Fujitsu Software

ServerView Infrastructure Manager V2.0

User's Manual Modification Information

[Manual Modification Information]

ServerView Infrastructure Manager V2.0 User's Manual

[Modification History]

Modification No.	Supplied date	Modified/Added Section	The Nearest Title	Modification Overview	Target Ver.
1	January 2017	1.2.6 Overview of Network Manager	The same as on the left side	Adding the explanation about Network Map	V2.0.0.c
2	January 2017	1.3.1 Images of ISM Functions for Each Scenario of Infrastructure Operation and Management	Figure 1.5 Image of functions: maintenance of managed nodes	Adding the image of setting switch information	V2.0.0.c
3	September 2016	1.4 Configuration	Fig. 1.6 Network configuration	Adding Note about the servers and services prepared outside ISM	V2.0
4	January 2017	1.4 Configuration	The same as on the left side	Adding the explanation when installing an OS to a managed node – server (managed server) using Profile Manager	V2.0.0.c
5	September 2016	1.5.1 System Requirements for ISM-VA (Virtual Machines)	The same as on the left side	Adding Note about disk capacity	V2.0
6	September 2016	1.5.3 Service Requirements Necessary for ISM Operations	System requirements for management terminals for file transfer	Adding the service requirements necessary outside ISM	V2.0

Modification No.	Supplied date	Modified/Added Section	The Nearest Title	Modification Overview	Target Ver.
7	September 2016	1.6 Precautions	Timing of completing OS installation	Adding the explanation about the RAID configuration in OS installation	V2.0
8	January 2017	1.6 Precautions	Using automatic data collection by Log Manager	Adding the explanation when the upper limit is set to the total size of log files	V2.0.0.c
9	September 2016	2.2.1.1 Registering Datacenters/Floors/Racks/Nodes	Registration of node OS information	Adding Note for the case of registering a domain user as node OS information	V2.0.0.c
10	January 2017	2.2.1.1 Registering Datacenters/Floors/Racks/Nodes	Node Detection	Adding Note about non-supported devices	V2.0.0.c
11	September 2016	2.2.1.2 Checking Datacenters/Floors/Racks/Nodes	Checking of node OS information	Adding the explanation for the case of registering a domain user as node OS information	V2.0.0.c
12	September 2016	2.2.2 Monitoring	Setting of monitoring items and threshold values	Adding the explanation about various LED statuses	V2.0
13	September 2016	2.2.2 Monitoring	Registration of alarm settings	Adding the explanation about event types	V2.0
14	September 2016	2.2.2 Monitoring	Registration of alarm settings	Adding the explanations for the case where you need to change the setting contents of an alarm and for maintenance mode	V2.0

Modification No.	Supplied date	Modified/Added Section	The Nearest Title	Modification Overview	Target Ver.
15	January 2017	2.2.2 Monitoring	Alarm statuses	Adding the explanation about how to register an MIB file	V2.0.0.c
16	September 2016	2.2.3 Profile Manager	Sample profile	"Creation of Profile" screen sample (GUI) is replaced.	V2.0
17	September 2016	2.2.3 Profile Manager	Procedure for editing and reassigning profiles	Adding the explanation about the setting items of an OS in editing profiles	V2.0
18	September 2016	2.2.3 Profile Manager	Required preparations before OS installation	Adding the explanation about import of ServerView Suite DVD Changing the explanation about the LAN to be PXE booted	V2.0 V2.0.0.c
19	September 2016	2.2.3 Profile Manager	Specifying behavior when assigning profiles	Adding the explanation about profile reassignment and about profile assignment while the power remains ON	V2.0
20	September 2016	2.2.4.1 Confirming firmware versions of nodes	The same of the left side	Adding the explanation about the screen displayed when [Column Display] field of Node List is switched to [Firmware]	V2.0
21	September 2016	2.2.4.2 Updating Firmware	The same as on the left side	Modifying wording(s)	V2.0
22	September 2016	2.2.4.2 Updating Firmware	Behavior during updates	Modifying wording(s)	V2.0
23	September 2016	2.2.4.2 Updating Firmware	Implementing firmware updates	Modifying wording(s)	V2.0

Modification No.	Supplied date	Modified/Added Section	The Nearest Title	Modification Overview	Target Ver.
				Adding Note upon performing firmware update for a PCI card	
24	September 2016	2.2.4.3 Checking Documentation that Is Supplied with Firmware Data	The same as on the left side	Modifying wording(s)	V2.0
25	January 2017	2.2.5 Log Manager	Types of collectable logs	Modifying the storage model	V2.0.0.c
26	January 2017	2.2.5 Log Manager	Monitoring function for disk capacities of log storage locations	Adding the explanation about the upper limit value for the total size of log files	V2.0.0.c
27	January 2017	2.2.6 Network Manager	The same as on the left side	Adding and modifying the overview explanation of Network Manager	V2.0.0.c
28	September 2016	2.2.6 Network Manager	The same as on the left side	Replacing image(s)	V2.0.0.c
29	January 2017	2.2.6 Network Manager	The same as on the left side	Adding and modifying the function list of Network Manager	V2.0.0.c
30	January 2017	2.2.6 Network Manager	Displaying network connection information	Adding the explanation about the connection relationship between a virtual machine(s)/virtual switch(s) and a physical port.	V2.0.0.c
31	September 2016	2.2.6 Network Manager	Displaying network connection information	Adding the explanation about the displayed screen of [Network Map]	V2.0

Modification No.	Supplied date	Modified/Added Section	The Nearest Title	Modification Overview	Target Ver.
32	January 2017	2.2.6 Network Manager	Displaying network connection information	Adding an item about the operating procedure to Note	V2.0.0.c
33	January 2017	2.2.6 Network Manager	Updating network management information	Adding the explanation about displaying the latest update time of network management information	V2.0.0.c
34	January 2017	2.2.6 Network Manager	Checking information on changes in network connections	Modifying wording(s)	V2.0.0.c
35	January 2017	2.2.6 Network Manager	Checking information on changes in network connections	Adding the explanation about the latest update date and time of connection information change	V2.0.0.c
36	January 2017	2.2.6 Network Manager	Setting reference information for changes in network connections	Adding the detailed information about reference point setting	V2.0.0.c
37	January 2017	2.2.6 Network Manager	Checking VLAN and LAG settings	Modifying the explanation about the procedure for checking VLAN Settings and Link Aggregation settings	V2.0.0.c
38	January 2017	2.2.6 Network Manager	The same as on the left	Adding the explanations about the procedures for changing VLAN settings and Link Aggregation Settings	V2.0.0.c

Modification No.	Supplied date	Modified/Added Section	The Nearest Title	Modification Overview	Target Ver.
39	September 2016	2.3.1 User Management	2.3.1.2 Managing User Groups	Adding the explanation about the upper limit value for the size of files that can be stored in ISM-VA Deleting a part of Note about authentication method Adding Note about virtual disk allocation after creating a user group	V2.0 V2.0.0.c
40	January 2017	2.3.1.3 Operating in Link with Microsoft Active Directory or LDAP	Activation procedure	Adding Note when operating in link with Microsoft Active Directory or LDAP	V2.0.0.c
41	January 2017	2.3.2 Repository Management	The same as on the left side	Adding Note about virtual disk allocation	V2.0.0.c
42	September 2016	2.3.2 Repository Management	Storing firmware data	Modifying wording(s) and some model names	V2.0
43	January 2017	2.3.3 Installing Emulex OneCommand Manager CLI and Qlogic QConverge Console CLI	The same as on the left side	Modifying the supplementary information about installation and operation methods of Emulex OneCommand Manager CLI、QLogic QConvergeConsole CLI	V2.0.0.c
44	September 2016	2.3.5.1 List of Commands in ISM-VA Management	Maintenance	Adding the command for setting an SNMP community name	V2.0
45	January 2017	2.3.5.1 List of Commands in ISM-VA Management	Event notification settings	Adding MIB file settings	V2.0.0.c

Modification No.	Supplied date	Modified/Added Section	The Nearest Title	Modification Overview	Target Ver.
46	September 2016	2.3.6 Management of Cloud Management Software	The same as on the left side	Adding the explanation about the management of cloud management software	V2.0.0.c
47	January 2017	2.4.3 When Deleting User Groups	The same as on the left side	Modifying a part of the explanation when deleting user groups	V2.0.0.c
48	September 2016	2.4.4 When Changing User Group Names	The same as on the left side	Modifying wording(s)	V2.0
49	September 2016	3.1 Workflow for Installing ISM	(1) Installation Design	Modifying some tasks in preparation	V2.0
50	September 2016	3.1 Workflow for Installing ISM	(6) Allocation of Virtual Disks	Modifying a part of the explanation in virtual disk allocation	V2.0
51	September 2016	3.1 Workflow for Installing ISM	Note	Adding Note about virtual disk	V2.0
52	September 2016	3.2.1.2 Estimation of Required Capacities for Repositories	Point	Adding the explanation about ServerView Suite DVD	V2.0
53	January 2017	3.2.3 Network Design	The same as on the left side	Adding the explanation about the network used by the OS	V2.0.0.c
54	September 2016	3.2.3 Network Design	Note	Adding the note about the initially overlapped IPs in ISM-VA	V2.0
55	September 2016	3.2.4 Setting of Node Names	The same as on the left side	Modifying the explanation about the characters allowed for node names	V2.0
56	September 2016	3.3.1 Installing on Microsoft Windows Server Hyper-V	The same as on the left side	Replacing a part of images	V2.0

Modification No.	Supplied date	Modified/Added Section	The Nearest Title	Modification Overview	Target Ver.
57	September 2016	3.3.2 Installing on VMware vSphere Hypervisor	The same as on the left side	Replacing a part of images	V2.0
58	September 2016	3.3.3 Installing on KVM	The same as on the left side	Modifying file names Replacing a part of images	V2.0
59	September 2016	3.4.1.1 For ISM-VA Running on Microsoft Windows Server Hyper-V (First Time)	The same as on the left side	Replacing a part of images	V2.0
60	September 2016	3.4.1.2 For ISM-VA Running on VMware vSphere Hypervisor (First Time)	The same as on the left side	Replacing a part of images	V2.0
61	September 2016	3.4.1.3 For ISM-VA Running on KVM (First Time)	The same as on the left side	Replacing a part of images	V2.0
62	September 2016	3.4.2 Initial Settings of ISM	The same as on the left side	Modifying a part of the examples of command execution results	V2.0
63	September 2016	3.4.2 Initial Settings of ISM	4. From the console, set the date and time.	Adding the setup procedure for use in a domain environment	V2.0.0.a
64	September 2016	3.7.1 Allocating Virtual Disks to Entire ISM-VA	For Microsoft Windows Server Hyper-V	Replacing a part of images	V2.0
65	September 2016	3.7.2 Allocating Virtual Disks to User Groups	For Microsoft Windows Server Hyper-V	Replacing a part of images	V2.0

Modification No.	Supplied date	Modified/Added Section	The Nearest Title	Modification Overview	Target Ver.
66	September 2016	4.1.1.1 For ISM-VA Running on Microsoft Windows Server Hyper-V (Second Time and Later)	The same as on the left side	Replacing a part of images	V2.0
67	September 2016	4.1.1.2 For ISM-VA Running on VMware vSphere Hypervisor (Second Time and Later)	The same as on the left side	Replacing a part of images	V2.0
68	September 2016	4.1.1.3 For ISM-VA Running on KVM (Second Time and Later)	The same as on the left side	Replacing a part of images	V2.0
69	September 2016	4.6.1 Deploying SSL Server Certificates	The same as on the left side	Adding the procedures for deploying a certificate Adding the procedures to create a unique SSL server certificate	V2.0
70	September 2016	4.8 Network Settings	The same as on the left side	Adding the explanation about the commands for setting up a DNS server	V2.0
71	September 2016	4.11 Displaying System Information	The same as on the left side	Modifying a part of the examples of command execution results	V2.0
72	September 2016	4.17 Setting of SNMP Community Name	4.16 Switching Levels of Trouble Investigation Logs	Adding the explanation about the commands for setting up SNMP community name	V2.0

Modification No.	Supplied date	Modified/Added Section	The Nearest Title	Modification Overview	Target Ver.
73	September 2016	4.18 DHCP server inside ISM-VA	4.16 Switching Levels of Trouble Investigation Logs	Adding the explanation about the DHCP server inside ISM-VA	V2.0.0.c
74	January 2017	4.19 MIB File Settings	4.16 Switching Levels of Trouble Investigation Logs	Adding the explanation about operation method of MIB file settings	V2.0.0.c
75	September 2016	Appendix A Uninstalling ISM-VA	Uninstalling from Microsoft Windows Server Hyper-V	Replacing a part of images	V2.0
76	September 2016	Appendix A Uninstalling ISM-VA	Uninstalling from VMware vSphere Hypervisor	Replacing a part of images	V2.0
77	September 2016	Appendix A Uninstalling ISM-VA	Uninstalling from KVM	Replacing a part of images	V2.0
78	January 2017	Appendix B Troubleshooting	Symptom: Execution of ismadm commands around 2:20 on Tuesdays results in an error.	Adding a troubleshooting article about ismadm command execution error.	V2.0.0.c
79	September 2016	Appendix B Troubleshooting	Symptom： For one of the following functions, the error "Communication	Modifying the wording(s)	V2.0

Modification No.	Supplied date	Modified/Added Section	The Nearest Title	Modification Overview	Target Ver.
			with server failed," is displayed when executing an operation to import a file.		
80	September 2016	Appendix B Troubleshooting	Symptom: Firmware updates for ETERNUS DX/AF models fail.	Modifying the wording(s) Adding ETERNUS AF	V2.0
81	January 2017	Appendix B Troubleshooting	Symptom: An error occurs when installing an OS with the Profile function.	Modifying the explanation about checking the connection of ISM-VA	V2.0.0.c
82	January 2017	Appendix B Troubleshooting	Symptom: The information displayed on the Network Map is outdated or incorrect.	Adding a troubleshooting article about Network Manager	V2.0.0.c
83	January 2017	Appendix B Troubleshooting	Symptom: Node logs are collected incorrectly or not at all.	Modifying the troubleshooting article about the upper limit value for the total size of log files	V2.0.0.c

Modification No.	Supplied date	Modified/Added Section	The Nearest Title	Modification Overview	Target Ver.
84	January 2017	Appendix B Troubleshooting	Symptom: Settings for log collection of a node cannot be made.	Modifying a wording(s)	V2.0.0.c
85	January 2017	Appendix B Troubleshooting	Symptom: "Operating System" and "ServerView Suite" cannot be specified in the log collection of a node.	Modifying a wording(s)	V2.0.0.c
86	September 2016	Appendix C Profile Settings Item	The same as on the left side	Adding the explanation about Profile Settings Items, as Appendix C Adding "1.2.4 Profiles for SUSE Linux Enterprise Server" in V2.0.0.c	V2.0 V2.0.0.c

Note: For detailed description of respective modifications, see the page corresponding to modification numbers. The style of modified descriptions differ as shown below, depending on the type of modification.

○ Modified description: The contents after modification are shown in blue color with dotted under line.

○ Added description: The added contents are shown in blue color.

○ Deleted description: The deleted contents are shown with a strike-though line. Note, however, that when the deleted contents can be easily noticed only with reference to "Modification Outline", their descriptions are omitted.

○ Replaced figures and images: Indication "Image replaced" is attached to the replaced figures and images.

○ If the explanation with the above-described style is difficult, the contents of Modification/Addition/Deletion are sometimes explained on "Modification Overview."

Modification No.1

1.2.6 Overview of Network Manager

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

- Checking of network connection statuses among multiple nodes in a connection diagram (Network Map) on the screen

- Checking of changed locations on the screen whenever there is a status change in network connections

- Checking and changing of the relationship between a virtual machine(s)/virtual switch(s) and a physical connection(s) by using a Network Map

- Checking of VLAN and Link Aggregation (LAG) settings for network switches and changing their settings

For details on Network Manager, see "2.2.6 Network Manager."

Modification No.2

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

Figure 1.5 Image of functions: maintenance of managed nodes
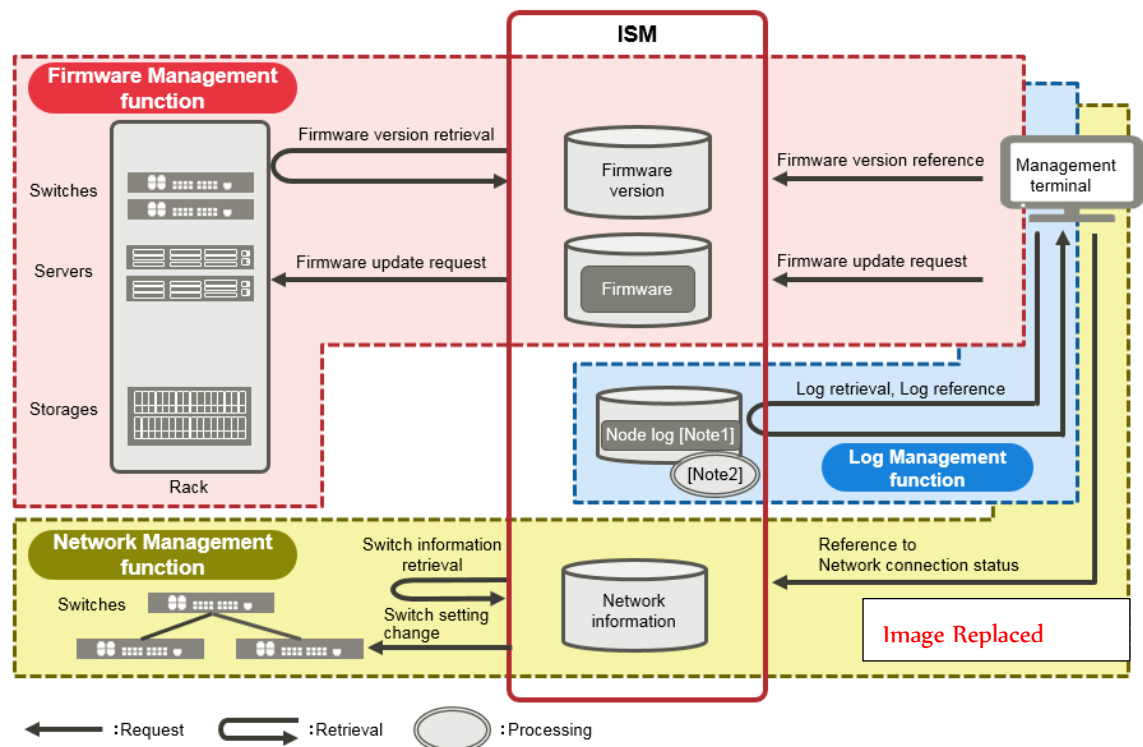
Modification No.3

1.4 Configuration
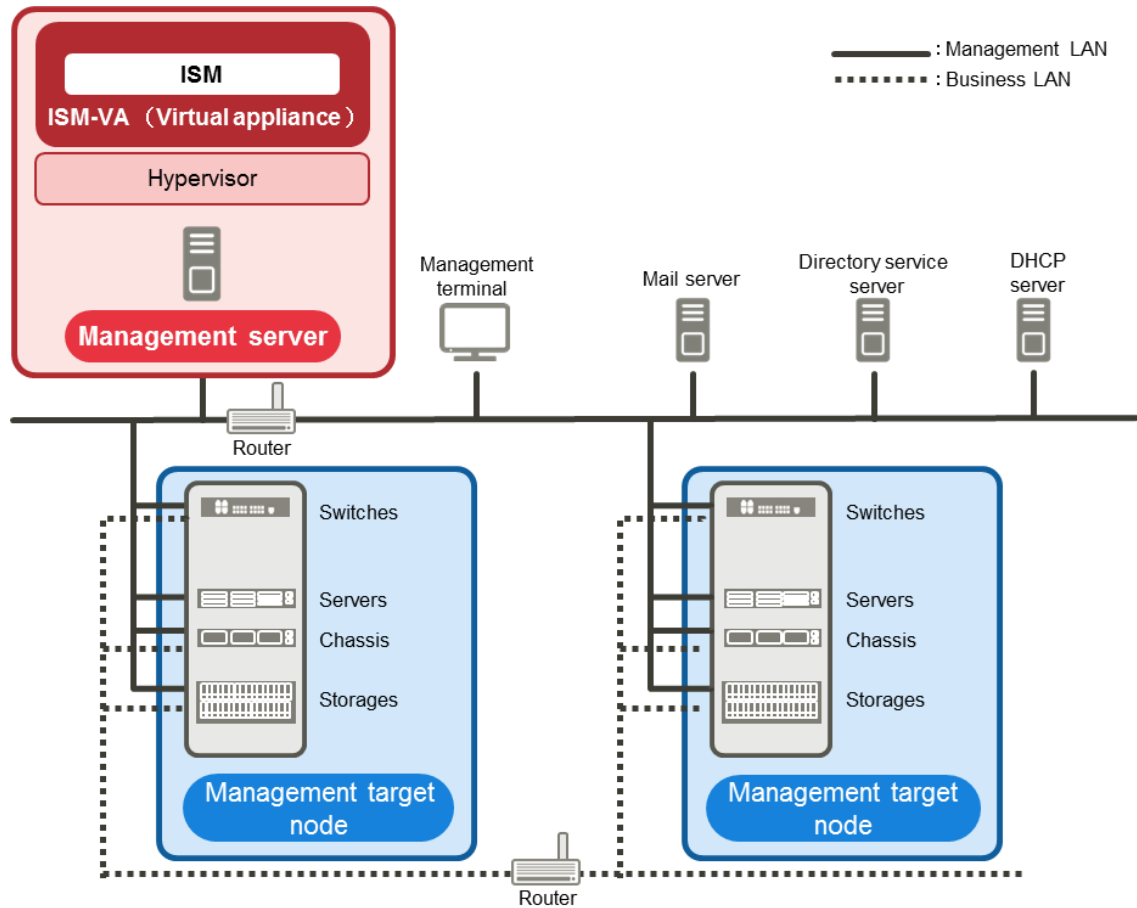
Note

For details on the servers and services prepared outside of ISM shown in Figure 1.6, see "1.5.3 Service Requirements Necessary for ISM Operations."

