FUJITSU Software
ServerView Infrastructure Manager V2.1

Operating Procedures

Preface

Purpose

This manual describes overviews of the initial settings and the operating procedures or using FUJITSU Software ServerView Infrastructure Manager (hereafter referred to as ISM). ISM is software for simpler and more efficient operation and management of a multitude of ICT devices that are running in datacenters and server rooms.

Related Manuals

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

Together with the manuals mentioned above, you can also refer to the latest information about ISM by contacting Fujitsu customer service partner.

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

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

http://manuals.ts.fujitsu.com

Intended Readers

This manual is intended for readers who consider using the product for comprehensive management and operation of such ICT equipment and possess basic knowledge about hardware, operating systems, and software.

Notation in this Manual

Notation

Keyboard

Keystrokes that represent nonprintable characters are displayed as key icons such as [Enter] or [F1]. For example, [Enter] means press 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

This document may use the following abbreviations.

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 Standard	Windows Server 2012 R2 Standard	
Microsoft(R) Windows Server(R) 2012 R2 Essentials	Windows Server 2012 R2 Essentials	
Microsoft(R) Windows Server(R) 2012 Datacenter	Windows Server 2012 Datacenter	Windows Server 2012
Microsoft(R) Windows Server(R) 2012 Standard	Windows Server 2012 Standard	
Microsoft(R) Windows Server(R) 2012 Essentials	Windows Server 2012 Essentials	
Microsoft(R) Windows Server(R) 2008 R2 Datacenter	Windows Server 2008 R2 Datacenter	Windows Server 2008 R2
Microsoft(R) Windows Server(R) 2008 R2 Enterprise	Windows Server 2008 R2 Enterprise	
Microsoft(R) Windows Server(R) 2008 R2 Standard	Windows Server 2008 R2 Standard	
Red Hat Enterprise Linux 7.3 (for Intel64)	RHEL 7.3	Red Hat Enterprise Linux or Linux
Red Hat Enterprise Linux 7.2 (for Intel64)	RHEL 7.2	
Red Hat Enterprise Linux 7.1 (for Intel64)	RHEL 7.1	
Red Hat Enterprise Linux 6.9 (for Intel64)	RHEL 6.9(Intel64)	
Red Hat Enterprise Linux 6.9 (for x86)	RHEL 6.9(x86)	
Red Hat Enterprise Linux 6.8 (for Intel64)	RHEL 6.8(Intel64)	
Red Hat Enterprise Linux 6.8 (for x86)	RHEL 6.8(x86)	
Red Hat Enterprise Linux 6.7 (for Intel64)	RHEL 6.7(Intel64)	
Red Hat Enterprise Linux 6.7 (for x86)	RHEL 6.7(x86)	
Red Hat Enterprise Linux 6.6 (for Intel64)	RHEL 6.6(Intel64)	

Official name	Abbreviation	
Red Hat Enterprise Linux 6.6 (for x86)	RHEL 6.6(x86)	SUSE Linux Enterprise Server or Linux
SUSE Linux Enterprise Server 12 SP2 (for AMD64 & Intel64)	SUSE 12 SP2(AMD64) SUSE 12 SP2(Intel64) or SLES 12 SP2(AMD64) SLES 12 SP2(Intel64)	
SUSE Linux Enterprise Server 12 SP1 (for AMD64 & Intel64)	SUSE 12 SP1(AMD64) SUSE 12 SP1(Intel64) or SLES 12 SP1(AMD64) SLES 12 SP1(Intel64)	
SUSE Linux Enterprise Server 12 (for AMD64 & Intel64)	SUSE 12(AMD64) SUSE 12(Intel64) or SLES 12(AMD64) SLES 12(Intel64)	
SUSE Linux Enterprise Server 11 SP4 (for AMD64 & Intel64)	SUSE 11 SP4(AMD64) SUSE 11 SP4(Intel64) or SLES 11 SP4(AMD64) SLES 11 SP4(Intel64)	
SUSE Linux Enterprise Server 11 SP4 (for x86)	SUSE 11 SP4(x86) or SLES 11 SP4(x86)	
VMware(R) vSphere(TM) ESXi 6.5	VMware ESXi 6.5	VMware ESXi
VMware(R) vSphere(TM) ESXi 6.0	VMware ESXi 6.0	
VMware(R) vSphere(TM) ESXi 5.5	VMware ESXi 5.5	

Terms

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

High Risk Activity

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

To Use This Product Safely

This document contains important information required for using this product safely and correctly. Read this manual carefully before using the product. In addition, to use the product safely, the customer 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

Modification History

Edition	Publication Date	Section		Modification Overview
01	July 2017	-		First edition
02	August 2017	Preface	Abbreviation	Added the abbreviation of OS
		2.5.1 Discover Nodes in the Network and Register Nodes	-	Added the node types in the node discovery
		2.5.2 Register a Node Directly	-	Added and modified the target models in the node registration
		2.6 Set up Network Connection	-	Replaced the image
		3.2 Check the Status of a Node	-	Replaced the image
		3.3 Display the Node Notification Information	-	Replaced the image
		4.3 Check the Error Point on the Network and its Affected Area	-	Replaced the image
		4.9.1 Link with the ISM Dashboard	-	Replaced the image

Contents

Chapter 1 Shared Operations

1.1 Display the Help Screen

A help screen has been prepared to describe detailed descriptions for each screen in ISM2.1. Refer to the help screen for descriptions for the content displayed.

In addition, there are two ways to display the help screen. Select an appropriate procedure to display the operating screen.

- Select the [⑦Help] - [Help] - [Help for this screen] in upper right side on each screen while it is displayed.

- Select the [⑦] in the upper right side on the wizard screen.

1.2 Refresh the Screen

Except for some screens, ISM acquires information when screens are displayed. The information in each screen will not be automatically refreshed while the screen is displayed. When you want to display the most recent information, execute the screen refresh procedure to refresh the screen.

When you select the refresh button (⟳Refresh), the information will be acquired again and the screen will be refreshed.

Chapter 2 Pre-Configurations

ISM manages four in layers: datacenter, floor, rack, and node. The meaning of each is as follows.

- Datacenter

  Datacenter corresponds to the building layer. This layer supposes a datacenter model with multiple floors.

- Floor

  This layer supposes a floor space where multiple racks are placed.

  The floor view can be displayed on the dashboard.

  Also, 3D view displays 3D graphics of the floor units.

- Rack

  This layer supposes a server rack with multiple management target devices (nodes) mounted.

- Node

  Management Target Devices.

Registration within each layer is executed using the following procedure.

1. Registration of datacenters

2. Floor registration (Registration of which data center that the floor is situated in)

3. Rack registration (Registration of which floor the rack is situated in)

4. Locating the rack on the floor (Registration of the rack's location on the floor)

5. Node registration (Registration of a node in a rack)

2.1 Register a Datacenter

Register the "Datacenter" layer showing the facility housing the datacenter.

1. From the Global Navigation Menu, select [Management] - [Datacenters] to display the [Datacenter List] screen.

2. Select the ![+] button to display the [Register Datacenter/ Floor/ Rack] wizard.

3. In [Object of Registration], select [Datacenter].

4. Enter the setting items, and then select the [Register] button. Refer to the help screen for descriptions on the setting items.

   How to display the help screen: Select the [⑦] in the upper right side on the wizard screen.

This finishes the datacenter registration. After datacenter registration is finished, the corresponding datacenter will be displayed on the [Datacenter List] screen.

2.2 Register a Floor

Register the "Floor" layer that signifies the machine room in the datacenter facility.

1. On the [Datacenter List] screen, select the ![+] button to display the [Register Datacenter/ Floor/ Rack] wizard.

2. In [Object of Registration], select [Floor].

3. Enter the setting items, and then select the [Register] button. For the [Datacenter] settings item, specify the datacenter registered in "2.1 Register a Datacenter." Refer to the help screen regarding other setting items.

   How to display the help screen: Select the [⑦] in the upper right side on the wizard screen.

This finishes the floor registration. After floor registration is finished, the corresponding floor is displayed on the [Datacenter List] screen.

2.3 Register a Rack

Register the "Rack" layer that signifies the server racks on the floor.

1. On the [Datacenter List] screen, select the [+] button to display the [Register Datacenter/ Floor/ Rack] wizard.

2. In [Object of Registration], select [Rack].

3. Enter the setting items, and then select the [Register] button. For setting items [Datacenter] and [Floor], select the datacenter and floor registered in "2.1 Register a Datacenter" and "2.2 Register a Floor" respectively. Refer to the help screen regarding other setting items.

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

This finishes the rack registration. After rack registration is finished, the rack will be displayed on the [Datacenter List] screen.

2.4 Locate a Rack on the Floor

Locate a rack on the floor.

1. On the [Datacenter List] screen, select the floor where the rack should be located to display the [Details of Floor] screen.

2. From the [Actions] button, select [Set Rack Position] to display the [Set Rack Position] wizard.

3. Select the [Add] button to display the [Add Unlocated Rack] wizard.

4. Select the rack to be added and select the [Add] button.

    Set the position of the rack and select the [Apply] button. Refer to the help screen for information on how to set the rack position.

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

This finishes the locating of the rack. After locating of the rack is finished, the rack will be displayed on the [Details of Floor] screen.

2.5 Register a Node

Node registration can be executed either by discovering and registering existing nodes in the network, or by directly entering the node information.

When the information registered in ISM and the information registered in the node does not match, the functionality of the ISM might be limited.

2.5.1 Discover Nodes in the Network and Register Nodes

1. From the Global Navigation Menu, select [Structuring] - [Node Registration] to display the [Node Registration] screen.

2. From the [Actions] button, select [Discovery] to display the [Discovery] wizard.

3. Enter the setting items and select the [Execute] button.

Table 2.1 Discovery

Setting items	Setting contents
Discovery IP Address range	Set the search range by specifying the IP address range.

Node Type	Select from the following items.
	
	 - Server(iRMC/BMC)
	
	  Select when you want to discover the server or PRIMEQUEST 3800B.
	
	 - PRIMEQUEST2000 (MMB+SSH+SNMP)
	
	  Select when you want to discover PRIMEQUEST 2000 series.

