

Infrastructure Manager White Paper

Software that manages and operates a data center, including servers, storage, networks, and facility devices, from one interface.

Contents

Abstract Feature 1 – Consolidation Triggering actions with API	2 2 4
Feature 2 – Visualization Visualization of CO ² Emissions for all nodes	4
Visualization of location and status of devices	
Feature 3 – Automation Device settings can be copied and applied to other devices	5
Other features Simplifiy ISM installation using virtual appliances	7 7
System Requirements Managed devices	7
Management nodes	7
Consoles	7
Licences	
Copyright Disclaimer	9 9

Abstract

Steps to improve infrastructure efficiency

In today's digital world, where more and more devices are connected via the internet, data is king and organizations that can differentiate and innovate using this information lead the game. To keep up with the increasing number of operations, companies keep adding more and more computing, storage or networking devices to the existing legacy setup. However, the number of IT resources used to manage the datacenter remains the same and hence a challenge.

Different types of devices require a variety of complex management software and tasks to manage infrastructure platforms. This leads to problems such as lower productivity, an increase in troubleshooting time and customer response time. Thanks to its total management of infrastructure platform devices, ISM solves these problems.

Fujitsu Infrastructure Manager (also referred to as "ISM" below) has a simple and intuitive interface that offers a complete view of datacenter status. One of the key functions of ISM is the multiple FW upgrading and OS deployment which significantly reduces the time and cost required for the activities. Furthermore, ISM provides an API for communicating with other applications and scripts and helps to automate tasks. ISM makes sure that sufficient datacenter infrastructure platform management is achieved.



Feature 1 – Consolidation Manage servers, storage, and network switches through a unified GUI.

A datacenter is made up of many types of devices, and the failure of one device impacts on the whole infrastructure environment, disrupting business operations. Organizations often use different vendor-specific or device-specific software to manage these components, making the overall administration inefficient and timeconsuming ISM indicates and manages servers, storage, network switches, and the entire system in a single GUI.



A variety of firmware updates can be executed in a single process

Firmware management is an important task of a datacenter administrator. Security awareness for firmware on devices and the importance of firmware management is growing. However, it is complicated for many administrators to manage it in view of the complexity and tools involved in updating each component. One of the reasons for this complexity is the existence of several types of firmware, especially on servers. BIOS, BMC, and firmware of PCI cards must be maintained. Furthermore, the update procedure is different depending on the device type and component type and is one of the key reasons which lead to firmware management difficulties.

ISM displays the firmware versions of all types of firmware and of all components in single view and provides single procedure to update all types of firmware. The administrator does not need to search for a device or component dedicated to the update procedure and can update multiple types of devices and components in a single process. The status and resources of VMware vSAN and Microsoft Storage Spaces Direct, as a base technology for HCI (Hyper Converged Infrastructure), are also displayed along with physical device information in the ISM dashboard.

RIJESU - FUERSU Software Infestructure M	anager Dashboard Structurin	y × Management × Events	∀ Settings ¥	🐥 21 📑 18 😨 1 - Taska 1	ndy v ISAAdministrator v 🍣
Virtual Resource List	Al Stronge Paols / Milesee Virtual	IAM / viactorialized			
✓ All Storage Peols	Information			Used capacity	
VMvare VitaalSAN	Status	0			Used capacity 15.7218
Microsoft Storage Spaces Direct	Pool Name	vsaidatastore1			Free capacity 6 297B
	Туре	Viduase Vidual SVN		Total capacity 22.01TB	
	Version	Virtual GAULO.2			
	Availability				
	Deduptiontion	Disable			
	Compression				
	cruster name	Vield, Boler I			
	Node List				
	Q. Search	<mark>O 🔺 🖗 🛇 </mark> 6/6			
	Node Litt				
	Node Name	Hest Name	Model Name	 IP Address 	0 OS Name 0
	-	Hadit	PRIMERAL RAZING MIZ	192.000.2013	
	1161-606W2	10612	PRIMERBY RX2530 M2	192.108.20.14	VMVate 6.0
	😋 нал-косма	HOOTO	PRIMEROV RX2530 M2	192.108.20.15	VMsvare 6.0
	😋 HSI RXSV4	H2ST4	PRIMERCY RX2530 M2	192.108.20.10	VMuare 6.0
	A HS1-0X5V5	HONTS	PRIMERCY R03530 M2	192.168.98.17	Websate 6.0
	😋 нал-колоче	HISTS	FRIMLHOV HX2530 MZ	192,168,20,10	Weater 6.0

Before

Several procedures, according to component type



Virtual resources from vCenter and other virtual machine management software are supported.

