2 FTP Access", you can access and obtain the collected maintenance data over FTP.



Note

Batch collection of maintenance data takes several hours to complete and requires large amounts of free disk space.

3. Download the collected maintenance data.

When you execute the command for collection, the output destination path and file names are displayed; access and download these over FTP as an administrator from the management terminal.



Note

- Maintenance data created in the storage directory for maintenance data are not deleted automatically. Use the FTP client software to manually delete any maintenance data that are no longer required. Since maintenance data are created each time you collect them, reducing the free disk space for ISM-VA if not deleted, other functions and operations may also be affected.
- vc-support log is collected from vCenter as maintenance documentation for the Virtual Resources Management function. For details, see "To collect ESX/ESXi and vCenter Server diagnostic data" from the following URL.

https://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2032892

In Step 6 of the log collection procedure in the URL above, for the ESXi host log collection target, select all the VSAN cluster ESXi hosts where an error has occurred.

4.6 Management of Virtual Disks

You can cancel or newly add allocations of virtual disks.

4.6.1 Cancel of Allocations of Virtual Disks

You can cancel allocations of virtual disks that you made according to "[3.7.2 Allocation of Virtual Disks to User Groups](#)."



- On canceling an allocation, all data that were stored in the user group will be lost.
- Allocations of virtual disks to Administrator groups cannot be canceled.
- Allocations of virtual disks to the entire ISM-VA as made according to "[3.7.1 Allocation of Virtual Disks to Entire ISM-VA](#)" cannot be canceled.

The following operating example shows how to cancel the allocation of a virtual disk to a user group named usrgpr1.

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

```
# ismadm service stop ism
```

3. Confirm that the virtual disk is allocated to usrgpr1.

```
# 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/usrgpr1vol-lv 10G   33M   10G    1% 'RepositoryRoot' /usrgpr1

PV          VG          Fmt Attr PSize  PFree
/dev/sda2   centos      lvm2 a--  19.51g    0
/dev/sdb1   usrgpr1vol lvm2 a--  10.00g    0
```

In this example, the VG named usrgpr1vol is allocated to usrgpr1.

4. Specify the User Group Name and unmount the virtual disk.

```
# ismadm volume umount -gdir usrgpr1
```

5. Specify the Volume Name (usrgpr1vol) for usrgpr1 and delete the virtual disk.

```
# ismadm volume delete -vol usrgpr1vol
Logical volume "usrgpr1vol" successfully removed.
```

6. Confirm the virtual disk settings.

Confirm that no virtual disk is set for usrgpr1 and that the previously used directory "/dev/sdb" is now free.

```
# ismadm volume show -disk
Filesystem      Size  Used Avail  Use% Mounted on
/dev/mapper/centos-root 16G  2.5G   13G   17% /
devtmpfs        1.9G    0   1.9G    0% /dev
tmpfs           1.9G  4.0K   1.9G    1% /dev/shm
```

```

tmpfs                1.9G  8.6M  1.9G    1% /run
tmpfs                1.9G    0  1.9G    0% /sys/fs/cgroup
/dev/sda1            497M  170M  328M   35% /boot
tmpfs                380M    0  380M    0% /run/user/0
tmpfs                380M    0  380M    0% /run/user/1001
/dev/sdb1                                (Free)

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

```

7. Restart ISM-VA.

```
# ismadm power restart
```

4.6.2 Allocation of Additional Virtual Disks to Entire ISM-VA

Using the same method as in "[3.7.1 Allocation of Virtual Disks to Entire ISM-VA](#)", you can additionally allocate multiple virtual disks to the entire ISM-VA.

4.6.3 Allocation of Additional Virtual Disks to User Groups

You can allocate virtual disks in addition to the ones you allocated according to "[3.7.2 Allocation of Virtual Disks to User Groups](#)."

The following operating example shows how to allocate an additional virtual disk to a user group named usrgpr1.

1. Connect to the virtual disk.

Carry out the operations described in Step 1 of "[3.7.2 Allocation of Virtual Disks to User Groups](#)."

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

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

```
# ismadm service stop ism
```

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

```

# ismadm volume show -disk
Filesystem          Size  Used Avail  Use% Mounted on
/dev/mapper/centos-root  16G  2.6G   13G   17% /
devtmpfs             1.9G    0   1.9G    0% /dev
tmpfs                1.9G  4.0K   1.9G    1% /dev/shm
tmpfs                1.9G  8.5M   1.9G    1% /run
tmpfs                1.9G    0   1.9G    0% /sys/fs/cgroup
/dev/sda1            497M  169M  329M   34% /boot
/dev/mapper/usrgpr1vol-lv 10G   33M   10G    1% 'RepositoryRoot' /usrgpr1
tmpfs                380M    0  380M    0% /run/user/0
/dev/sdc                                (Free)

PV          VG      Fmt  Attr PSize  PFree
/dev/sda2  centos  lvm2 a--  19.51g    0
/dev/sdb1  usrgpr1vol  lvm2 a--  10.00g    0

```

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

5. Execute the command for allocating additional virtual disks in order to allocate the added virtual disk to usrgpr1vol.

```
# ismadm volume extend -vol usrgpr1vol -disk /dev/sdc
Logical volume "/dev/mapper/usrgpr1vol-lv" resized.
```

6. Confirm the virtual disk settings.

Confirm that the newly added volume (/dev/sdc) is set for use by usrgpr1 (usrgpr1vol).

```
# ismadm volume show -disk
```

| Filesystem | Size | Used | Avail | Use% | Mounted on |
|---------------------------|------|------|-------|------|--------------------------|
| /dev/mapper/centos-root | 16G | 2.6G | 13G | 17% | / |
| devtmpfs | 1.9G | 0 | 1.9G | 0% | /dev |
| tmpfs | 1.9G | 4.0K | 1.9G | 1% | /dev/shm |
| tmpfs | 1.9G | 8.6M | 1.9G | 1% | /run |
| tmpfs | 1.9G | 0 | 1.9G | 0% | /sys/fs/cgroup |
| /dev/sda1 | 497M | 170M | 328M | 35% | /boot |
| /dev/mapper/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

4.7.1 Deployment of SSL Server Certificates

In ISM-VA, enable an SSL server certificate that was issued by an authentication authority.

1. Use FTP to transfer the SSL server certificate to ISM-VA.

Transfer destination: /Administrator/ftp

For information on how to transfer files via FTP, see "[2.1.2 FTP Access](#)."

2. From the Console as an administrator, log in to ISM-VA.
3. Deploy the SSL server certificate.

Execute the following command, specifying the "key" and "crt" files you transferred via FTP.

```
# 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 server certificate corresponding to the unique host name used inside a local network on the Linux server with the openssl command installed, with use of the following commands.

```
# openssl genrsa -rand /proc/uptime 2048 > server.key
# openssl req -new -key server.key -x509 -sha256 -days 365 -set_serial $RANDOM -extensions v3_req -out server.crt
```

- Specify an arbitrary file name for the file name of the certificate (server.key/server.crt).
- Specify the effective days of the certificate for days option.
- Specify the host name upon entering "Common Name" after executing openssl req command.

4.7.2 Display of SSL Server Certificates

You can have the SSL certificates displayed that are enabled in ISM-VA.

1. From the Console as an administrator, log in to ISM-VA.
2. Execute the command for showing the SSL server certificates.

```
# ismadm sslcert show
```

4.7.3 Export of SSL server certificates

You can export the SSL certificates that are enabled in ISM-VA.

1. From the Console as an administrator, log in to ISM-VA.
2. Execute the command for exporting the SSL server certificates.

```
# ismadm sslcert export -dir /Administrator/ftp
```

You can download the exported files via FTP.

4.8 License Settings

You can register, display, and delete server licenses and node licenses in ISM-VA.

1. From the Console as an administrator, log in to ISM-VA.
2. Execute the command for enabling licenses.

- Register license

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

- Show list of licenses

```
# ismadm license show
```

- Delete license

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



Note

After registering or deleting licenses, ISM-VA must be rebooted.

4.9 Network Settings

You can make and display the network settings.

1. From the Console as an administrator, log in to ISM-VA.
2. Execute a command for the network settings.

- Show network devices

```
# ismadm network device
```

- Modify 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 rebooted.

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
```

- Show network settings

```
# ismadm network show <LAN device name>
```

Example of command execution

```
# ismadm network show eth0
```

4.10 Event Notification Settings

You can register certificates to be used for event notifications from Monitoring and action scripts.

4.10.1 Registration of Certificates for Event Notification Mails

1. Use FTP to transfer the certificates.

Transfer destination: <User Group Name>/ftp/cert

For forwarding by FTP, see "[2.1.2 FTP Access](#)."

2. From the Console as an administrator, log in to ISM-VA.
3. Execute the command for registering certificates for event notification mails.

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

4.10.2 Registration of Action Scripts

1. Use FTP to transfer the scripts.

Transfer destination: <User Group Name>/ftp/actionscript

For forwarding by FTP, see "[2.1.2 FTP Access](#)."

2. From the Console as an administrator, log in to ISM-VA.

3. Execute the command for registering action scripts.

```
# ismadm event import -type script
```

4.10.3 Display of Certificates for Event Notification Mails

You can have the certificates for event notification mails displayed that are registered in ISM-VA.

```
# ismadm event show -type cert
```

4.10.4 Display of Action Scripts

You can have the action scripts displayed that are registered in ISM-VA.

```
# ismadm event show -type script
```

4.10.5 Deletion of Certificates for Event Notification Mails

You can delete the certificates for event notification mails that are registered in ISM-VA.

```
# ismadm event delete -type cert -file <Certificate file> -gid <User Group Name>
```

4.10.6 Deletion of Action Scripts

You can delete the action scripts that are registered in ISM-VA.

```
# ismadm event delete -type script -file <Script file> -gid <User Group Name>
```

4.11 ISM-VA Service Control

This function can stop and restart ISM--VA as well as control the services that run internally.

1. From the Console as an administrator, log in to ISM-VA.
2. Execute a command for controlling the ISM-VA service.

- Restart ISM--VA

```
ismadm power restart
```

- Stop ISM--VA

```
ismadm power stop
```

- Show list of internal services

```
ismadm service show
```

- Start internal service individually

```
ismadm service start <Service name>
```

Example of command execution: Start FTP server individually

```
# ismadm service start vsftpd
```

- Stop internal service individually

```
ismadm service stop <Service name>
```

Example of command execution: Stop FTP server individually

```
# ismadm service stop vsftpd
```

- Restart internal service individually

```
ismadm service restart <Service name>
```

Example of command execution: Restart FTP server individually

```
# ismadm service restart vsftpd
```

- Show status of internal service individually

```
ismadm service status <Service name>
```

Example of command execution: Display FTP server status individually

```
# ismadm service status vsftpd
```

- Enable internal service individually

```
ismadm service enable <Service name>
```

Example of command execution: Enable FTP server individually

```
# ismadm service enable vsftpd
```

- Disable internal service individually

```
ismadm service disable <Service name>
```

Example of command execution: Disable FTP server individually

```
# ismadm service disable vsftpd
```

4.12 Display of System Information

You can have the internal system information of ISM-VA displayed from the console.

1. From the Console as an administrator, log in to ISM-VA.
2. Execute the command for displaying the system information.

```
# ismadm system show
ISM Version      : <Version>
GUI Port Number  : 25566
Hostname         : localhost
Log Level        : small
```

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

4.13 Modification of Host Names

You can modify the host name of ISM-VA.

1. From the Console as an administrator, log in to ISM-VA.
2. Execute the command for modifying the host name.

```
# ismadm system modify -hostname ismva2
You need to reboot the system to enable the new settings.
Immediately reboots the system. [y/n]:
```



Note

- Enter the host name in lowercase letters.
- After executing the command, a reboot is required.
- To modify the default host name "localhost", you have to follow the procedure described in "[4.7 Certificate Activation](#)" and deploy a certificate in ISM-VA that corresponds to the modified host name.

4.14 Application of Patches

You can apply patches to ISM-VA.

1. Transfer the patch files to ISM-VA via FTP.

Transfer destination: /Administrator/ftp

For information on how to transfer files via FTP, see "[2.1.2 FTP Access](#)."

Forward the correction file in binary mode.

2. From the Console as an administrator, log in to ISM-VA.
3. In order to apply patches, stop the ISM service temporarily.

Stop the ISM service according to the procedure described in "[4.1.4 Start Up and Stop of ISM Service](#)."

4. Execute the command for applying patches.

Execute the following command, specifying the patch file.

```
# ismadm system patch-add -file <Patch file>
```

Example of command execution

```
# ismadm system patch-add -file /Administrator/ftp/SVISM_V200S20160606-02.tar.gz
```

5. After applying the patch, restart ISM-VA.

```
# ismadm power restart
```

4.15 Operation of Plug-in

You can apply and delete plug-in to/from ISM-VA, and display the plug-in applied to ISM-VA.

4.15.1 Application of Plug-in

1. Transfer the plug-in files to ISM-VA via FTP.

Transfer destination: /Administrator/ftp

For information on how to transfer files via FTP, see "[2.1.2 FTP Access](#)."

Forward the plug-in file in binary mode.

2. From the Console as an administrator, log in to ISM-VA.
3. In order to apply plug-in, stop the ISM service temporarily.

Stop the ISM service according to the procedure described in "[4.1.4 Start Up and Stop of ISM Service](#)."

4. Execute the command for applying plug-in.

Execute the following command, specifying the plug-in file.

```
# ismadm system plugin-add -file <Plug-in file>
```


Example of command execution

```
# ismadm system plugin-add -file /Administrator/ftp/FJSVsvism-ext-1.0.0-10.tar.gz
```

5. After applying the plug-in, restart ISM-VA.

```
# ismadm power restart
```

4.15.2 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.



Point

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 number of ISM-VA.

Plugin displays the applied plug-in name and its version.

4.15.3 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 ["4.15.2 Display of Plug-in."](#)

Example of command execution

```
# ismadm system plugin-del -name FJSVsvism-ext
Uninstall plugin <FJSVsvism-ext 1.0.0> ?
[y/n]:
```

After executing the command the uninstall plug-in confirmation screen is displayed.

2. Enter [y] to finalize the uninstallation.
3. After plug-in deletion, restart ISM-VA.

```
# ismadm power restart
```

4.16 Switch of Trouble Investigation Logs

You can switch whether to export a log to be used when investigating troubles.

1. From the Console as an administrator, log in to ISM-VA.

2. Execute the command for switching the log export for trouble investigation on and off.

- Enable log export

```
# ismadm system set-debug-flag 1
```

- Disable log export

```
# ismadm system set-debug-flag 0
```

4.17 Switch of Levels of Trouble Investigation Logs

You can switch export levels for logs to be used when investigating troubles.

