CA92344-2516-02

FUJITSU Software Infrastructure Manager V2.3
Infrastructure Manager for PRIMEFLEX V2.3
Instructions for Manage and Operate Nodes

October 2018

FUJITSU LIMITED

Note:

"Infrastructure Manager for PRIMEFLEX" is available only in Japan, APAC, and North America.

Modification History		
Edition	**Publication Date**	**Modification Overview**
01	August 2018	First Edition
02	October 2018	2.1 List of Available Port Numbers 2.2 Details of Node Settings 3.2 General Standards for Firmware Update Time 3.3 General Standards for Disk Usage in Using Log Management : Added the information of PSWITCH 4032P (supported ISM 2.3.0.b or later) 2.2 Details of Node Settings 3.3 2 : General Standards for Disk Usage in Using Log Management : Modified the name of Brocade VDX to VDX

This document provides information on pre-settings or environmental settings, as well as settings of nodes to be managed or operated and their reference information required to use FUJITSU Software Infrastructure Manager V2.3 and FUJITSU Software Infrastructure Manager for PRIMEFLEX V2.3.

Hereinafter, "Infrastructure Manager" is referred to as "ISM", and "Infrastructure Manager for PRIMEFLEX" is referred to as "ISM for PRIMEFLEX." When explanation is provided without distinguishing "Infrastructure Manager" from "Infrastructure Manager for PRIMEFLEX", it is referred to as "Infrastructure Manager" or "ISM" as a unified description.

For the details and abbreviations used in this document, refer to the manuals for ISM or ISM for PRIME FLEX listed below.

- User's Manual
- Glossary
- Settings for Monitoring Target OS and Cloud Management Software

Chapter 1 ISM Environmental Settings

1.1 DHCP/PXE Settings in Using Profile Management / Firmware Management

When using the following functions, use the PXE boot function.

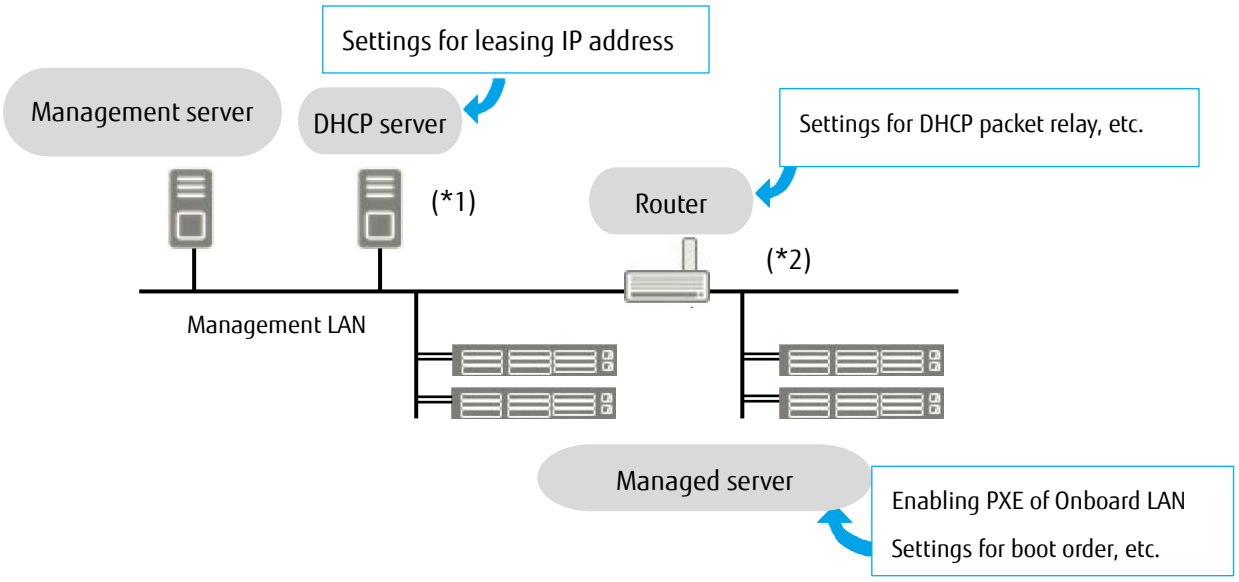
- Using the Profile Management to install an OS on a server
- Using the Firmware Management to execute offline update of a server or an installed IO card.

To operate PXE correctly, adequate prior preparation for managed server (node) and network configurations are required. This section provides information on the required operations for PXE boot.

Please note that for profile assignment other than OS installation and execution of firmware online update, the operations described in this section are not required.

1.1.1 Network Configuration Example

An example of network configuration in using PXE boot function and major preparatory operations are described below.



(*1): Instead of preparing an external DHCP server, you can use the DHCP server function in the ISM-VA (management server).
You can choose to use either the external DHCP server or the DHCP server in the managed server.

(*2): If the network segment is not split, a router is not required.

1.1.2 Required preparatory operations

Managed Server

You can use the onboard LAN port (*1) or LAN card for the PXE boot function.
Change BIOS settings as required and enable PXE boot from the LAN port. (*2)

(*1) Depending on the model of managed server, it may be described as “Dynamic LoM.”

(*2) You can specify the LAN port in the “PXE boot port” settings of each node.

Presetting:

- Configure so that the LAN port and PXE function are enabled.
  For onboard, these settings items are set as Enabled in factory shipment. Reset the settings items to Enabled if they have been changed to Disabled. For LAN cards, refer to the manuals, etc., of the respective cards.
- If PXE boot is set to Enabled for multiple network ports, check the settings of BIOS boot order and set the boot order so that the highest priority of ISM is given to the LAN port used for PXE boot in the network ports.

