FUJITSU Software
ServerView Infrastructure Manager V2.0

User's Manual

CA92344-1471-02
March 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 operation and management software that manages and operates ICT equipment, such as servers and storages, and facility equipment, such as PDUs, comprehensively.

Related Manuals

Manual Name	Notation in this Manual	Description
FUJITSU Software ServerView Infrastructure Manager V2.0 User's Manual	ServerView Infrastructure Manager V2.0 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 V2.0 Start Guide	ServerView Infrastructure Manager V2.0 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 V2.0 Operations Manual	FUJITSU Software ServerView Infrastructure Manager V2.0 Operations Manual	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 V2.0 Glossary	ServerView Infrastructure Manager V2.0 Glossary	The glossary provides definitions of the terminology that you need 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 Intel 64)	RHEL 7.2	
Red Hat Enterprise Linux 7.1 (for Intel 64)	RHEL 7.1	
Red Hat Enterprise Linux 6.8 (for Intel 64)	RHEL 6.8 (Intel64)	
Red Hat Enterprise Linux 6.8 (for x86)	RHEL 6.8 (x86)	
Red Hat Enterprise Linux 6.7 (for Intel 64)	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® vSphere™ ESXi 6.5	VMware ESXi 6.5	VMware ESXi
VMware® vSphere™ ESXi 6.0	VMware ESXi 6.0	
VMware® vSphere™ ESXi 5.5	VMware ESXi 5.5	

Terms

For the major terms and abbreviations used in this manual, see "ServerView Infrastructure Manager V2.0 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 needs 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

Contents

Chapter 1 Overview of ServerView Infrastructure Manager

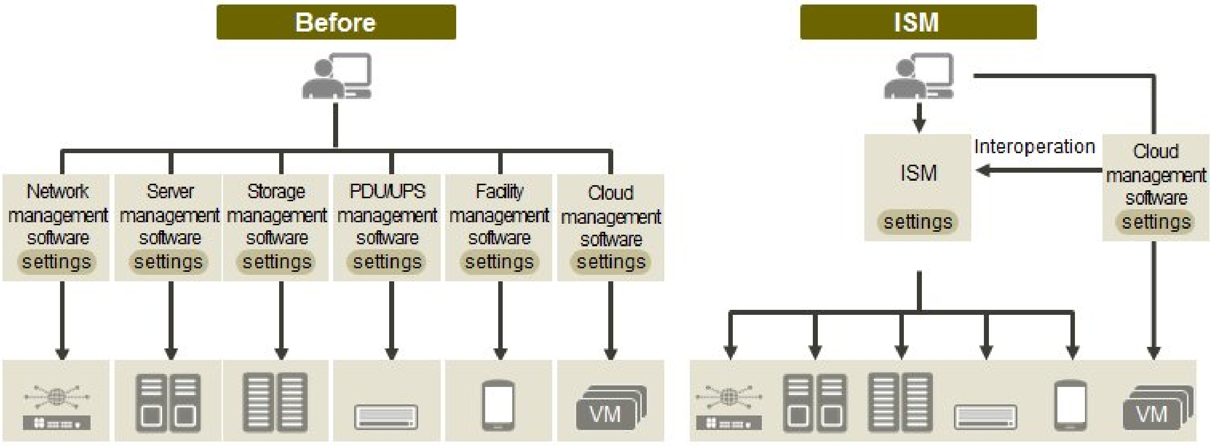
This chapter provides an overview of ServerView Infrastructure Manager.

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



Before
Network management software
settings
Server management software
settings
Storage management software
settings
PDU/UPS management software
settings
Facility management software
settings
Cloud management software
settings
VM
ISM
ISM
settings
Interoperation
Cloud management software
settings
VM

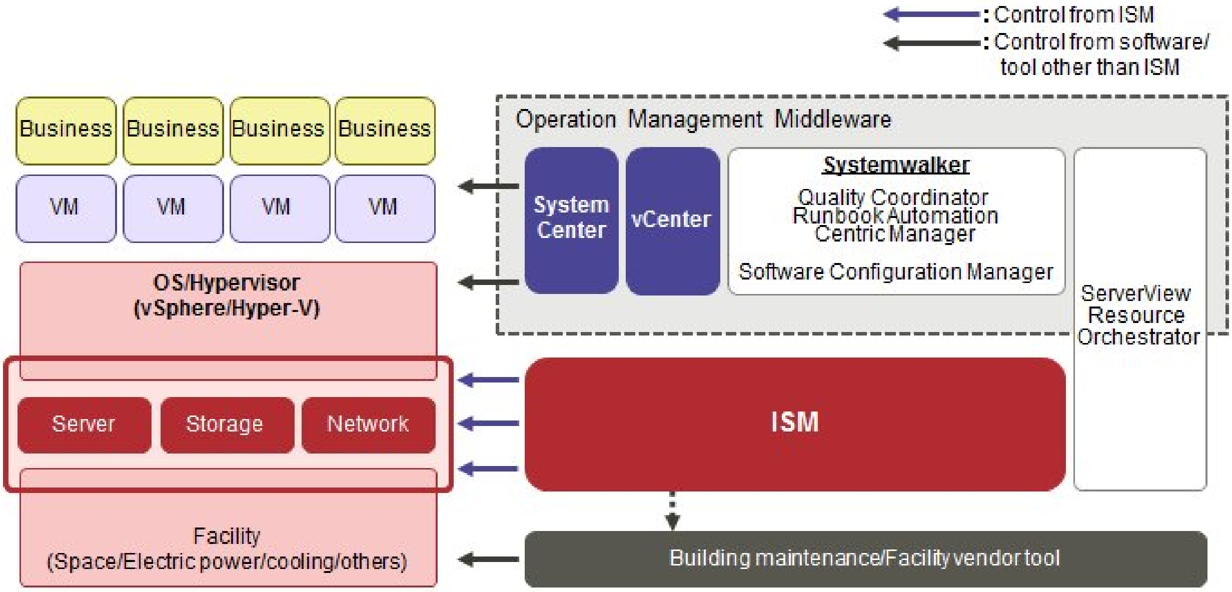
- Required respective operations and settings on tools used individually.
- Required respective designs and managements for operating systems including Interoperation of infrastructure.

- Enables an entire system operation on one screen with viewing the whole for infrastructure.
- Enables batch operation including infrastructure cooperating with plug-in Cloud management software and using tools you accustomed.

- Optimization of largely centralized operations of physical layers that reach to servers, storages, and networks
  - Collection and management of hardware assets and configuration information
  - Integration of multiple management screens into a single software suite
  - Unified 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


: Control from ISM
: Control from software/ tool other than ISM
Business
Business
Business
Business
VM
VM
VM
VM
OS/Hypervisor (vSphere/Hyper-V)
Server
Storage
Network
Facility (Space/Electric power/cooling/others)
Operation Management Middleware
System Center
vCenter
Systemwalker
Quality Coordinator
Runbook Automation
Centric Manager
Software Configuration Manager
ServerView Resource Orchestrator
ISM
Building maintenance/Facility vendor tool

1.2 Overview of function

This section provides 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 detect 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 locations 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 implements batch settings for the BIOS, iRMC as well as installation of OSes.

- Function for network switches:

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

- Function for ETERNUS storages:

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

To make node settings or install an OS, implement 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 any time as needed
- 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 any version as needed (can also be implemented 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 a centralized 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 the information of the physical network between managed nodes and port information on the Network Map
- Confirming the changes in the information of the network connection between managed nodes
- Confirming the virtual connections of the physical ports, the virtual switches and the virtual machines of the managed nodes
- 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."

1.3 ISM Functions and Scenarios of Infrastructure Operation and Management

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

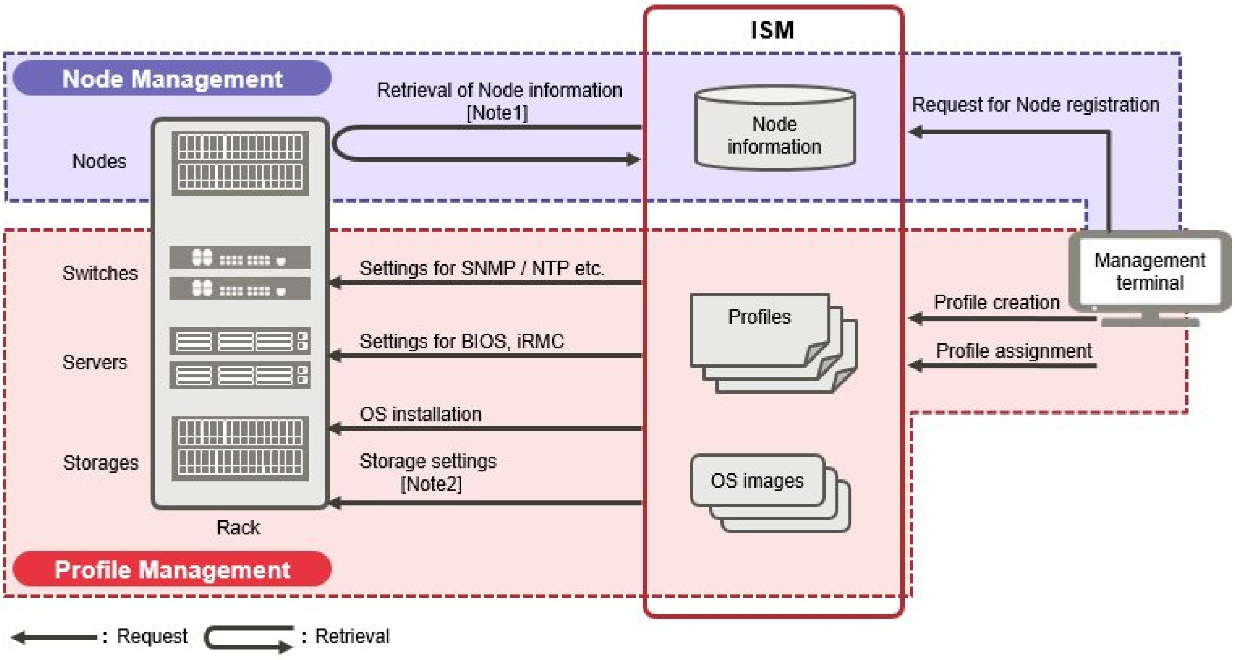
ISM function	Scenario of operation and management		
	System Configuration	Monitoring operations for managed nodes	Maintenance of managed nodes
Node Management	Y	Y	-
Monitoring	-	Y	-
Profile Management	Y	-	-
Log Management	-	Y	Y
Firmware Management	-	-	Y
Network Management	-	-	Y

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 1.3 Image of functions: system configuration



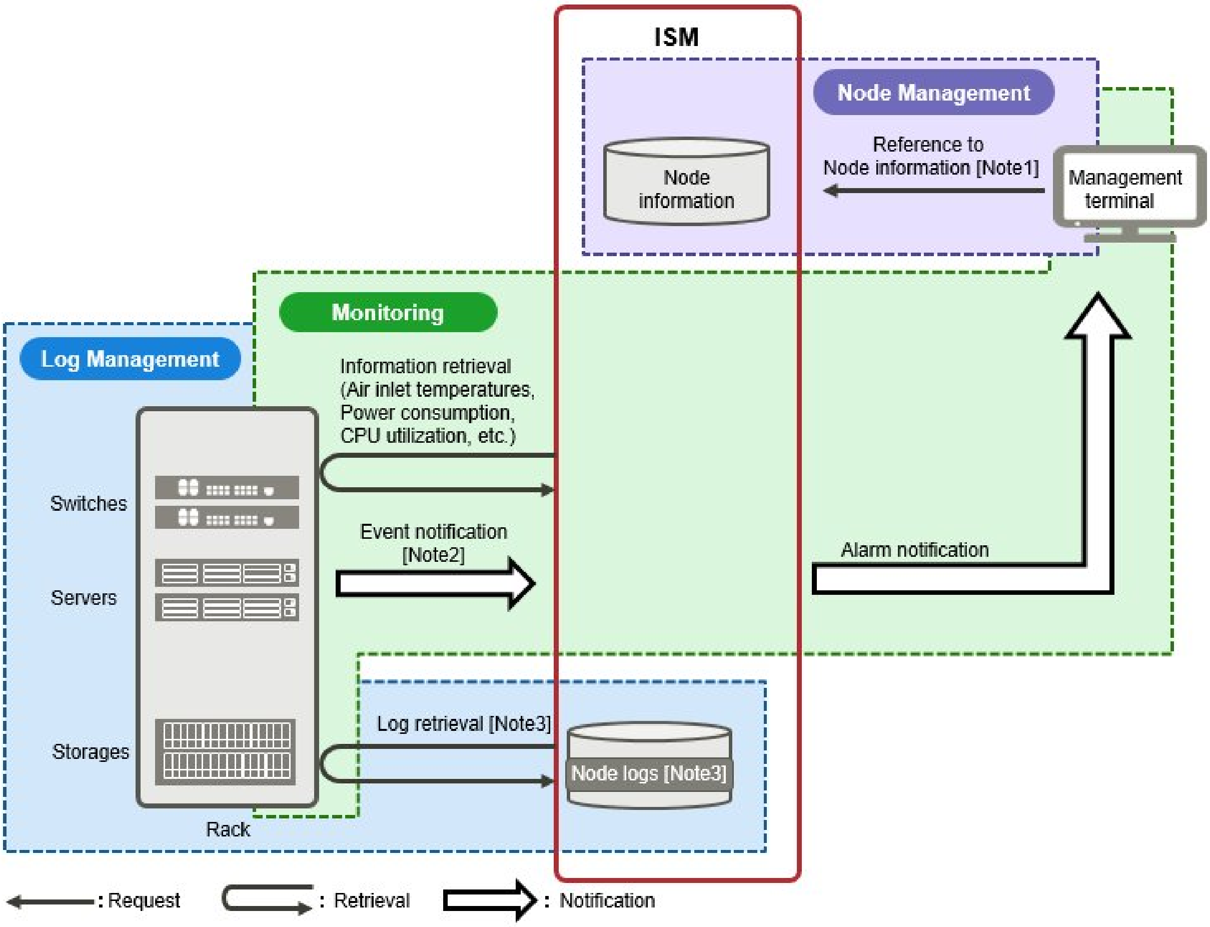
[Note 1] Model names, serial numbers, IP addresses, and similar hardware information

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

(2) Monitoring operations for managed nodes

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 1.4 Image of functions: monitoring operations for managed nodes



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

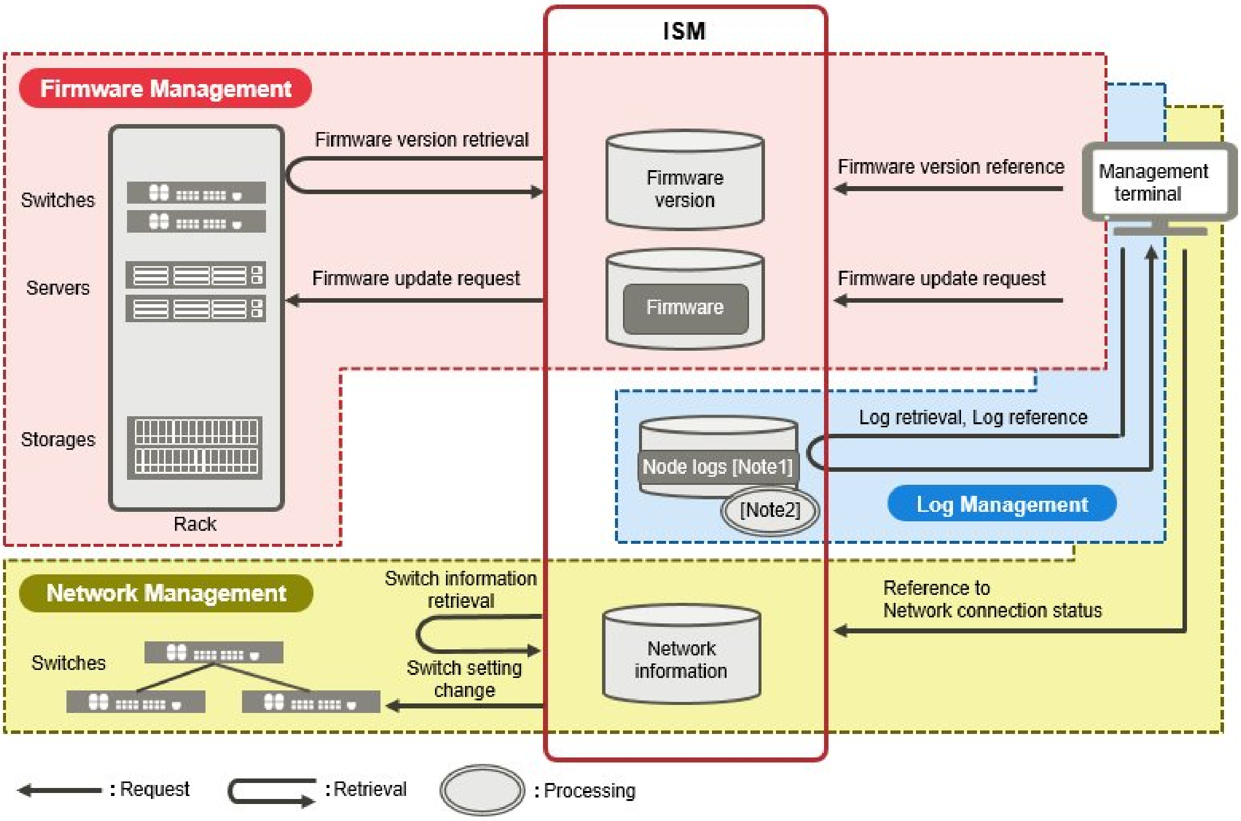
[Note 2] SNMP traps

[Note 3] 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 effectively using the Log Management, Firmware Management, and Network Management functions.

Figure 1.5 Image of functions: maintenance of managed nodes



[Note 1] Hardware logs and operating system logs

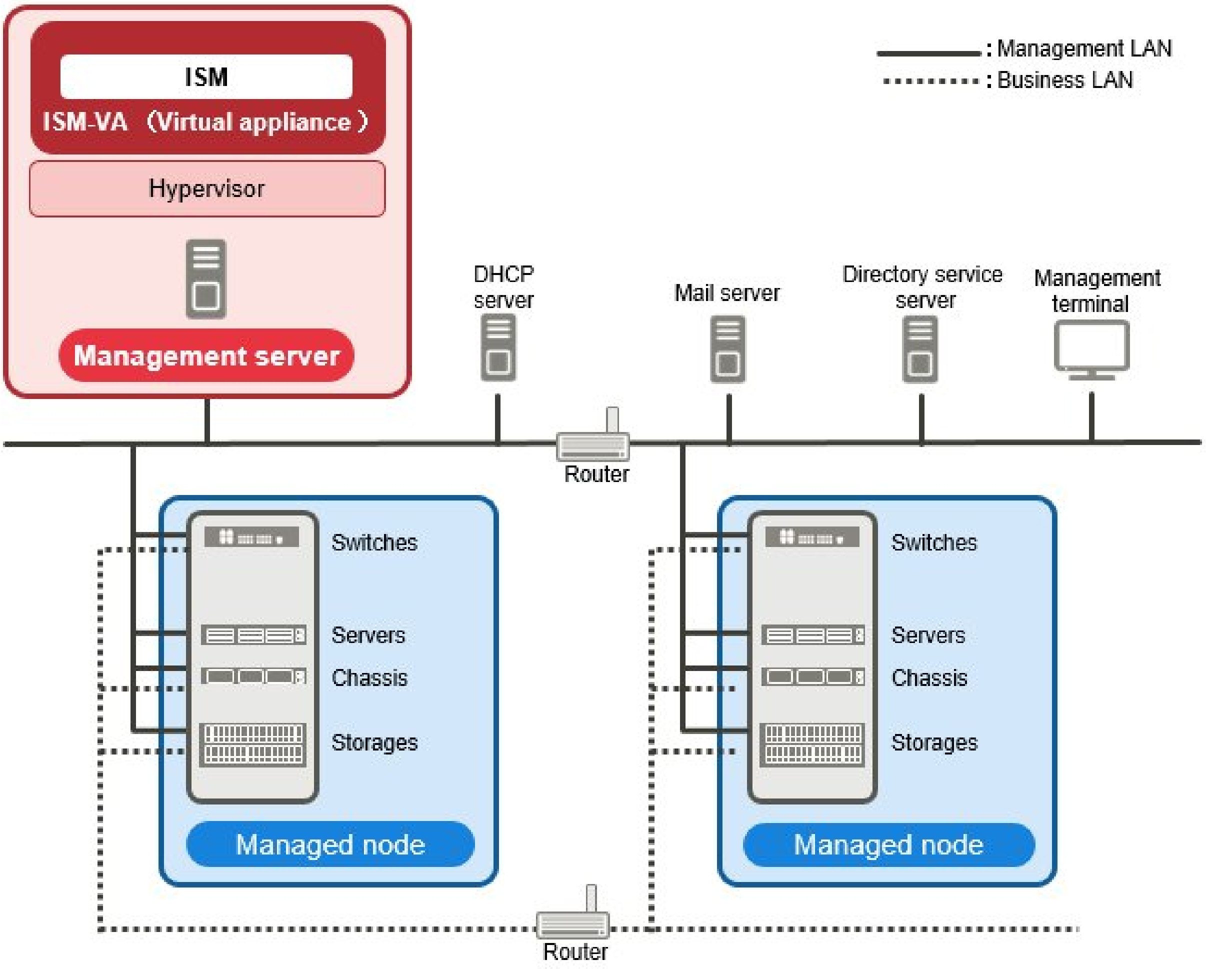
[Note 2] Processing of log searches

1.4 Configuration

In principle, ISM runs on a server that is separate from the servers to be managed. This manual calls 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 1.6 Network configuration



Note

For details on the server prepared externally to ISM described in Figure 1.6 Network configuration, 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.
	Business LAN	LAN used for transferring business 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		Personal computer 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.

Device and function		Description
	Storage	
	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 operating environments 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 [Note 1]
Memory capacity	8 GB or more [Note 1]
Free disk space	35 GB or more [Note 2] [Note 3] [Note 4]
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

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

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

[Note 2] This is the minimum disk capacity required for monitoring approximately 100 nodes. The disk space needs 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."

[Note 3] For backing up ISM-VA, a management server with free disk space equivalent to or larger than that of ISM-VA is required.

[Note 4] 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

Item	Description
Display	- Personal computer and server: 1280 x 768 pixels or more The window size of your browser for displaying the GUI of ISM must be at least 1280 x 768 pixels. - Tablet: display mounted to devices stated above
Network	100 Mbps or higher
Web browser	- PC and server: - Internet Explorer In order to display the "3D View" screen, update version (11.0.15 or higher) must be applied. - Microsoft Edge - Mozilla Firefox - Google Chrome - iPad: Safari 8 - Android tablet: Google Chrome
Related software	Acrobat Reader (for viewing manuals)

For the latest information on supported devices and 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)	An mail server is required when sending notification mails for abnormalities and changes in the statuses of managed nodes. Set up with [Settings] - [Alarms] - [SMTP Server]. Note In ISM only one mail server can be registered.
Directory services server	A directory server is required if using the following services. 1. When using it in User Management of ISM You can use the following two directory services.

Item	Description
	- OpenLDAP - Microsoft Active Directory Register the configured server in [Settings] - [General Settings] - [LDAP Server Setting]. 2. When using it in OS installation in Profile Settings of 1 as above is not used. The directory service, specified in the settings items in OS installation of Profile, is used. For details, see OS installation of Profile. Note - 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.
DHCP server	In the following cases it is required to set up a DHCP server. - When OS installation is done using the profile management function - When using the Offline Update of the firmware management function To enable PXE boot on the managed node (server), set it so that an appropriate IPv4 address can be leased to the node. Point The DHCP server function inside ISM-VA can be used instead of preparing a separate DHCP server. For how to use the DHCP function in ISM-VA, see "4.19 DHCP server inside ISM-VA."
DNS server	In the following cases it is required to set up a DNS server. - Accessing ISM by hostname. - Using FQDN for a variety of sever settings of ISM (such as operations in link with LDAP). For the method of setting up the server, see "Add DNS server" in "4.9 Network Settings." Point - 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 Modifying 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.
NTP server	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. Use ismadm command when you set up the NTP server for ISM. For how to set it up, see "Enable/Disable NTP synchronization" and "Add/Remove NTP server" in "3.4.2 Initial Settings of ISM."
Proxy server	A Proxy server is required when accessing ISM from a management client via a Proxy server.

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

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 need 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 configuration needs 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, implement a manual log collection to confirm that the log files are accumulated correctly and that there is no log collection error recorded in the [Event/Task] - [Event] - [Operations Log].

- If the volume of the log files reaches the "Warning threshold" set in "Node log" or "Archived Log" set for each user group in [Various Settings] an alert event will be registered in ISM events. Delete logs that are no longer needed. 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 V2.0 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 click [Certificates].
  3. Click [View Certificates].
  4. On the [Servers] tab, click [Add Exception].
  5. Under [Location], enter "https://<IP address of ISM server> or <FQDN name of ISM server>:25566/", and then click [Get Certificate].
  6. Confirm that the [Permanently store this exception] checkbox is checked, and then click [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, click the [Custom level] button and select [Enable] for the following items before you click 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 click 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 locations 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 confirm 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 click the [Login] button.

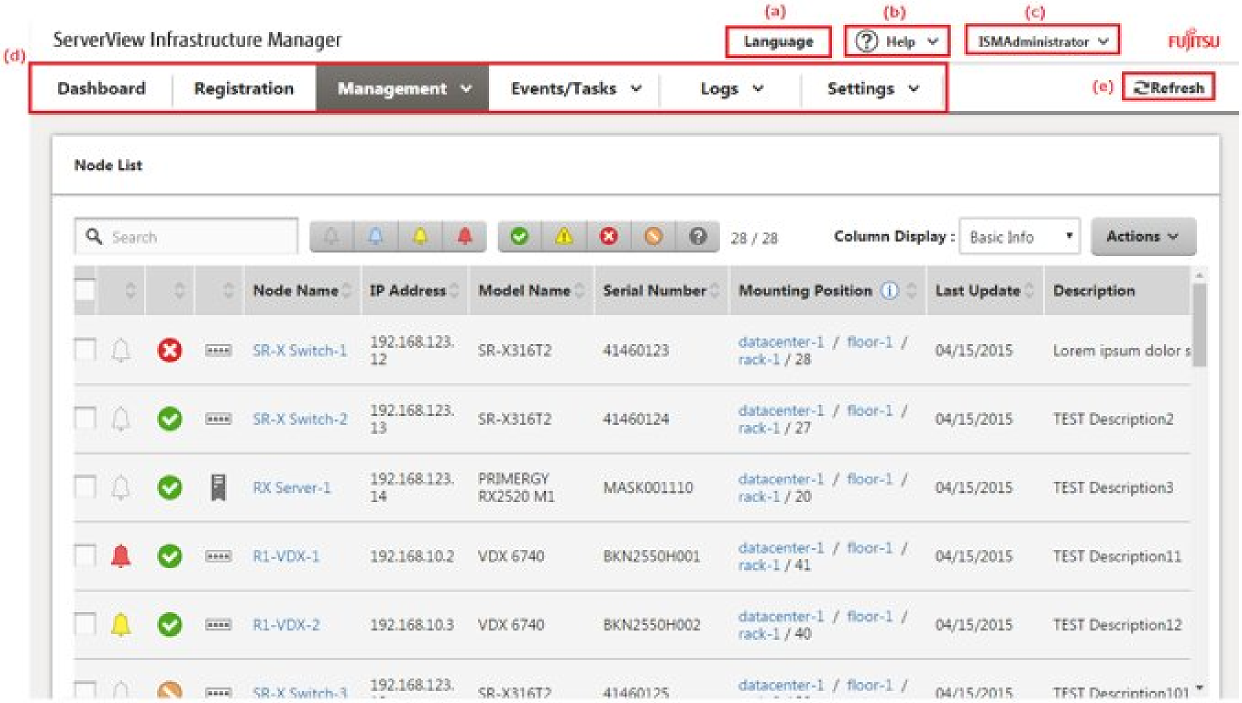
   If a warning for the security certificate is displayed, see "4.7 Certificate Activation" and do the authentication settings.

   ## 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.



				Node Name	IP Address	Model Name	Serial Number	Mounting Position	Last Update	Description
□		✗		SR-X Switch-1	192.168.123.12	SR-X316T2	41460123	datacenter-1 / floor-1 / rack-1 / 28	04/15/2015	Lorem ipsum dolor s
□		✓		SR-X Switch-2	192.168.123.13	SR-X316T2	41460124	datacenter-1 / floor-1 / rack-1 / 27	04/15/2015	TEST Description2
□		✓		RX Server-1	192.168.123.14	PRIMERGY RX2520 M1	MASK001110	datacenter-1 / floor-1 / rack-1 / 20	04/15/2015	TEST Description3
□		✓		R1-VDX-1	192.168.10.2	VDX 6740	BKN2550H001	datacenter-1 / floor-1 / rack-1 / 41	04/15/2015	TEST Description11
□		✓		R1-VDX-2	192.168.10.3	VDX 6740	BKN2550H002	datacenter-1 / floor-1 / rack-1 / 40	04/15/2015	TEST Description12
□				SR-X Switch-3	192.168.123.	SR-X316T2	41460125	datacenter-1 / floor-1 /	04/15/2015	TEST Description101

(a) Language

You can change the settings for the displayed Language, Date Format and Time Zone on the GUI.

(b) Help

You can access help and guidance information.

(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 click [Log out].

(d) Global Navigation menu

This menu serves to access the various screens of ISM.

(e) Refresh button

Clicking 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 click the [Refresh] button to update the screen.

If automatic refresh is set up for the following screens, the screens will be 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.

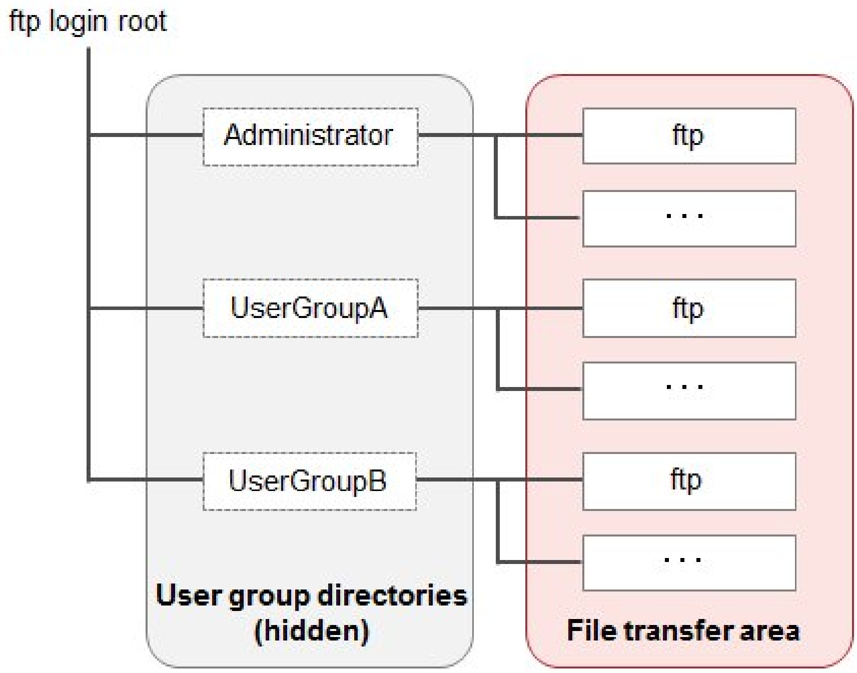
Immediately after login, the files and directories are hidden from the display for security reasons; go to the directory with the group name to which the login user belongs and access the file transfer area from there.

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. See "2.3.1.2 Managing User Groups" for details.
- 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.
- 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

Point

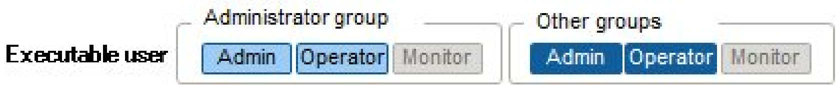
In order to allow users to use the various ISM functions, it is required that privileges (user roles) to access the user group in which each respective user is registered are allocated. For details on Node Management, see "2.3.1 User Management."

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	Admin	
	Operator role	Operator	Operator
	Monitor role	Monitor	Monitor
Other than administrator group	Administrator role	Admin	Admin
	Operator role	Operator	Operator
	Monitor role	Monitor	Monitor

In the following explanations, 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.