Modification No.4
1.4 Configuration

Managed nodes	Switch	Node that is an object of status monitoring and control by ISM.
	Storage	
	Server (Managed server)	Node that is an object of status monitoring and control by ISM. The LAN port that is used for BMC (iRMC) has to be connected to the management LAN. Ports other than the LAN port mentioned above have to be connected to the management LAN if you use Profile Manager to install an OS.

Modification No.5
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	35GB or more [Note 2] [Note 3] [Note 4]
Network	1Gbps or more
Hypervisor	Windows Server 2012/2012R2 VMware ESXi 5.5/6.0 Red Hat Enterprise Linux KVM

[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	8GB
101 to 400	4	8GB
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 information on estimating the disk capacity, 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.

Modification No.6

1.5.3 Service Requirements Necessary for ISM Operations

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

Item	Description
Mail server (SMTP server)	It is necessary to configure the mail server when sending a notifying mail of abnormalities and changes in the statuses of the managed nodes. [Setting] Set up with [Settings] - [Alarms] – [SMTP Server]. [Note] You can set up only one mail server for ISM.
Directory service server	It is necessary to configure the Directory Service when using it in the following situations. (1) When using it in User Management of ISM: You can use the following two directory services. ・OpenLDAP ・Microsoft Active Directory [Setting] You can register the configured server with [Settings] - [General Settings] – [LDAP Server Setting] in ISM. [Note] You can set up only one server for ISM. (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] When a monitoring target node uses a directory service, ISM does not work with the directory service which a monitoring target node belongs to. Individually set up the account capable of accessing the monitoring target node.
DHCP server	It is necessary to configure the DHCP server when using the profile management function to install an OS. To enable the PXE boot on the node (server) of OS installation destination, set up it

	so that an appropriate IPv4 address can be leased to the node.
	[Reference]
	You can also use ISM-VA as a DHCP server by activating the internal DHCP service of ISM-VA.
	Refer to "4.18 DHCP server inside ISM - VA" for the setting method when using ISM - VA as a DHCP server.
DNS server	It is necessary to configure the DHCP server when using it in the following situations.
	(1) Accessing ISM by hostname
	(2) Using FQDN for a variety of sever settings of ISM (such as operations in link with LDAP)
	[Note]
	For the method to set up the DNS server for ISM, refer to "Add DNS server" of "4.8 Network Settings."
	[Reference]
	・Manually set up a hostname for ISM-VA if you want to access ISM with the hostname under the condition where you do not use the DNS server. For the method to set up the hostname manually, refer to "4.12 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	It is necessary to configure the NTP server when synchronizing ISM with monitoring target nodes and with managed clients to avoid time lag between them.
	[Setting]
	Use ismadm command when you set up the NTP server for ISM.
	For the setting method, refer to "Setting of Enable/Disable of NTP Synchronization" and "Add/Remove NTP Server" of "3.4.2 Initial Settings of ISM"
Proxy server	It is necessary to configure the Proxy Server when accessing ISM from managed clients via a Proxy server.
	[Note]
	You cannot connect monitoring target nodes and ISM via a Proxy server.
Router	A router can be set up so that communications among respective networks are available when you configure multiple networks because you only can define one network interface for ISM.
	[Setting]
	Use the ismadm command when you set up the gateway for ISM.

	For the setting method, refer to "Modify network settings" of "4.8 Network Settings"

Modification No.7

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	Windows EULA screen during OS installation	At first login after accepting EULA and completing license input
Linux	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 for OS installation in the management server

For OS installation, you need ServerView Suite Installation DVD.

On this occasion, the number of logical drives configured with an array controller is only one if you perform OS installation using ServerView Suite Installation 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 necessary settings manually after installation.

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

Modification No.8

1.6 Precautions

Using automatic data collection by Log Manager

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.

- 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.

- ~~An upper limit is set for the total file size of logs that can be collected. As soon as the log capacity reaches 80% of the upper limit,~~ If the size of the log files reaches the [Warning threshold (%)] of [Archive Logs] or [Node Logs], set by the user groups in [Settings], a warning event will be recorded in ISM. In such a case, delete logs that are no longer needed in order to reduce the amount of files. Moreover, if it also reaches the set [Maximum Size (MB)], no more logs are saved.

- There is a set period/frequency for retaining collected logs, separately for each node. 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.

Modification No.9

2.2.1.1 Registering Datacenters/Floors/Racks/Nodes

Registration of node OS information

Executable user	Administrator group			Other groups		
	Admin	Operator	Monitor	Admin	Operator	Monitor

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 Active Directory realm name in the domain name field, and enter the user name without the realm name when you monitor a server by 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 the monitoring being performed by another domain user, to the OS to be monitored.

  For information on installation procedures, access your local support.

  When you use the domain user to monitor the OS, you need to do the DNS settings and domain environment settings.

  For information on how to do the settings, 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 in 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 log.

6. Click the [Refresh] button to update the display on the [OS] tab.

Modification No.10

Node Detection

Note

- The detected node information is effective only within the same session.

- In the manual detection result, devices that are not supported may also be displayed. Do not register unsupported devices.

Modification No.11

2.2.1.2 Checking Datacenters/Floors/Racks/Nodes

Checking of node OS information

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

Enter the FQDN of the Active Directory realm name in the domain ID field, and enter the user name without the realm name when you monitor an OS by using a domain user ID.

You can only display the items displayable through domain user privilege when a domain name is registered as account information and a domain user is registered as an account.

In this case, only the information that can be retrieved with domain user authorization is displayed on the GUI item.

For details on the settings for the OSes to be monitored, contact your local support.

Modification No.12

2.2.2 Monitoring

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

Modification No.13

2.2.2 Monitoring

Registration of alarm settings

Event types

There are two types of event as follows.

Event type	Description
Event	Various events that are detected internally in ISM Severity is specified. Specify the severity of the event that an alarm occurs for. (It is possible to specify multiple events)
Trap	SNMP traps sent from monitored nodes Based on the MIB information registered within ISM-VA, a list of receivable traps is displayed. Severity or individual traps are specified. Specify the severity of the trap that an alarm occurs for or specify this trap. If you select [System] in [Applicable Type], it will not be displayed.

Modification No.14
2.2.2 Monitoring

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 planned 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 the occurrence of alarms from being issued repeatedly for the node.

  For information on Maintenance Mode, see "5.1 Maintenance Mode."

Modification No.15

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 On the GUI of ISM, this is indicated by a blue 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 check the contents of the detected event.

When you have completed checking 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.

Registering MIB Files

The method of registering MIB files in ISM, as well as the methods of checking and deleting the registered MIB files are described. Note the following points for the MIB files to be registered.

Do not register multiple MIB files for which the same trap is defined. If you have registered multiple MIB files with the same trap defined, this is handled as if several of the same traps were received.

About MIB Files

The MIB file is an information that the network device managed by SNMP discloses to notify its status to outside, and it is standardized as MIB2 specified in RFC1213. The MIB file stands for a text-based file that defines the disclosed information. In order to exchange the SNMP traps, the receiving side needs to maintain the MIB file provided by the device side.

Add/Update the MIB file in the following cases.
- When adding a new MIB file to receive SNMP traps from Fujitsu external device.
- When updating the MIB file that has been registered in ISM due to firmware update.

1. Prepare an MIB file. Note that all the relevant files are necessary if the MIB file has any dependency relationship.
2. Connect to ISM-VA via FTP and transfer the MIB file.
3. Execute the MIB registration command from ISM-VA Management.
   For details, see "4.19.1 Registering MIB Files."

Note

- Although the registered MIB file can be deleted, when an SNMP trap defined in the detected MIB file is received, it is processed as an unknown trap.
- Do not register multiple MIB files with the same trap defined. When multiple MIB files with the same trap are registered, they are handled as if they received the same trap multiple times.

Registering MIB Files

You can add a new MIB file that has not yet been registered in ISM.
1. Prepare the MIB file. Note that all the relevant files are necessary that have dependency relationship with MIB files.
2. Connect to ISM-VA via FTP and transfer the MIB file.
3. Execute the MIB registration command from ISM-VA Management.

For details, see "4.19.1 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.

Checking MIB Files

You can check the names of MIB files registered in ISM using a list. To check the list of MIB file names, execute the MIB reference command for ISM-VA Management.
For details, see "4.19.2 Registering MIB Files."

Deleting MIB files

To deactivate the MIB files registered in ISM, you can delete the appropriate MIB files. To delete the MIB files, execute the MIB deletion command of ISM-VA Management.
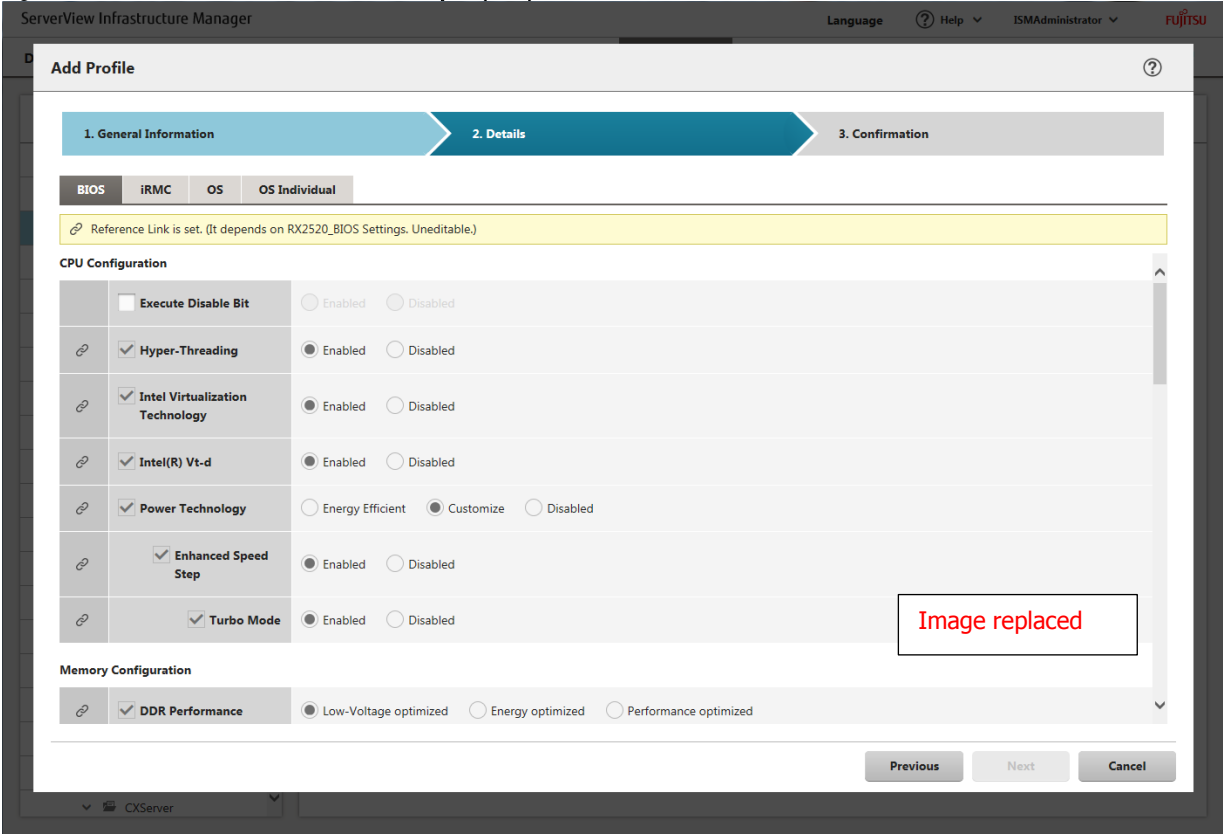For details, see "4.19.3 Deleting MIB Files."

Note

Whenever you delete an MIB file, you should pay attention to its dependency relationship. If you have deleted the MIB file having a dependency relationship(s), this could result in disabling receiving traps.

Modification No.16

2.2.3 Profile Manager

Sample profile

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

Modification No.17
2.2.3 Profile Manager
Procedure for editing and reassigning profiles

Executable user	Administrator group			Other groups		
	Admin	Operator	Monitor	Admin	Operator	Monitor

You can modify node settings by changing 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" are described in the profile, these items cannot be modified.

You can re-modify the contents of a profile while it is assigned to a node. When you do so, however, changes to the profile do not immediately carry over into changed node settings. For the time being, ISM handles this status as a mismatch between profile contents and node settings.

Reassign the re-modified 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.

Modification No.18

2.2.3 Profile Manager

Required preparations before OS installation

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

  If you are going to import an ISO image of the OS installation media, 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 necessary to import it separately for each 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 for each user group.

  For details, see "2.3.2 Repository Management."

- Use the PXE boot function on the target node. Let the network connections and the BIOS settings of the target server complete in advance, so as to enable PXE booting from the onboard LAN or LAN card. 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.

Modification No.19

2.2.3 Profile Manager

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, 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 in this case.

- Execute 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.

- 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.

Modification No.20
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 "2.2.1.1 Registering Datacenters/Floors/Racks/Nodes" - "Management of node information."

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

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

4. Check the [Current Version] field.

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

Point

As the number of nodes displayed on [Node] screen increases, it takes one to several minutes until the screen is displayed after switching [Column Display] field to [Firmware].

In this case, you can reduce the time taking for display the screen by limiting the number of nodes handled by a login user to within approximately 200 nodes.

The number of nodes handled by a login user can be set using the Node Group and User Group functions.

For details on Node Group function, see "2.3.1 User Management."

Moreover, when the list of firmware versions of all nodes is unnecessary for you in checking the version of a specific node, display "Details of Node" screen of your intended node, and then switch it to [Firmware] tab, so that you can check the firmware version of your intended node in a short time.

Modification No.21

2.2.4.2 Updating Firmware

Here, the following points are described:

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

For details on the operations for transferring firmware data to the repository, see "2.3.2 Repository Management."

Modification No.22

2.2.4.2 Updating Firmware

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.

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.
Switch Storage	Implement the firmware update with the node power remaining on. After the firmware update, you may have to reboot the node.

Modification No.23
2.2.4.2 Updating Firmware
Implementing firmware updates
Note

- While an update is in progress, please observe the following notes.
    - Do not power off the target node.
    - 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 ~~firmware files~~ import data or firmware data from the repository.
- Before you start any firmware update, check 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 information on importing firmware data, 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 registering OS information of nodes, see "2.2.1.1 Registering Datacenters/Floors/Racks/Nodes" - "Registration of node OS information." Also note that firmware updates of PCI cards are supported only for the following OS types:
    - CentOS
    - Red Hat Enterprise Linux

- Firmware updates for PCI cards mounted on servers are executed for all mounted cards of the same type.

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

- ~~For implementing a firmware update of any of the following PCI cards, the Emulex OneCommand Manager CLI must be installed on the servers on which these PCI cards are mounted.~~

    ~~Firmware names: : LPe1250, LPe12002, LPe16000, LPe16002, OCe10102, OCe14102~~

    ~~For information on installing the Emulex OneCommand Manager CLI, see "2.3.3 Installing Emulex OneCommand Manager CLI and Qlogic QConvergeConsole CLI."~~
- ~~For implementing a firmware update of any of the following PCI cards, the Qlogic QConvergeConsole CLI must be installed on the servers on which these PCI cards are mounted.~~

    ~~Firmware names : QLE2560, QLE2562, QLE2670, QLE2672~~

    ~~For information on installing the Qlogic QConvergeConsole CLI, see "2.3.3 Installing Emulex OneCommand Manager CLI and Qlogic QConvergeConsole CLI."~~
- For implementing a firmware update of Fujitsu PCI cards (FC/CNA/LAN cards) on Linux, Emulex OneCommand Manager CLI or QLogic QConvergeConsole CLI must be installed on the OS of the target server.

    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 ~~the following PCI cards~~ some nodes and PCI cards, the formats of the version numbers are different in the Current Version and the Latest Version columns, respectively.

    ~~Firmware names: QLE2560, QLE2562, QLE2670, QLE2672~~

    ~~The Current Version column displays <Firmware Version>_<BIOS Version>, whereas the Latest Version column displays <BIOS Version>.~~ For applicable nodes and PCI cards, and for how they are displayed, access your local support.

- In performing firmware update, you must apply firmware to some nodes in stepwise manner. See the documents attached to each firmware data.

- After updating 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, check 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.

Modification No.24

2.2.4.3 Checking Documentation that Is Supplied with Firmware Data

When you update the firmware, check 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 [Update Version] and [Repository Import Data], and then click the [Next] button.

5. In the [Document URL] field, select the URL and check the desired 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.

Modification No.25

2.2.5 Log Manager

Types of collectable logs

Log Manager 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 Manager 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 "export log" command Output results for "show events" command	Output results for "show events" command
Switch	SR-X	Output results for "show tech-support" command	Output results for "show logging syslog" command (Included in output results for "show techsupport" command)
	VDX	Various files created with the "copy support" command	Output results for "show logging raslog" command Output results for "show logging audit" command (Included in "<Any text string as needed>.INFRA_USER.txt.gz" file created with the "copy support" command)

Modification No.26

2.2.5 Log Manager

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 maximum size of stored log files is set to 10 GB each for Archived Logs, node logs (data for download), and node logs (data for log search). This setting value cannot be changed.~~ The upper limit for the total size (i.e., Size restriction) of various log files (i.e., 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 "User Groups" screen. For details on "User Groups" screen, see "2.3.1.2 Managing User Groups." ~~When any of these log file sizes~~ 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 ~~retrieved~~ stored.