Setting items	Setting contents
	- Switch, Storage, PRIMERGY BX Chassis (SSH+SNMP)
	Select when you want to discover storage, network switch, or PRIMERGY BX chassis.
	- Facility (SNMP)
	Select when you want to discover RackCDU, PDU, or UPS.

Set the required item for each node type.

Table 2.2 When selecting Server (iRMC/BMC) in [Node Type]

Setting items	Description
User Name	iRMC/BMC User Name
Password	iRMC/BMC Password
Port Number	iRMC/BMC Port Number (Default: 623)

Table 2.3 When selecting PRIMEQUEST2000 (MMB+SSH+SNMP) in [Node Type]

Setting items		Description
MMB		-
	User Name	MMB User Name
	Password	MMB Password
	Port Number	MMB Port Number (Default: 623)
SSH		-
	User Name	SSH User Name
	Password	SSH Password
	Port Number	SSH Port Number (Default: 22)
SNMP		-
	Version	Select SNMP Version
	Port Number	SNMP Port Number (Default: 161)
	Community	SNMP Community Name

Table 2.4 When selecting Switch, Storage, PRIMERGY BX Chassis (SSH+SNMP) in [Node Type]

Setting items		Description
SSH		-
	User Name	SSH User Name
	Password	SSH Password
	Port Number	SSH Port Number (Default: 22)
SNMP		-
	Version	Select SNMP Version
	Port Number	SNMP Port Number (Default: 161)
	Community	SNMP Community Name

Table 2.5 When selecting Facility (SNMP) in [Node Type]

Setting items	Description
Version	Select SNMP Version

Setting items	Description
Port Number	SNMP Port Number (Default: 161)
Community	SNMP Community Name

4. When a node is discovered, it will be output on the [Discovered Node List] screen.

   When the automatic refresh setting is disabled, the discovery status is not refreshed.
   Specify the refresh period in the automatic refresh settings or select the refresh button to refresh the screen.

5. When the status on the [Discovery Progress] screen is shown as [Complete], select the [Discovered Node List] tab.

6. Select the checkbox of the node to be registered.

7. On the [Discovered Node List] screen, select [Registration discovered nodes] to display the [Node Registration] wizard.

8. Follow the instructions in the [Node Registration] wizard and input the setting items. Refer to the help screen for descriptions on the setting items.

   How to display the help screen: Select the [⑦] in the upper right side on the wizard screen.

Table 2.6 Node information

Setting items	Setting contents

Node Name	Enter the node name. The following one-byte characters cannot be used.
	
	/\:*?"<>|
	
	xxxx_yyyy is already entered as node name by default.
	The character strings displayed in xxxx, yyyy are as follows.
	
	- xxxx
	
	   The following character strings are displayed according to node type.
	
	   In case of server: SV
	
	   In case of switch: SW
	
	   In case of storage: ST
	
	   In case of facility: CDU or PDU or UPS
	
	- yyyy
	
	   They are serial numbers for the node. When the serial numbers are not discovered, IP addresses are displayed.

Chassis Name	Enter the chassis name when PRIMERGY CX is discovered. When nodes mounted on the same chassis are discovered, enter the chassis name of the node mounted on smallest number of the slots. In a case of the other nodes on the same chassis, the chassis names are automatically entered. The following one-byte characters cannot be used. /\:*?"<>| SV_zzzz is entered in the chassis name by default. The serial numbers of the chassis are displayed in zzzz. When the serial numbers are not collected in discovery, IP addresses are displayed.
Web i/f URL	Enter the URL when you access Web i/f on the node.
Description	Enter the descriptions.

Refer to the Help screen for the descriptions of the discovered node list items.

How to display the help screen: Select the [⑦ Help] - [Help] - [Help for this screen] in upper right side on the screen while it is displayed.

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

    This finishes the node registration.

    After node registration is finished, the corresponding node will be displayed on the [Node List] screen.

    When an OS is installed on the target node, execute the following procedures.

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

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

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

Table 2.7 Edit OS Information

Setting items	Setting contents
OS Type	Select OS type.
OS version	Select the OS version.
OS IP address	After setting the IP version, enter the IP address of the OS management port (IPv4/IPv6 are supported).
Domain Name	Enter domain name in FQDN format.
Account	Enter the administrator account.
Password	Enter the password of the administrator account.
OS Connection Port Number	Enter the port number for connecting to the OS. When using Windows it is the port number of the WinRM service (default setting is 5986), when using Linux it is the port number of the SSH service (default setting is 22). When not entered, the default port number will be set.

12. After entering the OS information, select [Apply].

This finishes OS information editing. After OS information editing is finished, the OS information on the corresponding node can be acquired.

2.5.2 Register a Node Directly

1. From the Global Navigation Menu, select [Structuring] - [Node Registration] to display the [Node Registration] screen.

2. From the [Actions] button, select [Registration] and the [Node Manual Registration] wizard is displayed.

3. Follow the instructions in the [Node Manual Registration] wizard and input the setting items. Refer to the help screen for descriptions on the setting items.

    How to display the help screen: Select the [⑦] in the upper right side on the wizard screen.

4. Below is the description for the [Account] setting items in [1. Node Information] in the [Node Manual Registration] wizard.

Table 2.8 When "server" was selected in [Node Type] and PRIMERGY RX series, PRIMERGY CX series, PRIMERGY BX series (other than PRIMERGY BX900 S2), PRIMEQUEST 3800B, IPCOM VX2 series, or Generic Server (IPMI) was selected in [Model Name]

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

Table 2.9 When "server" was selected in [Node Type] and PRIMEQUEST 2000 series was selected in [Model Name]

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

Table 2.10 When "server" was selected in [Node Type] and PRIMERGY BX900 S2 was selected in [Model Name]

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

Table 2.11 When "switch" or "storage" was selected in [Node Type]

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

Table 2.12 When "facility" was selected in [Node Type]

Setting items		Description
SNMP		When not accessing the node through SNMP, uncheck the checkbox (Default: Checked).
	Version	SNMP Version

Setting items		Description
	Port Number	SNMP Port Number (Default: 161)
	Community	SNMP community name of facility

Table 2.13 When "other" was selected in [Node Type]

Setting items		Description
iRMC/BMC		When accessing the node through iRMC/BMC, check the checkbox (Default: Unchecked).
	User Name	User Name of iRMC/BMC
	Password	User Password of iRMC/BMC
	Port Number	iRMC/BMC Port Number (Default: 623)
SSH		When accessing the node through SSH, check the checkbox (Default: Unchecked).
	User Name	Node User Name
	Password	Password of Node User
	Port Number	SSH Port Number (Default: 22)
SNMP		When accessing the node through SNMP, check the checkbox (Default: Unchecked).
	Version	SNMP Version
	Port Number	SNMP Port Number (Default: 161)
	Community	SNMP community name of the node

From the Global Navigation Menu, select [Management] - [Nodes] to display the [Node List] screen.

It may take time to display the node list depending on the number of nodes registered in ISM.

This finishes the node registration.

After node registration is finished, the corresponding node will be displayed on the [Node List] screen.

When an OS is installed on the target node, execute the following procedures.

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

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

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

Table 2.14 Edit OS Information

| Setting items	Setting contents
OS Type	Select OS type.
OS version	Select the OS version.
OS IP address	After setting the IP version, enter the IP address of the OS management port (IPv4/IPv6 are supported).
Domain Name	Enter domain name in FQDN format.
Account	Enter the administrator account.
Password	Enter the password of the administrator account.
OS Connection Port Number	Enter the port number for connecting to the OS. When using Windows it is the port number of the WinRM service (default setting is 5986), when using Linux it is the port number of the SSH service (default setting is 22). When not entered, the default port number will be set.

7. After entering the OS account information has been finished, select apply.

This finishes the node registration. After node registration is finished, the corresponding node will be displayed on the [Node List] screen.

2.6 Set up Network Connection

The Network Map displays the physical connections of LAN cables among the managed nodes. In the case of LLDP (Link Layer Discovery Protocol) of the network port on the managed node is enabled, ISM retrieves the connection relation among the nodes and displays the connections on the Network Map. However, when the managed node does not support LLDP or is not enabled, the connections are not displayed automatically. In that case, you can manually set up connections between respective nodes.

1. From the Global Navigation Menu, select [Management] - [Network Map] to display the [Network Map Display] screen.
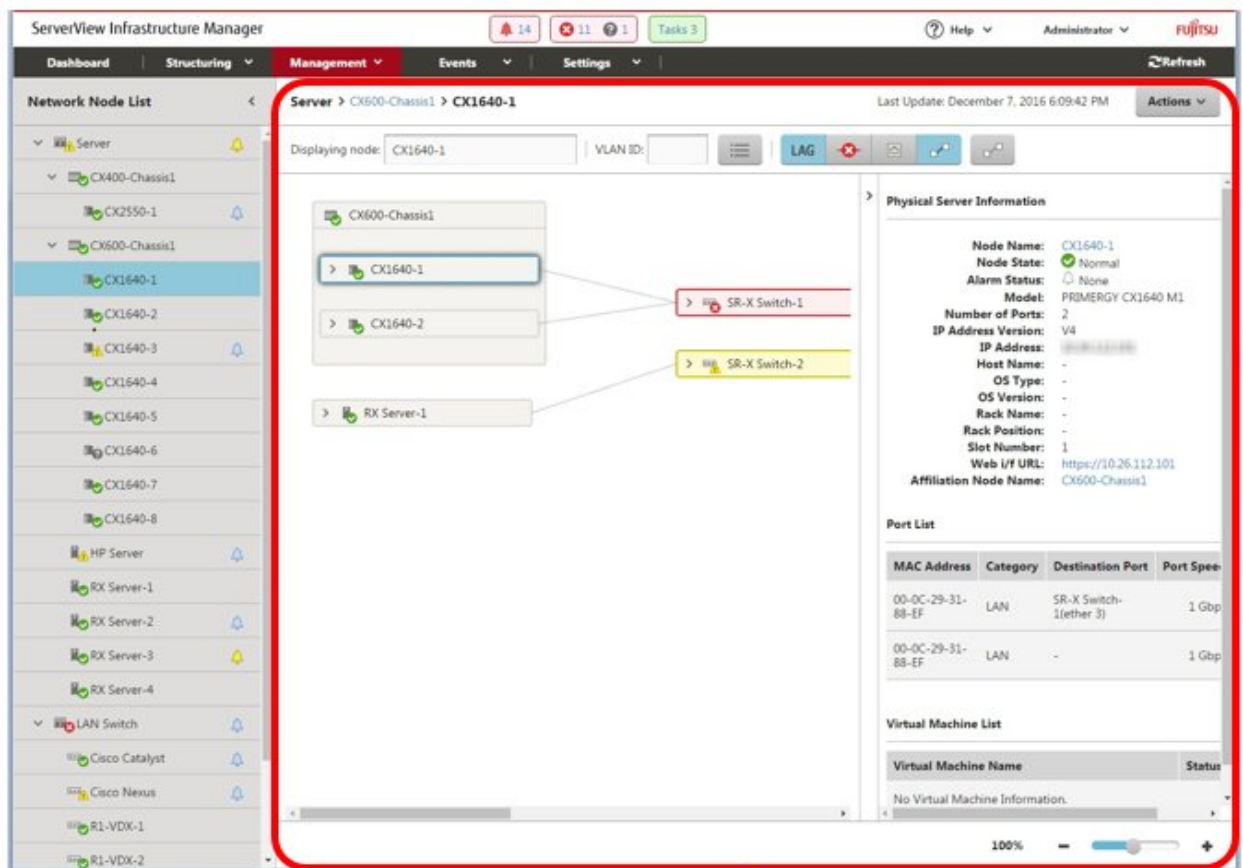
[Network Map Display] Screen