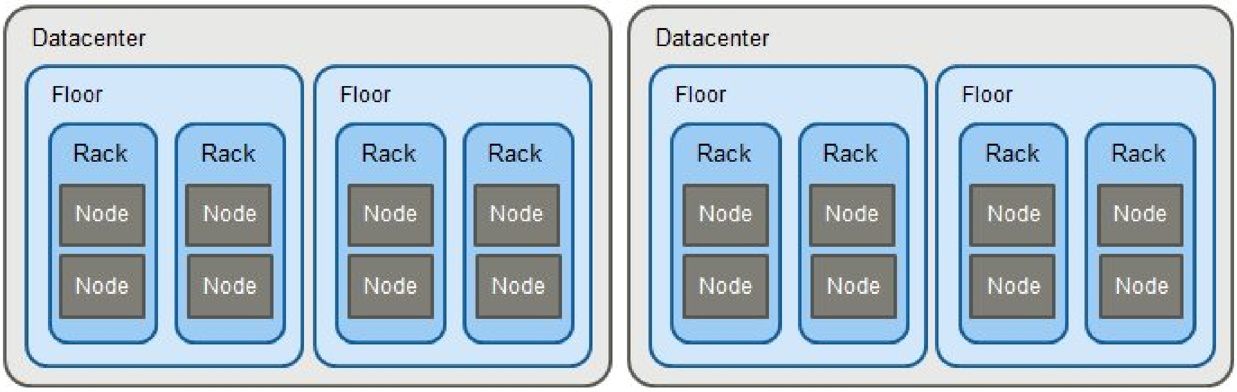
- 2.2.1.1 Registering Datacenters/Floors/Racks/Nodes
- 2.2.1.2 Confirming Datacenters/Floors/Racks/Nodes
- 2.2.1.3 Editing Datacenters/Floors/Racks/Nodes
- 2.2.1.4 Deleting Datacenters/Floors/Racks/Nodes

2.2.1.1 Registering 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

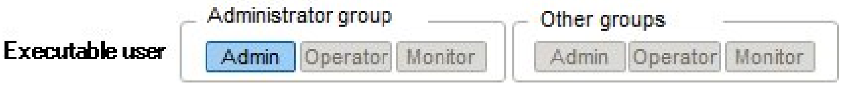


You can make the following operations:

- 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 Detection

Registration of datacenters/floors/racks

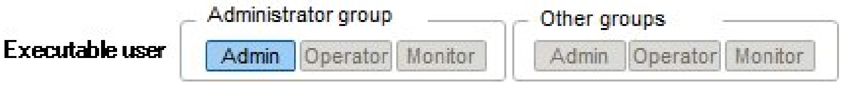


You can additionally register information on datacenters, floors, and racks in ISM. The datacenter, floor, and rack names to be registered must be set to unique names in ISM.

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

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

Registration of nodes



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
- Detecting and then registering nodes with the detection function of ISM

The following is a sample operation for manual registration in ISM. For the registration method that uses the detection function, see "Node Detection."

1. Confirm the device information that is required for node registration.

   Before node registration, it is required to confirm information such as the model names of devices to be registered and which IP addresses are set.

2. Enter the information that is required for registration.

   - Node Name

     Set a name that is unique across the entire ISM system.

   - Node Type

     Select the type of node to be registered.

   - Model

     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 needed.

3. Enter the account information for each node.
4. Enter the information for each node's installation position in the racks.
5. Select the node group(s) to which each node is going to belong.

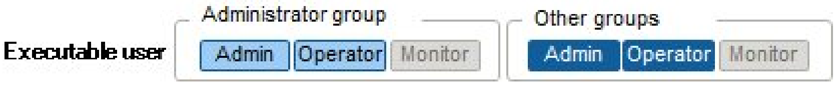
   If you do not specify a node group, the node is handled as not allocated to a node group. Nodes that are not allocated can be managed only by a user belonging to an Administrator group.

6. Execute the registration.

Point

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

Management of node information



On the "Management" screen, you can select a node and confirm its 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.

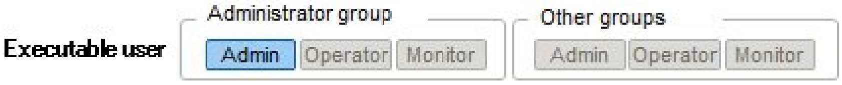
The following is a sample operation for retrieving the node information.

1. From the Global Navigation menu on the GUI of ISM, select [Management] - [Nodes] and open the "Node List" screen.
2. Select the node name of the applicable node and open the [Properties] tab.
3. Click the [Actions] button and select [Get Node Information].

   As soon as retrieval of the node information is complete, a log with the Message ID "10020303" is output to the [Event/Task] - [Event] - [Operations Log].

4. Click the [Refresh] button to update the display on the [Properties] tab.

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

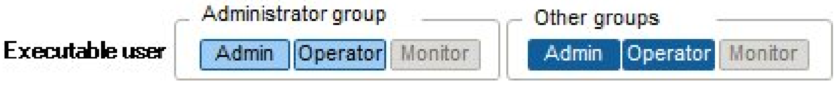
  You can set the information on installation positions in racks when you carry out node registration. Alternatively, you can also make the settings after node registration.

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] and open the "Node List" screen.
2. Select the applicable node, click the [Actions] button, and then select [Set Node Position].
3. Select the rack in which the node is mounted.
4. Select and then apply the location 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.

Note

- 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 need 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.

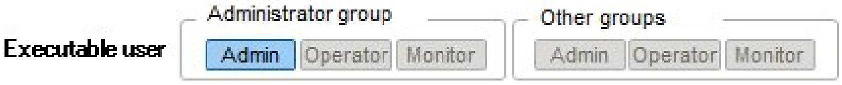
- Enter the domain name with uppercase letters when you register OS information.

The following is a sample operation.

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

   As soon as retrieval of the node information is complete, a log with the Message ID "10020303" is output to the [Event/Task] - [Event] - [Operations Log].
6. Click the [Refresh] button to update the display on the [OS] tab.

Node Detection



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

Detections have to be executed manually. You can make the following operations:

- Creating settings for manual detection and executing detections
- Confirming results of manual detection
- Registering detected nodes

Registering settings for manual detection

Set the required information for manual detection. Node Detection 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 detection, it is required to set the required account information for connecting to the nodes you want to detect.

The protocol used for detection varies with the type of node to be detected.

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

1. Open the "Registration" screen on the GUI.
2. Click the [Actions] button and select [Manual Discovery].
3. Enter the required information for manual detection.
4. Execute manual detection.

Confirming results of manual detection

Refresh the display for "Discovery Progress" on the "Registration" screen and wait until processing for detection finishes. When detection is complete, confirm the detected nodes on the "Discovered Node List" screen.

If the node information is successfully retrieved with the set account information, the status is shown as "Normal" and you can confirm the retrieved node information.

Note

- The detected node information is effective only within the same session.
- Devices that are not supported may be displayed in the manual detection results. Do not register devices that are not supported.

Registering detected nodes

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

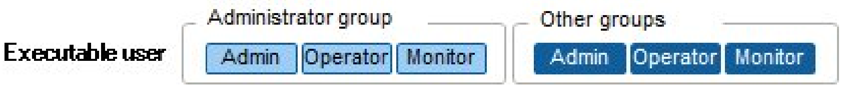
1. Confirm the detected nodes.
2. From the detected nodes, select the one(s) you want to register, then select the [Registration discovered nodes] button.
3. Enter the information that is required for node registration, such as node name, chassis name, web i/f URL, description.
4. Set the information 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 Detection is registered as account information for the node.

2.2.1.2 Confirming Datacenters/Floors/Racks/Nodes

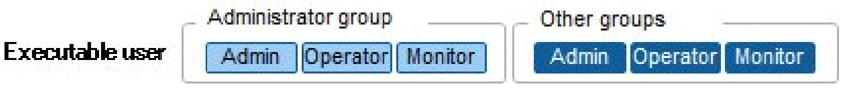
Here, you can confirm the information that is registered in ISM.

Confirming datacenters/floors/racks



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

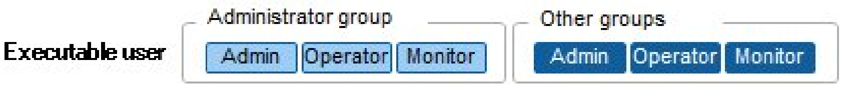
Confirming nodes



Confirm the nodes that are registered in ISM.

From the Global Navigation menu on the GUI of ISM, select [Management] - [Nodes] and open 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



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.

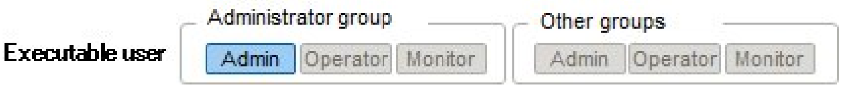
In this case, only the information items that can be retrieved with the domain user's access rights are displayed on the GUI.

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

2.2.1.3 Editing Datacenters/Floors/Racks/Nodes

Edit the information that is registered in ISM.

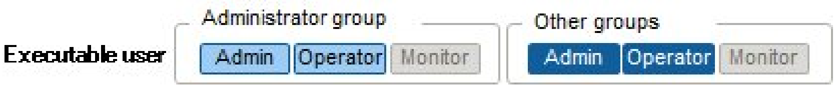
Editing datacenters, floors, and racks



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. Click the [Actions] button, and then select [Edit Datacenter], [Edit Floor], or [Edit Rack].
3. Edit information.
4. Click [Apply] to make the changed information contents effective.

Editing nodes



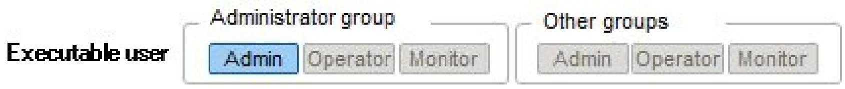
The following is the operation method for editing node information.

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

2.2.1.4 Deleting Datacenters/Floors/Racks/Nodes

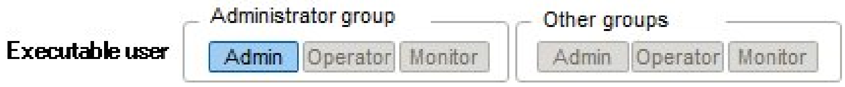
Delete any information that is registered in ISM.

Deletion of datacenters



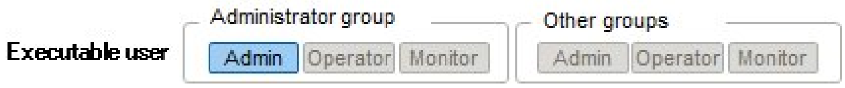
If you are going to delete a datacenter, you cannot do so if any floors are registered in that datacenter. Delete or move any floors before you delete the datacenter.

Deletion of floors



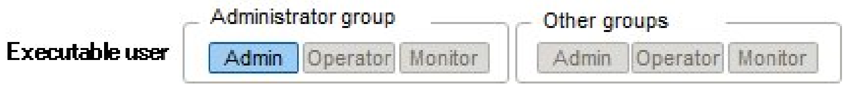
If you are going to delete a floor, you cannot do so if any racks are registered on that floor. Delete or move any racks before you delete the floor.

Deletion of racks



If you are going to delete a rack, you cannot do so 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

  Click the Refresh button.

- For Network Map

  Click the [Actions] button and 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.

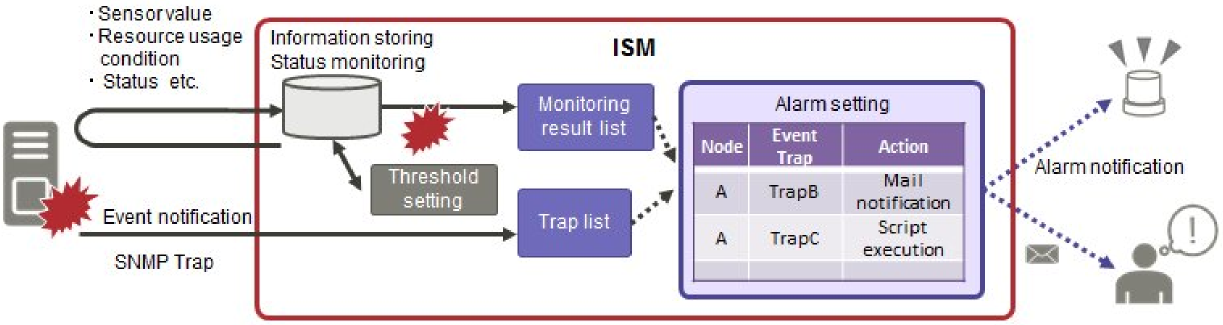
2.2.2 Monitoring

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.

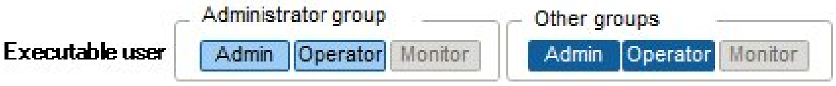
Figure 2.3 Image of Monitoring



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



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.

Default monitoring item	Description
Statuses of the various LEDs	Power LEDs, CSS LEDs, Identify LEDs, and Error LEDs are monitored. This is only applicable for PRIMERGY.

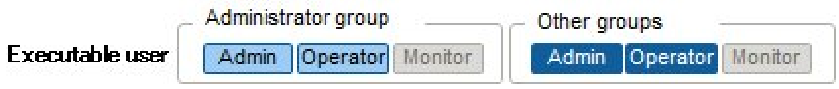
The following items can be additionally specified to be monitored.

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. Only nodes that are included in the power capping settings and where the power capping function is activated are monitored.

Procedure for adding monitoring items and threshold values

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

Action settings



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.
Trap forwarding	Forward the sent SNMP trap to the external SNMP manager. The following forwarding types can be selected. - Forward ISM as the sender The send SNMP trap will be processed as if it was sent straight from ISM. Apart from information on the sender, the trap information will be sent as it is. - Send received trap as it is. The received trap will be forwarded to the ISM manager as it is.

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)

Method of notation of macro	Overview
$_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 [Settings] - [Alarms].
2. Select [Actions] from the menu on the left side of the screen to open the "Action List" screen.
3. Click the [Actions] button on the right side of the screen and 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 Registering 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 [Settings] - [Alarms].
2. Select [SMTP Server] from the menu on the left side of the screen to open the "SMTP Server Settings" screen.
3. Click the [Actions] button on the right side of the screen and select [Edit] to register the 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 transfer 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 Registering Certificates for Event Notification Mails."

Trap forwarding

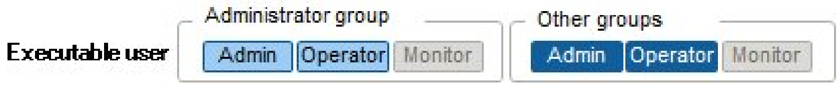
When transferring an SNMP

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

2. Select [SMTP Manager] from the menu on the left side of the screen to open the "SMTP Manager Settings" screen.

3. Click the [Actions] button on the right side of the screen and select [Edit] to register the SMTP manager information.

Registration of alarm settings



Alarm settings are made in advance to define what processing to implement 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 [Settings] - [Alarms].
2. Select [Alarms] from the menu on the left side of the screen to open the "Alarm List" screen.
3. Click the [Actions] button on the right side of the screen and select [Add] to add an alarm.

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

Event types

There are two types of event as follows.

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

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 detected. Alarm statuses can take on the following values.

Alarm status	Priority	Description
Error	High	This value changes when any of the following events is detected: - ISM event at Error level - SNMP trap at CRITICAL level On the GUI of ISM, this is indicated by a red bell icon (🔔)
Warning	Medium	This value changes when any of the following events is detected: - ISM event at Warning level - SNMP trap at MAJOR or MINOR level On the GUI of ISM, this is indicated by a yellow bell icon (🔔)
Info	Low	This value changes when any of the following events is detected: - ISM event at Info level - SNMP trap at INFORMATIONAL level

Alarm status	Priority	Description
		On the GUI of ISM, this is indicated by a green bell icon (🔔)
None	-	This is the status when no event is detected. On the GUI of ISM, this is indicated by a white bell icon (🔔)

An alarm status value of "Info" or higher means that an event corresponding to each level was detected. Open the "Events" screen from the [Events/Tasks] tab or the "Received Trap" screen from the [Logs] tab to confirm the contents of the detected event.

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

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

Point

- Alarm statuses are not deactivated automatically. However, if a status with a higher priority is detected, it will be displayed instead.
- Sometimes by design you may need 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.

  See "5.1 Maintenance Mode" for information on Maintenance mode.

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 do 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 will be processed as an unknown trap.
- Do not register plural MIB files for which the same trap is defined. If you have registered plural MIB files with the same trap defined, this is handled as if the plural of the same traps were received.

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 "4.20.1 Registering 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 "4.20.2 Displaying MIB Files."

Deleting MIB files

You can delete an MIB file(s) registered on ISM by deleting the corresponding MIB file. To delete the MIB file(s), execute the MIB deletion command of ISM-VA Management.

For details, see "4.20.3 Deleting 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 relationship(s), this could result in that receiving the traps is disabled.

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 as managed nodes
- Creating RAIDs/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 PRIMERGY CX	- BIOS setup - iRMC setup - OS installation
Network switch	SR-X	- Setting of administrator passwords - SNMP, NTP, and STP settings
	VDX	- Setting of administrator passwords - SNMP and NTP settings
Storage	ETERNUS DX	- 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 deactivating 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

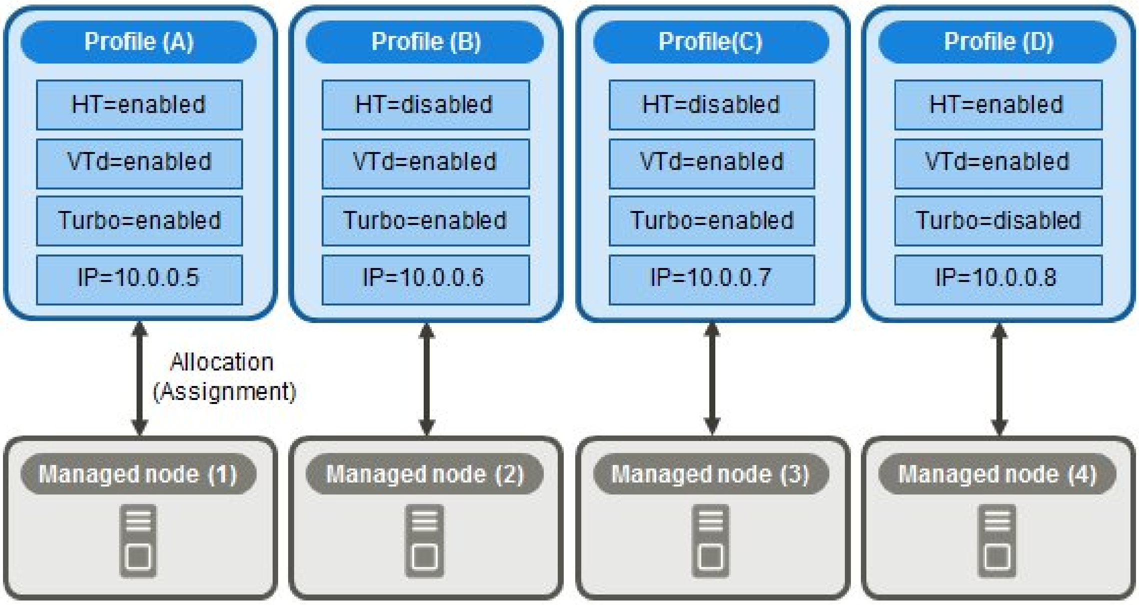
Profile usage

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 need one profile for each node to be managed by a profile.

Figure 2.4 Relationships between profiles and managed nodes

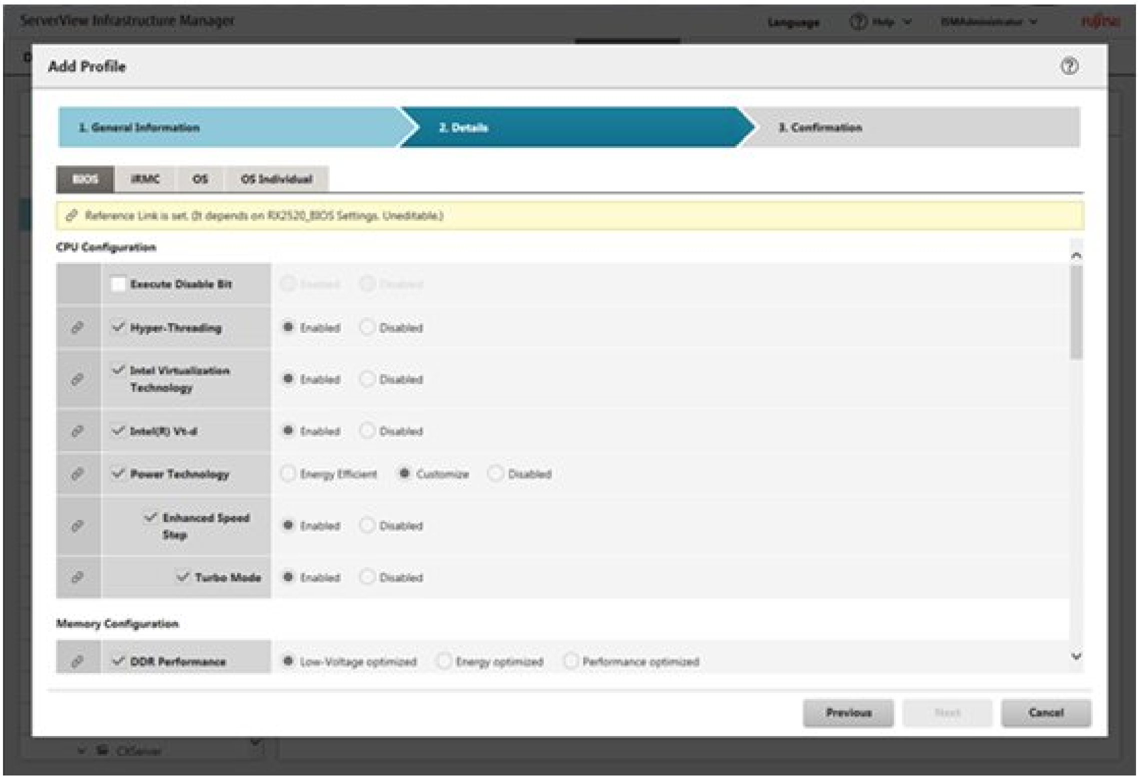


Note

When you assign a profile containing OS-related settings to a node, the OS will be newly installed 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)



Reference Link is set. (It depends on RX2520_BIOS Settings. Uneditable.)

CPU Configuration

- □ Execute Disable Bit: ○ Enabled ○ Disabled
- ✓ Hyper-Threading: ● Enabled ○ Disabled
- ✓ Intel Virtualization Technology: ● Enabled ○ Disabled
- ✓ Intel(R) Vt-d: ● Enabled ○ Disabled
- ✓ Power Technology: ○ Energy Efficient ● Customize ○ Disabled
- ✓ Enhanced Speed Step: ● Enabled ○ Disabled
- ✓ Turbo Mode: ● Enabled ○ Disabled

Memory Configuration

- ✓ DDR Performance: ● Low-Voltage optimized ○ Energy optimized ○ Performance optimized

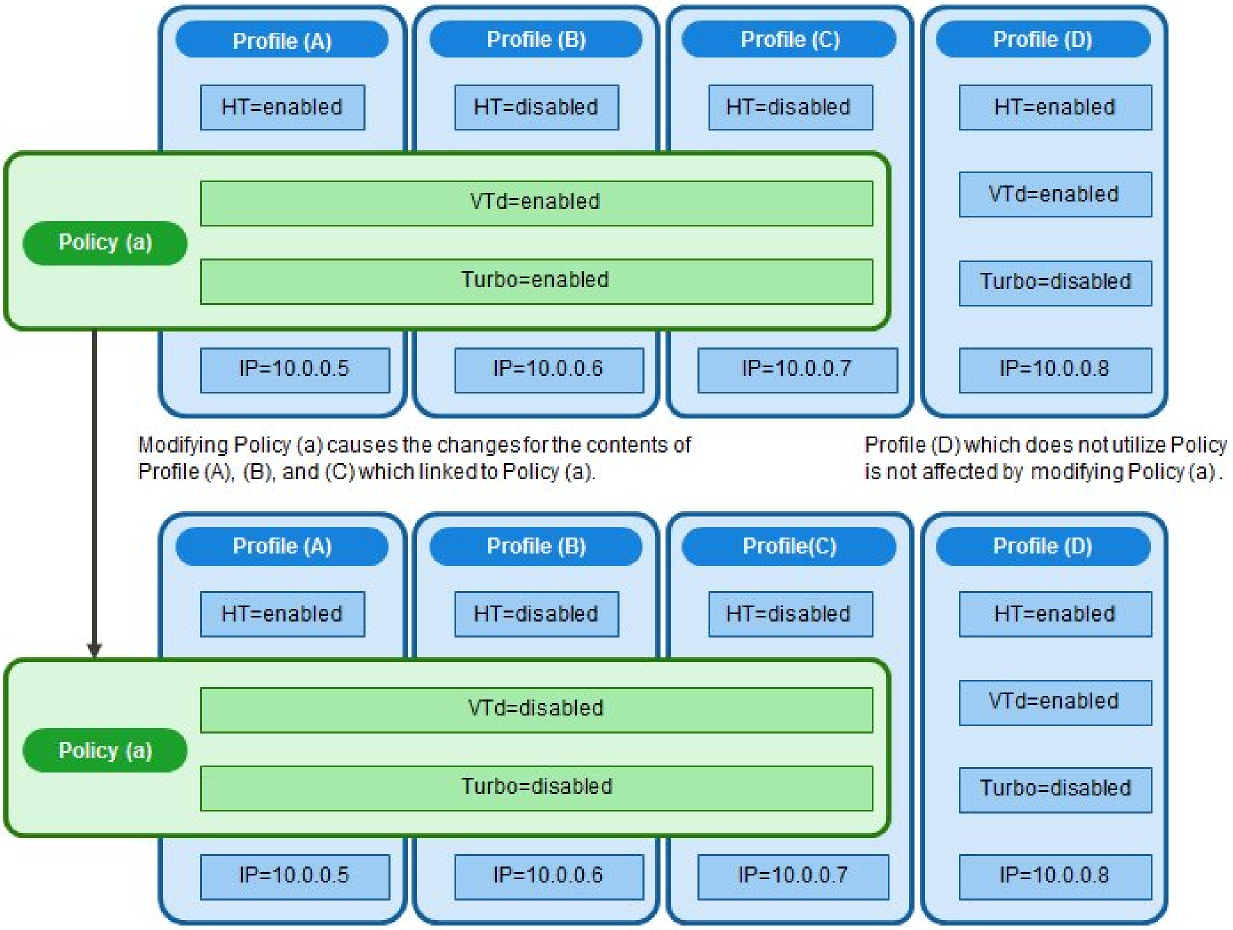
Profiles and policies

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 you can select the [Enable Advanced Settings]



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

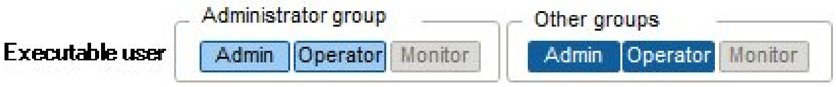
- If you are going to use a policy, be sure to create the policy before you create the profiles.
- You can use policies for the BIOS and iRMC settings on servers.

Profile groups and policy groups

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

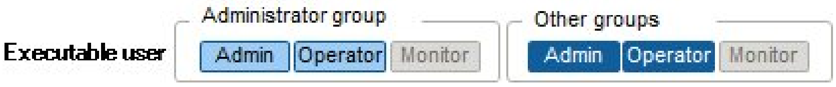
You can include profiles in profile groups, and policies in policy groups.

Procedure for creating policy groups



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

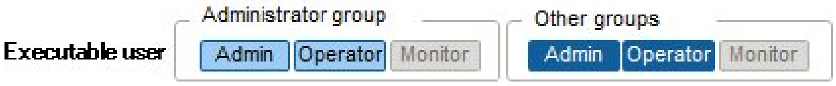
Procedure for creating policies



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

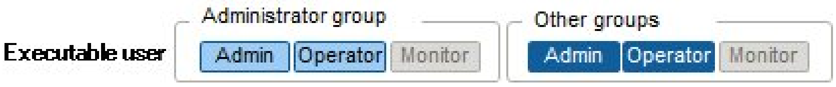
   From the policy setting items, select those setting values that you want to be reflected in the profile by selecting the corresponding checkboxes under [2. Details] in the [Add Policy] wizard. Policy setting items for which the checkbox is not selected will not take effect in the profile.

Procedure for creating profile groups



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

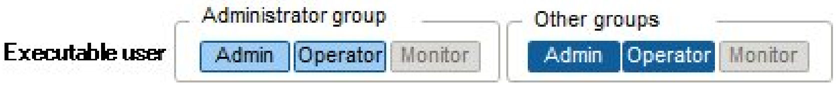
Procedure for creating profiles



1. From the Global Navigation menu on the GUI of ISM, select [Settings] - [Profiles].
2. With the location where you want to create a profile selected in the tree on the left, click 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



Note

- Performing 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, you need to prepare the required settings and files in advance. Please see the following:

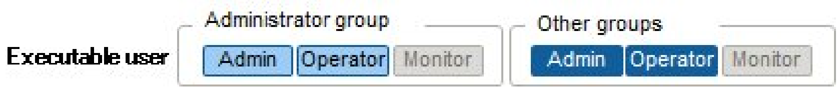
  "Required preparations before OS installation."

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 click the [Actions] button and select [Assign/Reassign Profile].

Point

Depending on the profile contents, profile assignment may require a long time to complete (for example, more than an hour). You can confirm the current progress of profile assignment on the "Task" 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. When doing so, 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 [Settings] - [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. Click the [Actions] button and select [Edit] to edit the profile.
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 click 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].

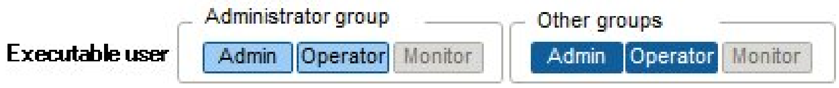
   For nodes whose settings do not match the profile, [Reassignment] is displayed under [Status].

   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 deactivating and deleting profiles



Executable user

Administrator group: Admin Operator Monitor

Other groups: Admin Operator Monitor

In the following cases, you have to deactivate 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."

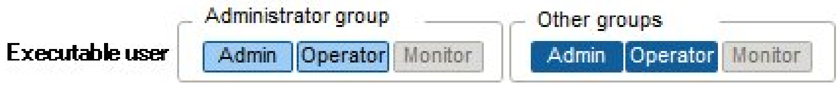
Procedure for deactivating profiles

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 click the [Actions] button and select [Release Profile].

Procedure for deleting profiles

1. From the Global Navigation menu on the GUI of ISM, select [Settings] - [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. Click the [Actions] button and select [Delete].
4. You can only delete profiles whose status is [Not Assigned].

Exporting and importing profiles



Executable user

Administrator group: Admin Operator Monitor

Other groups: Admin Operator Monitor

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 [Settings] - [Profiles].
2. Select the profiles to be exported.
3. Click the [Actions] button and select [Export].

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

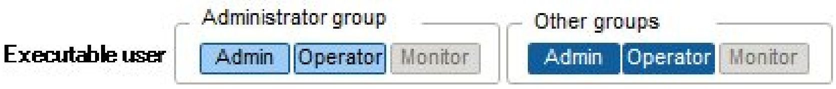
Procedure for importing profiles

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 [Settings] - [Profiles].
3. Select the location where the profile is stored in the tree on the left, click the [Actions] button and select [Import].
4. Enter the decryption password key you set up when exporting the profiles (mandatory), and then use the [Import] button to execute the import.

Point

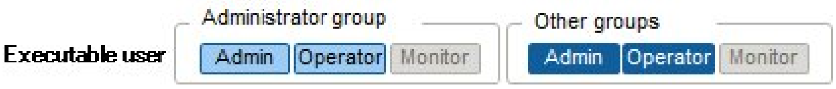
- When the import is complete, deleting the files you transferred to the FTP server in Step 1 does not cause any problem.
- Since profiles contain passwords and other security information, it is mandatory to set up a freely specifiable encryption key when you export profiles.

Procedure for editing profile groups



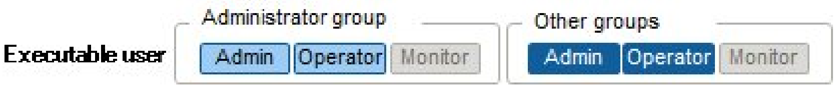
1. From the Global Navigation menu on the GUI of ISM, select [Settings] - [Profiles].
2. In the tree on the left, select the location of the profile group to be edited, and then select the profile group in the list on the right.
3. Click the [Actions] button and select [Edit] to edit the profile group.