DHCP Server/Router

You can either enable the DHCP function in the ISM-VA or operate the DHCP server in the same network segment as the management server and set so that the appropriate IPv4 address can be leased to the PXE boot LAN port. Note that the lease period must be set equal to or greater than 60 minutes.

Ex.) The scope settings when ISM-VA is connected with 192.168.1.100/24
Lease range: 192.168.1.128 to 192.168.1.159
Lease period: 8 days

If the managed server is connected with the network of a different segment, set up a router so that the DHCP packets, etc., required for PXE boot can be transferred to each other between the segments.
Likewise, set up the variety of ports used by ISM so that their communication is available.

ISM (Management Server)

There is no specific setting for PXE boot. Follow the "User’s Manual" to execute the procedures below.

- Allocating virtual disk(s) to overall ISM-VA/allocating virtual disk(s) to user groups
- Importing OS installation DVD (For OS installation)
- Importing ServerView Suite Update DVD (For Office update)
- Importing ServerView Suite DVD
- Registering managed server in ISM
  * When registering in ISM, register the iRMC user with “OEM” or “Administrator” authorization.

1.2 Pre-settings for Virtual Resource Management

Operations of virtualization platform can be monitored by using Virtual Resource Management.

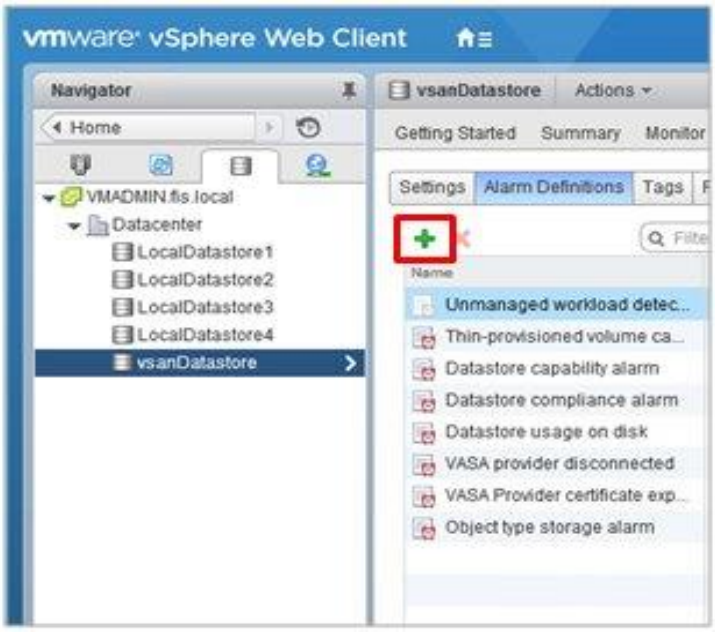
This section provides information about pre-settings required for Virtual Resource Management.

1.2.1 Pre-settings for VMware VSAN

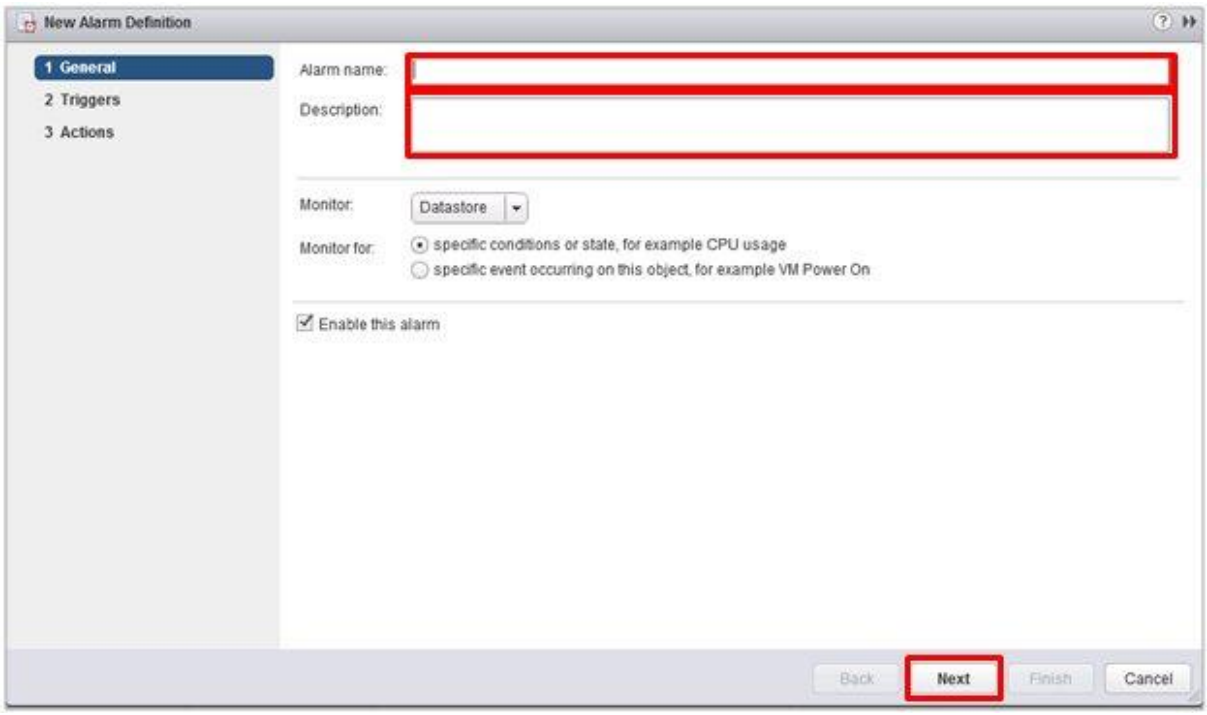
VMware VSAN alarm definition is required to enable the detection of VSAN datastore errors caused by a network disconnection between the VSAN hosts. The procedure below describes how to add VSAN alarm definitions.

