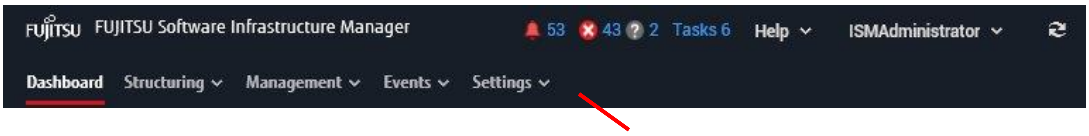
Infrastructure Manager /
Infrastructure Manager for PRIMEFLEX V3.0.0
Glossary

Edition 2.0 November 2024

CA92344-5738-02
Fsas Technologies Inc.

Modification History		
Edition	**Issue Date**	**Modification Overview**
1.0	September 2024	First Edition
2.0	November 2024	Changed the function name from "profile/policy for each model" to "profile/policy for specific model"

No.	Terms	Definitions
1	3D View	Displays in 3D the racks placed on the floor and the nodes inside the racks, and monitors the status of air inlet temperature and power consumption from a bird's eye view.
2	Account	Account is a string used as a label to identify the user of the computer. In ISM, user accounts to log in to ISM and account for nodes are used.
3	Alarm	Event notifications sent from nodes, notified information to nodes, and SNMP trap occurrences are collectively referred to as alarms. The alarms detected by ISM can be displayed on the screens below. ● [Events] - [Events] - [Operation Log] screen ● [Events] - [Events] - [SNMP Traps] screen The alarm that will be recorded on the operation log is classified based on the severity of the information; Error, Warning, or Info. For SNMP Trap, it is classified as Critical, Major, Minor, or Informational. An alarm setting can be specified which action to take when ISM detected the alarms.
4	Alarm Status	The alarm status is shown for each node where ISM detects the alarms. This means that more than one alarm has been detected on the corresponding node. The alarm status is deleted as the alarm confirmed by the operation of canceling the alarm.
5	Analysis VM	Analysis VM is a virtual machine to analyze the traffic of virtual environment.
6	Anomaly Detection	Anomaly Detection is to detect behavior that is not normal for the operation of hardware and software and the use of their resources.
7	Archived log	The log that collects node information and incorporates the status into ISM is called the archived log. The node has the following node information. ● Hardware log ● Operating system log ● ServerView Suite log
8	Audit log	When ISM has detected the following events, it is recorded as an audit log. ● User log in, log out, log in failure ● Unauthorized URI access ● Start, stop and anomalies in ISM ● Record of settings and operations of managed nodes The audit log can only be viewed by the ISM administrator.
9	Authentication Code	The information required to log in, in addition to the username and password, for the user with Multi-Factor Authentication enabled. This is the number that is displayed on the multi-factor authentication client application after the QR code displayed by ISM that is scanned by the multi-factor authentication client application installed on the device. It may also be called one-time passwords or verification code, depending on the multi-factor authentication client application.
10	CA Certificate	A certificate signed by a certification authority (CA)
11	Cloud Management Software	In addition to VMware vCenter Server and Microsoft System Center, ISM also handles Microsoft Failover Cluster as a Could Management Software. For the details of the supported cloud management software, refer to "User's Guide" - "Management of Cloud Management Software".
12	Dashboard	Screen that can display summarized outlines of the status of nodes etc. On Dashboard, various purposes of widgets can be selected and displayed as needed.