Procedure for deleting profile groups



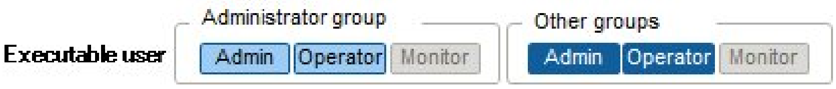
1. From the Global Navigation menu on the GUI of ISM, select [Settings] - [Profiles].
2. In the tree on the left, select the location of the profile group to be deleted, and then select the profile group in the list on the right.
3. Click the [Actions] button and select [Delete].

Procedure for editing policy groups



1. From the Global Navigation menu on the GUI of ISM, select [Settings] - [Profiles].
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. Click the [Actions] button and select [Edit] to edit the policy group.

Procedure for deleting policy groups



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

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. Click the [Actions] button and select [Delete].

Required preparations before OS installation

- The OS installation media and the ServerView Suite DVD need 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, increase 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, you do not need 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, you need 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 (iRMC, BIOS, and OS).

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, usually you need 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 and iRMC 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 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:

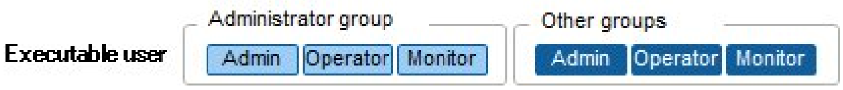
- Servers and any mounted PCI cards
- Storage devices
- Switches

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

Here, the following points are described:

- 2.2.4.1 Confirming firmware versions of nodes
- 2.2.4.2 Firmware update
- 2.2.4.3 Confirming Documentation that Is Supplied with Firmware Data

2.2.4.1 Confirming 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 "Management of node information" in "2.2.1.1 Registering Datacenters/Floors/Racks/Nodes."

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:

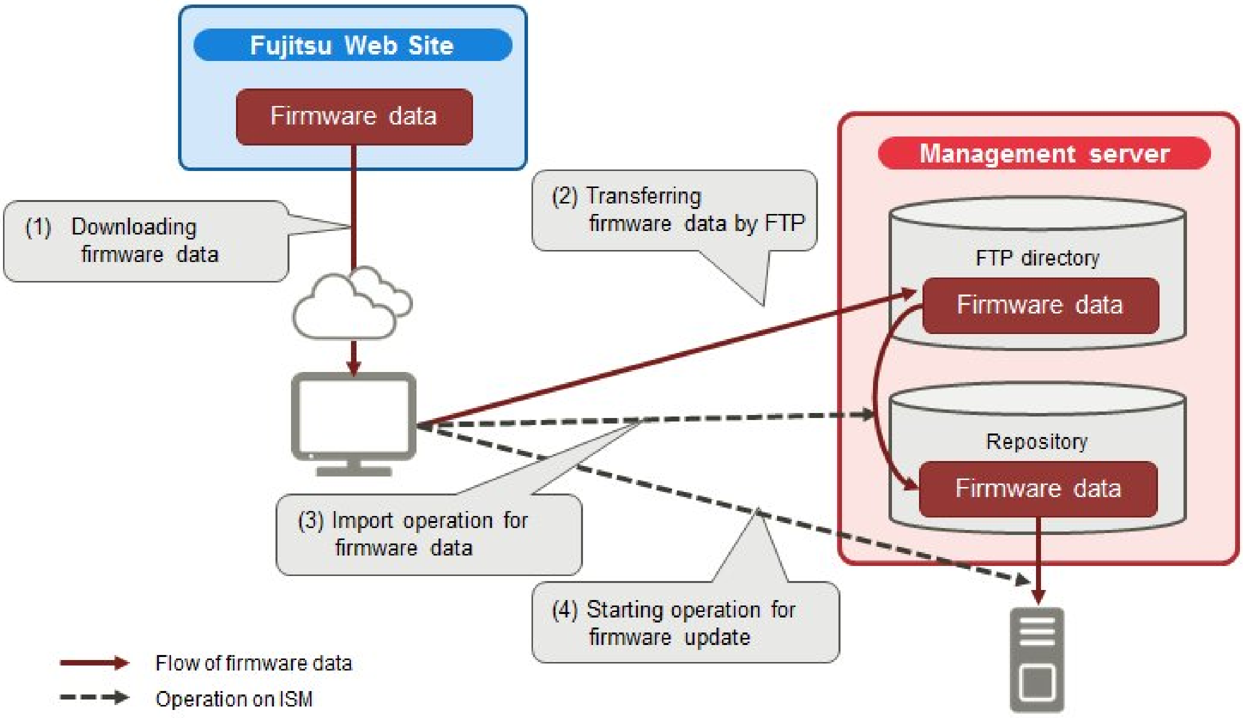
- Firmware updates
- Behavior during updates
- Implementing firmware updates

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



Fujitsu Web Site
Firmware data
(1) Downloading firmware data
(2) Transferring firmware data by FTP
Management server
FTP directory
Firmware data
Repository
Firmware data
(3) Import operation for firmware data
(4) Starting operation for firmware update
Flow of firmware data
Operation on ISM

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 device where firmware update should be done is turned on. Online Update can be done also if the power of the server (BIOS/iRMC) is turned off.

This method can be used when doing firmware update for servers (BIOS/iRMC/ with PCI card mounted), switches, and storage.

Offline Update

Update method for when the power of the device where firmware update should be done is turned off.

This method can be used when doing firmware update for servers (BIOS/iRMC/ with PCI card mounted).

When doing 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 need 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, increase the size of the LVM volume for the user group.

  If you are going to import an ISO image of the ServerView Suite DVD, increase the size of the LVM volume for the system. Once you imported the ServerView Suite DVD into ISM, there is no need 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. Complete the network connections and the BIOS settings of the target server in advance, so as to enable PXE booting from the management onboard 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 SCI 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.

Implement any updates according to the table shown below.

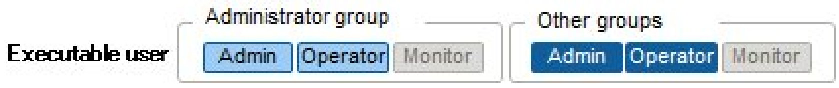
Online Update

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)	Updates can be carried out regardless of whether the server power is on or off. If you implement an update with the power remaining on, you need to reboot the server and turn the power on again in order to switch to the new firmware (BIOS). You can implement 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 implement an update with the power turned off, you need 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.
Server (with mounted PCI card)	Updates can be implemented on the server if a supported OS is running. The new firmware will run only after a reboot. You can implement the reboot whenever suits you best.
Switches Storage	Implement 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. During firmware update the server is powered on or restarted, the power will be turned off after the firmware update has been completed. After the firmware update has been completed, it will automatically be switched over to the new firmware.
Server (BIOS)	
Server (with mounted PCI card)	

Implementing 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.
- When you implement a firmware update on ETERNUS DX/AF, account information with a Maintainer role must already be registered in ISM.
- When you implement 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 information, see "Registration of node OS information" in "2.2.1.1 Registering Datacenters/Floors/Racks/Nodes." 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 will be updated to the same latest firmware version.
- For implementing a firmware update for PCI cards (FC/CAN/LAN cars) 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 implement 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, you need to reboot the server in order to switch to the new firmware. You can implement the reboot whenever suits you best.
    - If you implement an update of the server BIOS with the power remaining on, you need to reboot the server and turn the power on again in order to switch to the new firmware (BIOS). You can implement 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 implement an update of the server BIOS with the power turned off, you need 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 detected.

  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 done simultaneously. This upper limit is 50 for the entire ISM-VA. If firmware update is done on a specified number of nodes exceeding the upper limit, the firmware update will first be executed on the set maximum number of nodes, and after this has been completed the firmware update will be done 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. Activate the Maintenance Mode on the target node.

   See "5.1 Maintenance Mode" for information on Maintenance mode settings.

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" and the "Latest Version" on the node on which you are going to implement the update.

5. Select the checkbox for the node to be updated, then click the [Actions] button and select [Update Firmware].

6. 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 "Task" 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)

   Selecting [Events/Tasks] - [Tasks] from the Global Navigation menu on the GUI of ISM opens a list of tasks on the "Task" screen. Identify the applicable task by its task ID and task type.

7. After confirming on the "Task" screen that the relevant task has completed, deactivate the Maintenance Mode on the target node.

2.2.4.3 Confirming 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 [Management] - [Nodes].

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

3. Select the checkbox for the node to be updated, then click the [Actions] button and select [Update Firmware].

4. From the pull-down menu, select the update version and import data, and then select the [Next] button.

5. In the [Document URL] field, select the URL and confirm the documentation.

Point

- 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 a server(s) differs from the "Online Update" of the document(s) 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.

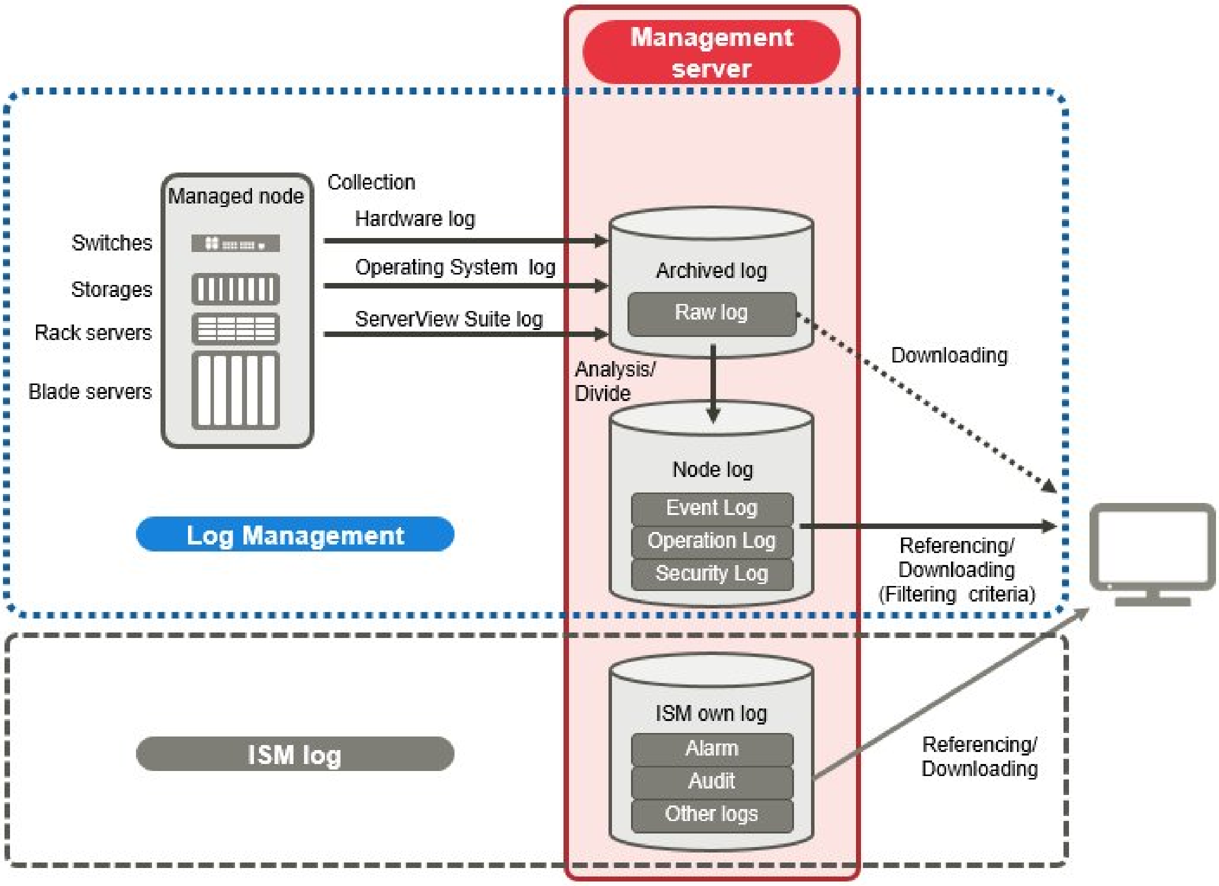
The bulk of log data that are collected from nodes according to these settings are called "Archived Logs."

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 you can download the Archived Logs, converted into ZIP files, to the management terminal whenever suits you best.

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 collectible 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 collectible 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
Storage	ETERNUS DX/AF	Output results for "show events" command Output results for "export log" command"	Output results for "show events" command
Switches	SR-X	Output results for "show tech-support" command	Output results for "show logging syslog" command (Included in output results for " show logging syslog" command)
	VDX	Various files created with the "copy support" command	Output results for the "show logging raslog" command. Output results for the "show logging audit" command (Included in "<Any text string as needed>.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)

OS for which to retrieve logs	Type of log to be collected	
	Name in OS	Classification in ISM
Linux	System log (/var/log/messages)	Operating system log (event log)
	System log (/var/log/secure)	Operating system log (security log)
VMware ESXi	System log (syslog.log)	Operating system log (event log)

Note

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

ServerView Suite logs

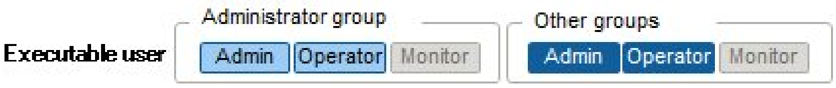
Log Management retrieves logs for the software (ServerView Suite products) that is running on the managed servers.

Software for which to retrieve logs	Type of node log to be collected
ServerView Agents	Output results for "PrimeCollect" command
ServerView Agentless Service	Output 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



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 any values for the log retention periods as needed.

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.

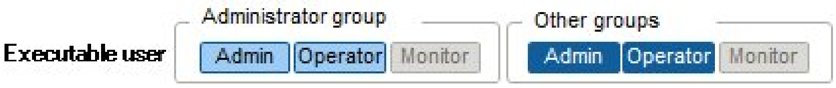
  By default, the retention periods for "Event Logs", "Operation Logs", and "Security Logs" are each set to 30 days.

  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



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 (mandatory 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 valid targets for collecting the three types of log: "Hardware Log", "Operating System Log," and "ServerView Suite Log."

If the Log Collection Target settings do not allow for 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.

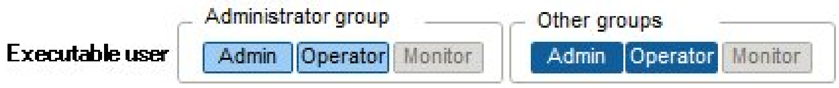
1. From the Global Navigation menu on the GUI of ISM, select [Management] - [Nodes].

2. In the [Column Display] field, select [Log 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. Click the [Actions] button and select [Edit Log Collection Settings].

Operations for log collection



Periodical log collection

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

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

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

Note

- With periodical log collection, if a node is in a status that does not allow for log collection at the scheduled starting time, that collection is skipped and implemented 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 implemented (power is off, no network communication available etc.)

  - A different operation has been implemented 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/Tasks] - [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.
- 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 [Management] - [Nodes].
2. In the [Column Display] field, select [Log 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. Click the [Actions] button and select [Collect Logs].

   The "Result" screen is displayed. Take a memo of the Task Detail number that is displayed on this screen.
5. Select [Events/Tasks] - [Tasks] to confirm the current processing status.

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

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

Note

- 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."

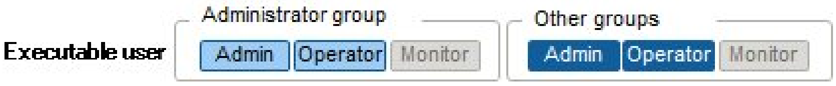
If the total size of each of the various log files approaches this capacity setting value its specified value, this is recorded as a warning/error event under [Events/Tasks] - [Events] - [Operation Log] in ISM. When the preset value is exceeded (when an error event was registered), new logs are no longer 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
Amount of log data exceeds 80% of the specified capacity The total size of log files exceeds the size of the specified value for monitoring the disk capacity: Example:	- Log collection is implemented. - A warning event is issued under [Events] - [Operation Log]. The contents of the displayed messages are as follows. - For Archived Logs:

Condition	Behavior
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.	The threshold value of the data size in archive log saving area was exceeded. Refer to "Deleting Archived Logs" - For node logs (data for download): The threshold value of the data size in node log (download data) saving area was exceeded. Refer to "Deleting node logs" - For node logs (data for log searches): The threshold value of the data size in node log (log search data) saving area was exceeded. Refer to "Deleting node logs"
Amount of log data exceeds the specified capacity The total size of log files exceeds the upper limit specified value: Example: When the specified upper limit value is 10GB the operation described on the right is carried out.	- Log collection is not implemented. - An error event is issued under [Events] - [Operation Log]. The contents of the displayed messages are as follows. - For Archived Logs: The predetermined capacity for an Archive log saving area was exceeded. Refer to "Deleting Archived Logs" - For node logs (data for download): The predetermined capacity for a node log (download data) saving area was exceeded. Refer to "Deleting node logs" - For node logs (data for log searches): The predetermined capacity for node log (log search data) saving area was exceeded. 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 [Logs] - [Node Logs].
2. 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 [Logs] - [Node Logs].
2. Click the [Filter] button.

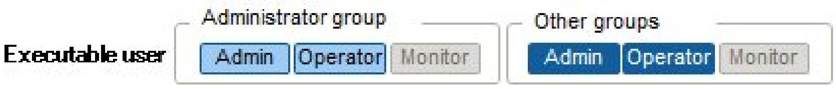
3. Enter the parameters on the "Filter" screen and click the [Filter] button.

   The logs that match the condition you entered are displayed.

Point

As a simple function for downloading logs, you can output the current display contents on the GUI screen to a CSV file. You can output data in CSV format by clicking the [Actions] button and selecting [Download Log List (CSV)].

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 [Logs] - [Node Logs].
2. Click the [Actions] button and select [Create Download Files].

   The "Result" screen is displayed. Take a memo of the Task Detail number that is displayed on this screen.
3. Wait until creation of the download files finishes.

   Select [Events/Tasks] - [Tasks] to confirm the current processing status.

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

   For the Task ID, confirm the number under Task Detail on the "Result" screen that is displayed after executing [Create Download Files].
4. When creation of the files for download is complete, click the [Actions] button and select [Check Download Files].

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

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

```
Log_20160601-20160607.zip
```

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

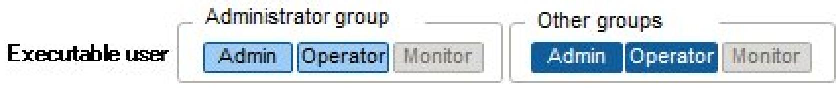
- Folder structure

```
<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 [Logs] - [Archived Logs].
2. Select the checkboxes for the Archived Logs to be downloaded.

   If you select the checkboxes for multiple Archived Logs, they will be downloaded and combined in a single zip file.
3. Click the [Actions] button and select [Create Download Files].

   The "Result" screen is displayed. Take a memo of the Task Detail number that is displayed on this screen.
4. Wait until creation of the download files finishes.

   Select [Events/Tasks] - [Tasks] to confirm the current processing status.

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

   For the Task ID, confirm the Task Detail number of which you took a memo on the "Result" screen.
5. When creation of the files for download is complete, click the [Actions] button and select [Check Download Files].

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.

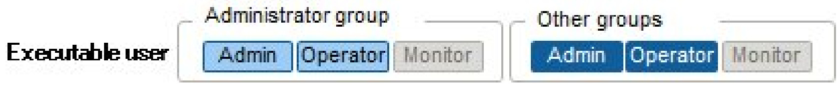
- Folder structure

```
<node name>_<node ID>\<date>_<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. To do so, 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 [Logs] - [Node Logs].
2. Click the [Actions] button and select [Delete Logs] to execute log deletion according to the instructions on the screen.

   The "Result" screen is displayed. Take a memo of the Task Detail number that is displayed on this screen.
3. Select [Events/Tasks] - [Tasks] to confirm the current processing status.

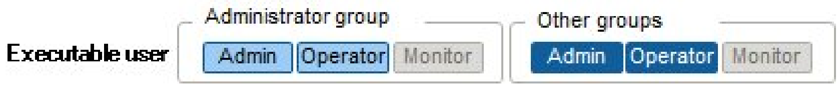
   Under Task Type, [Deleting Log files] is displayed.

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

Note

- Deleting node logs may take some time to complete. Therefore, 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, 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



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 [Logs] - [Archived Logs].
2. Select the checkboxes for the file names to be deleted. By selecting the checkboxes for multiple file names, you can delete them in a batch.
3. Click the [Actions] button and select [Delete] to execute deletion according to the instructions on the screen.

   The "Result" screen is displayed. Take a memo of the Task Detail number that is displayed on this screen.
4. Select [Events/Tasks] - [Tasks] to confirm the current processing status.

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

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

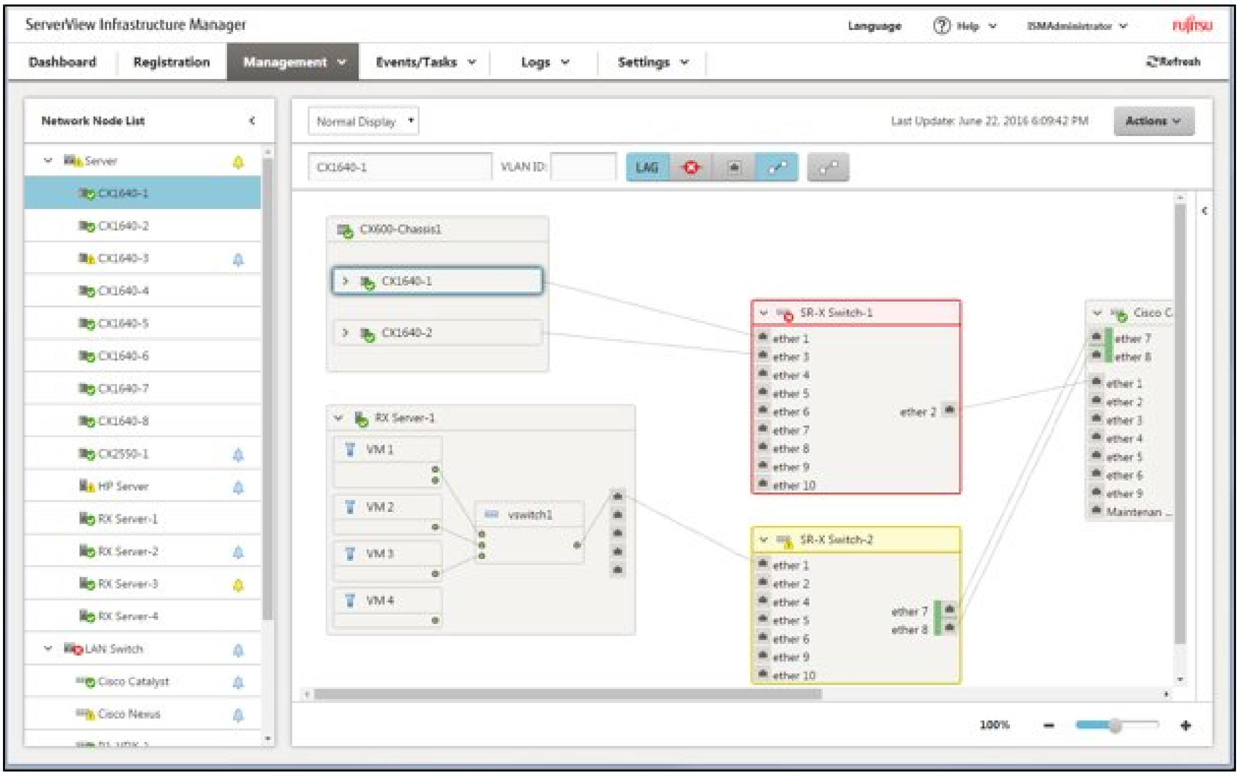
Note

- Deleting Archived Logs may take some time to complete. Therefore, 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:

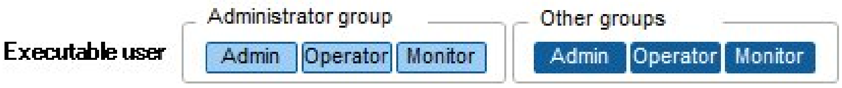
- Confirming information on physical network connections and port information between managed nodes on the Network Map
- Confirming the changes in the information on network connections between managed nodes
- Confirming the virtual connections of the physical ports, the virtual switches and the virtual 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
LAG	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 will be 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 expand the display of the ports within the node.

Note

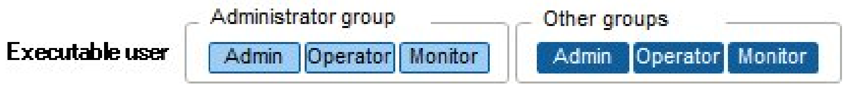
- LLDP (Link Layer Discovery Protocol) is used for retrieving information on physical network connections. If your nodes do not support LLDP or if LLDP is disabled, the information for actually existing connections cannot be retrieved. For information on whether a node supports LLDP and on how to confirm whether the LLDP settings of the node are enabled or disabled, confirm the technical specifications of each respective node.

- The displayed Network Map shows either the status retrieved when you last executed [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 relationship of a virtual switch(s)/virtual machine(s), you need, beforehand, to register the Cloud Management Software that manages a managed node(s) as well as the OS information on 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 Registering Datacenters/Floors/Racks/Nodes."

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. Click the [Actions] button and select [Refresh Network Information].
3. Select the [Yes] button.

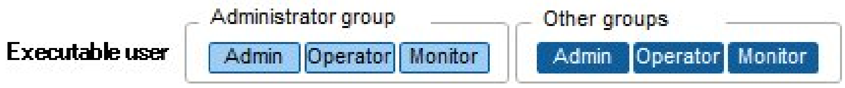
Note

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

Point

- Update the node information for each managed node before updating the network management information. See "Management of node information" in "2.2.1.1 Registering Datacenters/Floors/Racks/Nodes" 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 Events/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 detected connections. "Added" connections are displayed as bold lines, on the Network Map.

- Deleted

  "Deleted" is displayed for disconnections and previously detected 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, detect 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. Select the [Actions] button and select [Confirm connection state change].

   You can confirm "Added" and "Deleted" connection information separately.

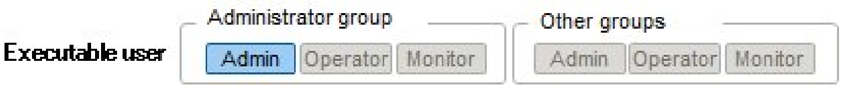
Point

The currently set "Reference Point" can be confirmed in "Last Update Time" in "Check changes in connection information."

Note

Selecting the [Refresh] button under [Confirm connection state change] updates the reference point in time 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 in time. You can modify this reference point in time when you want to set the reference point in time after changing, for example, the configuration of network connections. 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. Select the [Actions] button and select [Confirm connection state change]. The date and time of the latest refresh is the reference point in time that is currently set.

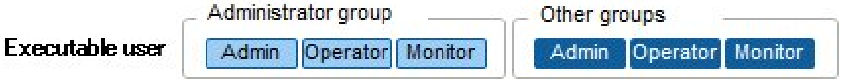
4. Select the [Refresh] button.

   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. Do 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.

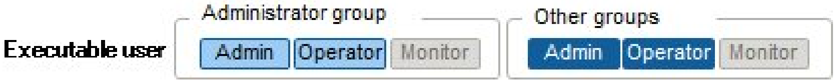
     The ports inside the node are opened and the Link Aggregation settings are displayed.

Point

- Switch ON and OFF to display the Link Aggregation settings on the network using the " LAG " 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



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 pull-down menu displayed at the upper left part of the Network Map, select [Multiple Setting].

4. Check to select the respective ports for which you want to set the same VLAN ID, and select [Multiple VLANs setting] from [Actions] button.

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.

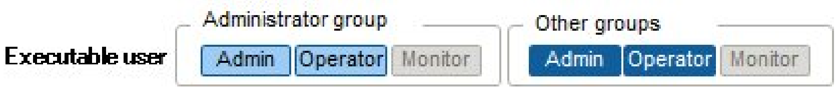
Point

VLAN settings can be changed also on a node basis. Select [LAG setting] from [Actions] button.

Note

- 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 ports that can be set up for a managed node at a time is one (1) and the number of VLAN IDs that can be set for a managed node is up to one hundred (100).
- There exists a reserved VLAN ID(s) 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



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. Select [LAG setting] from [Actions] button.

4. Select the name of the target node for which you set up a Link Aggregation and select [Add] of LAG (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.

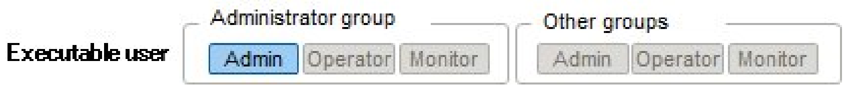
6. Confirm the setting contents of the Link Aggregation and select the [Register] button.

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, you need to change Link Aggregation settings for respective switches. To set Multi-Chassis Link Aggregation, it is required to first do 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. Confirm the requirements before setup.

Setting network connection information manually



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 pull-down menu that is displayed at the top left of the Network Map, 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

   If you want to cancel the settings you made manually after selecting the [Add] button, select the [Actions] button and execute [Cancel editing connections].

5. After adding all the connection information you want to set, select the [Actions] button and select [Save editing connections].
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.

Point

There are the following four types of power capping policies.

- Custom 1, custom 2

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

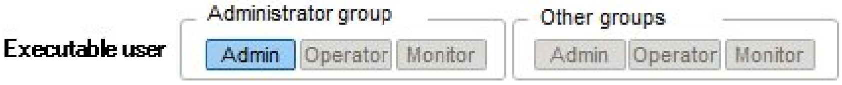
- Schedule

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

- Minimum

  Control where power capping is kept to a minimum.

Add/Edit power capping policies



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 [Power Capping stopped] or [Power Capping Activated].

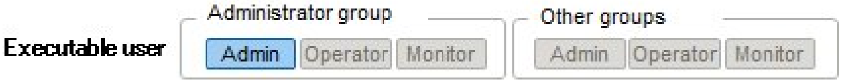
The maximum power consumption value will be used as a fixed value for nodes that power capping cannot be done for.

Power capping policy

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

Set operation schedule for schedule policy.

Enable/Disable power capping



Switch the power capping policy between enabled and disabled.

Point

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

Note

- For racks with an already implemented 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.
  It is required to do this for each rack both before and after migrating a node.

- 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 [Node Details] screen will not be displayed correctly.
  When the date and time set in ISM-VA passes it will be displayed correctly again.

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 range 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 2.9 Relationships between user groups, node groups, and roles."

Here, the following points are described:

- Types of user groups and access ranges 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 ranges of users belonging to each group

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

User group name	Access range
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 range 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

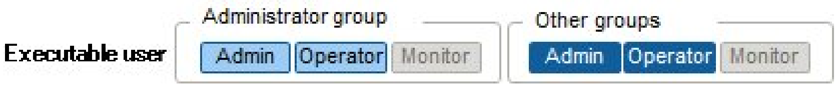
- For information on setting changes that can and cannot be made by operators, see the contents (indicated by icons) on the various functions that are provided in this manual. For information on the icon indications, see the explanation below.
- In the explanation below, users belonging to the Administrator 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 are indicated by the following icons.