I. Open the vSphere Web Client screen, from [Home] - select storage and select the created VSAN datastore.

   From the [Management] tab (or from the [Monitor] tab and select [Issues] in case of vCenter Server Appliance 6.5), select [Alarm Definitions] on the right side of the displayed screen and select [+].

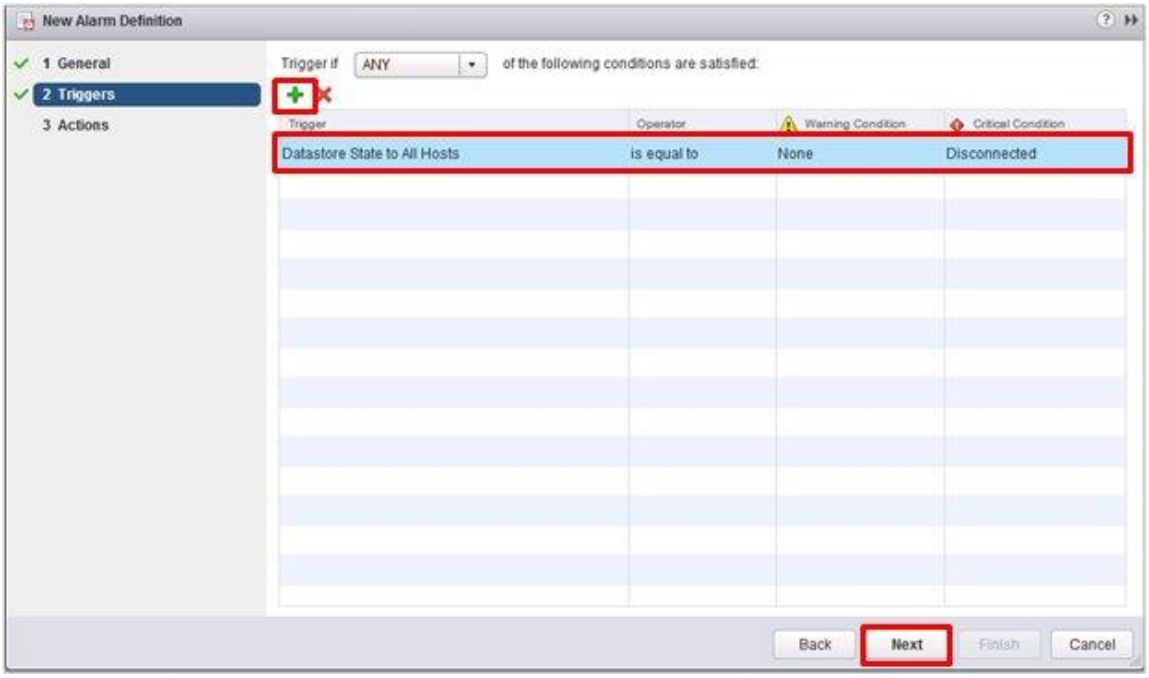


II. When the wizard screen is displayed, fill in [Alarm name] and [Description] as in the following chart, and then select the [Next] button.



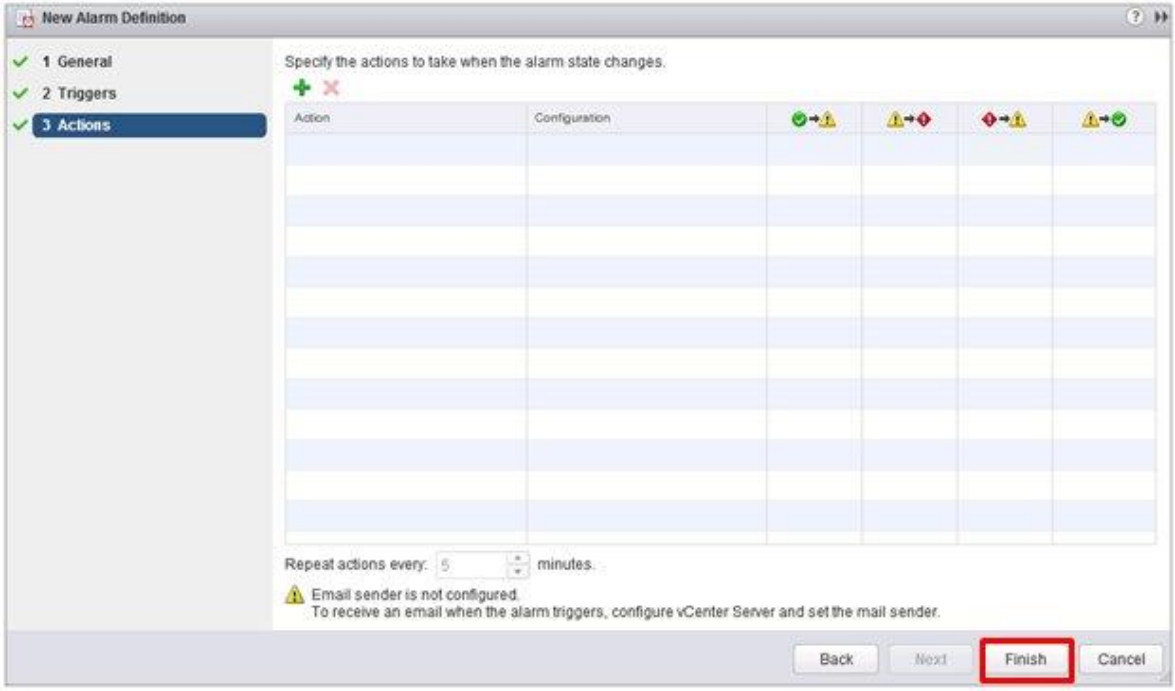
Item	Content
Alarm Name	Network disconnection between hosts
Description	Alarm when the network between the hosts is disconnected.