2. From the [Actions] button, select [Refresh network information] and select [Yes] to execute.

3. From the [Actions] button, select [Edit Connection].

4. Select the ▶ mark within the icon of the node to be connected to display the network port (▇).

5. Select the 2 ports to be connected. Select the [Add] button and the additional connections are displayed in green.

6. Repeat the procedure 3 to 5 as many times as the number of the connections you wish to add.

7. On the [Network Map Display] screen, select the [Save] button.

8. On the [Edit Connections Saved] screen, confirm the contents of the connections set up, then select the [Save] button and the additional connections are displayed in gray.

This finishes the procedure of network connection set up.

2.7 Set an Alarm

Set up of the external notifications for ISM, based on the alarm discovered when a node error occurred, (such as the various traps received from a node, or events discovered by monitoring function of ISM).

The followings are the notification methods.

- Execute an arbitrary script

- Send an e-mail

- Transfer the received trap to an external SNMP manager, or transfer an event discovered inside ISM as SNMP trap to an external SNMP manager

When sending e-mails, it is possible to encrypt the message with S/MIME.

When making the alarm settings, it should be assigned in the order of Action settings (notification method) - Alarm settings.

Point

Refer to the help screen for description on other setting items on each screen.

How to display the help screen: Select the [⑦] in the upper right side on the wizard screen.

1. Preparations are required before Action settings (notification method).

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

   [When executing scripts]

   a. Prepare script file.

   b. FTP is used to send it to ISM-VA. Access the ftp://<ISM-VA IP Address>/<User Group Name>/ftp/actionscript over FTP and store script files there.

   c. Log in to the ISM-VA console as the administrator user.

   d. Execute the ismadm event import -type script command.

      When executing the command, the script files stored in the FTP by each user will be imported in a batch.

   [When sending e-mails]

   a. On the [Alarms] screen, select [SMTP Server] to display the [SMTP Server settings] screen.

   b. From the [Actions] button, select [Edit] to display the [SMTP Server Settings] wizard.

   c. Enter the setting items, then select the [Apply] button.

      When sending an encrypted e-mail, execute the following settings as well.

   d. Prepare personal certificate.

      Confirm that the certificate is in PEM format and that the certification and recipient mail address is encrypted.

   e. FTP is used to send it to ISM-VA. Access the ftp://<ISM-VA IP Address>/<User Group Name>/ftp/cert using FTP and store the certificate there.

   f. Log in to the ISM-VA console as the administrator user.

   g. Execute the ismadm event import -type cert command.

      When executing the command, the certificates stored in the FTP by each user will be imported in a batch.

   [When transferring traps]

   a. On the [Alarms] screen, select [SNMP Manager] to display the [SNMP Manager Settings] screen.

   b. From the [Actions] button, select [Add] to display the [Add SNMP Manager] screen.

c. Enter the setting items, then select the [Apply] button.

2. From the Global Navigation Menu, select the [Evens] - [Alarms] to display the [Alarm Settings] screen.

3. Select [Actions] to display the [Action List] screen.

4. From the [Actions] button, select [Add] to display the [Add Action] wizard.

5. Enter the setting items, then select the [Apply] button.

6. After action addition is finished, the corresponding action will be displayed on the [Actions List] screen.

7. On the [Alarms] screen, select [Shared Alarm Settings] to display the [Shared Alarm Settings] screen.

8. From the [Actions] button, select [Edit] to display the [Edit Shared Alarm Settings] wizard.

9. Enter the setting items, then select the [Apply] button.

10. On the [Alarms] screen, select [Alarms] to display the [Alarm List] screen.

11. From the [Actions] button, select [Add] to display the [Add Alarm] wizard.

12. Follow the instructions on the [Add Alarm] wizard and enter the setting items.

13. After alarm addition is finished, the alarm will be displayed on the [Alarm List] screen.

This finishes the setup of node error notifications.

2.8 Make the Settings for Receiving SNMP Traps

2.8.1 Change in SNMP Settings

Make the settings for receiving SNMP traps. The default receiving settings are set as follows. Change the settings as required.

- SNMP version: SNMPv1/v2c

- Community: public

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

2. From the menu on the left side on the screen, select [Trap Reception] to display the [Trap Reception Setting List] screen.

3. From the [Actions] button on the right side on the screen, select [Add] to add the trap reception settings.

2.8.2 Add MIB File

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

1. Prepare MIB files. Note that when the MIB file has any dependency relationship, all the target files are required.

2. FTP is used to send it to ISM-VA. Access ftp://<IP address of ISM-VA>/Administrator/ftp/mibs via FTP, and store all the MIB files.

3. Log in to the ISM-VA console as the administrator user.

4. Execute the ismadm mib import command. Executing the command causes all the MIB files stored in FTP to be imported in batch.

2.9 Set a Log Collection Schedule

ISM follows the schedule set (example: every day at 23:00) and collects and accumulates node logs on a regular basis. It is possible to have different settings for each node. The set schedule can be executed and log collection executed at an arbitrary time.

1. From the Global Navigation Menu, select [Management] - [Nodes] to display the [Node List] screen.

   It may take time to display the node list depending on the number of nodes registered in ISM.

2. Select the node to be configured from the node list.

3. Select the [Log Settings] tab.

4. Execute [Edit Log Collection Settings] from the [Log Setting Actions] button in the [Log Settings] tab.

5. Enter the required settings on the settings screen, then select [Apply].

   - After selecting [Schedule Type], select the [Add] button and set the log collection time.

   - Check the [Enable Schedule execution] box. When the check is disabled, the created schedule will not be executed.

   - When the node is a server, [Operating System Log] and [ServerView Suite Log] can be selected as targets for log collection when the OS information is set correctly.

     However, [Hardware Log], [ServerView Suite Log] cannot be selected depending on the server type. In this case, log cannot be collected.

   Using the operations above, the log of the specified node will automatically be collected at the set time and accumulated in ISM.

6. When the log collection is executed according to the arbitrary timing in the settings, selecting the [Log Setting Action] button in the [Log Settings] tab and selecting [Collect Logs] executes the log collection. The [Collect Logs] operation will be registered as an ISM task. Select [Tasks] on the top of the Global Navigation Menu to confirm that the task has been completed.

2.10 Delete a Node

Delete a registered node.

1. From the Global Navigation Menu, select [Management] to display the [Node List] screen.

   It may take time to display the node list depending on the number of nodes registered in ISM.

2. Select the node to be deleted.

3. From the [Actions] button, select [Delete Node].

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

5. After node deletion is finished, the corresponding node will be deleted from the [Node List] screen.

This finishes node deletion.

2.11 Delete a Rack

Delete a registered rack.

1. From the Global Navigation Menu, select [Datacenters] to display the [Datacenter List] screen.

2. Select the rack to be deleted.

3. From the [Actions] button, select [Delete Rack] to start the Delete Rack wizard.

   Refer to the help screen regarding things to be careful about when deleting a rack.

   How to display the help screen: Select the [⑦] in the upper right side on the wizard screen.

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

2.12 Delete a Floor

Delete a registered floor.

1. On [Datacenter List] screen, select the floor to be deleted.

2. From the [Actions] button, select [Delete Floor] to start the Delete Floor wizard.

   Refer to the help screen regarding things to be careful about when deleting a floor.

   How to display the help screen: Select the [⑦] in the upper right side on the wizard screen.

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

2.13 Delete a Datacenter

Delete a registered datacenter.

1. On [Datacenter List] screen, select the datacenter to be deleted.

2. From the [Actions] button, select [Delete Datacenter] to start the Delete Datacenter wizard.

   Refer to the help screen regarding things to be careful about when deleting a datacenter.

   How to display the help screen: Select the [⑦] in the upper right side on the wizard screen.