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

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

Example:



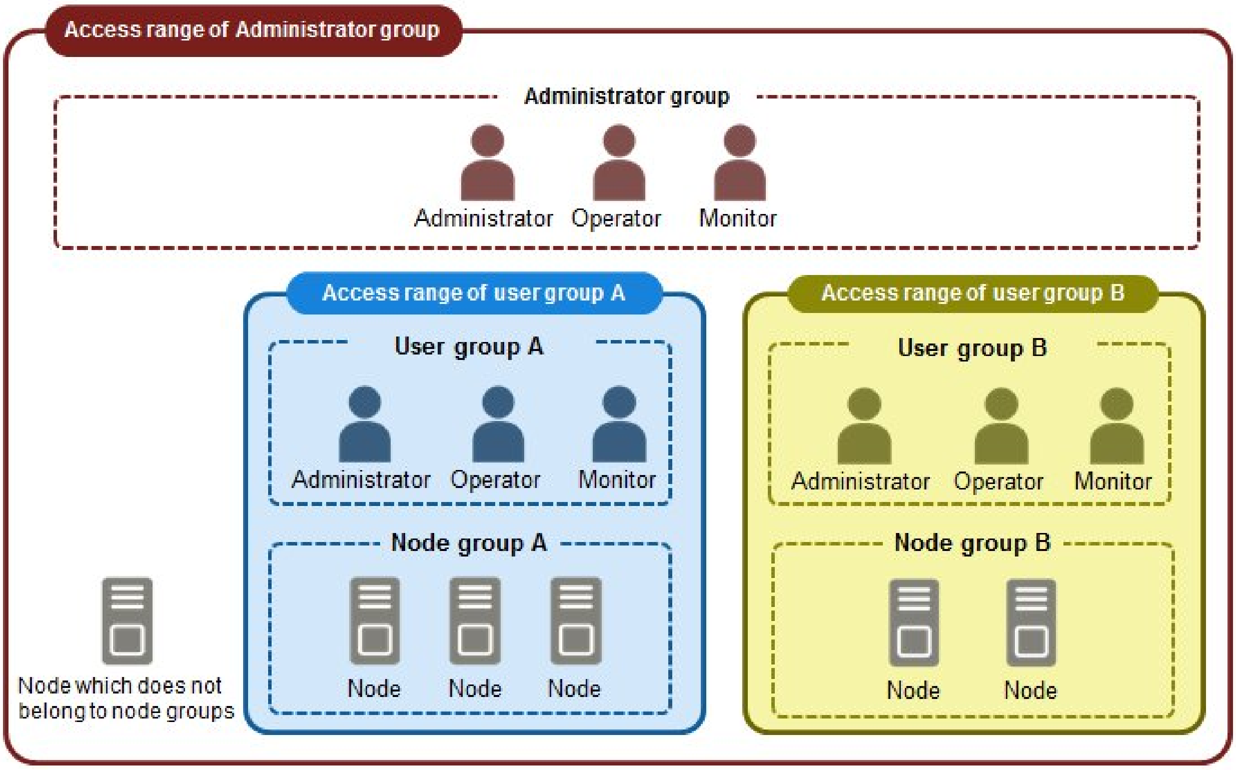
- When the display is as shown above, users with the following user affiliations can execute operations:
  - Users who belong to an Administrator group and have an Administrator or Operator role
  - Users who belong to a group other than an Administrator group and have an Administrator or Operator role
- 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 ranges, 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 2.9 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	- 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	- 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	- Allowed - Not allowed (Recommended)	
Example of forbidden character strings [Note1]	Up to a maximum of 256 can be specified	

Item	Parameter	Operations after settings
Expires	- Indefinite - 1 - 365 (days) (Recommended: 90 (days))	If logging in with another setting than "Indefinite", do the following operations. - 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	- 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 click 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 applying the ISM V2.0.0.e patch.
  - 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 "Adding node groups" in "2.3.1.4 Managing node groups" for details.
3. Register the nodes that belong to each node group. (You can also register more nodes later.)

   See "Editing node groups" in "2.3.1.4 Managing node groups" for details.
4. Create one or more user groups.

   See "Adding user groups" in "2.3.1.2 Managing User Groups" for details.
5. Create correlations between user groups and node groups as required.

   See "Editing user groups" in "2.3.1.2 Managing User Groups" for details.
6. Register the users that belong to each user group.

   See "Adding users" in "2.3.1.1 Managing ISM 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.

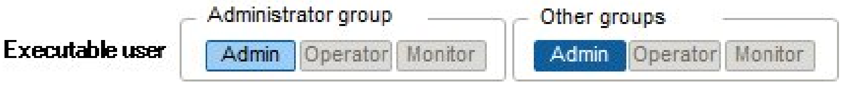
Operating user	Object of operation
Users who belong to an Administrator group and have an Administrator role	Operations can be made for all existing user groups.
Users who belong to groups other than Administrator groups and have an Administrator role	Operations can be made only for the user group to 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] - [General Settings] - [Users].
2. Click the [Actions] button and 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

  See "Types of user roles and operations executable by users having these roles."

- Description

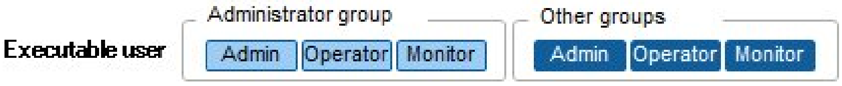
  Freely enter a description of the user (comment) as needed.

- 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] - [General Settings] - [Users].
2. Execute one of the following.

   - Select the checkbox for the user you want to edit, then click the [Actions] button and select [Edit].

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

The information that can be modified is as follows.

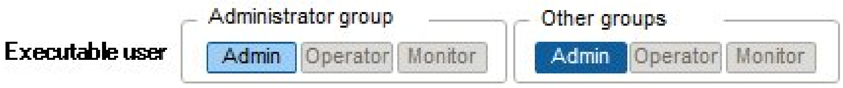
User information	Administrator group		Group other than administrator group	
	Administrator role	Operator role Monitor role	Administrator role	Operator role Monitor role
User Name	Y	Y	Y	Y
Password	Y	Y	Y	Y
User role	Y	N	Y	N
Description	Y	N	Y	N
Language	Y	Y	Y	Y
Date Format	Y	Y	Y	Y
Time Zone	Y	Y	Y	Y
User 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 you need 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] - [General Settings] - [Users].
2. Execute one of the following.
    - Select the checkboxes for the users you want to delete, then click the [Actions] button and select [Delete].
    - Click on the name of the user you want to delete and, when the information screen is displayed, click 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

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

1. From the Global Navigation menu on the GUI of ISM, select [Settings] - [General Settings] - [User Groups].
2. Click the [Actions] button and 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 needed.

- 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	Specify the total size of the files used by the user group to [Maximum Size] in units of MB. The total size of the files is the total of the following files. - Repository - Archived logs - Node logs - Files handled by ISM-VA in FTP If the actual usage size exceeds the specified [Maximum Size], an error message is output to the Operation Log. Even when the [Maximum Size] value is exceeded, this does not affect the operations of Repository, Archived Log, and Node Log.	Specify the threshold value outputting an alert message to the Operation Log to [Warning threshold] in units of %. A warning message is output to the Operation Log.
Repositories	Specify the total size of the files imported to Repository to [Maximum Size] in units of MB. If the total usage size of the imported files exceed the value of the specified [Maximum Size], the currently executed import to the Repository results in error and an error message is output to the Operation Log.	You cannot specify the value.
Archived logs	Specify the total size of Archived Log to [Maximum Size] in units of MB. If the total size of the Archived Log exceeds the specified [Maximum Size], newly created logs are not stored in Archived Log and an error message is output to the Operation Log. Note that if [Maximum Size] is set to the [0] default value, the occurred logs will not be archived and	Specify the threshold value outputting an alert message to the Operation Log to [Warning threshold] in units of %. A warning message is output to Operation Log.

Usage	Size Restriction	Threshold Monitoring
	every time an error message will be output in the operations log. The logs stored before exceeding the [Maximum Size] remains stored.	
Node log	You can specify the total size of download data and log search data to [Maximum Size] in units of MB. The log search data can only be specified to the Administrator user group. If either of the total size of download data or the log search data exceeds the value specified in [Maximum Size], neither download data nor log search data are output and an error message is output to the Operation Log. If the [Maximum Size] of either download data, log search data or both is set to the default [0], neither data will be output and an error message will be output in the operations log.	You can specify the threshold value that outputs an alert message to the size of download data and the size of log search data, to [Warning threshold]in units of %. A warning message is output to Operation Log.

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."

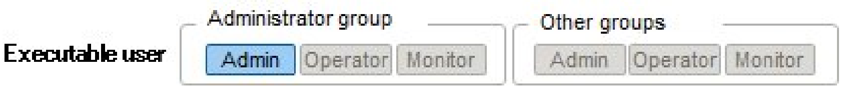
- Node group

  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 Allocating 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] - [General Settings] - [User Groups].
2. Execute one of the following.
   - Select the checkbox for the user group you want to edit, then click the [Actions] button and select [Edit].
   - Click on the name of the user group you want to edit and, when the information screen is displayed, click 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

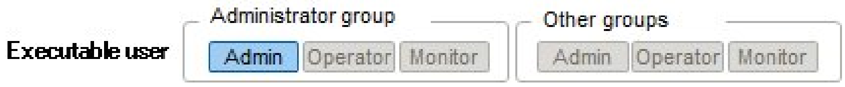
  Create correlations between user groups and node groups as required by selecting a node group.

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 deactivates 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] - [General Settings] - [User Groups].
2. Execute one of the following.
   - Select the checkboxes for the user groups you want to delete, then click the [Actions] button and select [Delete].
   - Click on the name of the user group you want to delete and, when the information screen is displayed, click the [Actions] button and select [Delete].

Note

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

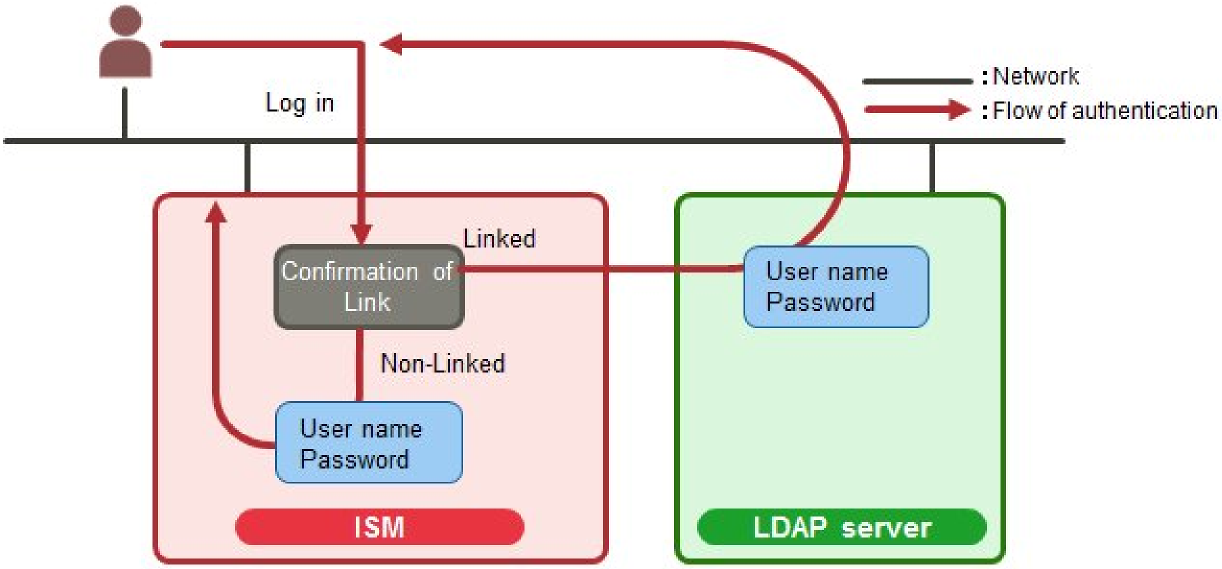
  Before you delete a user group, delete all users who belong to the user group, or change the affiliations of all users to other user groups.
- Even if you delete user groups that are correlated with node groups, the node groups will not be deleted.
- You cannot undo deletion of a user group.
- When you 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 centrally manage users and passwords of multiple services.

The following diagram gives an overview of a linked configuration.

Figure 2.10 Image of ISM in link with LDAP



1. Log in as a user.

   - If user is object of linked operation:

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

   - If user is no object of linked operation:

     Authentication is carried out by ISM.

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

Activation 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: - URL or IP address - ldap://<url> or ldap://<IP address> - ldaps://<url> or ldaps://<IP address>
Port Number	Specify the port number of the directory server.
Base DN	Specify the base DN for searching accounts. This information depends on the registered contents on the directory server. Example: - For LDAP: ou=Users,ou=system - For Microsoft Active Directory: DC=company,DC=com
Search Attribute	Specify the account attribute for searching accounts. Specify one of the following fixed character strings:

Item	Setting contents
	- For LDAP: uid - For Microsoft Active Directory: sAMAccountName
Bind DN	Specify the accounts that can be searched on the directory server. This information depends on the registered contents on the directory server. Example: - For LDAP: uid=ldap_search,ou=system - For Microsoft Active Directory: CN=ldap_search,OU=user_group,DC=company,DC=com "anonymous" is not supported.
Password	Specify the password for the account you specified under Bind DN.
SSL Authentication	If you want to use SSL for the connection to the directory server, set up SSL authentication.

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

5. From the Global Navigation menu on the GUI of ISM, select [Settings] - [Basic Info], then select [Users] and add the users you registered in Step 1.

   The information to be registered is as follows.

Item	Setting contents
User Name	Specify the names of the users you registered in Step 1.
Password	For situations when operation in link is deactivated, specify a password different from that in Step 1. Note that the password you specify here is also used when you log in via FTP.
User role	Specify the user role in ISM.
Description	Freely specify any values as needed.
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] - [Basic settings] - [LDAP server settings], 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.

Deactivation procedure

The method for deactivating 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."

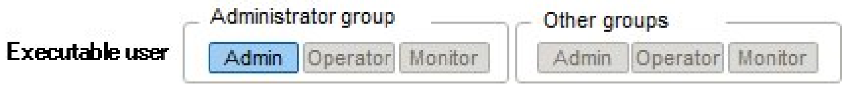
Both of the above operations activate the passwords you set during user registration or modified at a later stage.

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] - [General Settings] - [Node Groups].
2. Click the [Actions] button and select [Add].

Or

1. From the Global Navigation menu on the GUI of ISM, select [Management] - [Node Groups].
2. Click 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

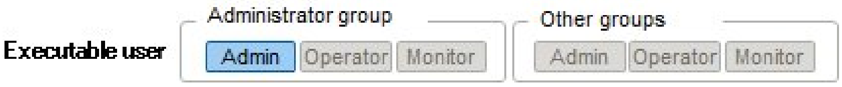
  Select multiple nodes for which the node group affiliation is [Unassigned].

  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] - [General Settings] - [Node Groups].
2. Execute one of the following.
    - Select the checkbox for the node group you want to edit, then click the [Actions] button and select [Edit].
    - Click on the name of the node group you want to edit and, when the information screen is displayed, click the [Actions] button and select [Edit].

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, click 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.

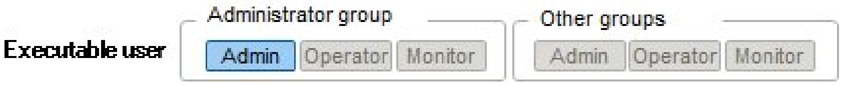
- Selection of Nodes to be Newly Assigned

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

To deactivate 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, click the [Actions] button (the lower one of the two displayed at the top right of the screen) and select [Assign to Node Group].
4. On the "Assign to Node Group" screen, click the [Select] button.
5. On the "Select Node Group" screen, select one of the following, and then click the [Select] button.
    - For deactivating a node assignment: [Unassigned]
    - For changing a node assignment: [<Node group to which to assign anew>]
6. On the "Assign to Node Group" screen, click 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] - [General Settings] - [Node Groups].
2. Execute one of the following.
    - Select the checkboxes for the node groups you want to delete, then click the [Actions] button and select [Delete].
    - Click on the name of the node group you want to delete and, when the information screen is displayed, click the [Actions] button and select [Delete].

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, click 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.
- Deactivate 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

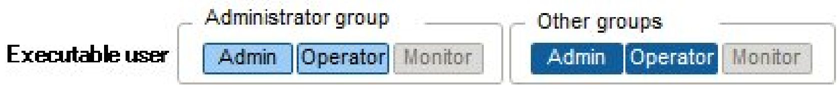
  These are used by the "2.2.3 Profile Management" and "2.2.4 Firmware Management" functions.

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	- Online Update BIOS/iRMC data as published on the FUJITSU PRIMERGY website - Offline Update
	iRMC of PRIMERGY unit	

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
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/ [Note 1]
BIOS of PRIMERGY unit	BIOS	
Cards mounted in PRIMERGY unit	FC	http://support.ts.fujitsu.com/globalflash/FibreChannelController/
	CNA	http://support.ts.fujitsu.com/globalflash/LanController/
Basic software for network switches	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/

[Note 1] 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

In ISM 2.0, 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 [Settings] - [Repositories].

3. Execute one of the following.

   - For storing the firmware data in the repository from DVD, click 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, click the [Actions] button on the [Import Data List] tab and select [Import Firmware].

4. Execute the operations according to the instructions on the screen.

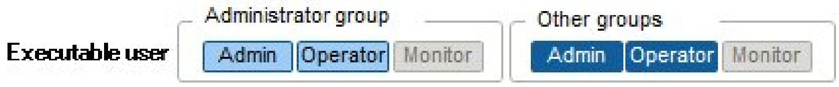
Importing to the repository may take some time to complete. After starting the import, the task is registered as a "Task" in ISM. Confirm the current status of the task on the "Task" screen.

Selecting [Events/Tasks] - [Tasks] from the Global Navigation menu on the GUI of ISM opens a list of tasks on the "Tasks" screen.

Point

The files you deployed on the FTP server of ISM are no longer needed after the import has finished, so you should 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.

Deleting firmware data from repository



The following is a sample operation.

From the Global Navigation menu on the GUI of ISM, select [Settings] - [Repositories].

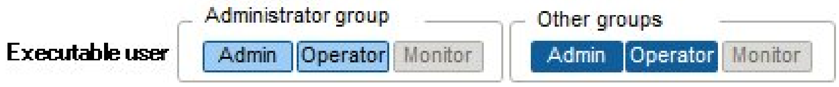
- If firmware data was stored in repository from DVD:

  1. Select [Import Data List].
  2. Select the checkboxes for the data to be deleted, then click the [Actions] button and select [Delete].
  3. Execute the operations according to the instructions on the screen.

- If firmware data downloaded from the FUJITSU website was stored in repository:

  1. Select [Firmware Data].
  2. Select the checkboxes for the data to be deleted, then click the [Actions] button and select [Delete].
  3. Execute the operations according to the instructions on the screen.

Importing firmware data

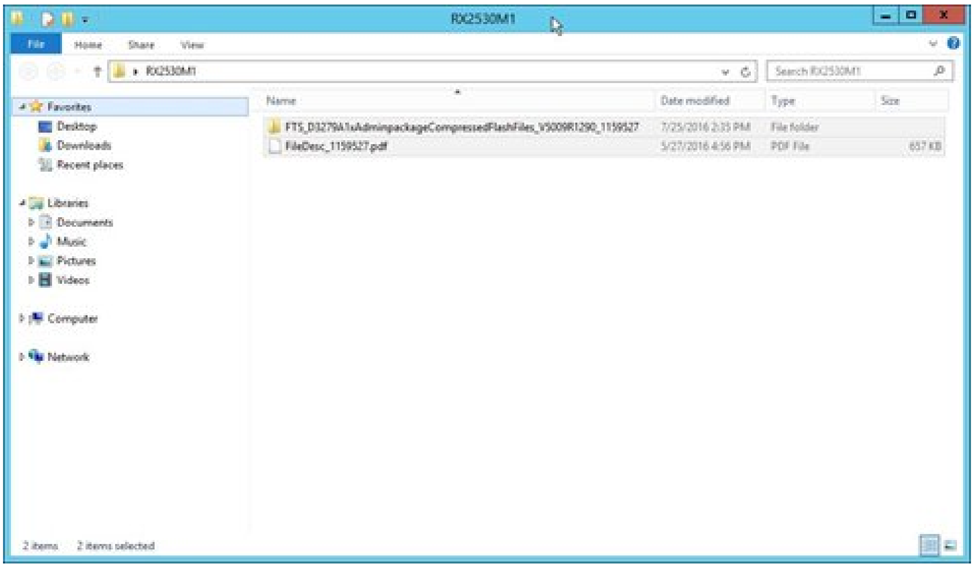


Below example shows the operations for importing firmware data by an administrator user who belongs to an Administrator group.

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.



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

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. When you do so, 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 [Settings] - [Repositories].

   b. Execute one of the following.

      - For importing an ISO image file into the repository, click the [Actions] button under [Import Data List] 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, click the [Actions] button under [Import Data List] 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 [Note 1]
BIOS	RX100 S8, CX2550 M1 etc.	BIOS version [Note 1]
FC	LPe1250, LPe12002	BIOS and FW versions [Note 2]
	LPeXXX except for LPe1250 and LPe12002	Firmware version [Note 2]
	QLEXXX	BIOS version [Note 2]
CNA	Oce10102 etc.	Firmware version [Note 1]
LAN Switch	SR-X model	Version of basic software [Note 1]
	VDX model	Firmware version [Note 1]

Type	Model	Version
ETERNUS DX/AF	ETERNUS DX/AF model	Firmware version [Note 1]

[Note 1] For information on the version, see the release notes.

[Note 2] For information on the version, see the release notes or the file name.

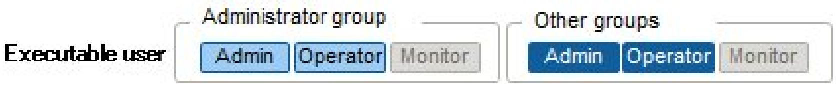
Importing to the repository may take some time to complete. After starting the import, the task is registered as a "Task" in ISM. Confirm the current status of the task on the "Tasks" screen.

Selecting [Events/Tasks] - [Tasks] from the Global Navigation menu on the GUI of ISM opens a list of tasks on the "Tasks" screen.

Point

- The files you deployed on the FTP server of ISM are no longer needed after the import has finished, so you should 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 character code conversion is not usually done, the letters might be corrupted in ISM-VA and import may not be done 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



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, implement below procedure.

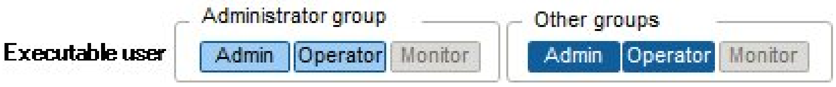
1. Prepare an ISO image of the OS installation media. For ESXi, prepare a FUJITSU custom image.
2. After logging in to ISM-VA over FTP, forward the ISO image you prepared into the "./<user group name>/ftp" directory.

   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 [Settings] - [Repositories].
4. In the menu on the left, select [OS/SVS], then select the [Actions] button and select [Import DVD].
5. 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 needed after the import has finished, so you should 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.

Deleting OS installation files from repository

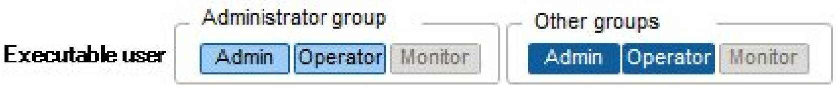


The procedure for deletion is as follows:

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

2. In the menu on the left, select [OS/SVS].
3. Select the checkboxes for the data to be deleted, then click the [Actions] button and select [Delete].
4. 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, implement the following procedure:

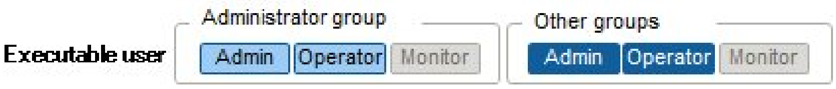
1. Prepare an ISO image of "ServerView Suite DVD."
2. After logging in to ISM-VA over FTP, forward the ISO image you prepared into the "./<user group name>/ftp" directory.

   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 [Settings] - [Repositories].
4. In the menu on the left, select [OS/SVS], then click the [Actions] button and select [Import DVD].
5. 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 needed after the import has finished, so you should 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.

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 [Settings] - [Repositories].
2. In the menu on the left, select [OS/SVS].
3. Select the checkboxes for the data to be deleted, then click the [Actions] button and select [Delete].
4. Execute the operations according to the instructions on the screen.

2.3.3 Installing Emulex OneCommand Manager CLI and Qlogic QConvergeConsole CLI

Note

- For implementing 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 implementing 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 and the QLogic QConvergeConsole CLI, respectively.

For information on the latest versions, access your local support.

2.3.4 Task Management

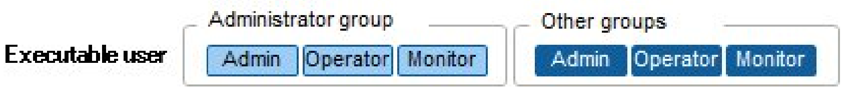
In ISM, any processing that takes time is managed as a "Task." You can view the current status of all tasks at once on the "Tasks" screen instead of the respective operating screens of each task.

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 Deactivation of profiles
Log Management	Collection of logs Deletion of logs

Method for displaying "Task" screen



1. Select [Events/Tasks] - [Task].

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. - Network Settings - Time settings

Function name	Overview of function
	- Initial locale settings
License Activation	This function activates 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. - Network Settings - Time settings - Local settings - Virtual disk settings - Modifying Host Names
Maintenance	This function serves to carry out all kinds of maintenance. - Confirmation of versions - Applying Patches - Collection of maintenance 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 network devices	ismadm network device
Modify network settings	ismadm network modify
Show network settings	ismadm network show

Time settings

Function	Command
Show time settings	ismadm time show
Show available time zones	ismadm time list-timezones
Set time zone	ismadm time set-timezone
Set date and time	ismadm time set-time

Function	Command
Enable/Disable NTP synchronization	ismadm time set-ntp
Add NTP server	ismadm time add-ntpserver
Remove NTP server	ismadm time del-ntpserver

Locale and keymap settings

Function	Command
Show locale and keymap	ismadm locale show
Show available locales	ismadm locale list-locales
Local settings	ismadm locale set-locale
Show available keymaps	ismadm locale list-keymaps
Set keymap	ismadm locale set-keymap

License Activation

Function	Command
Show list of licenses	ismadm license show
License Activation	ismadm license set
Delete license	ismadm license delete

Certificate Activation

Function	Command
Deploying SSL Server Certificates	ismadm sslcert set
Displaying SSL Server Certificates	ismadm sslcert show
Export SSL server certificates	ismadm sslcert export

ISM--VA Service Control

Function	Command
Restart ISM--VA	ismadm power restart
Stop ISM--VA	ismadm power stop
Modify destination port number of ISM	ismadm service modify
Show list of internal services	ismadm service show
Start internal service individually	ismadm service start
Stop internal service individually	ismadm service stop
Restart internal service individually	ismadm service restart
Show status of internal service individually	ismadm service status
Enable internal service individually	ismadm service enable
Disable internal service individually	ismadm service disable

Virtual disk settings

Function	Command
Add LVM volume	ismadm volume add
Allocate LVM volume to user group	ismadm volume mount
Cancel allocation of LVM volume to user group	ismadm volume umount
Show volume settings	ismadm volume show
Expand LVM volume size	ismadm volume extend
Expand size of LVM system volume	ismadm volume sysvol-extend
Remove LVM volume	ismadm volume delete

Maintenance

Function	Command
Collection of maintenance logs	ismadm system snap
Displaying System Information	ismadm system show
Applying Patches	ismadm system patch-add
Apply plugin	ismadm system plugin-add
Modifying Host Names	ismadm system modify
Switching Trouble Investigation Logs	ismadm system set-debug-flag
Setting of SNMP Community Name	ismadm snmp

Event Notification Settings

Function	Command
Register certificate for event notification mails / action script registration	ismadm event import
Show certificate for event notification mails / action script	ismadm event show
Delete certificate for event notification mails / action script	ismadm event delete

MIB File Settings

Function	Command
Registering MIB Files	ismadm mib import
Displaying MIB Files	ismadm mib show
Deleting MIB Files	ismadm mib delete

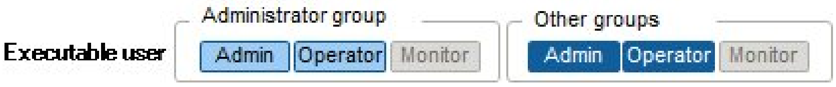
Note

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 Settings] - [Cloud Management Software].
2. Click the [Actions] button and 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.

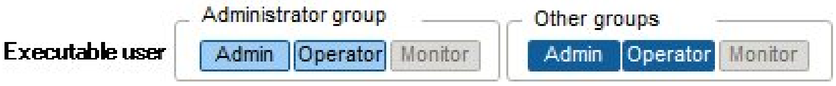
   - User Group

     Select the name of the user group to be managed.

4. Click 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 vCenter or SystemCenter 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. Do 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 Settings] - [Cloud Management Software].

3. Retrieve information using one of the following methods.

   - If retrieving information from all Cloud Management Softwares, select [Get Cloud Management Software Info] and then select [Execute].

   - If limiting the items to be retrieved, select the Cloud Management Software to be retrieved and select [Execute] from [Action] - [Retrieve Information].

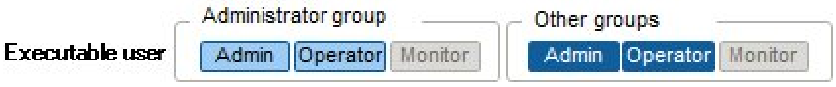
   As soon as retrieval of the information is complete, a log with the Message ID "10020503" is output to the [Event/Task] - [Event] - [Operations Log]. If there is Cloud Management Software where information could not be retrieved, a log will additionally be output in [Event/Task] - [Event] - [Operations Log]. Confirm that an error has not been output, then confirm the information of the virtual machine or virtual switch.

Note

- If registering both SystemCenter and the Microsoft Failover Cluster registered in System center in ISM, ISM will retrieve information from SystemCenter, 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.

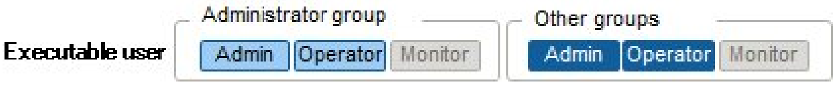
1. From the Global Navigation menu on the GUI of ISM, select [Settings] - [General Settings] - [Cloud Management Software], and then select the target Cloud Management Software on the displayed [Cloud Management Software List] screen.

2. Click the [Actions] button and select [Edit].

3. Edit information.

4. Execute [Register] 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 Settings] - [Cloud Management Software], and then select the target Cloud Management Software on the displayed [Cloud Management Software List] screen.

2. Click the [Actions] button and select [Delete].

3. Execute [Delete] to delete the Cloud Management Software.

2.4 Operations when Releasing Node Registrations and when Modifying Groups

When you are going to release a node registration or modify a group, perform the operations described below.

2.4.1 When Releasing Node Registrations

Before you release a node registration, complete the operations described below.

- If any tasks are being executed, wait until they have completed.

- Deactivate any profiles assignments you have made.

Point

If you deactivate a node registration while a profile assignment is active, this node registration will not be deactivated. (The profile remains with an "Assigned" status.) Deactivate 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, deactivate the profile.

- Delete any schedules for log collection from the relevant node.

- Delete any saved logs that were retrieved from the relevant node.

Point

- 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.

- Deactivate 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 Installing 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 and profile names
- Setting of Users

For information on the contents of these tasks, see "3.2 Installation Design for ISM."

(2) Installing ISM-VA

Install ISM-VA on a management server.

For information on the installation procedure, see "3.3 Installing 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 expand 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 Allocating 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
- Repositories
- Backups

Disk capacities cannot be expanded 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 issues logs through the following functions.

- Log Management

  The disk capacities for logs issued 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 added node expansions in the future into account.

  For information on how to estimate disk capacities for logs that are issued by Log Management, access your local support.

- Trouble investigation logs

  The log disk space needs to be expanded 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 expanding a log area is as follows:

  1. Allocate an additional virtual disk.

     For details, see "3.7.1 Allocating Virtual Disks to Entire ISM-VA."

  2. Switch the log level.

     For details, see "4.17 Switching 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 4 GB per OS type
Storage of ServerView Suite DVD	Import from ServerView Suite DVD	Approximately 8 GB per ServerView Suite DVD
Creation and storage of files for work	None	Approximately 0.5 GB

Point

- By correlating user groups and node groups, you can operate ISM separately for each node group. To do so, you have to prepare a separate repository for each user group. In this case, 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 expand 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 and iRMC 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.

1. You can avoid such IP address overlap by changing the IP address in the following procedure if an overlapped IP address is found. 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 Backing Up 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 Restoring ISM-VA."

Point

- It is recommended that you prepare separate networks for business use (business 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 make 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 expansion, 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 Installing ISM-VA

The ISM software is supplied with the "FUJITSU Software ServerView Infrastructure Manager 2.0.0 Media Pack."

Install ISM-VA according to the installation destination.