III. Select the [+] in the following screen, then set the items as in the following chart and select the [Next] button.

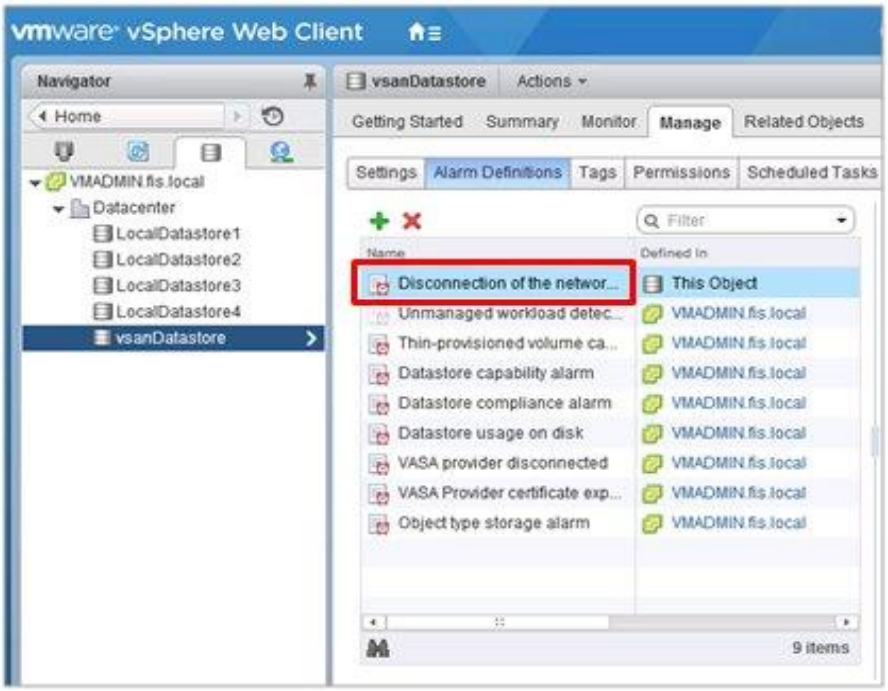


Item	Parameter
Trigger	Datastore Status to All Hosts
Operator	is equal to
Warning requirements	None
Maximum requirements	Disconnected

IV. No need to set Actions. Select the [Finish] button.



V. The new definition is added to the alarm definitions when completed.



1.2.2 Pre-settings for Storage Spaces Direct

For operation management of Microsoft Storage Spaces Direct, it is required to enable CredSSP authentication for all the nodes configure the memory storage pools, and settings for OS monitoring for ISM-VA. Execute it using the following procedure.

Settings for ISM-VA

Execute the settings for OS monitoring from ISM. For the setting procedure, refer to the “Section 2.1 of Setting procedures for Windows" in "Settings for Monitoring Target OS and Cloud Management Software."

Settings for nodes

Enable CredSSP authentication for all the nodes configure the memory pools.

Note

If you do not execute these settings, Virtual Resource Management cannot be used for Storage Spaces Direct.
The nodes configure the memory pools can be checked from the Server Manager and the Failover Cluster Manager.

I. Log in to the node as a user with domain administrator privileges and start PowerShell.
II. Execute the following command.

```
Enable-WSManCredSSP -Role client -DelegateComputer <Target node (Computer) name>
```

Wild card (*) can be used to specify all of the computer names in a domain.
Example:

```
Enable-WSManCredSSP -Role client -DelegateComputer *.pfdomain.local
```

III. And then, execute the following command.

```
Enable-WSManCredSSP -Role server
```

1.3 Notes on MIB File Import

This section describes the format of MIB file import in using ISM.

1.3.1 About the description format of MIB

By describing the specific format for the annotation in the trap definition, it is possible to indicate the severity of MIB etc., but it may not be processed as defined depending on the contents.

The annotation format of the Trap definition (TRAP-TYPE/NOTIFICATION-TYPE) of MIB conforms to the format proposed by Novell NMS.