No.	Terms	Definitions
13	Emergency Code(s)	The code used in Multi-Factor Authentication when the device displaying the Authentication Code becomes unusable due to malfunction or loss. You can log in to ISM using Emergency Code(s) instead of the Authentication Code.
14	Event	Event signifies all the incidents occurring on nodes managed by ISM and on cloud management software, and on ISM itself. Events are managed by the classification of operation logs, audit logs, and SNMP Traps.
15	Event Output Restricted Mode	Indicates whether or not to output events (described in No.14) to operation logs or audit logs. When Event Output Restricted Mode is enabled, ISM prevents events from occurring by stopping access to the management of cloud management software. Note that Event Output Restricted Mode is not enabled for nodes managed by ISM.
16	Event log	One of the logs output when node logs are displayed. Logs related to events.
17	Firmware Baseline	A function to compare the firmware versions between the managed node and the assigned firmware. This displays whether the node is operating with the intended firmware version compared with the user assigned firmware version.
18	Floor View	Image displaying the positions of the racks on the floor. Makes it possible to monitor the status of nodes within the racks deployed on the floor from a bird's eye perspective.
19	Global navigation menu	The root menu at the top of each ISM screen.  FUJITSU FUJITSU Software Infrastructure Manager 53 43 2 Tasks 6 Help ISMAdministrator Dashboard Structuring Management Events Settings Global Navigation Menu
20	HCL	Abbreviation for Hardware compatibility List. A list of firmware that is compatible with the OS (VMware ESXi version) and certified to operate.
21	ISM	Abbreviation of the product Infrastructure Manager.
22	ISM Administrator	ISM users who belong to an Administrator group and have an Administrator role.
23	ISM-VA	This product is provided in virtual appliance format. The virtual appliance that packaged ISM is described as ISM-VA.
24	Infrastructure	The ICT devices (servers, storages, switches) and server OS/hypervisors making up the information system.
25	Link with ISM	This is the link to display the information of the status of other ISM on Dashboard.
26	Link with Microsoft Active Directory Group	A function that links the groups of ISM to groups on Microsoft Active Directory. User accounts that belong to Microsoft Active Directory groups can log in to ISM without creating a user account in ISM.
27	Maintenance Mode	This setting indicates whether or not events (described in No.14) that occur on nodes managed by ISM or on ISM itself should or should not be output to the operation logs and audit logs. When Maintenance Mode is enabled, ISM prevents events from occurring by stopping access to management of the node.

No.	Terms	Definitions
28	Management server	A virtual machine on which ISM-VA runs is referred to as management server.
29	Management terminal	PC or tablet to operate ISM.
30	MS Storage Pool	Virtualized storage area managed by Microsoft Storage Spaces Direct. MS Storage pools is the software defined of multiple physical disks installed in a server as a virtualized storage area.
31	Network Map	The screen to manage the network. It is available to display the network connection status between nodes and to check the port settings, etc.
32	Node	The ICT equipment and facilities that are management targets of ISM are referred to as nodes.
33	Node Group	The management unit for nodes. Nodes are grouped into units according to the actual tasks, sections, etc. ISM can manage the target nodes by grouping. Node groups are managed by being correlated with user groups.
34	Node Status	Node Status is shown the actual status retrieved from the node.
35	Node log	The node log displays the log information that the node has (refer to the "Archived log") according to the requirement settings.
36	Offline Update	The firmware update when the node is powered off (For PCI cards, the server on which a PCI card is mounted is powered off).
37	Online Update	The firmware/driver update when the node is powered on (For PCI cards, the server on which a PCI card is mounted is powered on). For servers (BIOS/iRMC), it can be performed even when powered off.
38	Operation log	One of the logs that are output when node logs are displayed. Logs related to operation.
39	Operation log (ISM)	When the following events are detected by ISM, it is recorded as an operation log. ● The node status change in normal waiting status - abnormal status ● The temperature, power consumption, FAN rotation speed, resource utilization rate, disk transfer speed, and network transfer volume has become out of the normal range set for ISM ● Start and finish of the task ● Start, stop, and anomalies of ISM ● A record of settings and operations of managed nodes
40	Policy	Policy helps profile settings. Policy sets the same values for the same setting items for multiple profiles.
41	Policy Group	Profile Group/Policy Group To make it easy to handle large numbers of profiles and policies, besides creating optional groups with individual tree structures for profiles and policies, these can be created in special groups. Apart from the optionally created groups, groups created as default status also exist.
42	Power Capping	Sets an upper limit value for the power consumption of a rack, and controls the devices mounted in the rack to make sure that it keeps its target.
43	Power Capping Policy	Indicates the definitions of operation patterns in the Power Capping function. There are four types of definitions; two types of custom definitions, one definition of scheduling operation, and one definition of minimum power consumption operation. This function defines the upper limit value for power consumption in accordance with the operation pattern, and it can be operated by switching the operation pattern.