Switching the export level allows you to limit the sizes of logs to be exported.

| Log level | Approximate size of log to be exported |
|-----------------|--|
| small (default) | 10GB |
| medium | 40GB |
| large | 100GB |



Note

- Switching is available only from a lower to a higher level.
- After switching the log level, ISM-VA must be rebooted.

1. From the Console as an administrator, log in to ISM-VA.

2. Stop the ISM service.

Stop the ISM service according to the procedure described in "4.1.4 Start Up and Stop of ISM Service."

3. Execute the command for switching the level of the log for trouble 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 trouble 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 number 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 trouble investigation is effective.

4.18 DHCP Server inside ISM-VA

You can use ISM-VA as a DHCP server by starting the DHCP services inside ISM-VA.

A DHCP server is required when using the profile management function for OS installation. It is possible to either use an external DHCP server or to use the procedure below to set up ISM as a DHCP server and to use that. (In this case you can select which DHCP server is used according to the operating procedure described in "[4.18.4 Switch of DHCP Servers.](#)")

If you use only the external DHCP server, the following settings are not required.

4.18.1 Settings for DHCP Server inside ISM-VA

Set up the DHCP server inside ISM-VA. 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 of stopping and starting DHCP services, see "[4.18.2 Operation of DHCP Service inside ISM-VA.](#)"

To set up a DHCP server, you have two methods. Set up the DHCP server with the either method 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 by 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.

Specifying the following parameters is required. You cannot omit them.

-subnet

-netmask

-start

-end

-broadcast

Example of command execution

```
# ismadm dhcpsrv set-simple -subnet 192.168.1.0 -netmask 255.255.255.0 -start 192.168.1.150 -end
192.168.1.160 -broadcast 192.168.1.255 -dns 192.168.1.200 -gw 192.168.1.250

----- New Configuration -----
ddns-update-style none;
default-lease-time 86400;
max-lease-time 259200;

shared-network LOCAL-NET {
    subnet 192.168.1.0 netmask 255.255.255.0 {
```

```

range 192.168.1.150 192.168.1.160;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.1.255;
option vendor-class-identifier "PXEClient";
option domain-name-servers 192.168.1.200;
option routers 192.168.1.250;
    }
}

```

```

-----
Update DHCP configuration ? (Current settings are discarded)
[y/n]:

```

When command execution is complete, a message for confirming the value that you have set is displayed; enter "y" to confirm the setting.

Setup by conf file

Upload the conf file with description by using the ftp function of ISM-VA and feed the file with the command.

For forwarding by FTP, see "[2.1.2 FTP Access](#)."

```
# ismadm dhcpd set -file <conf file>
```

Example of command execution

```
# ismadm dhcpd set -file /Administrator/ftp/dhcpd.conf.new
```

4.18.2 Operation of DHCP Service inside ISM-VA

You can start and stop the DHCP services inside ISM-VA and display their statuses.

- Confirming DHCP service status

```
# ismadm service status dhcpd
```

Command output

```

Active: active (running) :DHCP service active status
Active: inactive (dead)  :DHCP service inactive status
/usr/lib/systemd/system/dhcpd.service; enable;    :Settings to enable when booting ISM-VA
/usr/lib/systemd/system/dhcpd.service; disabled;  :Settings not to enable when booting ISM-VA

```

- Manual startup of DHCP services

```
# ismadm service start dhcpd
```



Note

- Set up for the DHCP server before you start the DHCP services inside ISM-VA.

For information on how to setup DHCP servers, see "[4.18.1 Settings for DHCP Server inside ISM-VA](#)."

- When the DHCP server is in "dead" state even in active settings, confirm if an error is shown with "[4.18.3 Confirmation of DHCP Server Information inside ISM-VA](#)" - "Display of the DHCP server message."

- Manual stop of DHCP services

```
# ismadm service stop dhcpd
```

- Setup to enable DHCP services upon startup of ISM-VA

```
# ismadm service enable dhcpd
```

- Setup not to enable DHCP services upon startup of ISM-VA

```
# ismadm service disable dhcpd
```

4.18.3 Confirmation of DHCP Server Information inside ISM-VA

You can display DHCP server information inside ISM-VA.

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 setting contents (conf file) to the location where ftp access is possible

```
# ismadm dhcpdsvr export-conf -dir /Administrator/ftp
```

- Export a sample setting content (conf file) to the location where ftp access is possible

```
# ismadm dhcpdsvr export-sample -dir /Administrator/ftp
```

4.18.4 Switch of DHCP Servers

When you use a DHCP server in Profile function, you can switch to select whether to use the DHCP server inside ISM-VA or use the outside DHCP server.

- Display of the current setting

```
# ismadm dhcpdsvr show-mode
```

Command output

```
DHCP mode: local    : DHCP server inside ISM-VA is used in Profile function.
DHCP mode: remote  : The outside DHCP server is used in Profile function.
```

- Switching of the settings

- Setting up so that Profile is assigned with use of the DHCP server inside ISM-VA

```
# ismadm dhcpdsvr set-mode local
```

- Setting up so that Profile is assigned with use of the outside DHCP server

```
# ismadm dhcpdsvr set-mode remote
```

4.19 MIB File Settings

You can import MIB files that allow you to execute arbitrary Trap Reception in ISM-VA.

4.19.1 Registration of MIB Files

1. Transfer an MIB file via FTP.

Transfer destination: /Administrator/ftp/mibs

For the transfer method via FTP, see "[2.1.2 FTP Access](#)."

2. From the Console as an administrator, log in to ISM-VA.
3. Execute MIB file registration command.

```
# ismadm mib import
```

4.19.2 Display of MIB Files

You can display the MIB files registered on ISM-VA.

```
# ismadm mib show
```

4.19.3 Deletion of MIB Files

You can delete the MIB files registered on ISM-VA.

```
# ismadm mib delete -file <MIB file name>
```

4.20 Upgrade of ISM-VA

ISM-VA can be upgraded.

1. Transfer the upgrade files to ISM-VA via FTP.

Transfer destination: /Administrator/ftp

For information on how to transfer files via FTP, see "[2.1.2 FTP Access](#)."

2. From the Console as an administrator, log in to ISM-VA.
3. In order to execute upgrade, stop the ISM service temporarily.

Stop the ISM service according to the procedure described in "[4.1.4 Start Up and Stop of ISM Service](#)."

4. Execute the upgrade command.

Execute the following command, specifying the upgrade file.

```
# ismadm system upgrade -file <Upgrade files>
```

Example of command execution

```
# ismadm system upgrade -file /Administrator/ftp/ISM220_S2017xxxx-01.tar.gz
```

5. After executing the upgrade, restart ISM-VA.

```
# ismadm power restart
```

Chapter 5 Maintenance of Nodes

This chapter describes the maintenance of nodes.

5.1 Maintenance Mode

If you have to perform maintenance of a node after detecting a failure, it is recommended that you switch the affected node into Maintenance Mode within ISM.

As alarm detection and background processing in ISM is restricted for nodes that are switched into Maintenance Mode, this prevents alarms from being issued repeatedly for the 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. |
| Collection of node information | Collection of node information, which is periodically executed by ISM, is stopped. If required, collect the node information manually. |
| Node log collection | Scheduled log collections are skipped. If required, collect the node logs manually. |

Point

During Maintenance Mode, all functions other than those stated above remain available. For example, while a node is in Maintenance Mode, you can still execute the following operations:

- Assignment, reassignment, and release of profiles
- Firmware updates
- Manual collection of node information
- Manual collection of node logs

Setup Procedure for Maintenance Mode

1. Open the Details of Node screen.
2. Select the [Actions] button and select [Set into 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. Select the [Actions] button and select [Disable Maintenance Mode].

Note

- Enable/disable Maintenance Mode for PRIMEQUEST also enables/disables maintenance mode for the partitions and extension partitions under it. You can not specify a partition or extension partition and enable/disable maintenance.
- Enable/disable maintenance mode for 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], it is required to access and investigate the respective devices directly.

Appendix A Uninstallation of ISM-VA

Uninstall ISM-VA according to the installation destination.

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

- [Uninstalling from Microsoft Windows Server Hyper-V](#)
- [Uninstalling from VMware vSphere Hypervisor 5.5 or VMware vSphere Hypervisor 6.0](#)
- [Uninstalling from VMware vSphere Hypervisor 6.5](#)
- [Uninstalling from KVM](#)

Uninstalling from Microsoft Windows Server Hyper-V

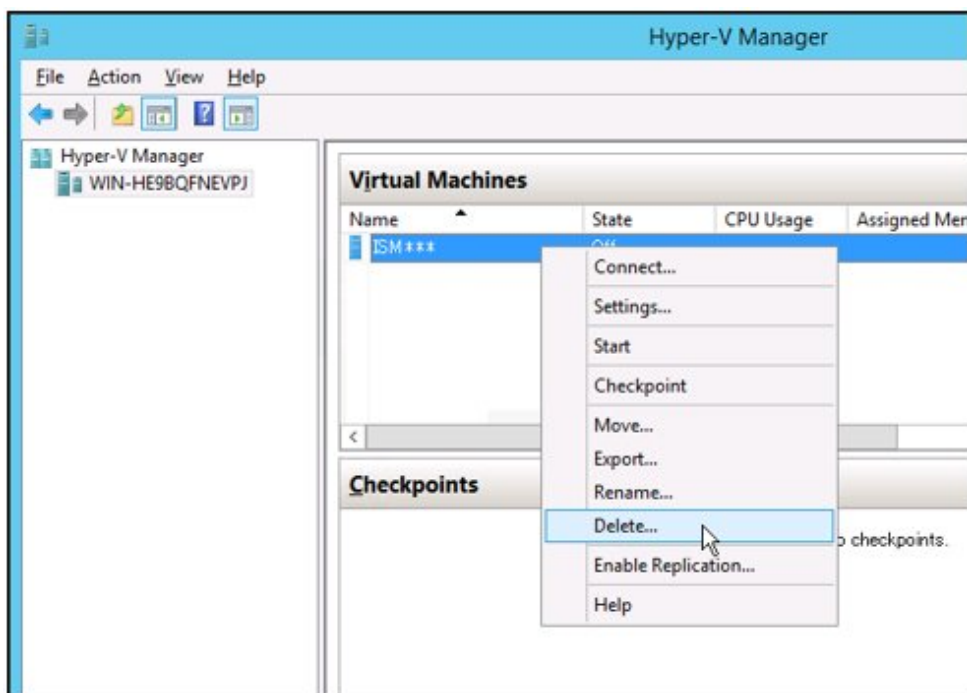
1. Stop ISM-VA.

See "[4.1.2 Termination of ISM-VA](#)" for details.

2. Start Hyper-V Manager, right-click on the installed ISM-VA, and then select [Settings].

Take a memo of the displayed storage location of the virtual hard disk that is allocated to the ISM-VA and of the corresponding file name.

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



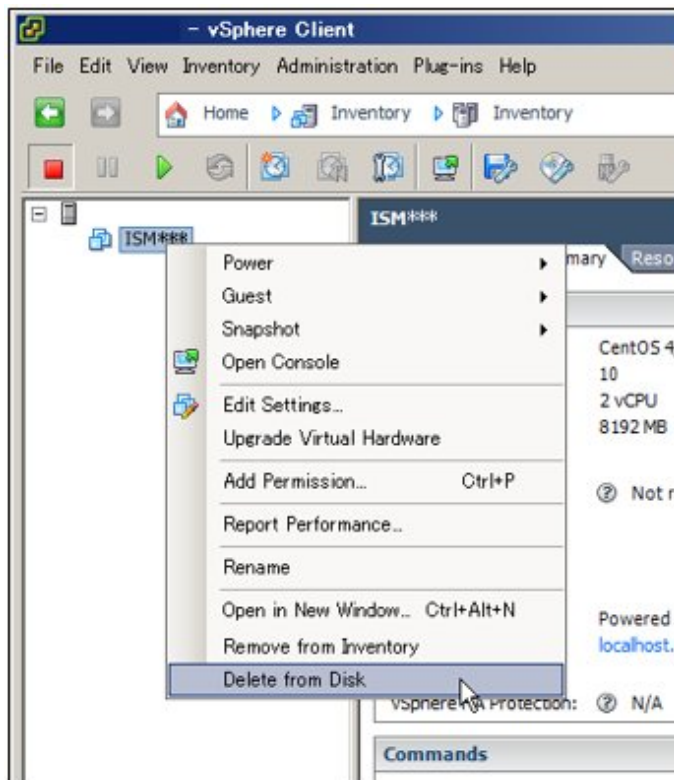
4. Use Explorer to remove the virtual hard disk for which you took the memo in Step 2.

Uninstalling from VMware vSphere Hypervisor 5.5 or VMware vSphere Hypervisor 6.0

1. Stop ISM-VA.

See "[4.1.2 Termination of ISM-VA](#)" for details.