Examples :

```
sniScVoltageTooHigh TRAP-TYPE
ENTERPRISE sniServerMgmt
VARIABLES {
trapServerName,
trapTime,
trapCabinetNumber,
trapObjectNumber,
trapString
}
DESCRIPTION
        "Power supply voltage is too high."
--#TYPE         "Voltage too high"
--#SUMMARY "Power supply voltage %d (%s) in cabinet %d at server %s is too high."
--#SEVERITY          CRITICAL
::= 652
```

Description of Comment Field

--#TYPE	Short name for the Trap. This name can be up to 40 characters long. It is used as a part of the trap message in ISM.
--#SUMMARY	Description of the trap with placeholders and format information for the actual parameters for trap transmission. It is used as a part of the trap message in ISM.
--#ARGUMENTS	List of parameters to substitute in the SUMMARY string. Parameters are substituted in the order in which they appear in the list. Each element of the list is the index (zero-based) of the parameter in the VARIABLES clause.
--#SEVERITY	Default severity assigned to the trap. This can be one of the following: - INFORMATIONAL - MINOR - MAJOR - CRITICAL

Note

- If --#TYPE is not defined, the object name is substituted.
- If --#SUMMARY is not defined, the contents of DESCRIPTION is substituted.
- If --#SEVERITY is not defined or if the severity type other than INFOMATIONAL/MINOR/MAJOR/ CRITICAL is defined, the severity of the trap is handled as INFORMATIONAL.

1.3.2 Countermeasure for when unknown trap was received

At the time of the trap reception, if the corresponding MIB is not registered, the severity is displayed as Unknown and the incorrect message will be displayed. If you receive the unknown trap, import the latest MIB and update the data. If you still receive the unknown trap even after the update, confirm that there is no abnormality in the devices.

Chapter 2 Details of Managed Nodes Settings

2.1 List of Available Port Numbers

It is required for ISM to communicate with devices. This section provides the information required on the available port numbers for communications. You must set these according to your device type or environment.

Available port numbers for ISM (The default port numbers)

Applicable Model	Function	Protocol	Available Port
PRIMERGY (RX/BX/CX/TX) PRIMERQUEST 3000B IPCOM VX2 (except PRIMERGY CX1430 M1)	Retrieval of node information	IPMI / HTTPS	623/443
	Monitoring	IPMI	623
	Trap reception	SNMP (Trap)	162
	Firmware update	IPMI / TFTP	623 / 69
	Log collection	IPMI / SSH / HTTPS	623 / 22 / 443
	Profile assignment (general)	IPMI	623
		HTTP	80
		HTTPS	443
	Profile assignment (only upon OS installation)	FTP	21
		DHCP	67
		TFTP	69
		SMB	445
		PXE	4011
		ISM-original	9213
PRIMERGY CX1430 M1	Retrieval of node information	IPMI / HTTPS	623 / 443
	Monitoring Firmware update	IPMI	623
PRIMERGY BX Chassis (MMB)	Retrieval of node information	SNMP / SSH	161 / 22
	Monitoring	SNMP / SSH	161 / 22
	Trap reception	SNMP (Trap)	162
	Firmware update	SNMP / SSH TFTP	161 / 22 69
	Log collection	SSH	22
PRIMEQUEST 2000Type3 PRIMEQUEST 3000E	Retrieval of node information	SNMP / IPMI	161 / 623
	Monitoring	SNMP / IPMI	161 / 623
	Trap reception	SNMP (Trap)	162
	Firmware update	FTP / SSH	21 / 22
	Log collection	IPMI	623
ETERNUS DX/AF	Retrieval of node information	SNMP / SSH	161 / 22
	Monitoring	SNMP	161
	Trap reception	SNMP (Trap)	162
	Firmware update	FTP / SSH	21 / 22
	Log collection	FTP / SSH	21 / 22

Applicable Model	Function	Protocol	Available Port
	Profile assignment	SSH	22
ETERNUS NR (NetApp)	Retrieval of node information	SNMP / SSH	161 / 22
	Monitoring	SNMP / HTTPS	161 / 443
	Trap reception	SNMP (Trap)	162
	Firmware update	-	-
	Log collection	SSH / HTTPS	22 / 443
	Profile assignment	-	-
SR-X	Retrieval of node information	SNMP / SSH	161 / 22
	Monitoring	SNMP	161
	Trap reception	SNMP (Trap)	162
	Firmware update	FTP / SSH	21 / 22
	Log collection	SSH	22
	Profile assignment	SSH	22
PSWITCH 2048P/T PSWITCH 4032P (supported ISM 2.3.0.b or later)	Retrieval of node information	SNMP / SSH	161 / 22
	Monitoring	SNMP	161
	Trap reception	SNMP (Trap)	162
	Firmware update	FTP / SSH	21 / 22
	Log collection	SSH	22
	Profile assignment	SSH	22
ExtremeSwitching VDX (Brocade VDX) (hereinafter, referred to as "VDX")	Retrieval of node information	SSH	22
	Monitoring	SNMP	161
	Trap reception	SNMP (Trap)	162
	Firmware update	FTP / SSH	21 / 22
	Log collection	SSH	22
	Profile assignment	SSH	22
Catalyst 3750-X Nexus 5000 Series	Retrieval of node information	SSH	22
	Monitoring	SNMP	161
	Trap reception	SNMP (Trap)	162
CFX2000F/R PRIMERGY Switch Blade / Converged Fabric Switch Blade (10Gbps 18/8+2)	Retrieval of node information	SSH	22
	Monitoring	SNMP	161
	Trap reception	SNMP (Trap)	162
	Firmware update	FTP / SSH	21 / 22
	Log collection	SSH	22
	Profile assignment	SSH	22
PRIMERGY BX Switch Blade (1Gbps/10Gbps)	Retrieval of node information	SSH	22
	Monitoring	SNMP	161
	Trap reception	SNMP (Trap)	162
	Firmware update	FTP / TFTP SSH	21 / 69 22
	Log collection	SSH	22
PRIMERGY BX LAN Pass-Thru Blade	Retrieval of node information Monitoring	SNMP	161 (communicate with MMB)
	Trap reception	SNMP (Trap)	162
Brocade FC Switch	Retrieval of node information	SSH	22
	Monitoring	SNMP	161
	Trap reception	SNMP (Trap)	162
PRIMERGY BX FC Switch Blade	Retrieval of node information	SSH	22
	Monitoring	SNMP	161
	Trap reception	SNMP (Trap)	162