To allow for ~~retrieving~~ storing 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: In a situation where the upper limit specified 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.	- 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: 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: In a situation where the upper limit specified value is 10GB, if the total size of the log files exceeds 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"

Modification No.27
2.2.6 Network Manager

Network Manager is a function that is mainly used for the following purposes:
- Checking information on physical network connections and port information between managed nodes
- Checking of changes in information on network connections between managed nodes
- Checking the virtual connections of the physical ports, the virtual switches and the virtual machines of the managed node
- Checking VLAN and ~~LAG~~ Link Aggregation settings and changing their settings

Modification No.28
2.2.6 Network Manager
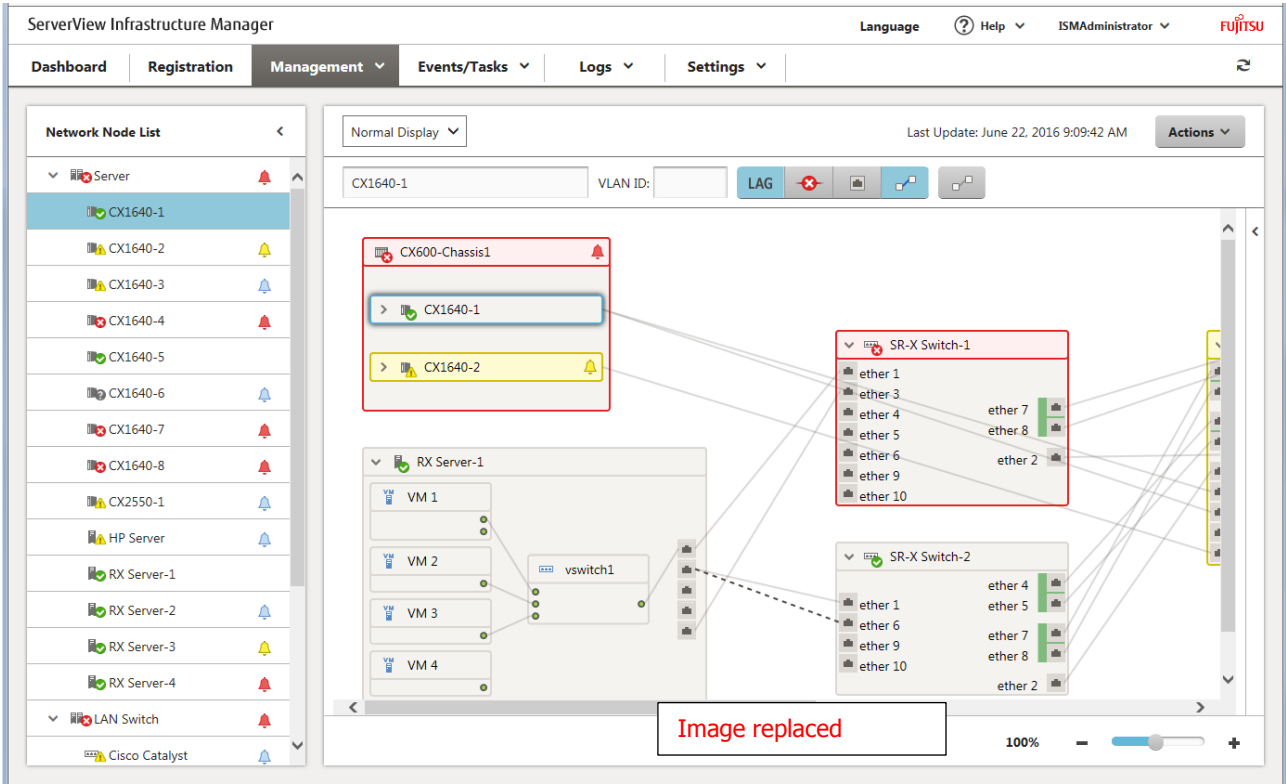
Modification No.29

2.2.6 Network Manager

Here, the following points are described:

- Displaying network connection information
- Updating network management information
- Checking information on changes in network connections
- Setting reference information for changes in network connections
- Checking VLAN and ~~LAG~~ Link Aggregation settings
- Changing VLAN settings
- Changing Link Aggregation settings
- Setting network connection information manually

Modification No.30

2.2.6 Network Manager

Displaying network connection information

Executable user	Administrator group			Other groups		
	Admin	Operator	Monitor	Admin	Operator	Monitor

You can graphically check the connection information on networks between managed nodes in a connection diagram (Network Map).

Easy operations allow you to display detailed information about each managed node, including the current statuses of their ports. Also, you can check the connection relationships between servers and network switches on a single screen. Likewise, you can also check the connection relationship between a virtual machine(s)/virtual switch(s) in a server and a physical port.

Modification No.31

2.2.6 Network Manager

Displaying network connection information

Point

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

- As the number of managed nodes screen increases, it takes one to several minutes to display the [Network Map] screen.

  In this case, you can reduce the time taken for displaying by limiting the number of nodes, handled by a login user, approximately within 200 nodes.

  The number of nodes handled by a login user can be set using the Node Group and User Group functions. For details on Node Group function, see "2.3.1 User Management."

Modification No.32

2.2.6 Network Manager

Displaying network connection information

Note

- LLDP (Link Layer Discovery Protocol) is used for retrieving information on 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 check whether the LLDP settings of the node are enabled or disabled, check the technical specifications of each respective node.

- The displayed ~~connection diagram~~ 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 check the most recent status after registering nodes, modifying any connections, or after an error, click the [Actions] button and execute [Refresh Network Information]. Likewise, whenever the hardware configuration of a node ~~was~~ is 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 managed nodes on ISM and to register the OS information of the managed nodes. For 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."

Modification No.33

2.2.6 Network Manager

Updating network management information

Executable user

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

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

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. Click 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

- Depending on the number of managed nodes, updating the network management information may take some time to complete. To confirm that the information update is complete, check the event in the Operation Log under Events/Tasks that indicates completion of the information update.

- The time of the latest update of the network management information is displayed in the upper right part of the Network Map. This latest update time indicates the time when the latest 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.

Modification No.34

2.2.6 Network Manager

Checking information on changes in network connections

Executable user

Administrator group			Other groups		
Admin	Operator	Monitor	Admin	Operator	Monitor

Checking information on changes in network connections

On the Network Map, you can check 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" is displayed for connections that were recently added and other newly detected connections. ~~In the connection diagram,~~ "Added" connections are displayed, as bold lines, on the Network Map.

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

Modification No.35

2.2.6 Network Manager

Checking information on changes in network connections

Point

The Last Update of [Confirm connection state change] is the currently set reference point in time.

Note

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

Modification No.36

2.2.6 Network Manager

Setting reference information for changes in network connections

	Administrator group			Other groups		
Executable user	Admin	Operator	Monitor	Admin	Operator	Monitor

The displayed information on changes in network connections is based on the changes ("Add" and "Delete") after a given reference point in time, and you can modify this reference point in time. You have 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 ("Add" and "Delete") 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 Manager 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 check.
   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. Click the [Actions] button and select [Confirm connection state change]. The Last Update is the currently set reference point in time.
4. Click the [Refresh] button.
   A confirmation screen is displayed.
5. Check the contents and click the [Yes] button.
   The reference point is updated to the time when you executed the [Update] operation.

Point

The reference settings for information on changes in network connections are updated automatically ~~when ISM services start up~~ only at the initial startup of ISM services.

Modification No.37

2.2.6 Network Manager

Checking VLAN and ~~TAG~~ Link Aggregation settings

Administrator group			Other groups		
Executable user	Admin	Operator	Monitor	Admin	Operator	Monitor

You can visually check the current settings of VLANs and ~~TAGs~~ Link Aggregations that are set up on network switches on ~~a dedicated GUI~~ the Network Map screen.
~~On In~~ the Network ~~connection diagram~~ Map, you can check ~~the settings~~ visually.

Operating procedure (example for VLAN)

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 Manager 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 check.
   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. ~~Click the [Actions] button and select [VLAN Display] - [Enable].~~ Enter the VLAN ID you want to display, in the VLAN ID text box.
4. ~~Enter the VLAN ID you want to have displayed, and then click the [Display] button.~~

Operating procedure (example for ~~TAG~~ Link Aggregation)

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 Manager 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 check.
   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 [Link Aggregation].~~
   Clicking the [>] icon of a node on the Network Map expands the port(s) within the node, and the settings of Link Aggregation are displayed.

Modification No.38
2.2.6 Network Manager

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. The Network Map is displayed at the center of the screen.
   When you open the Network Map, the uppermost node in the Network Node List on the upper left side of the screen has been pre-selected, and then select the node that serves as the connection point of the network that you want to set up.
3. From the pull-down menu displayed at the upper left part of the Network Map, select [Multiple Setting].
4. Click the [>] icon of the nodes in the Network Map to display the ports in the node, and click the checkbox of 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, edit the contents, and then click [Confirm] button.
6. Check the changed contents of the setting. Clicking [Register] button changes the VLAN setting.

Note
━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━

- VLAN settings have their own specifications and therefore may differ depending on the model of network switches. Make settings after checking 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).
- Depending on the model of the network switch, a reserved VLAN ID(s) might exist. You cannot change the settings of reserved VLAN ID. See the specifications of respective nodes.

━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━

Changing Link Aggregation (LAG) 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.
   When you open Network Map, the uppermost node in the Network Node List is already selected. Network Map is displayed at the center of the screen.
3. Select [LAG setting] from the [Actions] button.
4. Select the name of the target node for which you want to set up a Link Aggregation and select [Add] of LAG (Link Aggregation) Setting.
5. Enter the LAG Name and Mode, select the checkbox of the port for which you set the Link Aggregation, and then click [Confirm] button.
6. Check the setting contents of the Link Aggregation and click the [Register] button.

Note
━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━

- Link Aggregation settings have their own specifications and therefore may differ depending on the model of the network switches. Make settings after checking the device specifications.
- The LAG Name that can be set differs depending on the model of the network switch. For the scope of the names that can be set, see the specifications of respective nodes.
- The Mode that can be set differ depending on the models of network switches. For the modes that can be set, see the specifications of respective nodes.
- You cannot set up a Link Aggregation between ports having different VLAN IDs. Be sure to check that these ports have the same VLAN settings to change the Link Aggregation settings then do the settings.

- Whenever you set up an MLAG between different nodes, you need to change Link Aggregation settings for respective switches.

Modification No.39

2.3.1 User Management
2.3.1.2 Managing 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 upper limit for the total size of the files used by the user group and the warning threshold value of the alert.

Usage	Size Restriction	Threshold Monitoring

Across user group	- When enabled:
	
	Specify the total size of the files used by the user group to [Maximum Size (MB)] with the value in units of MB.
	The total size of the files indicate the sum of the following data.
	  − Repository
	  − Archived Log
	  − Node Log
	  − Files imported via FTP in ISM-VA
	
	If the actual usage size exceeds the specified [Maximum Size (MB)], an error message is output to the Operation Log. Even when the [Maximum Size (MB)] value is exceeded, this does not affect the operations of the Repository, Archived Log, and Node Log.
		- When enabled:
		
		~~Set~~ Specify the threshold value outputting an alert message to the Operation Log to [Warning threshold (%)]. Specify the value in units of %.
		- When disabled:
		
		The alert message is not output to the Operation Log.

Repository	- When enabled: Specify the total size of the files imported to Repository to [Maximum Size (MB)] with the value in units of MB. If the total usage size of the imported files exceeds the specified [Maximum Size (MB)] value, an error occurs when executing Repository results and an error message is output to the Operation Log.	You cannot specify the value.
Archived Log	Specify the total size of Archived Log to [Maximum Size (MB)] with the value in units of MB. If the total size of the Archived Log exceeds the specified [Maximum Size (MB)], newly created logs are not stored in Archived Log and an error message is output to the Operation Log. Furthermore, if the setting value of [Maximum	Specify the threshold value outputting the alert message to Operation Log to [Warning threshold (%)]. Specify the value in units of %.

	Size (MB)] remains stored as [0] default setting, Archived log is not stored, and error messages are output to the Operation Log each time.	
Node Log	You can specify the total size of the download data and log search data in [Maximum Size (MB)] with the value in units of MB. (You can specify the size of the log search data only for the Administrator group.) If the total size of either the download data or the log search data exceeds the specified [Maximum Size (MB)], neither data is output, and an error message is output to the Operation Log. Furthermore, if either or both data of the setting value remains stored as [0], default setting, neither data is output, and an error message is output to the Operation 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 (%)]. Specify the value in units of % An alert 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, see 3.2.1 "Estimation of Disk Resources."

- Select a node group.
  Create correlations between user groups and node groups as necessary 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.
- After creating a user group, immediately implement the procedure described 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 the directory size of Adding user groups.
   - Select a node group.
   Create correlations between user groups and node groups as necessary by selecting a node group.

Note

- You cannot change the group names of Administrator groups.
- You can only specify "ISM" as the authentication method for 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.

Modification No.40
2.3.1.3 Operating in Link with Microsoft Active Directory or LDAP
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: - For LDAP: uid - For Microsoft Active Directory: sAMAccountName Bind DN Specify the accounts that can be searched on the directory server
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.

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	User Group Name Specify the name of the user group you prepared in Step 4.

6. Check 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.

Modification No.41

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 data that are used for firmware updates
    These are used by the "Firmware Manager" and "Profile Manager" functions.
  - Storing of OS installation media that are used for installing OSes
    These are used by the "Profile Manager" function.
  - Storing of ServerView Suite DVD data that are used for installing OSes
    These are used by the "Profile Manager" function.

Point

Allocate virtual disks of ISM-VA to the disk area of the repository. For information on how to allocate virtual disks, see "3.2.1.2 Estimation of Required Capacities for Repositories" and "3.7 Allocation of Virtual Disks."

Note

If the disk area in a repository is not enough, this results in a failure to store the various data for repository management. See "3.2.1.2 Estimation of Required Capacities for Repositories ", "3.7 Allocation of Virtual Disks", and "2.3.1.2 Managing User Groups" to allocate a sufficient disk area to the repository.

Modification No.42
2.3.2 Repository Management

Storing firmware data

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 details on how to forward the folder, see "2.1.2 FTP Access."

2.   From the Global Navigation menu on the GUI screen 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 [Repositories Import Data List] tab and select [Import DVD].

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

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

Deleting firmware data from repository

-   If firmware data were stored in repository from DVD:

    1.   In the [Column Display] field, s Select [Repository Import Data List] tab.

    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 were stored in repository from FUJITSU website:

    1.   In the [Column Display] field, s Select [Firmware Data] tab.

    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

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

Locations for obtaining firmware ~~images~~ data

Download the firmware data for each respective model from the following websites.

Target firmware	Firmware type	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://www.fujitsu.com/jp/products/network/download/sr-x/firm/
	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 firmware updates.

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

1. Get ~~a~~ firmware ~~image~~ data from a location for obtaining firmware ~~images~~ data.

2. If you are not going to use an ISO image file, you can store the downloaded file in any folder that suits you best.

If the downloaded file is a compressed file, decompress it within the folder.
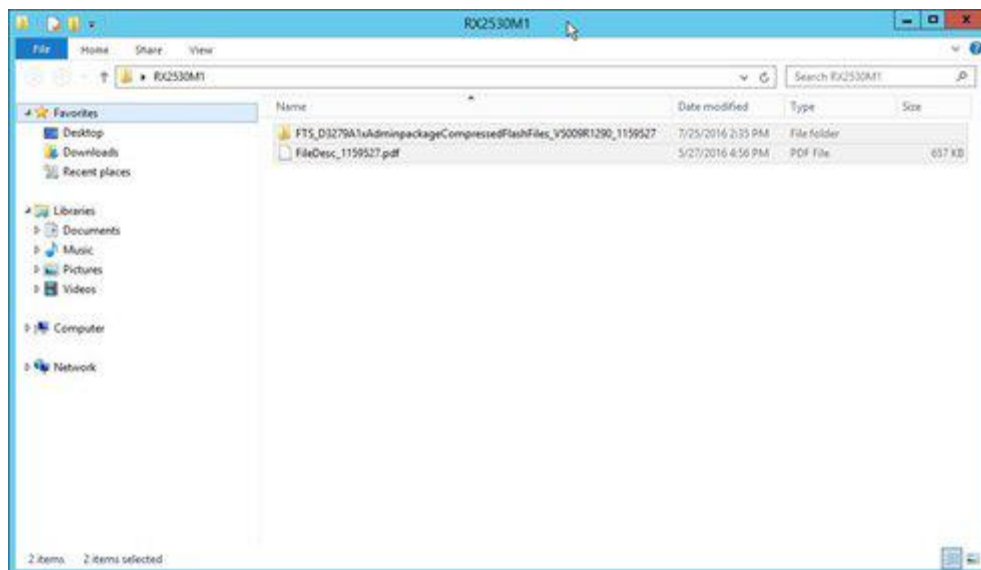
3. Use FTP to forward the data to ISM-VA.

   − Use FTP commands or FTP client software (such as FFFTP or WinSCP) to forward the data. 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.

64

- 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] - [Repository].

   b. Execute one of the following

      - For importing an ISO image file into the repository, click the [Actions] button under [~~Repositories~~ 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 [~~Firmware~~ [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]
	~~LPe1600, LPe16002~~ LPeXXX except for LPe1250 and LPe12002	Firmware version [Note 2]
	~~QLE2560, QLE2562, QLE2600, QLE2602~~ 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]
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. Check the current status of the task on the "Task" screen.

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

Modification No.43

2.3.3 Installing Emulex OneCommand Manager CLI and Qlogic QConvergeConsole CLI

Note

- For implementing a firmware update of a FUJITSU 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.

  Model names that require installation of the Emulex OneCommand Manager CLI are as follows:

  PG-FC203, PGBFC203, PG-FC203L, PGBFC203L, PG-FC204, PGBFC204, PG-FC204L, PGBFC204L, PY-FC201, PYBFC201, PY-FC201L, PYBFC201L, PY-FC202, PYBFC202, PY-FC202L, PYBFC202L, PY-FC221, PYBFC221, PYBFC221L, PY-FC222, PYBFC222, PYBFC222L, PY-CN302, PYBCN302, PYBCN302L, PY-CN202, PYBCN202, PY-CN202L, PYBCN202L,PY-LA3A2, PYBLA3A2, PYBLA3A2L, PY-LA3B2, PYBLA3B2, PYBLA3B2L

  Model names that require installation of the QLogic QConvergeConsole CLI are as follows:

  PG-FC205, PGBFC205, PG-FC205L, PGBFC205L, PG-FC206, PGBFC206, PG-FC206L, PGBFC206L, PY-FC211, PYBFC211, PY-FC211L, PYBFC211L, PY-FC212, PYBFC212, PY-FC212L, PYBFC212L, PY-FC311, PYBFC311, PYBFC311L, PY-FC312, PYBFC312, PYBFC312L

  For PCI cards that require installation of Emulex OneCommand Manager CLI and QLogic QConvergeConsole CLI, contact 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.

Modification No.44
2.3.5.1 List of Commands in ISM-VA Management

Maintenance

Function	Command
Collect maintenance logs	ismadm system snap
Show system information	ismadm system show
Apply patch	ismadm system patch-add
Apply plugin	ismadm system plugin-add
Modify host name	ismadm system modify
Switch trouble investigation logs	ismadm system set-debug-flag
Set SNMP community name	ismadm snmp

Modification No.45
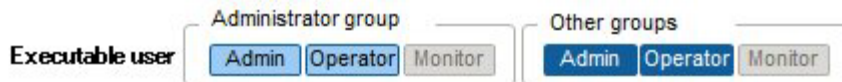## 2.3.5.1 List of Commands in ISM-VA Management

MIB file settings

Function	Command
Register MIB files	ismadm mib import
Show MIB files	ismadm mib show
Delete MIB files	ismadm mib delete

Modification No.46

2.3.6 Management of Cloud Management Software

When you use the functions in link with cloud management software, you register cloud management software with ISM.