2. Start vSphere Client, right-click on the installed ISM-VA, and then select [Delete from Disk].

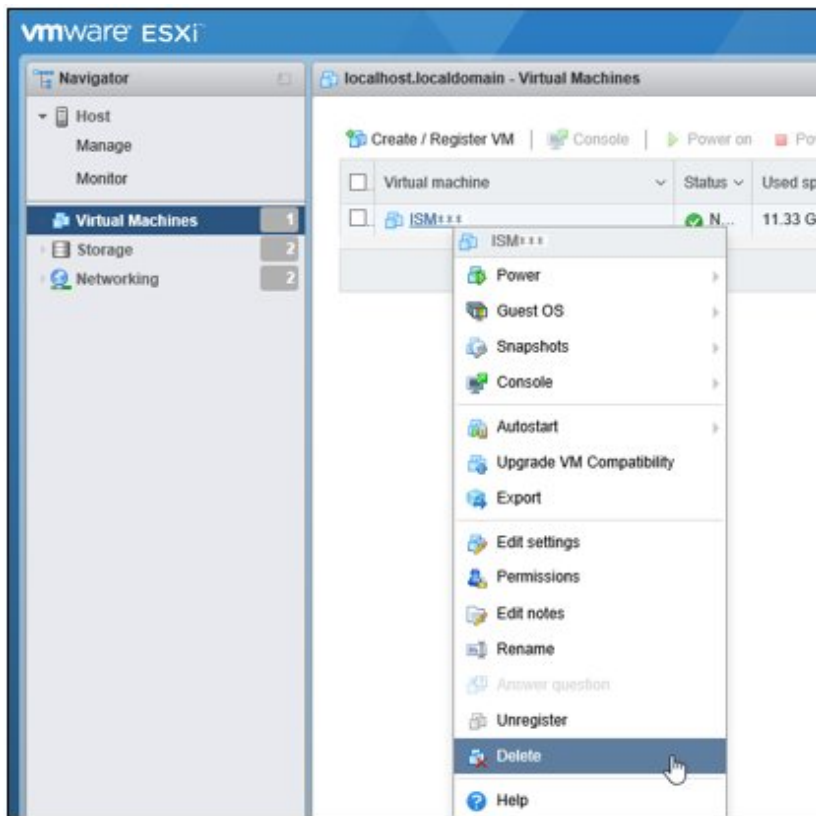


Uninstalling from VMware vSphere Hypervisor 6.5

1. Stop ISM-VA.

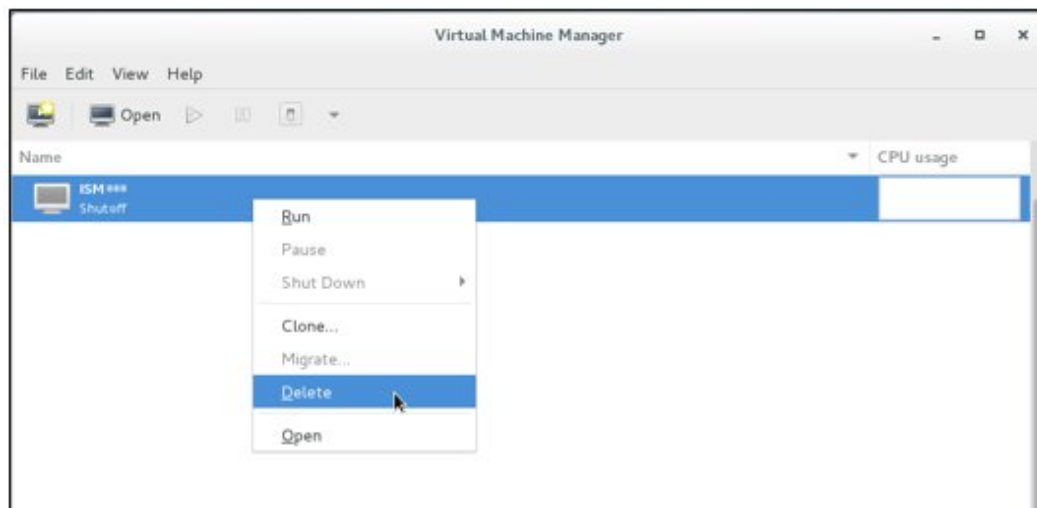
See "[4.1.2 Termination of ISM-VA](#)" for details.

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



Uninstalling from KVM

1. Stop ISM-VA.
See "[4.1.2 Termination of ISM-VA](#)" for details.
2. Start Virtual Machine Manager, right-click on the installed ISM-VA, and then select [Delete].



Appendix B Troubleshooting

This appendix describes the major causes and recovery methods for errors and unexpected behavior in ISM operation.

For items that are not described here and for details on causes and recovery methods, access your local support.

Symptom: Registration of a manually discovered node fails.

Causes and recovery methods

Check the serial number of the discovered node. If the node is already registered, delete the node and register it again.

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] - [Select] button
- From [Structuring] - [Firmware], select [Import] from the menu in the bottom left part of the screen, then select the [Firmware] - [Import Data List] - [Actions] - [Import DVD] - [Select] button.
- From [Structuring] - [Firmware], select [Import] from the menu in the bottom left part of the screen, then select the [Firmware] - [Import Data List] - [Actions] - [Import Firmware] - [Select] button.
- From [Structuring] - [Firmware], select [Import] from the menu in the bottom left part of the screen, then select the [ServerView Suite] - [Actions] - [Import DVD] - [Select] button.

Causes and recovery methods

- Confirm the files in the FTP folder and subfolders for the user group to which the user belongs; the files names should not contain any character coding other than UTF-8.
- Confirm the current status of data communication between ISM and the client.

Symptom: Failure in confirming status and control of node

Causes and recovery methods

- Confirm that the network between the target node and ISM is operating correctly.
- Confirm whether the power cable is connected to the respective device and whether power is supplied.
- Confirm whether the IP address registered in ISM matches that of the respective device (or OS). Especially after modifying any IP addresses, you should confirm that you did not forget to change the registration information in ISM.
- Check whether the user accounts registered in ISM match those in the respective device (or OS). Especially after modifying any passwords, you should confirm that you did not forget to change the registration information in ISM.
- Confirm that no other ISM function is being in use for the node to be manipulated with ISM (for example, starting a profile assignment while a firmware update is in progress).

Symptom: File downloads fail when using Internet Explorer 11.

Causes and recovery methods

File downloads may fail depending on your Internet Explorer settings. Modify your settings as follows:

On the [Internet Options] - [Security] tab, select the [Custom level] button and change the setting for [Downloads] - [File download] to [Enable].

Symptom: Fails to register Microsoft Active Directory as LDAP server settings.

Causes and recovery methods

When you register Active Directory registered a large number of user information (for example, 1,000 or more), check that environment variable called "MaxPageSize" in Active Directory has the value according to the registered user information.

Firmware Management

Symptom: The firmware to be updated cannot be specified when making operations for a firmware update.

Causes and recovery methods

- It is required that Firmware data must be imported and loaded in advance. If you have not imported them yet, carry out an import first.
- If you are importing firmware individually and there is a mistake 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 mistakes, 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 numbers of the current version on the node and of the firmware you imported.

Symptom: Online Update of the PCI card fails

Causes and recovery methods

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. See 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 recovery methods

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 recovery methods

Possibly, the conditions for enabling the Update Mode are not fulfilled.

See 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 recovery methods

- When using Offline Update it is required that the ServerView Suite DVD or the ServerView Suite Update DVD has been imported. Confirm that the ServerView Suite DVD or the ServerView Suite Update DVD has been imported.
- Possibly, there is a problem with the environment settings for running PXE boot. Confirm the following:
 - Whether DHCP servers are able to lease appropriate IP addresses
 - Whether, by any mistake, 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-VA

Profile Management

Symptom: An error occurs in assigning, reassigning, or release a profile on a PRIMERGY server.

Causes and recovery methods

You made the profile assignment operation with the power of the target node being on. For profile assignment on PRIMERGY units, be sure to make 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 recovery methods**

Making these settings from ISM may sometimes result in an error when there are ongoing connections to the target node from sources other than ISM over 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 the Profile function.**Causes and recovery methods**

- 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 number 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 number of the DVD to be used within the profile.
- Possibly, there is a problem with the environment settings for running PXE boot. Confirm the following:
 - Whether DHCP servers are able to lease appropriate IP addresses
 - Whether, by any mistake, 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-VA

Symptom: An error occurs when importing an exported profile or policy.**Causes and recovery methods**

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 recovery methods**

In order to retrieve and display connection information with ISM, it is first required to enable the LLDP function of each node. Enable LLDP with reference to the instruction manual or other documentation for the node. For nodes that support no LLDP, set up the connection information manually on the ISM screen.

Symptom: The information displayed on the Network Map is outdated or incorrect.**Causes and recovery methods**

- The contents displayed on the Network Map are equivalent to the information at the time you last executed [Refresh network information] on the GUI screen. Execute [Refresh network information].
- Whenever an item such as the port status of a node has changed, execute [Get Node Information] and then [Refresh network information].

Symptom: The virtual connection relationships are not displayed on the Network Map or there are mistakes in the displayed contents.**Causes and recovery methods**

To display the connection relationships between the virtual switches and the virtual machines, it is required to 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 recovery methods

- It is required that the network switch to be set can be accessed 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 recovery methods

- It is required that the network switch to be set can be accessed 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 differ. Check the device requirements to see if the LAG Name and Mode can be set.

Log Management

Symptom: Node logs of a node are collected incorrectly or not at all.

Causes and recovery methods

- When you have newly registered a node, log collection is not yet set to be executed. Set a schedule for log collection under [Log Settings].
- If the status on the [Log 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>) the archived log for the user group(<user group name>) reached the capacity(xxMB) set for log retention."
 - "During log collection for node(<node name>) the node log (download data) for the user group(<user group name>) reached the capacity(xxMB) set for log retention."
 - "During log collection for node(<node name>) the node log (log discovery data) reached the capacity(xxMB) set for log retention."

Symptom: Settings for node log collection log collection of a node cannot be made.

Causes and recovery methods

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 recovery methods

- When the OS information of a target node is not registered yet, or not yet obtained by 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.

Appendix C Profile Setting Items

C.1 BIOS/iRMC Setting Items of Profiles for PRIMERGY Servers

This section describes the items that you can set up with BIOS/iRMC tab, in profiles. You find some items that you are unable to set up or some items with different setting contents, depending on your server types. Therefore, set up your servers within the scope of support.

You can select Enable or Disable individually for the setting items in profiles. When you disable a setting item, the disabled item is not changed even after assigning the profile.

There are some cases where profiles and setting items on the actual device type may differ. For details of each item, see the manual of the target servers and apply settings to the items corresponding to the profile.

BIOS tab






| Item Name | | | Description | Parameter | |
|----------------------|---|--|---|--|--|
| CPU Configuration | | | | | |
| | Execute Disable Bit (Enabled/Disabled) | | This specifies Execute Disable Bit behavior of a CPU. Depending on the manual, this function is described as XD (eXecute Disable) bit or NX (No eXecute) bit. | Enabled=Function made available Disabled=Function disabled | |
| | Hyper-Threading (Enabled/Disabled) | | This specifies Hyper Threading Technology behavior of a CPU. When a CPU that is not equipped with the function is mounted, this setting is ignored. | Enabled=Function made available Disabled=Function disabled | |
| | Intel Virtualization Technology (Enabled/Disabled) | | This specifies virtualization support function behavior of a CPU. | Enabled=Function enabled Disabled=Function disabled | |
| | Intel (R) VT-d (Enabled/Disabled) | | This specifies Virtualization Technology for Directed I/O function behavior of a CPU. | Enabled=Function enabled Disabled=Function disabled | |
| | Power Technology (Energy Efficient/Customize/Disabled) | | This sets up the power source management behavior of a CPU. | Energy Efficient=Behavior optimized for power-saving Custom=Detailed behavior setup by using additional setting items. Disabled=Power source management function disabled | |
| | | Enhanced SpeedStep (Enabled/Disabled) | | This is the item you can set up only when Power Technology is Custom. This specifies EIST (Enhanced Intel SpeedStep Technology) behavior of a CPU. | Enabled=Function enabled Disabled=Function disabled |
| | | | Turbo Mode (Enabled/Disabled) | This is the item you can set up only when Enhanced SpeedStep is Enabled. This specifies Turbo Boost Technology behavior of a CPU. When a CPU that is not equipped with the function is mounted, this function is set to (Disabled) regardless of this setting. | Enabled=Function enabled Disabled=Function disabled |
| Memory Configuration | | | | | |
| | DDR Performance | | Memory modules operate with different speeds (Frequencies). The faster the speed | Low-Voltage optimized=The fastest setting available with low voltage | |




| Item Name | | Description | Parameter |
|------------------------------|---|---|---|
| | (Low-Voltage optimized/Energy optimized/Performance optimized) | the higher the performance. The slower the speed the more the power saved. The available memory speeds differ depending on the attached memory module configurations | Energy optimized=The slowest setting available with power-saving Performance optimized=The fastest setting available for achieving the highest performance |
| | Numa (Enabled/Disabled) | This specifies whether to use NUMA (Non-Uniform Memory Access) function. This is rendered meaningless when a multiprocessor configuration is not employed. | Enabled=NUMA function enabled Disabled=NUMA function disabled |
| Onboard Device Configuration | | | |
| | Onboard SAS/SATA (SCU) (Enabled/Disabled) | This specifies Onboard SAS/SATA storage controller unit (SCU) behavior. | Enabled=SCU enabled Disabled=SCU disabled |
| | SAS/SATA OpROM (Enabled/Disabled) | This item can be set up only when Onboard SAS/SATA (SCU) is Enabled. It specifies the Option ROM behavior of SAS/SATA controller. | Enabled=Option ROM enabled Disabled=Option ROM disabled |
| | SAS/SATA Driver (LSI MegaRAID/Intel RSTe) | This item can be set up only when SAS/SATA OpROM is Enabled. It specifies the Option ROM type of SAS/SATA controller. | LSI MegaRAID=Option ROM for Embedded MegaRAID used Intel RSTe=Option ROM for Intel RSTe used |
| Option ROM Configuration | | | |
| | Launch Slot X OpROM (Enabled/Disabled) | This specifies the execution of extended ROM of the option card mounted on each PCI slot. You can specify this for multiple slots, in profile. Do not specify this for the slot that does not exist on an actual device. | Enabled=Extended ROM executed Disabled=Extended ROM not executed |
| CSM Configuration | | | |
| | Launch CSM (Enabled/Disabled) | This specifies whether to execute CSM (Compatibility Support Module). Your legacy operating system can be booted only when CSM is loaded. | Enabled=CSM executed Disabled=CSM not executed |
| | Boot Option Filter (UEFI and Legacy / UEFI only / Legacy only) | This specifies which drive can be booted first. | UEFI and Legacy=Bootable from UEFI OS drive and Legacy OS drive UEFI only=Bootable only from UEFI OS drive Legacy only=Bootable only from Legacy OS drive |
| | Launch Pxe OpRomPolicy (UEFI only / Legacy only / Do not launch) | This specifies the PXE Option ROM to be boot. For PXE boot, there are available normal (Legacy) PXE boot and UEFI PXE boot. | UEFI only=UEFI Option ROM only booted Legacy only=Legacy Option ROM only booted Do not launch=Option ROM not booted |





| Item Name | | Description | Parameter |
|---------------|---|--|---|
| | Launch Storage OpRomPolicy (UEFI only / Legacy only / Do not launch) | This specifies Storage Option ROM to be booted. | UEFI only=UEFI Storage Option ROM only booted Legacy only=Legacy Storage Option ROM only booted Do not launch=Storage Option ROM not booted |
| | Other PCI Device Rom Priority (UEFI only / Legacy only) | This specifies the Option Rom booted with the devices other than a network, mass storage device and video. | UEFI only=UEFI Option ROM only booted Legacy only=Legacy Option ROM only booted |
| Network Stack | | | |
| | Network Stack (Enabled/Disabled) | This sets up whether UEFI Network Stack can be used for network access on UEFI. | Disabled=Use of UEFI network stack not permitted Enabled=Use of UEFI network stack permitted |
| | IPv4 PXE Support (Enabled/Disabled) | This specifies whether PXE UEFI Boot via IPv4 can be used with UEFI mode. | Disabled=Use of PXE UEFI Boot via IPv4 not permitted Enabled=Use of PXE UEFI Boot via IPv4 permitted |
| | IPv6 PXE Support (Enabled/Disabled) | This specifies whether PXE UEFI Boot via IPv6 can be used with UEFI mode. | Disabled=Use of PXE UEFI Boot via IPv6 not permitted Enabled=Use of PXE UEFI Boot via IPv6 permitted |