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

Chapter 3 Node Monitoring

3.1 Operate the Dashboard

The dashboard displays the widget showing various information about status, logs etc. Select the widget according to the needs of the user. The information required can be referenced.
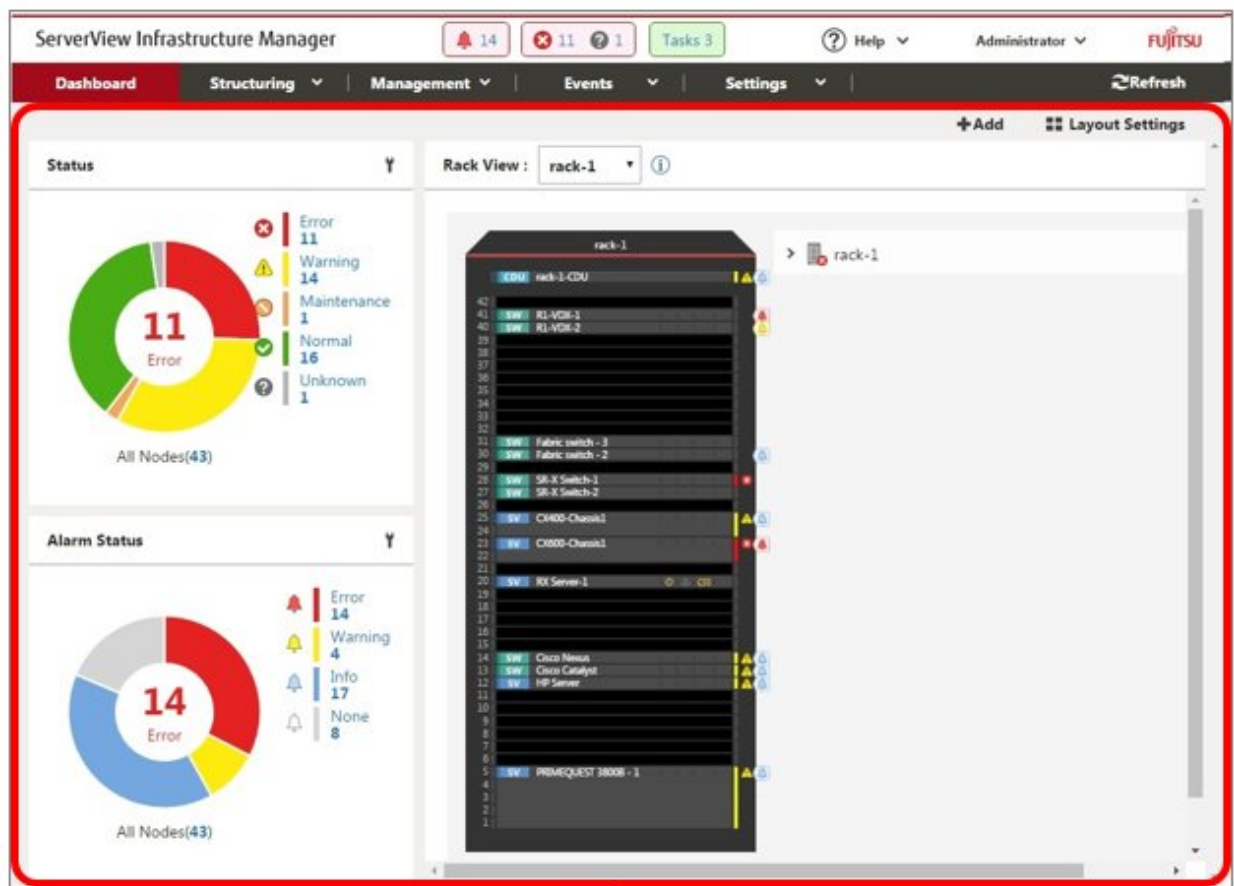
Refer to the help screen for how to select the widget to be shown on the dashboard.

How to display the help screen: Select the [⑦ Help] - [Help] - [Help for this screen] in upper right side on the screen while it is displayed.

3.2 Check the Status of a Node

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

1. Check the node status using the [Status] widget on the dashboard.

[Dashboard] screen

2. Refer to the help screen for detailed descriptions regarding the [Status] widget.

   How to display the help screen: Select the [⑦ Help] - [Help] - [Help for this screen] in upper right side on the screen while it is displayed.

3. In the [Status] widget, select the status to check (Error, Warning, Maintenance, Normal, and Unknown) to display the [Node List] screen.

   It may take time to display the node list depending on the number of nodes registered in ISM.

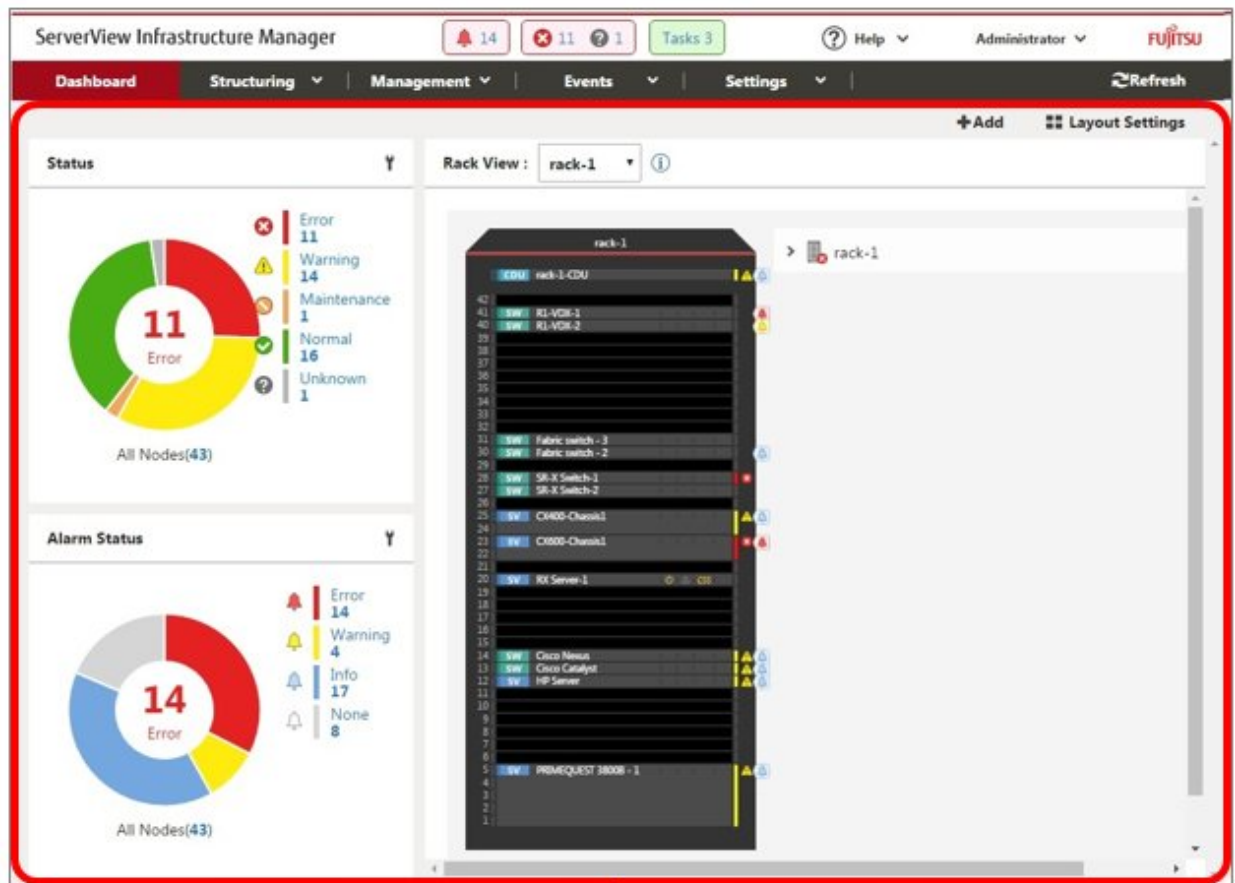4. The status of the node is displayed. Refer to the help screen for descriptions for the content displayed.

How to display the help screen: Select the [⑦Help] - [Help] - [Help for this screen] in upper right side on the screen while it is displayed.

This finishes the node status display.

3.3 Display the Node Notification Information

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

1. From the Global Navigation Menu, select [Dashboard] to display the [Dashboard] screen.

[Dashboard] screen

2. Refer to the help screen for descriptions regarding the [Alarm Status] widget.

How to display the help screen: Select the [⑦Help] - [Help] - [Help for this screen] in upper right side on the screen while it is displayed.

3. In the [Alarm Status] widget, select the status to be checked (Error, Warning, Info, and None) to display the [Node List] screen.

It may take time to display the node list depending on the number of nodes registered in ISM.

4. The nodes with the alarm status will be displayed. Refer to the help screen for descriptions for the content displayed.

How to display the help screen: Select the [⑦Help] - [Help] - [Help for this screen] in upper right side on the screen while it is displayed.

This finishes the display of the node notification information.

3.4 Display the Node Log

Display the logs collected from the managed node lined up in a time series. By specifying the requirements of the managed node, Severity, Category (Hardware, operating system) etc., the logs to be displayed can be narrowed down.

1. From the Global Navigation Menu, select [Structuring] - [Log Collection].

2. From the log collection menu, select [Node Log Search] to display the [Node Log List] screen.

3. When narrowing down the node logs displayed, select the [Filter] button to display the [Filter] wizard. Enter the filtering requirements into the [Filter] wizard, and then select the [Filter] button.

   Refer to the help screen for entering the filtering requirements.

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

4. The filtered node logs will be displayed on the [Node Log List] screen.

This finishes the node logs display.

3.5 Download the Archived Logs

The archived logs collected from the managed node can be downloaded.

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

2. From the log collection menu, select the [Management Logs] - [Archived Log] tab.

3. Check the checkbox of the node whose archived logs should be downloaded.

4. From the [Actions] button, select [Create Download Files] to display the [Create Download Files of Archived Log] wizard.

5. Enter the setting items, then select the [Apply] button.

   Refer to the help screen for entering the setting items.

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

6. The download file is created.

7. When selecting the [Download] button on the download file items, the download file created in Step 6 will be downloaded to the console.

This finishes the download of the archived logs.

Chapter 4 Operations for Each Use Scene

4.1 Check the Node where an Error Occurred

By displaying only the monitoring target nodes where an error occurred, it simplifies checking the information of error nodes.

ISM does not refresh the status of the nodes on the screen in real time. In order to display the current status of the node, select the refresh button to refresh the screen.

1. From the Global Navigation Menu, select [Dashboard].

2. In the [Status] widget, select the [Error] on the right side of ❌.

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

4. Check the status for the error nodes displayed.

4.2 Display the Node Logs of the Target Node

For collecting information about node errors, check whether there are errors in the node log contents by collecting and displaying the logs.