No.	Terms	Definitions
44	Privilege for VA Operation	Privilege required for registration, deletion, and replacement of environment settings, basic settings, and licenses of ISM-VA from the REST API.
45	Profile	Profiles have aggregated data to set the setting values for nodes in a batch. When a node is set in ISM, the steps are to first create a profile, which is then assigned. Both the node hardware settings and the OS installation can be performed through the profile.
46	Profile for specific model Policy for specific model	Profiles/Policies that can be set more detailed hardware settings by retrieving the setting items for specific model from the nodes. Profile for specific model can be assigned to the same model that retrieved the setting items. Policy for specific model is a structure that extracts the contents that have the same settings among multiple profiles for specific model and sets them all at once.
47	Rack View	Displays an image of the mounting positions of the nodes in a rack. The node model name, node status (normal/abnormal), node LED light status (On/Off) etc., are displayed.
48	Remote Script	Indicates the patch files, shell script files saved on the OS for the external host. This script is used in [Event] - [Alarms] - [Actions] screen - "Execute Remote Script".
49	Repository	The area in ISM-VA that ISM to store various types of data. It is mainly used for the following purposes: ● Storing firmware for firmware updates ● Storing OS installation images for OS installation ● Storing ServerView Suite DVDs for OS installation
50	SDS	Abbreviation for Software Defined Storage. Indicates a storage where the physical disks installed in the servers are collectively software-defined, as well as its management technology.
51	Security log	One of the logs output when node logs are displayed. Logs related to security.
52	Self-Signed Certificate	An SSL certificate that is signed with the private key of the server using the certificate
53	Setup Key	The string to set in the multi-factor authentication client application. For users with Multi-Factor Authentication enabled, this is an alternative to scanning the QR code that is displayed in the ISM GUI when logging in for the first time. It may also be called a private key or code, depending on the multi-factor authentication client application.
54	Single Sign-On	In general, Single Sign-On (SSO) is a centralized session and user authentication service in which one set of login credentials (authentication) can be used to access (permit) multiple web servers. Single Sign-On for ISM is a function that enables you to operate nodes that are registered on the Web GUI of a PRIMERGY server (iRMC), when you log in to ISM.
55	SSL Certificate	A digital certificate for SSL or TLS encrypted communication
56	Storage Pool (ISM)	Virtualized storage resource formed by integration of physical disks installed in the server. You can flexibly create storage resources and manage them without having to consider the physical configurations, such as the number of disks installed in the server and its capacity. The following storage pools can be managed with the ISM virtual resource management function. ● VSAN data store of VMware VSAN ● MS Storage pools of Microsoft Storage Spaces Direct
57	Storage Spaces Direct	Storage Spaces Direct or S2D. A function to manage virtual storage provided by Microsoft.

No.	Terms	Definitions
58	Task	Among the processes executed in ISM, tasks signify the processes that takes time. The status of processing is displayed on the "Task" screen. For the details of the processes executed in tasks, refer to "User's Guide" - "Task Management".
59	User Group	The unit used by ISM to manage users. There are two types of groups; administrator group and other than administrator group, such as users grouped by the actual tasks, sections, etc.
60	User Role	The operation authority used by ISM. There are three types of roles; administrator role, operator role, and monitor role. These can be assigned to arbitrary user groups.
61	vSAN	Abbreviation for Virtual SAN. A function to manage virtual storage provided by VMware.
62	Virtual Resource	Virtualized system resources managed by ISM. ISM can manage storage pools as virtual resources.
63	Widget	The various components displayed on the dashboard are called widgets. Since each widget displays different contents, allocate the widgets as needed on Dashboard.
64	[Refresh] button	The [Refresh] button is used for refreshing the screen. ISM fundamentally does not refresh the screen automatically.