User Guide - English

FUJITSU

Fujitsu Software ServerView Suite

# Fujitsu Software ServerView Plug-in for VMware vCenter V5.0.0

Edition August 2024

## Comments... Suggestions... Corrections...

The User Documentation Department would like to know your opinion of this manual. Your feedback helps us optimize our documentation to suit your individual needs.

Feel free to send us your comments by e-mail to
manuals@fujitsu.com.

## Documentation creation according to ISO 9001 and ISO 27001

To ensure high quality and information security standards while creating documentation, the quality management system and information security management system of Etteplan are certified in compliance with ISO 9001 and ISO 27001.

Etteplan Germany GmbH | www.etteplan.com

## Copyright and trademarks



Delivery subject to availability; right of technical modifications reserved.

All hardware and software names used are trademarks of their respective manufacturers.

# Contents

# 1 Overview

## 1.1 Virtualization solutions from Fujitsu - ServerView Suite and vSphere

**Virtualization solutions from Fujitsu**

Fujitsu is committed to total virtualization - from servers to storage to networks - and to virtualization software and operation management tools. The partnership between VMware and Fujitsu brings you continuity of technology assets, more efficient resource use, and steps toward the elimination of IT complexity.

**VMware and Fujitsu ServerView integrated virtualization support**

ServerView supports the CIM management standard, making it possible to monitor and manage VMware vSphere-based environments more reliably and securely. Administrators can view all physical and virtual machines through a single interface.

In addition, Fujitsu Software ServerView Integration Solutions for VMware vCenter also support the Redfish DMTF standard. Redfish provides another possible interface for particularly secure monitoring of VMware vSphere-based environments.

**vSphere Client**

VMware vSphere provides several interfaces for data center managment and virtual machine access: vSphere Client, VMware Host Client, and vSphere Command-Line Interface.

The vSphere Client is the primary method for system administrators and end users to interact with the virtual data center environment created by VMware vSphere.

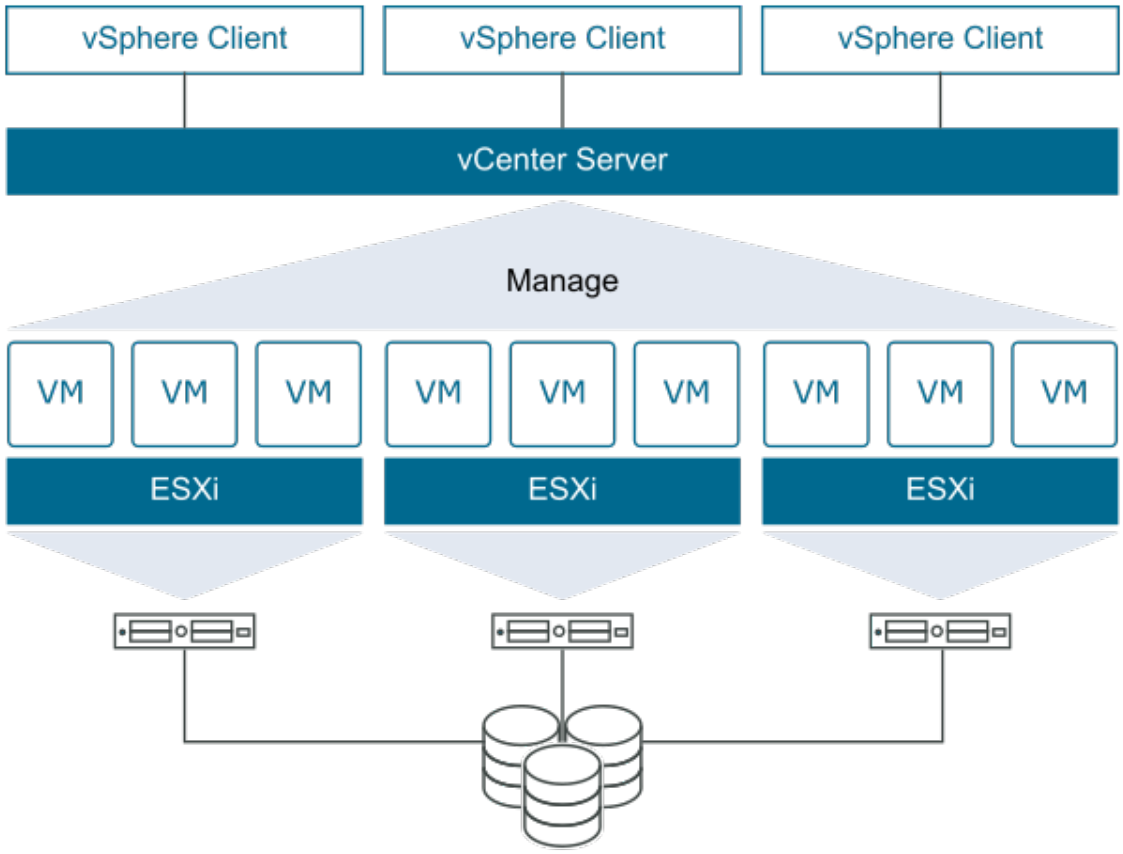


Figure 1: VMware vSphere data center physical topology - (Source: http://www.vmware.com/support/pubs/)

The vSphere Client is a cross-platform application that can connect only to vCenter Server. It has a full range of administration functionality and an extensible plug-in-based architecture.

All administrative functions are available through the vSphere Client.

You can use the vSphere Client to access vCenter Server through a Web browser. vSphere Client uses the VMware API to mediate the communication between the browser and the vCenter Server.

It is possible to extend vSphere in different ways to create a solution for a unique IT infrastructure. vSphere Client can be extended by creating plug-in modules. A complete plug-in solution adds new capabilities to the vSphere Client graphical user interface. In this way third-party companies can integrate their GUIs and show information as desired.

### ServerView Suite and vSphere

The ServerView Suite has implemented the ServerView ESXi CIM Provider, which is part of the VMware ESXi release. In addition, Fujitsu has implemented the Fujitsu Software ServerView Plug-in for VMware vCenter (SV Plug-in), which shows the values of a host system provided by the ServerView ESXi CIM Provider. For ESXi-based hosts the SV Plug-in also supports

monitoring via the Redfish interface. It is also possible to monitor most of the storage values via IPMI, although not all the values are available in this way.

The Fujitsu Software ServerView Plug-in for VMware vCenter (SV Plug-in) offers you a home page with a **Getting Started** view and a **Summary** view, which gives an overview of the information items provided by the SV Plug-in.

Via the **Monitor** tabs for ESXi hosts, vCenters, and clusters, the SV Plug-in provides you with detailed information about Fujitsu PRIMERGY servers. This information includes properties of the system, fans, temperature sensors, power supplies, system processors, memory modules and the RAID subsystem.

The SV Plug-in also includes the SV vCenter Service, which routes Fujitsu PRIMERGY-specific events to the vCenter event management to be monitored in the vSphere Client.

## 1.2 Integration approaches

The Fujitsu Software ServerView Plug-in for VMware vCenter (SV Plug-in) integrates Fujitsu PRIMERGY-specific information into the vSphere Client interface. There are two approaches to do this:

Data integration

in the event and alarm management of the vSphere Client itself.

Full sites integrated

in the vSphere Client offer the Fujitsu PRIMERGY-specific data of ESXi hosts, hosts of vCenters or clusters.

## 1.3 Monitoring and managing possibilities

### 1.3.1 Collecting monitoring data - CIM, Redfish, IPMI

The SV Plug-in uses the following interfaces for monitoring an ESXi-based host:

**CIM** (Common Information Model)
When available, default protocol for server monitoring is CIM. The monitoring data is provided by the SV ESXi CIM Provider.

**Redfish** (Redfish Scalable Platforms Management API)
You can toggle to Redfish. In this case the monitoring data is provided by the iRMC.

**IPMI** (Intelligent Platform Management Interface)
It is also possible to monitor most of the monitoring data via IPMI, although not all the values are available in this way. Via IPMI the iRMC also provides the monitoring data.

## 1.3.2 Monitoring and managing features

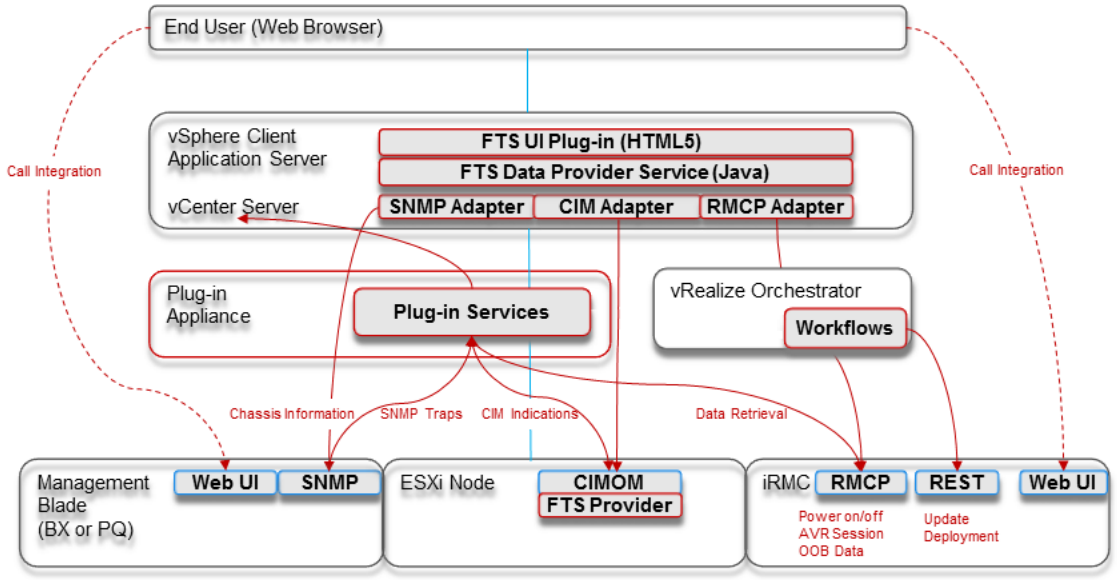


Figure 2: Architecture of the Fujitsu Software ServerView Plug-in solution for VMware vCenter

### Detailed information on a selected host and Fujitsu PRIMERGY Actions

The SV Plug-in offers various options for monitoring ESXi hosts: Status icons provide quick information. Detailed views provide more information on a selected host.

And a number of Fujitsu PRIMERGY action items support calling a monitoring tool or making settings on the host.

For ESXi 7.x and older: In regular operation, the SV Plug-in generally shows the values of a host system provided by the ServerView ESXi CIM Provider.

For ESXi 7.x and older: You can also use the values of a host system provided by the Redfish interface of its iRMC for monitoring, provided the iRMC has a suitable firmware version. It is also possible to monitor most of the storage values via IPMI. Redfish and IPMI are only available if the iRMC credentials are configured (see "Configure iRMC credentials: 'IPMI configuration'" on page 59). If all protocols are available, you can toggle between CIM, Redfish and IPMI communication interfaces. Be aware that not all the values are available via IPMI.

For ESXi as of 8.0: You can ony use Redfish and IPMI.

### Storage view

The **Storage** view provides an overview of the RAID controllers found on the host and details of their logical drives and physical disks.

### Driver Monitor view

Via the **Driver Monitor** view you can monitor and manage events relating to the components of a monitored host, as listed in the OS event log on the monitored host.

### System Event Log view

Events of PRIMERGY systems will be forwarded to the vSphere Event Manager. You can also view the System Event Log, including specialized cause and resolution information.

### Monitoring vCenter or cluster host servers

The SV Plug-in offers lists of the hosts assigned to a vCenter or cluster. It offers less information on the individual host via this access point than via the inventory tree item **Hosts**, but all Fujitsu PRIMERGY Actions are available.

### SV vCenter Service - Integration in event and alarm management of vCenter

The SV Plug-in includes the SV vCenter Service, which routes Fujitsu PRIMERGY-specific events to the vCenter event management to be monitored in the vSphere Client. If a Fujitsu PRIMERGY host detects a problem, it will create a CIM indication and send it to subscribed destinations. An alarm is also created and can be configured for further actions. If SV vCenter Service is subscribed to the host, it will receive the CIM indication. It creates a vCenter event and forwards it to vCenter Server. So the Fujitsu PRIMERGY-specific event is shown in the regular **Monitor-Events** sub-tab of the vSphere Client.

### Remote Management possibilities: Remote console (AVR), iRMC Web interface, and system identification LED

The SV Plug-in offers some iRMC-based operations - called **FUJITSU PRIMERGY Actions** - depending on the capabilities of the selected host. They make it very easy for the administrator to connect directly to an ESXi-based host and its iRMC.

The SV Plug-in enables you to start a session with the onboard management controller (iRMC) of a managed PRIMERGY system via its web interface or to contact a remote console. There are Fujitsu PRIMERGY vCenter role definitions designed for using single sign-on when starting the iRMC Web interface and remote console.

To simplify service tasks, the SV Plug-in allows you to turn the system identification LED of the PRIMERGY server on/off.

### Proactive HA - a vCenter cluster feature

vSphere High Availability (HA) now also detects the hardware conditions of the ESXi host and allows you to evacuate the virtual machines before the hardware issues cause an outage to virtual machines with the help of Proactive HA.

Proactive HA works in conjunction with the SV Plug-in to receive the health status of the hardware components such as memory, fans and power supplies. The support for the new

feature is implemented in SV vCenter Service via the FujitsuHealthProvider, which communicates with vCenter and sends health status updates.

## 1.4 What's new

This edition of the manual applies to Fujitsu Software ServerView Plug-in for VMware vCenter V5.0.0 and replaces the online manual "Fujitsu Software ServerView Plug-in for VMware vCenter V4.3.5", February 2023 edition.

The manual features the following changes and enhancements:

- The remote console (AVR) is supported again with the new vSphere releases. The corresponding sections and notes have therefore been added again, see among others "Remote console (AVR)" on page 115.
- VMware dropped support for CIM starting with vSphere 8.0. Therefore, ServerView ESXi CIM Provider are no longer supported. To gather the values of a host system as of version 8.0, iRMC must be configured to get these values from Redfish or IPMI. The description has been adapted accordingly.
- Oracle Linux, the successor to CentOS, is now in use. The description has been adapted accordingly, see among others "Updating Oracle Linux" on page 34.
- An update of the components of the ServerView VMware vCenter Plug-in Appliance to version 5.0.0 is only possible from ServerView VMware vCenter Plug-in Appliance version 4.3.5, see "Updating" on page 33.
- Setting iRMC credentials for multiple servers is only possible for servers with CIM. Therefore, hosts with ESXi as of 8.0 cannot be used for setting iRMC credentials for multiple servers, see "Setting iRMC credentials for multiple servers" on page 62.
- The **Getting started** view on the home page of the SV Plug-in changed. All necessary links are now in left panel, see "Getting Started view" on page 78.
- CX hosts are no longer supported as of the new vSphere releases. The relevant sections have been removed.
- The **ServerView Update Management** view is no longer supported. The relevant sections have been removed.

## 1.5 Target groups and purpose of this manual

This manual is intended for system administrators, network administrators and service technicians who already have a basic knowledge of hardware and software.

The manual explains how you can monitor a VMware vSphere-based server with ServerView and vSphere, and describes how to deploy the Fujitsu Software ServerView Plug-in for VMware vCenter.

## 1.6 Documentation for the ServerView Suite

The documentation can be downloaded free of charge from the Internet. You will find the online documentation in the download section of the Fujitsu Technical Support pages.

To download the documentation, proceed as follows:

1. Open the web page https://support.ts.fujitsu.com/IndexDownload.asp?PaOpenTab=manuals.
2. Click **Browse For Product**. A list of product lines opens.
3. Select **Software** - **ServerView** - **Operation**. A list of products opens.
4. Select the appropriate product from the product list.

   The corresponding page with the **Documents** tab opens.

Only for English and German Fujitsu Technical Support pages: If no tab is displayed, select **OS Independent (BIOS, Firmware, etc.)** under **Selected operating system** and then click **Documents** tab.

## 1.7 ServerView Suite link collection

Via the ServerView Suite link collection, Fujitsu provides you with numerous downloads and further information on the ServerView Suite and PRIMERGY servers.

Under **ServerView Suite**, links are offered on the following topics:

- Forum
- Service Desk
- Manuals
- Product information
- Security information
- Software downloads
- Training

**Software downloads** includes the following downloads:

- Current software statuses for the ServerView Suite as well as additional Readme files.
- Information files and update sets for system software components (BIOS, firmware, drivers, ServerView Agents, and ServerView Update Agent) for updating the PRIMERGY servers via ServerView Update Manager or for locally updating individual servers via ServerView Update Manager Express.
- The current versions of all documentation on the ServerView Suite.

You can retrieve the downloads free of charge.

Under **PRIMERGY Server**, links are offered on the following topics:

- Service Desk
- Manuals
- Product information
- Spare parts catalogue

**Access to the ServerView Suite link collection**

You can access the link collection of the ServerView Suite in one of two ways:

- Via the following link:

  http://support.ts.fujitsu.com/prim_supportcd/SVSSoftware/start.html

- Via the ServerView Suite DVD 2:

  1. In the start window of the ServerView Suite DVD 2, select the option **ServerView Software Products**.
  2. On the menu bar select **Links**.

This opens the start page of the ServerView Suite link collection.

## 1.8 Abbreviations and notation of product variants

**SV Plug-in**

In the following, **SV Plug-in** is short for **FUJITSU Software ServerView Plug-in for VMware vCenter**.

**vSphere Client**

The vSphere Client, introduced in vSphere 6.5, is an HTML5-based client and is included with vCenter Server. As of vSphere 7.0, the vSphere Client has been deprecated. The vSphere Client is the primary interface for connecting to and managing vCenter Server

instances.

Task instructions in this guide are based on the vSphere Client.

**iRMC S4/S5**

Most of the task instructions in this guide refer equally to iRMC S4 and iRMC S5. Therefore you will usually find the notation 'iRMCS S4/S5'. If a specification refers to only one of the two, you will find the exact notation 'iRMC S4' or 'iRMC S5'.

## 1.9 Typographic conventions

The following typographic conventions are used:

| Convention | Explanation |
|---|---|
|  | Various types of risk, namely health risks, risk of data loss and risk of damage to devices. |
|  | Additional relevant information and tips. |
| **bold** | References to names of interface elements. |
| `monospace` | System output and system elements, e.g., file names and paths inside text blocks. |
| **`monospace semibold`** | Commands, system output, syntax and statements that are to be entered using the keyboard outside text blocks. |
| blue continuous text | A link to a related topic. |
| purple continuous text | A link to a location you have already visited. |
| <abc> | Variables which must be replaced with real values. |
| [abc] | Options that can be specified (syntax). |
| [Key] | Key on your keyboard. If you need to enter text in uppercase, the Shift key is specified, e.g.,[Shift] + [A] for an A. If you need to press two keys at the same time, this is indicated by a plus sign between the two key symbols. |
| Quotation marks | For names of chapters and manuals. |

Table 1: Typographic conventions

### Screenshots

Some of the screenshots are system-dependent, so some of the details shown may differ from your system. There may also be system-specific differences in menu options and commands.

## 1.10 Overview of requirements and ports

For the interaction between SV Plug-in, vCenter appliance, vSphere Client, iRMC and update/ deployment services, requirements are listed in the respective chapters.

This chapter lists all this information to give an overview.

### 1.10.1 Port information

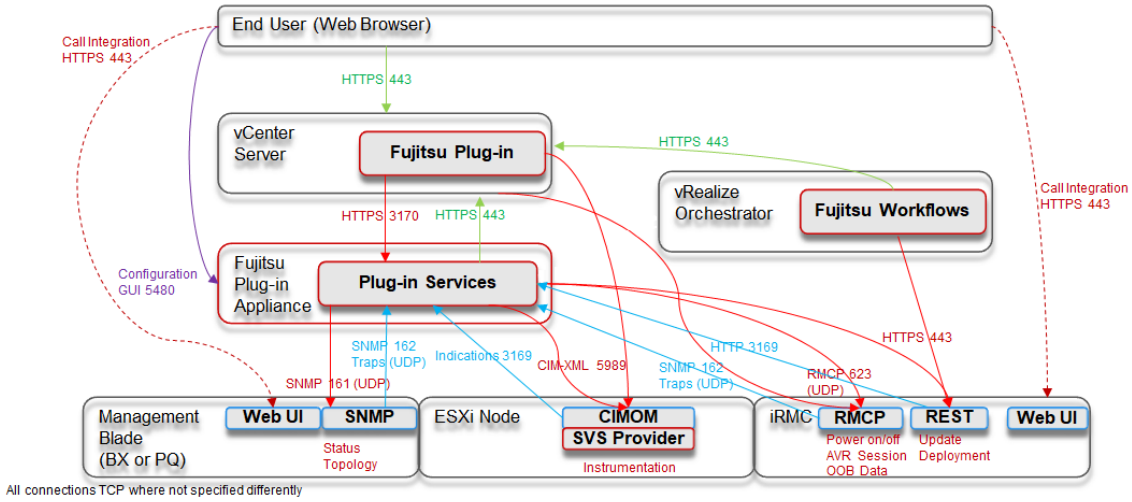


Figure 3: SV Plug-in: Ports and connections

**Local ports:**

| | |
|---|---|
| 161, 162 | SNMP |
| 443 | HTTPS (also Redfish) |
| 623 | IPMI |
| 3169 | indication subscription |
| 3170 | HTTPS port |
| 5480 | appliance administration |
| 5989 | CIM |

## 1.10.2 Requirements for installing

### 1.10.2.1 Requirements for monitored hosts

- The ESXi version must be ESXi 7.0 ≥ GA or ESXi 8.0 ≥ GA.
- SV ESXi RAID Core Provider ≥ 8.30.08 must be installed.
- Update Manager Express (UME) > 12.17.09.03 must be in the repository.