1. To display the log correctly, the already collected logs will be processed before collecting the most recent log.

   From the Global Navigation Menu, select [Structuring] - [Log Collection], then select [Node Log Search] from the log collection menu to display the [Node Log List] screen. When the node logs have been shown previously, the messages will be displayed in the list. Delete logs as required.

   [Delete Logs]

   a. From the log collection menu, select the [Management Logs] - [Node Log] tab.

   b. On the [Node Log] tab screen, check the checkbox of the node whose node logs should be deleted.

   c. From the [Actions] button, select [Delete Node Log Files] to show the [Delete Node Log Files] wizard.

   d. Enter the setting items, then select the [Delete] button.

      Refer to the help screen for entering the setting items.

      How to display the help screen: Select the [⑦] in the upper right side on the wizard screen.

2. Select the [Actions] button, select [Collect Logs] to display the [Collect Logs] wizard.

3. Select the [Select] button, select the nodes displayed on the [Select Target Nodes] screen.

4. By selecting the [Run] button on the [Collect Logs] screen, collection is executed.

   Since collection is executed in the background, the results are not reflected immediately. When the update button in selected, depending on the collection status, any collected messages will be added.
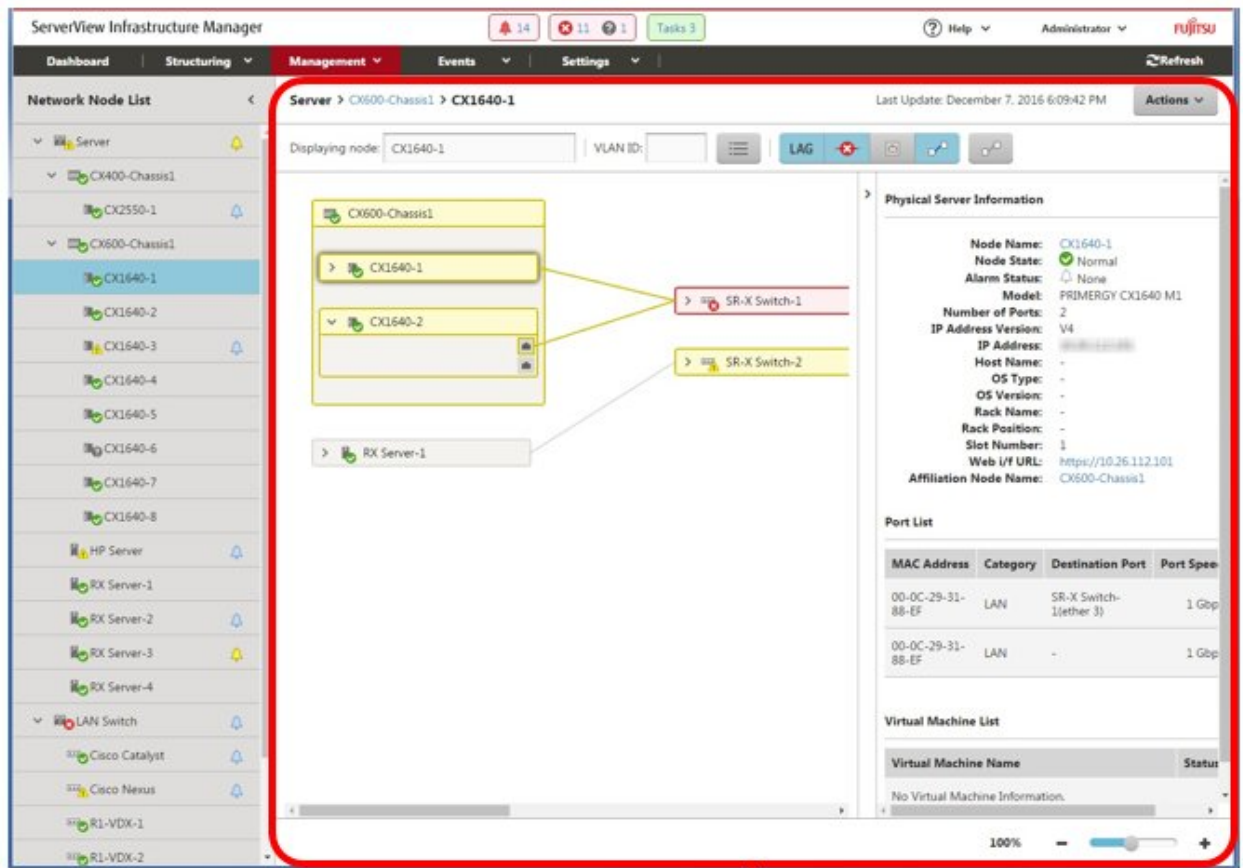
This finishes the node logs display.

4.3 Check the Error Point on the Network and its Affected Area

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

1. From the Global Navigation Menu, select [Management] - [Network Map] to display the [Network Map Display] screen.

[Network Map Display] Screen

2. Check the node indicated in red. The node where an error occurs turns red.

3. When the [Switching display affected area of error] button on the top of the Network Map is OFF, change it to ON.

4. The connection in the affected area, the port frame or the node frame is displayed in yellow.

   When virtual networks are configured, the virtual machines within the affected area, the virtual switches, and the virtual connections are also displayed in yellow.

This finishes the check for error point on the network and its affected area.

4.4 Set up Server

4.4.1 Set up Server BIOS

Set up BIOS for servers registered in ISM.

For the BIOS setup procedure, refer to "4.4.8 Assign Profile."

4.4.2 Set up Server iRMC

Set up iRMC for servers registered in ISM.

For the iRMC setup procedure, refer to "4.4.8 Assign Profile."

4.4.3 Set up Server MMB

Set up MMB for servers registered in ISM.

For the MMB setup procedure, refer to "4.4.8 Assign Profile."

4.4.4 Install Server OS

Install OSes on the servers registered in ISM.

The following OSes can be installed.

- Windows Server

- Red Hat Enterprise Linux

- SUSE Linux Enterprise Server

- VMware

  1. Prepare environment configurations

     When installing an OS, it is required to create a DHCP server.

     For details, contact Fujitsu customer service partner.

  2. Prepare the OS image

     As a preparation setting when installing the OS, import the OS image into the repository in advance. For the repository management, refer to "2.3.2 Repository Management" in the "FUJITSU Software ServerView Infrastructure Manager V2.1 User's Manual."

  3. Create a profile (or set up)

     OS installation is executed by the profile assignment. To install an OS, a profile must be created or set up.

  4. Assign a profile

     The OS registered in the profile, after the profile assignment, will be installed.

     For the procedure on profile assignment, refer to "4.4.8 Assign Profile."

4.4.5 Set up Server Virtual IO

Set up virtual IO for servers registered in ISM.

For the virtual IO setup procedure, refer to "4.4.8 Assign Profile."

4.4.6 Create Policy

The template containing hardware settings for node is called a policy. When a lot of nodes are managed, input into the profile is simplified by policies specified by common factors. Creating this policy. It is optional to create a policy and it is not always required when creating a profile.

  1. From the Global Navigation Menu, select [Structuring] - [Profiles] to display the [Profile Settings] screen.

  2. From the [Profile Settings] screen on the left side menu, select [Policy Settings] - [All Policies] to display the [All Policies] screen.

  3. From the [All Policies] screen, select [Actions] button - [Add Policy] to display the [Add Policy] wizard.

     - When setting the BIOS policy

       On the [1. General Information] screen in the [Add Policy] wizard, select [BIOS] in the [Policy Type] field.

     - When setting iRMC policy

       On the [1. General Information] screen in the [Add Policy] wizard, select [iRMC] in the [Policy Type] field.

     - When setting MMB policy

       On the [1. General Information] screen in the [Add Policy] wizard, select [MMB] in the [Policy Type] field.

Follow the [Add Policy] wizard and enter the other setting items. Refer to the help screen for entering the setting items.

How to display the help screen: Select the [⑦] in the upper right side on the wizard screen.

4. After policy addition is finished, the corresponding policy will be displayed on the [All Policies] screen.

This finishes policy creation.

4.4.7 Create Profile

Profiles are collections of settings for node hardware or OS installation, they need to be created individually for each node.

1. Create a policy.

   For creating a policy, refer to "4.4.6 Create Policy." A policy is not always required for creating a profile.

   Moreover, already created policies can be applied.

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

3. From the [All Profiles] screen - [Actions] button, select [Add Profile] to display the [Add Profile] wizard.

4. Follow the instructions on the [Add Profile] wizard and enter the setting items.

🅿 Point
・・
Refer to the help screen for entering the setting items.

How to display the help screen: Select the [⑦] in the upper right side on the wizard screen.
・・

[When setting up BIOS using policy]

a. In the [Add Profile] wizard - [1.General Information] - [BIOS Policy], select the created policy (or a policy to be reused).

b. Enter the other setting items on the [1.General Information] screen and select [Next].

c. In the [2. Details] - [BIOS] tab, the setting values with the selected policies are automatically entered.

d. Set the other items as required.

[When setting up iRMC using policy]

a. In the [Add Profile] wizard - [1.General Information] - [iRMC Policy], select the created policy (or a policy to be reused).

b. Enter the other setting items on the [1.General Information] screen and select [Next].

c. In the [2. Details] - [iRMC] tab, the setting values with the selected policies are automatically entered.

d. Set the other items as required.

[When setting up MMB using policy]

a. In the [Add Profile] wizard - [1.General Information] - [MMB Policy], select the created policy (or a policy to be reused).

b. Enter the other setting items on the [1.General Information] screen and select [Next].

c. In the [2. Details] - [MMB] tab, the setting values with the selected policies are automatically entered.

d. Set the other items as required.

[When installing an OS]

a. In the [Add Profile] wizard - [1.General Information] - [OS Type], select the OS type to be installed.

b. Enter the other setting items on the [1.General Information] screen and select [Next].

c. Select the [2. Details] - [OS] tab to enter the setting items.

d. Select the [2. Details] - [OS Individual] tab to enter the setting items.

[When setting up virtual IO]

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

b. In the [2. Details] - [VirtualIO] tab, select [Settings] and follow the instructions on the wizard to enter the setting items.

5. After profile addition is finished, the corresponding profile will be displayed on the [All Profiles] screen.

This finishes the profile creation.