iRMC tab




| Item Name | | Description | Parameter |
|------------------|--|--|---|
| iRMC GUI | | | |
| | Default Language (English/German/Japanese) | This performs initial settings for languages. This is enabled from the next time iRMC Web interface is invoked. | English=English by default German=German by default Japanese=Japanese by default |
| Power Management | | | |
| | POST Error Halt (Continue/Halt on error) | This sets up the operation in response to the occurrence of an error upon server boot. | Continue=Boot continued even after the occurrence of an error Halt on error=Boot interrupted until the key entry when an error occurs |
| | Power Restore Policy (Restore to powered state prior to power loss/Always power off/ Always power on) | This sets up the power source operation upon power restore operation after interruption of AC power source input. | Restore to powered state prior to power loss=State upon power source interruption maintained (Powered on if a server is powered on upon interruption/ Not powered on if the server is powered off.) Always power off=Always powered off Always power on=Always powered on |
| | Power Control Mode (OS Controlled/Minimum Power) | This sets up the power-saving and noise canceling operations for a server. | OS Controlled=Control by OS followed |

| Item Name | Description | Parameter |
|-------------------|--|---|
| |  Note When you disable Enhanced SpeedStep on BIOS settings, this setting also becomes disabled. | Minimum Power=Operation where priority is placed on reduction in power consumption (Schedule)=Setup by Profile Management unavailable (Power capping)=Setup by Profile Management unavailable |
| Fan Test | | |
| Fan Check Time | This becomes enabled when executing fan tests. | Enter the start time of fan test. |
| Disable Fan Test | This sets up whether to conduct periodical fan diagnoses. | (Checked)=Fan tests not conducted (Unchecked)=Tests conducted every day at the specified time |
| Software Watchdog | | |
| Software Watchdog | This specifies whether to use software watchdog to perform periodic communication confirmations while an OS is running.  Note This setting becomes enabled after rebooting the server. | (Checked)=Communication monitored (Unchecked)=Communication not monitored |
| Behavior | This specifies the behavior for the case where communication is disabled.  Note This setting becomes enabled after rebooting the server. | Select the item from the pulldown menu. Continue=Nothing executed Reset=Server rebooted Power cycle=Powered ON after powering OFF the server once |
| Time out time | This specifies the period for judging communication to be disabled.  Note This setting becomes enabled after rebooting the server. | Specify the value from 1 to 100 minutes. |
| Boot Watchdog | | |
| Boot Watchdog | This specifies whether to monitor the period between POST completion and OS start, with use of Boot Watchdog.  Note This setting becomes enabled after rebooting the server. | (Checked)=Period monitored (Unchecked)=Period not monitored |
| Behavior | This specifies behavior for the case where an OS does not start within the specified time. | Select the item from the pulldown menu. |

| Item Name | | Description | Parameter |
|--------------------------------------|---------------|--|---|
| | |  Note This setting becomes enabled after rebooting the server. | Continue=Nothing executed Reset=Server rebooted Power cycle=Powered ON after powering OFF the server once |
| | Time out time | This specifies the period for judging that an OS has failed to start.  Note This setting becomes enabled after rebooting the server. | Specify the value from 1 to 100 minutes. |
| Time | | | |
| Time Mode (System RTC/NTP Server) | | This specifies whether to obtain the time setting of iRMC from a managed server or to obtain it from an NTP server. | System RTC=Time of iRMC obtained from the system clock of a managed server NTP Server=Time of iRMC synchronized with that of an NTP server which operates based on specific time as its reference time source by using Network Time Protocol (NTP) |
| RTC Mode (Local Time/UTC) | | You can select whether to display iRMC time in UTC (Coordinated Universal Time) format or in local time format. | Local Time=iRMC time displayed in local time format UTC=iRMC time displayed in UTC (Coordinated Universal Time) format |
| NTP Server 0 | | This specifies the IP address or the DNS name of the primary NTP server. | Enter the IP address or DNS strings. |
| NTP Server 1 | | This specifies the IP address or the DNS name of the secondary NTP server. | Enter the IP address or DNS strings. |
| Time Zone | | You can set up the time zone corresponding to the location where the server is placed. | Select the item from the pulldown menu. |
| Ports and Network Services Settings | | | |
| Telnet Enabled | | This specifies whether to enable Telnet connection. | (Checked)=Telnet connection enabled (Unchecked)=Telnet connection disabled |
| Telnet Port (Default: 3172) | | This specifies Telnet port number of iRMC. | Enter the port number. 3172 by default |
| SSH Enabled | | This specifies whether to enable ssh connection. | (Checked)=ssh connection enabled (Unchecked)=ssh connection disabled |
| SSH Port (Default: 22) | | This specifies Telnet port number of ssh. | Enter the port number. 22 by default |
| SNMP Generic Configuration | | | |
| SNMP Enabled | | This specifies whether to enable SNMP.  Note You cannot set up the setting items that are not shown on the Web UI screen of iRMC. | Enabled=SNMP enabled Disabled=SNMP disabled |

| Item Name | Description | Parameter |
|--|--|--|
| | Depending on the firmware versions, you cannot set up some setting items even though the setting items are shown on the Web UI screen of iRMC. Disable the setting items if you fail to assign a profile. | |
| SNMP Port (Default: 161) | This specifies a port where an SNMP service is in an idle state.  Note You cannot set up the setting items that are not shown on the Web UI screen of iRMC. Depending on the firmware versions, you cannot set up some setting items even though the setting items are shown on the Web UI screen of iRMC. Disable the setting items if you fail to assign a profile. | Enter the port number. UDP 161 by default |
| SNMP Service Protocol (All (SNMPv1/v2c/v3)/Only SNMPv3) | This specifies the protocol of SNMP services.  Note You cannot set up the setting items that are not shown on the Web UI screen of iRMC. Depending on the firmware versions, you cannot set up some setting items even though the setting items are shown on the Web UI screen of iRMC. Disable the setting items if you fail to assign a profile. | All (SNMPv1/v2c/v3)=All protocols (SNMPv1/v2c/v3) supported Only SNMPv3=Only SNMPv3 supported |
| SNMP v1/v2c Community | This specifies the community strings in the cases of SNMP v1/v2c.  Note You cannot set up the setting items that are not shown on the Web UI screen of iRMC. Depending on the firmware versions, you cannot set up some setting items even though the setting items are shown on the Web UI screen of iRMC. Disable the setting items if you fail to assign a profile. | |
| SNMPv3 User Configuration | | |
| SNMPv3 Enabled (Enabled/Disabled) | This specifies whether to enable SNMPv3 support for users.  Note - To create/change SNMPv3 users, it is required to enable SNMP with the Network Settings -> SNMP. | Enabled=SNMPv3 support enabled Disabled=SNMPv3 support disabled |

| Item Name | Description | Parameter |
|----------------------------------|---|--|
| | <ul style="list-style-type: none"> - To use SNMPv3, it is required to set a password with at least 8 characters. - You cannot set up the setting items that are not shown on the Web UI screen of iRMC. Depending on the firmware versions, you cannot set up some setting items even though the setting items are shown on the Web UI screen of iRMC. Disable the setting items if you fail to assign a profile. | |
| SNMPv3 Access Privilege | <p>This specifies users' access privilege.</p> <p> Note</p> <ul style="list-style-type: none"> - To create/change SNMPv3 users, it is required to enable SNMP with the Network Settings -> SNMP. - To use SNMPv3, it is required to set a password with at least 8 characters. - You cannot set up the setting items that are not shown on the Web UI screen of iRMC. Depending on the firmware versions, you cannot set up some setting items even though the setting items are shown on the Web UI screen of iRMC. Disable the setting items if you fail to assign a profile. | Always read-only |
| Authentication (SHA/MD5/None) | <p>This selects the authentication protocol that SNMPv3 uses for authentication.</p> <p> Note</p> <ul style="list-style-type: none"> - To create/change SNMPv3 users, it is required to enable SNMP with the Network Settings -> SNMP. - To use SNMPv3, it is required to set a password with at least 8 characters. - You cannot set up the setting items that are not shown on the Web UI screen of iRMC. Depending on the firmware versions, you cannot set up some setting items even though the setting items are shown on the Web UI screen of iRMC. Disable the setting items if you fail to assign a profile. | SHA=SHA used MD5=MD5 used None=Authentication disabled |
| Privacy (DES/AES/None) | <p>This specifies a privacy protocol that SNMPv3 uses for encrypting SNMPv3 traffic.</p> | DES=DES used AES=AES used None=Privacy disabled |

| Item Name | Description | Parameter |
|--------------------------------|---|--|
| |  Note <ul style="list-style-type: none"> - To create/change SNMPv3 users, it is required to enable SNMP with the Network Settings -> SNMP. - To use SNMPv3, it is required to set a password with at least 8 characters. - You cannot set up the setting items that are not shown on the Web UI screen of iRMC. Depending on the firmware versions, you cannot set up some setting items even though the setting items are shown on the Web UI screen of iRMC. Disable the setting items if you fail to assign a profile. | |
| SNMP Trap Destination | | |
| SNMP Trap Community Name | This specifies an SNMP trap community. | Enter the SNMP trap community strings |
| SNMPv3 Selected User | This specifies an SNMPv3 user already defined as an SNMPv3 trap destination.  Note You cannot set up the setting items that are not shown on the Web UI screen of iRMC. Depending on the firmware versions, you cannot set up some setting items even though the setting items are shown on the Web UI screen of iRMC. Disable the setting items if you fail to assign a profile. | Enter the SNMP user strings |
| Destination SNMP Server 1 to 7 | This specifies the DNS name or the IP address of a server which belongs to the community set up as "Trap destination." | Enter the IP address or the DNS strings of an SNMP server. |
| Protocol | This specifies the Version of SNMP protocol used for receiving traps.  Note You cannot set up the setting items that are not shown on the Web UI screen of iRMC. Depending on the firmware versions, you cannot set up some setting items even though the setting items are shown on the Web UI screen of iRMC. Disable the setting items if you fail to assign a profile. | Select the item from the pulldown menu. SNMPv1, SNMPv2c or SNMPv3 |

C.2 MMB Setting Items of Profiles for PRIMEQUEST2000 Series Partitions

This section describes the items that you can set up in the MMB tab in profiles.

MMB Tab

| Item Name | | Description | Parameter |
|--------------------------|--------------------------------------|---|---|
| Automatic Server Restart | | | |
| | Targeted | Specify whether to set ASR (Automatic Server Restart) | (Checked)=Perform setting (Unchecked)=Do not execute settings |
| | Number of Restart Tries | Set the number of retries to restart the OS if the OS shuts down because of watchdog or a hardware error. | Select whether to use restart and the number of restarts (1 - 10). |
| | Action after exceeding Restart tries | Set the action to take after the number of retries set above. | Power OFF=Stop reboot and turn the power of the partitions OFF (Stop rebooting and power off) Stop=Stop reboot and stop partitions (Stop rebooting) NMI Interruption=Stop reboot and assert NMI interruption for the partitions (Diagnostic Interrupt assert) |
| Boot Watchdog | | | |
| | Targeted | Specify whether to set the boot watchdog. | (Checked)=Perform setting (Unchecked)=Do not execute settings |
| | Boot Watchdog | This means enable/disable of Boot Watchdog. Specify whether to monitor the time before OS start. | (Checked)=Time monitored (Unchecked)=Time not monitored |
| | Timeout time(seconds) | If the time set here is exceeded and the OS does not start it is judged to be an error. | Specify a value between 1 - 6000 seconds. |
| | Action when watchdog expires | Specify the action taken if the OS does not start after the time specified has been exceeded. | Continue=Continue processing Reset=Restart Power Cycle=The power is first turned OFF, then turned ON |
| Software Watchdog | | | |
| | Targeted | Specify whether to set the software watchdog. | (Checked)=Perform setting (Unchecked)=Do not execute settings |
| | Software Watchdog | This means enable/disable of Software Watchdog. Specify whether to execute regular communication checks while the OS is running. | (Checked)=Communication checked (Unchecked)=Communication not checked |
| | Timeout time(seconds) | If the time set here is exceeded and there is no communication it is judged to be an error. | Specify a value between 1 - 6000 seconds. |
| | Action when watchdog expires | Specify the action taken if there is no communication after the time specified has been exceeded. | Continue=Continue processing Reset=Restart Power Cycle=The power is first turned OFF, then turned ON |

| Item Name | | | | Description | Parameter |
|-----------|--|--|--|-------------|---------------------|
| | | | | | NMI= Make NMI occur |

C.3 OS Setting Items of Profiles for Servers

This section describes the items that you can set up with OS/OS Individual tabs, in profiles. When it comes to the items with "Omittable", you can install the OSes without setup on the profiles. If omitted, no setting is applied, or the default settings of OSes are applied.

C.3.1 Profiles for Windows Server

This applies to the following OS.