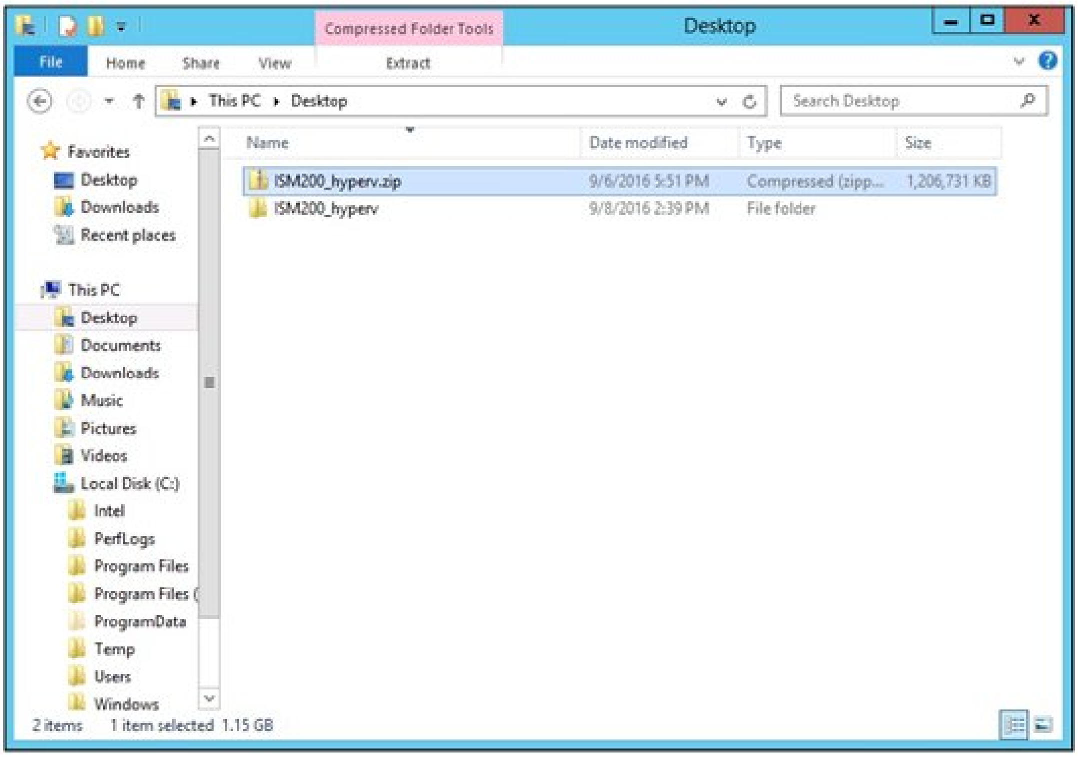
The following procedures describes how to install ISM-VA on Microsoft Windows Server Hyper-V, VMware vSphere Hypervisor, and KVM.

- 3.3.1 Installing on Microsoft Windows Server Hyper-V
- 3.3.2 Installing on VMware vSphere Hypervisor
- 3.3.3 Installing on KVM

3.3.1 Installing on Microsoft Windows Server Hyper-V

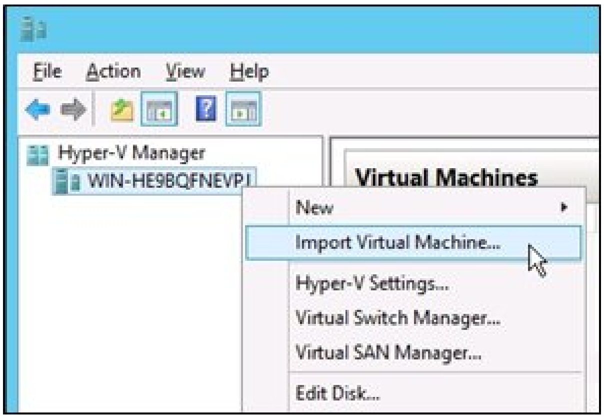
For installation, use the zip file that is included in the DVD media. For details on selecting installation destinations and network adapters that are to be specified midway during installation, refer to the Hyper-V manuals.

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.



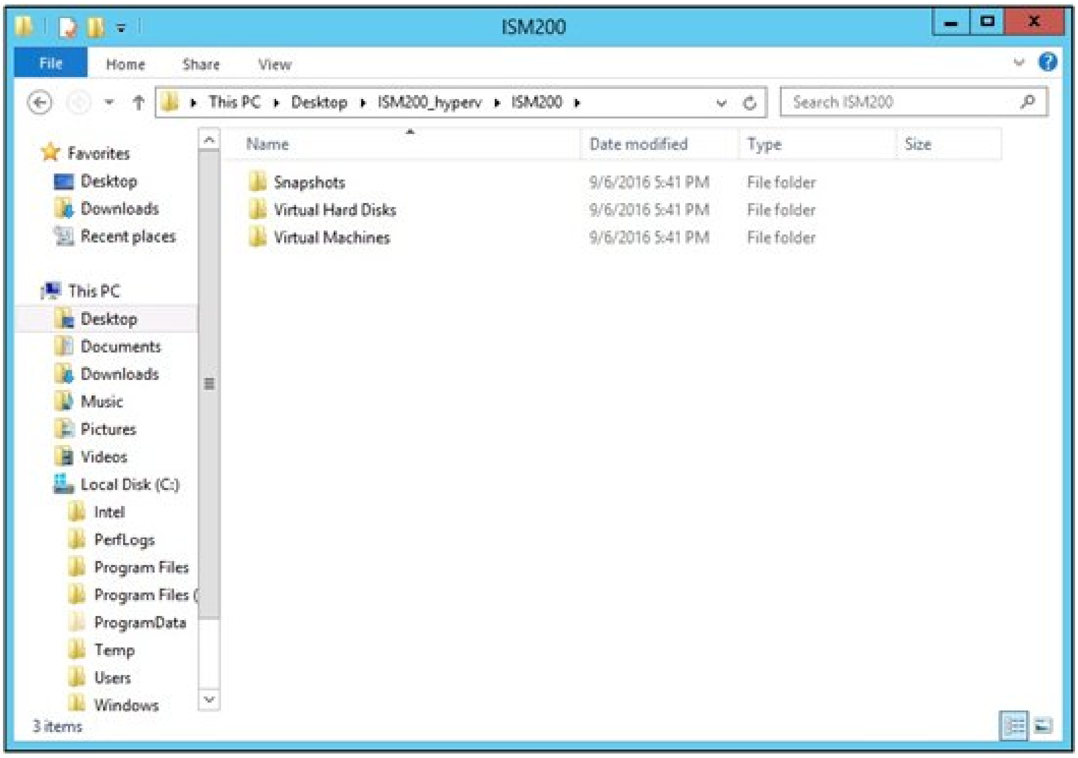
Name	Date modified	Type	Size
ISM200_hyperv.zip	9/6/2016 5:51 PM	Compressed (zipp...	1,206,731 KB
ISM200_hyperv	9/8/2016 2:39 PM	File folder	

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



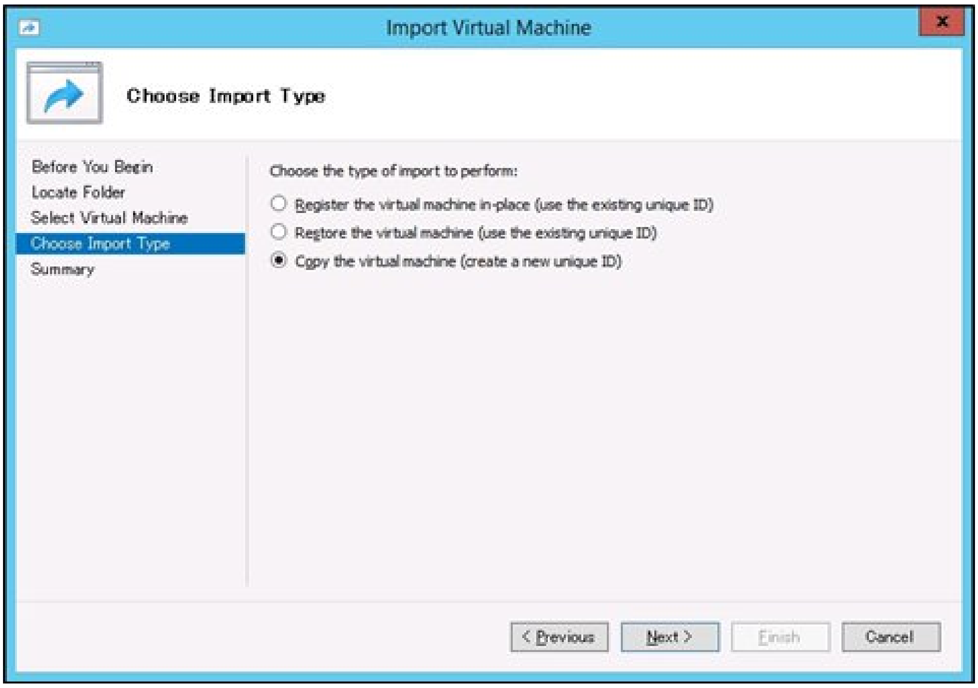
3. On the "Select Folder" screen, select the directory in which you deployed the file in Step 1.

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



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

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



Choose the type of import to perform:

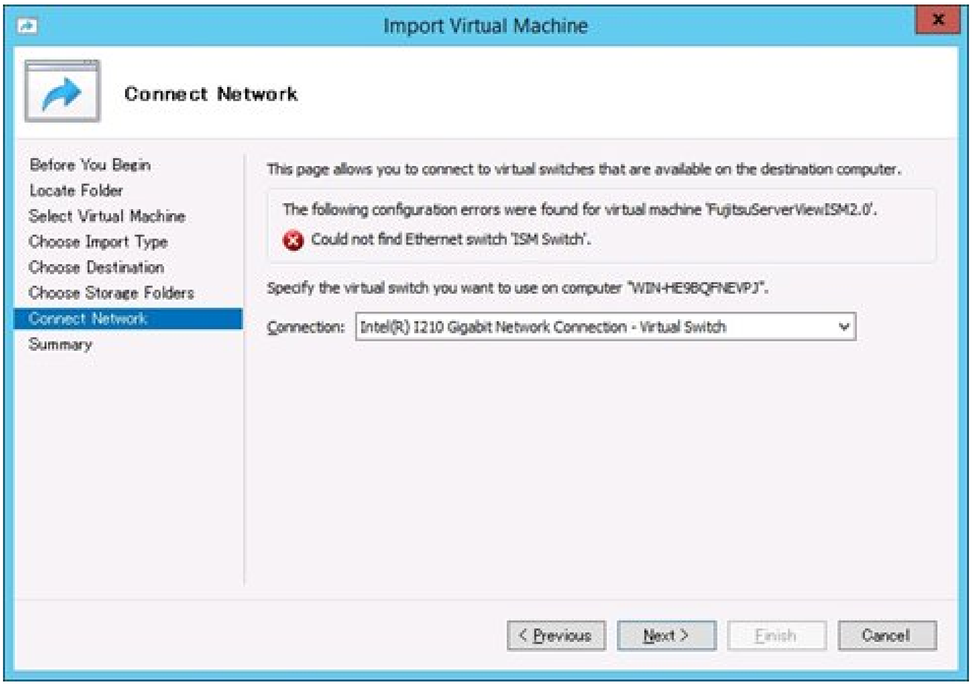
○ Register the virtual machine in-place (use the existing unique ID)

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

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

5. On the "Choose 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 click [Next].



Import Virtual Machine

Connect Network

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

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

Could not find Ethernet switch 'ISM Switch'.

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

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

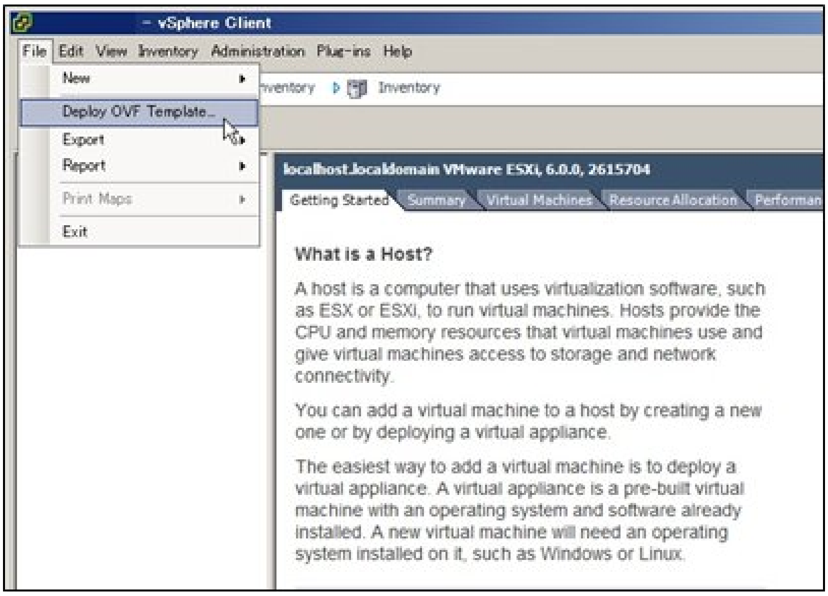
7. Click [Finish] to finish the import wizard.

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 Installing on VMware vSphere Hypervisor

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

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



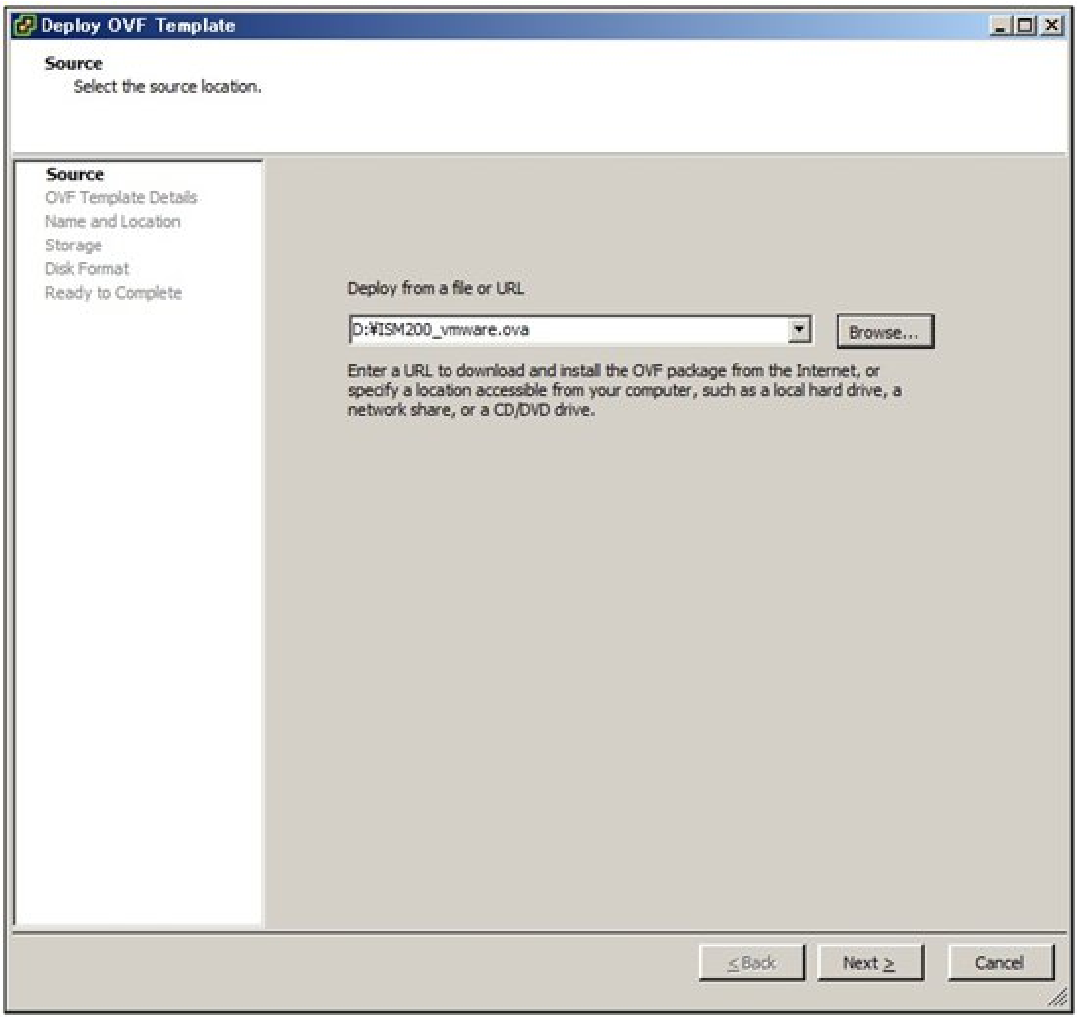
What is a Host?

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

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

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

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



Source

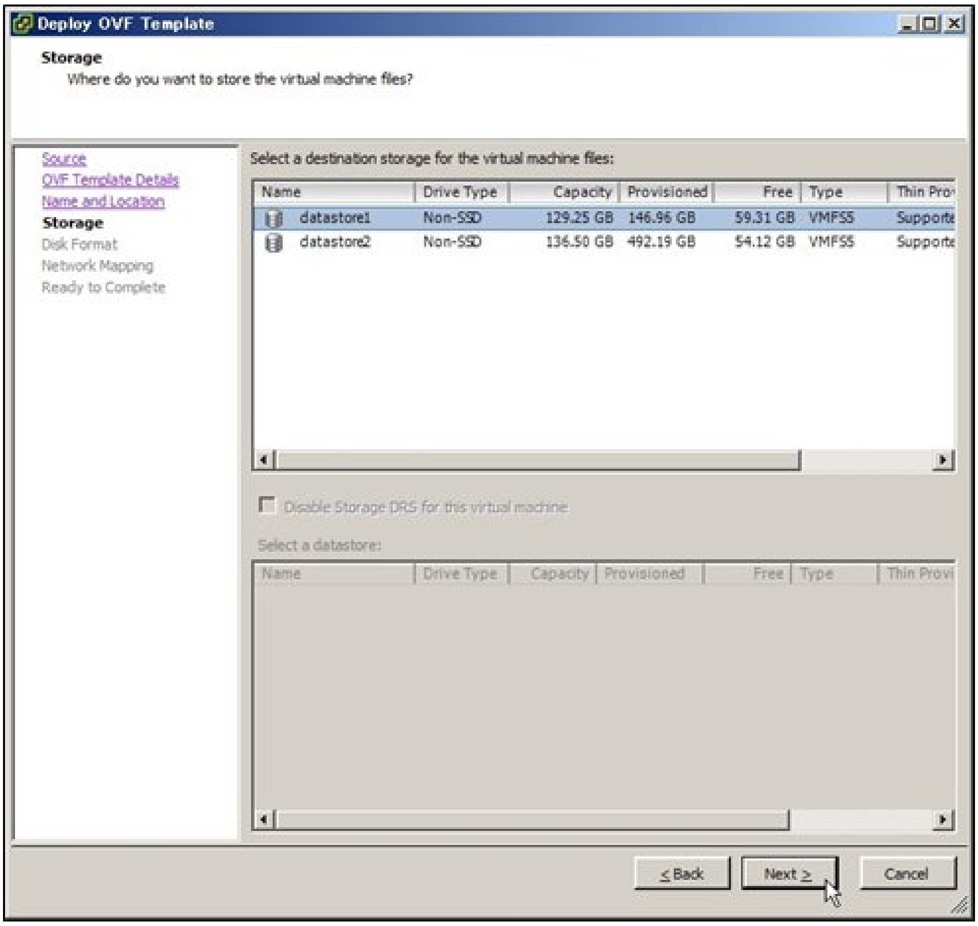
Select the source location.

Deploy from a file or URL

D:¥ISM200_vmware.ova

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

3. On the "Storage" screen, specify the location where the virtual machine is saved, and then click [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:

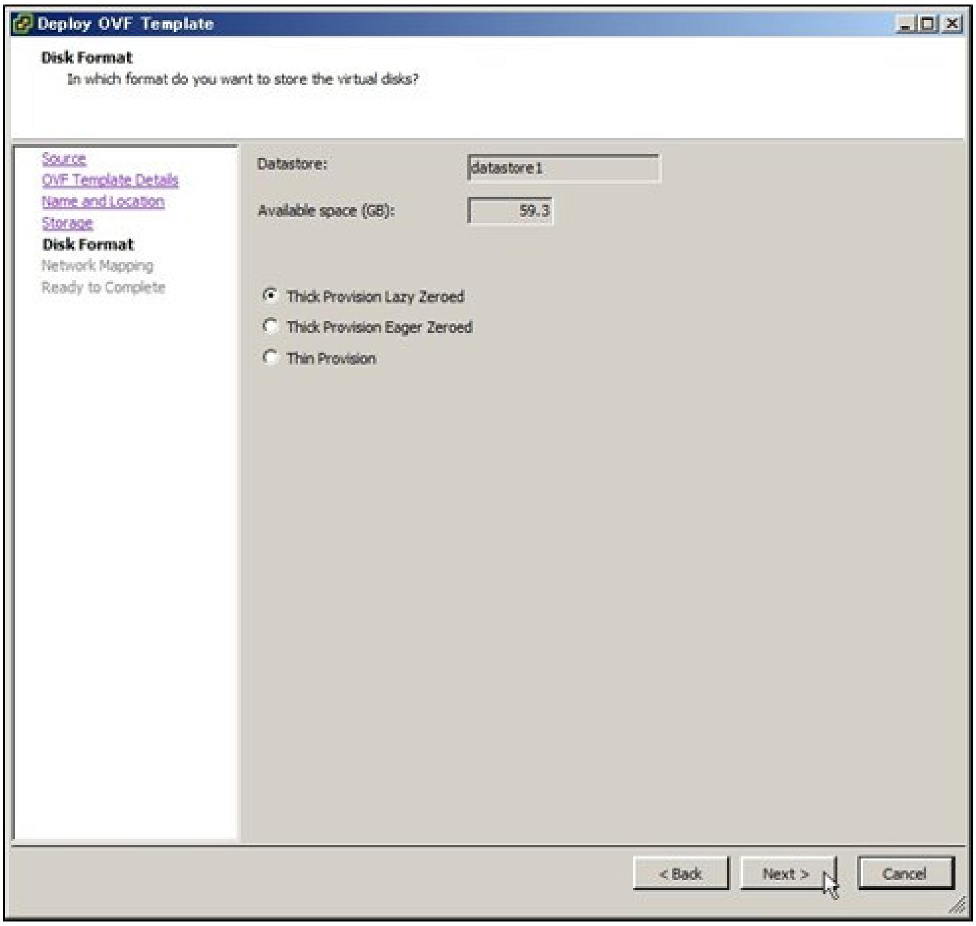
Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Pro
datastore1	Non-SSD	129.25 GB	146.96 GB	59.31 GB	VMFS5	Supporte
datastore2	Non-SSD	136.50 GB	492.19 GB	54.12 GB	VMFS5	Supporte

□ Disable Storage DRS for this virtual machine

Select a datastore:

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Provi

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



Deploy OVF Template

Disk Format

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

Datastore: datastore1

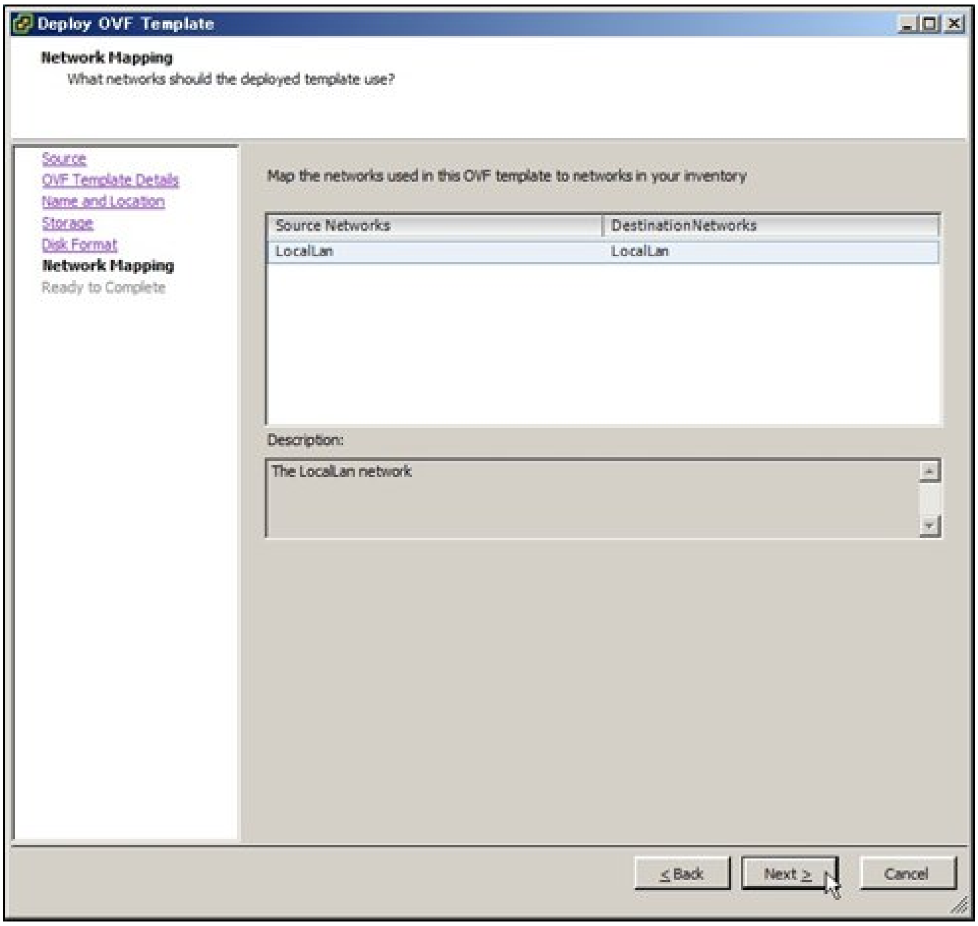
Available space (GB): 59.3

● Thick Provision Lazy Zeroed

○ Thick Provision Eager Zeroed

○ Thin Provision

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



Deploy OVF Template

Network Mapping

What networks should the deployed template use?

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

Source Networks	DestinationNetworks
LocalLan	LocalLan

Description:

The LocalLan network

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

3.3.3 Installing 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 ISM200_kvm.tar.gz
ISM200kvm/
ISM200_kvm/ISM200_kvm.qcow2
ISM200_kvm/ISM200.xml
```

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

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

   ```
   # cp ISM200_kvm.qcow2 /var/lib/libvirt/images
   ```

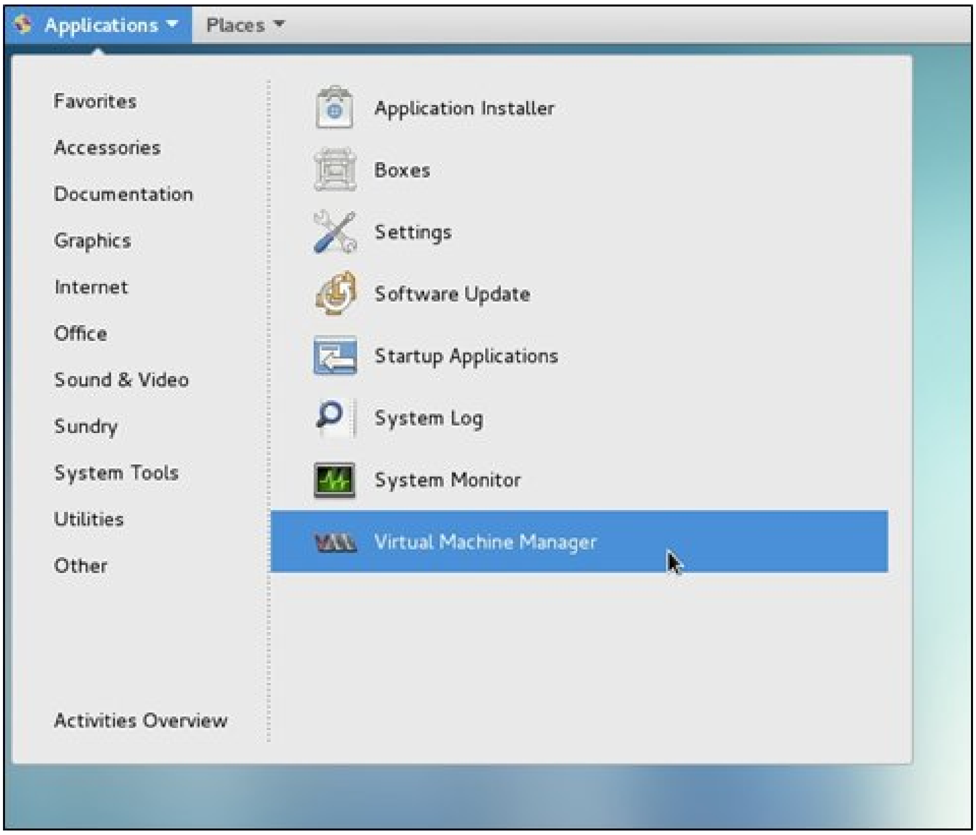
   b. Copy the xml file to /etc/libvirt/qemu.

   ```
   # cp ISM200.xml /etc/libvirt/qemu
   ```

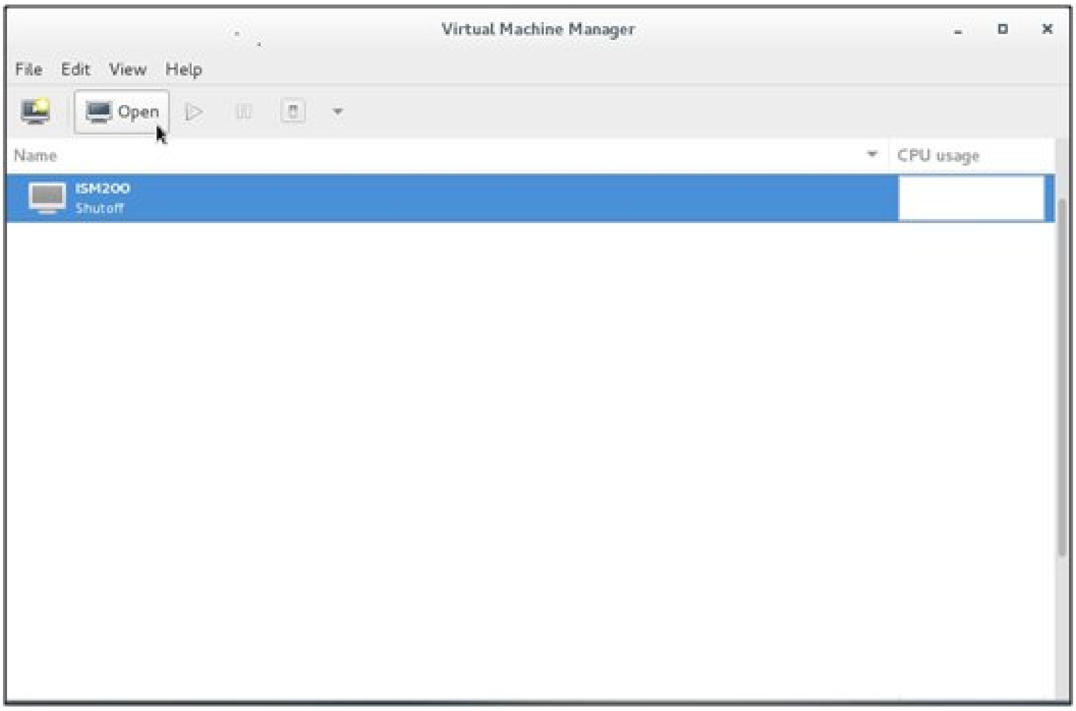
3. Specify the xml file to register ISM-VA.