**Additional requirements for update and deployment (hosts)**

- The host system must have an iRMC:

  iRMC S4, firmware > 9.08f

  or

  iRMC S5, firmware > 1.25P
- The iRMC must offer the following:
  - **iRMC User Role**: **Administrator**
  - eIM ≥ V13.19.01 (stored on the iRMC S5 SD card)

**Additional requirements for the use of Redfish (hosts)**

- The iRMC must offer the following:
  - Redfish must be enabled as a service and the user needs the appropriate Redfish role.

### 1.10.2.2 Requirements for the vCenter application server

**Linux**

- vCenter/vSphere version must be at least V8.0.

### 1.10.2.3 Requirements for the web browser

- The web browser used must be

  Microsoft Edge ≥ V44

  or

  Mozilla Firefox ≥ V60

  or

  Google Chrome ≥ V75

### 1.10.3 Requirements for logging in to vCenter Server using the vSphere Client

**vCenter Server and vSphere Client**

In vSphere V6.7 U1 and later, the vSphere Client is installed as part of the vCenter Server appliance deployment. This way, the vSphere Client always points to the same vCenter single sign-on instance.

### 1.10.4 Requirements for single sign-on on iRMC

To perform the iRMC functions with single sign-on, the following requirements must be met:

- The iRMC credentials must be configured with an iRMC user account that has the **Administrator** / **OEM** LAN channel privilege (see "Configure iRMC credentials: 'IPMI configuration'" on page 59).
- The vCenter user must have the privileges defined in the FUJITSU PRIMERGY role definitions.

### 1.10.5 Requirements for integration in the event management of the vSphere Client

These requirements are only valid for ESXi based hosts with CIM.

vSphere Client

- CIM and SNMP

  ESXi-based host

  ServerView ESXi CIM Provider must be installed on the ESXi-based host whose events are to be displayed in the vSphere Client interface.

- SV vCenter Service must be connected to the vCenter to which the host is assigned (see "SV vCenter Service configuration" on page 56).
- SV vCenter Service must be subscribed to this host (see "Monitoring vCenter or cluster host servers" on page 100). You can find an overview of the hosts subscribed to an SV vCenter Service in the **SV vCenter Configuration Overview** (see "SV vCenter Service Configuration Overview" on page 108).

# 2 Installing the Appliance

Fujitsu has implemented the ServerView VMware vCenter Plug-in Appliance for installing the SV Plug-in. The appliance offers a pre-installed virtual machine which is based on Oracle Linux 8.6 and includes the SV Plug-in installation. Using the appliance you can deploy this virtual machine on a vSphere host or a vSphere cluster.

When user updates the vCenter from version 7.0 to 8.0, the older version of the SV Plug-in must first be uninstalled and deregistered. Only afterwards can the new version of the SV Plug-in be installed and registered.

**Localization:**

The language supported for ServerView VMware vCenter Plug-in Appliance is English.

The languages supported for using the SV Plug-in are English, German and Japanese.

## 2.1 Provisioning

You can obtain the ZIP download file of the SV Plug-in in the following ways:

- Download from the Fujitsu website support.ts.fujitsu.com:

  Choose: **Downloads** - **Browse for Product** - **Software** - **ServerView** - **Integration** - **VMware Integration Solutions** - **Applications**.

- Download from the ServerView Suite DVD (web: http://download.ts.fujitsu.com/prim_supportcd/. The ServerView Suite DVD version displays a link to this website.):

  Choose: **Software Products** - **ServerView** - **Integrations Solutions** - **ServerView Integration in VMware vCenter**.

  

  Due to the ServerView Suite DVD capacity problem, the ZIP download file of the SV Plug-in as a whole cannot be offered via the ServerView Suite DVD. There is a link to the Fujitsu website, therefore an internet connection is necessary.

The ZIP download file of the SV Plug-in contains the following directories:

- **appliance**
  - Installation package:

    **ServerView_VMware_vCenter_Plug-in_Appliance_<version>_OVF10.ova**
  - Upgrade ISO-file
- **common**
- **documentation**
- **legal**

# 2.2 Requirements for installing

## 2.2.1 Requirements for monitored hosts

- The ESXi version must be ESXi 7.0 ≥ GA or ESXi 8.0 ≥ GA.
- SV ESXi RAID Core Provider ≥ 8.30.08 must be installed.
- Update Manager Express (UME) > 12.17.09.03 must be in the repository.

### 2.2.1.1 Additional requirements for update and deployment (hosts)

- The host system must have an iRMC:

  iRMC S4, firmware > 9.08f

  or

  iRMC S5, firmware > 1.25P
- The iRMC must offer the following:
  - **iRMC User Role**: **Administrator**
  - eIM ≥ V13.19.01 (stored on the iRMC S5 SD card)

### 2.2.1.2 Additional requirements for the use of Redfish (hosts)

- The iRMC must offer the following:
  - Redfish must be enabled as a service and the user needs the appropriate Redfish role.

### 2.2.2 Requirements for the vCenter application server

- vCenter/vSphere version must be at least V8.0.

### 2.2.3 Requirements for the web browser

- The web browser used must be

  Microsoft Edge ≥ V44

  or

  Mozilla Firefox ≥ V60

  or

  Google Chrome ≥ V75

## 2.3 Deploying, configuring and registering the ServerView VMware vCenter Plug-in Appliance

The ServerView VMware vCenter Plug-in Appliance is deployed on a vSphere host or a vSphere cluster via the vSphere Client.

### 2.3.1 Deploying the ServerView VMware vCenter Plug-in Appliance

After downloading the OVF package (see "Provisioning" on page 20), you can deploy it using the vSphere Client.

A second way to deploy the OVF package of the the ServerView VMware vCenter Plug-in Appliance is the VMware OVF tool. Basic information on how to use the VMware OVF tool to deploy the OVF package of the ServerView VMware vCenter Plug-in Appliance can be found in "Deploying the ServerView VMware vCenter Plug-in Appliance using the VMware OVF tool" on page 27.

Before you begin: It is essential to ensure that the ServerView VMware vCenter Plug-in Appliance has a Fully Qualified Domain Name (FQDN) and that it has also been entered in the DNS server.

**Procedure:**

1. Log in into vSphere Client (see "Log in to vCenter Server using the vSphere Client" on page 39).

2. In the vSphere Client inventory right-click any vSphere host or vSphere cluster on which the ServerView VMware vCenter Plug-in Appliance is to be deployed, and select **Deploy OVF Template**.
3. On the **Select an OVF template** page, select the OVA template of the ServerView VMware vCenter Plug-in Appliance.
4. Click **Next**.
5. On the **Select a name and folder** page, enter a unique name for the ServerView VMware vCenter Plug-in Applicance and select a deployment location.
6. Click **Next**.
7. On the **Select a computer resource** page, select a resource where to run the deployed template of the ServerView VMware vCenter Plug-in Applicance.
8. Click **Next**.
9. On the **Review details** page, verify the details of the template of ServerView VMware vCenter Plug-in Appliance.
10. Click **Next**.
11. On the **Select storage** page, define where and how to store the files for the deployed template of the ServerView VMware vCenter Plug-in Appliance.

    The **Select storage** window opens.

    

    The appliance is configured to use a maximum of 100GB storage. It is recommended to use thin provisioning so that the storage will grow with usage. Its actual size depends on the repository used for update handling.

    **Select virtual disk format:**

    In the **Select virtual disk format:** field, select **Thin provision**.
12. On the **Select networks** page, select a source network and map it to a destination network.

    **Destination Network**

    In the **Destination Network** field, select the network in which the vCenter is located.
13. Click **Next**.
14. On the **Customize template** page, customize the deployment properties of the template of the ServerView VMware vCenter Plug-in Appliance.

**Hostname**

Name of the host.

The host name must be an FQDN.

Format: <name of the appliance>.<domain name>.<suffix>

It is recommended to use fixed IP address and network parameters instead of DHCP. Check the entry in the DNS server.

**root Password**

Password for the user **root**.

For automatic deployment you can set the root password with this OVF environment variable if desired.

Leave empty to interactively set the root password during the first boot of the ServerView VMware vCenter Plug-in Appliance. See "Open a remote console." on page 26.

If you leave the following fields empty, the virtual machine of the ServerView VMware vCenter Plug-in Appliance will use DHCP to get its network configuration. This is not recommended!

**Default Gateway**

The default gateway address for the virtual machine of the ServerView VMware vCenter Plug-in Appliance.

Leave empty if you want to use DHCP.

**DNS**

The domain name servers for the virtual machine of the ServerView VMware vCenter Plug-in Appliance.

Leave empty if you want to use DHCP.

**Network 1 IP Address**

The IP address for the interface of the ServerView VMware vCenter Plug-in Appliance.

Leave empty if you want to use DHCP.

**Network 1 Netmask**

The netmask or prefix for the interface of the ServerView VMware vCenter Plug-in Appliance.

Leave empty if you want to use DHCP.

15. Click **Next**.
16. On the **Ready to complete** page, review the page.

17. On the **Ready to complete** page, click **Finish**.

    Depending on your network speed, the deployment can take several minutes. You can view the progress in the progress dialog box.

18. When the deployment is complete, select the appliance in the inventory of the vSphere Client, right-click, and select **Power on**.

    A green right arrow is displayed next to the icon of the appliance virtual machine in the inventory list.

    

    If **vSphere Client (HTML5) restriction:** Using the vSphere Client (HTML5), the user interface seems to freeze during powering-on and this question is not displayed.

    1. Switch to the **Monitor** tab.
    2. In the **Monitor** tab, select the item **Issues and Alarms** - **All Issues**.

       The list of **All Issues** is displayed.
    3. In the list of **All Issues**, the following question is displayed:

       ```
       Cannot connect the virtual device ide0:0 because no
       corresponding device is available on the host. Do you
       want to try to connect this virtual device every time
       you power on the virtual machine?
       ```
    4. Click the **Answer Question ...** button on the left above the list.
    5. Answer the question with **No**.

    The virtual machine of the appliance is initialized.

19. If you have not entered the root password yet, switch to the console and enter the password for root:
    1. Open a remote console.
    2. Start the ServerView VMware vCenter Plug-in Appliance.

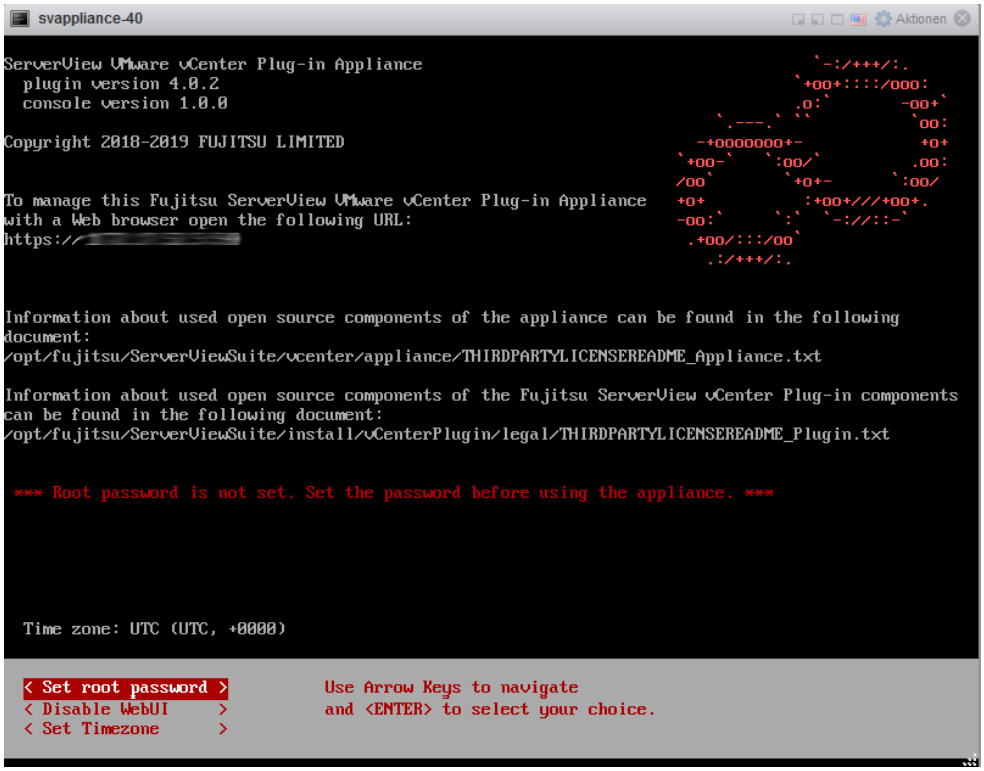


Figure 4: ServerView VMware vCenter Plug-in Appliance - setting the root password

    3. Set the root password.
20. When the deployment is complete, select the appliance in the inventory of the vSphere Client, right-click, and select **Edit Settings ...**.

    The **<appliance name> - Edit Settings** window opens.
21. Select the **VM Options** tab - **VMware Tools** - **Time (*)**.

    Synchronize the ServerView VMware vCenter Plug-in Appliance time with the vSphere host/cluster, and set the correct time zone for the ServerView VMware vCenter Plug-in Appliance using the administration UI of the apppliance **https://<fqn>:5480**.
22. In the **VM Options** tab, click **OK**.

    The **<appliance name> - Edit Settings** window closes.
23. Register the SV Plug-in on the vCenter Server, see "Configuring and registering the ServerView VMware vCenter Plug-in Appliance" on page 28.

### 2.3.2 Deploying the ServerView VMware vCenter Plug-in Appliance using the VMware OVF tool

A second way to deploy the OVF package of the the ServerView VMware vCenter Plug-in Appliance is the VMware OVF tool. For further information about the VMware OVF tool please see the VMware documentation.

**Command to execute**

```
ovftool --X:injectOvfEnv --powerOn --acceptAllEulas --
noSSLVerify --prop:app.hostname=<VM_HOSTNAME> --prop:app.
rootpw=<VM_ROOT_PASSWORD> --diskMode=thin --name=<MY_VM_NAME>
ServerView_VMware_vCenter_Plug-in_Appliance_4.0.0.
ova vi://root:<ESXI_PASSWORD>@<ESXI_HOST>
```

**Explanatory notes on the variables**

| Variable | Meaning |
|---|---|
| <VM_HOSTNAME> | Hostname to set in the virtual machine of the ServerView VMware vCenter Plug-in Appliance |
| <VM_ROOT_PASSWORD> | Password of the root user to set in the virtual machine of the ServerView VMware vCenter Plug-in Appliance |
| <MY_VM_NAME> | Name to assign to the virtual machine of the ServerView VMware vCenter Plug-in Appliance |
| <ESXI_PASSWORD> | Password of the root user of the ESXi server where the virtual machine of the ServerView VMware vCenter Plug-in Appliance will be created |
| <ESXI_HOST> | ESXi server where the virtual machine of the ServerView VMware vCenter Plug-in Appliance will be created |

### 2.3.3 Configuring and registering the ServerView VMware vCenter Plug-in Appliance

Before you begin: Use either Firefox or Chrome browsers, as Microsoft Edge could cause problems.

1. Start the Web UI of the ServerView VMware vCenter Plug-in Appliance in a web browser: **https://<FQDN or IP of appliance>:5480**.

   The **Login** page is displayed.

2. Log in with user root credentials.

   The main page of the Web UI of the ServerView VMware vCenter Plug-in Appliance is displayed.

   The main page of the Web UI of the ServerView VMware vCenter Plug-in Appliance has the following tabs:

   - System
   - vCenter
   - Hostname
   - Network
   - Update

   In the following only the settings in the Web UI of the ServerView VMware vCenter Plug-in Appliance are described, which are necessary for configuring and registering the ServerView VMware vCenter Plug-in Appliance. For further information to the Web UI of the ServerView VMware vCenter Plug-in Appliance see "The ServerView VMware vCenter Plug-in Appliance" on page 42.

3. Select the **vCenter** tab.

   The **vCenter Configuration** view tab is displayed.

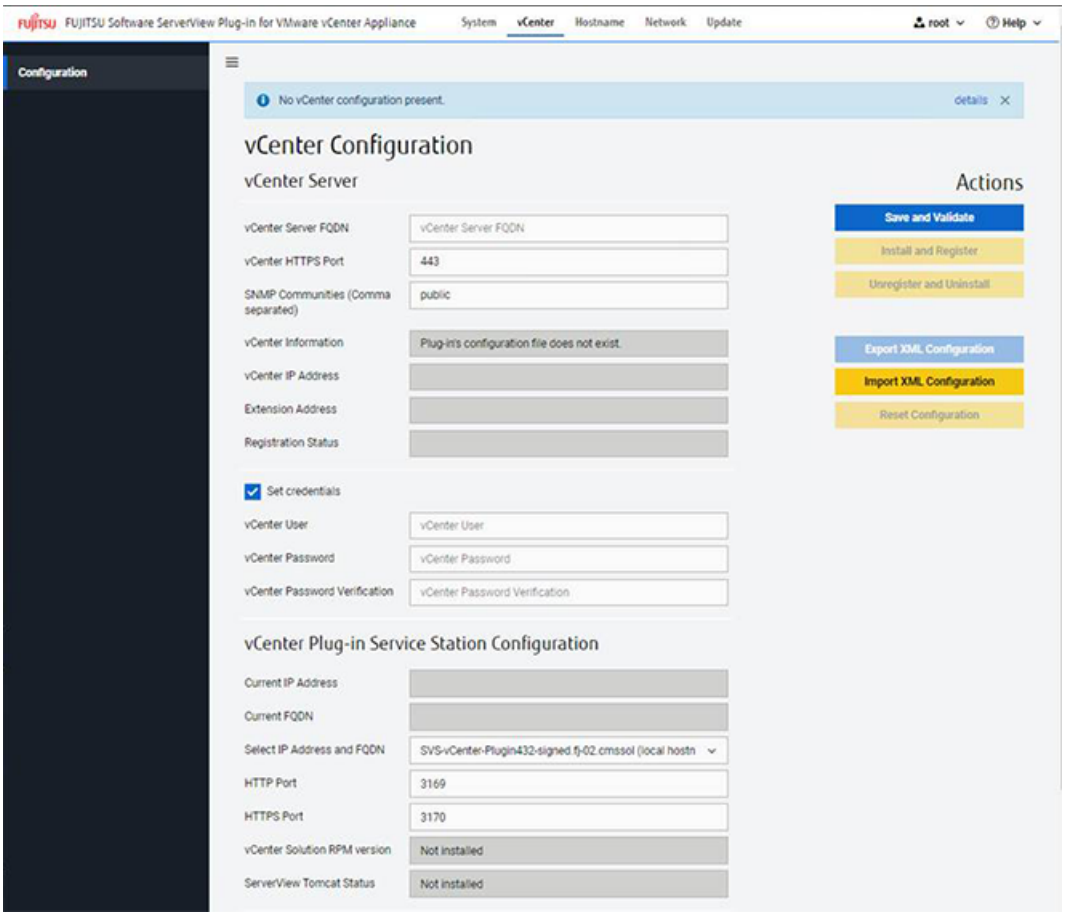


Figure 5: Web UI of the ServerView VMware vCenter Plug-in Appliance: **vCenter Configuration** view

4. Enter the settings necessary for the installation in the **vCenter Configuration** view.

   The **vCenter Configuration** view is divided into two areas:

   - **vCenter Server**
   - **vCenter Plug-in Service Station Configuration**

   **vCenter Server - vCenter Server FQDN**
   Network name of vCenter server which the SV Plug-in is intended to be registered to.