ISM can communicate with VMware vCenter Server, OpenStack, and similar kinds of virtual resource management software. It collects and displays information and status of physical and virtual nodes.

Enable visibility and control of both physical and virtual devices.

ISM collects and displays information about physical and virtual devices from VMware, Microsoft and other software. On the other hand, ISM also provides physical device information in a view on vCenter. This collaboration makes seamless, easy maintenance between virtual and physical resources.

VMINUT VALCHAR VALCHAR 41 C1 C1 Advancementation Control C1 C1 Advancementation Control C1 <

When a physical server has to be booted to maintain the system, seamless procedures, such as the shutdown or migration of virtual machines, checking of physical server inventory, and updating of firmware, are possible in VMware or Microsoft view.

Triggering actions with API

All functions and information provided in the ISM GUI can be triggered with external programs or scripts using integrated API. ISM can be integrated in an existing management stack using an API.

Feature 2 – Visualization Visualization of CO² Emissions for all nodes

ISM collects and displays the carbon footprint of nodes with power consumption support. Sustainability monitor support graphical and trend analysis of CO2 emissions, ranking high-emission nodes, and exporting data for external reporting.



Visualization of location and status of devices

Devices mounted on a rack are visualized in an ISM view. Devices have an LED on the front panel to indicate status and the indicator is also visible. Administrators can see the location of a failed device in a rack as if they were standing in front of it.

2 I	808-1	> 🔥 rack-1		4
41 SW HS1-VDX-gyo 40 SW HS1-VDX-gyo 39	mu-1 mu-2	✓ 📕 HS1-RX-SV	/-4	Operate ID LED
38 SW HS1-VDK-kann	61	* 🖲		
36		Name	HS1-RX-SV-4	
35 SW Fabric switch-1		Status	Normal	
33		Alaum Status	() Noos	
32		Alarm Status	io reone	
31 SV HS1-RX-SV-1		Model Name	PRIMERGY RX2530 M2	
29 SV H51-RX-SV-3	0 & CI5 10	IP Address	192.168.20.16	
28 SV H51-8X-SV-4	0 🔺 CE 10	Mounting Position	28	
26 SV HS1-8X-SV-6	0 & C5 ID	Web i/f URI	https://192.168.20.16	
25		nub of one	nii pay 192.100.20.10	
24 23 SW HS2-5HE-avor	su-1	SUB URL	Show Sub UKL	
22 SW HS2-SHE-gyor	NJ-2	LED	 Power On 	
21			Error Blinking	
19 SW HS2-SRX-kann	-1		CIS CSS 0#	
18			in Identify Off	
17 SV H52-CX400		•	to identity Off	
15		_		
14 SW Cisco Nexus		A		
13 SW Cisco Catalyst		4		

View the entire datacenter floor status in a single 3D visualization.

The entire status of a datacenter is visible in a single converged view.

This view displays hardware failure status, the severity of received SNMP traps, intake air temperature, power consumption, as well as a visual image of the device.

It is very easy to locate faulty hardware in a datacenter and directly click on the device to investigate the problem.



Displayed failure status



Displayed inlet air temperature

Devices with outdated firmware that require updates are highlighted.

ISM periodically collects firmware information applied on managed devices. Collected information is displayed in a table, and old versions of firmware that are currently applied are highlighted in device information. Notify administrators using alarms.