```
# virsh define /etc/libvirt/qemu/ISM200.xml
```

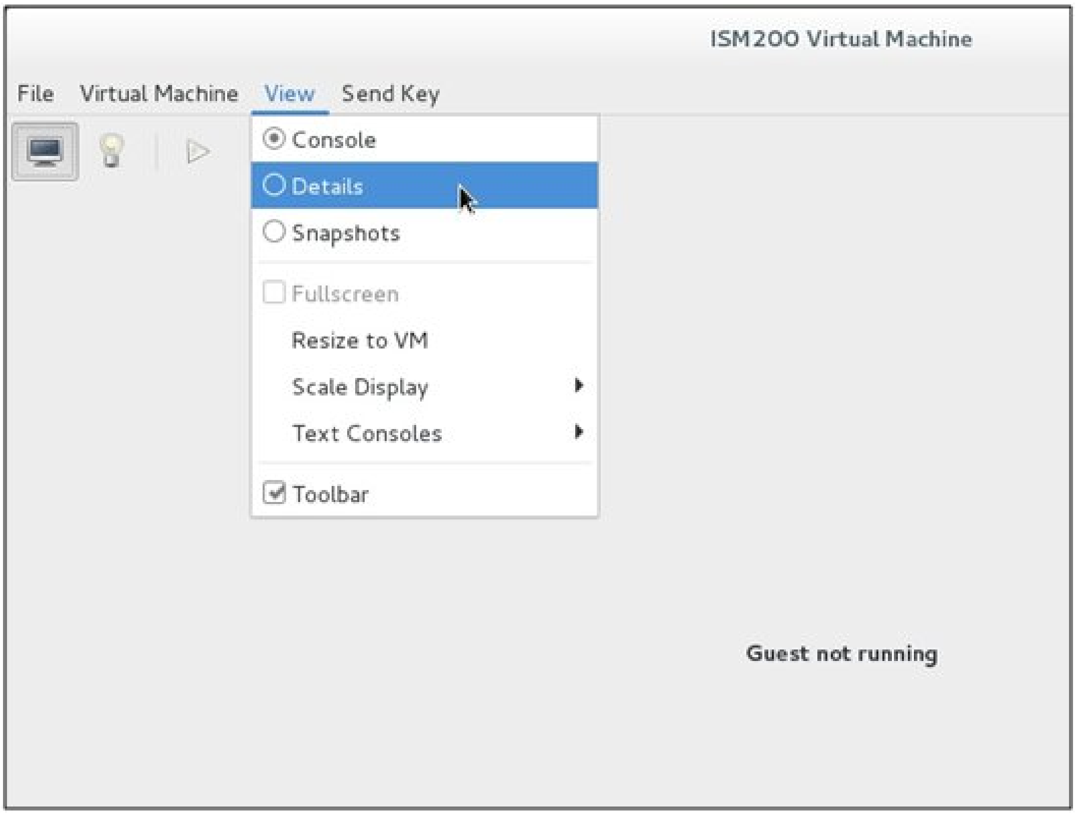
4. Click on [Virtual Machine Manager] to open Virtual Machine Manager.



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

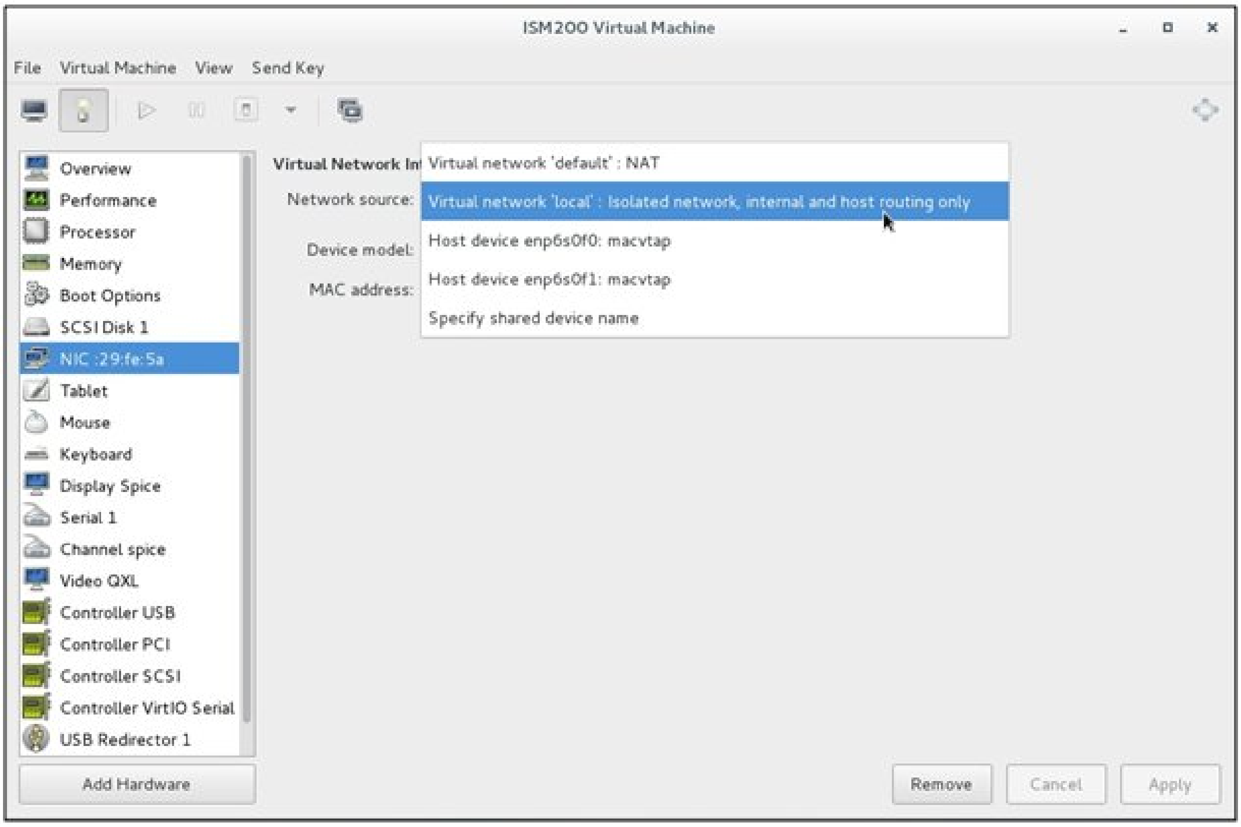


6. On the "ISM-VA Virtual Machine" screen, select [Details] from the [View] menu.



Guest not running

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 click [Apply].



Network source: Virtual network 'local' : Isolated network, internal and host routing only

3.4 Environment Settings for ISM-VA

Make the initial settings after installing ISM.

3.4.1 First Start of ISM-VA

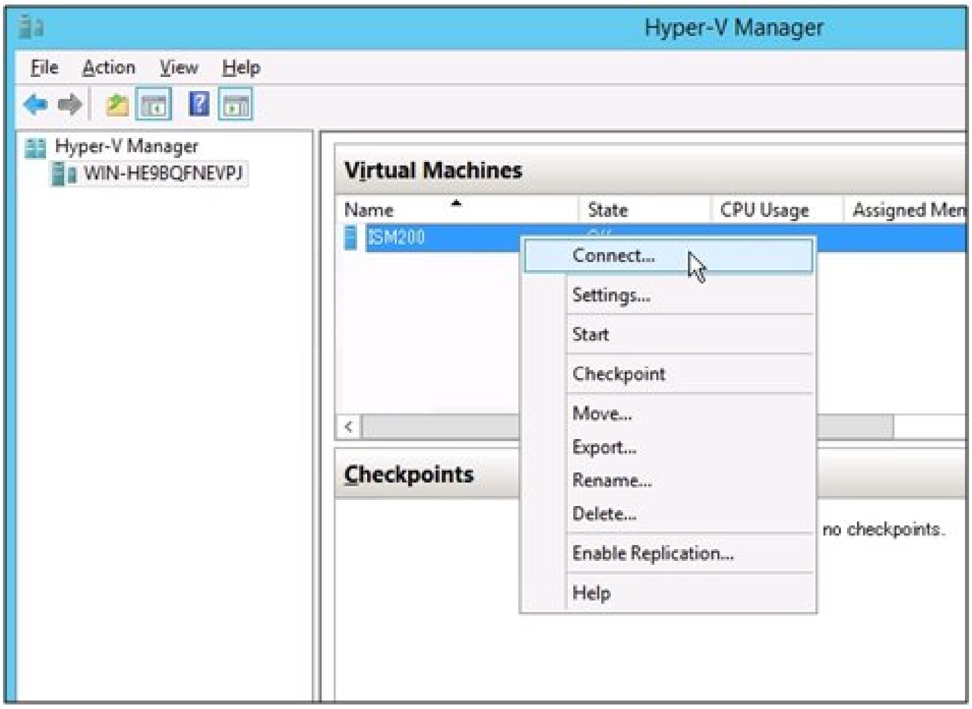
Use the respective function of the hypervisor on the installation destination to start up ISM-VA. Start up ISM-VA as a host OS user with administrator privileges.

The following procedures describes how to start up ISM-VA from Microsoft Windows Server Hyper-V, VMware vSphere Hypervisor, and KVM.

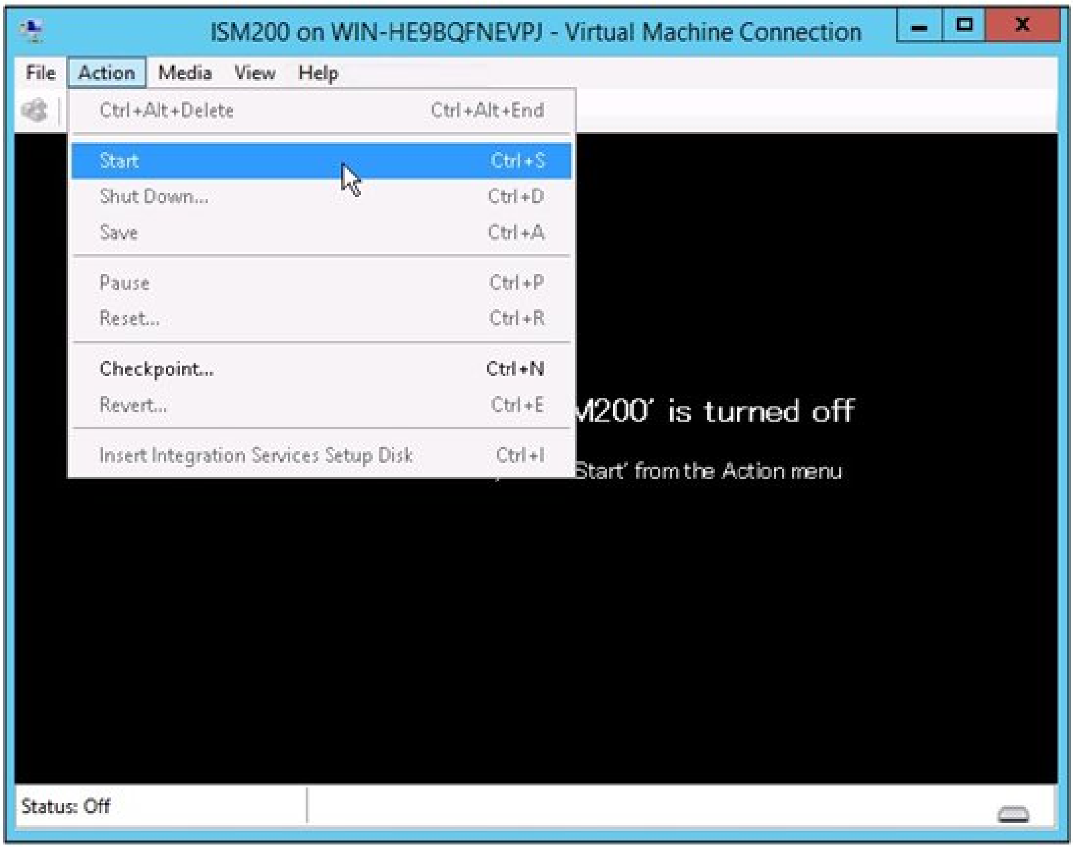
- 3.4.1.1 For ISM-VA Running on Microsoft Windows Server Hyper-V (First Time)
- 3.4.1.2 For ISM-VA Running on VMware vSphere Hypervisor (First Time)
- 3.4.1.3 For ISM-VA Running on KVM (First Time)

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].

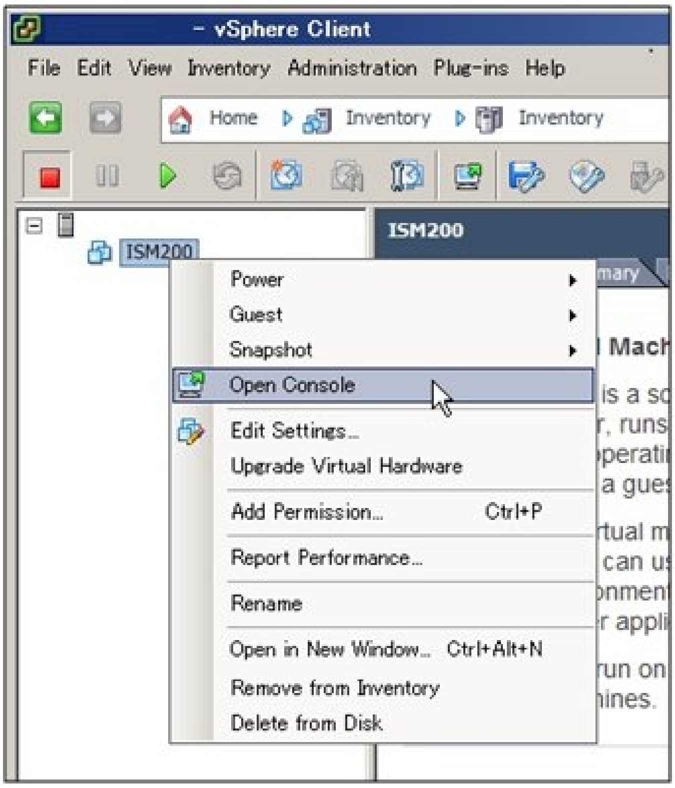


2. On the "Virtual Machine Connection" screen, select [Start] from the [Action] menu to start ISM-VA.

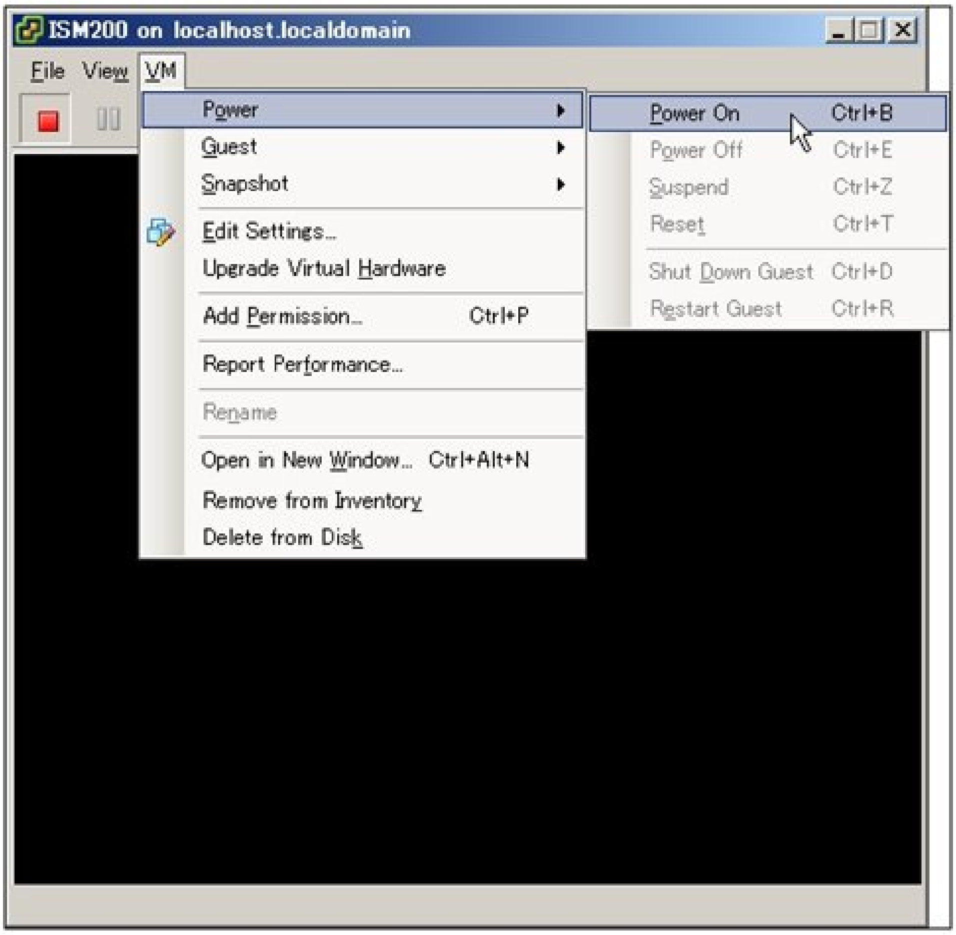


3.4.1.2 For ISM-VA Running on VMware vSphere Hypervisor (First Time)

1. In vSphere Client, right-click on the installed ISM-VA, and then select [Open Console].

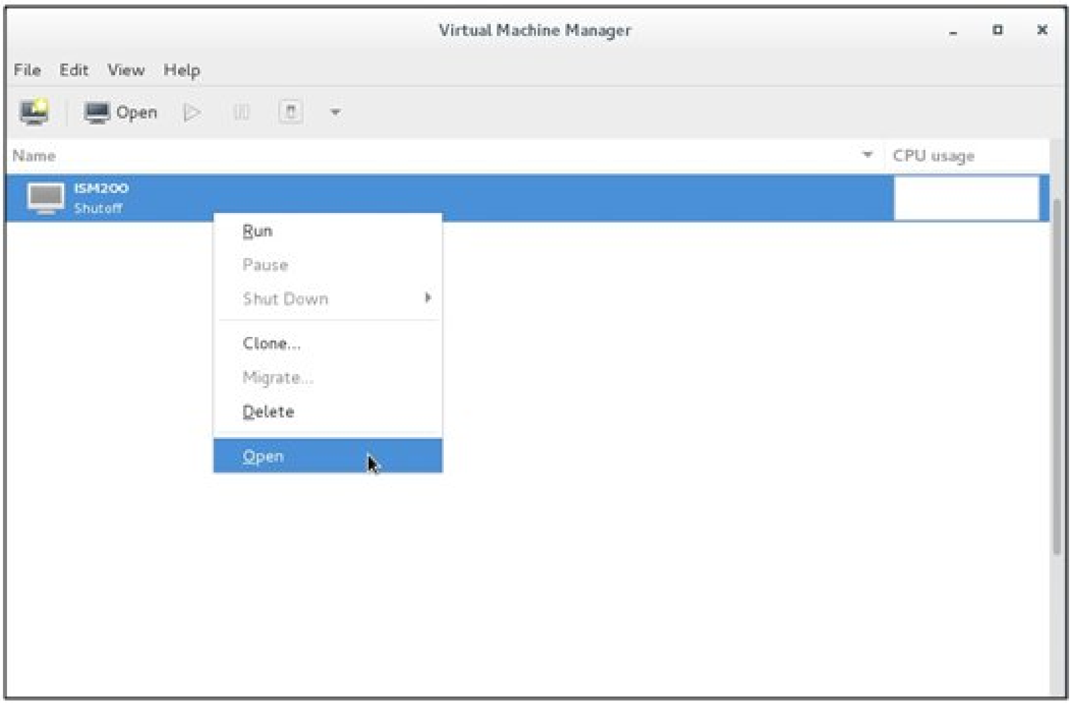


2. On the "Console" screen, select [Power] - [Power On] from the [VM] menu to start ISM-VA.

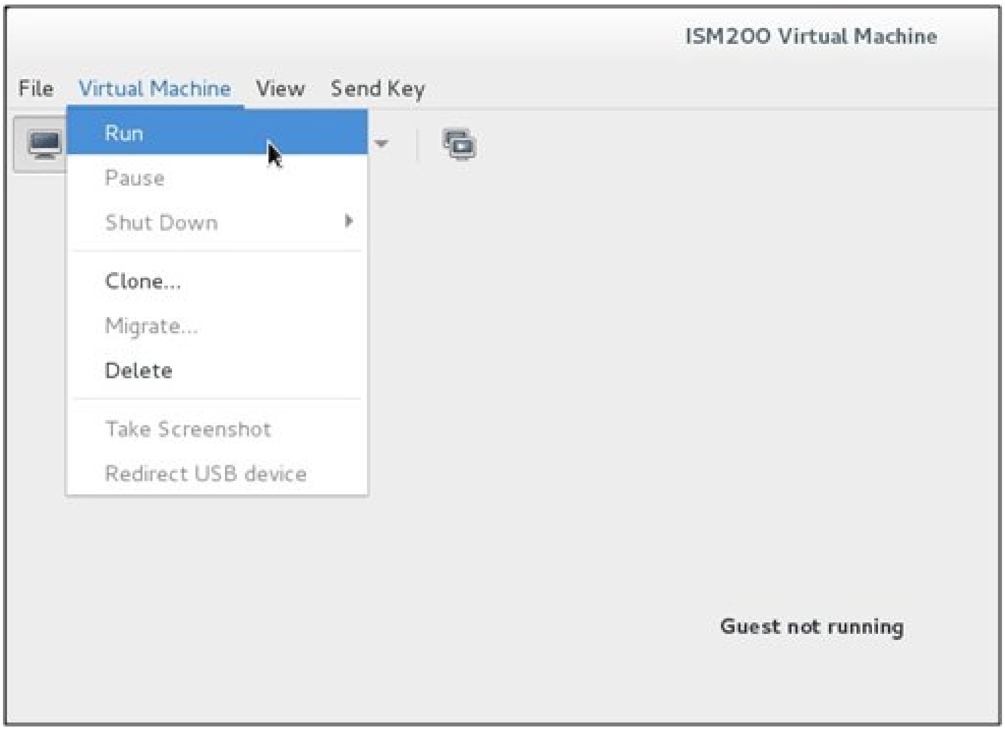


3.4.1.3 For ISM-VA Running on KVM (First Time)

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 commands to make the basic settings for ISM.

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.

In order to register licenses, 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
   ```

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

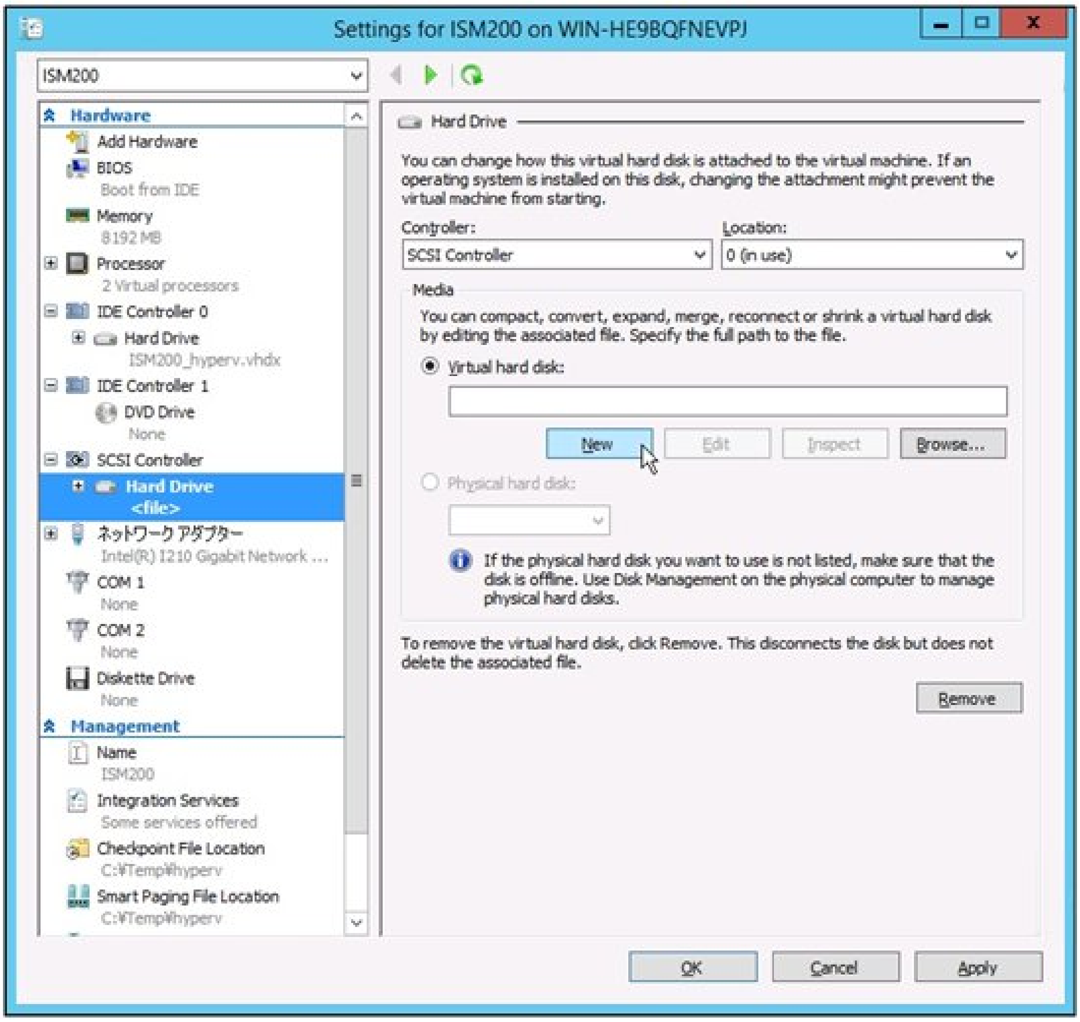
Virtual disks are resources for expanding ISM-VA disk capacities. The storage of logs, repositories, and backups requires large capacities of disk resources. Moreover, these capacities vary with the respective operating methods and scales of managed nodes. Allocating voluminous resources to virtual disks 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 Allocating Virtual Disks to Entire ISM-VA

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

   For Microsoft Windows Server Hyper-V



Settings for ISM200 on WIN-HE9BQFNEVPJ

Hard Drive

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

Controller: SCSI Controller

Location: 0 (in use)

Media

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

● Virtual hard disk:

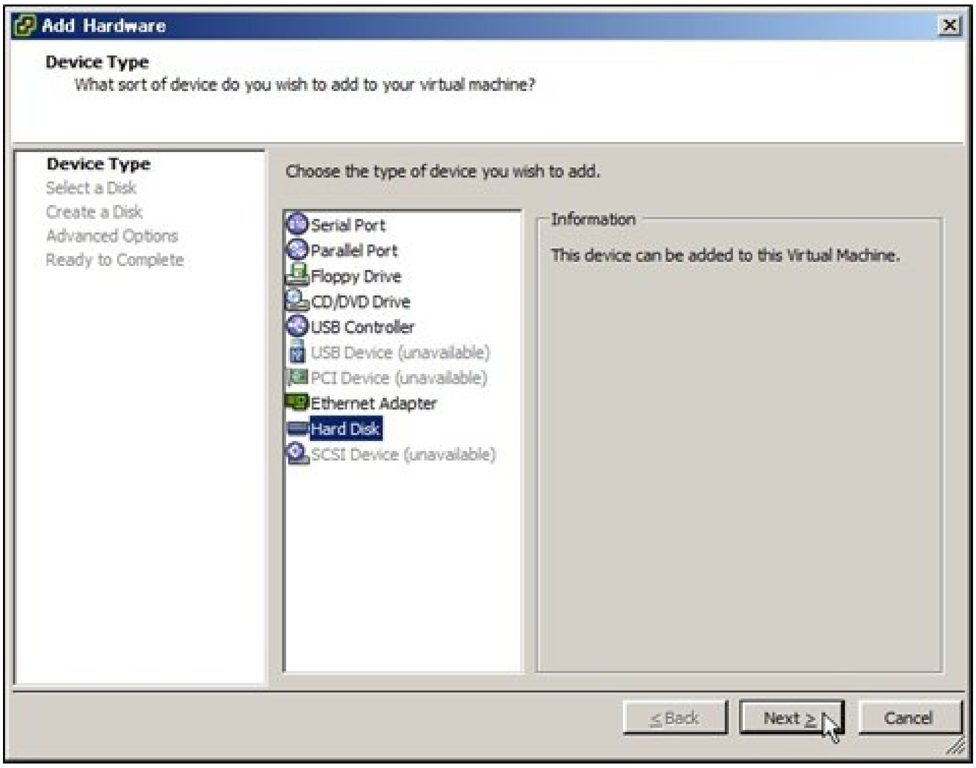
○ Physical hard disk:

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

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

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

For VMware vSphere Hypervisor



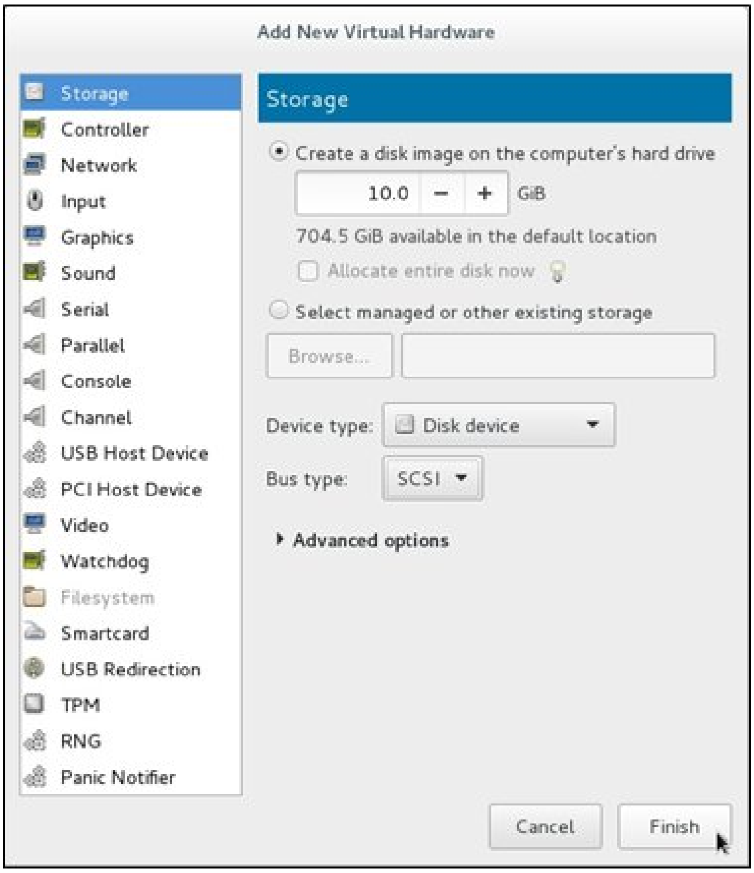
Device Type
What sort of device do you wish to add to your virtual machine?

Choose the type of device you wish to add.

This device can be added to this Virtual Machine.

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

For KVM



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

10.0 − + GiB

704.5 GiB available in the default location

□ Allocate entire disk now

○ Select managed or other existing storage

Device type: Disk device

Bus type: SCSI

For 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 whether the virtual disks you added in Step 1 are correctly recognized.