   **vCenter Server - vCenter HTTPS Port**
   HTTPS port of vCenter server (default: **443**).

   **vCenter Server - SNMP Communities (Comma separated)**
   Comma separated list of SNMP communities.

   **vCenter Server - Set credentials**
   The entries in the following fields are to be used as credentials to access vCenter server and register the SV Plug-in in it.

**vCenter Server - vCenter User**
User name of the credentials to access vCenter server.

**vCenter Server - vCenter Password**
Password of the credentials to access vCenter server.

**vCenter Server - vCenter Password Verification**
Securing repetition of the password of the credentials to access vCenter server.

**vCenter Plug-in Service Station Configuration - Select IP Address and FQDN**
Dropdown-list of IP addresses and network names of the current host. You must choose one of them. The selected item will be used by vCenter server to communicate with the ServerView VMware vCenter Plug-in Appliance.

If the host has more than one network adapter, you may see more than one IP address in the list.

The list also contains the local host name, which may not be resolved by other hosts in your network. By default, the host name entered during the deployment of the OVA template is selected.

**vCenter Plug-in Service Station Configuration - HTTP Port**
HTTP port to use for the plug-in service (default: **3169**).

**vCenter Plug-in Service Station Configuration - HTTPS Port**
HTTPS port to use for the plug-in service (default: **3170**).

5. Under **Actions** click the **Save and Validate** button.

   The ServerView VMware vCenter Plug-in Appliance will try to connect to the vCenter server using the specified configuration. If the connection is successful, the specified configuration will be stored locally on the vCenter server and the following fields will be filled in:

   **vCenter Server - vCenter Information**
   Idenfication of the vCenter server, e.g. **VMware vCenter Server 6.7.0 build-10244857** (is displayed when the specified configuration has been validated, see "Configuring and registering the ServerView VMware vCenter Plug-in Appliance" on page 28).

   **vCenter Server - vCenter IP Address**
   IP address of the vCenter server (is displayed when the specified configuration has been validated, see "Configuring and registering the ServerView VMware vCenter Plug-in Appliance" on page 28).

   **vCenter Server - Extension Address**
   URL of a plug-in currently registered in the vCenter server indicated under **vCenter IP Address** (is displayed when the specified configuration has been validated, see "Configuring and registering the ServerView VMware vCenter Plug-in Appliance" on page 28).

   **vCenter Server - Registration Status**
   Informs you whether the extension address points to the host on which the SV Plug-in is to be installed or to another:

   - **<empty>**

     No plug-in is registered. You can start the installation of the SV Plug-in.

   - **Registered for other hos**t

     A plug-in from another host is already registered in the selecte vCenter server.

     
     Installation cannot be executed.

   - **Registered for this host**

     The plug-in from this host is registered.

   **vCenter Plug-in Service Station Configuration - Current IP Address**
   IP address of the current host. The vCenter Server uses it to connect to the ServerView VMware vCenter Plug-in Appliance.

   **vCenter Plug-in Service Station Configuration - Current FQDN**
   FQDN of the current host. The vCenter Server uses it to connect to the ServerView VMware vCenter Plug-in Appliance.

6. Under **Actions** click **Install and Register**.

   The message **Installation is running** is displayed at the top of the **vCenter Configuration** view.

   
   The installation and registration process may take some minutes.

   After the installation process has been successfully completed, the message **Installation finished with success** is displayed at the top of the **vCenter Configuration** view.

   After a successful installation, the following fields of the **vCenter Configuration** view are filled in as follows:

   **vCenter Server - Extension Address**
   URL of the the ServerView VMware vCenter Plug-in Appliance.

   **vCenter Server - Registration Status**
   Is filled-in with **Registered for this host**.

   **vCenter Plug-in Service Station Configuration - vCenter Solution RPM version**
   Version of the SV Plug-in's RPM package that is installed on the ServerView VMware vCenter Plug-in Appliance.

   **vCenter Plug-in Service Station Configuration - ServerView Tomcat Status**
   Status of the Tomcat service.

   
   This value has to be **Running**.

7. Check whether the SV Plug-in is visible along with the client plug-ins:

   From the Home page of the vSphere Client, select **Administration** - **Solutions** - **Client Plug-ins**.

8. To display the **IPMI configuration** dialog used in the following step, you must log out of the vSphere Client and log in again.

9. Set the iRMC credentials, see "Configure iRMC credentials: 'IPMI configuration'" on page 59.

10. After the installation process has been successfully completed, log out of vSphere Client and log back in again.

    
    It is recommended to clear the browser cache as well as the Java cache once the installation process has been successfully completed.

It is recommended to restart all vSphere Client services that use the SV Plug-in to ensure consistency between VMware vCenter Server extension registration and Client client plug-in administration.

## 2.4 Updating

You can update the components of the ServerView VMware vCenter Plug-in Appliance and Oracle Linux.

### 2.4.1 Updating the components of the ServerView VMware vCenter Plug-in Appliance

An update of the components of the ServerView VMware vCenter Plug-in Appliance to version 5.0.0 is only possible from ServerView VMware vCenter Plug-in Appliance version 4.3.5.

1. Download the latest ISO image of the ServerView VMware vCenter Plug-in Appliance, see "Provisioning" on page 20.
2. Copy the ISO image to a data store of the virtual machine.
3. Connect the CD/DVD drive and the ISO image.
4. Start the Web UI of the ServerView VMware vCenter Plug-in Appliance in a web browser: **https://<FQDN or IP of appliance>:5480**.

   The **Login** page is displayed.
5. Log in with user root credentials.

   The main page of the Web UI of the ServerView VMware vCenter Plug-in Appliance is displayed.
6. Select the **Update** tab at the top of theServerView VMware vCenter Plug-in Appliance.

   The **Appliance updates** view is displayed.

   The **Appliance updates** view displays a list of the components of the ServerView VMware vCenter Plug-in Appliance. The **Local** column specifies the currently installed version of the component. The version of the SV Plug-in corresponds to the one in the name of the template file and the ISO file for an update.

7. Click the **Check updates** button.

   It is checked whether a newer version is available for one of the components.

   A message is displayed at the top of the view, e.g. **There are new updates**. The **Update** column of the list displays the version found in the ISO image for that component.

   **Plugin** - Note, that installing the update in the **Appliance updates** view is a different process than installing the program in the **vCenter Configuration** view (see "'vCenter' tab" on page 46). If the SV Plug-in was not installed and registered in the **vCenter Configuration** view , the update in the **Appliance updates** view will only copy the installation packages to the ServerView VMware vCenter Plug-in Appliance.

   **Web application** - If the web application is updated, no success message will be displayed. Only the message about the continuation of the update will disappear and the application will be restarted.

8. If a newer version of a component is available in the image, click the **Install updates** button.

   The newer version of the component is installed.

   The installation process may take a few minutes.

   After the installation process has been successfully completed, a message is displayed at the top of the view, e.g. **Plugin installed with success.**.

## 2.4.2 Updating Oracle Linux

**Requirements**

Supported Operating Systems (Appliance):

Oracle Linux 8.6

**Procedure**

The update process of Oracle Linux is handled using the YUM package manager.

1. Start the Web UI of the ServerView VMware vCenter Plug-in Appliance in a web browser: **https://<FQDN or IP of appliance>:5480**.

   The **Login** page is displayed.

2. Login with user root credentials.

   The main page of the Web UI of the ServerView VMware vCenter Plug-in Appliance is displayed.

3. Select the **Update** tab at the top of theServerView VMware vCenter Plug-in Appliance.

   The **Appliance updates** view is displayed.

4. Click the menu item **Settings** on the left side of the **Appliance updates** view.

   The **System updates settings** view opens.

5. Select the desired settings in the **System updates settings** view.

   **Install only security updates**
   All updates are installed by default. You can specify that only the security-relevant updates are installed.

   **Use a local repository**
   You can specify that a local repository is to be used. If you want to use a local repository, enter its URL in the **Local repostitory base URL** field.

6. Click the **Save Settings** button to store the desired settings above.

7. Click the menu item **System** on the left side of the **System updates settings** view.

   The **System updates** view opens.

8. Click the **Check updates** button.

   Updates are requested on the official Oracle Linux update servers. If updates are found, they will be listed in the **System updates** view.

   

   If an error message is displayed, you may need to set up a proxy for the YUM package management system in the **Network** - **Proxy** view, see "'Network' tab" on page 51.

9. If you want to install the updates found, click the **Install updates** button.

   As long as the installation process is running, the following message will be displayed: **Updates installation started. Status will refresh automatically.**.

   

   The installation process will take some time.

   After the installation process has been successfully completed, a message is displayed at the top of the view, e.g. **Installation ended successfully.**.

10. If the message **System reboot is required** is displayed, reboot the system.

## 2.5 Unregistering and uninstalling

It is necessary to unregister and uninstall the ServerView VMware vCenter Plug-in Appliance before removing the virtual machine of the appliance. Otherwise the registration on the vCenter server will remain and you will have to remove it manually using the Managed Object Browser (MOB), which is part of the vSphere Web Services SDK. MOB is a graphical interface that allows you to navigate the objects on a server and to invoke methods. For further information see https://pubs.vmware.com.

Before you begin: Use either Firefox or Chrome browsers. Using Microsoft Edge could cause problems.

1. Start the Web UI of the ServerView VMware vCenter Plug-in Appliance in a web browser: **https://<FQDN or IP of appliance>:5480**.

   The **Login** page is displayed.

2. Login with user root credentials.

   The main page of the Web UI of the ServerView VMware vCenter Plug-in Appliance is displayed.

   The main page of the Web UI of the ServerView VMware vCenter Plug-in Appliance has the following tabs:

   - System
   - vCenter
   - Hostname
   - Network
   - Update

   In the following only the settings in the Web UI of the ServerView VMware vCenter Plug-in Appliance are described, which are necessary for unregistering and uninstalling the ServerView VMware vCenter Plug-in Appliance. For further information to the Web UI of the ServerView VMware vCenter Plug-in Appliance see "The ServerView VMware vCenter Plug-in Appliance" on page 42.

3. Select the **vCenter** tab.

   The **vCenter Configuration** view tab is displayed.

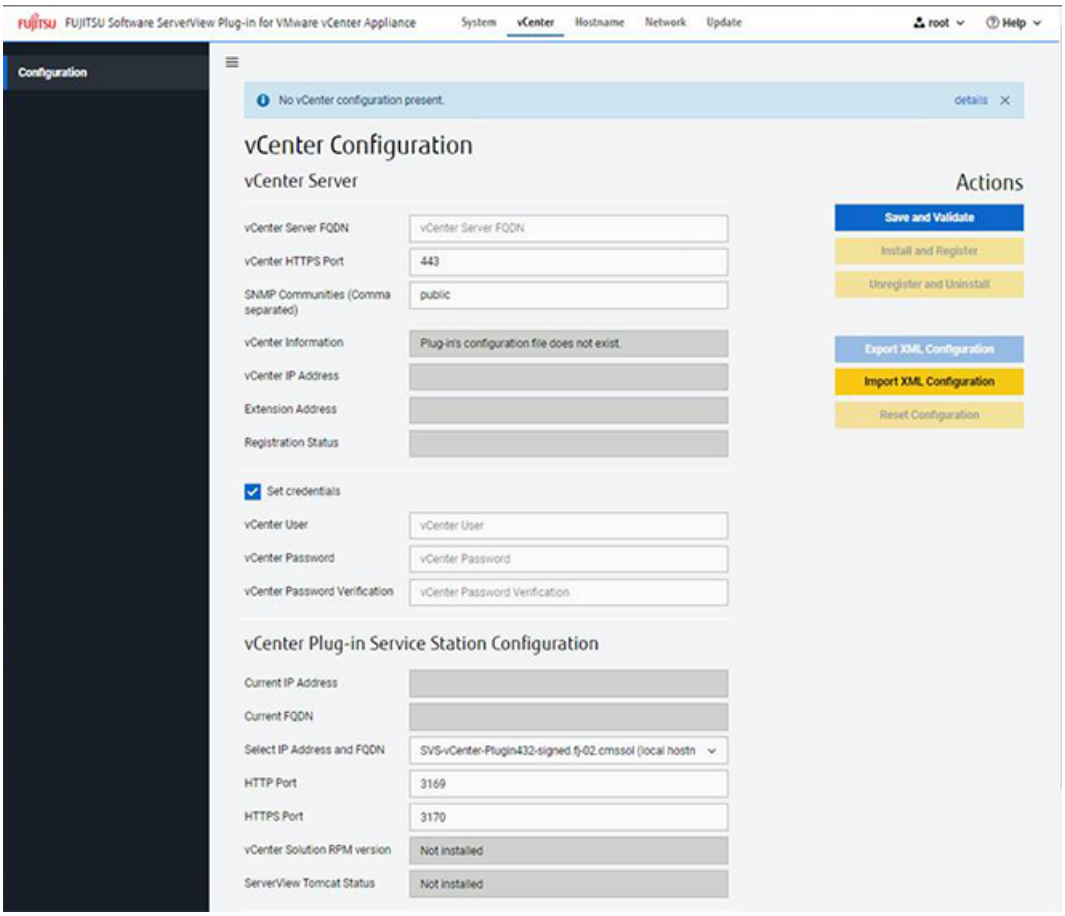


Figure 6: Web UI of the ServerView VMware vCenter Plug-in Appliance: **vCenter Configuration** view

4. Under **Actions** click the **Unregister and De-install** button.

   

   The uninstallation can only run if the setting **vCenter Server** - **Registration Status** in the **vCenter Configuration** view points to the ServerView VMware vCenter Plug-in Appliance to be uninstalled. The field has to display **Registered for this host**.

   The message **De-installation is running** is displayed at the top of the **vCenter Configuration** view.

   

   The unregisteration and uninstallation process may take up to a few minutes.

   After a successful uninstallation, the following fields of the **vCenter Configuration** view are filled in as follows:

   **vCenter Server - Extension Address**
   The field should be empty.

   **vCenter Server - Registration Status**
   The field should be empty.

   **vCenter Plug-in Service Station Configuration - vCenter Solution RPM version**
   Is filled-in with **Not installed**.

   **vCenter Plug-in Service Station Configuration - ServerView Tomcat Status**
   Is filled-in with **Not installed**.

   

   The uninstallation operation does not remove the configuration of the SV Plug-in that is stored in the ServerView VMware vCenter Plug-in Appliance.

5. After the uninstallation process has been successfully completed, log out of vSphere Client and log in to it again.

   

   It is recommended to clear the browser cache and the Java cache too after the installation process has been successfully completed.

   

   It is recommended to restart all vSphere Client services that use the SV Plug-in to ensure consistency between VMware vCenter Server extension registration and Web Client client plug-in administration.

6. You can remove the virtual machine of the ServerView VMware vCenter Plug-in Appliance.

# 3 Log in to vCenter Server using the vSphere Client

**Localization:**

The languages supported for using the SV Plug-in are English, German and Japanese. If the browser language matches one of these languages, the corresponding language will be selected for the SV Plug-in.

## 3.1 Requirements for logging in to vCenter Server using the vSphere Client

**vCenter Server and vSphere Client**

In vSphere V6.7 U1 and later, the vSphere Client is installed as part of the vCenter Server appliance deployment. This way, the vSphere Client always points to the same vCenter single sign-on instance.

## 3.2 Procedure

1. Open a web browser and enter the URL

   **vSphere Client:**

   https://<FQDN-or-IP-Address-of-VC>/ui

   The default port is 9443, but this can be changed during vSphere Client installation.

2. If a warning message about a potential security risk is displayed, select to continue to the website:

   **Microsoft Edge**

   1. Click **Details**.
   2. Under the additional message that is displayed, click **Go on to the webpage**.

   **Google Chrome**

   1. Click **Advanced**.
   2. Under the additional message that is displayed, click **Proceed to vcenter_server_ip_address_or_fqdn**.

3. On the vSphere Welcome page, select **Launch vSphere Client (HTML5)**.
4. If the warning message about a potential security risk appears again, repeat .....
5. If a warning message about a potential security risk is displayed again, select to continue to the website:

   **Microsoft Edge**

   1. Click **Details**.
   2. Under the additional message that is displayed, click **Go on to the webpage**.

   **Google Chrome**

   1. Click **Advanced**.
   2. Under the additional message that is displayed, click **Proceed to vcenter_server_ip_address_or_fqdn**.
6. In the **Username** text box, enter the user name that is registered on the vCenter single sign-on and has permissions on vCenter Server.
7. In the **Password** text box, enter the password.
8. Click **Login**.

   The vSphere Client connects to all the vCenter Server systems that the specified user has permissions for, allowing you to view and manage your vSphere inventory.

# 3.3 vSphere Client user interface

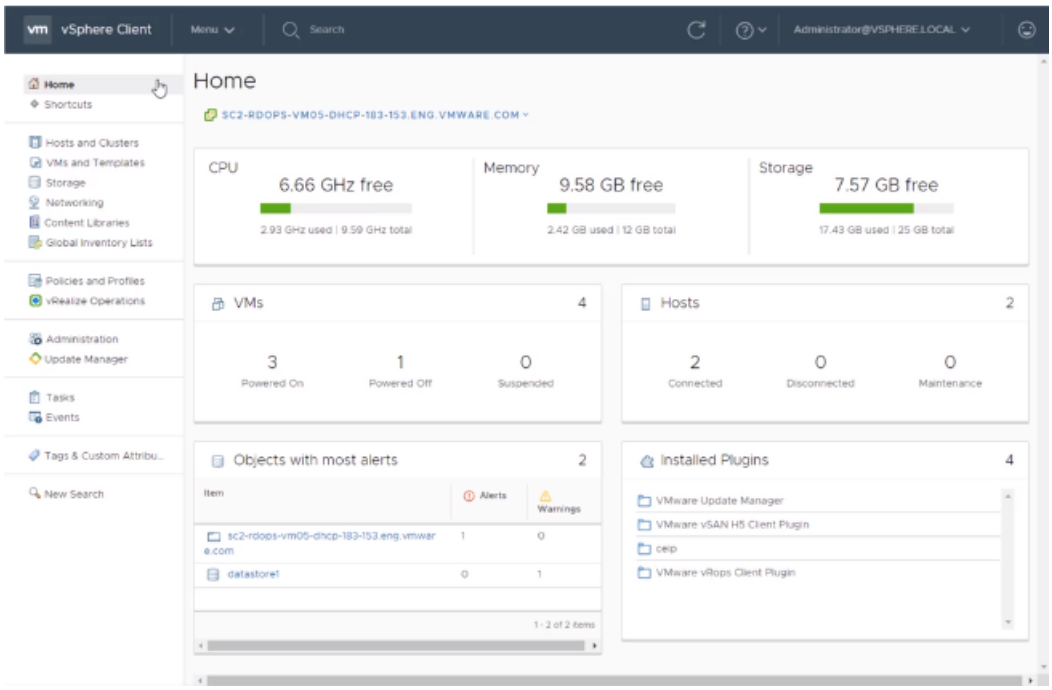


Figure 7: Home page of the vSphere Client user interface (Source: www.vmware.com)

The main parts of the vSphere Client user interface are the **Menu** area with the inventory trees and menu items, on the left side, and the central panel, in the middle and right area. Your selections in the **Menu** area drive the contents of the vSphere Client central panel.

You can access the contents of the **Menu** area at any time via the header of the vSphere Client.

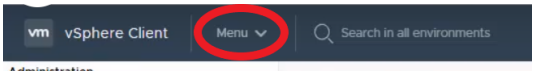


Figure 8: Detail of the vSphere Client header

In the inventory trees of the **Menu** area you find the usual listings, for example **Host and Clusters**. When you select an object in an inventory tree, information about it appears in the central panel. When you click a new object in the central panel, the inventory tree is restructured accordingly.

# 4 Configuration tasks and concepts

## 4.1 The ServerView VMware vCenter Plug-in Appliance

To save system resources, you can disable the web application of the ServerView VMware vCenter Plug-in Appliance. Click on your user name in the upper right corner of the application window. A menu will open. Select **Disable WebUI** from the menu. The application window is closed and cannot be called up again. You can re-enable the web application of the ServerView VMware vCenter Plug-in Appliance via its console interface, see "Console interface of the ServerView VMware vCenter Plug-in Appliance" on page 54.

### 4.1.1 Starting the Web UI of the ServerView VMware vCenter Plug-in Appliance

1. Start the Web UI of the ServerView VMware vCenter Plug-in Appliance in a web browser: **https://<FQDN or IP of appliance>:5480**.

   The **Login** page is displayed.

2. Login with user root credentials.

   The main page of the Web UI of the ServerView VMware vCenter Plug-in Appliance is displayed.

