Infrastructure Manager: Overview

White Paper

FUJITSU

An overview of software that helps manage and operate whole datacenter environment that includes infrastructure platforms such as servers, storage, network and facility devices, from a single interface.

Contents

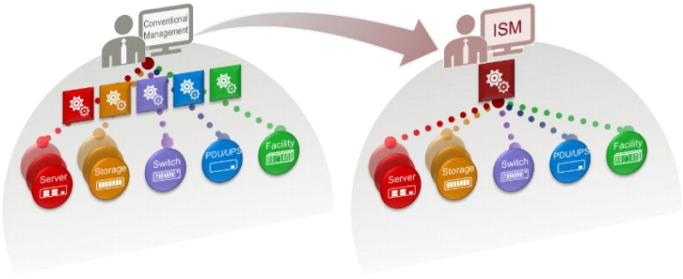
Abstract

Path to achieving software-defined infrastructure

In today's digital world, where more and more devices are connected via the internet, data is king and organizations that are able to differentiate and innovate using this information lead the game. In order 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.

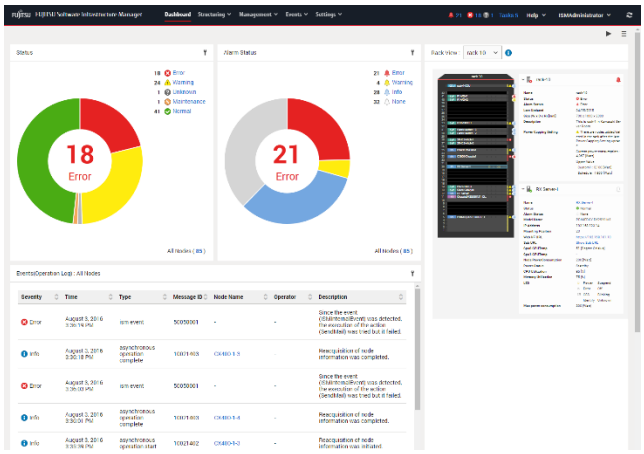
Infrastructure Manager (also referred to as "ISM" below) has a simple and intuitive interface that offers a complete view of datacenter status. One of the key functions of ISM is the multiple FW upgrading and OS deployment which significantly reduces the time and cost required for the activities. Furthermore, 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

Servers, storage, and network switches are managed using a single 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 time consuming ISM indicates and manages servers, storage, network switches, and the entire system in a single GUI.



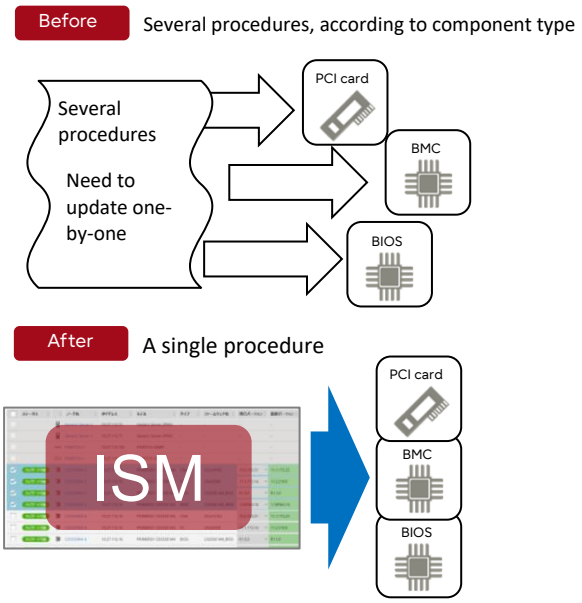
A variety of firmware updates can be carried out in a single process

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 have to 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

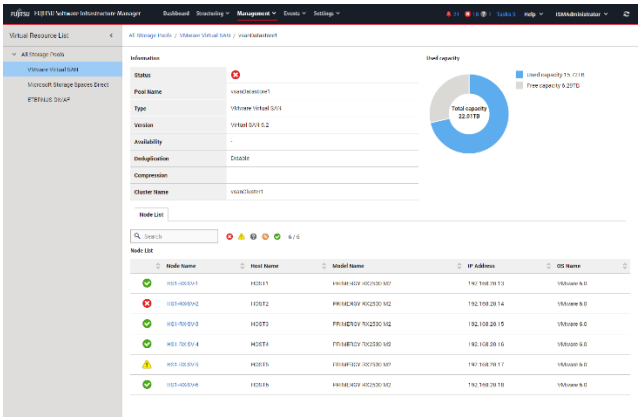
provides single procedure to update all types of firmware. The administrator does not need to search for a device or component dedicated to the update procedure and can update multiple types of devices and components in a single process.