1000												
and a	Q. Search	Update M	odo: All	v L Displa	ry only upd	alable rodes 13871	158			Filter	Actives ~	
sueire	Status 0	0 Node Name	0 IP Address	Model Name	Type	Firmware Name ()	Overent Version ()	Latest (Online) 📵 🖯	Latest (Office)	0 0 60	SM Offline C	
Script	=	201 SP-X 04	102.100.123.12	596031612								
		50 X 502	Rd1 2 192.108123.13	57 X116T2								
	Epitester	Ex Serve	147,1681,121,54	PRIMERGY R12220 MI	1116	Calored LAN_D		- 42				
		FX Serve	e1 192,100,123,14	POBARTON REDUCE MI	. FO	LAN POI Card 4	A	+ e				
	Typhatable	For form	192.108.128.34	PRINCEON BY2020 MT	8126	\$52550 V1 (RMC	7 73553 30	+ 7.83983.00	7.62783.58			
	Правле	FX Serve	192,160 123,14	PRIMEPOX DE2020 MT	RMC	010 0/0 11.14.03	948.5481150	- 98.0.3 8,81.17.0	÷		20	
		ногох	W2 192.108.28.14	PAILSFEER RE2530 M2								
		252 R14/261	192.108.18.2	V38 6740								
			190.16819.3	V38.6740								
		55 EF-X 84	101-3 102.108.123.12	89-X816T2								
		E Costo Chessian		CK000 MT								
			(0.26.312.10)	PUMPECY CC680.60								
	=	01 Scool	10.26112.182	PRIMERGY OX1640 MT								
		08 ¹ . COM	10.26.112.100	PRIMETOY COMMONT								
		-		MIN DO								

Relation between virtual machine physical machine - cache disk - capacity disk

It could not easily trace virtual machines accessing physical disks. ISM's "I/O Resource Impact Analysis" shows the structure of VMware vSAN on a GUI screen, broken down into virtual machine, physical server, cache disk, and capacity disk, allowing you to trace the relationship between virtual machines and physical disks.



Network connections are displayed on a map.

ISM displays the network connection of virtual resources, including virtual switches, as well as physical resources on a map.

Administrators can see the impact of physical and virtual server failures in a single view.



Feature 3 – Automation Device settings can be copied and applied to other devices

It is possible to configure device settings by creating a group of settings, referred to as a "profile", and applying the profile to the hardware. Then, this profile can be copied over to other devices which support the same settings.

For example: when you set up 10 servers with the same settings, you only need to create one profile. You can copy the profile to nine other servers. If you want to change something on a server, you can change the settings for each server. The parameters of an OS installation can also be saved to a profile, reducing the number of steps and time involved in deployment.



Events automatically trigger predefined actions.

You can configure ISM to send an e-mail automatically when it receives an SNMP trap or detects an event, such as a device failure. Sending SNMP traps to other stations, logging messages to Syslog servers, and the execution of Support task automation using APIs. a batch file or a script on an external server can be configured as well as sending an e-mail. This function makes troubleshooting easier and minimizes system downtime.

Automatically sets thresholds based on learning results and detects anomalies.

ISM collects data periodically and defines what is "usual" situation automatically not only by single parameter like standard threshold monitoring but by several parameters with special logic. Definitions are dynamically updated based on usage. ISM detects anomalies using a special algorithm beyond simple threshold monitoring. When an unusual trend is detected, a message appears on the GUI with a recommended solution.

Predicting resource fluctuations in VMware vSAN environments.

ISM simulates the resource fluctuation by adding server or disks. For example, adding server nodes to a vSAN cluster and see how fluctuation is going down.



ISM does provide an API for triggering actions such as getting device information or updating firmware. You can create an automated process by combining other applications that have API. For example, if you need to load new firmware on several servers during the night before starting a service, you can complete the task efficiently and with certainty by scripting using the ISM API. Similarly, the following steps are implemented in a script and automated. Collect status from VMware or OpenStack, and check if all virtual machines are stopped on the device

Check if newer firmware is available for the device using the ISM API Update the firmware using the ISM API

Other features Simplifiy ISM installation using virtual appliances

ISM is provided as a virtual machine appliance. You can start ISM simply by deploying the virtual machine image in your virtualization environment (VMware ESXi, Hyper-V, KVM for RHEL,Suse, Nutanix and Proxmox) with a few settings.

Devices are managed without the need for agent software

You are not required to install special programs like agent software on managed devices. ISM communicates via a management network port that is embedded in a device such as an iRMC, which is the BMC name of the FUJITSU Server PRIMERGY and PRIMEQUEST or with management protocol standards, SNMP or IPMI to communicate with 3rd party devices. Once you have registered the device in ISM, ISM starts to collect status data and information from the device automatically.

No pre-configuration is needed on the device side.