4.4.8 Assign Profile

Assign the profile to the servers registered in ISM, set up the server BIOS/iRMC/MMB/virtual IO or install an OS.

1. Create a profile. (For creating a profile, refer to "4.4.7 Create Profile.")

2. From the Global Navigation Menu, select [Management] - [Nodes] to display the [Node List] screen.

   It may take time to display the node list depending on the number of nodes registered in ISM.

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

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

5. From the [Actions] button, select [Assign/Reassign Profile] to show the [Profile Assignment] wizard.

6. Follow the instructions on the [Profile Assignment] wizard and enter the setting items.

   Refer to the help screen for entering the setting items.

   How to display the help screen: Select the [⑦] in the upper right side on the wizard screen.

7. After the BIOS/iRMC/MMB/virtual IO settings or the OS installation is finished, the [Status] field on the [Node List] screen will display [Assigned] for the corresponding server.

This finishes the node profile application.

Point

By setting tags to nodes beforehand it is possible to filter the nodes by tags on the [Node List] screen. Filtering nodes makes it easier to extract target nodes.

4.5 Check Firmware Version of the Server

Display the firmware version of the servers registered in ISM.

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

2. Select a node name of target device, collect node information from the [Node Information] dialog - [Get Node Information].

   Execute it for the same number of the node to confirm the firmware version.

3. On the [Firmware] screen, the firmware version of the server will be displayed in the [Current Version] column.

This finishes the check of the firmware version of the server.

Point

- It may take time to acquire node information because it is executed in the asynchronous.

- When acquisition of node information is completed, the log of message ID "10020303" is output in [Events] - [Events] - [Operation Log].

- By setting tags to nodes beforehand it is possible to filter the nodes by tags on the [Node List] screen. Filtering nodes makes it easier to extract target nodes.

4.6 Update the Server Firmware

Update the firmware of the servers registered in ISM.

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

2. Download the firmware of the iRMC/BIOS from the website. Download the firmware for the target model from the website below.

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

3. Store the downloaded file in an arbitrary folder. When the downloaded file is compressed, decompress the file in the folder.
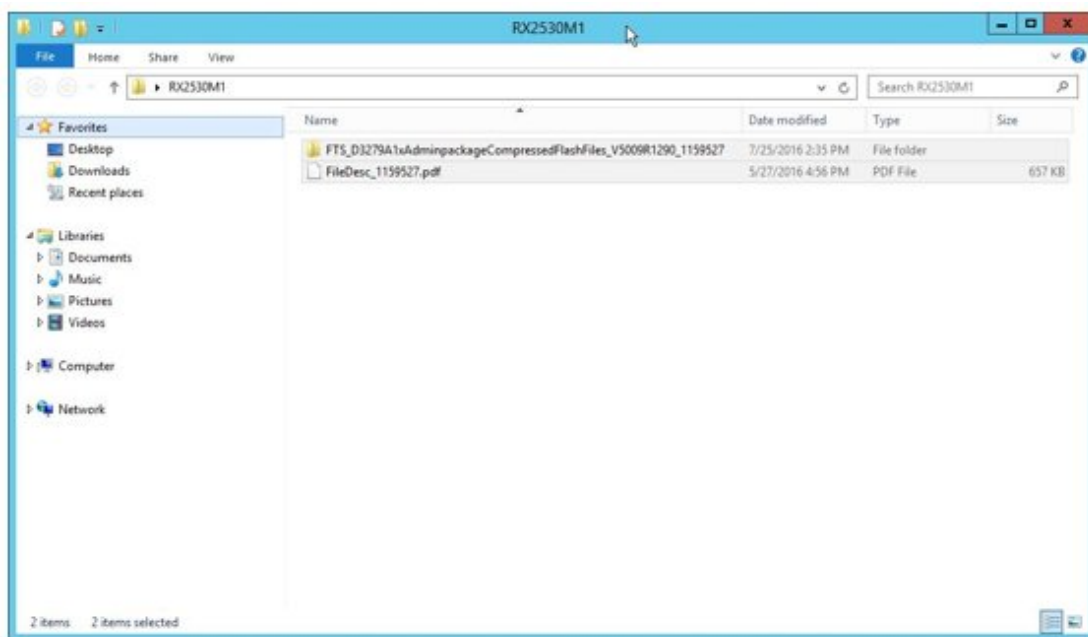
4. FTP is used to send it to ISM-VA. Make sure to transfer it with the same structure as the folder.

   Transfer them by using FTP command or FTP client software (such as FFFTP or WinSCP). At the time, set the character code as UTF-8 to be converted.

📝 Note

· ·

Do not use Windows Explorer because the character code is not handled correctly.

· ·

   After logging in to ISM-VA with the FTP client software, move from the root directory to the "<user group name>/ftp" directory and transfer the data into this directory.

5. Import firmware.

   From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Firmware] - [Import] in the left tree part. From the [Actions] button in the [Import Data List] tab, select [Import Firmware].

   Follow the instructions on the screen and enter the file location, type, model and version, then select [Assign].

   Enter versions to be entered using the table below.

Table 4.1 Versions to be entered

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

   After starting the import, the operations will be registered as ISM tasks. Check the status of the operations on the [Tasks] screen.

Select [Tasks] on the top of the Global Navigation Menu to display a list of the tasks on the [Tasks] screen.

6. Confirm that the firmware has been imported.

   From the Global Navigation Menu, select [Structuring] - [Firmware] - [Import] in the left tree part to display the [Import] screen. Select the [Firmware Data] tab on the right side on the screen.

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

7. Set the target server to maintenance mode.

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

   Select the node name that is target for firmware update, assign the maintenance mode in the [Node Information] dialog - [Switch Maintenance Mode].

8. Select target server.

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

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

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

9. Starting firmware update.

   Follow the instructions on the [Update Firmware] wizard and enter the setting items. Refer to the help screen for entering the setting items.

   How to display the help screen: Select the [⑦] in the upper right side on the wizard screen.

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

   Check the status of the operations on the [Tasks] screen.

   Select [Tasks] on the top of the Global Navigation Menu to display a list of the tasks on the [Tasks] screen.

10. When you update the BIOS and PCI cards with online firmware update, restart the target server.

11. Release maintenance mode for the target server.

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

    Select the node name that is target for firmware update, release the maintenance mode in the [Node Information] dialog - [Switch Maintenance Mode].

12. Confirm that the firmware version of the target server has been updated.

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

    Select a node name executed firmware update, collect node information from the [Node Information] dialog - [Get Node Information].

    On the [Firmware] screen, the version number is displayed after update.

This finishes the server firmware update.

℗ Point
. . . .

By setting tags to nodes beforehand it is possible to filter the nodes by tags on the [Node List] screen. Filtering nodes makes it easier to extract target nodes.
. . . .

4.7 Set up Switch and Storage

4.7.1 Create Profile

Create a profile (aggregate of hardware settings).

1. From the [Profile Settings] screen on the left side menu, select [Profile Settings] - [All Profiles] to display the [All Profiles] screen.

2. From the [All Profiles] screen - [Actions] button, select [Add Profile] to display the [Add Profile] wizard.

3. Follow the instructions on the [Add Profile] wizard and enter the setting items.

   Enter RAID configuration, SNMP settings, account and other settings for each device.

   Refer to the help screen for entering the setting items.

   How to display the help screen: Select the [⑦] in the upper right side on the wizard screen.

4. After profile addition is finished, the corresponding profile will be displayed on the [All Profiles] screen.

This finishes the profile creation.

4.7.2 Assign Profile

Assign the profile to the node registered in ISM.

1. Create a profile. (For creating profile, refer to "4.7.1 Create Profile.")

2. From the Global Navigation Menu, select [Management] - [Nodes] to display the [Node List] screen.

   It may take time to display the node list depending on the number of nodes registered in ISM.

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

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

5. From the [Actions] button, select [Assign/Reassign Profile] to show the [Profile Assignment] wizard.

6. Follow the instructions on the [Profile Assignment] wizard and enter the setting items.

   Refer to the help screen for entering the setting items.

   How to display the help screen: Select the [⑦] in the upper right side on the wizard screen.

7. After assignment of the profile has been finished, on the [Node List] screen the [Status] column of the node will be displayed as [Assigned].

This finishes the node profile application.

4.7.3 Change in VLAN Settings of LAN Switch

Change VLAN settings of LAN switch from the Network Map.

1. From the Global Navigation Menu, select [Management] - [Network Map] to display the [Network Map Display] screen.

2. Select [Actions] - [Multiple VLANs setting] to enter the setting changes.

3. By LAN Switch on the Network Map, select the port to change the VLAN settings.

4. Select [Setting] in upper right side to enter the setting changes.

5. Confirm the changes and select [Register] to execute the setting changes if there is no problem.

6. Refresh the network management information after the execution, and then confirm that the changes are applied on the Network Map. The [VLANs setting] operation will be registered as an ISM task. Select [Tasks] on the top of the Global Navigation Menu to confirm that the task has been completed.

This finishes the VLAN setting changes.

4.7.4 Change in Link Aggregation of LAN Switch

Change Link Aggregation of LAN switch from the Network Map.

1. From the Global Navigation Menu, select [Management] - [Network Map] to display the [Network Map Display] screen.

2. Select [Actions] - [Link Aggregation setting].

3. Select the node to change the Link Aggregation settings, then select either of [Add], [Change] or [Delete].

4. Enter the setting change, select [Confirm].

5. Confirm the changes and select [Register] to execute the setting changes if there is no problem.

6. Refresh the network management information after the execution, and then confirm that the changes are applied on the Network Map.

This finishes the Link Aggregation setting changes.

4.8 Power Capping

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

The upper limit of the power consumption is configured by each of the power capping policy (definitions according to the operational pattern).

The power capping policy operates two types of custom definitions, one definition for schedule operation, and one definition for the minimum power consumption operation (Minimum), by switching the four types in total.

In order to use power capping, it is required beforehand to set [Add power capping settings] (the node information for the power capping target and definition for power capping policy) to enable power capping policies.

Note

Power capping policy is managed by each rack. It is required to review the power capping settings (node power settings, the upper limit value for power capping policy) related to each rack.

- Add a node to the rack

- Remove a node from the rack

- Move a node to another rack

4.8.1 Confirm the Current Power Capping Status

Confirm the power capping status of the target rack.