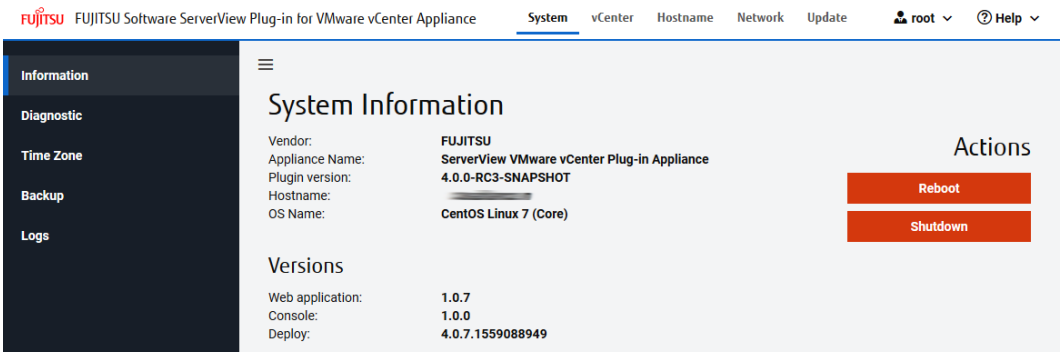


Figure 9: Web UI of the ServerView VMware vCenter Plug-in Appliance: **System** tab - **Information** menu item

## 4.1.2 The views of the Web UI of the ServerView VMware vCenter Plug-in Appliance

The main page of the Web UI of the ServerView VMware vCenter Plug-in Appliance has the following tabs:

- **System**
- **vCenter**
- **Hostname**
- **Network**
- **Update**

### 4.1.2.1 'System' tab

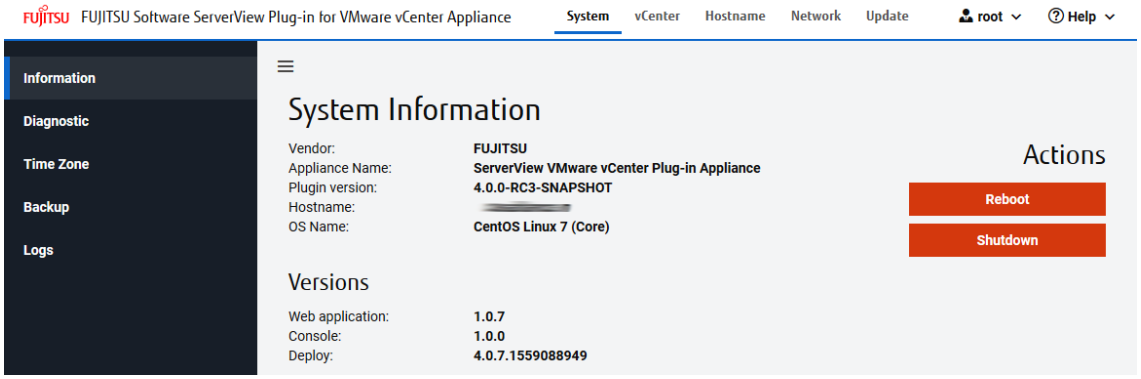


Figure 10: Web UI of the ServerView VMware vCenter Plug-in Appliance: **System** tab - **Information** menu item

#### 'System Information' view

The menu item **Information** on the left side of the view called via the **System** tab calls the **System Information** view.

The **System Information** view displays information on the ServerView VMware vCenter Plug-in Appliance including the versions of the components of the appliance.

The version of the SV Plug-in corresponds to the one in the name of the template file and the ISO file for an update.

The **Deploy** version is not changed during an update process. The **Deploy** version of the originally deployed template is displayed.

**Reboot**

You can reboot the system by clicking the **Reboot** button on the right side of the **System Information** view.

**Shutdown**

You can shutdown the system by clicking the **Shutdown** button on the right side of the **System Information** view.

#### 'Diagnostic' view

The menu item **Diagnostic** on the left side of the view called via the **System** tab calls the **Diagnostic** view.

The **Diagnostic** view displays information on CPU, memory, disk and network usage.

#### 'Time Zone Settings' view

The menu item **Time Zone** on the left side of the view called via the **System** tab calls the **Time Zone Settings** view.

Under **Time Zone Settings** you can set the time zone for your system.

**Save Settings**

You can save the new **System Time Zone** setting clicking the **Save Settings** button on the right side of the **Time Zone Settings** view.

#### 'Backup' view

The menu item **Backup** on the left side of the view called via the **System** tab calls the **Backup** view.

In the **Backup** view you can import data of the previous version of the ServerView VMware vCenter Plug-in Appliance or export the data of this version of the ServerView VMware vCenter Plug-in Appliance so that you can import it into the next version.

The data include:

- System and network settings
- vCenter Server and ServerView VMware vCenter Plug-in configuration
- ServerView VMware vCenter Plug-in data

**Import**

You can import data of ServerView VMware vCenter Plug-in Appliance from one version into a higher versionby clicking the **Import** button on the right side of the **Backup** view.

**Export**

You can export the data of ServerView VMware vCenter Plug-in Appliance (so that you can import it into the next version) by clicking the **Export** button on the right side of the **Backup** view.

### 'System Logs' view

The menu item **Logs** on the left side of the view called via the **System** tab calls the **System Logs** view.

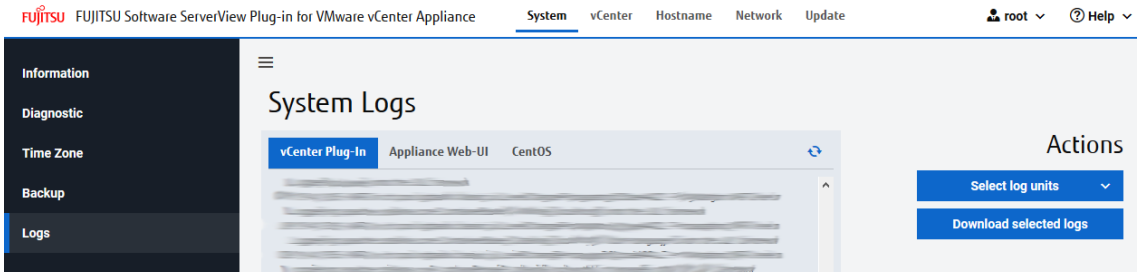


Figure 11: Web UI of the ServerView VMware vCenter Plug-in Appliance: **System** tab - **Logs** menu item

On the **System Logs** view, the content of the logs is displayed in a large field under the **System Logs** heading. Above this field, tabs offer you the possibility to switch from the content of a log to another. You can display **vCenter Plug-in** log, **Appliance Web-UI** log and **CentOS** log.

To refresh the display of the currently displayed log, click on the icon above the log display field on the right.

You can download logs and save them in a ZIP file. You can select different logs for download.

**Select log units**

You can select different logs for download clicking the **Select log units** button on the right side of the **System Logs** view.

The logs available for selection are grouped into two groups:

- **FUJITSU ServerView Logs**

  If the SV Plug-in is not yet installed, most positions of the **FUJITSU ServerView Logs** category will not be displayed.

  - **appliance Web-UI**

    The log of the ServerView VMware vCenter Plug-in Appliance Web-UI.

  - **SVSInstaller.log**

    The log of the plug-in installer.

  - **svs.mv.db**

    vCenter Plug-in database. It is not a log like the other positions.

  - **Logs of various plug-in components**

    E.g. catalina, svs-services.

- **CentOS Logs**

  Logs of the system services, e.g. atd, rsyslog, tuned.

**Download selected logs**

You can save the files selected with the help of the **Select log units** button in a ZIP file by clicking the **Download selected logs** button on the right side of the **System Logs** view.

### 4.1.2.2 'vCenter' tab

In the **vCenter Configuration** view you can install the SV Plug-in and register it in the vCenter server. You can also unregister and de-install the SV Plug-in.

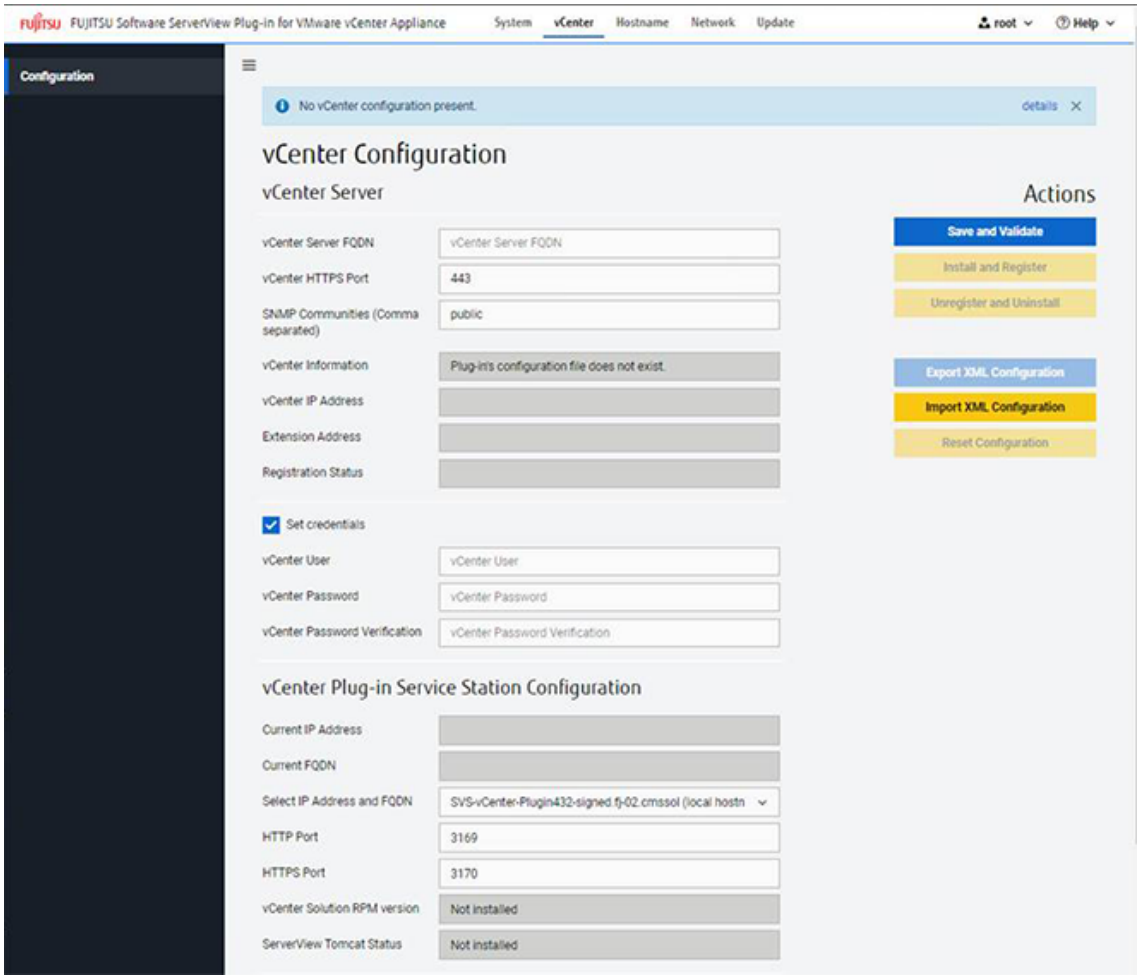


Figure 12: Web UI of the ServerView VMware vCenter Plug-in Appliance: **vCenter Configuration** view

The **vCenter Configuration** view is divided into two areas:

- **vCenter Server**
- **vCenter Plug-in Service Station Configuration**

#### 4.1.2.3 'vCenter Server'

The **vCenter Server** area of the **vCenter Configuration** view offers you options for configuring the server the SV Plug-in is intended to work with, and displays information about its state.

**vCenter Server FQDN**
Network name of vCenter server which the SV Plug-in is intended to be registered to.

**vCenter HTTPS Port**
HTTPS port of vCenter server (default: **443**).

**SNMP Communities (Comma separated)**
Comma separated list of SNMP communities.

When you have completed the above settings and the below settings from **Set credentials** to **vCenter Password Verification**, click the **Save and Validate** button, see "Save and Validate" on page 49. The ServerView VMware vCenter Plug-in Appliance will try to connect to the vCenter server using the specified configuration.

**vCenter Information**
Idenfication of the vCenter server, e.g. **VMware vCenter Server 6.7.0 build-10244857** (is displayed when the specified configuration has been validated, see "Save and Validate" on page 49).

**vCenter IP Address**
IP address of the vCenter server (is displayed when the specified configuration has been validated, see "Save and Validate" on page 49).

**Extension Address**
URL of a plug-in currently registered in the vCenter server indicated under **vCenter IP Address** (is displayed when the specified configuration has been validated, see "Save and Validate" on page 49).

**Registration Status**

Informs you whether the extension address points to the host on which the SV Plug-in is to be installed or to another:

- **<empty>**

  No plug-in is registered. You can start the installation of the SV Plug-in, see "Installing the Appliance" on page 20.

- **Registered for other hos**t

  A plug-in from another host is already registered in the selecte vCenter server.

  

  Installation cannot be executed.

- **Registered for this host**

  The plug-in from this host is registered.

**Set credentials**

The entries in the following fields are to be used as credentials to access vCenter server and register the SV Plug-in in it.

**vCenter User**

User name of the credentials to access vCenter server.

**vCenter Password**

Password of the credentials to access vCenter server.

**vCenter Password Verification**

Securing repetition of the password of the credentials to access vCenter server.

### 4.1.2.4 'vCenter Plug-in Service Station Configuration'

The **vCenter Plug-in Service Station Configuration** section of the **vCenter Configuration** view offers you options for configuring the plug-in service that will run on the ServerView VMware vCenter Plug-in Appliance, and displays information about its status.

When you have completed the settings in this area, click the **Save and Validate** button, see "Save and Validate" on page 49. The ServerView VMware vCenter Plug-in Appliance will try to connect to the vCenter server using the in the **vCenter Server** area (see "'vCenter Server'" on page 47) specified configuration.

**Current IP Address**

IP address of the current host. The vCenter Server uses it to connect to the ServerView VMware vCenter Plug-in Appliance.

**Current FQDN**

FQDN of the current host. The vCenter Server uses it to connect to the ServerView VMware vCenter Plug-in Appliance.

**Select IP Address and FQDN**

Dropdown-list of IP addresses and network names of the current host. You must choose one of them. The selected item will be used by vCenter server to communicate with the ServerView VMware vCenter Plug-in Appliance.

If the host has more than one network adapter, you may see more than one IP address in the list.

The list also contains the local host name, which may not be resolved by other hosts in your network. By default, the host name entered during the deployment of the OVA template is selected.

**HTTP Port**

HTTP port to use for the plug-in service (default: **3169**).

**HTTPS Port**

HTTPS port to use for the plug-in service (default: **3170**).

**vCenter Solution RPM version**

Version of the SV Plug-in's RPM package that is installed on the ServerView VMware vCenter Plug-in Appliance.

**ServerView Tomcat Status**

Status of the Tomcat service.

This value has to be **Running**.

### 4.1.2.5 Buttons in the 'vCenter Configuration' view

**Save and Validate**

When you have completed the settings in the **vCenter Server** area (see "'vCenter Server'" on page 47), click the **Save and Validate** button. The ServerView VMware vCenter Plug-in Appliance will try to connect to the vCenter server using the specified configuration. If the connection is successful, the specified configuration will be stored locally on the vCenter server and the fields in the **vCenter Server** area (see "'vCenter Server'" on page 47) will be filled in.

**Install and Register**

Clicking the **Install and Register** button starts the configuring and registering of the ServerView VMware vCenter Plug-in Appliance. For further information see "Configuring and registering the ServerView VMware vCenter Plug-in Appliance" on page 28.

**Unregister and De-install**

Clicking the **Unregister and De-install** button starts the unregistering and uninstalling of the ServerView VMware vCenter Plug-in Appliance. For further information see "Unregistering and uninstalling" on page 36.

**Export XML Configuration**

The parameters you have entered in the **vCenter Configuration** view are stored locally in the ServerView VMware vCenter Plug-in Appliance. The **Export XML Configuration** button allows you to export the locally stored configuration parameters to a file.

For security reasons, the password is not included in this file.

**Import XML Configuration**

The **Import XML Configuration** button allows you to import the configuration parameters stored in an exported file in the **vCenter Configuration** view.

For security reasons, the password is not included in this file.

**Reset Configuration**

The **Reset Configuration** button allows you to remove the current configuration parameters in the **vCenter Configuration** view and reset them to the default values.

The configuration parameters in the **vCenter Configuration** view cannot be changed if the SV Plug-in is already installed and registered.

### 4.1.2.6 'Hostname' tab

The **Appliance Hostname Configuration** view allows you to change the local name of the host.

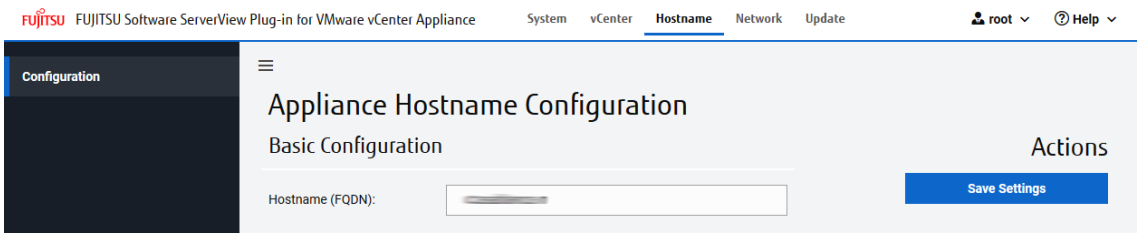


Figure 13: Web UI of the ServerView VMware vCenter Plug-in Appliance: **Appliance Hostname Configuration** view

**Hostname (FQDN)**

Local name of the host.

**Save Settings**

When you have completed the settings in the **Appliance Hostname Configuration** view, click the **Save Settings** button. The specified configuration will be stored locally.

It is possible that this host name is not immediately visible in the network. If the DNS server does not allow dynamic updates, this host name will remain a local name only.

### 4.1.2.7 'Network' tab

**'Status' view**

The menu item **Status** on the left side of the view called via the **Network** tab calls the **Status** view.

The **Status** view displays the current configuration of the gateway, DNS servers and network interfaces.

**'Address' view**

The menu item **Address** on the left side of the view called via the **Network** tab calls the **Address** view.

In the **Address** view you can change the network configuration.

**'Proxy' view**

The menu item **Proxy** on the left side of the view called via the **Network** tab calls the **Proxy** view.

The **Proxy** view displays the HTTP proxy configuration and you can change it in this page. There are separate proxy configurations for HTTP protocol, HTTPS protocol and YUM package management system.

### 4.1.2.8 'Update' tab

In the views of the **Update** tab you can update the ServerView VMware vCenter Plug-in Appliance and Oracle Linux.

For further information see "Updating" on page 33.

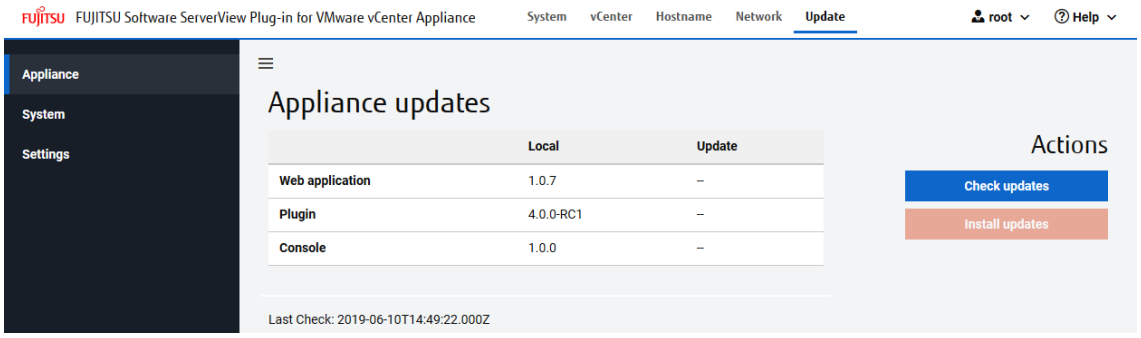


Figure 14: Web UI of the ServerView VMware vCenter Plug-in Appliance: **Update** tab - **Appliance** menu item

#### 'Appliance updates' view

The menu item **Appliance** on the left side of the view called via the **Update** tab calls the **Appliance updates** view.

The **Appliance updates** view displays a list of the components of the ServerView VMware vCenter Plug-in Appliance. The **Local** column specifies the currently installed version of the component.

The version of the SV Plug-in corresponds to the one in the name of the template file and the ISO file for an update.

#### Check updates

You can check whether a newer version is available for one of the components. Attach the ISO image to the virtual machine and click the **Check updates** button.

A message is displayed at the top of the view, e.g. **There are new updates**. The **Update** column of the list displays the version found in the ISO image for that component.