Applicable Model	Function	Protocol	Available Port
	Firmware update	SSH	22
	Log collection	SSH	22
Asetek Rack CDU Schneider Electric Metered Rack Mount PDU Schneider Electric Smart-UPS	Retrieval of node information	SNMP	161
	Monitoring	SNMP	161
	Trap reception	SNMP (Trap)	162

Target OS	Function	Protocol	Available Port
Windows	Retrieval of OS information	WSMAN	5986
	Monitoring	WSMAN	5986
	Firmware update	-	-
	Log collection	WSMAN	5986
Linux	Retrieval of OS information	SSH	22
	Monitoring	SSH	22
	Firmware update	SSH	22
	Log collection	SSH	22
VMware ESXi	Retrieval of OS information	vSphere API / CIM	443 / 5989
	Monitoring	vSphere API	443
	Firmware update	-	-
	Log collection	REST	443

2.2 Details of Node Settings

To manage nodes with the use of ISM, it is required to set up the connection information on the node side. This section provides the required connection information for set up.

2.2.1 Connection Information

To establish a connection with the nodes, and before performing node registration, the following settings are required on the node side. For more information, refer to the manuals of the respective devices.

Y: Required -: Not required

Node	Connection Information			
	IPMI Account (*1)/ Password	SSH Account / Password	Information Required to Enter for SNMP (*2)	HTTPS Account / Password
PRIMERGY(RX/CX/TX) (Except for CX1430 M1)	Y	-	-	- (*4)
PRIMERGY CX1430 M1	Y	-	-	Y
PRIMEQUEST 2000Type3	Y	Y	Y	–
PRIMEQUEST 3000E	Y	Y	Y	–
PRIMEQUEST 3000B	Y	-	-	- (*4)
ETERNUS DX/AF	-	Y	Y	–
ETERNUS NR	-	Y	Y	–
SR-X	-	Y	Y	–
PSWITCH 2048P/T PSWITCH 4032P (supported ISM 2.3.0.b or later)	-	Y	Y	–
VDX (Brocade VDX)	-	Y	Y	–
Brocade FC Switch	-	Y	Y	–
Cisco Catalyst	-	Y	Y	–
Cisco Nexus	-	Y	Y	–
PRIMERGY BX Chassis (MMB)	-	Y	Y	–
PRIMERGY BX Server Blade	Y	-	-	–
PRIMERGY BX Switch Blade (1Gbps/10Gbps)	-	Y	Y	–
PRIMERGY BX LAN Pass-Thru Blade	-	-	- (*3)	–
PRIMERGY BX FC Switch Blade	-	Y	Y	–
PRIMERGY Switch Blade / Converged Fabric Switch Blade (10Gbps 18/8+2)	-	Y	Y	–
CFX2000F/R	-	Y	Y	–
AsetekRackCDU	-	-	Y	–
SchneiderElectric Metered RackMountPDU	-	-	Y	–
SchneiderElectric Smart-UPS	-	-	Y	–

For the models which are confirmed for operation, please contact your local Fujitsu customer service partner.

(*1): Use the account with administrator access privilege or OEM.

(*2): For SNMP v1 or v2, it is required to enter the community name.

For SNMP v3, it is required to enter the user name, security level, authentication protocol (when authentication is used), authentication password (when authentication is used), encrypted protocol (when encryption is used), encrypted password (when encryption is used).

(*3): PRIMERGY BX LAN Pass-Thru Blade requires connection information settings of the chassis (MMB).

(*4): You can only specify HTTPS port number. The account/password will be the same as its IPMI.

2.2.2 Required Settings for Management

Confirm the following settings in addition to the connection information settings.

[PRIMERGY]

- When you are using the iRMC S4 firmware version 9.00 or later for the PRIMERGY S8/M1/M2/M3 generation server, it is required to change the IPMI Privileges and Permissions of Web UI of iRMC to retrieve the SAS card information of the ISM node details.
  Execute the following procedure to change the IPMI Privileges and Permissions.
  [User Management] – [iRMC S4 User Management] – [IPMI Privileges/Permissions] - mark the checkbox of [Redfish Enabled].
  [User Management] – [iRMC S4 User Management] – [IPMI Privileges/Permissions] - change the box of [Redfish Role] to Administrator.

[SR-X]

- Enable LLDP settings

[VDX (Brocade VDX)]

- Enable LLDP settings
- Set the IP address of the management LAN port for each switch

[ETERNUS DX/AF]

- As the port connecting to ISM, use the maintenance port of Control Module.
  (If connecting to a remote port, the firmware update function, the log collection function and profile assignment function may not work.)

[PRIMEQUEST 2000 Type3, PRIMEQUEST 3000E]

- For the MMB account settings (account settings for IPMI connection) for ISM, use the account that

registered in the Web UI [Network Configuration] → [Remote Server Management] of PRIMEQUEST.

- For the SSH account settings for ISM, use the account that registered in the WEB UI [User Administration] → [User List] of PRIMEQUEST. The access privileges must be administrator or CE.