When you set up a new device in your datacenter an IP address usually needs to be configured, or an administrator must get the IP address that was assigned by DHCP by logging into BIOS. A combination of ISM and the latest PRIMERGY models (M4 generation and later) eliminates such pre-configuration processes. ISM detects PRIMERGY automatically when PRIMERGY is attached to the same network segment, after which you can configure all server settings from ISM view. You do not need to connect a display and keyboard to each server for management.

System Requirements Managed devices

Туре	Model
Server	FUJITSU Server PRIMERGY / PRIMEQUEST
Storage	FUJITSU Storage ETERNUS DX, AF, NR
Network device	FUJITSU Network SH, SR-X, IPCOM VX / CISCO Catalyst, Nexus / Brocade VDX, ICX
Other	PDU / UPS / Rack / CDU

Details for supported models and functions are available on the support matrix.

Management nodes

ISM is provided as virtual machine appliance (VA). These are the minimum requirements to be assigned to a virtual machine appliance.

Item	Description
CPU	2 cores
Memory	16GB
Disk	70GB
Network	1Gbps
Hypervisor	 MS Hyper-V VMware ESXi KVM (RHEL,SUSE;Nutanix,Proxmox,others)

Consoles

These are the requirements for a console to access the ISM GUI.

Item	Description
Web	Microsoft PC, server, tablet:
browser	- Microsoft Internet Explorer
	- Microsoft Edge
	- Mozilla Firefox
	- Google Chrome
	Android tablet: Google Chrome
	iPad: Safari

Licences

ISM	Control:	Maintain:	Dynamize:	Deploy:	Integrate:		
Essentials:	Node Management* Health status Event Management Capacity / Threshold Management Inventory management	Update Management Logging and auditing Performance Management	Dashboard + Widgets Auto discovery				
Advanced: Same as Essentials +adv. features	Sustainability Monitor Power consumption Central Access Server (CAS)	Profile Management Firmware baseline Archive management	Enhanced Dashboard Widgets Virtual-IO management Network topology Management	Automate device configuration Mass OS installation	In Enterprise Management In vendor specific management 3 rd Party platforms (monitoring only)		
Licenses:	Free ISM Essentials include 1000 node licenses (license key are part of the virtual appliance)						
	 Advanced node Licenses offered with1, 5, 10,20,100 bundles Multi node licenses can be assigned only to a single ISM instance. 						
	 A license is required for each managed node of ISM Advanced Term based licenses with 1, 3 and 5 years offering 						
Support:	 5x9h and 7x 24 h for Essentials and Advanced SNS offering available for a period of 1, 3 and 5 years 						

*ISM Supports all devices as Server, Storage, Switches,

Facility listed on the Support Matrix

Copyright

- Fsas Technologies and Fsas Technologies logo are trademarks of Fsas Technologies Inc.
 Registered in many jurisdictions worldwide.
- Microsoft, Windows, Windows Vista, Windows Server, Hyper-V, Active Directory, or other names of Microsoft products and product names are registered trademarks of the Microsoft Corporation in the USA and in other countries.
- Linux is a registered trademark of Linus Torvalds in the USA and in other countries.
- Red Hat, RPM, and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat Inc. in the USA and other countries.
- VMware, VMware logos, VMware ESXi, VMware SMP, and VMotion are registered trademarks

of VMware, Inc. in the USA and in other countries.

 Other company names and product names are trademarks or registered trademarks of their respective companies. All other products are works of their respective companies.

Disclaimer

Technical data is subject to modification and delivery is subject to availability. Any liability that data and illustrations are complete, actual, or correct is excluded. Designations may be trademarks and/or copyrights of their respective manufacturers, and the use of such by third parties for their own purposes may infringe the rights of such owners.

Contact

Fsas Technologies Website: <u>https://www.fsastech.com/en-eu/</u> © Fsas Technologies 2025. All rights reserved. Fsas Technologies and Fsas Technologies logo are trademarks of Fsas Technologies Inc. registered in many jurisdictions worldwide. Other product, service and company names mentioned herein may be trademarks of Fsas Technologies or other companies. This document is current as of the initial date of publication and subject to be changed by Fsas Technologies without notice. This material is provided for information purposes only and Fsas Technologies assumes no liability related to its use.