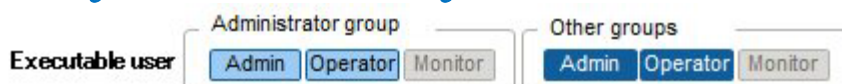### Registering Cloud Management Software

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 [Register].
3. Enter the information that is required for registration.
    - Cloud Management Software Name
       Set a name that is unique across the entire ISM system.
    - IP Address
       Set the IP address of the cloud management software.
       Register the cluster virtual IP 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.
    - Account Information
       Set the domain name, [Account Name], and [Password] for the CMS.
       Enter the domain name by using uppercase letters. If the CMS is joined to the domain, also set the [Domain Name].
    - URL
       Set the URL for accessing the web management screen for the cloud management software.
       If you specify a virtual management software that provides a web management function for [Type], set the URL for accessing the web management screen.
    - 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.

Note

If you specify Microsoft Failover Cluster as [Type], make sure to set the [Domain Name].

Retrieving Information from Cloud Management Software

In ISM, the following information can be retrieved from the registered cloud management software at intervals of 24 hours.

・ Virtual Machine Information

The retrieved virtual machine information is managed in correlation with the OS information of the node registered with ISM. The virtual machine information of each retrieved node can be checked on the [Virtual Machines] tab of the "Details of Node" screen.

Finally, the time of information retrieval from the cloud management software is displayed in [Last update time]. This is not displayed if information retrieval has not been executed before.
To retrieve the information from the cloud management software manually, execute the following procedure.
1. From the Global Navigation menu on the GUI of ISM, select [Settings] - [General Settings] - [Cloud Management Software].
2. Click the [Get CMS Info] button to execute the information retrieval.
As soon as retrieval of the information is complete, a log with the Message ID "10020503" is output to the event log.

Note

If you delete a virtual machine from Hyper-V Manager in the environment of using Microsoft Failover Cluster, also delete the virtual machine from Roles of the Failover Cluster Manager.

Editing Cloud Management Software

Executable user

Administrator group			Other groups		
Admin	Operator	Monitor	Admin	Operator	Monitor

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

Executable user

Administrator group			Other groups		
Admin	Operator	Monitor	Admin	Operator	Monitor

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.

Modification No.47

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, and SVS DVD data, ~~and firmware data~~ from the repository.
- Delete any schedules for log collection.
- Delete any saved logs.

Modification No.48
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

Modification No.49

3.1 Workflow for Installing ISM

(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
- ~~Configuration of~~ Network design
- Setting node ~~names and profile~~ names
- User Settings

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

3.1 Workflow for Installing ISM

(6) Allocation of Virtual Disks

Allocate virtual disks in order to expand the disk capacities of ISM-VA.

For information on the tasks necessary 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.

Modification No.51
3.1 Workflow for Installing ISM

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."

Modification No.52
3.2.1.2 Estimation of Required Capacities for Repositories
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 necessary to estimate the required disk capacities (otherwise 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 necessary to estimate the required disk capacity on the LVM volume in the system area.

Modification No.53

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.

3.2.3 Network Design

Note

- ISM-VA starts by default while the IP address "192.168.1.101" remains enabled. Be careful about overlapping with IP addresses of the other devices within the network.

    You can avoid such IP address overlap by changing the IP address in the following procedure if an overlapped IP address is found.

    1. Install ISM-VA on a hypervisor other than the one in the actual environment.
    2. Change the IP address of ISM-VA.
    3. Back it up according to the procedure described in "4.3.1 Backingup ISM-VA."
    4. Restore the ISM-VA that was backed up with hypervisor in the actual environment, according to the procedure described in "4.3.2 Restoring ISM-VA.

Modification No.55
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 ~~use~~ a maximum of 64 ~~alphanumeric~~ characters, ~~hyphen (-), and underscore (_)~~ for each node name.
Note, however, that you cannot use the following characters.

Slash (/), Backslash(\), colon (:), Asterisk (*), Question mark (?), Double quotation ("), Angle brackets (<>), or Pipeline (|)

Modification No.56

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.
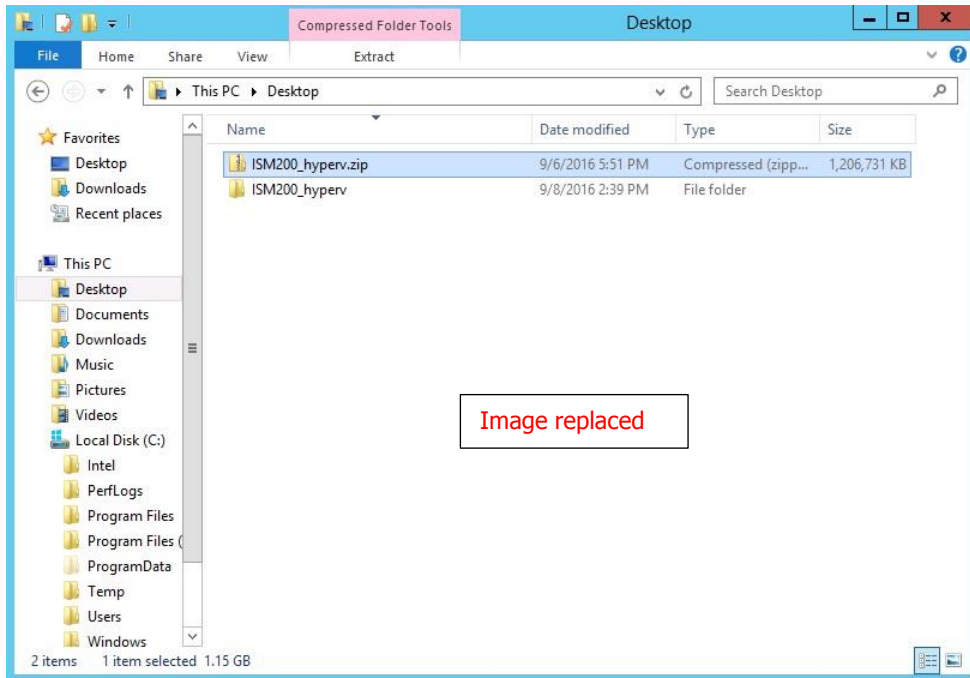
2. Start Hyper-V Manager, right-click on the Windows server to be used as the Hyper-V host, and then select [Import Virtual Machine].
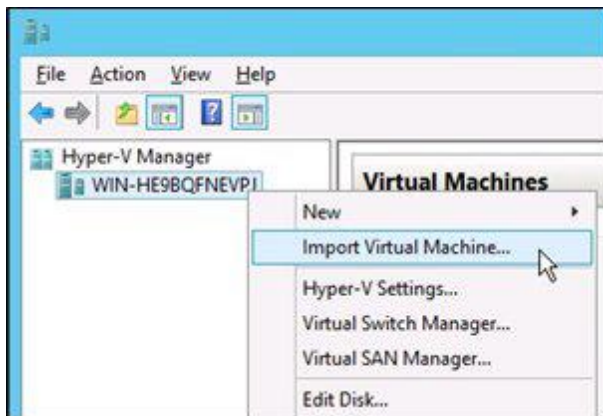
3. On the "Select Folder" screen, select the directory in which you deployed the file in Step 1.

The directory to be selected is the parent directory of the directories "Snapshots," "Virtual Hard Disks," and "Virtual Machines."
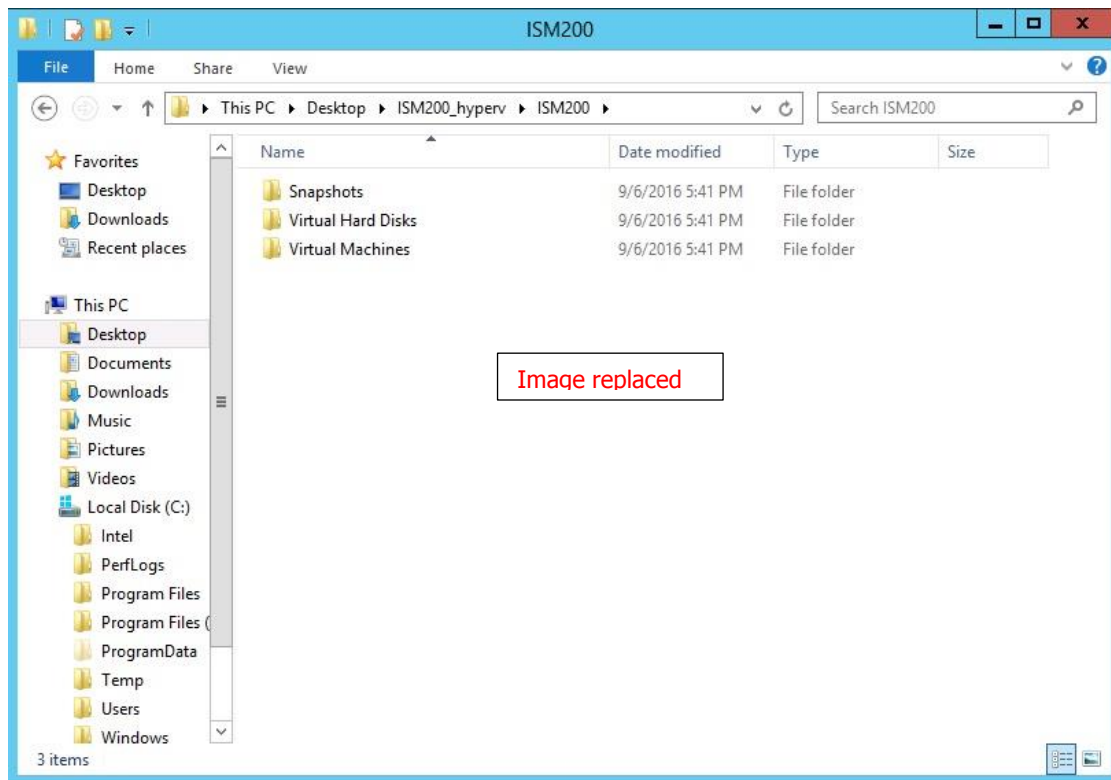
Modification No.57
3.3.2 Installing on VMware vSphere Hypervisor
For installation, use the ova file that is included in the DVD media.
1.   Start vSphere Client and select [Deploy OVF Template] from the [File] menu

2.   On the source selection screen, select the ova file that is included in the DVD media, and then click [Next].
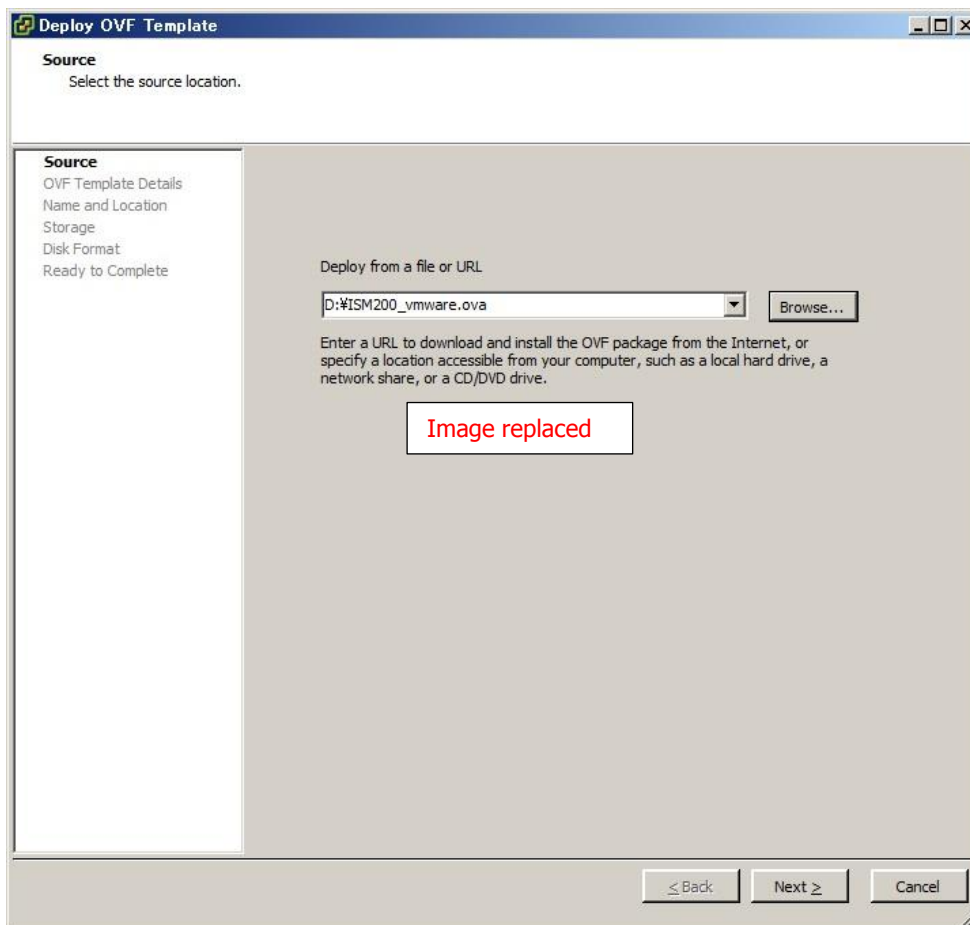
Modification No.58

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 ~~ISMV200si421~~ISM200_kvm.tar.gz
    ~~ISMV200si421~~ISM200_kvm/
    ~~ISMV200si421~~ISM200_kvm/~~ISMV200si421~~ISM200_kvm.qcow2
    ~~ISMV200si421~~ISM200_kvm/~~ISMV200si421~~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 ~~ISMV200si421~~ISM200_kvm.qcow2 /var/lib/libvirt/images
        ```

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

        ```
        # cp ~~ISMV200si421~~ISM200.xml /etc/libvirt/qemu
        ```

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

    ```
    # virsh define /etc/libvirt/qemu/~~ISMV200si421~~ISM200.xml
    ```

4. Click on [Virtual Machine Manager] to open Virtual Machine Manager.
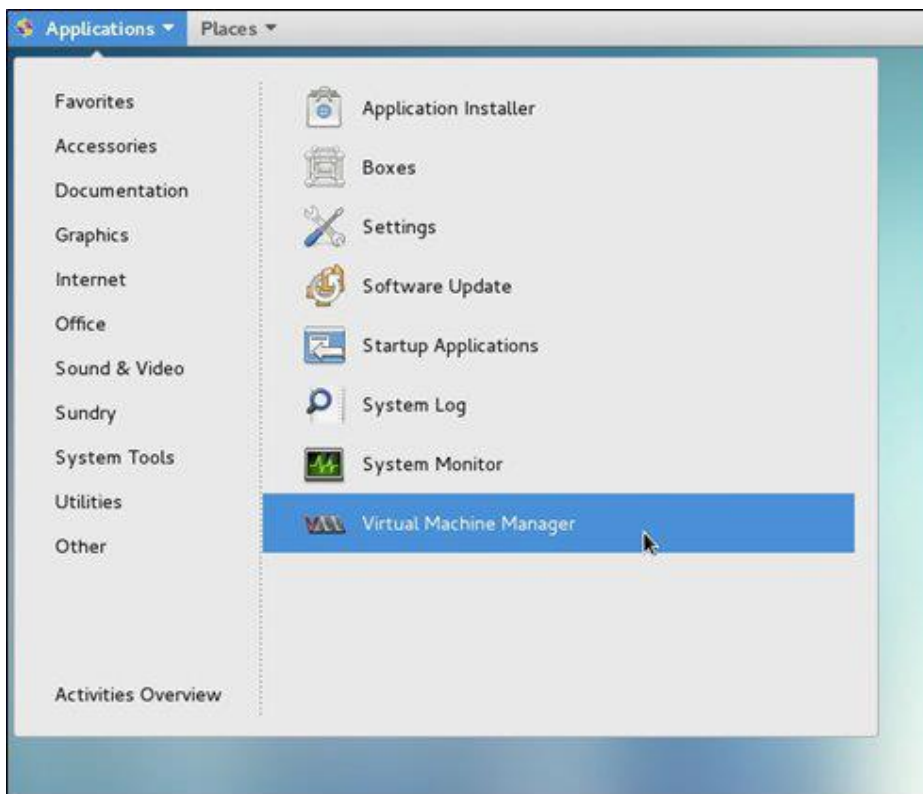
5. In Virtual Machine Manager, select ISM-VA, and then click [Open].
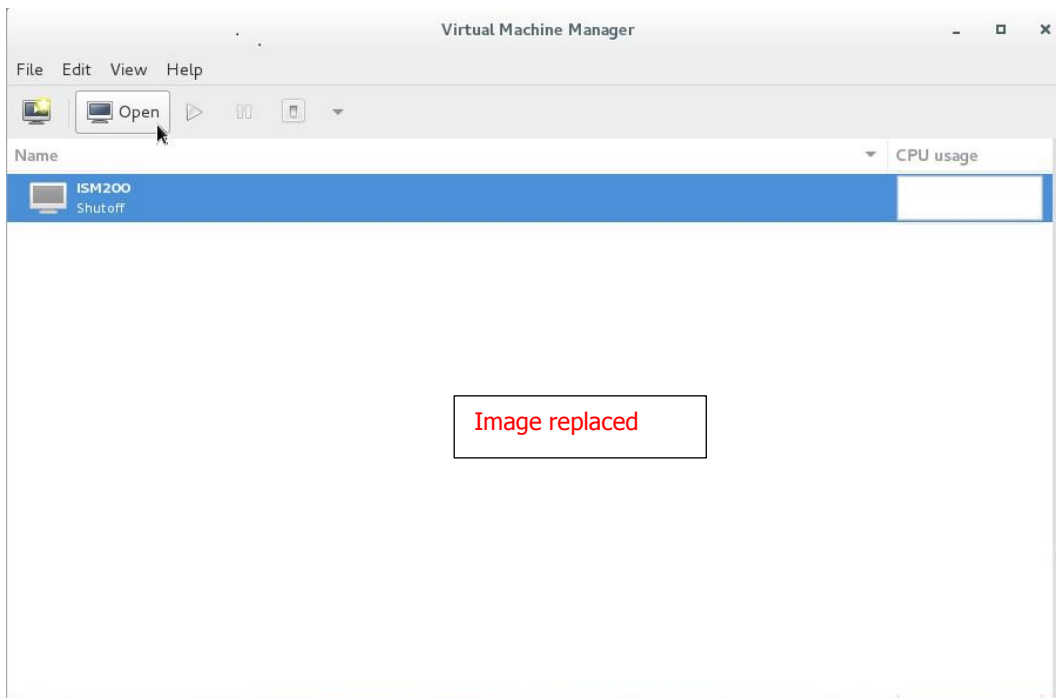
6. On the "ISM-VA Virtual Machine" screen, select [Details] from the [View] menu.
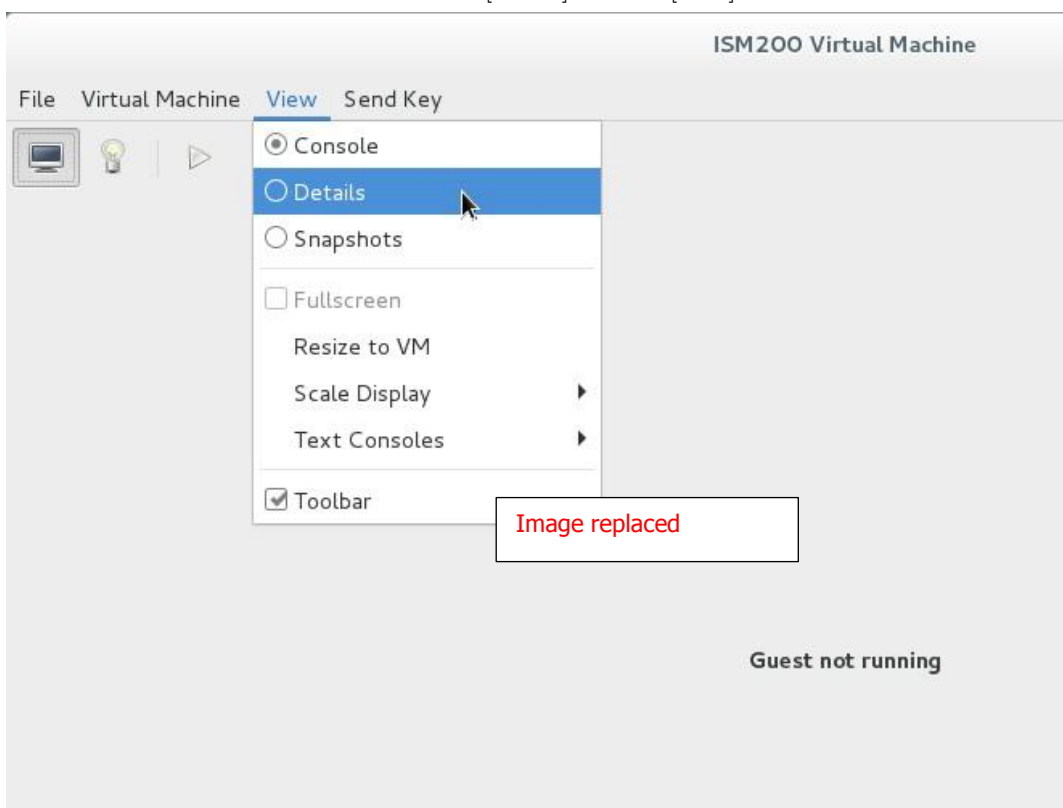
7. On the details screen for ISM-VA, select [NIC] and the virtual network or host device to which to connect ISM-VA, and then click [Apply].
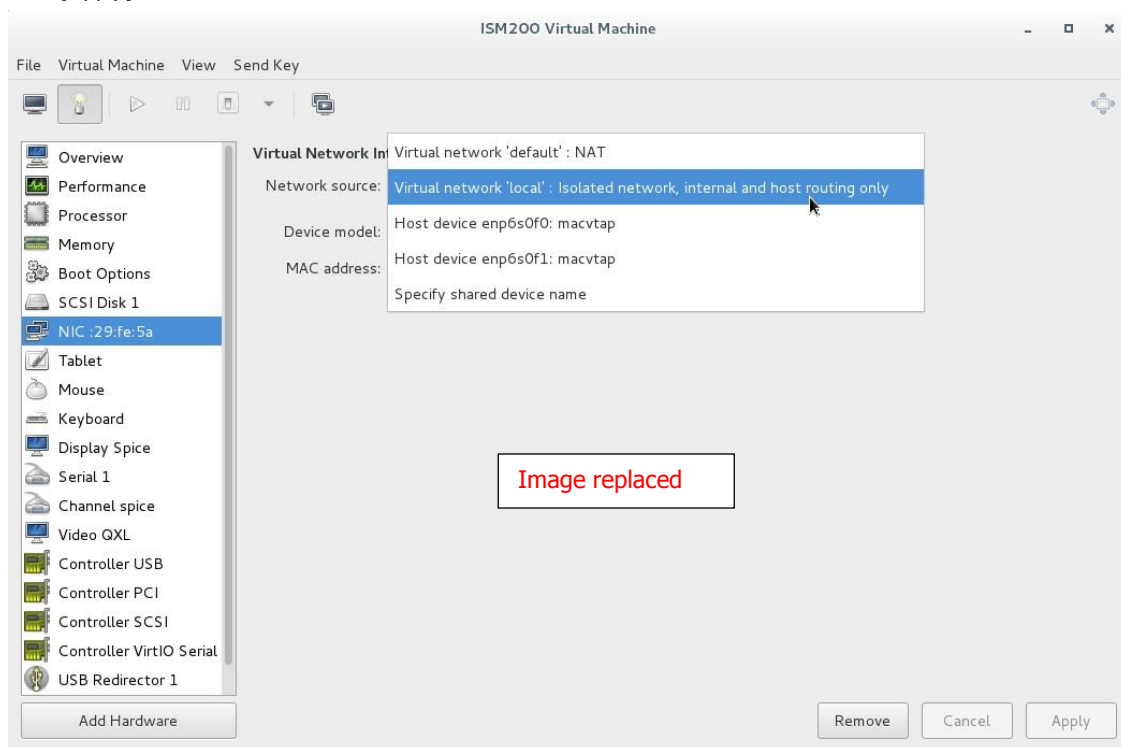
Modification No.59