Virtual resources provided by vCenter and other virtual machine management software are supported

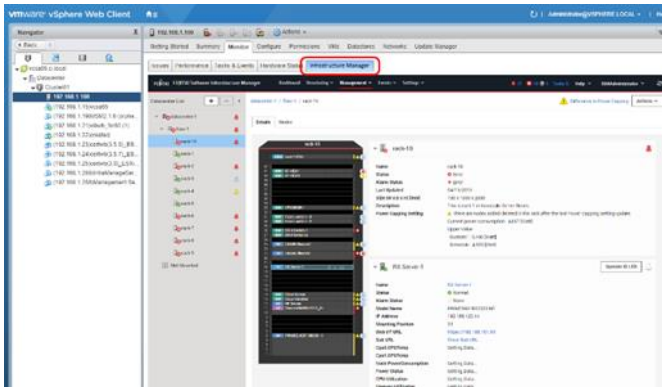
ISM can communicate with VMware vCenter Server, OpenStack, and similar kinds of virtual resource management software. It collects and displays information and status of physical and virtual nodes.

The status and resources of VMware vSAN and Microsoft Storage Spaces Direct, which are in the spotlight these days as a base technology for HCI (Hyper Converged Infrastructure), are also displayed along with physical device information in the ISM dashboard.



Enabling physical and virtual devices to be seen and controlled

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.



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.

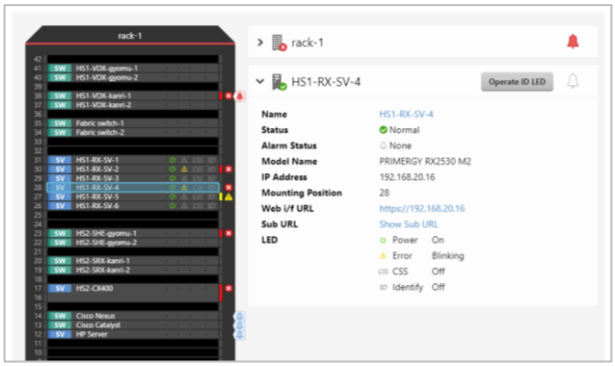
ISM can be integrated in an existing management stack using an API.

Feature 2 – Visualization

Visualization of 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.



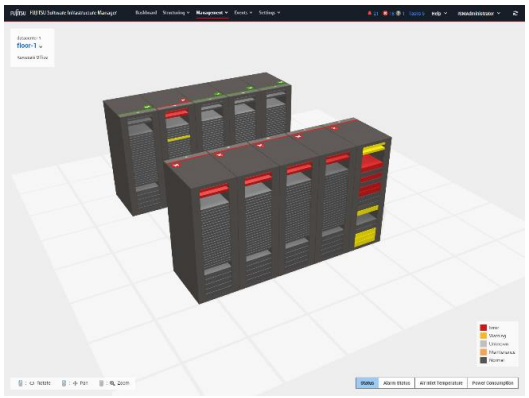
Entire datacenter floor status seen in a single 3D view

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

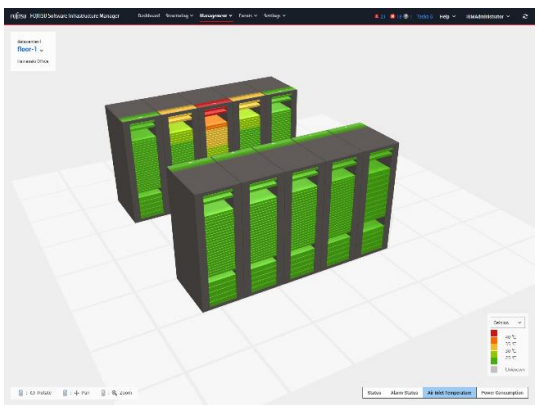
This view displays hardware failure status, the severity of received SNMP traps, intake air temperature, power consumption, as well as a visual image of the device.

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

Displayed failure status

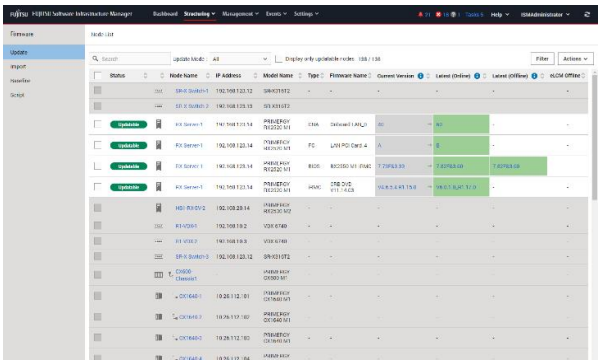


Displayed inlet air temperature



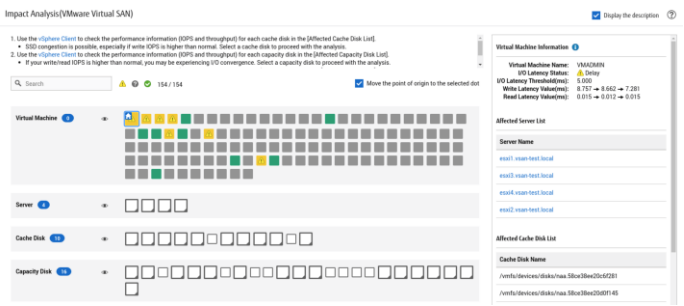
Devices that have old firmware and require updating are indicated

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.