1. In the [Datacenter List] screen, select the rack that you want to confirm the power capping setting status for.

2. Confirm the contents in the power capping setting status displayed in the upper right side on the rack details screen.

Table 4.2 Power capping status

Power capping status	Description
Not set Power Capping	Power capping has not been set up.
Stopped Power Capping	Power capping has been set up but all power capping policies are disabled. To enable it, select the [Actions] button to select [Enable/Disable Power Capping Policy].
Power Capping	Power capping has been set up and at least one power capping policy is enabled.
Updating Power Capping	The power capping settings are being updated.
Difference in Power Capping	A node was added or deleted after the power capping was set up. It is required to enter the node power settings of the added device and to review the upper limit of the power capping policy.

4.8.2 Add/change the Power Capping Settings of the Rack

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

1. In the [Datacenter List] screen, select the rack that you want to add or edit the power capping policy for.

2. Select the following from the [Actions] button.

   - When adding a new power capping setting: [Add Power Capping Setting]

   - When editing all the set power capping policy settings: [Edit Power Capping Setting]

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

Rack power consumption column

The current power capping status value is displayed.

Table 4.3 Rack power consumption column

Item	Description
Current status	Displays the latest status of the power capping settings.
It is currently enabled policy	Displays the policy that has been enabled in [Enable/Disable Power Capping Policy].
Max power consumption	Displays the total maximum power consumption value currently entered in the node power settings.
Fixed power	Displays the entered total fixed power value (the total maximum power value of devices not using power capping).
Power consumption	The current total power consumption of the devices capable of power capping (mainly servers) and the maximum power consumption of devices that does not use power capping.

[Node power settings] tab

Enter the settings value of the nodes using power capping.

Table 4.4 [Node power settings] tab

Item	Description
Node type	Type of each node.
Node Name	Name of each node.
Fixed power	Use the maximum power consumption value entered as a fixed value. Check when handling it as a fixed power. For the devices that ISM cannot retrieve the power consumption value, this will be enabled automatically.
Max power consumption	Enter the maximum power consumption value as specification in catalogs. When calculating internally, it is used as the possible range of node power capping. For devices where power capping cannot be used it is calculated using appropriate fixed power values.
Power consumption	Displays the current power consumption value retrieved from the nodes.
Business Priority	- Low When the power reaches to the upper power value, it becomes the target for the power capping. - Middle When capping the power for Low devices is not enough, it will be the power capping target. - High When capping the power for Low and Middle devices are not enough, it will be the power capping target. - Critical Out of target for power capping. However, when minimum policy is enabled power capping will be used.

[Power Capping Policy] tab

Register the setting values for the three types of power capping policies.

For the upper limit power consumption target, upper limit values for two types of custom policies, upper limit value for schedule policy as well as schedule can be set.

Table 4.5 [Power Capping Policy] tab

Item		Description
Power capping policy		
	Custom 1,2	Operation will be executed with the set upper limit value specified for power consumption.
	Schedule	When schedule policy is enabled, it is operated using the specified upper limit value during the duration of the schedule (day, time).
	Minimum	Operations will be executed using minimal power consumption, including devices whose business priority is Critical.
Displayed value		
	Upper Value	Enter the upper limit target value for each policy.
	Fixed Value	The total value of the maximum power consumption of the devices that are out of target for power capping.
	Enabled/Disabled	Displays the status of the power capping policy.
Setting details of schedule		
	All day	Check when not specifying operating time.

	Specify Time	Check when setting start time and completion time.
		
		 - Start Time
		
		   Set the time to start using scheduled power capping. Set the value in the ISM-VA time zone.
		
		 - End Time
		
		   Set the time to complete operating scheduled power capping. Set the value in the ISM-VA time zone.

	Day of the week	Check the day when scheduled power capping is operated. Multiple days can be selected.

📑 Note

The upper limit value is the power capping target value. Whereas the capping is normally executed to make sure that the power consumption is lower than the upper limit, when the upper limit is set low it may exceed the power consumption.

🅿 Point

When setting it as in the example below, it will be scheduled from Sunday 23:00 to Monday 5:00 in the ISM-VA time zone.

Setting Example)

 - Start Time: 23:00

 - End Time: 5:00

 - Day of the week: Sunday

4.8.3 Enable the Power Capping Policy of the Racks

Enable the power capping policy for the applicable racks.

1. In the [Datacenters List] screen, select the rack that you want to enable power capping policy for.

2. From the [Actions] button, select [Enable/Disable Power Capping Policy].

3. In the row of the power capping policy you want to enable, set [Enable/Disable] - [After Changing] to [Enable], then select [Apply].

   The displayed content is as follows.

Table 4.6 The displayed content in the [Enable/Disable Power Capping Policy] screen

Item	Description
Policy Name	Name of the power capping policy. There are four types: custom 1, custom 2, schedule, and minimum.
Upper Value	The upper limit target value entered for each policy in the power capping settings.
Fixed Value	The total value of the maximum power consumption of the devices that are out of target for power capping.
Enabled/Disabled	Displays the status of the power capping policy.

Note

- Whereas all power capping policies are enabled independently, when minimum is set it is executed with highest priority. In this case, it will be operated with the minimum power consumption also for devices where the business priority in [Setting by nodes] in the power capping settings is Critical.

- When multiple power capping policies other than minimum are enabled, the policy with the lowest upper power consumption limit value will be executed.

4.8.4 Delete Power Capping Settings for Racks

Delete all power capping settings information for the rack.

1. In the [Datacenters List] screen, select the rack that you want to delete the power capping settings for.

2. From the [Actions] button, select [Delete Power Capping Setting].

3. Confirm that it is the rack that the settings should be deleted for, then select the [Delete] button.
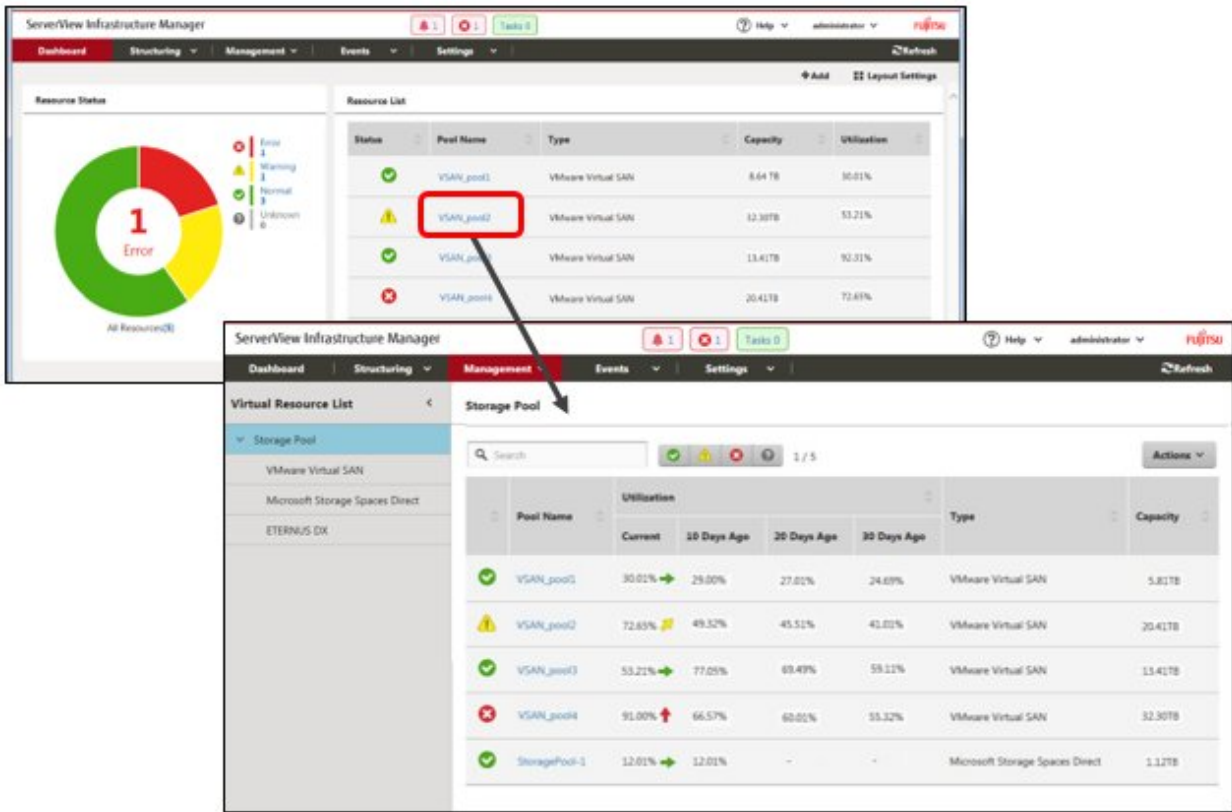
4.9 Manage Virtual Resource

4.9.1 Link with the ISM Dashboard

By adding the information display screen (the widget) for the virtual resource management on the ISM dashboard, it is possible to display the details of the target resource information to be checked directly from the dashboard.