[PRIMERGY BX]

- Switch Blade: Enable LLDP settings
- Fibre Channel Switch Blade : Enable SW-MIB settings
  Example of command execution:

```
snmpconfig --enable mibCapability -mib_name SW-MIB
```

- When the power of the Chassis is OFF, information cannot be retrieved from MMB. Therefore, the relation between the server blade and connection blade look temporarily cancelled. When the status of the power is ON, select the chassis, go to the [Action] button - [Get Node information] and execute the operation.

2.2.3 Required Settings for Notification

Make the settings for SNMP traps in addition to the settings for connection information and for required information for management.
For details, refer to the manuals of the respective devices.

For the devices listed below, Engine ID is automatically input when selecting the target node in Trap Reception settings.

Y: Supported　- : Not supported

Node	Availability of Automatic input of Engine ID
PRIMERGY(RX/CX/TX)	Y
PRIMEQUEST 2000Type3	-
PRIMEQUEST 3000E	Y
PRIMEQUEST 3000B	Y
ETERNUS DX/AF	Y
ETERNUS NR	-
SR-X	Y (*1)
PSWITCH 2048P/T PSWITCH 4032P (supported ISM 2.3.0.b or later)	Y
VDX (Brocade VDX)	Y
Brocade FC Switch	Y
Cisco Catalyst	Y
Cisco Nexus	Y
PRIMERGY BX Chassis (MMB)	-
PRIMERGY BX Server Blade	Y
PRIMERGY BX Switch Blade (1Gbps/10Gbps)	Y (*1)

Node	Availability of Automatic input of Engine ID
PRIMERGY BX LAN Pass-Thru Blade	-
PRIMERGY BX FC Switch Blade	Y
PRIMERGY Switch Blade / Converged Fabric Switch Blade (10Gbps 18/8+2)	Y (*1), (*2)
CFX2000F/R	Y (*1), (*2)
AsetekRackCDU	-
SchneiderElectricMetered RackMountPDU	-
SchneiderElectricSmart-UPS	-

(*1): When SNMP v3 Engine ID is not set for the following devices and selecting the target node in the ISM Trap Reception settings, the Engine ID is not automatically input. To automatically input the Engine ID, set the SNMP v3 Engine ID for the devices in advance.

- PRIMERGY BX Switch Blade (10Gbps)
- PRIMERGY Switch Blade / Converged Fabric Switch Blade (10Gbps 18/8+2)
- CFX2000F/R
- SR-X

(*2): When fabric is configured and SNMP v3 Engine ID has been set for the devices, set each Engine ID with the same values in the whole fabric.

Chapter 3 Details of Other Settings

3.1 ETERNUS DX/AF Drive Enclosure Display

ISM is capable of managing drive enclosures connected to a control enclosure of ETERNUS DX/AF as its nodes.

This section provides the required setting information to manage drive enclosures.

3.1.1 Registration of Drive Enclosure

A drive enclosure is automatically registered with ISM as its node by the following procedure.

I. Register the controller enclosure of ETERNUS DX/AF with ISM as its node and a drive enclosure connected.

II. After completion of node information retrieval of the controller enclosure, the drive enclosure is displayed on a node list.

3.1.2 Details of Node Information of Drive Enclosure

The details of node information of the drive enclosure is displayed in the details of node information of the controller enclosure in ISM.

3.1.3 Status of Drive Enclosure

The drive enclosure status is always displayed as "Unknown." This is because the drive enclosures are intensively managed by a controller enclosure. Refer the controller enclosure node information.

3.1.4 Deletion of Drive Enclosure

Drive enclosure is deleted from a node list in the following cases.

- Controller enclosure node information retrieval is executed after a drive enclosure is cut off from the controller enclosure.
- The node of the controller enclosure is deleted from ISM.

3.2 General Standards for Firmware Update Time

It may take time to update firmware with the use of the Firmware Manager of ISM. This section provides guideline standards for the time required to update firmware.

When making plans to update firmware, refer the times described below. Moreover, interrupting the firmware update before completion should be avoided.

Note

The times described below indicate the time taken for updating the current firmware with standard configurations. Since the time may vary depending on the firmware version, network configurations and/or network load conditions, it is recommended to plan with enough margin, including time to address unexpected troubles.

General Standards for Firmware Update Time

Target of Firmware Update	Standard Time / Unit	Note
Firmware update of iRMC in PRIMERGY	Online update 10 to 20min.	
	Offline update 15 to 30min.	If the server is set to be turned ON after the firmware is assigned, it takes an additional 15 minutes.
Firmware update of BIOS in PRIMERGY	Online update 1 to 2min.	To assign firmware, it is required to account for time powering the server ON/OFF separately.
	Offline update 15 to 30min.	If the server is set to be turned ON after the firmware is assigned, it takes an additional 15 minutes.
Firmware update of iRMC in PRIMEQUEST 3800B	Online update 10 to 20min.	
Firmware update of BIOS in PRIMEQUEST 3800B	Online update 5 to 15min.	To assign firmware, it is required to account for time powering the server ON/OFF separately.
Firmware update of PRIMEQUEST 2000 series,3000 series	70 to 130min.	
PRIMERGY BX900S2 MMB	10 to 20min.	The time noted in the left is the time taken per