- Windows Server 2008 R2 SP1
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

OS tab

| Item Name | | | Description | Parameter | |
|--------------------------------------|--|-------------------|---|--|--|
| Installation Image | | | | | |
| | Type of Installation | | This specifies to install an OS with core installation or with full installation. | Select from the screen. | |
| | Type of Installation Media | | This selects the type of media used for installation. | Select the item from the pulldown menu. When you select Microsoft Media, then it is required to enter its product key. | |
| | ServerView Suite DVD (Install Latest Version/Specify Version) | | This specifies the version of ServerView Suite DVD used for installation. | Install Latest Version=The latest version of ServerView Suite registered in the repository used. Specify Version=ServerView Suite with the specified version used | |
| Management LAN network port settings | | | | | |
| | Network port specification | | This specifies the port of the network used for the management LAN. | (Checked)= Specify the network port for Management LAN. | |
| | | Method to specify | This selects the method of specifying the network port for Management LAN. [Note1] | Select the item from the pulldown menu. | |
| | | | Network Card | This is set if you specify "Port Number" in Method to specify. Select the type of network card that you use. | Select from the screen. Enter the PCI slot number if you select a PCI card. |
| | | | Port Number | This is entered if you specify "Port Number" in Method to specify. | Enter the port number that you use. |
| | | | MAC Address | This is entered if you specify "MAC address" in Method to specify. | Enter the MAC address of the network that you use. |
| RAID & Disk Configuration | | | | | |
| | Use Array Controller | | This is selected when you use a server-built-in array controller as an OS installation destination. | (Selected)=Array controller used [Note2] | |

| Item Name | | Description | Parameter |
|-------------------------|---|--|--|
| | Use existing RAID Volume | This uses the volume already created on an array controller. | (Selected)=Existing array configuration used |
| | Create new RAID Volume | This configures a new array and creates a volume in the array to use it. | (Selected)=A new array configured Additionally, select the type of array controller, RAID level and the number of disks installed in the RAID, from the pull-down menu. |
| | Do not use Array Controller | This is selected when you use a drive other than the array controller as an OS installation destination. | (Selected)=Drive other than array controller used Additionally, select the type of the drive that you use from the screen. |
| Volume 1 | | | |
| | Volume Label | This specifies a volume name. | Enter the volume name strings. [Note3] |
| | File System | This specifies the type of a file system. | Always NTFS |
| | Partition Size Setting (Automatic/Manual) | This specifies a partition size. | Automatic=Partition with appropriate size automatically created Manual=Partition with the entered size created |
| | Quick Format | This specifies whether to use Quick Format in formatting a partition. | Yes=Quick Format performed No=Usual formatting performed (It takes longer time.) |
| | Usage | This specifies the purpose of use of a partition. | Always Boot or OS. |
| Basic Settings | | | |
| | Time Zone | This specifies a time zone. | Select the item from the pull-down menu. |
| | Region and Language | This specifies a region and language. | Select the item from the pull-down menu. |
| | Keyboard | This specifies the language and type of keyboard. | Select the item from the pull-down menu. |
| System settings | | | |
| | Display Resolution [px] | This specifies the display resolution immediately after OS installation. | Select the item from the pull-down menu. [Note4] Example: 600x480, 800x600, 1024x768 or 1280x1024 |
| | Refresh Rate [Hz] | This specifies the display refresh rate immediately after OS installation. | Select the item from the pull-down menu. [Note4] |
| | # of Colors [bit] | This specifies the number of colors displayed on a screen immediately after OS installation, with bit count. | Select the item from the pull-down menu. [Note4] |
| Adding Role and Feature | | | |
| | Install SNMP Service | This specifies whether to install SNMP services. | (Checked)=SNMP services installed |
| | SNMP Trap Setting | This specifies the community name and trap destination upon sending SNMP traps. | Select the Add button to set up arbitrary value. [Omittable] |

| Item Name | | Description | Parameter |
|---|--|--|--|
| | Community Name | This specifies community name when sending SNMP traps. | Enter the community name strings when sending. |
| | Trap Destination | This specifies the destination to send SNMP traps. | Enter the character strings of IP address for the destination. |
| | SNMP Security Service | This specifies the name of an acceptable SNMP community and its privilege. | Select the Add button to set up arbitrary value. [Omittable] |
| | Acceptable community name | This specifies the name of an acceptable SNMP community. | Enter the community name strings of acceptable community. |
| | Community privilege | This specify the privilege of acceptable SNMP community. | Select the item from the pulldown menu. None=None Read Create=Read, Create Read Write=Read Write Read Only=Read Only Notify=Notification |
| | Send Authentication Trap | This specifies whether to send authentication traps in response to the SNMP request from an unknown host or community. | (Checked)=Authentication traps sent (Unchecked)=Authentication traps not sent |
| | Accepting SNMP Packets (Accept SNMP Packets from Default Host (LocalHost)/Accept SNMP Packets from These Hosts) | This specifies whether to accept SNMP packets from Localhost. | (Accept SNMP Packets from Default Host (LocalHost))=SNMP packets accepted from Localhost (Accept SNMP Packets from these Hosts)=SNMP packets accepted from the following specified host name. Additionally, the host names are described. |
| | SNMP Setting Agent | Enter a contact and its physical location. | You can use character strings that contain Japanese. [Omittable] |
| | Service | This specifies the information about SNMP hosts from 5 options. | Arbitrary service checked |
| | Remote Desktop | This specifies whether Remote Desktop is available. | (Checked)=Remote Desktop enabled (Unchecked)=Remote Desktop disabled |
| Remote Assistance (Only when the type of installation is full installation) | | This specifies whether Remote Assistance is available. | Specify the permissible scope on the screen. Specify Invitation Ticket Time as required. |
| Firewall Settings | | This creates a firewall exception required in registering a target server with SCVMM. Access from the following applications is enabled. - Windows Management Instrumentation(WMI) - Sharing files and printing devices | (Checked)=Firewall exception created (Unchecked)=Firewall exception not created |

| Item Name | | Description | Parameter |
|-------------------------------------|-------------------------------------|---|---|
| | Additional Application | | |
| | Java Runtime Environment | Specify whether to install Java Runtime Environment. You must specify this when you install ServerView RAID Manager. | (Checked)=Install Application [Note5] |
| | ServerView Agent | This specifies whether to install ServerView Agent. You can specify it when you install SNMP services. | (Checked)=Install Application [Note6] |
| | ServerView Update Agent | This specifies whether to install ServerView Update Agent. You can specify it when you install ServerView Agent. | (Checked)=Install Application [Note6] |
| | DSNAP | This specifies whether to install DSNAP. | (Checked)=Install Application [Note7] |
| | Software Support Guide | This specifies whether to install Software Support Guide. | (Checked)=Install Application [Note7] |
| | ServerView RAID Manager | This specifies whether to install ServerView RAID Manager. | (Checked)=Application installed |
| Executing Script after Installation | | | |
| | Executing Script after Installation | This specifies whether to execute a script after installation. | (Checked)=Script executed after installation |
| | The Directory forwarded to OS | This specifies the directory forwarded to an OS after installation. | Specify the directory forwarded to the OS after installation. |
| | Script executed after Installation | This specifies the script to be executed. [Note8] | Specify the script to be executed. |

[Note1]: If the Universal Multi-Channel (UMC) function of the CNA card is enabled, set the MAC address and not the port number.

[Note2]: If using an array controller, set it so that there are no inconsistencies with the "Onboard Device Configuration" settings for the BIOS.

[Note3]: Volume names must be set by one-byte alphanumeric characters/symbols for Windows Server 2016.

[Note4]: This is installed with default settings when you set up a value unsupported by the OS.

[Note5]: This is only possible to install when Full Installation has been selected in the "Type of Installation" setting.

[Note6]: The application is installed in Japanese when you select Japanese on "Region and Language" settings. Otherwise, the application is installed in English.

[Note7]: This can be installed only when you select Japanese on "Region and Language" settings.

[Note8]: The specified script is executed by Windows "cmd /c" command.

OS Individual tab

| Item Name | Description | Parameter |
|----------------------------|---|---|
| Type of Installation media | This selects the type of media used for installation. | Always the installation media specified on OS tab |
| User Name | A user name is entered. | Enter the user name. |
| Organization | The organization to which a user belongs is entered. | Enter the organization. |

| Item Name | | Description | Parameter |
|------------------------|------------------------|--|--|
| Computer Name | | The name of a computer for identifying it on the network is entered. | Enter the computer name. |
| Administrator Password | | A password is entered. | Enter the password. |
| Work Group/Domain | | | |
| | Work Group/Domain | You select one of Work Group or Domain to participate in. | Work Group=Participation in Work Group Domain=Participation in Domain [Note1] |
| | Work Group/Domain Name | This specifies the name of Work Group or Domain. | Enter the character string. [Note2] |
| | Domain User Name | A domain user name for the case of Domain is entered. | Enter the character string. |
| | Domain Password | A password for the case of Domain is entered. | Enter the character string. |
| Network | | | |
| | DHCP | This selects whether to specify a fixed IP address or use DHCP for the IP address of Management LAN. | (Checked)=DHCP used (Unchecked)=Fixed IP specified |
| | IP Address | A fixed IP address is specified when you do not use DHCP. | Enter the IP address in IPv4 format. |
| | Subnet Mask | A subnet mask is specified when you do not use DHCP. | Enter the subnet mask in IPv4 format. |
| | Default Gateway | A gateway is specified when you do not use DHCP. | Enter the IP address of the gateway in IPv4 format. |
| | DNS server | The IP address of a DNS server is specified when you do not use DHCP. | Enter the IP address of the DNS server in IPv4 format. |
| | DNS Domain Name | A domain name is specified when you do not use DHCP. | Enter the domain name character string. |

[Note1]: This is set up for Work Group when you are unable to connect to the domain server.

[Note2]: Set a work group name within 15 characters. A double-byte character is counted as 2 characters and single-byte character is counted as 1 character.

C.3.2 Profiles for VMware ESXi

The applicable OS are described below.

- VMware ESXi 5.5 update3
- VMware ESXi 6.0 update1, update2
- VMware ESXi 6.5

OS tab

| Item Name | | Description | Parameter |
|--------------------|----------------------------|---|---|
| Installation Image | | | |
| | Type of Installation Media | This selects the type of media used for installation. | Select the item from the pulldown menu. |

| Item Name | | Description | Parameter |
|---------------------------------------|--|---|---|
| | ServerView Suite DVD (Install Latest Version/Specify Version) | This specifies the version of ServerView Suite DVD used for installation. | Install Latest Version=The latest version of ServerView Suite registered in the repository used. Specify Version=ServerView Suite with the specified version used |
| Management LAN network port settings | | | |
| | Network port specification | This specifies the port of the network used for the management LAN. | (Checked)= Specify the network port for Management LAN. |
| | Method to specify | This selects the method of specifying the network port for Management LAN. [Note1] | Select the item from the pulldown menu. |
| | Network Card | This is set if you specify "Port Number" in Method to specify. Select the type of network card that you use. | Select from the screen. Enter the PCI slot number if you select a PCI card. |
| | Port Number | This is entered if you specify "Port Number" in Method to specify. | Enter the port number that you use. |
| | MAC Address | This is entered if you specify "MAC address" in Method to specify. | Enter the MAC address of the network that you use. |
| RAID & Disk Configuration | | | |
| | Use Array Controller | This is selected when you use a server-built-in array controller as an OS installation destination. | (Selected)=Array controller used [Note2] [Note3] |
| | Use existing RAID Volume | This uses the volume already created on an array controller. | (Selected)=Existing array configuration used |
| | Create new RAID Volume | This configures a new array and creates a volume in the array to use it. | (Selected)=A new array configured Additionally, select the type of array controller, RAID level and the number of disks installed in the RAID, from the pulldown menu. |
| | Do not use Array Controller | This is selected when you use a drive other than the array controller as an OS installation destination. | (Selected)=Drive other than array controller used Additionally, select the type of the drive that you use from the screen. |
| Basic Settings | | | |
| | Keyboard | This specifies the language and type of keyboard. | Select the item from the pulldown menu. |
| Network | | | |
| | Setup | This specifies whether to make a setup with VM Standard Network. | (Checked)=Standard Network created |
| | VLAN ID to Use | Enter VLAN ID. "0" is entered when you do not use VLAN. | Enter the VLAN ID |
| Register to Cloud Management Software | | | |
| | Register to Cloud Management Software | This specifies whether to automatically register on vCenter subsequently after completion of ESXi installation. Set a fixed IP address as the IP address set by using [OS Individual] tab if you perform the | (Checked)=Register (Unchecked)=Do not register |

| Item Name | | Description | Parameter |
|-------------------------------------|--|---|---|
| | | automatic registration. Additionally, specify "0" to VLAN ID on "OS" tab. | |
| | Cloud Management Software Name to register host with | This specifies the vCenter of the registration destination. | Select from the registration destinations registered beforehand in the on the left side of the [Settings] - [General] - [Cloud Management Software] screen. |
| | Folder Name or Cluster Name to register host with | This specifies the folder name or the cluster name of the registration destination. | Specify the folder name or the cluster name of the registration destination. |
| Executing Script after Installation | | | |
| | Executing Script after Installation | This specifies whether to execute a script after installation. | (Checked)=Script executed after installation |
| | The directory of Script | This specifies the directory in which the script executed after installation is stored. | Specify the directory in which the script executed after installation is stored. |
| | Script executed after Installation | This specifies the script executed after installation. [Note4] | Specify the script executed after installation. |

[Note1]: If the Universal Multi-Channel (UMC) function of the CNA card is enabled, set the MAC address and not the port number.

[Note2]: If using an array controller, set it so that there are no inconsistencies with the "Onboard Device Configuration" settings for the BIOS.

[Note3]: "Onboard SATA array controllers" cannot be used in VMware ESXi.

[Note4]: Describe the script with plain text format in the file. This is executed as %post processing during automatic installation (kickStart). %firstboot --interpreter=busybox description allows it to be executed as %firstboot --interpreter=busybox processing.

OS Individual tab

| Item Name | | Description | Parameter |
|----------------------------|----------------------------------|---|---|
| License Agreement | | This selects whether to agree with VMware License Agreement. Make sure to check the box to show that you accept. | (Checked)=Agreement with VMware License (Unchecked)=Not in agreement with VMware License |
| Type of Installation media | | This selects the type of media used for installation. | It is always the installation media specified in the OS tab |
| Root Password | | A password is entered. | Enter the password. |
| Network | | | |
| | DHCP | This selects whether to specify a fixed IP address or use DHCP for the IP address of Management LAN. | (Checked)=DHCP used (Unchecked)=Fixed IP specified |
| | IP Address | A fixed IP address is specified when you do not use DHCP. | Enter the IP address in IPv4 format. |
| | Subnet Mask | A subnet mask is specified when you do not use DHCP. | Enter the subnet mask in IPv4 format. |
| | Default Gateway | A gateway is specified when you do not use DHCP. | Enter the IP address of the gateway in IPv4 format. |
| | DNS server | A DNS server is specified by its IP address when you do not use DHCP. | Enter the IP address of the DNS server in IPv4 format. |
| | Get Computer Name Via DNS Server | This specifies whether to use the computer name obtained from DNS. | (Checked)=Obtained from DNS |

| Item Name | | | Description | Parameter |
|-----------|--|---------------|---|---|
| | | | You can select Checked/Unchecked when DHCP is disabled. | (Unchecked)=Arbitrary computer name specified |
| | | Computer Name | Arbitrary computer name (host name) is specified when you do not obtain a computer name (host name) from DNS. | Enter the host name. |

C.3.3 Profiles for Red Hat Enterprise Linux

The applicable OS are described below.