Figure 4.1 Display the widgets on the ISM dashboard
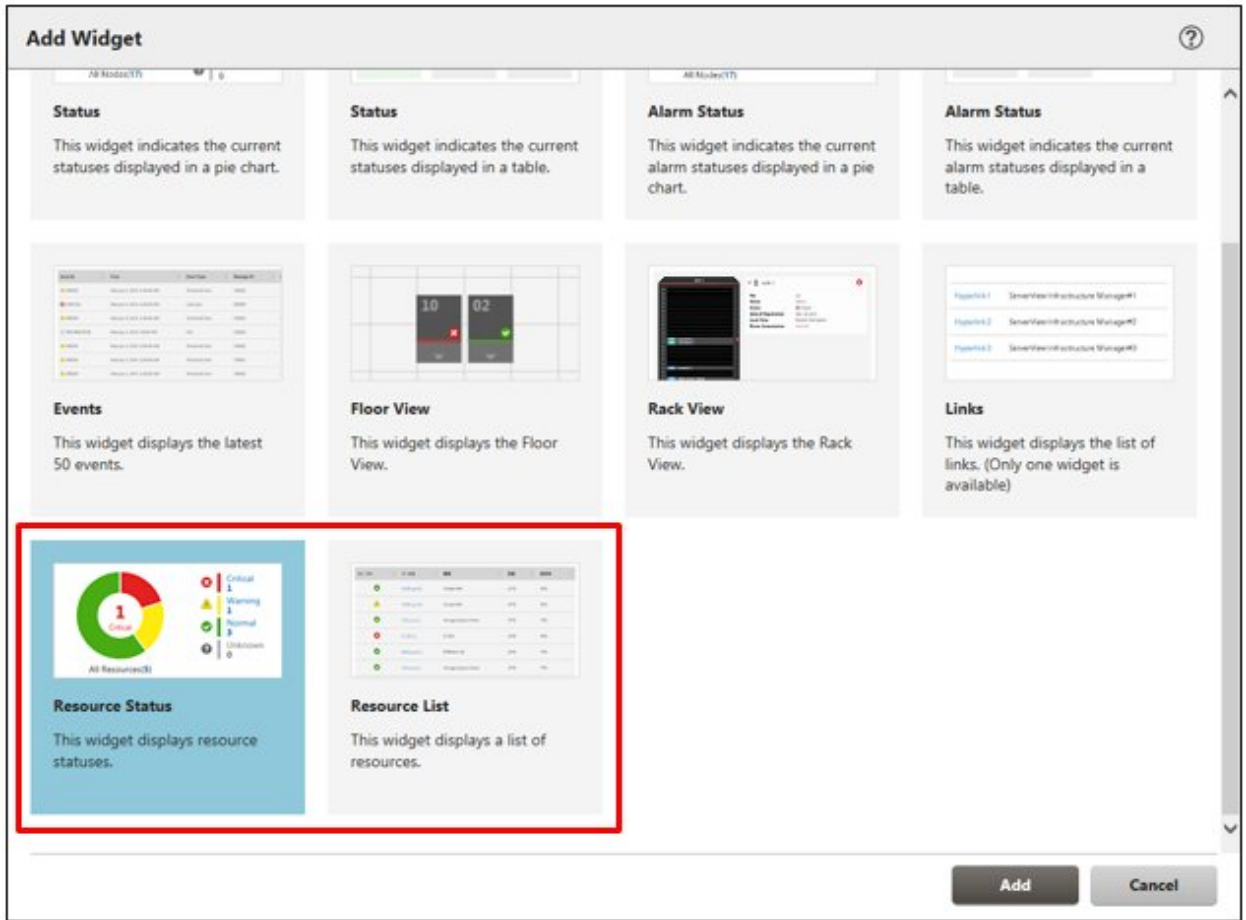

Add the widget onto the ISM dashboard

The procedures to add the widget onto the ISM dashboard are as follows.
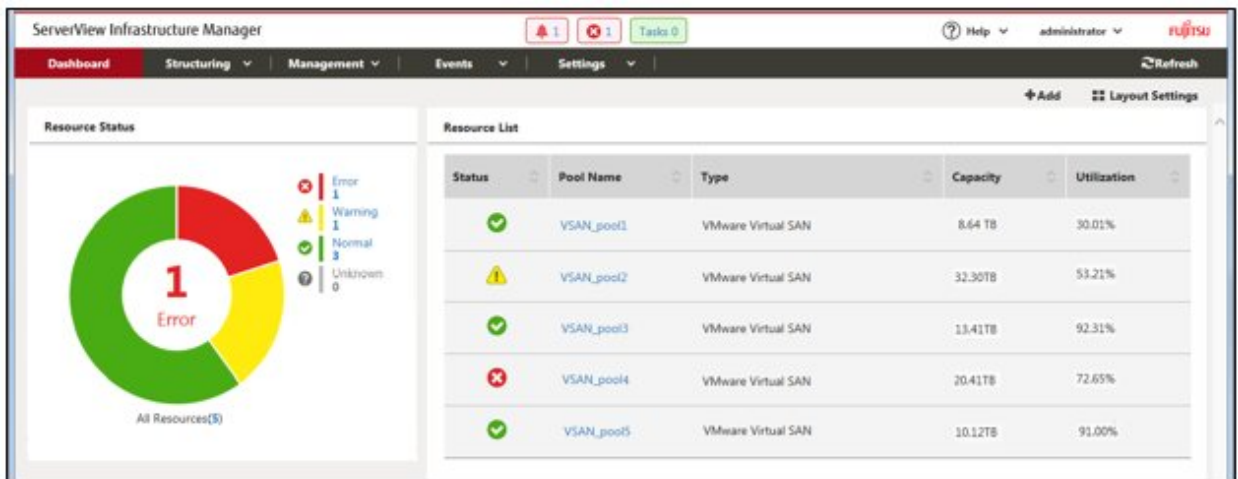
1. Select [+Add] on the top part.

The Add Widget menu is displayed.

[Resource Status] and [Resource List] are the display widgets for virtual resources.

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

   The selected widget is displayed on the dashboard.

4.9.2 Link with Node Information ([SDS] tab)

By embedding the virtual resource management information into the Details of Node screen, they link with each other.
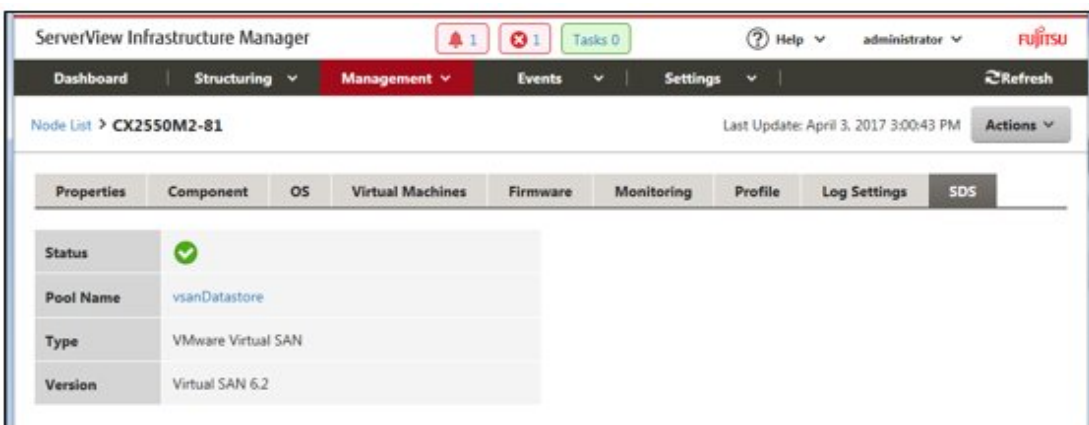
1. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Nodes] to select the node name on the [Node List] screen.

   The Details of Node screen is displayed.
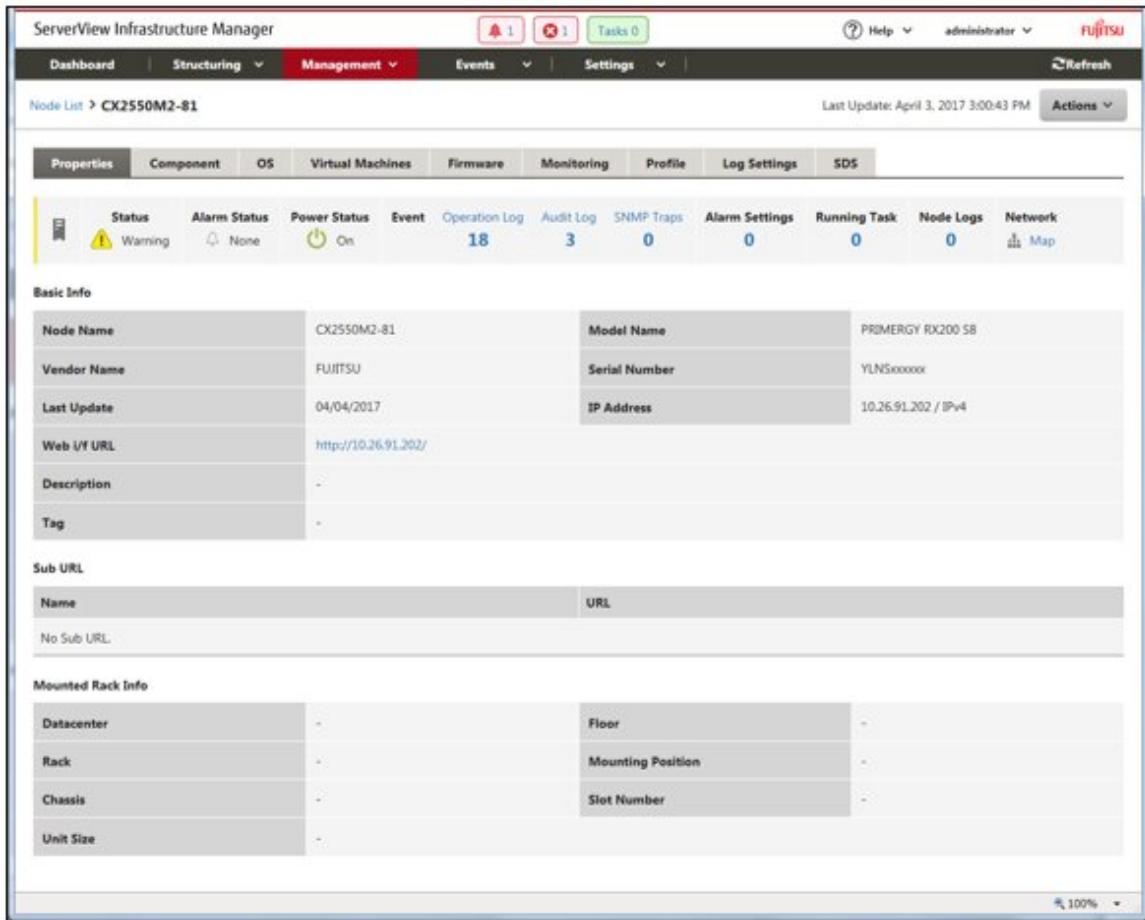
2. Select the [SDS] tab.

   The storage pool information related to the node is displayed.

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