   Example:

```
# ismadm volume show -disk
Filesystem               Size  Used Remaining Used% Mounting position
/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
File system               Size  Used  Remaining  Used%  Mounting position
/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.

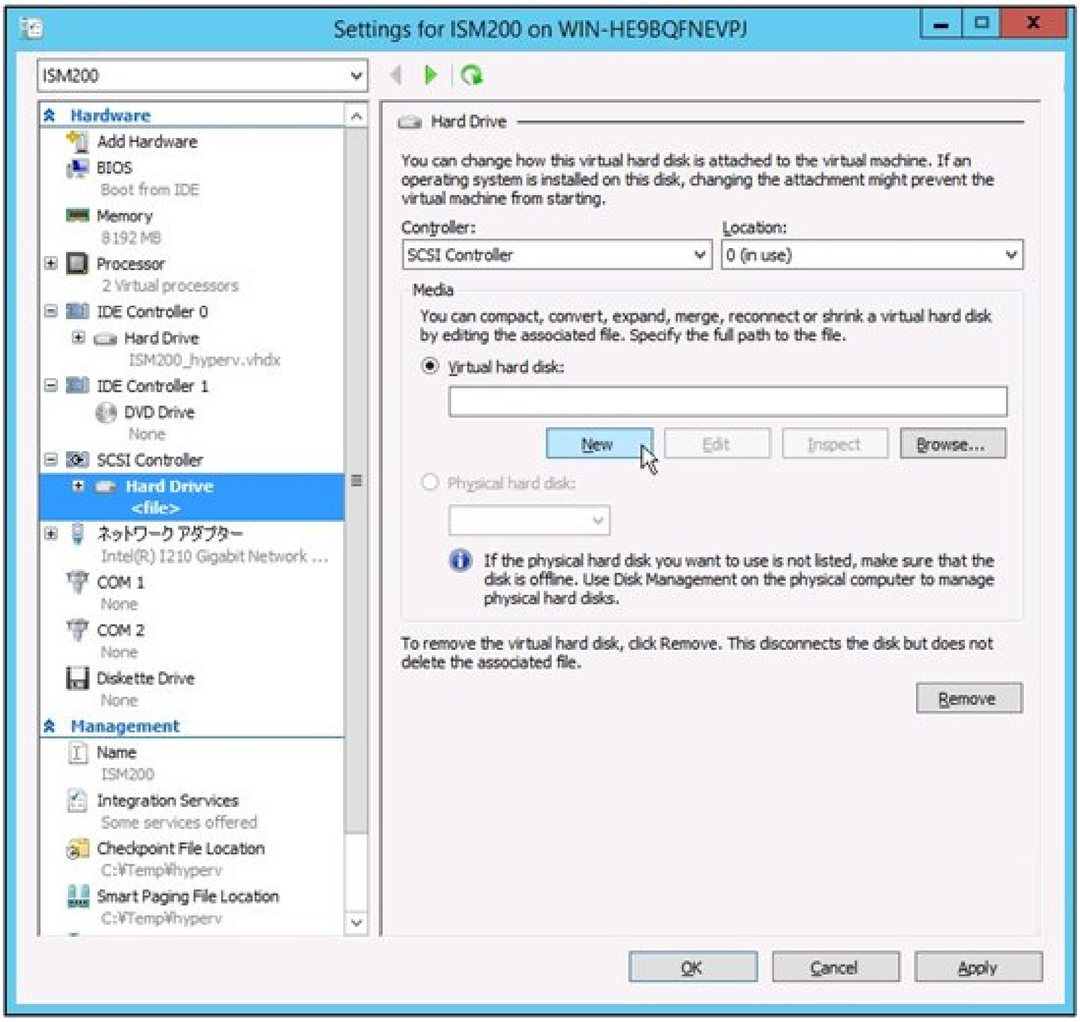
```
# ismadm power restart
```

3.7.2 Allocating Virtual Disks to User Groups

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

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

For Microsoft Windows Server Hyper-V



Settings for ISM200 on WIN-HE9BQFNEVPJ

Hard Drive

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

Controller: SCSI Controller

Location: 0 (in use)

Media

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

● Virtual hard disk:

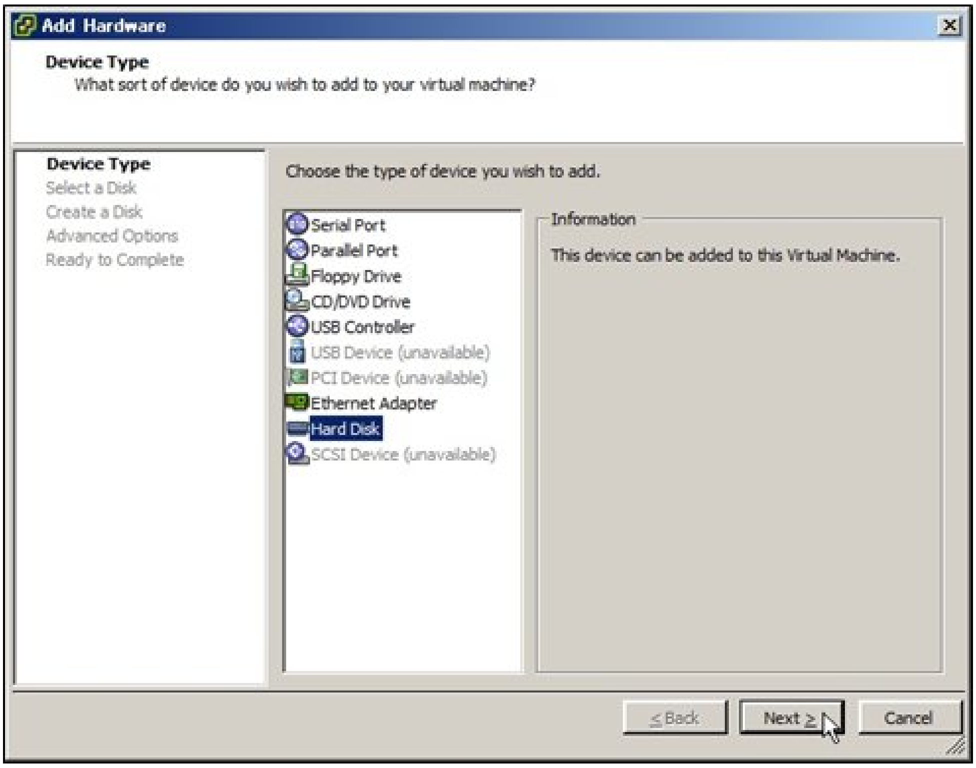
○ Physical hard disk:

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

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

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

For VMware vSphere Hypervisor



Add Hardware

Device Type

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

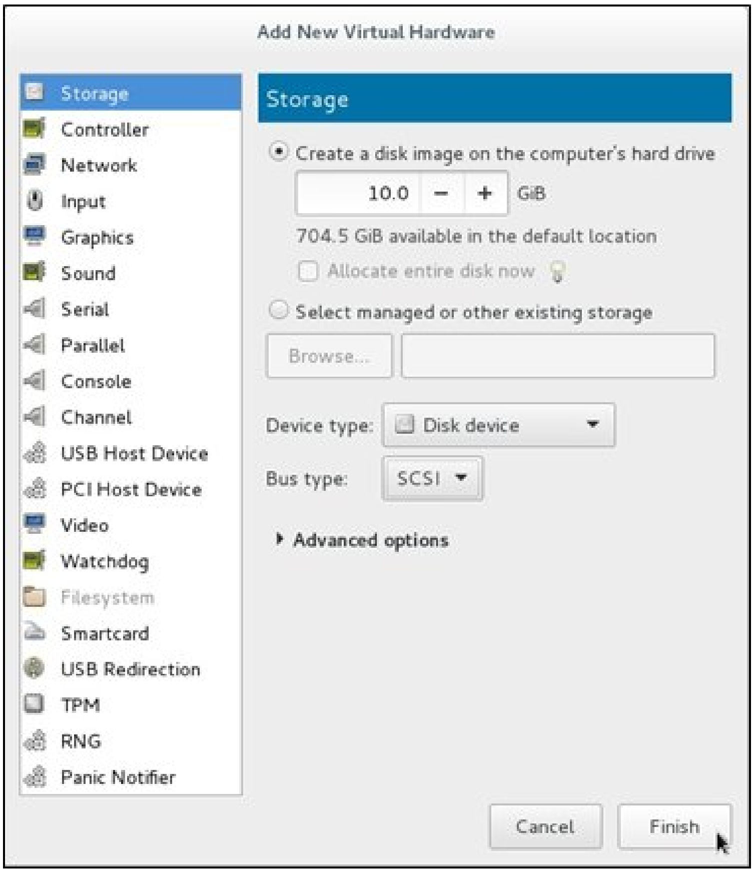
Choose the type of device you wish to add.

Information

This device can be added to this Virtual Machine.

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

For KVM



Add New Virtual Hardware

Storage

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

10.0 − + GiB

704.5 GiB available in the default location

□ Allocate entire disk now

○ Select managed or other existing storage

Device type: Disk device

Bus type: SCSI

For 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 whether the virtual disks you added in Step 1 are correctly recognized.

   Example:

```
# ismadm volume show -disk
File system               Size  Used  Remaining  Used%  Mounting position
/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. Activate 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
File system               Size  Used  Remaining  Used%  Mounting position
/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
```

Chapter 4 Controlling ISM

This chapter describes how to control ISM.

4.1 Starting Up and Terminating ISM

Sometimes, you may need to start up or terminate ISM manually for maintenance or other reasons.

4.1.1 Starting Up ISM-VA

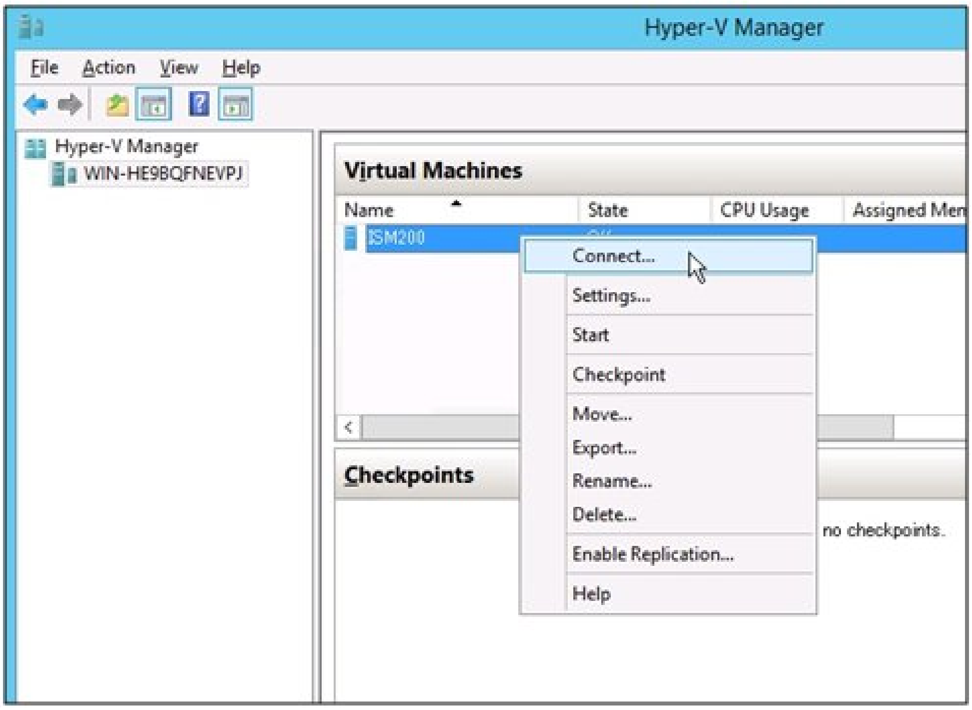
Use the respective function of the hypervisor on the installation destination to start up ISM-VA. Start up ISM-VA as a host OS user with administrator privileges.

The following procedures describe how to start up ISM-VA from Microsoft Windows Server Hyper-V, VMware vSphere Hypervisor, and KVM.

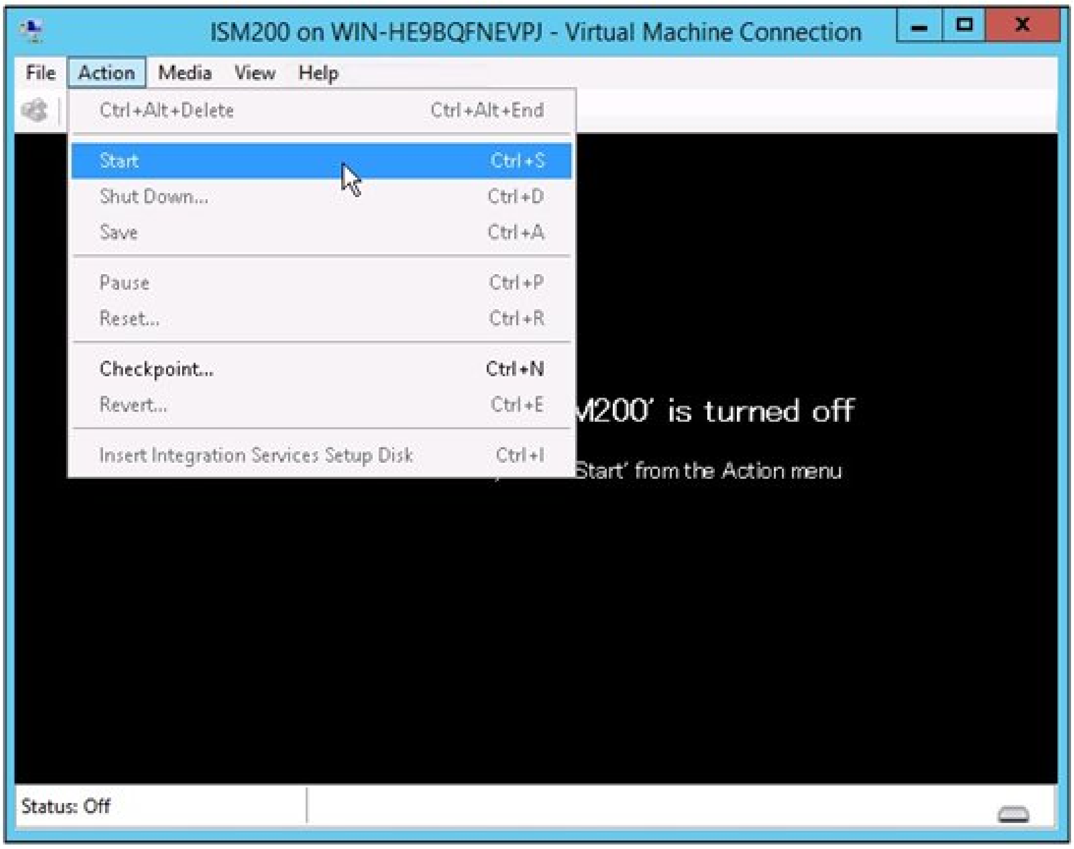
- 4.1.1.1 For ISM-VA Running on Microsoft Windows Server Hyper-V (Second Time and Later)
- 4.1.1.2 For ISM-VA Running on VMware vSphere Hypervisor (Second Time and Later)
- 4.1.1.3 For ISM-VA Running on KVM (Second Time and Later)

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].

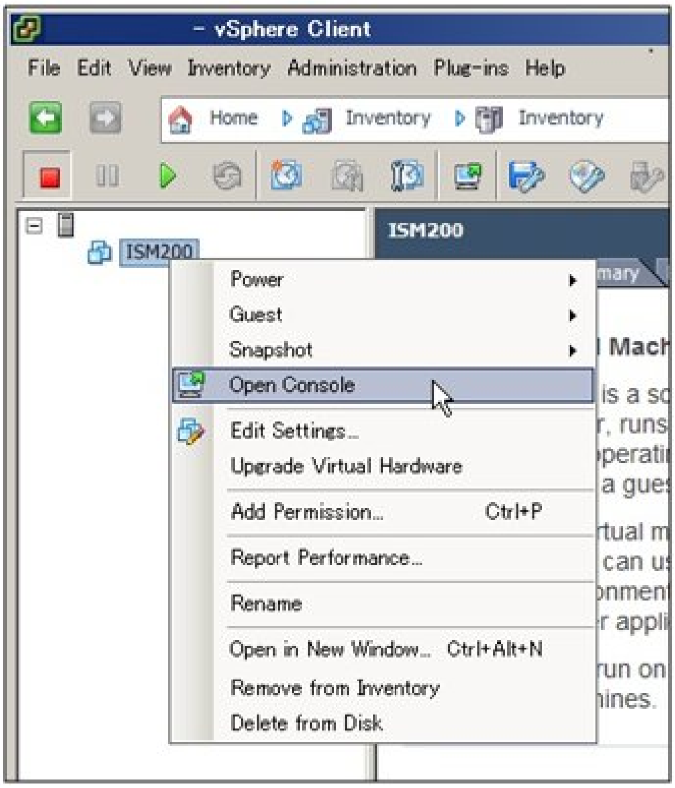


2. On the "Virtual Machine Connection" screen, select [Start] from the [Action] menu to start ISM-VA.

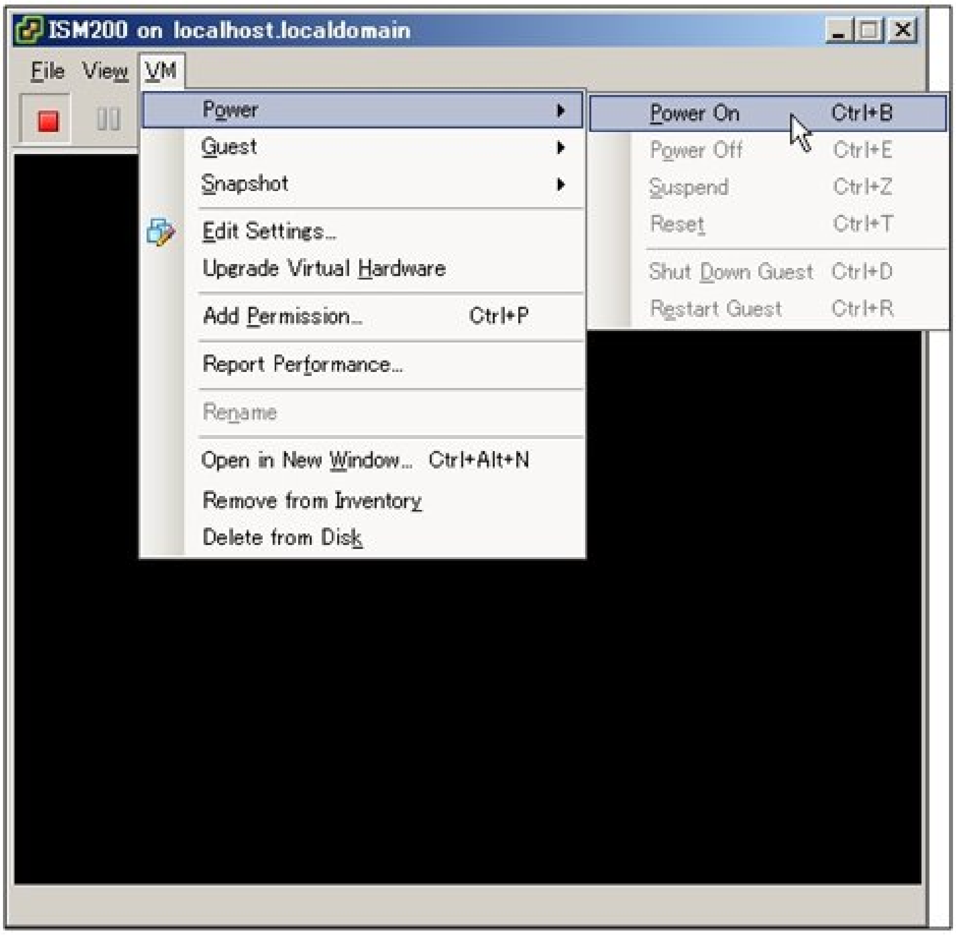


4.1.1.2 For ISM-VA Running on VMware vSphere Hypervisor (Second Time and Later)

1. In vSphere Client, right-click on the installed ISM-VA, and then select [Open Console].

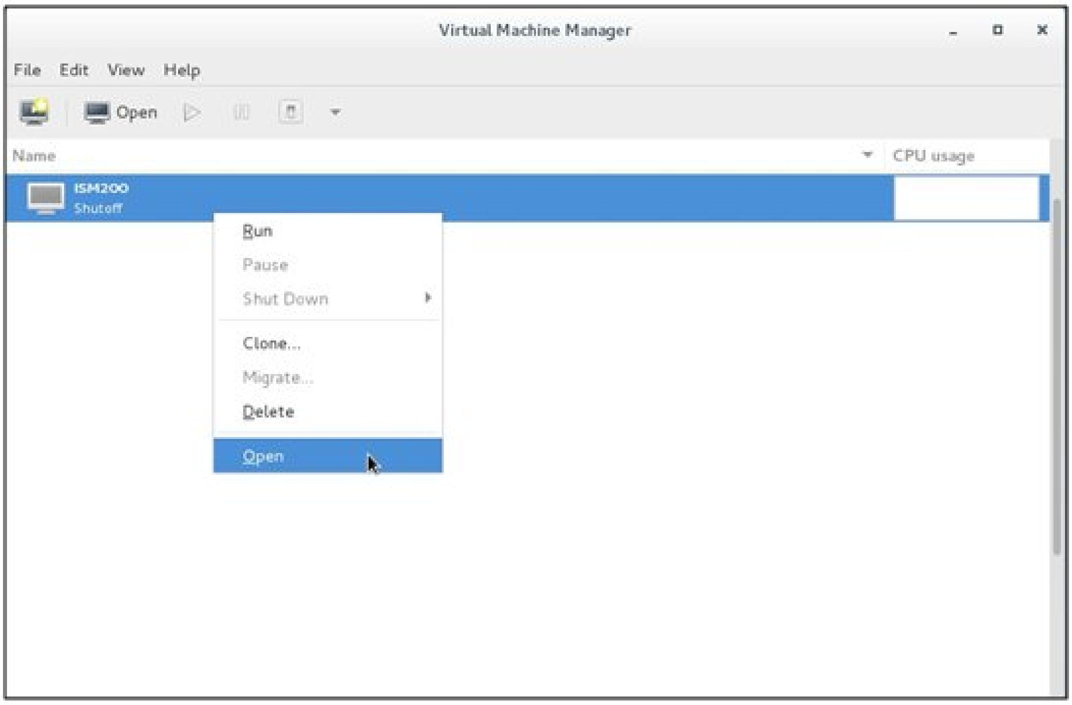


2. On the "Console" screen, select [Power] - [Power On] from the [VM] menu to start ISM-VA.

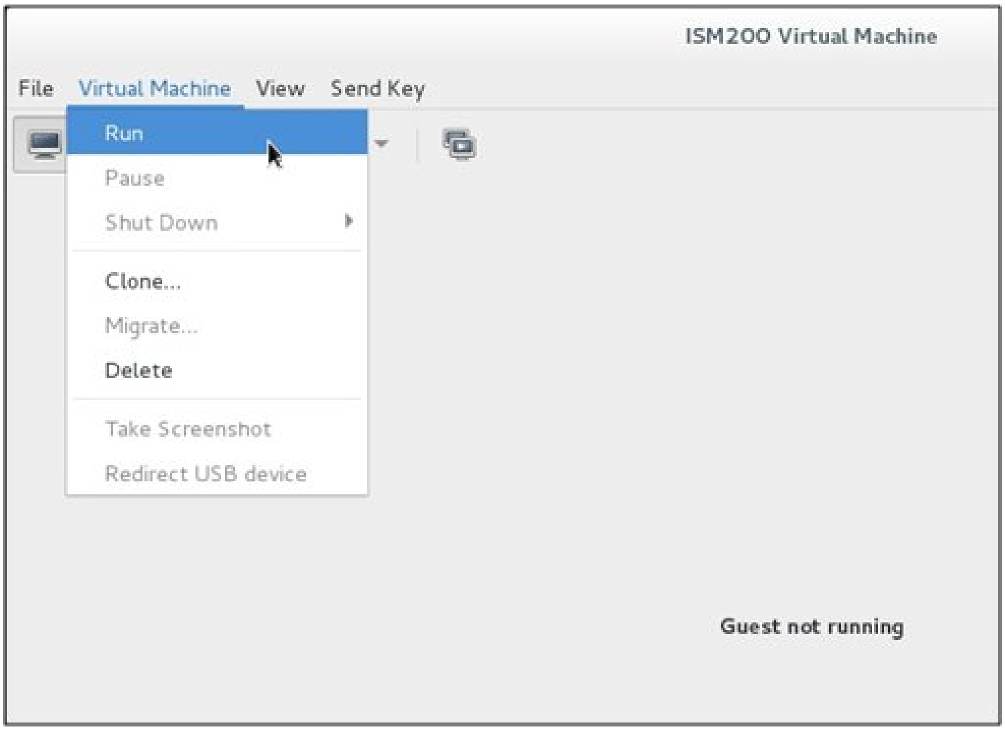


4.1.1.3 For ISM-VA Running on KVM (Second Time and Later)

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.



Point

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 Terminating 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 "Task" screen to confirm that all tasks are terminated.

   a. Select [Events/Tasks] - [Tasks].

   b. On the "Task" screen, confirm that all statuses are either "Complete" or "Cancel-Complete."

   c. If there are any tasks with a status other than "Complete" or "Cancel-Complete," either wait until they finish, or cancel them manually.

      To cancel a task that is being executed, select the task and then [Actions] - [Cancel]. Cancel all tasks that are currently being executed.

      Tasks of the "Firmware Update" 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 Restarting 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 Terminating ISM-VA."

2. Execute the following command to restart ISM-VA.

```
# ismadm power restart
```

4.1.4 Starting and Stopping 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.

Starting ISM service

1. Execute the following command to start the ISM service.

```
# ismadm service start ism
```

Stopping 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 Terminating 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 done 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		Setting Contents	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	

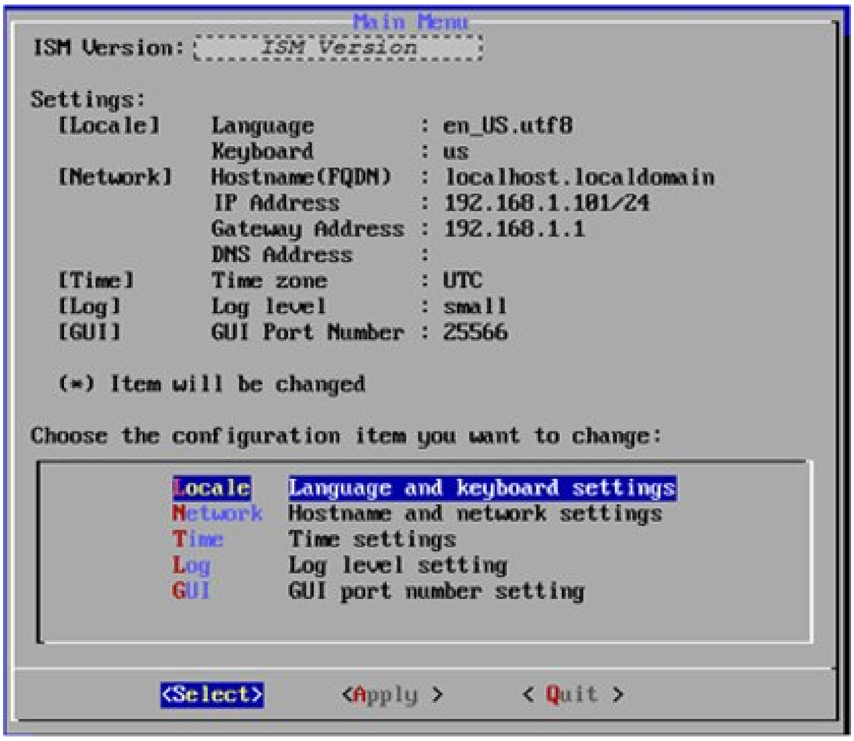
Item		Setting Contents	Corresponding ismadm command
Time	Timezone	Time zone setting	ismadm time set-timezone
Log	Log level	Damage investigation log size setting	ismadm system change-log-level
GUI	GUI port number	Web GUI connection port setting	ismadm service modify -port

The following is method for using the ISM-VA basic settings menu.

1. From the console, log in to ISM-VA as administrator.
2. Start using the ISM-VA basic settings menu command.

```
# ismsetup
```

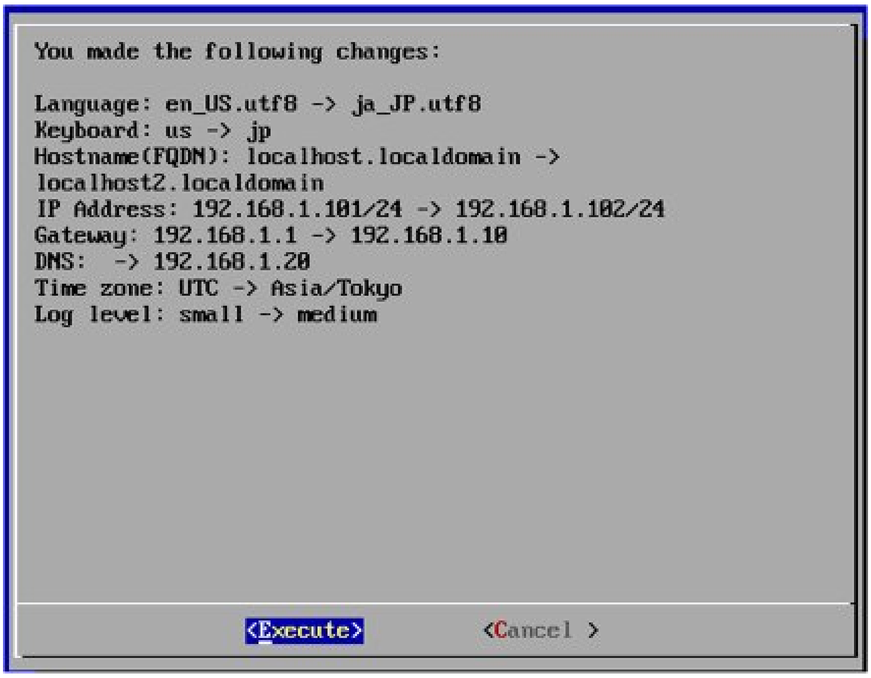
The screen below is displayed.



```
                           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
  [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].

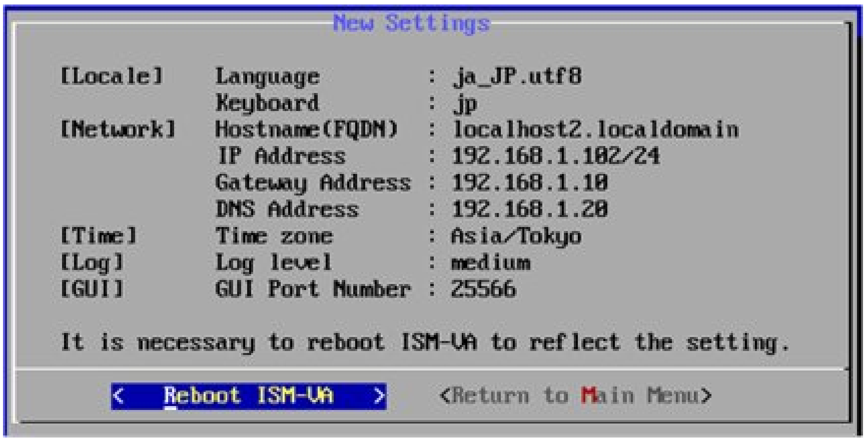
5. Confirm the changes, then select [Execute].



```
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
```

After the change processing has finished the change results are displayed.

6. To apply the changes, select [Reboot ISM-VA] and restart ISM-VA.



```
                          New Settings

  [Locale]    Language          : ja_JP.utf8
              Keyboard          : jp
  [Network]   Hostname(FQDN)    : localhost2.localdomain
              IP Address        : 192.168.1.102/24
              Gateway Address   : 192.168.1.10
              DNS Address       : 192.168.1.20
  [Time]      Time zone         : Asia/Tokyo
  [Log]       Log level         : medium
  [GUI]       GUI Port Number   : 25566

  It is necessary to reboot ISM-VA to reflect the setting.
```

4.3 Modifying Destination Port Number of ISM

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 Backing Up and Restoring 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 Terminating ISM-VA."

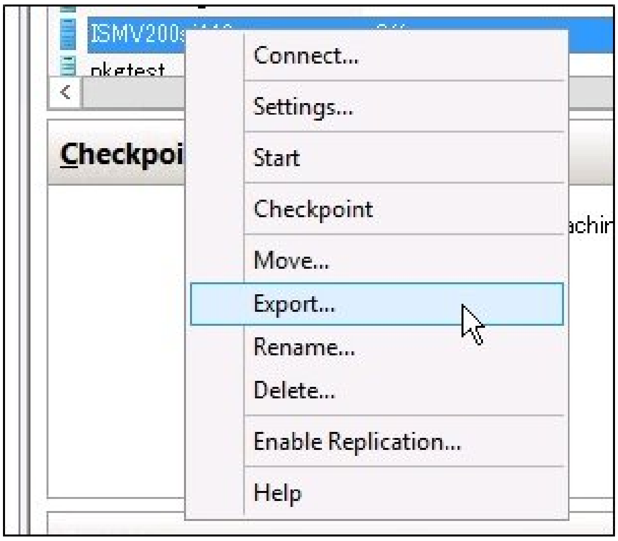
4.4.1 Backing Up ISM-VA

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.

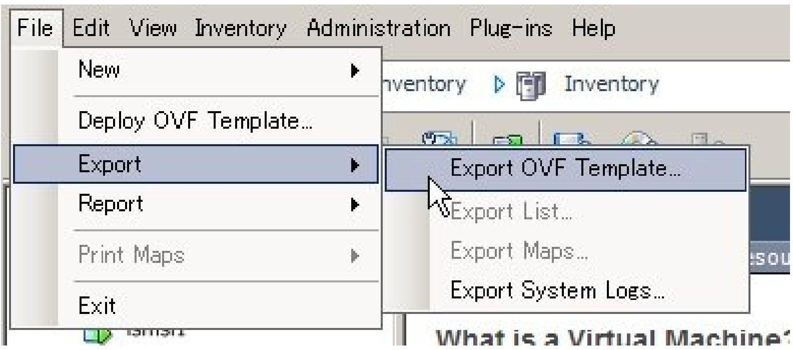
Backing Up ISM-VA Running on Microsoft Windows Server Hyper-V

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



Backing Up ISM-VA Running on VMware vSphere Hypervisor

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



Backing Up ISM-VA Running on KVM

Back up the KVM files that are stored in the following locations to any other locations as needed.

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

4.4.2 Restoring ISM-VA

To restore ISM-VA, use the backed up files and implement the procedure described in "3.3 Installing ISM-VA."

4.5 Collecting Data for Maintenance

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 needed. 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.

4.6 Management of Virtual Disks

You can cancel or newly add allocations of virtual disks.

4.6.1 Canceling Allocations of Virtual Disks

You can cancel allocations of virtual disks that you made according to "3.7.2 Allocating Virtual Disks to User Groups."

Note

- On canceling an allocation, all data that were stored in the user group will be lost.
- Allocations of virtual disks to Administrator groups cannot be canceled.
- Allocations of virtual disks to the entire ISM-VA as made according to "3.7.1 Allocating Virtual Disks to Entire ISM-VA" cannot be canceled.

The following operating example shows how to cancel the allocation of a virtual disk to a user group named usrgrp1.

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

2. In order to cancel allocation of the virtual disks, stop the ISM service temporarily.

```
# ismadm service stop ism
```

3. Confirm that the virtual disk is allocated to usrgrp1.

```
# ismadm volume show -disk
File system               Size  Used  Remaining  Used%  Mounting position
/dev/mapper/centos-root    16G  2.5G   13G       17%    /
devtmpfs                  1.9G     0  1.9G        0%    /dev
tmpfs                     1.9G  4.0K  1.9G        1%    /dev/shm
tmpfs                     1.9G  8.6M  1.9G        1%    /run
tmpfs                     1.9G     0  1.9G        0%    /sys/fs/cgroup
/dev/sda1                 497M  170M  328M       35%    /boot
tmpfs                     380M     0  380M        0%    /run/user/0
tmpfs                     380M     0  380M        0%    /run/user/1001
/dev/mapper/usrgrp1vol-lv     10G   33M   10G    1% 'RepositoryRoot'/usrgrp1

  PV         VG          Fmt  Attr PSize  PFree
  /dev/sda2  centos      lvm2 a--  19.51g    0
  /dev/sdb1  usrgrp1vol  lvm2 a--  10.00g    0
```

In this example, the VG named usrgrp1vol is allocated to usrgrp1.