- Red Hat Enterprise Linux 6.6 (for x86)
- Red Hat Enterprise Linux 6.6 (for Intel64)
- Red Hat Enterprise Linux 6.7 (for x86)
- Red Hat Enterprise Linux 6.7 (for Intel64)
- Red Hat Enterprise Linux 6.8 (for x86)
- Red Hat Enterprise Linux 6.8 (for Intel64)
- Red Hat Enterprise Linux 7.1 (for Intel64)
- Red Hat Enterprise Linux 7.2 (for Intel64)
- Red Hat Enterprise Linux 7.3 (for Intel64)

OS tab

| Item Name | | | Description | Parameter | |
|--------------------------------------|--|-------------------|---|--|--|
| Installation Image | | | | | |
| | Type of Installation Media | | This selects the type of media used for installation. | Select the item from the pulldown menu. | |
| | ServerView Suite DVD (Install Latest Version/Specify Version) | | This specifies the version of ServerView Suite DVD used for installation. | Install Latest Version=The latest version of ServerView Suite registered in the repository used. Specify Version=ServerView Suite with the specified version used | |
| Management LAN network port settings | | | | | |
| | Network port specification | | This specifies the port of the network used for the management LAN. | (Checked)= Specify the network port for Management LAN. | |
| | | Method to specify | This selects the method of specifying the network port for Management LAN. [Note1] | Select the item from the pulldown menu. | |
| | | Network Card | This is set if you specify "Port Number" in Method to specify. Select the type of network card that you use. | Select from the screen. Enter the PCI slot number if you select a PCI card. | |
| | | | Port Number | This is entered if you specify "Port Number" in Method to specify. | Enter the port number that you use. |
| | | | MAC Address | This is entered if you specify "MAC address" in Method to specify. | Enter the MAC address of the network that you use. |
| Basic Settings | | | | | |
| | Region and Language | | This specifies a language. | Select the item from the pulldown menu. | |
| | Keyboard | | This specifies the type of a keyboard. | Select the item from the pulldown menu. | |

| Item Name | | Description | Parameter |
|---------------------------|---|---|--|
| | Time Zone | This specifies a time zone. | Select the item from the pulldown menu. |
| | System clock users UTC | This specifies the type of time used as System Clock. | (Checked)=UTC used (Unchecked)=Local time used |
| RAID & Disk Configuration | | | |
| | Use Array Controller | This is selected when you use a server-built-in array controller as an OS installation destination. | (Selected)=Array controller used |
| | Use existing RAID Volume | This uses the volume already created on an array controller. | (Selected)=Existing array configuration used |
| | Create new RAID Volume | This configures a new array and creates a volume in the array to use it. | (Selected)=A new array configured Additionally, select the type of array controller, RAID level and the number of disks installed in the RAID, from the screen. |
| | Do not use Array Controller | This is selected when you use a drive other than the array controller as an OS installation destination. | (Selected)=Drive other than array controller used Additionally, select the type of the drive that you use from the screen. [Note2] |
| Partition | | Specify the items below to each mount point, such as, /boot/var, shown on [Profile] screen. | |
| | (Checkbox on the left side of each mount point) | This specifies whether to create an independent partition to a mount point. | (Checked)=Partition created (Unchecked)=Partition not created |
| | File System Type | This specifies the type of file systems. | Select the item from the pulldown menu. Ex.: ext2, ext3 or ext4 |
| | Size | This specifies a partition size. | Enter a decimal value. |
| | Fill to maximum allowable size | This specifies whether to allocate spare disk capacity to the specified partition. Specifying this is not required when you create another partition on free space after installing Linux. | (Checked)=Spare capacity allocated to the specified partition to extend the capacity (Unchecked)=Partition with the specified capacity created |
| Select Package | | | |
| | Initialize package selection | This changes the initial choice of a package group shown on the screen as the packages to be installed and a new package. | Minimal system=Minimum required packages All=all packages[Note3] Default package groups=Recommended packages[Note3] |
| | Package Group | This specifies the package group to be installed. | (Checked)=Installed (Unchecked)=Not installed |
| | New Package | This individually specifies the package name to be installed. | Enter the package name with the appropriate strings of characters. Description with more than one line is allowed per one line for one package. |
| Bootloader Option | | | |
| | Install Bootloader | This specifies whether to install a bootloader. | (Checked)=Bootloader installed |

| Item Name | | Description | Parameter |
|-------------------------------------|--|--|---|
| | | | This item is always checked. |
| | Install Bootloader on | This specifies the installation destination of a bootloader. | MBR=Installed on Master Boot Record This item is always set to "MBR." |
| | Kernel parameters | This specifies a kernel parameter. | Enter the character strings specified as the kernel parameter. [Omittable] |
| Security-Enhanced Linux | | | |
| | SE Linux | This specifies whether to use SE Linux. | Select the item from the pulldown menu. Enforcing, Disabled or Permissive |
| Authentication | | | |
| | Use Shadow Passwords | This specifies whether to use shadow passwords. | (Checked)=Used (Unchecked)=Not used [Note4] |
| | Use MD5 | This specifies whether to use MD5 for password encryption. | (Checked)=Used (Unchecked)=Not used |
| | Enable nscd | This specifies whether to use Name Switch Cache Daemon. | (Checked)=Used (Unchecked)=Not used |
| Application Wizard | | Specify the application automatically installed after OS installation. | |
| | Select Application Wizard (a variety of applications) | This specifies the application to be installed. The type of applications differs depending on distribution. [Note5] | (Checked)=Application installed |
| Executing Script after Installation | | | |
| | Executing Script after Installation | This specifies whether to execute a script after installation. | (Checked)=Script executed after installation |
| | The Directory forwarded to OS | This specifies the directory forwarded to an OS after installation. | Specify the directory forwarded to the OS after installation. |
| | Script executed after Installation | This specifies the script to be executed. [Note6][Note7] | Specify the script to be executed. |

[Note1]: If the Universal Multi-Channel (UMC) function of the CNA card is enabled, set the MAC address and not the port number.

[Note2]: PRIMEQUEST 2000 series, iSCSI is not supported. For the support status, refer to the manuals of servers and ServerView Suite DVD.

[Note3]: If you use ServerView Suite DVD V11.16.04 or later, some package groups are not installed. In such cases, manually install them.

[Note4]: "Shadow Passwords" is always enabled regardless of profile settings.

[Note5]: The applications in the table below show the case where ServerView Suite DVD V11.16.04, V12.16.10 is used. These may be changed in the future in response to the update of ServerView Suite DVD.

Y=Can be specified by ISM, N=Cannot be specified by ISM

| Application | RHEL 6.x(x86) | RHEL 6.x(Intel64) | RHEL 7.x |
|--|---------------|-------------------|----------|
| ServerView Agentless Service | N | Y | Y |
| ServerView SNMP Agents | Y | Y | Y |
| ServerView CIM Providers | N | Y | Y |
| ServerView Update Agent (online flash) | Y | Y | Y |

| Application | RHEL 6.x(x86) | RHEL 6.x(Intel64) | RHEL 7.x |
|--|---------------|-------------------|----------|
| ServerView Operations Manager (Note: Set SELinux to Disabled when you install it.) | Y | Y | Y |
| ServerView RAID Manager | Y | Y | Y |
| AIS Connect (Note: This cannot be set up for ServerView Suite DVD V12.16.10 or later) | Y | Y | N |
| Java Runtime Environment | Y | Y | Y |
| Dynamic Reconfiguration utility for PRIMEQUEST2000 | N | Y | Y |
| PRIMEQUEST REMCS Option for PRIMEQUEST2000 | N | Y | Y |
| HBA blockage function for PRIMEQUEST2000 | N | Y | Y |
| SIRMS Agent for PRIMEQUEST2000 | Y | Y | Y |
| ServerView Mission Critical Option for PRIMEQUEST2000 | N | Y | Y |

[Note6]: When you execute a script from another script, assign execution privilege to invoke it.

[Note7]: This executes the specified script with the sh command.

OS Individual tab

| Item Name | | Description | Parameter |
|----------------------------|----------------------------------|---|--|
| Type of Installation media | | This selects the type of media used for installation. | It is always the installation media specified in the OS tab |
| Root Password | | A password is entered. | Enter the password. |
| Network | | | |
| | Get Computer Name Via DNS Server | | (Checked)=Obtained from DNS (Unchecked)=Arbitrary computer name specified |
| | Computer Name | Arbitrary computer name (host name) is specified when you do not obtain a host name from DNS. | Enter the host name. |
| | DHCP | | (Checked)=DHCP used (Unchecked)=Fixed IP specified |
| | IP Address | A fixed IP address is specified when you do not use DHCP. | Enter the IP address in IPv4 format. |
| | Subnet Mask | A subnet mask is specified when you do not use DHCP. | Enter the subnet mask in IPv4 format. |
| | Default Gateway | The default gateway is specified when you do not use DHCP. | Enter the IP address of the gateway in IPv4 format. |
| | DNS server | A DNS server is specified by its IP address when you do not use DHCP. | Enter the IP address of the DNS server in IPv4 format. |

C.3.4 Profiles for SUSE Linux Enterprise Server

The applicable OS are described below.

- SUSE Linux Enterprise Server 11 SP4 (for x86)

- SUSE Linux Enterprise Server 11 SP4 (for AMD64 & Intel64)
- SUSE Linux Enterprise Server 12 (for AMD64 & Intel64)
- SUSE Linux Enterprise Server 12 SP1 (for AMD64 & Intel64)

OS tab

| Item Name | | Description | Parameter |
|--------------------------------------|--|---|--|
| Installation Image | | | |
| | Type of Installation Media | This selects the type of media used for installation. | Select the item from the pulldown menu. |
| | ServerView Suite DVD (Install Latest Version/Specify Version) | This specifies the version of ServerView Suite DVD used for installation. | Install Latest Version=The latest version of ServerView Suite registered in the repository used. Specify Version=ServerView Suite with the specified version used |
| Management LAN network port settings | | | |
| | Network port specification | This specifies the port of the network used for the management LAN. | (Checked)= Specify the network port for Management LAN. |
| | Method to specify | This selects the method of specifying the network port for Management LAN. [Note1] | Select the item from the pulldown menu. |
| | Network Card | This is set if you specify "Port Number" in Method to specify. Select the type of network card that you use. | Select from the screen. Enter the PCI slot number if you select a PCI card. |
| | Port Number | This is entered if you specify "Port Number" in Method to specify. | Enter the port number that you use. |
| | MAC Address | This is entered if you specify "MAC address" in Method to specify. | Enter the MAC address of the network that you use. |
| Basic Settings | | | |
| | Region and Language | This specifies a language. | Select the item from the pulldown menu. |
| | Keyboard | This specifies the type of a keyboard. | Select the item from the pulldown menu. |
| | Time Zone | This specifies a time zone. | Select the item from the pulldown menu. |
| | System clock uses UTC | This specifies the type of time used as System Clock. | (Checked)=UTC used (Unchecked)=Local time used |
| RAID & Disk Configuration | | | |
| | Use Array Controller | This is selected when you use a server-built-in array controller as an OS installation destination. | (Selected)=Array controller used [Note2] |
| | Use existing RAID Volume | This uses the volume already created on an array controller. | (Selected)=Existing array configuration used |
| | Create new RAID Volume | This configures a new array and creates a volume in the array to use it. | (Selected)=A new array configured Additionally, select the type of array controller, RAID level and the number of disks installed in the RAID, from the screen. |
| | Do not use Array Controller | This is selected when you use a drive other than the array controller as an OS installation destination. | (Selected)=Drive other than array controller used |

| Item Name | | Description | Parameter |
|-------------------------|---|---|--|
| | | | Additionally, select the type of the drive that you use from the screen. [Note3] |
| Partition | | Specify the items below to each mount point, such as, /boot/var, shown on [Profile] screen. | |
| | (Checkbox on the left side of each mount point) | This specifies whether to create an independent partition to a mount point. | (Checked)=Partition created (Unchecked)=Partition not created |
| | File System Type | This specifies the type of file systems. | Select the item from the pulldown menu. Ex.: ext2, ext3 or ext4 [Note4] |
| | Size | This specifies a partition size. | Enter a decimal value. |
| | Fill to maximum allowable size | This specifies whether to allocate spare disk capacity to the specified partition. Specifying this is not required when you create another partition on free space after installing Linux. | (Checked)=Spare capacity allocated to the specified partition to extend the capacity (Unchecked)=Partition with the specified capacity created |
| Select Package | | | |
| | Initialize package selection | This changes the initial choice of a package group shown on the screen as the packages to be installed and a new package. | Minimal system=Minimum required packages Install everything=All the packages Default package groups=Recommended packages |
| | Package Group [Note5] | This specifies the package group to be installed. | (Checked)=Installed (Unchecked)=Not installed |
| | New Package | This individually specifies the package name to be installed. | Enter the package name with the appropriate strings of characters. Description with more than one line is allowed per one line for one package. |
| Bootloader Option | | | |
| | Install Bootloader | This specifies whether to install a bootloader. | (Checked)=Bootloader installed This item is always checked. |
| | Install Bootloader on | This specifies the installation destination of a bootloader. | MBR=Installed on Master Boot Record This item is always set to "MBR." |
| | Kernel parameters | This specifies a kernel parameter. | Enter the character strings specified as the kernel parameter. [Omittable] |
| Security-Enhanced Linux | | | |
| | SE Linux | This specifies whether to use SE Linux. | This item is always set to "Disabled." |
| Authentication | | | |
| | Use Shadow Passwords | This specifies whether to use shadow passwords. | This item is always set to "Checked (Used)." |
| | Use MD5 | This specifies whether to use MD5 for password encryption. | This item is always set to "Unchecked (Not Used)." |

| Item Name | | Description | Parameter |
|---|--|--|---|
| | Enable nscd | This specifies whether to use Name Switch Cache Daemon. | This item is always set to "Checked (Used)." |
| Application Wizard | | Specify the application automatically installed after OS installation. | |
| | Select Application Wizard (a variety of applications) | This specifies the application to be installed. The type of applications differs depending on distribution. [Note6] | (Checked)=Application installed |
| Executing Script after Installation [Note7] | | | |
| | Executing Script after Installation | This specifies whether to execute a script after installation. | (Checked)=Script executed after installation |
| | The Directory forwarded to OS | This specifies the directory forwarded to an OS after installation. | Specify the directory forwarded to the OS after installation. |
| | Script executed after Installation | This specifies the script to be executed. [Note8][Note9] | Specify the script to be executed. |

[Note1]: If the Universal Multi-Channel (UMC) function of the CNA card is enabled, set the MAC address and not the port number.

[Note2]: If using an array controller, set it so that there are no inconsistencies with the "Onboard Device Configuration" settings for the BIOS.