**Install updates**

**Plugin** - Note, that installing the update in the **Appliance updates** view is a different process than installing the program in the **vCenter Configuration** view (see "'vCenter' tab" on page 46). If the SV Plug-in was not installed and registered in the **vCenter Configuration** view , the update in the **Appliance updates** view will only copy the installation packages to the ServerView VMware vCenter Plug-in Appliance.

**Web application** - If the web application is updated, no success message will be displayed. Only the message about the continuation of the update will disappear and the application will be restarted.

If a newer version of a component is available in the image, click the **Install updates** button.

The newer version of the component is installed.

The installation process may take a few minutes.

After the installation process has been successfully completed, a message is displayed at the top of the view, e.g. **Plugin installed with success.**.

**'System updates' view**

The menu item **System** on the left side of the view called via the **Update** tab calls the **System updates** view.

In the **System updates** view you can install updates for Oracle Linux. The installation process is handled using the YUM package manager.

In the **System updates settings** view you can make settings for the Oracle Linux update to be started via the **System updates** view, see "'System updates' view" on page 53.

**Check updates**

Clicking the **Check updates** button updates are requested on the official Oracle Linux update servers. If updates are found, they will be listed in the **System updates** view.

If an error message is displayed, you may need to set up a proxy for the YUM package management system in the **Network** - **Proxy** view, see "'Network' tab" on page 51.

**Install updates**

If you want to install the updates found by clicking the **Check updates** button above, click the **Install updates** button.

As long as the installation process is running, the following message will be displayed: **Updates installation started. Status will refresh automatically.**.

The installation process will take some time.

After the installation process has been successfully completed, a message is displayed at the top of the view, e.g. **Installation ended successfully.**.

If the message **System reboot is required** is displayed, reboot the system.

**'System updates settings'**

The menu item **Settings** on the left side of the view called via the **Update** tab calls the **System updates settings** view.

In the **System updates settings** view you can make settings for the Oracle Linux update to be started via the **System updates** view, see "'System updates' view" on page 53.

**Install only security updates**

All updates are installed by default. You can specify that only the security-relevant updates are installed.

**Use a local repository**

You can specify that a local repository is to be used. If you want to use a local repository, enter its URL in the **Local repository base URL** field.

**Save Settings**

Clicking the **Save Settings** button stores the settings above.

### 4.1.3 Console interface of the ServerView VMware vCenter Plug-in Appliance

The ServerView VMware vCenter Plug-in Appliance has a very simple console interface. Via the console interface you can perform the following actions:

- Log into a shell.
- Disable or enable the Web UI of the ServerView VMware vCenter Plug-in Appliance.
- Set the time zone.

The console interface displays the current URL of the ServerView VMware vCenter Plug-in Appliance.

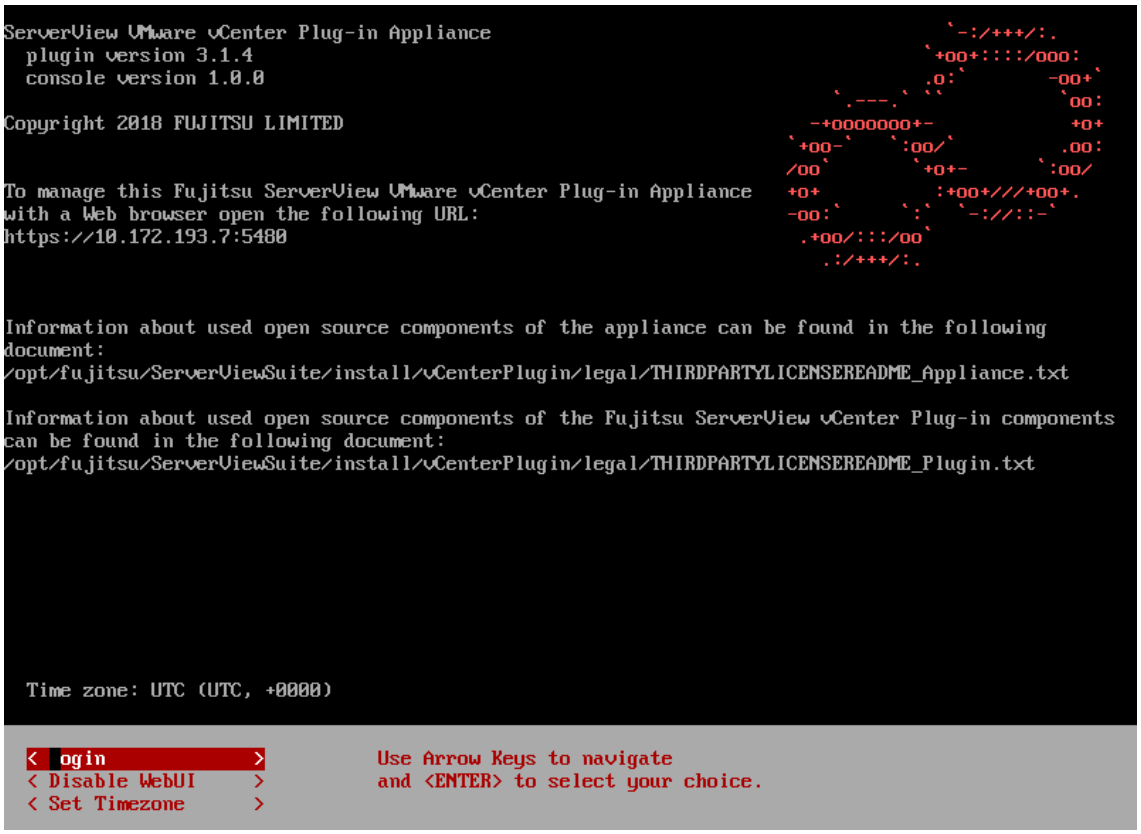


Figure 15: Console interface of the ServerView VMware vCenter Plug-in Appliance

### 4.1.4 Configuring the port of the the Web UI of the ServerView VMware vCenter Plug-in Appliance via a system file

You can configure the port of the the Web UI of the ServerView VMware vCenter Plug-in Appliance via the following system file:

**/opt/fujitsu/ServerViewSuite/vcenter/appliance/vm.properties.json**

1. Change the **webui.port**.

```
(...)
"webui": {
"protocol": "https",
"port": "5480"
}
```

2. Save the file.

3. Restart the Web application of the ServerView VMware vCenter Plug-in Appliance.

You may have to change the firewall settings additionally.

### 4.1.5 Configuring switching between HTTP and HTTPS via a system file

You can configure the switch between HTTP and HTTPS via the following system file:

**/opt/fujitsu/ServerViewSuite/vcenter/appliance/vm.properties.json**

1. Change the **webui.protocol** field to **http**.

```
(...)
"webui": {
"protocol": "https",
"port": "5480"
}
```

2. Save the file.
3. Restart the Web application of the ServerView VMware vCenter Plug-in Appliance.

If HTTPS support is enabled, an SSL certificate will be generated during the Web application start process. If you want to generate a new self-signed certificate, remove the **/opt/fujitsu/ServerViewSuite/vcenter/appliance/resources/https.pfx** file and restart the Web application.

## 4.2 SV vCenter Service configuration

You can use the **SV vCenter Service Configuration Overview** to manage all the SV vCenter Services installed in your environment.

For performance reasons we recommend one SV vCenter Service per vCenter server.

### 4.2.1 Opening the SV vCenter Service Configuration Overview

1. In the **Menu** area of the vSphere Client, select the item **Administration**.
2. Select the sub-item **FUJITSU PRIMERGY**.
3. Select the sub-item **SV vCenter Service Configuration**.

   In the central panel of the vSphere Client the **SV vCenter Service Configuration Overview** opens.

For further information see "SV vCenter Service Configuration Overview" on page 108.

### 4.2.2 Adding a vCenter to the SV vCenter Service

The following procedure will help if a connection problem with an SV vCenter Service occurs: If a vCenter is connected to a failing SV vCenter Service and you connect it to another SV vCenter Service, the vCenter will be disconnected from the failing SV vCenter Service and added to the new one.

If you have changed the privileges in one of the FUJITSU PRIMERGY role definitions and you connect the vCenter (to which the role is assigned) to another SV vCenter Service, the role definitions will be overwritten! See "Changing privileges of a role definition" on page 66.

1. In the **SV vCenter Service Configuration Overview**, select an SV vCenter Service in the **Service Location** selection box.

   The current properties of the selected SV vCenter Service are displayed.
2. Click the + icon.

   A dialog opens:

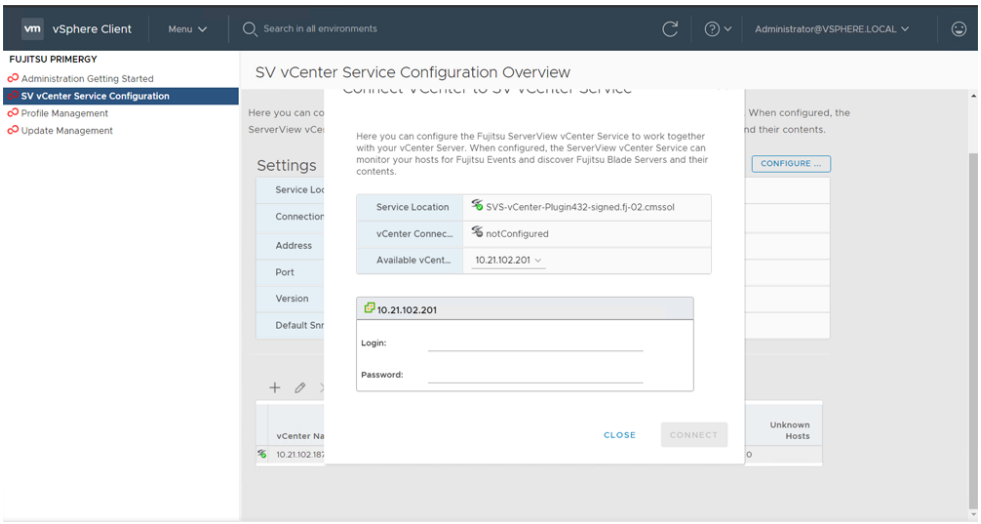


Figure 16: Add a vCenter to the SV vCenter Service

3. Select one vCenter in the **Available vCenters** selection box.

   The current connection status of the selected vCenter is displayed.
4. Enter the user name and password of the administrator account of the vCenter.
5. Click **Connect**.

   The vCenter is added to the SV vCenter Service.

### 4.2.3 Updating the vCenter credentials

It may be necessary to update the credentials of a vCenter (e.g. if the administrator password has changed).

1. In the **SV vCenter Service Configuration Overview**, select an SV vCenter Service in the **Service Location** selection box.

   The current properties of the selected SV vCenter Service are displayed.
2. In the **vCenter Name** list, select the desired vCenter.
3. Click the pencil icon.

   A dialog opens.
4. Enter the user name and password of the administrator account of the vCenter.
5. Click **Update Connection**.

   The vCenter credentials are updated on the SV vCenter Service.

### 4.2.4 Removing a vCenter from the SV vCenter Service

An SV vCenter Service requires at least one vCenter to be connected. Therefore, it is only possible to disconnect a vCenter if more than one vCenter is connected. To disconnect all vCenters from an SV vCenter Service, uninstall the SV vCenter Service.

1. In the **SV vCenter Service Configuration Overview**, select one SV vCenter Service in the **Service Location** selection box.

   The current properties of the selected SV vCenter Service are displayed.
2. In the **vCenter Name** list, select the desired vCenter.
3. Click the **X** icon.

   The vCenter is disconnected from the SV vCenter Service.

## 4.3 Configure iRMC credentials: 'IPMI configuration'

In order to monitor a host via Redfish or IPMI, the user name and password for iRMC must be configured in vCenter Server.

The iRMC is an IPMI 2.0-compatible Baseboard Management Controller (BMC) providing out-of-band monitoring and power management capabilities as well as additional advanced features.

In the vSphere/SV Plug-in environment, the iRMC credentials are initially stored in two different locations independently of each other:

- in vSphere/vCenter

  as **IPMI/iLO setting for Power Management (DPM)**

  Detailed information is required, including the MAC address of the iRMC.

  The **IPMI/iLO setting for Power Management (DPM)** configuration is helpful for performing power management functions from the vCenter.

  It is also important, for example, if the ServerView Offline Update and ServerView Cluster Offline Update workflows are called directly from the VMware Orchestrator.
- in the SV Plug-in

  as **IPMI configuration**

You can store the iRMC credentials via the **IPMI configuration** dialog of the SV Plug-in right away as in **IPMI/iLO setting for Power Management (DPM)** configuration in vSphere/vCenter.

### 4.3.1 Privileges required for the iRMC user (Redfish/ IPMI)

The user configured in vCenter Server must have the following privileges:

**Redfish**

**iRMC User Role**: **OEM**. Redfish must be enabled as a service and the user needs the appropriate Redfish role.

**IPMI**

The iRMC user account must have the LAN channel privilege of **OEM** to use single sign-on when starting iRMC, or to start other IPMI actions from the SV Plug-in.

It is possible, however, to limit the iRMC privileges depending on the role of the current vCenter user. For more information see "Starting iRMC functions with/without single sign-on" on page 67.

The iRMC credentials (user name and password) must be configured to have access to a number of iRMC-based actions on an ESXi host:

- Toggle Identify LED
- Start the iRMC Web Interface with single sign-on
- Start the Remote Console (AVR)
- Start a System Report

Note that the **Enable IPMI Over LAN** option have to be enabled in the iRMC settings.

### 4.3.2 Procedure

There are two possibilities to set the iRMC credentials:

- Setting iRMC credentials for a single server

  - See "Setting iRMC credentials for a single server" on page 61.

- Setting iRMC credentials for multiple servers

  - See "Setting iRMC credentials for multiple servers" on page 62.

Be careful when editing the credential information. If invalid credentials are entered, it may take a few minutes before you see an error message. If the iRMC credentials are configured and the wrong credentials are entered, the configuration will take place with no change.

#### 4.3.2.1 Setting iRMC credentials for a single server

1. Log in to vCenter Server using the vSphere Client (see "Log in to vCenter Server using the vSphere Client" on page 39).
2. Start the **FUJITSU PRIMERGY Action Configure IPMI** (for an ESXi host, see "Starting a FUJITSU PRIMERGY Action" on page 91).
3. Click the item/icon **IPMI Configuration**.

   The following dialog is displayed:

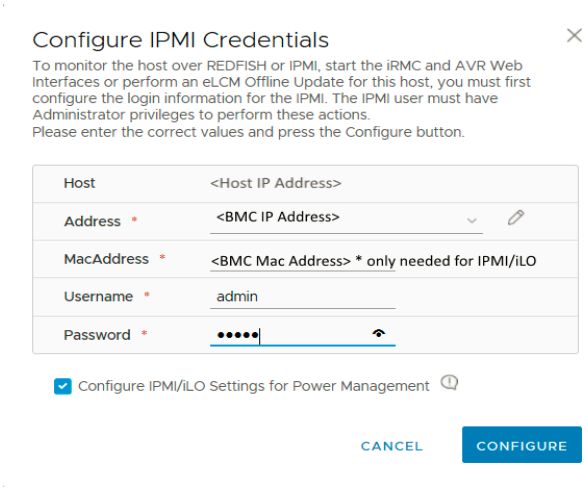


Figure 17: IPMI configuration dialog of the SV Plug-in (vSphere Client)

**Host**

IP address or FQDN of the host

**Address**

IP address of the iRMC of the host

Is retrieved directly from the host when the dialog is started.
If the CIM provider is not available (host down or host not connected), you must enter the BMC address manually. The given BMC address is checked for validity.

If there is more than one BMC IPv4 address, a selection box is shown, where you can choose which one you want to use. If you switch between the addresses, the corresponding MAC address will be shown in the **MacAddress** input field.

**MacAdress (only needed for IPMI/iLO)**

MAC address of the iRMC of the host.

The MAC address is only necessary if the checkbox **Configure IPMI/iLO Settings for Power Management** (see below) is activated.

The MAC address is retrieved directly from the host when the dialog is started.

If it is not possible to obtain a MAC address of the iRMC, you can enter it manually.

**Username**

iRMC user name

Note the privileges required by the user to use Redfish/ IPMI (see "Privileges required for the iRMC user (Redfish/ IPMI)" on page 60).

**Password**

iRMC password

Note the privileges required by the user to use Redfish/ IPMI (see "Privileges required for the iRMC user (Redfish/ IPMI)" on page 60).

**Configure IPMI/iLO Settings for Power Management**

Activate this checkbox to store the iRMC credentials via the **IPMI configuration** dialog of the SV Plug-in right away in **IPMI/iLO setting for Power Management (DPM)** configuration in vSphere/vCenter.

4. Click **CONFIGURE** to send and store the user credentials.

Once this user information is stored in vCenter Server, you only have to do this in the case of changes (e.g. if the credentials have been changed on the host).

#### 4.3.2.2 Setting iRMC credentials for multiple servers

Setting iRMC credentials for multiple servers is only possible for servers with CIM. Therefore, hosts with ESXi as of 8.0 cannot be used for setting iRMC credentials for multiple servers.

1. Start the FUJITSU PRIMERGY Action **Configure IPMI** for a vCenter, folder, DataCenter, or cluster (for a vCenter or cluster see "FUJITSU PRIMERGY Actions" on page 103).

   The parent container is searched for all hosts. All hosts found in the container and their configuration status (**Configured**, **Not Configured**, **Unknown**) are displayed in the dialog that is now displayed.

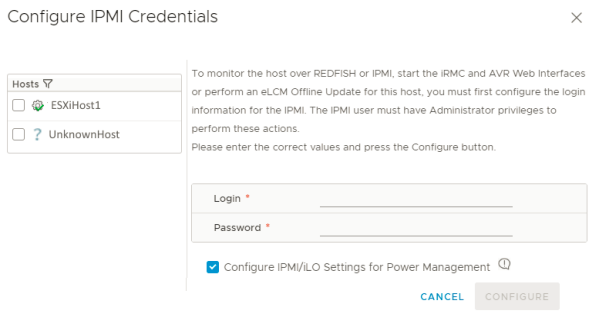


   Figure 18: IPMI configuration dialog of the SV Plug-in (vSphere Client (HTML5))

2. In the left pane of the IPMI configuration dialog a list of the hosts found is displayed.

   Check the hosts you want to configure.

   Alternatively, you can check all hosts at once by clicking the  icon.

3. In the right pane of the IPMI configuration dialog give the credentials:

   **Login (mandatory)**
   iRMC user name

   
   Note the privileges required by the user to use Redfish/ IPMI (see "Privileges required for the iRMC user (Redfish/ IPMI)" on page 60).

   **Password (mandatory)**
   iRMC password

   
   Note the privileges required by the user to use Redfish/ IPMI (see "Privileges required for the iRMC user (Redfish/ IPMI)" on page 60).

   **Configure IPMI/iLO Settings for Power Management**
   Activate this checkbox to immediately store the iRMC credentials via the **IPMI configuration** dialog of the SV Plug-in in the **IPMI/iLO setting for Power Management (DPM)** configuration in vSphere/vCenter.

4. Click **CONFIGURE** to send the user credentials.

   A confirmation dialog is displayed.

5. Confirm that you want to start a task.

   The dialog confirms the start of the task.

The SV vCenter Service now scans the hosts selected in the list. The SV vCenter Service uses CIM requests to query the IP and Mac address of each host. At the same time the SV vCenter Service checks the connection to the iRMC. If the connection works, the SV vCenter Service sets the credentials for the host. If an error occurs in this process for a host, a message informs about the problem - see "Error events (IPMI/iLO configuration)" on page 64.

If the SV vCenter Service has processed all hosts selected in the list, the task is terminated. You can see information about the completed task in the task manager of the parent container.

Once this user information is stored in vCenter Server, you only have to do this again in the case of changes (e.g. if the credentials have been changed on the host).

**Error events (IPMI/iLO configuration)**

If an error occurs in the IPMI configuration process for a host, an event message informs about the problem. You will find the event message in the event log. Each message is assigned to a target. If possible, the concrete affected host is given under **Target**. Otherwise, the parent container is given.

The following error event messages can be given:

**Update IPMI credentials for node <name of the node> has failed**

General update IPMI credentials failure event.

Service has failed to update IPMI credentials. If the problem persists, see **svs-vcenter-svc.log** for more details.

**Invalid IPMI credentials for node**

Credentials provided by the user are invalid.

**Can't retrieve BMC ip address for node <name of the node>**

Service cannot retrieve the IP address of the iRMC .

This event can be triggered by connection problems to the host. Check if the host's CIM service is working. You may also enable IPMI or Redfish protocol for the host.

**Node was not found by moid <name of moid>**

The system didn't recognize the moid of the host.