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].
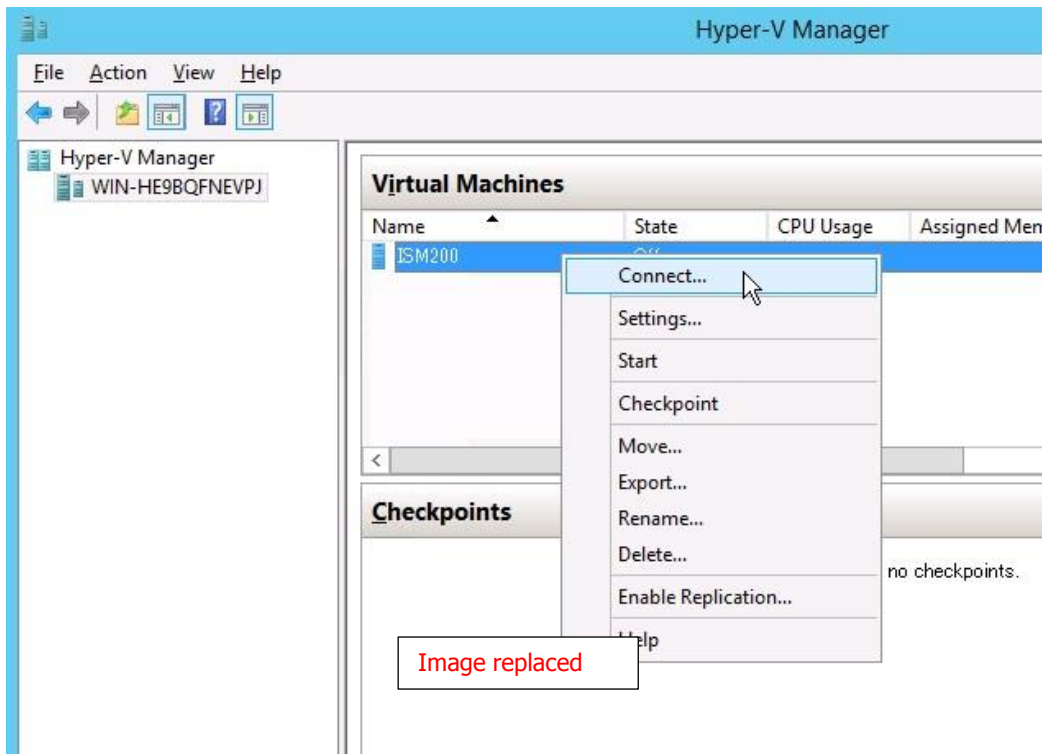
2. On the "Virtual Machine Connection" screen, select [Start] from the [Actions] menu to start ISM-VA.
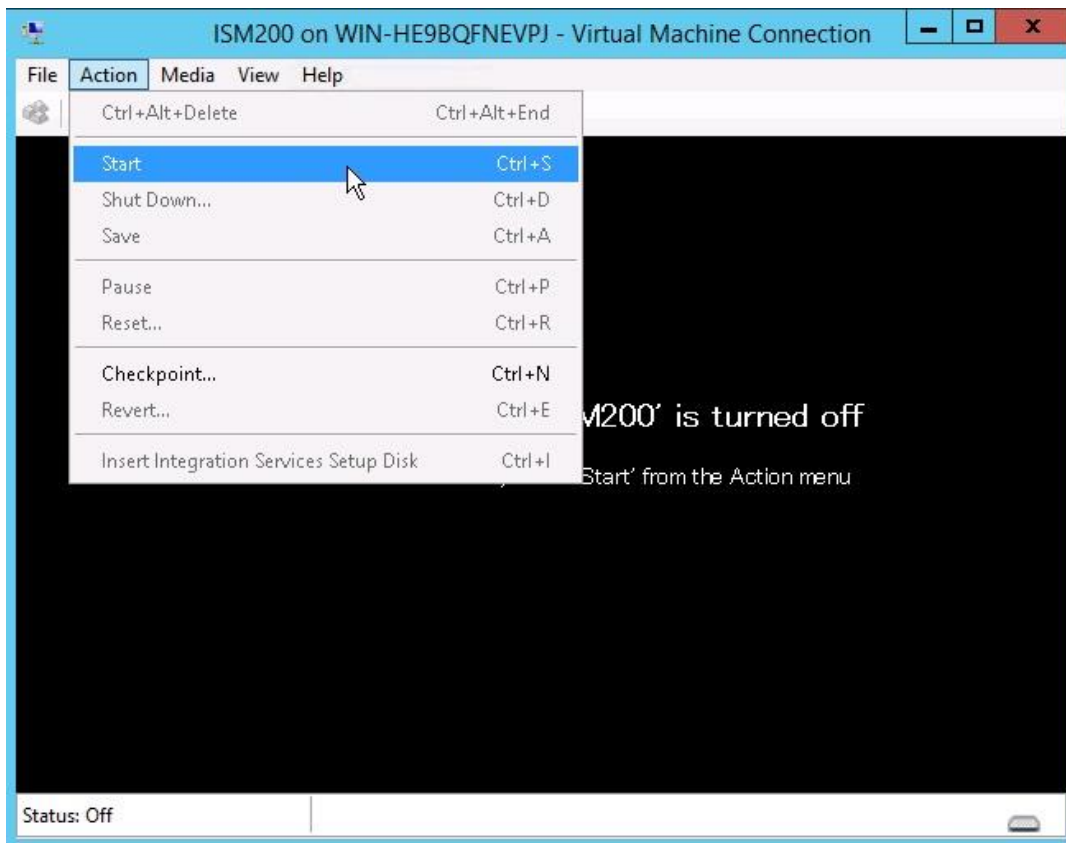
Modification No.60

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.

Modification No.61

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].
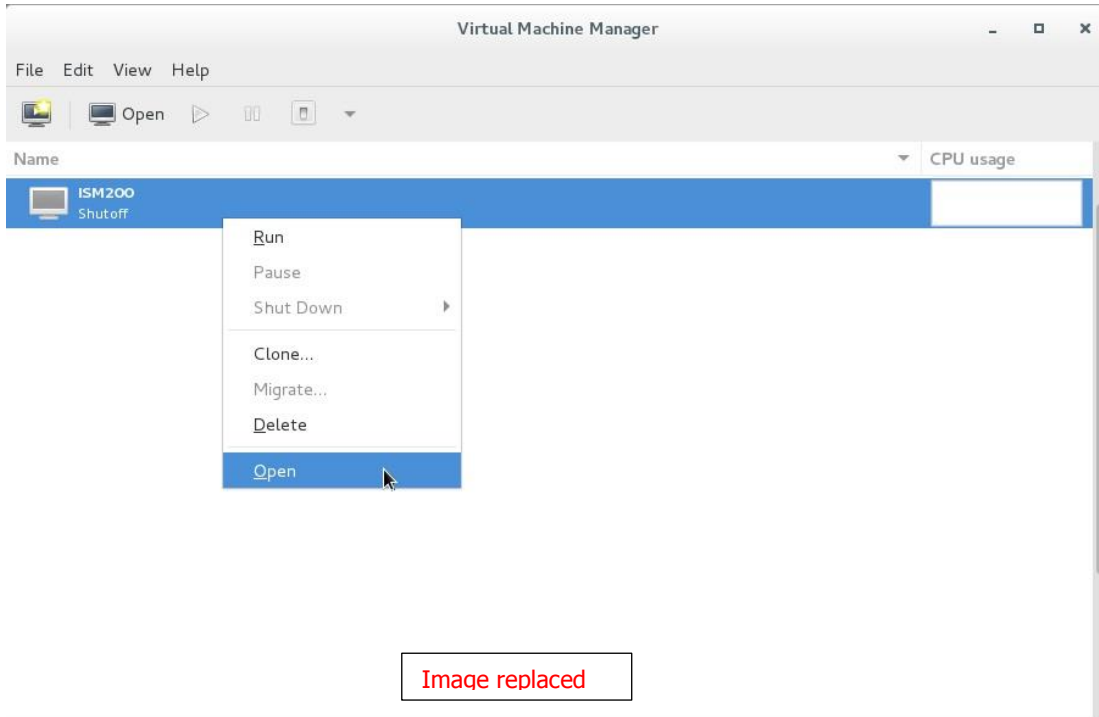
Image replaced

2. On the "ISM-VA Virtual Machine" screen, select [Run] from the [VM] menu to start ISM-VA.

Image replaced
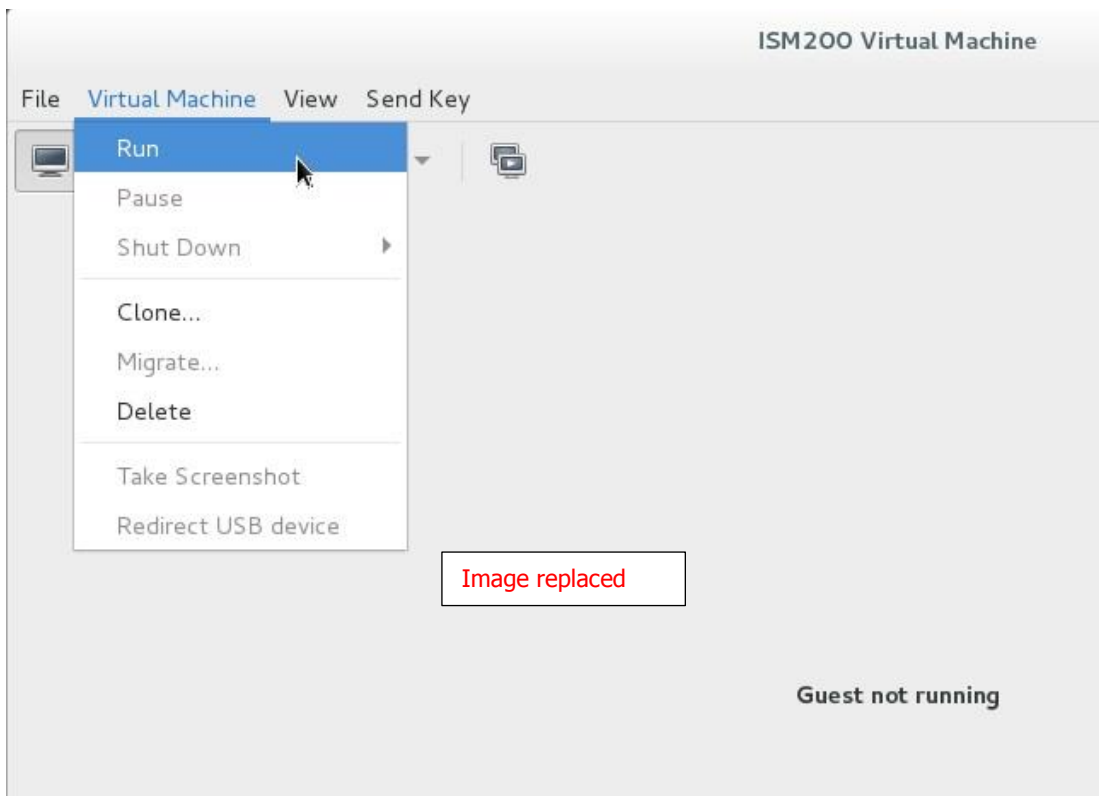
Modification No.62
3.4.2   Initial Settings of ISM

4. From the console, set the date and time.

    Use the following method to check 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
            RTC time: THU 2016-06-09 16:57:40
           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
```

Modification No.63
3.4.2 Initial Settings of ISM

5. Set the domain environment from the console.

This setting is unnecessary 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 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
```

Modification No.64
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
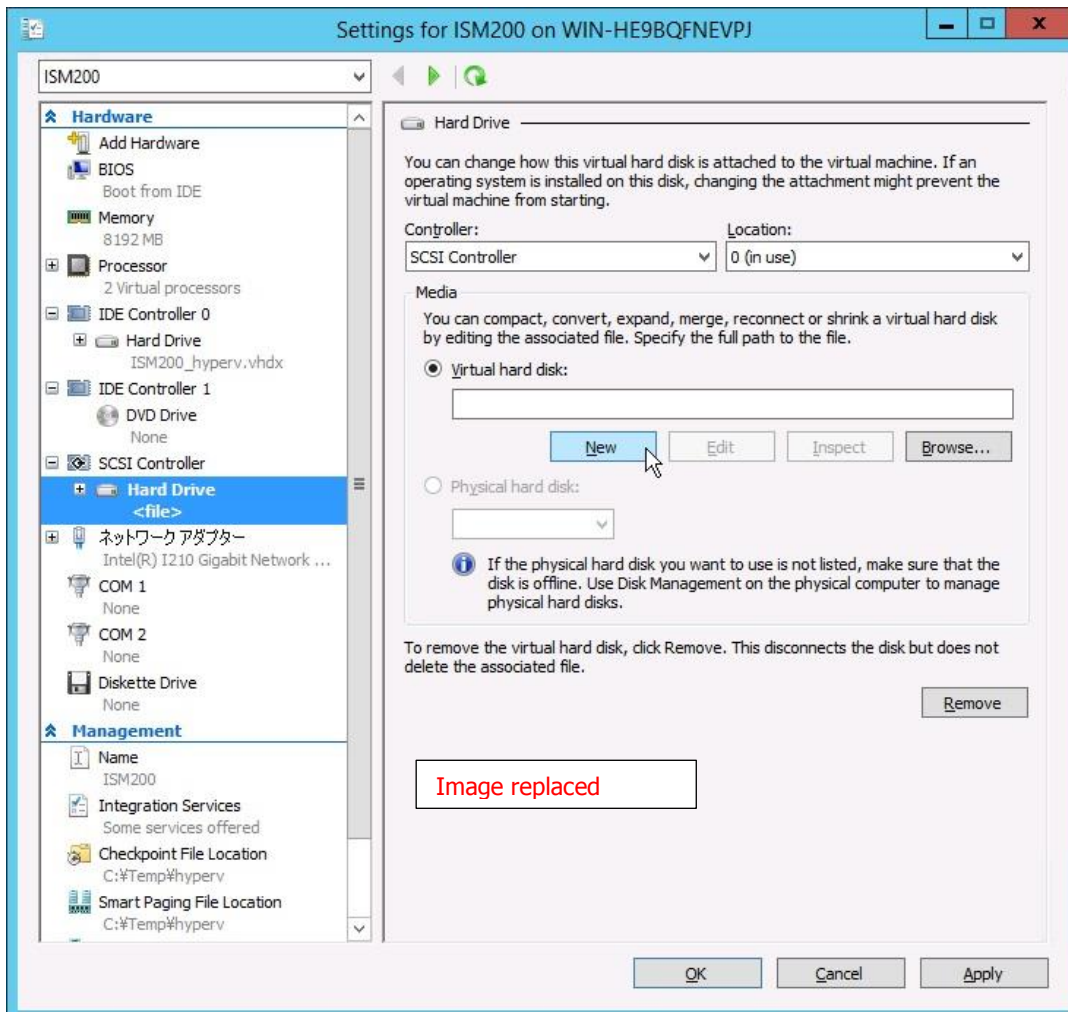
Create the virtual disks so as to be controlled by SCSI controllers.