[Note3]: PRIMEQUEST 2000 series, iSCSI is not supported. For the support status, refer to the manuals of servers and ServerView Suite DVD.

[Note4]: In SLES 11 SP4, ext4 only supports Read. In SLES 12, ext4 can support both the Read/Write. Note, however, that these are not the official support by SLES.

[Note5]: In SLES 12, even in the case where "X-Windows System" is not specified for the package group, you cannot start it by the console. Pressing [Ctrl] + [Alt] + [F1] allows you to log in from the console.

[Note6]: The applications in the table below show the case where ServerView Suite DVD V11.16.04, V12.16.10 is used. These may be changed in the future version upgrades of ServerView Suite DVD.

Y=Can be specified by ISM, N=Cannot be specified by ISM

| Applications (For SLES) | SLES 11 SP4(x86) | SLES 11 SP4(Intel64) | SLES 12 type |
|--|------------------|----------------------|--------------|
| ServerView Agentless Service | N | Y | Y |
| ServerView SNMP Agents | Y | Y | Y |
| ServerView CIM Providers | N | N | N |
| ServerView Update Agent (online flash) | Y | Y | Y |
| ServerView Operations Manager | N | N | N |
| ServerView RAID Manager | Y | Y | Y |
| AIS Connect (Note: This cannot be set up for ServerView Suite DVD V12.16.10 or later) | N | N | N |
| Java Runtime Environment | Y | Y | Y |
| Dynamic Reconfiguration utility for PRIMEQUEST2000 | N | N | N |
| PRIMEQUEST REMCS Option for PRIMEQUEST2000 | N | N | N |
| HBA blockage function for PRIMEQUEST2000 | N | N | N |
| SIRMS Agent for PRIMEQUEST2000 | N | N | N |

| Applications (For SLES) | SLES 11 SP4(x86) | SLES 11 SP4(Intel64) | SLES 12 type |
|---|------------------|----------------------|--------------|
| ServerView Mission Critical Option for PRIMEQUEST2000 | N | N | N |

[Note7]: In SLES 12, this does not support the script execution after installation.

[Note8]: When you execute a script from another script, assign execution privilege to invoke it.

[Note9]: This executes the specified script with the sh command.

OS Individual tab

| Item Name | | Description | Parameter |
|----------------------------|----------------------------------|---|--|
| Type of Installation media | | This selects the type of media used for installation. | It is always the installation media specified in the OS tab |
| Root Password | | A password is entered. | Enter the password. |
| Network | | | |
| | Get Computer Name Via DNS Server | | (Checked)=Obtained from DNS (Unchecked)=Arbitrary computer name specified |
| | Computer Name | Arbitrary computer name (host name) is specified when you do not obtain a host name from DNS. | Enter the host name. |
| | DHCP | | (Checked)=DHCP used (Unchecked)=Fixed IP specified |
| | IP Address | A fixed IP address is specified when you do not use DHCP. | Enter the IP address in IPv4 format. |
| | Subnet Mask | A subnet mask is specified when you do not use DHCP. | Enter the subnet mask in IPv4 format. |
| | Default Gateway | The default gateway is specified when you do not use DHCP. | Enter the IP address of the gateway in IPv4 format. |
| | DNS server | A DNS server is specified by its IP address when you do not use DHCP. | Enter the IP address of the DNS server in IPv4 format. |
| | | | |

C.4 Virtual IO Setting Items of Profiles for PRIMERGY Servers

C.4.1 Card Settings

Set for each card that you want to use.

| Item Name | | Description | Parameter |
|------------------------------|-----------------|------------------------------------|---|
| Number of onboard card slots | | Select the number of onboard. | Select the item from the pulldown menu. |
| Number of PCI card slots | | Select the number of cards to use. | Select the item from the pulldown menu. |
| Card slot | | | |
| | Onboard slot | | |
| | Card type | Select the type to use. | Select from the screen. |
| | Number of ports | Select the number of ports to use. | Select the item from the pulldown menu. |
| | PCI card | | |

| Item Name | | Description | Parameter |
|-----------|-----------------|------------------------------------|---|
| | Card type | Select the type to use. | Select from the screen. |
| | Number of ports | Select the number of ports to use. | Select the item from the pulldown menu. |

Note

- Assign virtual addresses and to the virtual IO settings for the LAN, FC, CNA cards/boards mounted on the server. Operation where only one part of the cards/boards or one part of the ports has been assigned virtual addresses is not supported.
- Virtual IO settings cannot be used for cards and boards (including items where the number of cards/boards is set to 0) that were removed from the settings when profiles were edited. It will normally not be recognized from the OS (depending on the OS and the drivers it might be recognized and displayed).

C.4.2 Port Settings

It is required to set it up for the number of cards set in "[C.4.1 Card Settings](#)."

The following settings for each card are described separately for each card type.

| Item Name | | Description | Parameter |
|---------------------------|--------------------------------|--------------------------------------|---|
| Port information | | | |
| | Use a virtual address | Select if using a virtual address. | (Checked)= Use virtual address. |
| | Use SR-IOV | Select if using SR-IOV. | (Checked)= Use SR-IOV |
| | Do not display boot menu (F12) | Select to not display the boot menu. | (Checked)= Do not display boot menu |
| UEFI boot mode | | Select the boot mode to use. | Select from the screen. |
| If the card type is a CNA | | | |
| | Function type | Select the Function of CNA. | Select the item from the pulldown menu. |
| | Boot | Select boot method. | Select the item from the pulldown menu. |
| | SR-IOV | Select if enabling SR-IOV. | (Checked)=Enable SR-IOV |
| If the card type is LAN | | | |
| | Function type | Select the Function of LAN. | It will always be set to LAN. |
| | Boot | Select boot method. | Select the item from the pulldown menu. |
| | SR-IOV | Select if enabling SR-IOV. | (Checked)=Enable SR-IOV |
| If the card type is FC | | | |
| | Function type | Select the Function of FC | It will always be set to FC. |
| | Boot | Set boot method. | Select the item from the pulldown menu. |
| | SR-IOV | Select if enabling SR-IOV. | (Checked)=Enable SR-IOV |

Note

If installing OS on a local disk (SATA or SAS) the Boot setting cannot be used for the virtual IO. Before applying profiles, manually change the server boot order so that the server PXE boot is prioritized.

C.4.3 Boot Settings

Use the arrow button to the right of each item when changing the bot priority.

Set for the same number of onboard cards or PCI cards/ports that you set in "[C.4.1 Card Settings](#)" or "[C.4.2 Port Settings](#)."

The following describes the parameters for the various functions, not regarding whether they are onboard or PCI cards.

| Item Name | | Description | Parameter |
|-------------------------------|------------------|--|--|
| If the function type is LAN | | | |
| | IP protocol | Selections for IP protocol | Select from the screen. |
| If the function type is FCoE | | | |
| | Connection speed | Select connection speed. | Select the item from the pulldown menu. Automatic, 1 Gbit/s, 2 Gbit/s, 4 Gbit/s, 8 Gbit/s, 16 Gbit/s |
| | Connection type | Select connection form | Select from the screen. |
| First target | | | |
| | Port name (WWPN) | Enter WWPN of the storage to start with SAN boot. | Enter WWPN. |
| | LUN | Enter LUN of the storage to start with SAN boot. | Enter LUN. |
| Second target | | | |
| | Port name (WWPN) | Enter WWPN of the storage to start with SAN boot. | Enter WWPN. |
| | LUN | Enter LUN of the storage to start with SAN boot. | Enter LUN. |
| If the function type is iSCSI | | | |
| Initiator parameter | | | |
| | Address setting | Select the method for retrieving the address of the initiator. | Select from the screen. |
| | Initiator name | Enter IQN of the initiator. | Enter IQN. The character string entered require to start and end with alphanumerical characters, and except for this it should be made up of less than 223 alphanumerical characters or symbols (period ".", colon ":", or hyphen "-"). |
| | VLAN ID | Enter the VLAN ID that HBA uses to send requests. | Enter the VLAN ID |
| | IPv4 | Enter the IP address used for the initiator if you selected "Fixed" in the address settings. | Enter the IP address. |
| | Subnet Mask | Enter the subnet mask if you selected "Fized" in the address settings. | Enter the subnet mask. |
| | Gateway address | Enter the address of the gateway if you selected "Fixed" in the address settings. | Enter the gateway address. |
| Target parameter | | | |
| | IP Address | Select the method for retrieving the address of the target. | Select from the screen. |
| | Target name | Enter the IQN of the target. | Enter IQN. The character string entered require to start and end with alphanumerical characters, and except for this it should be made up of less than 223 alphanumerical |

| Item Name | | Description | Parameter |
|-----------|-----------------------|--|---|
| | | | characters or symbols (period ".", colon ":", or hyphen "-"). |
| | IPv4 | Enter the IP address used by the target if you selected "Fixed" in the IP address settings. | Enter the IP address. |
| | Port (opt) | Enter the target port number if you selected "Fixed" in the IP address settings. | Enter the port number. |
| | LUN | Enter the LUN number of the target if you selected "Fixed" in the IP address settings. | Enter LUN number. |
| | Authentication Method | Select authentication method. | Select from the screen. |
| | CHAP user name | Enter authentication user name if you selected "CHAP" or "Mutual CHAP" for the authentication method. | Enter the authentication user name. The character string entered should consist of less than 127 alphanumerical characters or symbols [Note1]. |
| | CHAP Password | Enter the password used for CHAP authentication if you selected "CHAP" or "Mutual CHAP" for the authentication method. | Enter the password. The character string entered should consist of between 12 and 16 alphanumerical characters or symbols [Note1]. |
| | Mutual CHAP Password | Enter the password used for Mutual CHAP authentication if you selected "Mutual CHAP" for the authentication method. | Enter the password. The character string entered should consist of between 12 and 16 alphanumerical characters or symbols [Note1]. |

[Note1]: Depending on the hardware model it might not be possible to use symbols. It is recommended that you only use alphanumerical characters.

C.4.4 CNA Settings

Set if you specified "CNA" for onboard or PCI card type in "[C.4.1 Card Settings](#)."

Set for the number of CNA function types set in "[C.4.2 Port Settings](#)."

The following describes the parameters for the various card types.

| Item Name | | Description | Parameter |
|---|----------------------|------------------------------------|---|
| If the function is an FCoE type | | | |
| | Minimum bandwidth[%] | Enter the minimum bandwidth value. | Enter the minimum bandwidth value. [Note1] |
| | Maximum bandwidth[%] | Enter the maximum bandwidth value. | Enter the maximum bandwidth value. [Note1] |
| If the function is a LAN or an iSCSI type | | | |
| | Minimum bandwidth[%] | Enter the minimum bandwidth value. | Enter the minimum bandwidth value. [Note1] |
| | Maximum bandwidth[%] | Enter the maximum bandwidth value. | Enter the maximum bandwidth value. [Note1] |
| | VLAN ID | Enter VLAN ID. | Enter VLAN ID. |

[Note1]: Set so that all the totals of one IO channel equals 100.

If the total bandwidth for one IO channel is not 100, internally adjust the bandwidth values accordingly.

C.4.5 Virtual Address Settings

Set it up for the number of card information entered in "[C.4.1 Card Settings](#)."

The following describes the parameters for each card type.

| Item Name | | Description | Parameter |
|---------------------------|----------------------------|--|---|
| If the card type is a LAN | | | |
| | Virtual address allocation | Select if using virtual address allocation. | (Checked)= Allocate virtual addresses |
| | Virtual address[Note1] | | |
| | MAC | Enter virtual MAC address. | Enter virtual MAC address. Two rows each of alphanumerical letters separated by a comma (,) or a hyphen (-). |
| If the card type is an FC | | | |
| | Virtual address allocation | Select if using virtual address allocation. | (Checked)= Allocate virtual addresses |
| | Virtual address[Note1] | | |
| | WWNN | Enter virtual WWNN. | Enter virtual WWNN. Two rows each of alphanumerical letter separated by a comma (,). |
| | WWPN | Enter virtual WWPN. | Enter virtual WWPN. Two rows each of alphanumerical letter separated by a comma (,). |
| If the card type is a CNA | | | |
| | Virtual address allocation | Select if using virtual address allocation. | (Checked)= Allocate virtual addresses |
| | Virtual address[Note1] | | |
| | WWNN | Enter the virtual WWNN if the application is an "FCoE" type. | Enter virtual WWNN. Two rows each of alphanumerical letter separated by a comma (,). |
| | WWPN | Enter the virtual WWPN if the application type is "FCoE." | Enter virtual WWPN. Two rows each of alphanumerical letter separated by a comma (,). |
| | E-MAC | Enter the virtual E-MAC address if the application is an "FCoE" type. | Enter virtual E-MAC address. Two rows each of alphanumerical letters separated by a comma (,) or a hyphen (-). |
| | MAC | Enter virtual MAC address if the function is an "iSCSI" or a "LAN" type. | Enter virtual MAC address. Two rows each of alphanumerical letters separated by a comma (,) or a hyphen (-). |

[Note1]: Only set if "Allocate virtual addresses" was checked.



Note

- It is required that the IQN, WWPN and virtual MAC address is unique across the system.

Except for the same card, it is required that the WWNN is unique across the system.

There is a risk that the volume is damaged if overlapping IQN, WWPN or WWNN access the same volume at the same time.

Network communication is not possible if virtual MAC addresses overlap.

- Multicast MAC addresses can not be used as virtual MAC addresses.

If you set virtual IP addresses arbitrarily there is a risk that they might overlap with the factory shipping values of other cards.

It is recommended that you set the virtual address within the following range.


- MAC address(00:19:99:3E:D2:A1 - 00:19:99:3F:CC:A1)
- WWN(50:01:99:93:ED:2A:10:00 - 50:01:99:93:FC:C9:FF:FF)




C.5 Setting Items of Profiles for Storage



This section describes the items that you set up in the profiles for ETERNUS DX Series. Some of selectable items may differ depending on the type of your storage.

For details of each item, see the manual for your storage.