This event is associated with the parent container for which the configuration task was performed.

Maybe you can fix this problem by reconnecting this host so that the system can rediscover the host and process its information.

**Configure IPMI Credentials is not supported for non-Fujitsu Host: <name of the host>**

The host is not supported by Fujitsu.

The **Configure IPMI/iLO Settings** task can only be performed for Fujitsu hosts.

**Some tasks failed. Check events tab for details**

General update IPMI credentials failure event.

The service could only update the IPMI credentials for some of the selected hosts. If the problem persists, see **svs-vcenter-svc.log** for more details.

**Could not finish the process. Start again**

The service was not able to finish the configuring task due to the Event Service down time.

## 4.4 FUJITSU PRIMERGY vCenter role definitions and iRMC single sign-on

The single sign-on functionality no longer works in iRMC S5. When calling the iRMC Web Interface from SV Plug-in, the user will be requested to log in to the iRMC Web Interface.

The SV Plug-in has four role definitions. They are designed for using single sign-on when starting the iRMC Web Interface and remote console (AVR).

All role definitions contain the system privileges as well as the privilege **Host.CIM.CIM Interaction**, which is needed to operate the SV Plug-in itself. For more information see "FUJITSU PRIMERGY vCenter role definitions" on page 66.

It is possible to add the extended iRMC privileges to a FUJITSU PRIMERGY vCenter role definition, see "Starting iRMC functions with/without single sign-on" on page 67. You can also use the FUJITSU PRIMERGY vCenter role definitions to limit iRMC functionality, see "Examples of using role definitions to limit iRMC functionality" on page 70.

The **Role Definitions** sub-tab of the **Plug-in Definitions** view on the home page of the SV Plug-in (see "ROLE DEFINITIONS" on page 81) lists the predefined FUJITSU PRIMERGY roles. If the role definitions have been reconfigured after installation, the changes relevant to correct processing of the SV Plug-in will be marked.

### 4.4.1 FUJITSU PRIMERGY vCenter role definitions

Four new role definitions have been added to the SV Plug-in:

FUJITSU PRIMERGY Plug-in Administrator

Contains all the privileges needed to start the iRMC Web Interface and AVR using single sign-on with the iRMC LAN channel privilege level of **Administrator**.

The user can also change the configuration for alarms.

FUJITSU PRIMERGY Plug-in Super Operator

Contains a subset of the SV Plug-in **Administrator** privileges that are needed to start the iRMC Web Interface using single sign-on with the iRMC LAN channel privilege of **Operator** and plus the extended iRMC privileges **ConfigureBMC**, **RemoteStorage**, and **AVR**.

The user can make some configuration changes (but, for example, no firmware changes).

The user can also acknowledge alarms.

The user can start AVR from within the iRMC Web Interface.

FUJITSU PRIMERGY Plug-in Operator

Contains only the privileges needed to start the iRMC Web Interface using single sign-on with the iRMC LAN channel privilege of **Operator**, plus the extended iRMC privilege **AVR**.

The user will be able to perform shutdown/reboot on the host, but cannot make any configuration changes.

The user can also acknowledge alarms.

The user can start AVR from within the iRMC Web Interface.

FUJITSU PRIMERGY Plug-in Monitor

Contains only the privileges needed to start the iRMC Web Interface using single sign-on with the iRMC LAN channel privilege of **User**.

The user can start AVR from within the iRMC Web Interface.

### 4.4.2 Changing privileges of a role definition

The **Role Definitions** sub-tab of the **Plug-in Definitions** view on the home page of the SV Plug-in lists the predefined FUJITSU PRIMERGY role definitions, which are generated during the installation process (see "ROLE DEFINITIONS" on page 81).

If the role definitions have been reconfigured after installation, the changes relevant to correct processing of the SV Plug-in will be marked.

#### Configuring the FUJITSU PRIMERGY role definitions

To change the privileges in one of these role definitions, use the vSphere Client user interface.

If you need to change the privileges in one of the FUJITSU PRIMERGY role definitions, clone the role and change the privileges in the clone.
If you update the SV Plug-in version, or connect the vCenter to another SV vCenter Service, the role definitions will be overwritten!

1. In the **Menu** area of the vSphere Client, select the item **Administration**.
2. Select the sub-item **Access Control**.
3. Select the sub-item **Roles**.
4. Select the desired role and click the pencil icon to edit.
5. Select privileges for the role.
6. Click **OK**.

## 4.4.3 Starting iRMC functions with/without single sign-on

When starting the iRMC Web Interface, their iRMC LAN channel privilege will be adjusted to match the privilege level of the vCenter user.

The single sign-on functionality no longer works in iRMC S5. When calling the iRMC Web Interface from SV Plug-in, the user will be requested to log in to the iRMC Web Interface.

### 4.4.3.1 Requirements for single sign-on on iRMC

To perform the iRMC functions with single sign-on, the following requirements must be met:

- The iRMC credentials must be configured with an iRMC user account that has the **Administrator** / **OEM** LAN channel privilege (see "Configure iRMC credentials: 'IPMI configuration'" on page 59).
- The vCenter user must have the privileges defined in the FUJITSU PRIMERGY role definitions.

### 4.4.3.2 iRMC functions with single sign-on

#### Location button LED

If the iRMC credentials have been configured (see "Configure iRMC credentials: 'IPMI configuration'" on page 59), any vCenter user can toggle the location button LED on/off.

**Remote console (AVR)**

To start AVR directly with single sign-on, the vCenter user must have the privileges defined in the **FUJITSU PRIMERGY Plug-in Administrator** role (see "FUJITSU PRIMERGY vCenter role definitions" on page 66); however, AVR can be started by any user from within the iRMC Web Interface.

**iRMC Web Interface**

If the vCenter user has the privileges defined in the **FUJITSU PRIMERGY Plug-in Administrator** role (see "FUJITSU PRIMERGY vCenter role definitions" on page 66), they will be able to start iRMC with single sign-on.

In all other cases, iRMC can be started via login by the iRMC user.

#### 4.4.3.3 iRMC S4/S5 Web Interface SSO enhancements

The iRMC S4/S5 Web Interface can be started with one of three iRMC roles:

- Administrator
- Operator
- User

**iRMC extended privileges**

iRMC also offers four extended privileges which can be granted together with the roles:

- ConfigureBMC - perform system configuration on the host
- AVR - start AVR (Advanced Video Redirection)
- ConfigureUsers - configure user accounts (iRMC, CAS, LDAP)
- RemoteStorage - perform remote image and media operations

These extended privileges can be used together with the iRMC roles. All users can start AVR from within the iRMC Web Interface. Since the **ConfigureBMC** privileges allow extensive access to iRMC configuration functionality, it is recommended to use the predefined SV Plug-in **Super Operator** role (see "FUJITSU PRIMERGY vCenter role definitions" on page 66).

The **RemoteStorage** and **ConfigureUsers** privileges map to just one vCenter privilege:

- RemoteStorage : Host.Config.Storage
- ConfigureUsers : Host.Local.ManageUserGroups

They can therefore be easily added to an SV Plug-in **Operator** or **Monitor** role (see "Examples of using role definitions to limit iRMC functionality" on page 70).

### Correlation between the FUJITSU PRIMERGY SV Plug-in roles and iRMC S4/S5 Web Interface functionality

The following table shows the correlation between the FUJITSU PRIMERGY SV Plug-in role definitions and iRMC S4/S5 Web Interface functionality:

| Predefined FUJITSU PRIMERGY vCenter role definition | iRMC LAN channel privilege | iRMC Web Interface functionality |
|---|---|---|
| FUJITSU PRIMERGY Plug-in Administrator | Administrator | Can perform all functions of the iRMC Web Interface<br>• View settings and information<br>• Toggle location button LED on/off<br>• Perform system shutdown/reboot<br>• Remote image mount<br>• Configure media options<br>• Configure system settings<br>• RAID configuration<br>• Prime Collect<br>• AIS Connect<br>• System report<br>• BIOS backup and update<br>• iRMC reboot and update<br>• Internal event log view/clear<br>• Configure users<br>• Start AVR |
| FUJITSU PRIMERGY Plug-in Super Operator | Operator +<br>ConfigureBMC<br>RemoteStorage<br>AVR | • View settings and information<br>• Toggle location button LED on/off<br>• Perform system shutdown/reboot<br>• Remote image mount<br>• Configure media options<br>• Configure system settings<br>• Start AVR |

| Predefined FUJITSU PRIMERGY vCenter role definition | iRMC LAN channel privilege | iRMC Web Interface functionality |
|---|---|---|
| FUJITSU PRIMERGY Plug-in Operator | Operator +<br>RemoteStorage<br>AVR | • View settings and information<br>• Toggle location button LED on/off<br>• Perform system shutdown/reboot<br>• Remote image mount<br>• Configure media options<br>• Start AVR |
| FUJITSU PRIMERGY Plug-in Monitor | User +<br>AVR | • View limited set of settings and information<br>• Toggle location button LED on/off<br>• Start AVR |

### 4.4.4 Examples of using role definitions to limit iRMC functionality

In this example, a FUJITSU PRIMERGY SV Plug-in user **Monitor** is given limited access to the iRMC with single sign-on.

The administrator might wish to create a user with very limited privileges. The user should be able to start the iRMC Web Interface with the LAN channel privilege of **User**, but not make any changes on the system or perform a system shutdown.

1. A user is created (for example, **monitor**).
2. The target (vCenter, cluster or single host) is configured to have the permission:
   - user: **monitor**
   - role: **FUJITSU PRIMERGY Plug-in Monitor**

#### 4.4.4.1 vCenter user "monitor" and iRMC access without SSO (iRMC S4)

**Situation:**

- When the user logs in, they can start the iRMC Web Interface, but must log in using an iRMC user name and password.
- They will have the LAN channel privileges corresponding to that account.
- The iRMC credentials (see "Configure iRMC credentials: 'IPMI configuration'" on page 59) will not be used.

**vSphere Client:**

User without SSO privileges or no iRMC credentials configured (see "Configure iRMC credentials: 'IPMI configuration'" on page 59).

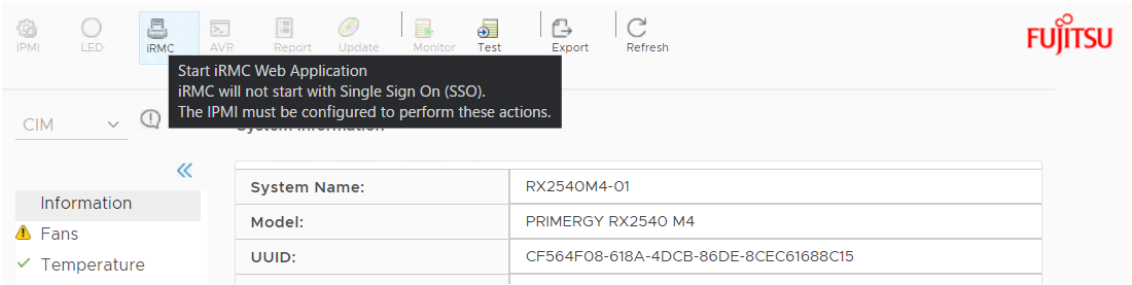


Figure 19: Example: vCenter user **monitor** and iRMC access without SSO - vSphere Client

**SV Plug-in:**

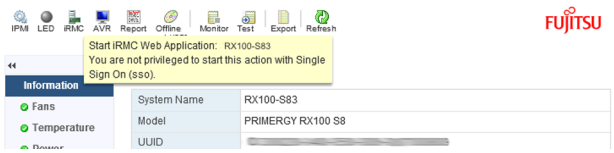


Figure 20: Example: vCenter user **monitor** and iRMC access without SSO - SV Plug-in

### 4.4.4.2 vCenter user "monitor" and iRMC access with SSO as iRMC user "User"

**Situation:**

The iRMC credentials must be configured with an iRMC user who has the LAN channel privilege of **Administrator** / **OEM**, e.g. **admin** / **admin** (see "Configure iRMC credentials: 'IPMI configuration'" on page 59 and "Starting iRMC functions with/without single sign-on" on page 67).

When the user logs in, they will be able to start the iRMC Web Interface with SSO but they only have the LAN channel privileges of user.

**vSphere Client:**

A vCenter user with the **FUJITSU PRIMERGY Plug-in Monitor** role; iRMC credentials are configured (**admin / admin**, see "Configure iRMC credentials: 'IPMI configuration'" on page 59).

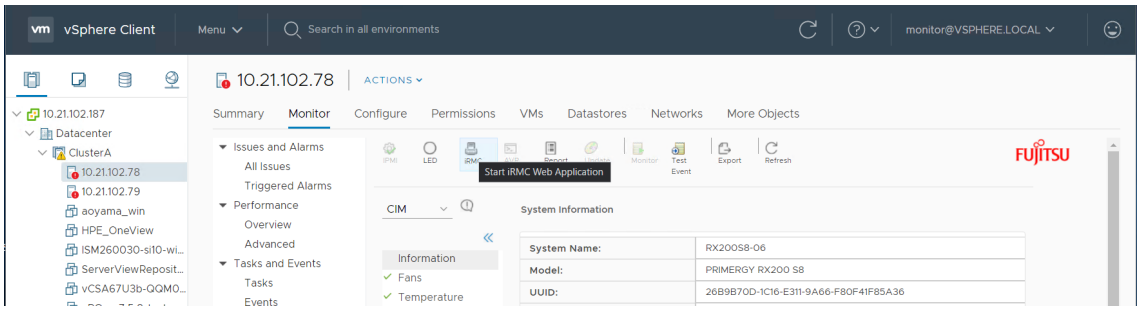


Figure 21: Example: vCenter user **monitor** and iRMC access with SSO as iRMC user **User** - vSphere Client

**SV Plug-in:**

The figure below shows the iRMC Web Interface with the user **admin** logged in but with the LAN channel privilege **User**. The user **admin** can only perform actions that are allowed for a user (e.g. **Toggle location button LED**) but cannot perform system shutdowns or configure the system in any way.

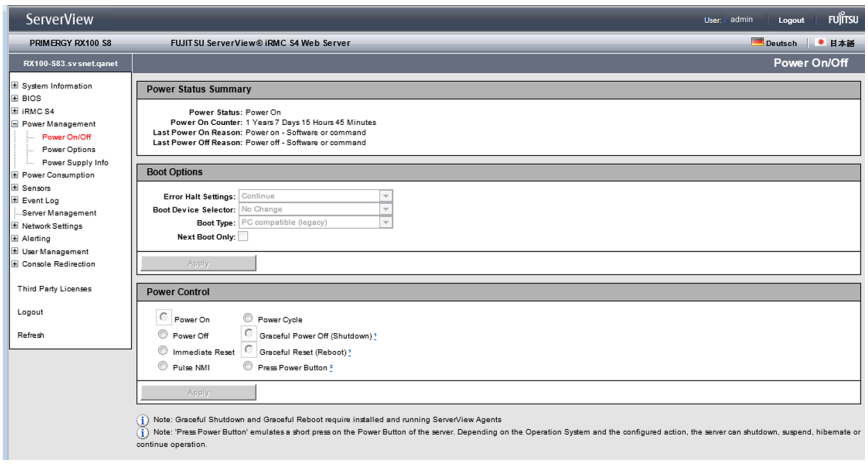


Figure 22: Example: vCenter user **monitor** and iRMC access with SSO as iRMC user **User** - SV Plug-in

### 4.4.4.3 vCenter user "monitor2" and iRMC "User" access and extended privilege "RemoteStorage"

**Situation:**

In this example, the vCenter administrator will create a user **monitor2**. This user should be able to start iRMC S4/S5 with SSO as the iRMC user **User**, but also be able to mount a remote image.

In this case it is necessary to grant the role more privileges than are predefined.

If you need to change the privileges in one of the FUJITSU PRIMERGY role definitions, clone the role and change the privileges in the clone. If you update the SV Plug-in version, or connect the vCenter to another SV vCenter Service, the role definitions will be overwritten!

The vCenter administrator must perform the following:

1. Configuring iRMC credentials with a user account that has the LAN channel privilege of **Administrator** or **OEM** (see "Configure iRMC credentials: 'IPMI configuration'" on page 59).
2. In the **Menu** area of the vSphere Client under **Administration** - **Access Control** - **Roles**:
   a. Choosing the **FUJITSU PRIMERGY Plug-in Monitor** role and cloning this role.
   b. Renaming this clone **PluginMonitorPlusStorage**.
   c. Adding the privilege **Host->Configuration->Storage Partition Configuration** to the **FUJITSU PRIMERGY Plug-in Monitor** role.
   d. Saving the **FUJITSU PRIMERGY Plug-in Monitor** role.
3. Creating a new vCenter user named **monitor2**.
4. Navigating to the vCenter or host for which the user is to have this functionality:
   a. Right-clicking the desired vCenter or host, and selecting **Add Permission** in the context menu.
   b. Selecting the user **monitor2** and assigning the role **PluginMonitorPlusStorage**.

**vSphere Client:**

Logged in as **monitor2**, the user can navigate to the SV Plug-in view for the host and start the iRMC Web Interface:

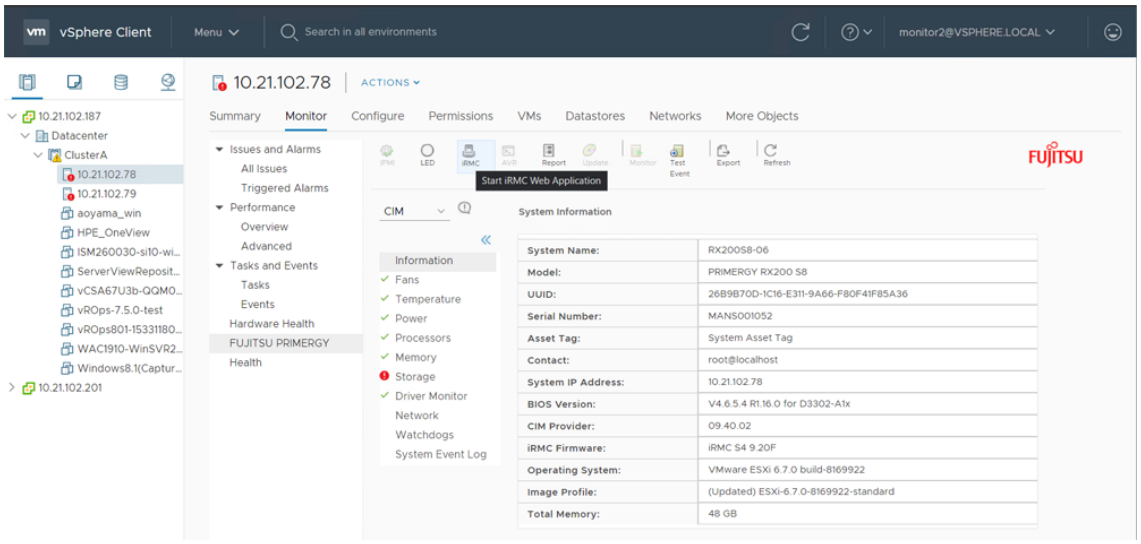


Figure 23: vCenter user **monitor2** and iRMC **User** access and extended privilege **RemoteStorage** - vSphere Client

### SV Plug-in:

The user is logged in as the iRMC administrator **admin**, but only with the LAN channel privilege of **User**. But they can also perform remote storage actions:

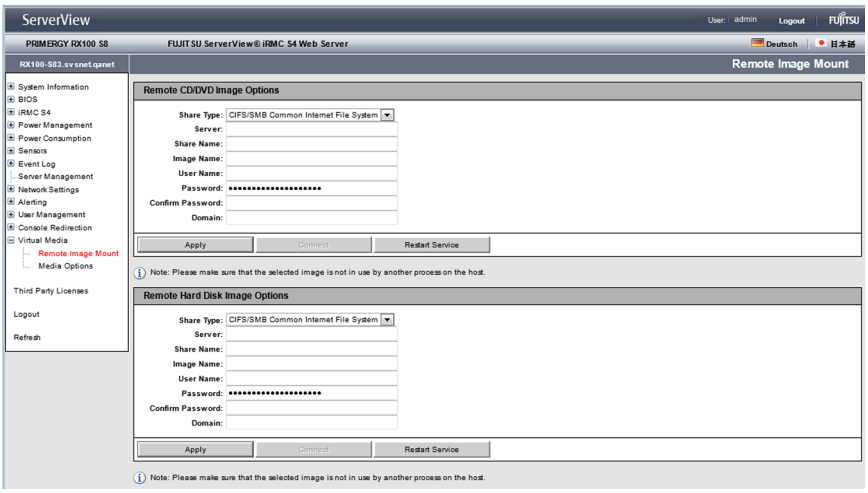


Figure 24: Example: vCenter user **monitor2** and iRMC **User** access and extended privilege **RemoteStorage** - SV Plug-in

# 5 SV Plug-in: Getting started and summary

The SV Plug-in home page **FUJITSU PRIMERGY** starts with a **Getting Started** view. The links under the navigator tree item **FUJITSU PRIMERGY** offer the views of the SV Plug-in home page. The **Summary** view gives an overview of the information items provided by the SV Plug-in. There is also a **Plug-in Definitions** view, which lists all FUJITSU PRIMERGY events and shows the FUJITSU PRIMERGY alarms and the role definitions that can be used to assign permissions to an entity (see "FUJITSU PRIMERGY vCenter role definitions and iRMC single sign-on" on page 65).