4. Specify the User Group Name and unmount the virtual disk.

```
# ismadm volume umount -gdir usrgrp1
```

5. Specify the Volume Name (usrgrp1vol) for usrgrp1 and delete the virtual disk.

```
# ismadm volume delete -vol usrgrp1vol
  Logical volume "usrgrp1vol" successfully removed.
```

6. Confirm the virtual disk settings.

   Confirm that no virtual disk is set for usrgrp1 and that the previously used directory "/dev/sdb" is now free.

```
# ismadm volume show -disk
File system               Size  Used  Remaining  Used%  Mounting position
/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 Allocating Additional Virtual Disks to Entire ISM-VA

Using the same method as in "3.7.1 Allocating Virtual Disks to Entire ISM-VA," you can additionally allocate multiple virtual disks to the entire ISM-VA.

4.6.3 Allocating Additional Virtual Disks to User Groups

You can allocate virtual disks in addition to the ones you allocated according to "3.7.2 Allocating Virtual Disks to User Groups."

The following operating example shows how to allocate an additional virtual disk to a user group named usrgrp1.

1. Connect to the virtual disk.

   Carry out the operations described in Step 1 of "3.7.2 Allocating 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.

```
File system               Size  Used  Remaining  Used%  Mounting position
/dev/mapper/centos-root    16G  2.6G   13G       17 %    /
devtmpfs                  1.9G     0  1.9G        0%    /dev
tmpfs                     1.9G  4.0K  1.9G        1%    /dev/shm
tmpfs                     1.9G  8.5M  1.9G        1%    /run
tmpfs                     1.9G     0  1.9G        0%    /sys/fs/cgroup
/dev/sda1                 497M  169M  329M       34 %    /boot
/dev/mapper/usrgrp1vol-lv  10G   33M   10G        1%    'RepositoryRoot'/usrgrp1
tmpfs                     380M     0  380M        0%    /run/user/0
/dev/sdc                                              (Free)

  PV         VG      Fmt  Attr PSize  PFree
  /dev/sda2  centos  lvm2 a--  19.51g    0
  /dev/sdb1  usrgrp1vol  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 usrgrp1vol.

```
# ismadm volume extend -vol usrgrp1vol -disk /dev/sdc
  Logical volume "/dev/mapper/usrgrp1vol-lv" resized.
```

6. Confirm the virtual disk settings.

   Confirm that the newly added volume (/dev/sdc) is set for use by usrgrp1 (usrgrp1vol).

```
# ismadm volume show -disk
File system               Size  Used  Remaining  Used%  Mounting position
/dev/mapper/centos-root    16G  2.6G   13G       17%    /
devtmpfs                  1.9G     0  1.9G        0%    /dev
tmpfs                     1.9G  4.0K  1.9G        1%    /dev/shm
tmpfs                     1.9G  8.6M  1.9G        1%    /run
tmpfs                     1.9G     0  1.9G        0%    /sys/fs/cgroup
/dev/sda1                 497M  170M  328M       35%    /boot
/dev/mapper/usrgrp1vol-lv  15G   33M   15G        1%    'RepositoryRoot'/usrgrp1
tmpfs                     380M     0  380M        0%    /run/user/0
tmpfs                     380M     0  380M        0%    /run/user/1001

  PV         VG      Fmt  Attr PSize  PFree
  /dev/sda2  centos  lvm2 a--  19.51g    0
  /dev/sdb1  usrgrp1vol lvm2 a--  10.00g    0
  /dev/sdc1  usrgrp1vol lvm2 a--   5.00g    0
```

7. Restart ISM-VA.

```
# ismadm power restart
```

4.7 Certificate Activation

4.7.1 Deploying SSL Server Certificates

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

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 any 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 Displaying SSL Server Certificates

You can have the SSL certificates displayed that are activated in ISM-VA.

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

2. Execute the command for showing the SSL server certificates.

   ```
   # ismadm sslcert show
   ```

4.7.3 Export SSL server certificates

You can export the SSL certificates that are activated in ISM-VA.

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

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 Activation

You can register, display, and delete server licenses and node licenses in ISM-VA.

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

2. Execute the command for activating 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. Log in to ISM-VA from the console as an administrator.

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>
   ```

   Note

   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 Registering Certificates for Event Notification Mails

1. Use FTP to transfer the certificates.

   Transfer destination: <User Group Name>/ftp/cert

   For information on how to transfer files via FTP, see "2.1.2 FTP Access."

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

3. Execute the command for registering certificates for event notification mails.

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

4.10.2 Registering Action Scripts

1. Use FTP to transfer the scripts.

   Transfer destination: <User Group Name>/ftp/actionscript

   For information on how to transfer files via FTP, see "2.1.2 FTP Access."

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

3. Execute the command for registering action scripts.

   ```
   # ismadm event import -type script
   ```

4.10.3 Displaying 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 Displaying Action Scripts

You can have the action scripts displayed that are registered in ISM-VA.

```
# ismadm event show -type script
```

4.10.5 Deleting 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 Deleting 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. Log in to ISM-VA from the console as an administrator.
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: Activate FTP server individually

   ```
   # ismadm service enable vsftpd
   ```

- Disable internal service individually

```
ismadm service disable <Service name>
```

Example of command execution: Deactivate FTP server individually

```
# ismadm service disable vsftpd
```

4.12 Displaying System Information

You can have the internal system information of ISM-VA displayed from the console.

1. Log in to ISM-VA from the console as an administrator.
2. Execute the command for displaying the system information.

```
# ismadm system show
ISM Version     : 2.0.0 (S20160901-01)
GUI Port Number : 25566
Hostname        : localhost
Log Level       : small
```

4.13 Modifying Host Names

You can modify the host name of ISM-VA.

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

2. Log in to ISM-VA from the console as an administrator.
3. In order to apply patches, stop the ISM service temporarily.

   Stop the ISM service according to the procedure described in "4.1.4 Starting and Stopping 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 Plugins Control

You can apply and delete plugins to/from ISM-VA, and display the plugins applied to ISM-VA.

4.15.1 Applying Plugins

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

3. In order to apply plugins, stop the ISM service temporarily.

   Stop the ISM service according to the procedure described in "4.1.4 Starting and Stopping ISM Service."

4. Execute the command for applying plugins.

   Execute the following command, specifying the plugin file.

```
# ismadm system plugin-add -file <Plugin file>
```

   Example of command execution:

```
# ismadm system plugin-add -file /Administrator/ftp/FJSVsvism-ext-1.0.0-10.tar.gz
```

5. After applying the plugin, restart ISM-VA.

```
# ismadm power restart
```

4.15.2 Displaying Plugins

Display of the applied plugin version

```
# ismadm system plugin-show
  FJSVsvism-ext 1.0.0
```

Command output

Displayed in the form of plugin name and version.

Example of command execution

```
# ismadm system plugin-show
  FJSVsvism-ext 1.0.0
```

Point

You can also display the information about plugins with use of the command "ismadm system show" from "4.12 Displaying System Information."

```
# ismadm system show
ISM Version    : 2.0.0.a (S20160908-01)
GUI Port Number    : 25566
Hostname    : localhost
Log Level    : small
Plugin        : FJSVsvism-ext 1.0.0
```

Command output

Plugin: Displaying the applied plugin name and its version

4.15.3 Deleting Plugins

Uninstallation of applied plugins

```
# ismadm system plugin-del -name <Plugin Name>
```

The plugin name is displayed with the command output in "4.15.2 Displaying Plugins."

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 screen for confirmation of plugin uninstallation is displayed. Enter [y] to confirm the uninstallation.

After plugin deletion, restart ISM-VA.

```
# ismadm power restart
```

4.16 Switching Trouble Investigation Logs

You can switch whether or not to output a log to be used when investigating troubles.

1. Log in to ISM-VA from the console as an administrator.
2. Execute the command for switching the log output for trouble investigation on and off.
   - Enable log output

     ```
     # ismadm system set-debug-flag 1
     ```

   - Disable log output

     ```
     # ismadm system set-debug-flag 0
     ```

4.17 Switching Levels of Trouble Investigation Logs

You can switch output levels for logs to be used when investigating troubles.

Switching the output level allows you to limit the sizes of logs to be issued.

Log level	Approximate size of log to be issued
small (default)	10 GB
medium	40 GB
large	100 GB

Note

- Switching is available only from a lower to a higher level.
- After switching the log level, ISM-VA must be rebooted.

1. Log in to ISM-VA from the console as an administrator.
2. Stop the ISM service.

   Stop the ISM service according to the procedure described in "4.1.4 Starting and Stopping 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     : 2.0.0
   GUI Port Number : 25566
   Hostname        : localhost
   Log Level       : medium
   ```

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 Setting of SNMP Community Name

You can change the name of SNMP communities.

1. Log in to ISM-VA from the Console as an administrator.
2. Execute the command for setting an SNMP community name.

   - Change SNMP community name:

     ```
     # ismadm snmp set -name {Community Name}
     ```

   - Show SNMP community name:

     ```
     # ismadm snmp show
     ```

4.19 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 "4.19.4 Switching DHCP servers."

If you use only the external DHCP server, the following settings are not required.

4.19.1 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 "4.19.2 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 mandatory. 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 dhcpsrv set -file <conf file>
```

Example of command execution

```
# ismadm dhcpsrv set -file /Administrator/ftp/dhcpd.conf.new
```

4.19.2 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 "4.19.1 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 "4.19.3 Confirming 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
```

4.19.3 Confirming DHCP server information inside ISM-VA

You can display DHCP server information inside ISM-VA.

You can do the following:

Display the contents of the currently-set DHCP server,

Display messages of the DHCP server,

Export the current set contents (conf file) to the location where ftp access is possible, and

Export a sample conf file to the location where ftp access is possible.

- Display of the contents of the currently set DHCP server

  ```
  # ismadm dhcpsrv show-conf
  ```

- Display of the DHCP server message

  ```
  # ismadm dhcpsrv show-msg [-line]
  ```

  20 lines are displayed when you execute it without option.

  You can specify the number of displayed lines by specifying the option [-line].

  Example of command execution

  ```
  # ismadm dhcpsrv show-msg -line 50
  ```

- Export of the current setting contents (conf file) to the location where ftp access is possible

  ```
  # ismadm dhcpsrv export-conf -dir /Administrator/ftp
  ```

- Export a sample setting content (conf file) to the location where ftp access is possible

  ```
  # ismadm dhcpsrv export-sample -dir /Administrator/ftp
  ```

4.19.4 Switching 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 dhcpsrv 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 dhcpsrv set-mode local
    ```

  - Setting up so that Profile is assigned with use of the outside DHCP server

    ```
    # ismadm dhcpsrv set-mode remote
    ```

4.20 MIB File Settings

You can import an MIB file(s) that allows you to receive any traps in ISM-VA.

4.20.1 Registering 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. Log in to ISM-VA from the console as an administrator.
3. Execute MIB file registration command.

```
# ismadm mib import
```

4.20.2 Displaying MIB Files

You can display the MIB file(s) registered on ISM-VA.

```
# ismadm mib show
```

4.20.3 Deleting MIB Files

You can delete the MIB file(s) registered on ISM-VA.

```
# ismadm mib delete -file <MIB file name>
```

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 deactivation of profiles
- Firmware updates
- Manual collection of node logs

Procedure for activating Maintenance Mode

1. Open the "Details of Node" screen.
2. Click the [Actions] button and select [Set into Maintenance Mode].

   When the screen for confirmation is displayed, confirm the node name and click [Yes].

Procedure for deactivating Maintenance Mode

1. Open the "Details of Node" screen.
2. Click the [Actions] button and select [Deactivate Maintenance Mode].

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 [Event/Task]-[Event]-[Operations log], you need to access and investigate the respective devices directly.

Appendix A Uninstalling ISM-VA

Uninstall ISM-VA according to the installation destination.

The following procedures describes 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
- Uninstalling from KVM

Uninstalling from Microsoft Windows Server Hyper-V

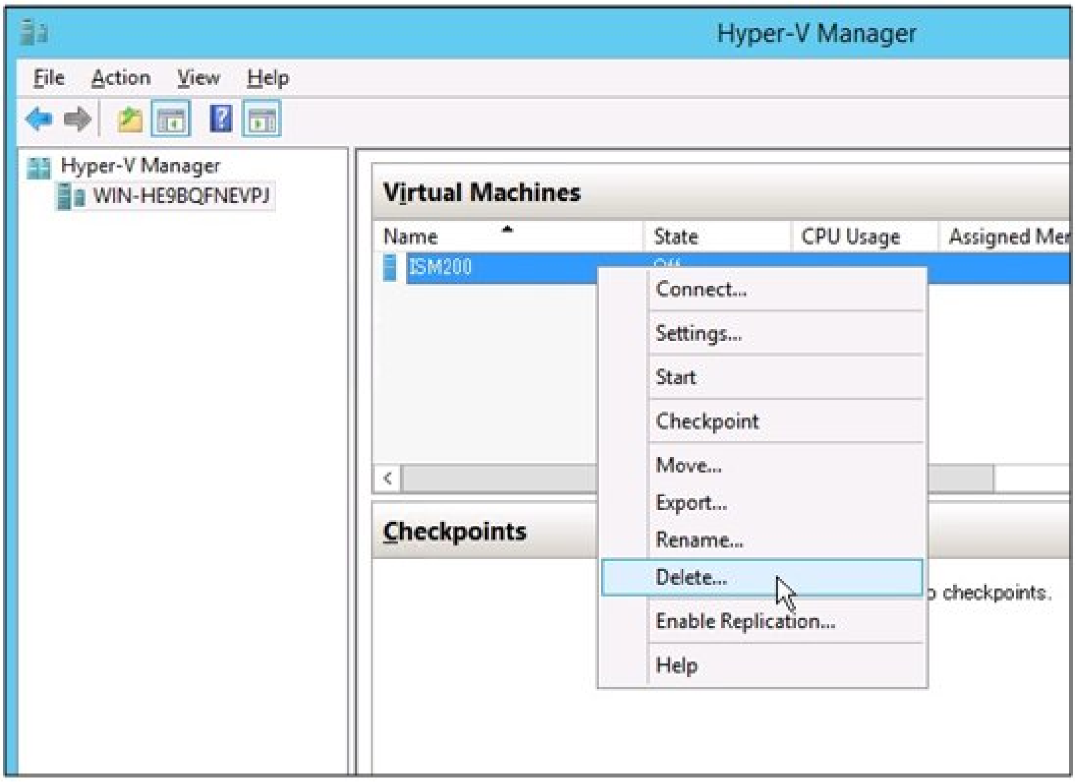
1. Stop ISM-VA

   See "4.1.2 Terminating 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].



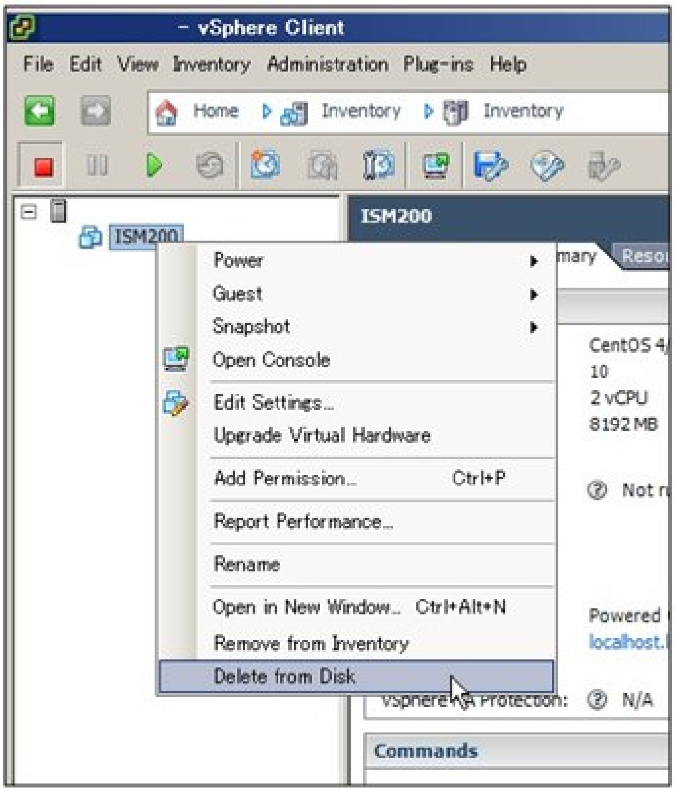
4. Use Explorer to remove the virtual hard disk for which you took the memo in Step 2.

Uninstalling from VMware vSphere Hypervisor

1. Stop ISM-VA

   See "4.1.2 Terminating ISM-VA" for details.

2. Start vSphere Client, right-click on the installed ISM-VA, and then select [Delete from Disk].

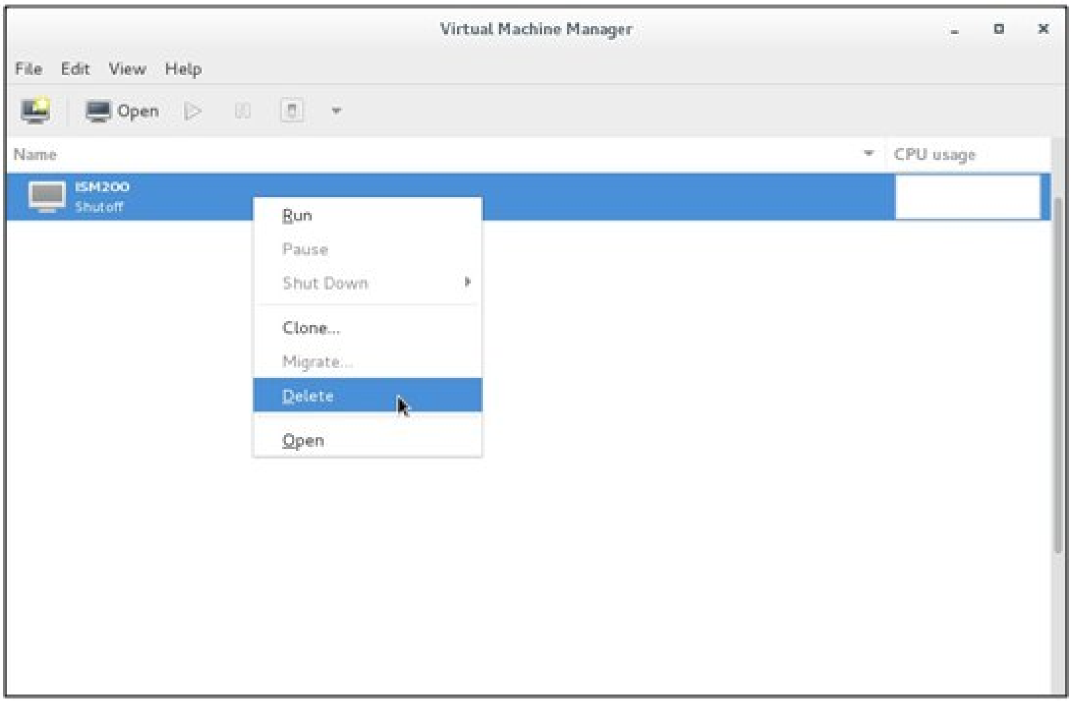


Uninstalling from KVM

1. Stop ISM-VA

   See "4.1.2 Terminating 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 detected node fails.

Causes and recovery methods

Confirm the serial number of the detected 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. Either of the following messages is displayed.

- [Settings] - [Profiles] - [Actions] - [Import] - [Select] button
- [Settings] - [Repositories] - [Firmware] - [Import Data List] - [Actions] - [Import DVD] - [Select] button
- [Settings] - [Repositories] - [Firmware] - [Import Data List] - [Actions] - [Import Firmware] - [Select] button
- [Settings] - [Repositories] - [OS / SVS] - [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.
- Confirm 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, click the [Custom level] button and change the setting for [Downloads] - [File download] to [Enable].

Symptom: Execution of ismadm commands around 2:20 a.m. on Tuesdays results in an error.

- Applicable commands:

  ismadm service disable

  ismadm service enable

  ismadm service restart

  ismadm service show

  ismadm service start

ismadm service status

ismadm service stop

ismadm time add-ntpserver

ismadm time del-ntpserver

- Displayed error messages

  Either of the following messages is displayed.

  Failed to list unit files: Message did not receive a reply (timeout by message bus)

  Failed to list unit files: Connection reset by peer

Causes and recovery methods

ISM-VA kernel commands are restarted at 2:20 a.m. on Tuesdays. Executing the following ismadm commands during the restart of the kernel commands may result in an error.

When such error occurs, re-execute the ismadm command.

Firmware Management

Symptom: The firmware to be updated cannot be specified when making operations for a firmware update.

Causes and recovery methods

- 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. Confirm 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. Confirm 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.
- There might be a problem in the environment settings for running PXE boot. Confirm the following.
    - Whether DHCP server is able to lease appropriate IP addresses
    - Whether the PXE function is disabled in the BIOS settings of the node
    - Whether the onboard LAN of the node is connected to ISM-VA, etc.

Profile Management

Symptom: An error occurs in assigning, reassigning, or deactivating 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 deactivating 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 implement 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 implement profile assignment. If no version number is specified for the ServerView Suite DVD to be used within the profile, the latest imported DVD will be 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, you first have 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 is a mistake(s) in the displayed contents.

Causes and recovery methods

To display the virtual connection relationships you need, beforehand, to register the Cloud Management Software that manages a managed node(s) on ISM to register the OS information of the managed node.

Confirm 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. Confirm 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. Confirm 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. Confirm 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. Confirm [Event/Task]-[Event], 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.
  - The predetermined capacity for an Archive log saving area was exceeded.
  - The predetermined capacity for a node log (download data) saving area was exceeded.
  - The predetermined capacity for node log (log search data) saving area was exceeded.

Symptom: Settings for node log collection log collection of a node cannot be made.

Causes and recovery methods

If the node status is "Exempt" confirm 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.node log collection.

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 Settings Items

C.1 BIOS/iRMC Settings 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.

For details of each item, see the manual for your server.

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 the higher the performance. The slower the	Low-Voltage optimized=The fastest setting available with low voltage

Item Name	Description	Parameter
(Low-Voltage optimized/Energy optimized/Performance optimized)	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 OpROM / Legacy OpROM)	This specifies the Option Rom booted with the devices other than a network, mass storage device and video.	UEFI OpROM=UEFI Option ROM only booted Legacy OpROM=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 booting/Stop booting)	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 (Return to the state before power disconnection/Do not power on/ 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	This sets up the power-saving and noise canceling operations for a server.	OS Controlled=Control by OS followed

Item Name	Description	Parameter
(Control by OS/Power-saving operation)	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 cconfirmations 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 done
		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 done
		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 management target server or to obtain it from an NTP server.	System RTC=Time of iRMC obtained from the system clock of a management target 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 PRIMERGY 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.	Enabled=SNMP enabled
		Disabled=SNMP disabled

Item Name	Description	Parameter
	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.	
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.	Enabled=SNMPv3 support enabled
		Disabled=SNMPv3 support disabled

Item Name	Description	Parameter
	Note - To create/change SNMPv3 users, you need to enable SNMP with the Network Settings -> SNMP. - To use SNMPv3, you need 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	This specifies users' access privilege. Note - To create/change SNMPv3 users, you need to enable SNMP with the Network Settings -> SNMP. - To use SNMPv3, you need 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)
	This selects the authentication protocol that SNMPv3 uses for authentication.
	Note
	- To create/change SNMPv3 users, you need to enable SNMP with the Network Settings -> SNMP.
	- To use SNMPv3, you need 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.
		SHA=SHA used
		MD5=MD5 used
		None=Authentication disabled

Item Name	Description	Parameter
	Disable the setting items if you fail to assign a profile.	

Privacy
(DES/AES/None)
	This specifies a privacy protocol that SNMPv3 uses for encrypting SNMPv3 traffic.
	Note
	- To create/change SNMPv3 users, you need to enable SNMP with the Network Settings -> SNMP.
	- To use SNMPv3, you need 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.
		DES=DES used
		AES=AES used
		None=Privacy disabled

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	Select the item from the pulldown menu. SNMPv1, SNMPv2c or SNMPv3

Item Name	Description	Parameter
	screen of iRMC. Disable the setting items if you fail to assign a profile.	

C.2 OS Settings items of profiles for PRIMERGY 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.2.1 Profiles for 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, you then need 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. [Note 1]	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]
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 Likewise, select the type of array controller, RAID level and the number of

Item Name	Description	Parameter
		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 Likewise, 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. [Note 3]
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 pulldown menu.
Region and Language	This specifies a region and language.	Select the item from the pulldown menu.
Keyboard	This specifies the language and type of keyboard.	Select the item from the pulldown menu.
System settings		
Display Resolution [px]	This specifies the display resolution immediately after OS installation.	Select the item from the pulldown menu. [Note 4] Example: 600x480, 800x600, 1024x768 or 1280x1024
Refresh Rate [Hz]	This specifies the display refresh rate immediately after OS installation.	Select the item from the pulldown menu. [Note 4]
# 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 pulldown menu. [Note 4]
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.	Click on Add button to set up any value. [Omittable]
SNMP Security Service	This specifies the name of an acceptable SNMP community and its privilege.	Click on Add button to set up any value. [Omittable]
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

Item Name	Description	Parameter
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.	(Accepting of SNMP Packets (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 Likewise, the host name(s) is (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.	Any service checked
Remote Desktop	This specifies whether or not 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 or not 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
Additional Application		
Java Runtime Environment	Specify whether or not 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		

Item Name	Description	Parameter
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 activated, 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.
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. [Note 2]
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.

Item Name	Description	Parameter
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.2.2 Profiles for VMware ESXi 5.5/VMware ESXi 6.0/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.
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. [Note 1]	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 Likewise, select the type of array controller, RAID level and the number of

Item Name	Description	Parameter
		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 Likewise, 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	VLAN ID is entered. "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 automatic registration. Likewise, specify "0" to VLAN ID on "OS" tab.	(Checked)=Register (Unchecked)=Do not register
Cloud Management Software Name to register host with	This specifies the vCenter of the registration destination.	Select from the registration destinations registered beforehand on [Settings] - [Basic Settings] - [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. [Note 4]	Specify the script executed after installation.

[Note1]: If the Universal Multi-Channel (UMC) function of the CNA card is activated, 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.	(Checked)=Agreement with VMware License

Item Name	Description	Parameter
	Make sure to check the box to show that you accept.	(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. You can select Checked/Unchecked when DHCP is disabled.	(Checked)=Obtained from DNS (Unchecked)=Any computer name specified
Computer Name	Any computer name (host name) is specified when you do not obtain a computer name (host name) from DNS.	Enter the host name.

C.2.3 Profiles for Red Hat Enterprise Linux

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. [Note 1]	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.

Item Name	Description	Parameter
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 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 Likewise, 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 Likewise, select the type of the drive that you use from the screen.
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 or not 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 expand 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 [Note2] Default package groups=Recommended packages [Note2]

Item Name	Description	Parameter
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 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 [Note2]
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. [Note 4]	(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. [Note5] [Note6]	Specify the script to be executed.

[Note1]: If the Universal Multi-Channel (UMC) function of the CNA card is activated, set the MAC address and not the port number.

[Note2]: When you use ServerView Suite DVD (V11.16.04 or later), some package groups are not installed. In such cases, manually install them.

[Note3]: "Shadow Passwords" is always enabled regardless of profile settings.

[Note4]: 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 Wizard	RHEL 6.8 (x86) /RHEL 6.7(x86) /RHEL 6.6(x86)	RHEL 6.8 (Intel64) /RHEL 6.7(Intel64) /RHEL 6.6(Intel64)	RHEL 7.3 /RHEL 7.2 /RHEL 7.1
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
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

[Note5]: When you execute a script from another script, assign execution privilege to invoke it.

[Note6]: This executes the specified script with 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	This specifies whether to use the computer name obtained from DNS.	(Checked)=Obtained from DNS (Unchecked)=Any computer name specified
Computer Name	Any computer name (host name) is specified when you do not obtain a host name from DNS.	Enter the host name.
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	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.2.4 Profiles for SUSE Linux Enterprise Server

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. [Note 1]	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 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 [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 Likewise, 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 Likewise, select the type of the drive that you use from the screen.
Partition	Specify the items below to each mount point, such as, /boot/var, shown on [Profile] screen.	

Item Name	Description	Parameter
(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 [Note 3]
Size	This specifies a partition size.	Enter a decimal value.
Fill to maximum allowable size	This specifies whether or not 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 expand 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 [Note4]	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)."
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	This specifies the application to be installed.	(Checked)=Application installed

Item Name	Description	Parameter
(a variety of applications)	The type of applications differs depending on distribution. [Note 5]	
Executing Script after Installation [Note6]		
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. [Note7] [Note8]	Specify the script to be executed.

[Note1]: If the Universal Multi-Channel (UMC) function of the CNA card is activated, 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]: 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.

[Note4]: 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.

[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 version upgrades of ServerView Suite DVD.

Y=Can be specified by ISM, N=Cannot be specified by ISM

Applications (For RHEL)	SLES 11 SP4(x86)	SLES 11 SP4(intel64)	SLES 12 /SLES 12 SP1
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

[Note6]: In SLES 12, this does not support the script execution after installation.

[Note7]: When you execute a script from another script, assign execution privilege to invoke it.

[Note8]: 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		

Item Name	Description	Parameter
Get Computer Name Via DNS Server	This specifies whether to use the computer name obtained from DNS.	(Checked)=Obtained from DNS (Unchecked)=Any computer name specified
Computer Name	Any computer name (host name) is specified when you do not obtain a host name from DNS.	Enter the host name.
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	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 Settings 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 pull down 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 pull down 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 pull down menu. The selectable type differs depending on the models of ETERNUS and selected disk inch. SAS, NL-SAS, SED or SSD

Item Name	Description	Parameter
Disk Size	This specifies the type of disk drive (disk size) built in a disk array.	Select the item from the pull down 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. Note You cannot specify the volume name already set up for a device.	Specify the name of a volume to be created on the RAID group. You can enter 1 to 16 characters.
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 pull down 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 pull down 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 pull down 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 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.

Item Name	Description	Parameter
		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.
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 pull down 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.
Detail Settings		
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.

Item Name	Description	Parameter
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 location of a mounted slot on the disk drive used for the array configuration.
- You cannot specify the location of a mounted slot on the disk drive used for the hot spare configuration.

C.4 Settings 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.4.1 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 Likewise, enter the agent address in IPv4 format.
SNMP Engine ID	This specifies whether to enable an SNMP engine ID.	(Checked)=SNMP engine ID enabled Likewise, 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 pull down menu. Off, v1 or v2c

Item Name	Description	Parameter
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.
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 pull down 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 pull down 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 Likewise, specify the item from the pull down menu. none: Read not permitted all: Read permitted
Write	This specifies whether to enable SNMP MIB write.	(Checked)=Enabled Likewise, specify the item from the pull down menu. none: Write not permitted all: Write permitted
Notify	This specifies whether to enable SNMP MIB trap notify.	(Checked)=Enabled Likewise, specify the item from the pull down menu.

Item Name	Description	Parameter
		none: Read-out not permitted all: Read-out permitted

Authentication tab

Item Name	Description	Parameter
Account		
Change Administrator Password	This specifies whether to change an 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	This specifies whether to enable auto time adjustment.	(Checked)=Enabled
Server Setting	This specifies whether to enable the settings for a time-provider server.	(Checked)=Enabled (Unchecked)=Disabled

Protocol
(Time/SNTP)
	This specifies the protocol to be used.	Time=TCP used
		SNTP=UDP used

Address	This specifies the IP address of a time-provider server.	Enter the IP address of the time-provider server.
Interval Setting	This specifies whether to enable the interval for auto time adjustment.	(Checked)=Enabled (Unchecked)=Disabled
Interval Setting (On Startup/Period)	This specifies the interval of auto time adjustment.	On Startup=Adjusted upon startup Period=Adjusted at any period Likewise, enter the period on the screen.
Set time zone	This specifies whether to enable time zone setting.	(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 Likewise, select the item from the pulldown menu.

C.4.2 Profiles for VDXs

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

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 pull down menu. v1, v2c or v3
v3 Security Level	This specifies the security level for SNMPv3.	Select the item from the pull down menu. auth, noauth or priv
Read	This specifies whether to enable SNMP MIB read.	(Checked)=Enabled Likewise, specify the item from the pull down menu. none: Read not permitted all: Read permitted
Write	This specifies whether to enable SNMP MIB write.	(Checked)=Enabled Likewise, specify the item from the pull down menu. none: Write not permitted all: Write permitted
Notify	This specifies whether to enable SNMP MIB trap notify.	(Checked)=Enabled Likewise, specify the item from the pull down 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 Likewise, select a group from the pulldown menu.
Write	This specifies whether to enable SNMP community write.	(Checked)=Enabled Likewise, 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.

Item Name	Description	Parameter
Trap Version	This specifies the SNMP trap version.	Select the item from the pull down 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.
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 pull down 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 pull down 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 an administrator password.	(Checked)=Administrator password changed

Item Name			Description	Parameter
		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
		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).