Target of Firmware Update	Standard Time / Unit	Note
		MMB.
Firmware update of network switch SR-X	2 to 10min.	
Firmware update of fabric switch CFX2000R/F, converged fabric switch blade	10 to 20min.	
Firmware update of converged switch VDX	15 to 30min.	
Firmware update of PSWITCH 2048P/T PSWITCH 4032P (supported ISM 2.3.0.b or later)	20 to 30min.	
Firmware update of LAN switch blade	10 to 20min.	
Firmware update of Cisco Systems Nexus series	30 to 50min.	
Firmware update of Cisco Systems Catalyst series	10 to 20min.	
Firmware update of FC switch blade	10 to 20min.	
Firmware update of PCI card	Online update 5 to 15min.	To assign firmware, it is required to account for time powering the server ON/OFF separately. The time noted in the left is the time taken per card.
	Offline update 15 to 20min.	The time noted in the left is the time taken per card.
Firmware update of ETERNUS DX/AF series	10 to 60min.	When a unified environment exists and multiple controller enclosures are installed, the update time will be longer.

3.3 General Standards for Disk Usage in Using Log Management

ISM is capable of periodically collecting logs from nodes and accumulating them on ISM-VA by using the Log Management. This section provides the information on the area for accumulating the collected logs and general standards for accumulated data amount.

The collected logs are accumulated on the log storage area on a virtual disk(s) allocated to user groups. See allocation of virtual disk to each user group of ISM-VA.

Note

- The following are the default settings for log retention period and the number of generations. Change the log retention period and the number of generations as required.
-

Archived Logs	Node Logs (data for download/data for log search)
7 Generations	30 days

・ The capacity described on this document is reference value for specific configurations and operations. The capacity can vary greatly depending on the actual use conditions.

3.3.1 Type of Managed Logs and their Accumulation Area

Log Management creates archived logs, node logs (data for download) and node logs (data for log search) after the collection of logs.

Each of the above logs is accumulated in the following log storage areas.

Log Type	Storage Area
Archived Logs	Log storage area for the user group Related to the node group to which a node belongs (*1)
Node Logs (data for download)	
Node Logs (data for log search)	Log storage area for Administrator group (*2)

(*1) If a node group is not related to a user group, these logs are accumulated in the log storage area of Administrator group.

(*2) The node logs (data for log search) of all nodes are accumulated in the log storage area of the Administrator group. Even if a node group is related to a user group(s) other than the Administrator group, these logs are accumulated in the log storage area of the Administrator group.

3.3.2 General Standards for Log Capacity

[Capacity for Archived Logs]

General Standard for one generation per node

Log Collection Target			Standard Capacity
Hardware	Server	PRIMERGY	1KB
		PRIMEQUEST 3000B	1KB
		IPCOM VX2	1KB
	Chassis	PRIMERGY BX	100KB
		PRIMEQUEST 3000E	50KB
	Connection Blade	Ethernet Switch	100KB
		Fibre Channel Switch	10MB
	Switch	SR-X	50KB
		CFX	100KB
		PSWITCH 2048P/T PSWITCH 4032P (supported ISM 2.3.0.b or later)	350KB
		VDX (Brocade VDX)	50MB
		Cisco Catalyst	1MB
		Cisco Nexus	1MB
	Storage	ETERNUS DX/AF	10MB
		ETERNUS NR (NetApp) Cluster	100KB
		ETERNUS NR (NetApp) Chassis	500MB
Operating system	Windows		5MB
	Linux		5MB
	VMware ESXi		3MB
	IPCOM OS		50MB
ServerView Suite	ServerView Agents		Windows：10MB Linux：80MB
	ServerView Agentless Service		
	ServerView RAID Manager		

[Capacity for Node Logs (data for download)]

General standard for 30 days' worth per node

Log Collection Target			Standard Capacity
Hardware	Server	PRIMERGY	50KB
		PRIMEQUEST 3000B	50KB
		IPCOM VX2	50KB
	Chassis	PRIMERGY BX	50KB
		PRIMEQUEST 3000E	500KB
	Connection Blade	Ethernet Switch	100KB
		Fibre Channel Switch	50KB
	Switch	SR-X	100KB
		CFX	100KB
		PSWITCH 2048P/T PSWITCH 4032P (supported ISM 2.3.0.b or later)	150KB
		VDX (Brocade VDX)	100KB
		Cisco Catalyst	50KB
		Cisco Nexus	50KB
	Storage	ETERNUS DX/AF	100KB
		ETERNUS NR (NetApp) Cluster	200KB
Operating system	Windows		1MB
	Linux		1MB
	VMware ESXi		4MB
	IPCOM OS		1MB

[Capacity for Node Logs (data for log search)]

General standard for 30 days' worth per node

Log Collection Target			Standard Capacity
Hardware	Server	PRIMERGY	500KB
		PRIMEQUEST 3000B	500KB
		IPCOM VX2	500KB
	Chassis	PRIMERGY BX	500KB
		PRIMEQUEST 3000E	500KB
	Connection Blade	Ethernet Switch	1MB
		Fibre Channel Switch	500KB
	Switch	SR-X	1MB
		CFX	1MB
		PSWITCH 2048P/T PSWITCH 4032P (supported ISM 2.3.0.b or later)	1MB
		VDX (Brocade VDX)	1MB
		Cisco Catalyst	500KB
		Cisco Nexus	500KB
	Storage	ETERNUS DX/AF	1MB
		ETERNUS NR (NetApp) Cluster	2MB
Operating system	Windows		15MB
	Linux		15MB
	VMware ESXi		50MB
	IPCOM OS		15MB