Via the **SV vCenter Service Configuration** link under **Administration**, you can configure the vCenter Service to work together with your vCenter Server.

## 5.1 Entry point

There are two options to open the home page of the SV Plug-in:

- Via the **Home** page of the vSphere Client.
- Via the **Shortcuts** page of the vSphere Client.

### 5.1.1 Open the home page of the SV Plug-in via the Home page of the vSphere Client

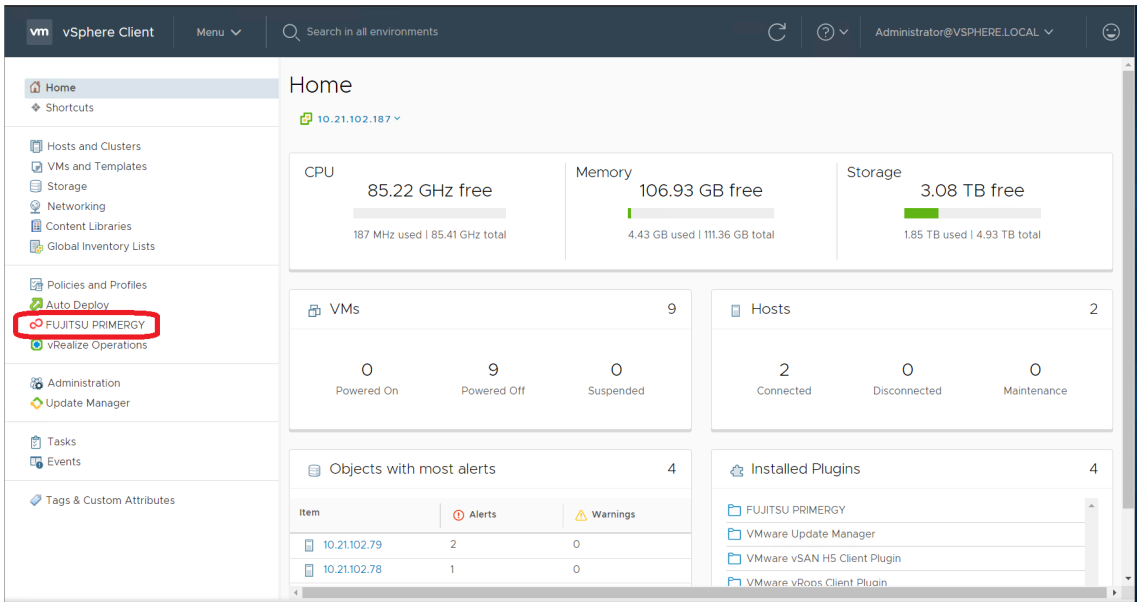


Figure 25: Link to the home page of the SV Plug-in in the **Home** page of the vSphere Client

The link leads to the **Getting Started** view on the home page of the SV Plug-in.

### 5.1.2 Open the home page of the SV Plug-in via the Shortcuts page of the vSphere Client

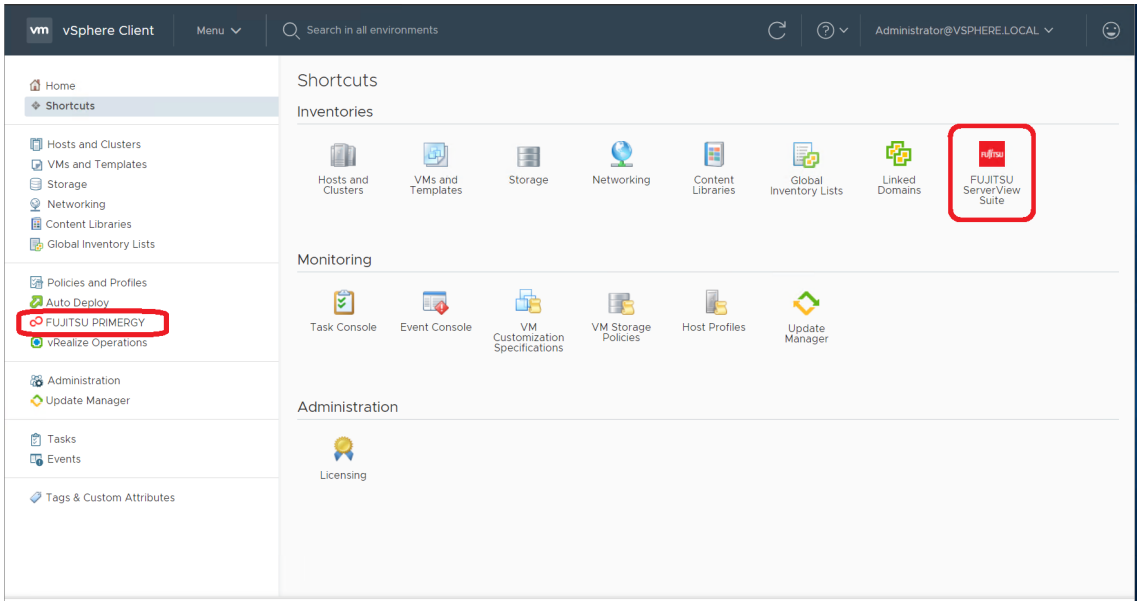


Figure 26: Link to the home page of the SV Plug-in in the **Home** page of the vSphere Client

Both links **FUJISTU PRIMERGY** and **FUJITSU ServerView Suite** lead to the **Getting Started** view on the home page of the SV Plug-in.

## 5.2 Views on the home page of the SV Plug-in

The home page of the SV Plug-in contains the following views:

**Getting Started**

The **Getting Started** view on the home page of the SV Plug-in gives general information about the SV Plug-in (see "Getting Started view" on page 78).

**Summary**

The **Summary** view on the home page gives an overview of the information items provided by the SV Plug-in (see "Summary view" on page 78).

**Plug-in Definitions**

The **Plug-in Definitions** view on the home page of the SV Plug-in offers several sub-tabs, among them **EVENT DEFINITIONS**, **ALARM DEFINITIONS** and **ROLE DEFINITIONS**.

The **EVENT DEFINITIONS** sub-tab of the **Plug-in Definitions** view on the home page of the SV Plug-in lists the event definitions that are set by the SV Plug-in (see "EVENT DEFINITIONS" on page 80).

The **ALARM DEFINITIONS** sub-tab of the **Plug-in Definitions** view on the home page of the SV Plug-in lists the predefined FUJITSU PRIMERGY alarms (see "ALARM DEFINITIONS" on page 81).

The **ROLE DEFINITIONS** sub-tab of the **Plug-in Definitions** view on the home page of the SV Plug-in lists the role definitions that can be used to assign permissions to an entity (see "ROLE DEFINITIONS" on page 81 and "FUJITSU PRIMERGY vCenter role definitions and iRMC single sign-on" on page 65).

**SV vCenter Service Configuration**

The **SV vCenter Service Configuration** view gives an overview of all SV vCenter Services that are available. You can also see the status of the hosts of the SV vCenter Services. Via **CONFIGURE** you can configure the Fujitsu ServerView vCenter Service to work together with your vCenter Server (see "SV vCenter Service Configuration" on page 82).

## 5.3 Getting Started view

1. In the **Menu** area of the vSphere Client, select the item **FUJITSU PRIMERGY**.

   The **Getting Started** view on the home page of the SV Plug-in opens.

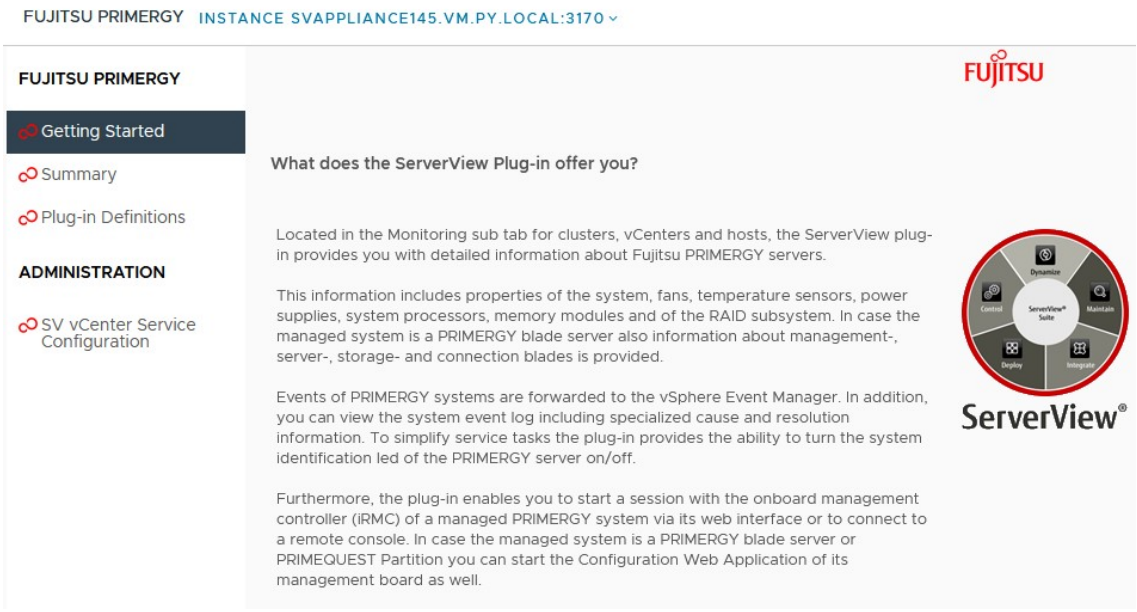


Figure 27: **Getting Started** view on the home page of the SV Plug-in

The **Getting Started** view on the home page of the SV Plug-in gives general information about the SV Plug-in.

## 5.4 Summary view

1. In the **Menu** area of the vSphere Client, select **FUJITSU PRIMERGY** - **Summary**.

   The **Summary** view on the home page of the SV Plug-in opens.

The **Summary** view on the home page of the SV Plug-in gives an overview of the information items provided by the SV Plug-in:

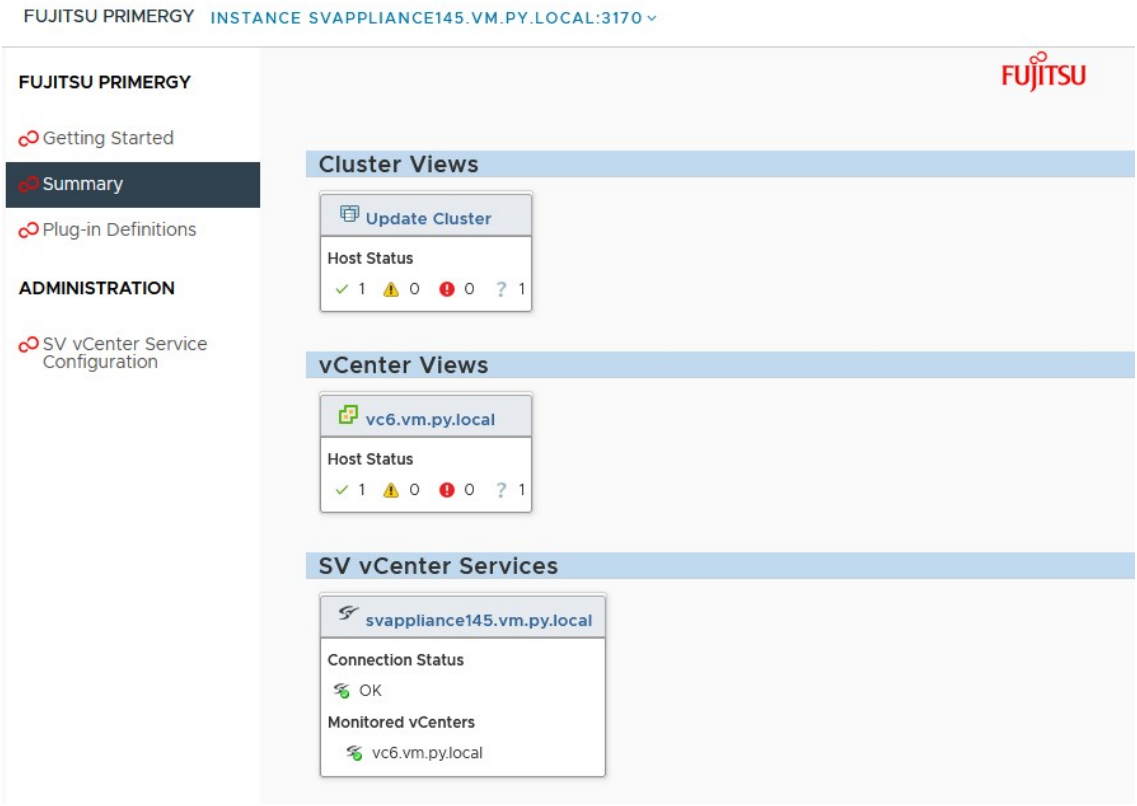


Figure 28: **Summary** view on the home page of the SV Plug-in

### Cluster Views

An overview of all clusters discovered by the SV vCenter Service. You can also see the status of the hosts of the clusters.

1. Click the title of an item box to open the view with detailed information about this cluster (see "Monitoring vCenter or cluster host servers" on page 100).

### vCenter Views

An overview of all vCenters discovered by the SV vCenter Service. You can also see the status of the hosts of the vCenters.

1. Click the title of an item box to open the view with detailed information about this vCenter (see "Monitoring vCenter or cluster host servers" on page 100).

### SV vCenter Services

An overview of all SV vCenter Services that are available. You can also see the status of the hosts of the SV vCenter Services.

1. Click the title of an item box to open the view with detailed information about this SV vCenter Service (see "Properties of SV vCenter Services" on page 109).

# 5.5 Plug-in Definitions view

1. In the **Menu** area of the vSphere Client, select **FUJITSU PRIMERGY** - **Plug-in Definitions**.

   The **Plug-in Definitions** view on the home page of the SV Plug-in opens.

The **Plug-in Definitions** view on the home page of the SV Plug-in offers several sub-tabs, among them **EVENT DEFINITIONS**, **ALARM DEFINITIONS**, and **ROLE DEFINITIONS**.

## 5.5.1 EVENT DEFINITIONS

The **EVENT DEFINITIONS** sub-tab of the **Plug-in Definitions** view on the home page of the SV Plug-in lists the event definitions that are set by the SV Plug-in. If you have more than one vCenter in your environment, you can choose which one you would like to view the definitions for under **Providers**.

If the hosts are monitored by the SV vCenter Service, these indications will be forwarded to the vCenter event management (see "Integration in the event management of the vSphere Client" on page 107).

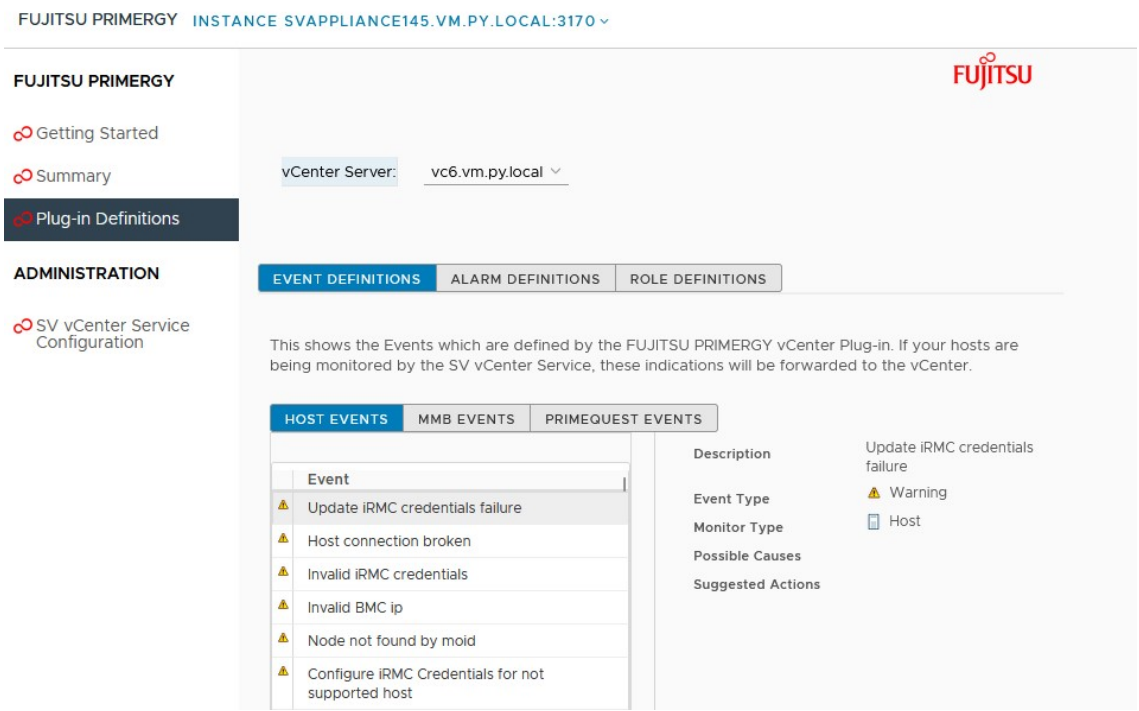


Figure 29: **EVENT DEFINITIONS** tab in the **Plug-in Definitions** view on the home page of the SV Plug-in

There is one sub-tab in this **EVENT DEFINITIONS** tab: **HOST EVENT**. The list in this tab has the columns **Event Type** and **Description** and can be sorted according to these items.

More information on the selected list entry is displayed on the right.

## 5.5.2 ALARM DEFINITIONS

The **ALARM DEFINITIONS** sub-tab of the **Plug-in Definitions** view on the home page of the SV Plug-in lists the predefined FUJITSU PRIMERGY alarms. If you have more than one vCenter in your environment, you can choose which one you would like to view the definitions for under **Providers**.

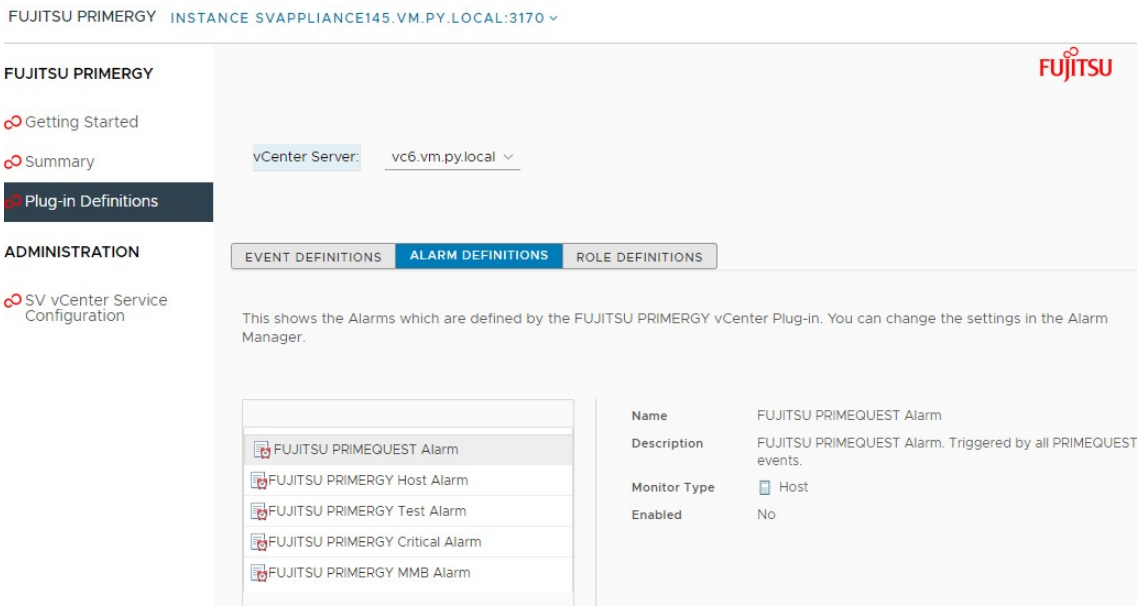


Figure 30: **ALARM DEFINITIONS** in the **Plug-in Definitions** view on the home page of the SV Plug-in

The new alarm definitions help you to define specific alarm actions depending on the target type (**Host**) of the event.