Modification No.65
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
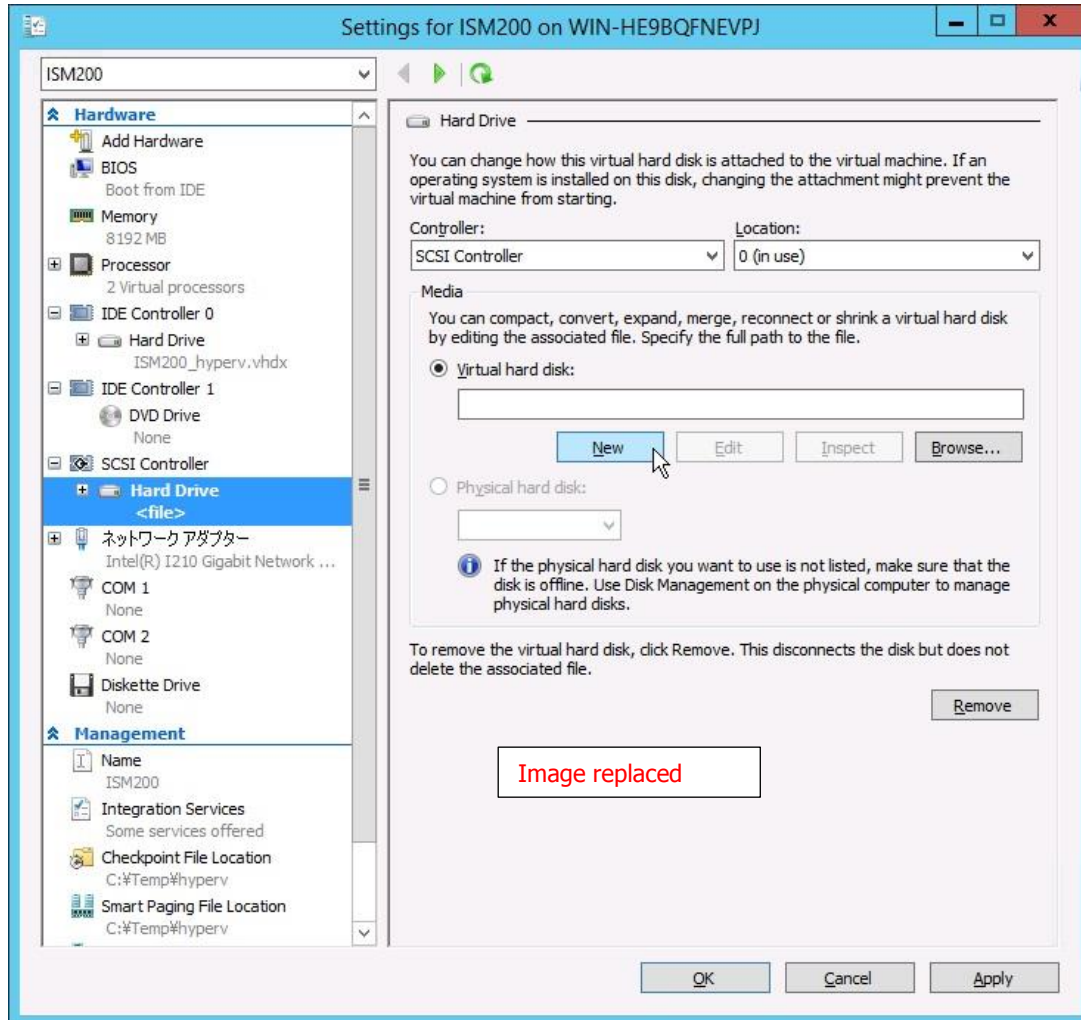
Create the virtual disks so as to be controlled by SCSI controllers.

Modification No.66

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].
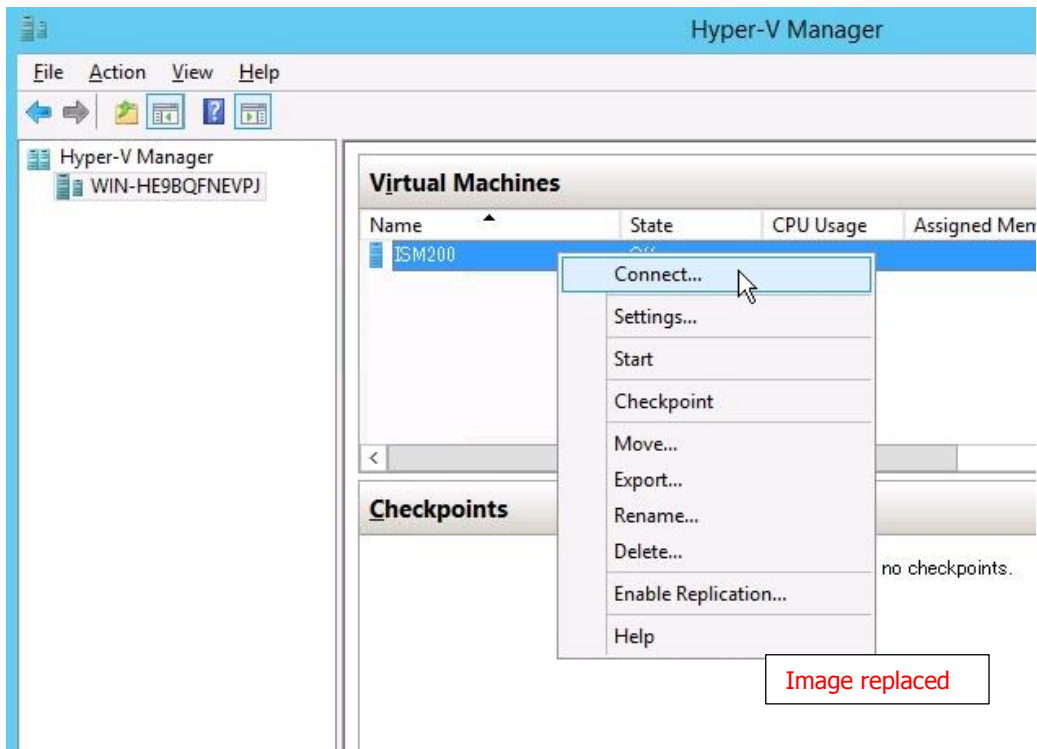
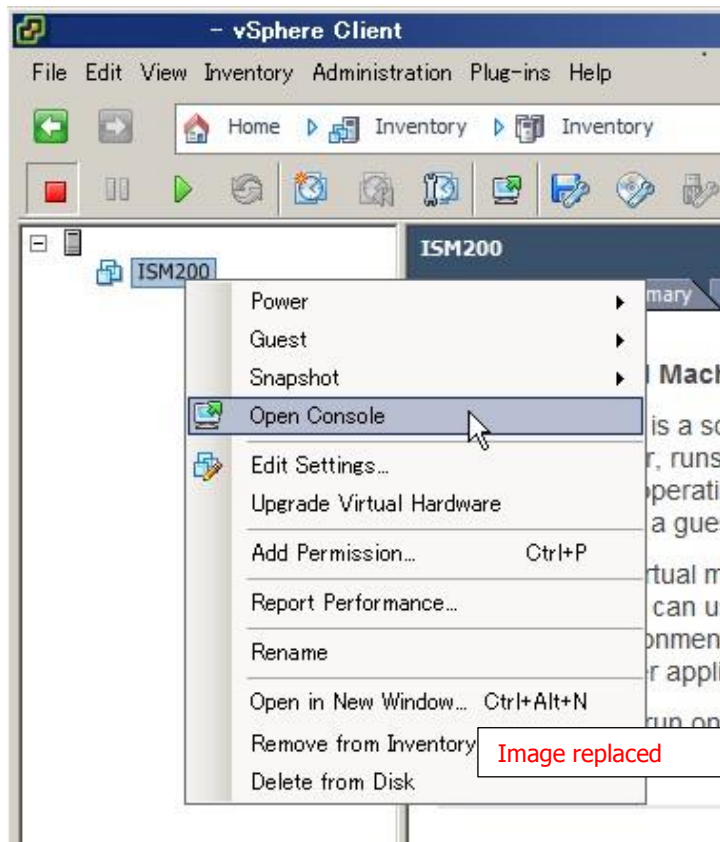2. On the "Virtual Machine Connection" screen, select [Start] from the [Actions] menu to start ISM-VA.
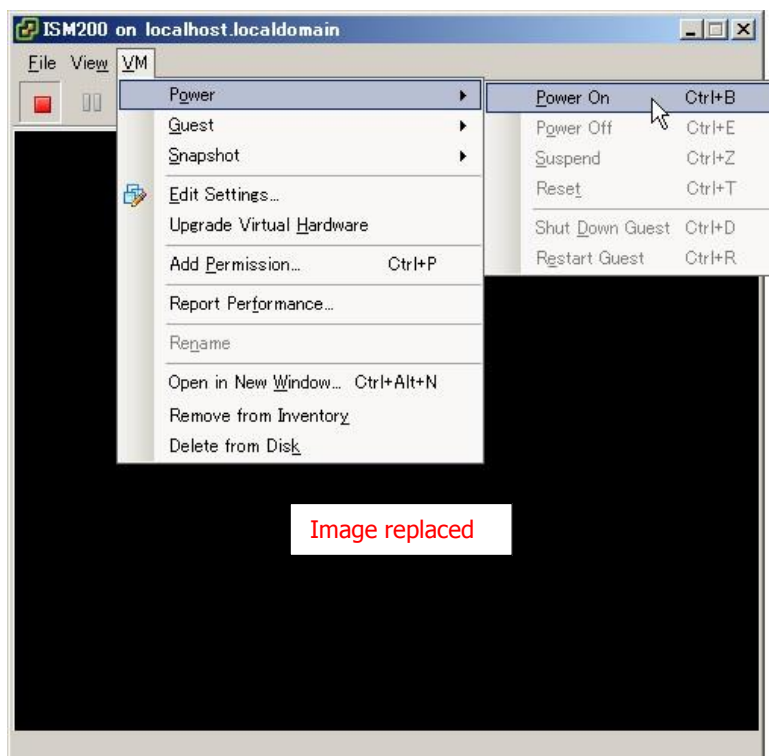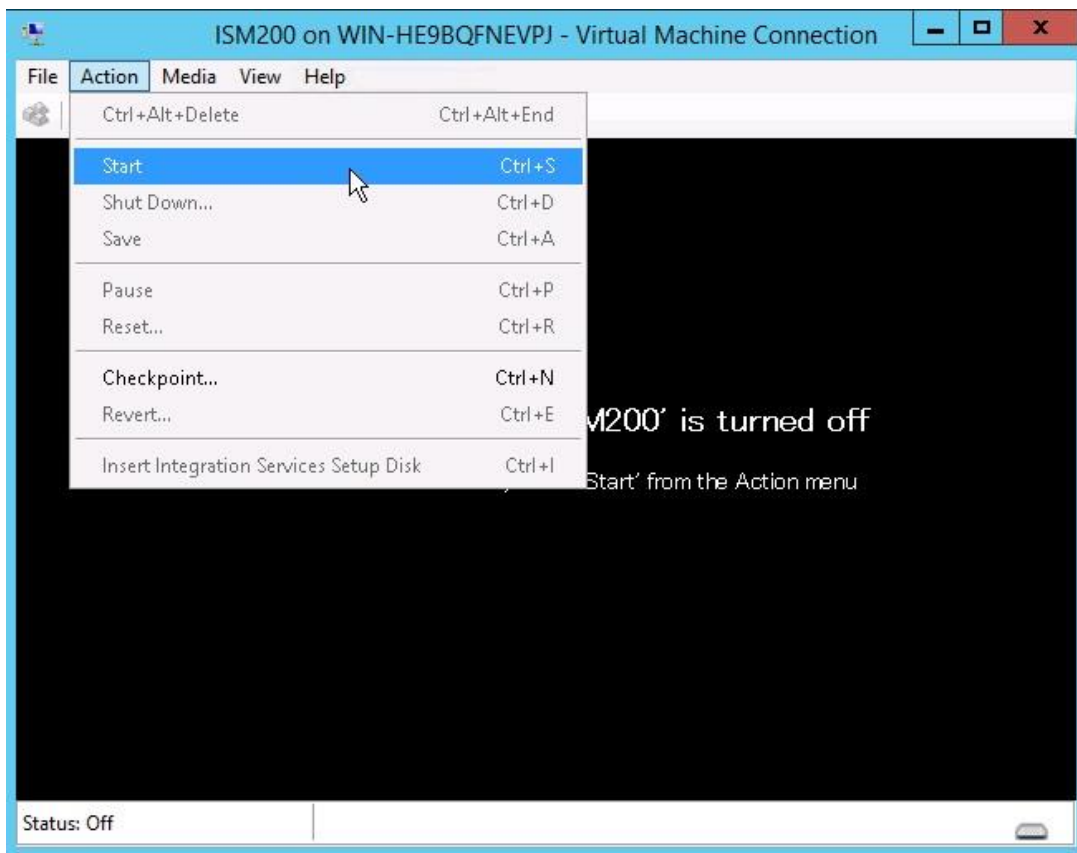
Modification No.67

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].
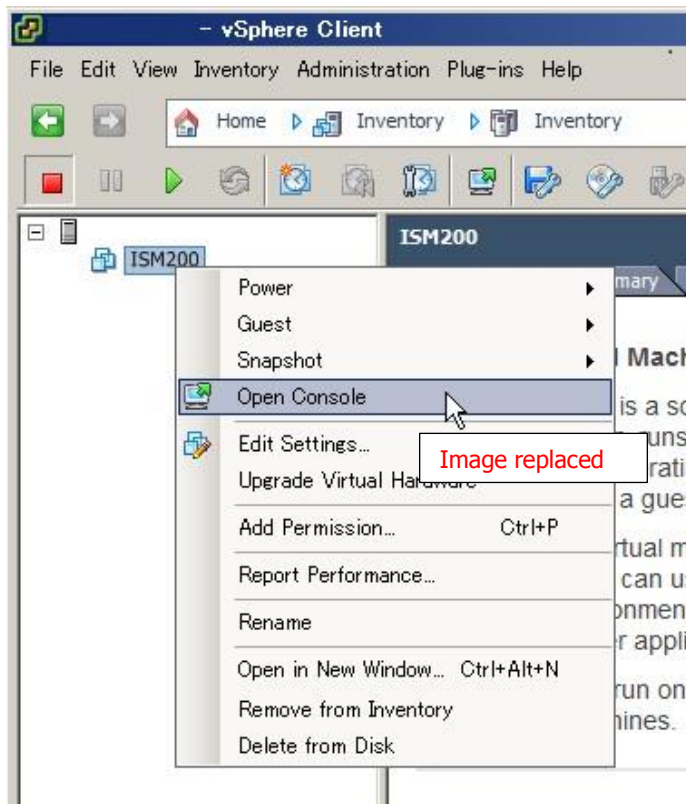

2. On the "Console" screen, select [Power] - [Power On] from the [VM] menu to start ISM-VA.
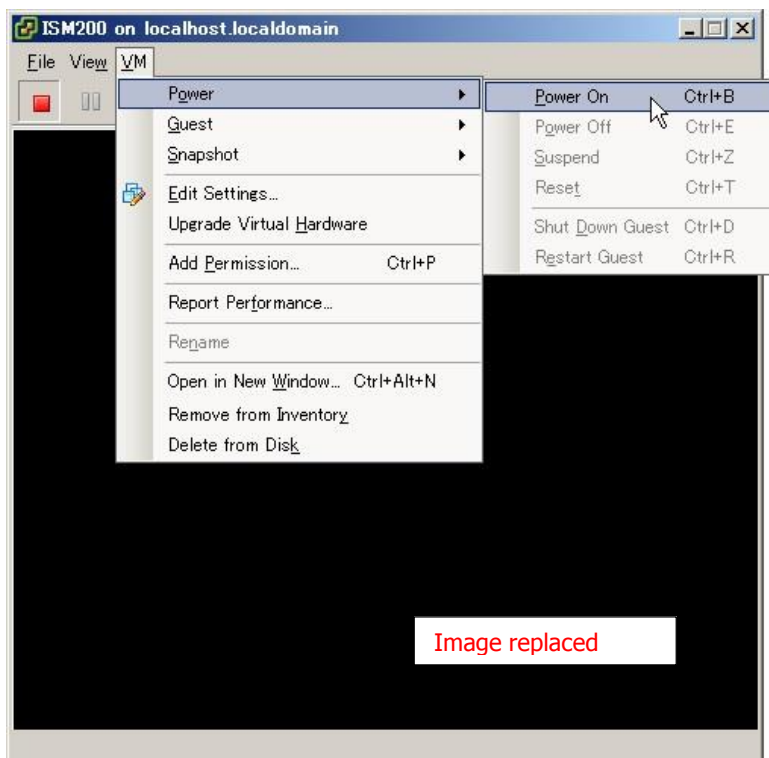
Modification No.68

## 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].
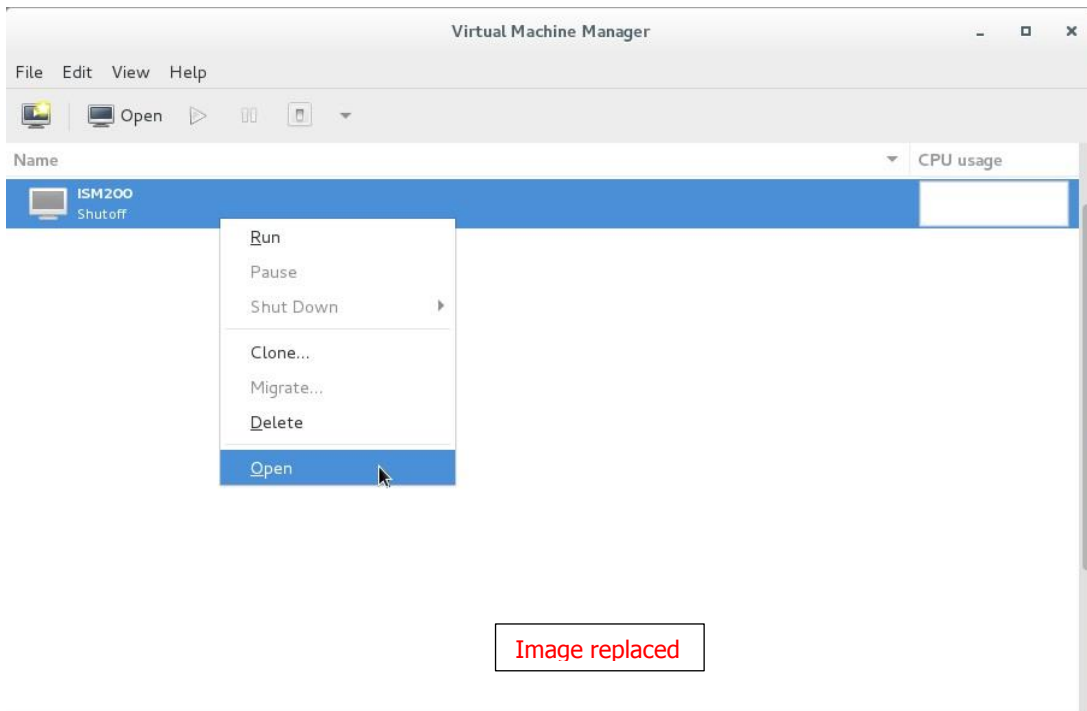
Image replaced

2. On the "ISM-VA Virtual Machine" screen, select [Run] from the [VM] menu to start ISM-VA.

Image replaced
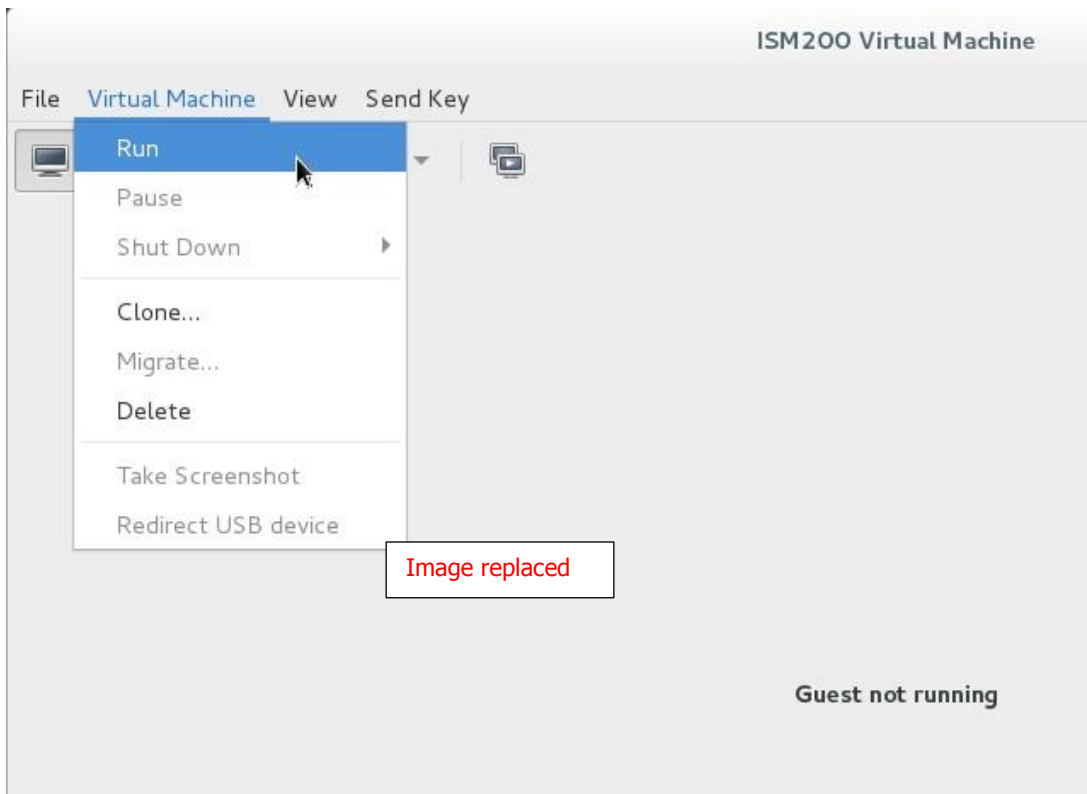
Modification No.69

4.6.1 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.