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

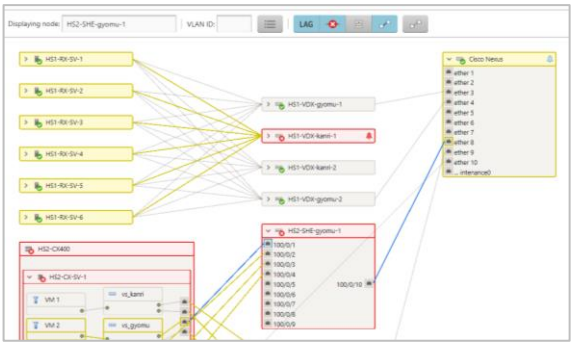
It could not easily trace virtual machines accessing physical disks. ISM's "I/O Resource Impact Analysis" shows the structure of VMware vSAN on a GUI screen, broken down into virtual machine, physical server, cache disk, and capacity disk, allowing you to trace the relationship between virtual machines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



Network connection is displayed on 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.

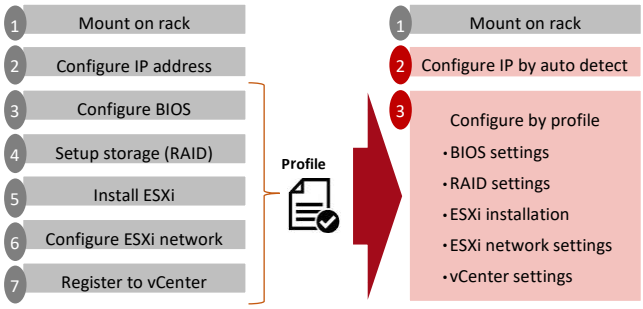


Feature 3 – Automation

Device settings can be copied and deployed 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.



Defined actions are called automatically by events

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 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.

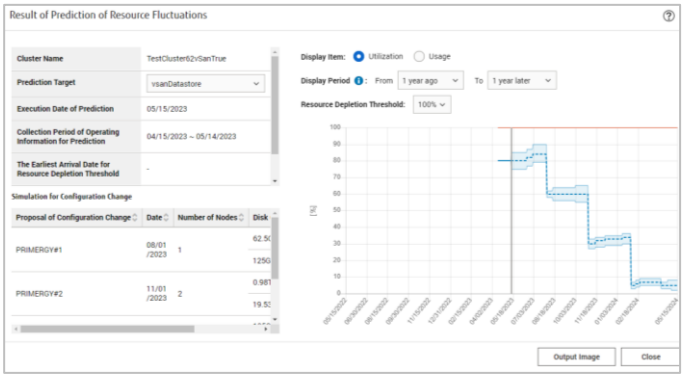
Automatically sets thresholds based on the learning results, and detect anomaly

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. Furthermore, the definitions are updated dynamically by usage. Based on that ISM detects "unusual" by a special algorithm which is not just threshold monitoring.

When unusual trend is detected, a message appears on the GUI, and also recommended solution is displayed.

Prediction of 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.



Using API to support task automation

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.

1. Collect status from VMware or OpenStack, and check if all virtual machines are stopped on the device

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

Other features

Program is provided as virtual appliance to make installation easier

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, RHEL KVM) with a few settings.

Devices are managed without 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. Once you have registered the device in ISM, ISM starts to collect status data and information from the device automatically.

No pre-configuration is required 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 has to 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

Type	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
Hyper-visor	- Hyper-V - VMware ESXi - KVM

Consoles

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

Item	Description
Device	PC, server, Windows10 tablet, Android tablet, iPad
Web browser	PC, server, Windows10 tablet: - Microsoft Internet Explorer - Microsoft Edge - Mozilla Firefox - Google Chrome Android tablet: Google Chrome iPad: Safari

Licenses

Required licenses

ISM requires the following licenses for use.

- Server licenses
  1x license is required for the ISM VM appliance

- Node licenses
  A license is required for each node managed by ISM.

Product lineup

- Server license
- node license
- 5-node license
- 10-node license
- 20-node license
- 100-node license

Note: a multinode license can be assigned only to a single ISM instance (VA).

Copyright

Disclaimer

Contact

Fujitsu Technology Solutions GmbH
Mies-van-der-Rohe-Strasse 8
D-80807 Munich

Website: www.fujitsu.com