RAID & Disk Configuration tab

| Item Name | | Description | Parameter |
|--------------------|-----------------|---|--|
| RAID Configuration | | | |
| | RAID Group Name | This specifies a RAID group name.  Note You cannot specify the RAID group name already set up for a device. | Enter the RAID group names. You can enter 1 to 16 characters. |
| | RAID Level | This specifies the RAID level of a disk array to be configured. | Select the item from the pulldown menu. RAID1, RAID5, RAID6 or RAID1+0 |
| | Number of Disks | This specifies the number of disks built in a disk array. | Specify the number of disks. The selectable number differs depending on the selected RAID level. |
| | Disk Inch | This specifies the type of disk drive (drive outer size). | Select the item from the pulldown menu. 2.5 Inch or 3.5 Inch |
| | Disk Type | This specifies the type of disk drive (interface type) built in a disk array. | Select the item from the pulldown menu. The selectable type differs depending on the models of ETERNUS and selected disk inch. SAS, NL-SAS, SED or SSD |
| | Disk Size | This specifies the type of disk drive (disk size) built in a disk array. | Select the item from the pulldown menu. The selectable size differs depending on the selected disk inch and disk type. 300GB, 450GB, 1TB, etc. |
| | Volumes | | |
| | Volume Name | This specifies the name of a volume to be created on a RAID group. | Specify the name of a volume to be created on the RAID group. You can enter 1 to 16 characters. |

| Item Name | | Description | Parameter |
|------------------|-----------------|---|--|
| | |  Note You cannot specify the volume name already set up for a device. | |
| | Volume Size | This specifies volume size to be created on a RAID group. | Specify the volume size on the text box to select the item from pulldown menu. Specifying "max" for the last volume size causes all the remaining size of the RAID group to be allocated. For ETERNUS DX60 S2, you cannot specify "max." MB, GB or TB |
| Global Hot Spare | | | |
| | Disk Inch | This specifies the type of disk drive (drive outer size) defined as a hot spare. | Select the item from the pulldown menu. 2.5 Inch or 3.5 Inch |
| | Disk Type | This specifies the type of disk drive (interface type) defined as a hot spare. | Select the item from the pulldown menu. The selectable type differs depending on the models of ETERNUS and selected disk inch. SAS, NL-SAS, SED or SSD |
| | Disk Size | This specifies the type of disk drive (disk size) defined as a hot spare. | Select the item from the pulldown menu. The selectable size differs depending on the selected disk inch and disk type. 300GB, 450GB, 1TB, etc. |
| Host Affinity | | | |
| LUN Group | | | |
| | LUN Group Name | This specifies a LUN group name.  Note You cannot specify the LUN group name already set up for a device. | Specify the LUN group name strings. |
| | Volumes | | |
| | Volume Name | This specifies the name of a volume which belongs to a LUN group. | Enter the name of the volume which belongs to the LUN group. Specify the volume created by a profile or the volume already created on a device. |
| Port Group | | | |
| | Port Group Name | This specifies a port group name.  Note You cannot specify the port group name already set up for a device. | Specify the port group name. You can enter 1 to 16 characters. |

| Item Name | | Description | Parameter |
|-----------|------------------|---|--|
| | Ports | | |
| | Port Number | This specifies the port number which belongs to a port group. | Specify the port number which belongs to the port group with a triple-digit number. |
| | Host Group | | |
| | Host Group Name | This specifies a host group name.  Note You cannot specify the host group name already set up for a device. | Specify the host group name. You can enter 1 to 16 characters. |
| | Host Type | This specifies the type of a host group. | Select the item from the pulldown menu. iSCSI or FC |
| | Hosts | | |
| | Host Name | This specifies the host name which belongs to a host group.  Note You cannot specify the host name already set up for a device. | Specify the name of the host which belongs to the host group. You can enter 1 to 16 characters. |
| | Host iSCSI | This specifies the iSCSI name which defines a host name. Can be entered when the host type of a host group is iSCSI name. | Enter iSCSI name. Enter "iqn." or "eui." at the beginning. |
| | Host WWN | This specifies the host WWN which defines a host name. You can enter it when the host type of a host group is FC. | Enter the host WWN. You can enter 16 hexadecimal characters. |
| | Setting Details | | |
| | Pre Run Command | The control command to execute on ETERNUS before executing profile assignment (RAID/Hot Spare/Host Affinity settings) is described. Leave the checkbox unchecked unless a special request is made. | See "CLI User Guide" of your device for the described contents. |
| | Post Run Command | The control command to execute on ETERNUS after completion of profile assignment (RAID/Hot Spare/Host Affinity settings) is described. Leave the checkbox unchecked unless a special request is made. | See "CLI User Guide" of your device for the described contents. |

Point

- You cannot specify the position of a mounted slot on the disk drive used for the array configuration.

- You cannot specify the position of a mounted slot on the disk drive used for the hot spare configuration.

C.6 Setting Items of Profiles for Switches

This section describes the items that you set up, in the profiles for switches.

For details of each item, see the manual of your switch.

C.6.1 Profiles for SRX

SNMP tab

| Item Name | | Description | Parameter |
|---------------------------|---------------------------------|--|--|
| SNMP Service | | | |
| | SNMP Service Setting | This specifies whether to use SNMP service settings. | (Checked)=Used (Unchecked)=Not used |
| | SNMP Agent and Trap (ON/OFF) | This specifies whether to enable or disable SNMP agents and traps. | ON=Function enabled OFF=Function disabled |
| | SNMP Agent Setting | This specifies whether to use SNMP agent settings. | (Checked)=Used (Unchecked)=Not used |
| | Agent Address | This specifies whether to enable an agent address. | (Checked)=Agent address enabled Additionally, enter the agent address in IPv4 format. |
| | SNMP Engine ID | This specifies whether to enable an SNMP engine ID. | (Checked)=SNMP engine ID enabled Additionally, enter the SNMP engine ID. |
| SNMP Host (SNMPv1 or v2c) | | | |
| | Number | This specifies an SNMP host definition number. | Select the item from the pulldown menu. |
| | Address | This specifies the IP address of an SNMP host. | Specify the IP address of the SNMP host in IPv4 format. |
| | Community Name | This specifies the community name of an SNMP host. | Enter the community name of the SNMP host. |
| | Trap | This specifies whether to send SNMP traps. | Select the item from the pulldown menu. Off, v1 or v2c |
| | Write | This specifies whether to permit writing from an SNMP manager. | (Checked)=Permitted (Unchecked)=Not permitted |
| SNMP User (SNMPv3) | | | |
| | Number | This specifies an SNMP user definition number. | Select the item from the pulldown menu. |
| | User Name | This specifies an SNMP user name. | Enter the SNMP user name. |
| | Address Setting | This specifies whether to enable an SNMP host address. | (Checked)=Enabled (Unchecked)=Disabled |
| | Host Number | This specifies an SNMP host definition number. | Select the item from the pulldown menu. |

| Item Name | | Description | Parameter |
|-----------|-------------------------|--|--|
| | Host Address | This specifies the IP address of an SNMP host. | Enter the IP address strings of the SNMP host. |
| | Trap Setting | This specifies whether to enable SNMP trap settings. | (Checked)=Enabled (Unchecked)=Disabled |
| | Host Number | This specifies an SNMP host definition number. | Select the item from the pulldown menu. |
| | Host Address | This specifies the IP address of an SNMP host. | Enter the IP address strings of the SNMP host. |
| | Authentication Setting | This specifies whether to enable SNMP authentication protocol. | (Checked)=Enabled (Unchecked)=Disabled |
| | Authentication Protocol | This specifies the SNMP authentication protocol. | Select the item from the pulldown menu. None, MD5 or SHA |
| | Authentication Password | This specifies an SNMP authentication password. | Enter the SNMP authentication password. |
| | Privacy Setting | This specifies whether to enable SNMP privacy settings. | (Checked)=Enabled (Unchecked)=Disabled |
| | Privacy Protocol | This specifies the SNMP privacy protocol. | Select the item from the pulldown menu. None or DES |
| | Privacy Password | This specifies an SNMP privacy password. | Enter the SNMP privacy password. |
| | Read | This specifies whether to enable SNMP MIB read. | (Checked)=Enabled Additionally, specify the item from the pulldown menu. none: Read not permitted all: Read permitted |
| | Write | This specifies whether to enable SNMP MIB write. | (Checked)=Enabled Additionally, specify the item from the pulldown menu. none: Write not permitted all: Write permitted |
| | Notify | This specifies whether to enable SNMP MIB trap notifications. | (Checked)=Enabled Additionally, specify the item from the pulldown menu. none: Read-out not permitted all: Read-out permitted |

Authentication tab

| Item Name | | Description | Parameter |
|-----------|-------------------------------|--|--|
| Account | | | |
| | Change Administrator Password | This specifies whether to change the administrator password. | (Checked)=Administrator password changed |
| | Password | This specifies a new administrator password. | Enter the password. |

NTP tab

| Item Name | | Description | Parameter |
|----------------------|----------------------|---|--|
| Auto Time Adjustment | | | |
| | Auto Time Adjustment | | (Checked)=Enabled |
| | Server Setting | | (Checked)=Enabled (Unchecked)=Disabled |
| | | Protocol (Time/SNTP) | Time=TCP used SNTP=UDP used |
| | | Address | Enter the IP address of the time-provider server. |
| | Interval Setting | | (Checked)=Enabled (Unchecked)=Disabled |
| | | Interval Setting (On Startup/Period) | On Startup=Adjusted upon startup Period Specification=Execute during arbitrary period Additionally, enter the period on the screen. |
| | | Set time zone | (Checked)=Enabled (Unchecked)=Disabled |
| | | Time Zone from GMT | This specifies the time zone used by a device. Select the item from the pulldown menu. |

STP tab

| Item Name | | Description | Parameter |
|--------------------------------------|-----|--|--|
| STP (Spanning Tree Protocol) Setting | | | |
| | STP | This specifies whether to enable STP settings. | (Checked)=Enabled Additionally, select the item from the pulldown menu. |

C.6.2 Profiles for VDXs**SNMP tab**

| Item Name | | Description | Parameter |
|--------------------------------|----------------------|---------------------------------|--|
| SNMP Service | | | |
| | SNMP Service Setting | | (Checked)=Used (Unchecked)=Not used |
| | | SNMP Agent and Trap (ON/OFF) | ON=Function enabled OFF=Function disabled |
| Group (for Community and User) | | | |
| | Group Name | | This specifies a group name. Enter the group name. |
| | SNMP Version | | This specifies the SNMP version. Select the item from the pulldown menu. v1, v2c or v3 |
| | | v3 Security Level | This specifies the security level for SNMPv3. Select the item from the pulldown menu. |

| Item Name | | Description | Parameter |
|----------------------|----------------|---|--|
| | | | auth, noauth or priv |
| | Read | This specifies whether to enable SNMP MIB read. | (Checked)=Enabled Additionally, specify the item from the pulldown menu. none: Read not permitted all: Read permitted |
| | Write | This specifies whether to enable SNMP MIB write. | (Checked)=Enabled Additionally, specify the item from the pulldown menu. none: Write not permitted all: Write permitted |
| | Notify | This specifies whether to enable SNMP MIB trap notifications. | (Checked)=Enabled Additionally, specify the item from the pulldown menu. none: Read-out not permitted all: Read-out permitted |
| Community (for Host) | | | |
| | Community Name | This specifies an SNMP community name. | Enter the community name strings. |
| | Group | This specifies the group which a community belongs to. | (Checked)=Enabled Additionally, select a group from the pulldown menu. |
| | Write | This specifies whether to enable SNMP community write. | (Checked)=Enabled Additionally, select the item from the pulldown menu. Enabled or Disabled |
| Hosts | | | |
| | Address | This specifies the IP address of an SNMP host. | Enter the IP address of the host with the strings based on IPv4 or IPv6 address notations. |
| | Community Name | This specifies an SNMP community name. | Select the item from the pulldown menu. |
| | Severity Level | This specifies the SNMP trap level. | Select the item from the pulldown menu. |
| | Trap Version | This specifies the SNMP trap version. | Select the item from the pulldown menu. v1 or v2c |
| | UDP Port | This specifies an SNMP trap sending port. | Enter the SNMP trap sending port. The value between "0" and "65535" can be specified. |
| User (for v3 Host) | | | |
| | User Name | This specifies an SNMP user name. | Enter the user name between 1 and 64 characters. |
| | Group | This specifies an SNMP group name. | Enter the group name between 1 and 64 characters. |

| Item Name | | Description | Parameter |
|-----------|-------------------------|--|---|
| | Authentication Setting | This specifies whether to enable SNMP authentication settings. | (Checked)=Enabled |
| | Authentication Protocol | This specifies the SNMP authentication protocol. | Select the item from the pulldown menu. MD5, SHA or NoAuth |
| | Authentication Password | An SNMP authentication password is entered. | Enter the authentication password between 1 and 32 characters. |
| | Privacy Setting | This specifies whether to enable SNMP privacy settings. | (Checked)=Enabled |
| | Privacy Protocol | This specifies SNMP privacy protocol. | Select the item from the pulldown menu. DES, AES128 or NoPriv |
| | Privacy Password | This specifies an SNMP privacy password. | Enter the privacy password strings between 1 and 32 characters. |
| v3 Host | | | |
| | Address | This specifies the IP address of an SNMP host. | Enter the IP address of the host with the strings based on IPv4 or IPv6 address notations. |
| | User Name | This specifies an SNMP user name. | Enter the user name between 1 and 16 characters. |
| | Severity Level | This specifies the SNMP trap level. | Select the item from the pulldown menu. |
| | Notify Type | This specifies an SNMP notify type. | Select the item from the pulldown menu. |
| | Engine ID | This specifies an SNMP engine ID. | Specify the engine ID "0:0:0:0:0:0:0:0" to "FF:FF:FF:FF:FF:FF:FF:FF" with strings. Its character strings pattern is the same as that of MAC address. |
| | UDP Port | This specifies an SNMP trap sending port. | Enter the SNMP trap sending port. The value between "0" and "65535" can be specified. |

Authentication tab

| Item Name | | Description | Parameter |
|-----------|-------------------------------|--|---|
| Account | | | |
| | Change Administrator Password | This specifies whether to change the administrator password. | (Checked)=Administrator password changed |
| | Password | This specifies a new administrator password. | Enter the password between 8 and 32 characters. |

NTP tab

| Item Name | | Description | Parameter |
|----------------------|----------------------|--|-------------------|
| Auto Time Adjustment | | | |
| | Auto Time Adjustment | This specifies whether to enable auto time adjustment. | (Checked)=Enabled |

| Item Name | | Description | Parameter |
|-----------|--|----------------|--|
| | | Server Setting | This specifies whether to enable the settings for a time-provider server. (Checked)=Enabled (Unchecked)=Disabled |
| | | Address | This specifies the IP address of a time-provider server. Enter the IP address of the time-provider server with the character strings based on IPv4 or IPv6 address notations. |
| | | Set time zone | This specifies whether to enable time zone setting. (Checked)=Enabled (Unchecked)=Disabled |
| | | Region City | This specifies region information. Enter the region information in the form of (Region)/(City). |