Modification No.70
4.8 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
   ```

Modification No.71
4.11 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
```

Modification No.72
4.17 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
   ```

Modification No.73

4.18 DHCP server inside ISM-VA

You can use ISM-VA as a DHCP server by starting the DHCP services inside ISM-VA.

The DHCP server is mandatory when installing an OS with the profile management function. In this case, it is possible either to use an external DHCP server or to use the ISM-VA, set up using the following procedure, as a DHCP server.

(In that case, specify which DHCP server to use according to the procedure shown in "4.18.4 Switching DHCP servers".)

If you use only the DHCP server outside ISM-VA, the settings for DHCP server inside ISM-VA is unnecessary.

4.18.1 Settings for DHCP server inside ISM-VA

Set up the DHCP server inside ISM-VA.

After the setup, the settings are made effective by stopping the DHCP services and starting them again.

For stopping and starting of DHCP services, see "4.18.2 Operation of DHCP services 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.

(1) 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.
(2) 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
```

Note

Stop DHCP services and start them after changing the settings for the DHCP server.
For the methods of stopping and starting DHCP services, see "4.18.2 Operation of DHCP services inside ISM-VA."

4.18.2 Operation of DHCP service inside ISM-VA
You can start and stop the DHCP services inside ISM-VA and display their statuses.

- Checking DHCP service status.

```
# ismadm service status dhcpd
```

Command output
Active: active (running): DHCP service active status
Active: inactive (dead) : DHCP service inactive status

/usr/lib/systemd/system/dhcpd.service; enable; : Settings to enable when booting ISM-VA

/usr/lib/systemd/system/dhcpd.service; disabled; : Settings not to enable when booting ISM-VA

- Manual startup of DHCP services

```
# ismadm service start dhcpd
```

Note

- Set up for the DHCP server before you start the DHCP services inside ISM-VA.
  For information on how to setup DHCP servers, see "4.18.1 Settings for DHCP server inside ISM-VA."
- When the DHCP server is in "dead" state even in active settings, check to see if an error is shown with "4. 18. 3 Checking DHCP server information inside ISM-VA - Display of the message of the DHCP server."

- Manual stop of DHCP services

```
# ismadm service stop dhcpd
```

- Setup to enable DHCP services upon startup of ISM-VA

```
# ismadm service enable dhcpd
```

- Setup not to enable DHCP services upon startup of ISM-VA

```
# ismadm service disable dhcpd
```

4.18.3 Checking 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
```

4.18.4 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
```

Modification No.74
4.19 MIB File Settings
In ISM-VA you can import an MIB file(s) that allows to receive any traps.

4.19.1 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 the MIB file registration command.

```
# ismadm mib import
```

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

```
# ismadm mib show
```

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

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

Modification No.75
Appendix A Uninstalling ISM-VA

Uninstalling from Microsoft Windows Server Hyper-V

1. Stop ISM-VA.

   For details, see "4.1.2 Terminating ISM-VA."

2. Start Hyper-V Manager, right-click on the installed ISM-VA, and then select [Settings].

   Take a memo of the displayed storage location of the virtual hard disk that is allocated to the ISM-VA and of the corresponding file name.

3. In Hyper-V Manager, right-click on the installed ISM-VA, and then select [Delete].
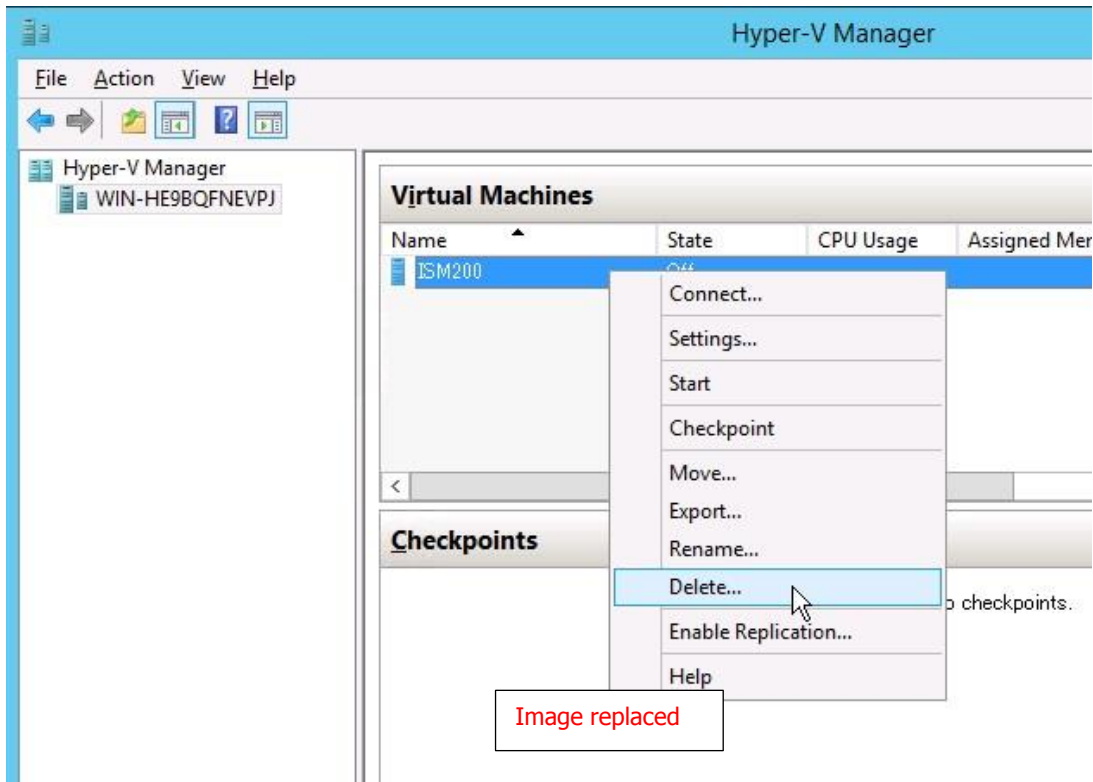
4. Use Explorer to remove the virtual hard disk for which you took the memo in Step 2.

Modification No.76
Appendix A Uninstalling ISM-VA

Uninstalling from VMware vSphere Hypervisor

1. Stop ISM-VA.

   For details, see "4.1.2 Terminating ISM-VA."

2. Start vSphere Client, right-click on the installed ISM-VA, and then select [Delete from Disk].
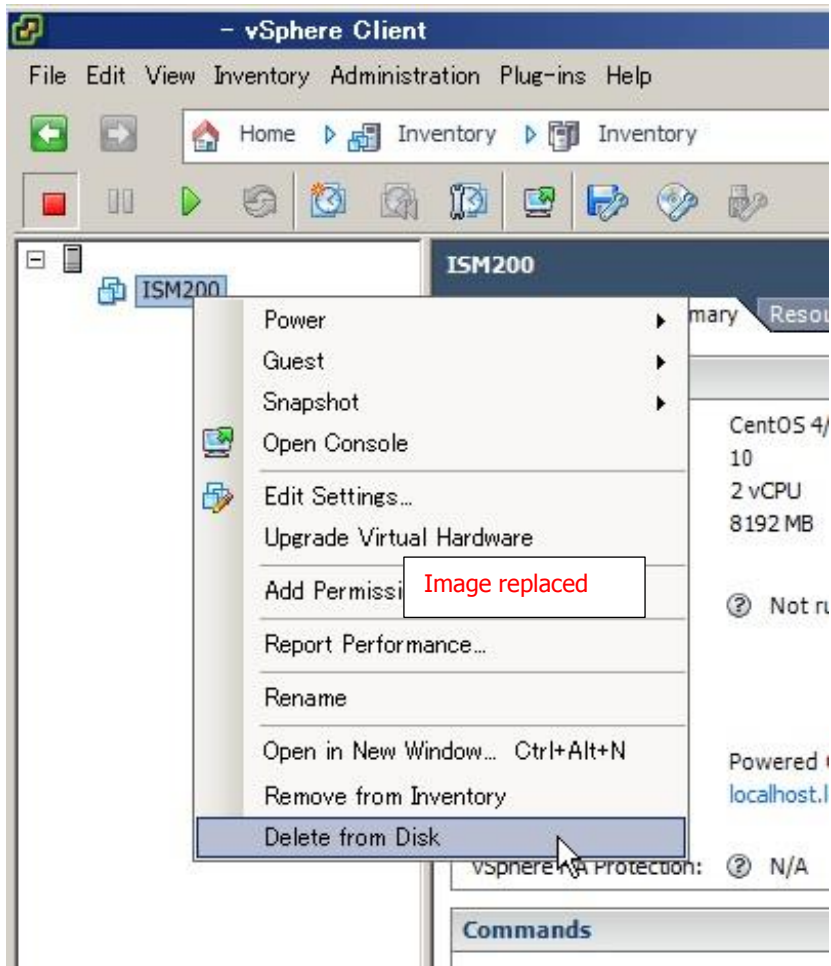
Modification No.77
Appendix A Uninstalling ISM-VA

Uninstalling from KVM

1. Stop ISM-VA.
   For details, see "4.1.2 Terminating ISM-VA."

2. Start Virtual Machine Manager, right-click on the installed ISM-VA, and then select [Delete].
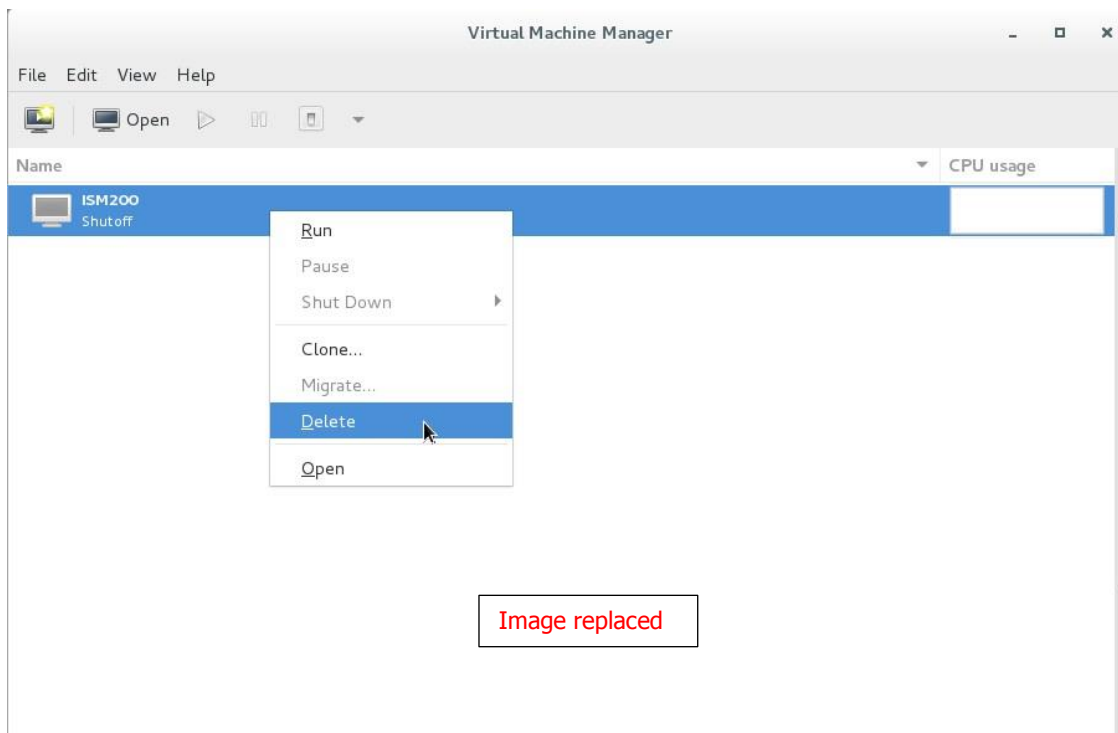
Modification No.78

Appendix B Troubleshooting

Symptom: Execution of ismadm commands around 2:20 AM on Tuesday's 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 AM 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.

Modification No.79
Profile Manager

Symptom： For one of the following functions, the error "Communication with server failed," is displayed when executing an operation to import a file.

- [Settings]-[Profile]-[Actions]-[Import]-[Select] button
- [Settings]-[Repositories]-[Firmware]-[Repositories Import Data List]-[Actions]-[Import DVD]-[Select] button
- [Settings]-[Repositories]-[Firmware]-[Firmware Import Data List]-[Actions]-[Import Firmware]-[Select] button
- [Settings]-[Repositories]-[OS/SVS]-[Actions]-[Import DVD]-[Select] button

Causes and recovery methods

- Check 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.
- Check the current status of data communication between ISM and the client.

Modification No.80
Firmware Manager

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 check whether your environment fulfills the conditions for enabling the Update Mode.

Modification No.81
Profile Manager

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. Check 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
    There may also be other causes.

Modification No.82

Network Manager

Symptom : The connection relationship of a virtual switch(s)/virtual machine(s) is not displayed on Network Map or there is a mistake(s) in the displayed contents.

Causes and recovery methods

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) on ISM to register the OS information of the managed node. Check to see if the cloud management software information is properly registered and the OS information of the managed node is properly registered.

Modification No.83

Log Manager

Symptom: ~~Node's~~ 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.
- Check the [Target] of the log type you specify for log collection. For schedule settings, confirm that the [Enable schedule execution] checkbox is selected.
- If you are able to collect logs by executing [Collect Logs] on the GUI screen but not with the schedule settings you made, it is possibly caused by the node power being off at the time of scheduled execution. Check the contents of the schedule.
- ~~Log collection is not executed if the file size of a node log exceeds 10 GB.~~ If the total size of log files exceeds the upper limit (i.e., Size restriction) specified value already set in Edit User Group Settings, no new log is stored. Check [Events/Tasks] - [Events] and, if there are records like ~~"The predetermined capacity for an Archive log saving area was exceeded" or "The predetermined capacity for a node log saving area was exceeded,"~~ "The predetermined capacity for an Archive log saving area was exceeded", "The predetermined capacity for a node log (for download data) saving area was exceeded," or "The predetermined capacity for a node log (for log search data) saving area was exceeded" at the timing of log collection, delete some of the previously collected logs to reduce the amount of files.

Modification No.84

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

Causes and recovery methods

If the node status is "Exempt," check whether the node actually supports log collection. If the status is "Exempt" although the node supports log collection, maybe ISM did not yet obtain the node information, so check the network connection with the node and the node property settings, and then execute [Get Node Information].

Modification No.85

Symptom: "Operating System" and "ServerView Suite" cannot be specified in ~~node log collection~~ log collection of a node.

Causes and recovery methods

- When the OS information of a target node is not registered yet, or not yet obtained by ISM, it cannot be specified. Register the OS information before you execute [Get Node Information].
- Depending on the type of OS, you may not be able to specify "ServerView Suite" as it may not be eligible for information retrieval.

Modification No.86

Appendix C Profile Settings Items

1.1.1 BIOS/iRMC Settings items of profiles for PRIMERGY servers

This section describes the items that you can set up in the BIOS/iRMC tab in profiles. Depending on your server types you may find some items that you are unable to set up or some items with different setting contents. Therefore, set up your servers within the scope of support.
You can select Enable or Disable individually for the profiles setting items. 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. This function is also called [XD (eXecute_Disable)_bit]_or_[NX_(No eXecute)_bit]_depending on the HW manuals.	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 to be 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 an 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 an 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 becomes disabled regardless of this setting.	Enabled=Function enabled Disabled=Function disabled
Memory Configuration		
DDR Performance (Low-Voltage optimized/Energy optimized/Performance optimized)	Memory modules operate with different speeds (Frequencies). The faster the speed the higher the performance. The slower the speed the more the power saved. The available memory speeds differ depending on the attached memory module configurations	Low-Voltage optimized=The fastest setting available with low voltage Energy optimized=The slowest setting available with power-saving Performance optimized=The fastest setting available for achieving the highest performance

Item Name	Description	Parameter
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.~~ When _ _ _ multiprocessor configuration is not used, this setting is to be ignored.	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 a 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 booted. 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
Launch Storage OpRomPolicy (UEFI only / Legacy only / Do not launch)	This specifies the 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 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

Item Name	Description	Parameter
		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 (Control by OS/Power-saving operation)	This sets up the power-saving and noise canceling operations for a server. **Note** When you disable Enhanced SpeedStep in BIOS settings, this setting also becomes disabled.	OS Controlled=Control by OS followed Minimum Power=Operation where priority is placed on reduction in power consumption (Schedule)=Setup by Profile Manager unavailable (Power capping)=Setup by Profile Manager 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 perform periodic communication checks while an OS is running, with use of software watchdog. **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.	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
After Timeout Delay	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, using Boot Watchdog. **Note** This setting becomes enabled after rebooting the server.	(Checked)=Period monitored (Unchecked)=Period not monitored.
Behavior	This specifies behavior for a situation where an OS does not start within the specified time. **Note** This setting becomes enabled after rebooting the server.	Select the item from the pulldown menu. Continue=Nothing done Reset=Sever rebooted Power cycle= Powered ON after powering OFF the server once
After Timeout delay	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**	Local Time=iRMC time displayed in local time format

Item name	Description	Parameter
	Time) format or 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 the Telnet port number of iRMC.	Enter the port number. 3172 by default
SSH Enabled	This specifies whether to enable ssh connection.	(Checked)=ssh connection enabled (Unchecked)=ssh connection disabled
SSH Port (Default: 22)	This specifies Telnet port number of ssh.	Enter the port number. 22 by default
SNMP Generic Configuration		
SNMP Enabled	This specifies whether to enable SNMP. **Note** You cannot set up the setting items that are not shown on the Web UI screen of iRMC. 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.	Enabled=SNMP enabled Disabled=SNMP disabled
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.	All (SNMPv1/v2c/v3)=All protocols (SNMPv1/v2c/v3) supported Only SNMPv3=Only SNMPv3 supported

Item name	Description	Parameter
	Disable the setting items if you fail to assign a profile.	
SNMP v1/v2c Community	This specifies the community strings in the cases of SNMP v1/v2c. **Note** You cannot set up the setting items that are not shown on the Web UI screen of iRMC. Depending on the firmware versions, you cannot set up some setting items even though the setting items are shown on the Web UI screen of iRMC. Disable the setting items if you fail to assign a profile.	
SNMPv3 User Configuration		
SNMPv3 Enabled (Enabled/Disabled)	This specifies whether to enable SNMPv3 support for users. **Note** To create/change SNMPv3 users, 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.	Enabled=SNMPv3 support enabled Disabled=SNMPv3 support disabled
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 are unable to set up the settings items that are not shown on the Web UI screen of iRMC. Depending on the firmware versions, you are unable to set up some settings items even though the settings items are shown on the Web UI screen of iRMC. Disable the settings items if you fail to assign a profile.	Always read-only

Item name	Description	Parameter
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. Disable the setting items if you fail to assign a profile.	SHA=SHA used MD5=MD5 used None=Authentication disabled
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	Enter the IP address or the DNS strings of an SNMP server.

122

Item name	Description	Parameter
	community set up as "Trap destination."	
Protocol	This specifies the Version of SNMP protocol used for receiving traps. **Note** ━━━━━━━━━━━ You cannot set up the setting items that are not shown on the Web UI screen of iRMC. Depending on the firmware versions, you cannot set up some setting items even though the setting items are shown on the Web UI screen of iRMC. Disable the setting items if you fail to assign a profile. ━━━━━━━━━━━	Select the item from the pulldown menu. SNMPv1, SNMPv2c or SNMPv3

1.2   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.

1.2.1   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 whether 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 ServerView Suite that is used and is registered in Repository. Specify Version=ServerView Suite of the specified version used.
Management LAN network port settings		
Network port specification	This specifies the port of the network used for Management LAN.	(Checked) =Specify the network port for Management LAN.
Method for specifying	This selects the method of specifying the network port for Management LAN.	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 the item 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 for specifying.	Enter the port number that you use.
MAC Address	This is entered if you specify "MAC	Enter the MAC address of the network

123

Item name			Description	Parameter
			address" in Method for specifying.	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. (*8)
		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 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. (*6)
	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 use purpose 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. (*1) Ex.: 600×480, 800×600, 1024×768 or 1280×1024
	Refresh Rate [Hz]		This specifies the display refresh rate immediately after OS installation.	Select the item from the pulldown menu. (*1)
	# 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. (*1)
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	(Checked)=Authentication traps sent

Item name			Description	Parameter
			authentication traps in response to the SNMP request from an unknown host or community.	(Unchecked)=Authentication traps not sent
	Acception of SNMP Packets (Accept SNMP Packets from Default Host (LocalHost)/Accept SNMP Packets from These Hosts)		This specifies whether to accept SNMP packets from Localhost.	(Acception 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 necessary.
Firewall Settings			This creates a firewall exception necessary for 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		This specifies whether to install Java Runtime Environment. This is mandatory to specify when you install ServerView RAID Manager.	(Checked)=Application installed (*9)
	ServerView Agent		This specifies whether to install ServerView Agent. You can specify it when you install SNMP services.	(Checked)=Application installed (*2)
	ServerView Update Agent		This specifies whether to install ServerView Update Agent. You can specify it when you install ServerView Agent.	(Checked)=Application installed (*2)
	DSNAP		This specifies whether to install DSNAP.	(Checked)=Application installed (*7)
	Software Support Guide		This specifies whether to install Software Support Guide.	(Checked)=Application installed (*7)
	ServerView RAID Manager		This specifies whether to install ServerView RAID Manager.	(Checked)=Application installed
Executing Script after Installation				
	Execute 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 (*3).	Specify the script to be executed.

*1: This is installed with default settings when you set up a value unsupported by the OS.

125

*2: The application is installed in Japanese when you select Japanese on "Region and Language" settings. Otherwise, the application is installed in English.

*3: The specified script is executed by Windows "cmd /c" command.

*6: Volume names must be set by one-byte alphanumeric characters/symbols for Windows Server 2016.

*7: This can be installed only when you select Japanese on "Region and Language" settings.

*8: When using the Array Controller, set it so that it does not conflict with the "Onboard Device Configuration" setting of the BIOS.

*9: It can be installed only when "Full Installation" is selected for the "Type of Installation" setting.

OS Individual tab

Item name	Description	Parameter
Type of Installation	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 (*4)
Work Group/Domain Name	This specifies the name of Work Group or Domain.	Enter the character string (*5)
Domain User Name	A domain user name for the case of Domain is entered.	Enter the character string.
Domain Password	A password for the case of Domain is entered.	Enter the character string.
Network		
DHCP	This selects whether to specify a fixed IP address or use DHCP for the IP address of Management LAN.	(Checked)=DHCP used (Unchecked)=Fixed IP specified
IP Address	A fixed IP address is specified when you do not use DHCP.	Enter the IP address in IPv4 format.
Subnet Mask	A subnet mask is specified when you do not use DHCP.	Enter the subnet mask in IPv4 format.
Default Gateway	A gateway is specified when you do not use DHCP.	Enter the IP address of the gateway in IPv4 format.
DNS Server	The IP address of a DNS server is specified when you do not use DHCP.	Enter the IP address of the DNS server in IPv4 format.
DNS Domain Name	A domain name is specified when you do not use DHCP.	Enter the domain name character string.

*4: This is set up for Work Group when you are unable to connect to the domain server.

*5: 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.

1.2.2　Profiles for VMware ESXi 5.5/VMware ESXi 6.0

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 ServerView Suite that is used and is registered in Repository.

Item name			Description	Parameter
				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 Management LAN.	（Checked）=Specify the network port for Management LAN.
	Method for specifying		This selects the method of specifying the network port for Management LAN.	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 the item 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 for specifying.	Enter the port number that you use.
		MAC Address	This is entered if you specify "MAC address" in Method for specifying.	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(*2)(*3)
		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 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 a 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. If you perform the automatic registration, set a fixed IP address as the IP address set by using [OS Individual] tab. Likewise, specify "0" to VLAN ID on "OS" tab.	(Checked) =Registered (Unchecked) = Not registered
		CMS 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				
	Execute 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.

Item name	Description	Parameter
Script executed after Installation	This specifies the script executed after installation.(*1)	Specify the script executed after installation.

*1: Describe the script with plain text format in the file.
　　This is executed as %post processing during automatic installation (kickStart). %firstboot description allows it to be executed as %firstboot processing.
*2: When using the Array Controller, set it so that it does not conflict with the "Onboard Device Configuration" setting of the BIOS.
*3: On VMware ESXi, "Onboard SATA Array Controller" cannot be used.

OS Individual tab

Item name	Description	Parameter
License Agreement	This selects whether to agree with VMware License Agreement. Be sure to check and indicate that you have agreed.	(Checked)=Agreement with VMware License (Unchecked)=Not in agreement with VMware License
Type of Installation Media	This selects the type of media used for installation.	Always the installation media specified on 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 (host name) obtained from DNS. You can select Checked/Unchecked when DHCP is disabled.	(Checked)=Obtained from DNS (Unchecked)=Any host name specified.
Computer Name	Any computer name (host name) is specified when you do not obtain a computer name from DNS.	Enter the host name.

1.2.3　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 ServerView Suite that is used and is registered in Repository. 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 Management LAN.	（Checked）=Specify the network port for Management LAN.
Method for specifying	This selects the method of specifying the network port for Management LAN.	Select the item from the pulldown menu.

	Port Number	This is set if you specify "Port Number " in Method to specify. Select the type of network card that you use.	Select the item 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 for specifying.	Enter the port number that you use.
	MAC Address	This is entered if you specify "MAC address" in Method for specifying.	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 (*12)
	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 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.
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 unnecessary 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 selects a new package.	Minimal system=Minimum necessary packages Install everything=All the packages Default package groups=Recommended packages (*7)
Package Group		This specifies the package group to be installed.	(Checked)=Installed (Unchecked)=Not installed
New Package		This individually specifies the package	Enter the package name with the

		name to be installed.	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 (*3)
	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. (*4)	(Checked)=Application installed
Executing Script after Installation			
	Execute 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 the OS after installation.	Specify the directory forwarded to the OS after installation.
		Script executed after Installation	This specifies the script to be executed. (*8) (*9)	Specify the script to be executed.

*3: "Shadow Passwords" is always enabled regardless of profile settings.
*4: 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.

Application	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 7.2 /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 (*10)	Y	Y	Y
ServerView RAID Manager	Y	Y	Y
AIS Connect (*11)	Y	Y	N
Java Runtime Environment	Y	Y	Y

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

*7: When you use ServerView Suite DVD (V11.16.04), some package groups are not installed. In such cases, manually install them.
*8: When you execute a script from another script, assign execution privilege to invoke it.
*9: This executes the specified script with sh command.

*10 : Set SELinux to Disabled when you install it.

*11: This cannot be set for ServerView Suite DVD V12.16.10 .

*12: When using the array controller, set it so that it does not conflict with the "Onboard Device Configuration" setting of the BIOS.

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.
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 is specified when you do not obtain a computer name from DNS.	Enter the computer 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.

1.2.4 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 ServerView Suite that is used and is registered in Repository. 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 for specifying	This selects the method of specifying the network port for Management LAN.	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 the item 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 for specifying.	Enter the port number that you use.
MAC Address	This is entered if you specify "MAC address" in Method for specifying.	Enter the MAC address of the network that you use.
Basic Settings		
Region and Language	This specifies a language.	English is only available.
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(*8)
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

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	This specifies the type of file systems.	Select the item from the pulldown menu. Ex.: ext2, ext3 or ext4 (*1)
Size (MB)	This specifies a partition size.	Enter a decimal value.
Fill to maximum allowable size	This specifies whether to allocate spare disk capacity to the specified partition. Specifying this is unnecessary 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 between a package group shown on the screen as the packages to be installed and a new package.	Minimal system=Minimum necessary packages Install everything=All the packages Default package groups=Recommended packages
Package Group (*2)	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

SELinux	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 (a variety of applications)	This specifies the application to be installed. The type of applications differs depending on distribution. (*4)	(Checked)=Application installed
Executing Script after Installation (*3)		
Execute 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 the OS after installation.	Specify the directory forwarded to the OS after installation.
Script executed after Installation	This specifies the script to be executed. (*5) (*6)	Specify the script to be executed.

*1: 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 ones officially support by SLES.

*2: In SLES 12, even in a 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.

*3: In SLES 12, this does not support the script execution after installation.

*4: The applications in the table below show the case where ServerView Suite DVD V11.16.04 is used. These may be changed in future version upgrades of the ServerView Suite DVD.

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 (*7)	N	N	N
Java Runtime Environment	Y	Y	Y

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

*5: When you execute a script from another script, assign execution privilege to invoke it.

*6: This executes the specified script with the sh command.

*7: This cannot be set up for ServerView Suite DVD V12.16.10.

*8: When using the array controller, set it so that it does not conflict with the "Onboard Device Configuration" setting of the BIOS.

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
Root Password	A password is entered.	Enter the password.
Network		
Get Computer Name Via DNS Server	This specifies whether to use the computer name (host name) obtained from DNS.	(Checked)=Obtained from DNS (Unchecked)=Any host 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.

Item name	Description	Parameter
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 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.

1.3   Settings items of profiles for storage

This section describes the items that you set up in the profiles for ETERNUS DX/AF Series. Some of the selectable items may differ depending on the type of your storage.
For details of each item, see the manual for your storage.

RAID & Disk Configuration tab

Item name	Description	Parameter
RAID Configuration		
RAID Group Name	This specifies a RAID group name. **Note** You cannot specify the RAID group name already set up for a device.	Enter the RAID group names. You can enter 1 to 16 characters.
RAID Level	This specifies the RAID level of a disk array to be configured.	Select the item from the pulldown menu. RAID1, RAID5, RAID6 or RAID1+0
Number of Disks	This specifies the number of disks built in a disk array.	Specify the number of disks. The selectable number differs depending on the selected RAID level.
Disk Inch	This specifies the type of disk drive (drive outer size).	Select the item from the pulldown menu. 2.5 Inch or 3.5 Inch
Disk Type	This specifies the type of disk drive (interface type) built in a disk array.	Select the item from the pulldown menu. The selectable type differs depending on the models of ETERNUS and selected disk inch. SAS, NL-SAS, SED or SSD
Disk Size	This specifies the type of disk drive (disk size) built in a disk array.	Select the item from the pulldown menu. The selectable size differs depending on the selected disk inch and disk type. 300GB, 450GB, 1TB, etc.
Volume		

Item name	Description	Parameter
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 by selecting the item from the 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

Item name	Description	Parameter
Disk Inch	This specifies the type of disk drive (drive outer size) defined as a hot spare.	Select the item from the pulldown menu. 2.5 Inch or 3.5 Inch
Disk Type	This specifies the type of disk drive (interface type) defined as a hot spare.	Select the item from the pulldown menu. The selectable type differs depending on the models of ETERNUS and selected disk inch. SAS, NL-SAS, SED or SSD
Disk Size	This specifies the type of disk drive (disk size) defined as a hot spare.	Select the item from the pulldown menu. The selectable size differs depending on the selected disk inch and disk type. 300GB, 450GB, 1TB, etc.

Host Affinity

LUN Group

Item name	Description	Parameter
LUN Group Name	This specifies a LUN group name. **Note** ━━━━━━ You cannot specify the LUN group name already set up for a device. ━━━━━━	Specify the LUN group name strings.

Volumes

Item name	Description	Parameter
Volume Name	This specifies the name of a volume which belongs to a LUN group.	Enter the name of the volume which belongs to the LUN group. Specify the volume created by a profile or the volume already created on a device.

Port Group

Item name	Description	Parameter
Port Group Name	This specifies a port group name. **Note** ━━━━━━ You cannot specify the port group name already set up for a device.	Specify the port group name. You can enter 1 to 16 characters.

Item name			Description	Parameter
	Ports			
		Port Number	This specifies the port number which belongs to a port group.	Specify the port number which belongs to the port group with a triple-digit number.
	Host Group			
		Host Group Name	This specifies a host group name. **Note** You cannot specify the host group name already set up for a device.	Specify the host group name. You can enter 1 to 16 characters.
		Host Type	This specifies the type of a host group.	Select the item from the pulldown menu. iSCSI or FC
	Hosts			
		Host Name	This specifies the host name which belongs to a host group. **Note** You cannot specify the host name already set up for a device.	Specify the name of the host which belongs to the host group. You can enter 1 to 16 characters.
		iSCSI Name	This specifies the iSCSI name which defines the host name. You can enter it when the host type of a host group is iSCSI name.	Enter iSCSI name. Enter "iqn." or "eui." at its head.
		Host WWN	This specifies the host WWN which defines the 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		Describes the control command to execute on ETERNUS before executing profile assignment (RAID/Hot Spare/Host Affinity settings) is described. Leave the checkbox unchecked unless a special request is made.	See "CLI User Guide" of your device for the described contents.
	Post Run Command		Describes the control command to execute on ETERNUS after completion of profile assignment (RAID/Hot Spare/Host Affinity settings). 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.

1.4　Settings items of profiles for switches

This section describes the items that you set up in the profiles of switches.
For details on each item, see the manual of your switch.

1.4.1　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 Type		This specifies whether to send SNMP traps.	Select the item from the pulldown menu. Off, v1 or v2c
	Write		This specifies whether to permit writing from an SNMP manager.	(Checked)=Permitted (Unchecked)=Not permitted
SNMP User (SNMPv3)				
	Number		This specifies an SNMP user definition number.	Select the item from the pulldown menu.
	User Name		This specifies an SNMP user name.	Enter the SNMP user name.
	Address Setting		This specifies whether to enable an SNMP host address.	(Checked)=Enabled (Unchecked)=Disabled
		Host Number	This specifies an SNMP host definition number.	Select the item from the pulldown menu.
		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 of the SNMP host.
	Authentication Setting		This specifies whether to enable SNMP authentication protocol.	(Checked)=Enabled (Unchecked)=Disabled
		Authentication Protocol	This specifies the SNMP authentication protocol.	Select the item from the pulldown menu. none, md5 or sha
		Authentication Password	This specifies an SNMP authentication	Enter the SNMP authentication

Item name	Description	Parameter
	password.	password.
Privacy Setting	This specifies whether to enable SNMP privacy settings.	(Checked)=Enabled (Unchecked)=Disabled
Privacy Protocol	This specifies the SNMP privacy protocol.	Select the item from the pulldown menu. none or des
Privacy Password	This specifies an SNMP privacy password.	Enter the SNMP privacy password.
Read	This specifies whether to enable SNMP MIB read.	(Checked)=Enabled Likewise, specify the item from the pulldown menu. none: Read not permitted all: Read permitted
Write	This specifies whether to enable SNMP MIB write.	(Checked)=Enabled Likewise, specify the item from the pulldown 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 pulldown menu. none: Read-out not permitted all: Read-out permitted

Authentication tab

Item name	Description	Parameter
Account		
Change Administrator Password	This specifies whether to change 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.
Time Zone Setting	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.

1.4.2   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 pulldown the pulldown menu. v1, v2c or v3
v3 Security Level	This specifies the security level for SNMPv3.	Select the item from pulldown the pulldown menu. auth, noauth or priv
Read	This specifies whether to enable SNMP MIB read.	(Checked)=Enabled Likewise, specify the item from the pulldown menu. none: Read not permitted all: Read permitted
Write	This specifies whether to enable SNMP MIB write.	(Checked)=Enabled Likewise, specify the item from the pulldown 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 pulldown menu. none: Read-out not permitted all: Read-out permitted
Community (for Host)		
Community Name	This specifies an SNMP community name.	Enter the community name strings.
Group	This specifies the group which a community belongs to.	(Checked)=Enabled 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
Host		
Address	This specifies the IP address of an SNMP	Enter the IP address of the host with

Item name	Description	Parameter
	host.	the strings based on IPv4 or IPv6 address notations.
Community Name	This specifies an SNMP community name.	Select the item from the pulldown menu.
Severity Level	This specifies the SNMP trap level.	Select the item from the pulldown menu.
Trap Version	This specifies the SNMP trap version.	Select the item from the pulldown menu. v1 or v2c
UDP Port	This specifies an SNMP trap sending port.	Enter the SNMP trap sending port. The value between "0" and "65535" can be specified.
User (for v3 Host)		
User Name	This specifies an SNMP user name.	Enter the user name between 1 and 64 characters.
Group	This specifies an SNMP group name.	Enter the group name between 1 and 64 characters.
Authentication Settings	This specifies whether to enable SNMP authentication settings.	(Checked)=Enabled
Authentication Protocol	This specifies the SNMP authentication protocol.	Select the item from the pulldown menu. MD5, SHA or NoAuth
Authentication Password	An SNMP authentication password is entered.	Enter the authentication password between 1 and 32 characters.
Privacy Settings	This specifies whether to enable SNMP privacy settings.	(Checked)=Enabled
Privacy Protocol	This specifies SNMP privacy protocol.	Select the item from the pulldown menu. DES, AES128 or NoPriv
Privacy Password	This specifies an SNMP privacy password.	Enter the privacy password strings between 1 and 32 characters.
v3 Host		
Address	This specifies the IP address of an SNMP host.	Enter the IP address of the host with the character 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: 0" to "FF: 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
Password	This specifies a new administrator	Enter the password between 8 and 32

140

Item name			Description	Parameter
			password.	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 setting 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.
		Time Zone Setting	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).