After a new or update installation of the SV Plug-in, any changes made to an alarm (e.g. actions) will be lost and you must reconfigure the action as needed.

There is also a test alarm which you can use to test the event/alarm handling in general. This will be triggered from a test event. All of these new definitions have no actions and are disabled. To use them you must enable them and possibly configure an action for each.

## 5.5.3 ROLE DEFINITIONS

The **ROLE DEFINITIONS** sub-tab of the **Plug-in Definitions** view on the home page of the SV Plug-in lists the predefined FUJITSU PRIMERGY roles. If you have more than one vCenter in your environment, you can choose which one you would like to view the definitions for under **Providers**.

This view shows the FUJITSU PRIMERGY vCenter role definitions that are generated during the installation process. They describe the minimum privilege level to perform SV Plug-in

actions and can be used to assign permissions to an entity. For more information see "FUJITSU PRIMERGY vCenter role definitions" on page 66.

For more information about the concept and about using these role definitions to limit iRMC functionality, see "FUJITSU PRIMERGY vCenter role definitions and iRMC single sign-on" on page 65.

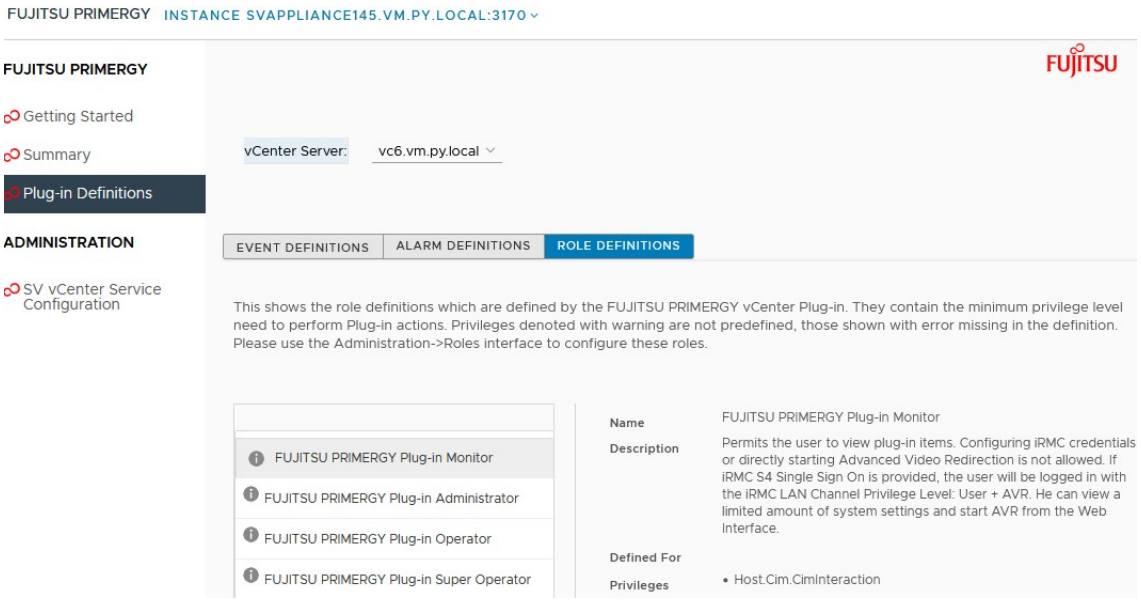


Figure 31: **ROLE DEFINITIONS** in the **Plug-in Definitions** view on the home page of the SV Plug-in

The **Defined For** field gives you the name of the vCenter (cluster, host) to which this role definition is assigned. You can also see the user to whom the role definition has been assigned.

If the role definitions have been reconfigured after installation, the changes relevant to correct processing of the SV Plug-in will be marked as follows:

*

This privilege was not predefined and has been added after installation. It is not required for correct processing of the SV Plug-in.

*** (in red)

This privilege is missing. It has been removed since installation and must be added again for correct processing of the SV Plug-in.

## 5.6 SV vCenter Service Configuration

The **SV vCenter Service Configuration** view gives an overview of all SV vCenter Services that are available. You can also see the status of the hosts of the SV vCenter Services.

1. In the **Menu** area of the vSphere Client, select **FUJITSU PRIMERGY** - **SV vCenter Service Configuration**.

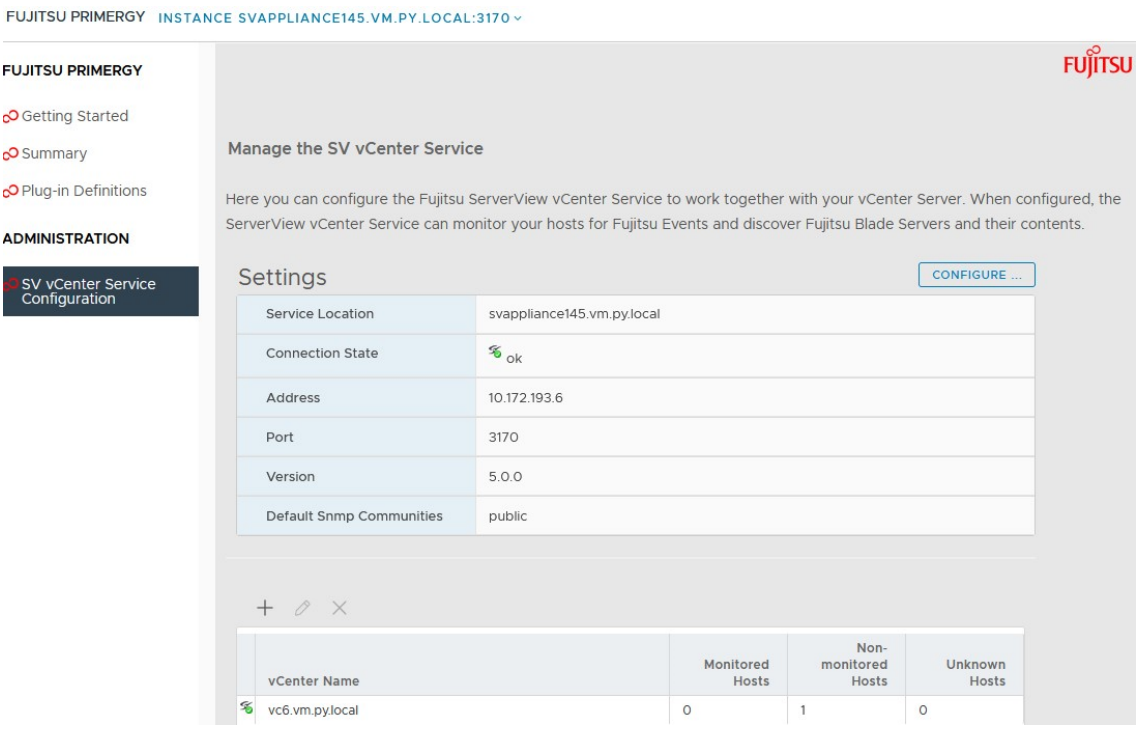


Figure 32: **SV vCenter Service Configuration** view on the home page of the SV Plug-in

The **SV vCenter Service Configuration** view on the home page of the SV Plug-in opens.

2. Click **CONFIGURE** to configure the Fujitsu ServerView vCenter Service to work together with your vCenter Server. When configured, the ServerView vCenter can monitor your hosts for Fujitsu Events and discover Fujitsu Blade Servers and their contents (see "SV vCenter Service configuration" on page 56).

# 6 Monitoring ESXi-based hosts

The SV Plug-in offers various options for monitoring ESXi-based hosts:

**Information on the selected host**

Status icons provide quick information, while detailed views provide more information - see "Information on the selected host - Status icons, items and views" on page 86.

For ESXi 7.x and older: In regular operation, the SV Plug-in generally shows the values of a host system provided by the ServerView ESXi CIM Provider.

For ESXi 7.x and older: You can also use the values of a host system provided by the Redfish interface of its iRMC for monitoring, provided the iRMC has a suitable firmware version. It is also possible to monitor most of the storage values via IPMI. Redfish and IPMI are only available if the iRMC credentials are configured (see "Configure iRMC credentials: 'IPMI configuration'" on page 59). If all protocols are available, you can toggle between CIM, Redfish and IPMI communication interfaces. Be aware that not all the values are available via IPMI.

For ESXi as of 8.0: You can ony use Redfish and IPMI.

**FUJITSU PRIMERGY Actions**

A number of action items support calling a monitoring tool or making settings on the host - see "FUJITSU PRIMERGY Actions (iRMC-based operations)" on page 91.

If a remote console (AVR) or the iRMC Web Interface is started, the SV Plug-in will consider the privileges of the current user - see "Starting iRMC functions with/without single sign-on" on page 67.

**Integration in event management of the vSphere Client**

The SV Plug-in includes the SV vCenter Service, which routes FUJITSU PRIMERGY-specific events to the vCenter event management to be monitored in the vSphere Client (see "Integration in the event management of the vSphere Client" on page 107).

## 6.1 Access to the SV Plug-in information of an ESXi-based host

1. In the **Menu** area of the vSphere Client, select **Hosts and Clusters**.
2. Select the desired host.
3. Click the **Monitor** tab.

   The **Monitor** tab is displayed, with a **Menu** area on the left.

   At the bottom of this menu area you will find the **FUJITSU PRIMERGY** menu item, which opens the views of the SV Plug-in.

   The **FUJITSU PRIMERGY** menu item is only available if two conditions are met:
   - The vendor of the selected host is Fujitsu.
   - The version of the ESXi operating system is at least V5.0.

4. Click the **FUJITSU PRIMERGY** menu item to display the interface of the SV Plug-in.

## 6.2 SV Plug-in information of an ESXi-based host

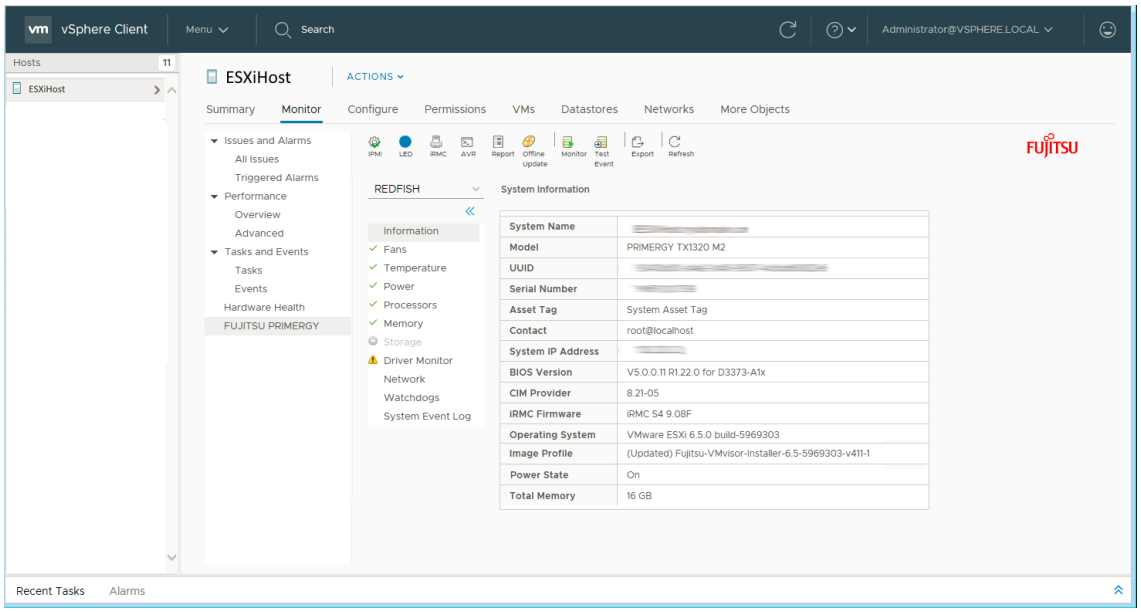


Figure 33: SV Plug-in information of an ESXi host (vSphere Client)

## 6.2.1 Information on the selected host - Status icons, items and views

Time of data acquisition: If the SV Plug-in is called, it will retrieve the data from the chosen protocol on the host. Whenever you click the status item tree, the SV Plug-in retrieves the data again. If you click the **Refresh** icon of vSphere, a new data retrieval cycle will be initiated.

For ESXi 7.x and older: In regular operation, the SV Plug-in generally shows the values of a host system provided by the ServerView ESXi CIM Provider.

For ESXi 7.x and older: You can also use the values of a host system provided by the Redfish interface of its iRMC for monitoring, provided the iRMC has a suitable firmware version. It is also possible to monitor most of the storage values via IPMI. Redfish and IPMI are only available if the iRMC credentials are configured (see "Configure iRMC credentials: 'IPMI configuration'" on page 59). If all protocols are available, you can toggle between CIM, Redfish and IPMI communication interfaces. Be aware that not all the values are available via IPMI.

For ESXi as of 8.0: You can ony use Redfish and IPMI.

In the main workspace, on the left of the SV Plug-in view, you will find a status item tree:

1. Clicking an item provides detailed information to the right of the status item tree.
   - You can collapse or expand the status item tree to allow more/less space for detailed information on the right.
   - The detailed information on the right is displayed in tables. You can change the column widths and sort the columns as needed.

### 6.2.1.1 Icons

**Status icons**

Each item is preceded by a status icon:

| | |
|---|---|
| | **ok** |
| | degraded |
| | error |

| | |
|---|---|
|  | not present<br>If you click this item, no information will be shown to the right of the status item tree. |
|  | unknown |
|  | retrieving data |

**IPMI Configuration Status icons**

The second column after the host names indicates the status of IPMI configuration:

| | |
|---|---|
|  | IPMI configured |
|  | IPMI not configured |

If the IPMI Configuration Status icons are active, you can click them to start the IPMI configuration dialog directly, see "Configure iRMC credentials: 'IPMI configuration'" on page 59.

### 6.2.1.2 Status items and views

It might be that a table is reduced to certain columns only. In this case, you can expand an item by clicking the arrow in front of it to get more information.

For some components the new value **CSS** (customer self-service) may be shown. These are components that can be replaced by the customer themselves in the case of an error.

**Information**

General information about the host:

System Name, Model, UUID, Serial Number, Asset Tag, Contact, System IP Address, BIOS Version, CIM Provider Version, iRMC Firmware Version, Operating System Version, Image Profile, Power State, Total Memory

**Fans**

Information about the fans installed in the system:

Status, Designation, Current Speed, Maximum Speed (SVCIMp< V6.31), Nominal Speed (SVCIMp< V6.31), Fail Reaction, Shutdown Delay, State, Quality (Current Speed / Nominal Speed) (SVCIMp >=V6.31), CSS (SVCIMp >=V6.31)

**Temperature**

Detailed information about the temperature sensors installed in the system:

Status, Designation, Temperature, Warning Level, Critical Level, Fail Reaction, State, CSS Component

**Power**

Information about the power supplies installed in the system:

Status, Designation, State, Product Name (SVCIMp >=V6.31), Total Capacity, CSS (SVCIMp >=V6.31)

**Processors**

Detailed information about the system processor configuration:

Status, Designation, Frequency (MHz), Manufacturer, Type, L1 Cache, L2 Cache, L3 Cache, Enabled Cores, Cores, Logical Threads, State, CSS (SVCIMp >=V6.31)

**Memory**

Detailed information about the memory modules installed in the system:

Status, Designation, Type, Size (MB), Frequency (MHz), State, Maximum Frequency (SVCIMp >=V6.31), Voltage (SVCIMp >=V6.31), CSS (SVCIMp >=V6.31), Manufacturer (SVCIMp >=V6.31), Serial Number (SVCIMp >=V6.31)

**Storage**

Overview of the RAID controllers found and details of their logical drives and physical disks (see "Storage view" on page 94).

**Driver Monitor**

Overview of the components of a host as well as of the associated events contained in the OS event log on the managed server (see "Driver Monitor view" on page 97).

**Network**

Information about the network interfaces configured on the system:

Name, Address Type (primary or iRMC), IP Address, MAC Address

If a component is not accessible, there is no status information available for it.

**Watchdogs**

Information about the watchdogs configured on the system:

Type, Active, Action, Timeout

If a component is not accessible, there is no status information available for it.

**System Event Log**

A list of the entries found in the System Event Log together with cause/resolution information.

The ServerView ESXi CIM Provider supports the System Event Log view. The entries will be retrieved automatically via CIM.

## 6.2.2 Monitoring via Redfish and agentless management via IPMI

In addition, SV Plug-in also supports the Redfish DMTF standard, provided the iRMC has a supporting firmware version (see "Overview of requirements and ports" on page 17). You can toggle to Redfish. In this case the monitoring data is provided by the iRMC.

It is also possible to monitor most of the storage values via IPMI, although not all the values are available in this way. Via IPMI the iRMC also provides the monitoring data.

Redfish and IPMI are only available if the IPMI/Redfish credentials are configured (see "Monitoring via Redfish and agentless management via IPMI" on page 90).

In particular the following views change:

**Driver Monitor** view

The **Driver Monitor** view is not available via IPMI.

Not all the values are available via Redfish.

**Storage** view

Via IPMI the **Storage** view offers a list of the physical disks and their status.

Not all the values are available via IPMI.

### Toggle between CIM, Redfish and IPMI

In the main workspace, on the left of the SV Plug-in view, you will find the status item tree (see "Information on the selected host - Status icons, items and views" on page 86).

On the left, above the status item tree, one item of an selection list is displayed:

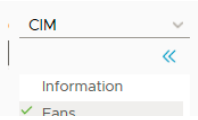


Figure 34: Toggle between CIM, Redfish and IPMI (vSphere Client)

You can toggle between CIM, Redfish and IPMI:

1. Click the icon to change the communication interface.

### 6.2.3 FUJITSU PRIMERGY Actions (iRMC-based operations)

The SV Plug-in offers some FUJITSU PRIMERGY Actions, depending on the capabilities of the selected host.

The iRMC credentials (user name and password, see "Configure iRMC credentials: 'IPMI configuration'" on page 59) must be configured to have access to a number of iRMC-based actions on an ESXi host:

- Toggle Identify LED
- Start the iRMC Web Interface with single sign-on
- Start the Remote Console (AVR)
- Start a System Report
- Start an export of data

In addition, when the credentials are configured, it is possible to view monitoring data from the system over IPMI, which can be useful if problems with the CIM Provider arise.

These IPMI-based actions are always enabled in the context menu, even if the credentials are not configured or the user does not have the privilege to perform the action. In this case an error message will be shown if the action is started.

For how to configure the user name and password for iRMC, see "Configure iRMC credentials: 'IPMI configuration'" on page 59.

#### 6.2.3.1 Starting a FUJITSU PRIMERGY Action

There are two ways to start one of these FUJITSU PRIMERGY Actions:

- In the top left of the SV Plug-in interface in the main workspace, up to ten icons are displayed.
- The FUJITSU PRIMERGY Actions can be started independently of the SV Plug-in interface:

  In the center panel of the vSphere Client, select the desired host in the inventory tree.

### 6.2.3.2 The FUJITSU PRIMERGY Actions


**Refresh**

1. Click this icon to refresh the current view of the SV Plug-in.

This **Refresh** function only refreshes the views/information of the SV Plug-in - not of the vSphere Client.
Consequently, this function is only available among the icons in the top left of the SV Plug-in interface - not in the **Actions** menu.


**Configure IPMI ...**

1. Click this icon to start the iRMC credentials configuration dialog (see "Configure iRMC credentials: 'IPMI configuration'" on page 59).


**Toggle Identify LED**

1. Click this icon to toggle the Locate LED on and off:

Locate icon is blue: locate LED is on.

Locate icon is gray: locate LED is off.

The icon is displayed if an iRMC address is available.


**Start iRMC**

1. Click this icon to launch the iRMC Web Interface in a new window.

The icon is displayed if an iRMC address is available.

See "Starting iRMC functions with/without single sign-on" on page 67.


**Start Remote Console**

1. Click this icon to launch a remote console (AVR) in a new window.

The icon is displayed if an iRMC address is available.

See "Starting iRMC functions with/without single sign-on" on page 67.


**Start a System Report**

1. Click this icon to start an iRMC system report in a new window.

See "iRMC system report" on page 116.


**Toggle FUJITSU Event Monitoring**

1. Click this icon to turn the subscription of the host to the SV vCenter Service on/off (see "Integration in the event management of the vSphere Client" on page 107).

   This action is depicted in four ways, depending on the current subscription status:


The host is subscribed to the SV vCenter Service. Events will be monitored by the SV vCenter Service and forwarded.


The host is not subscribed to the SV vCenter Service. No events will be monitored by the SV vCenter Service or forwarded.


The subscription status of the host is unknown due to connection problems with the SV vCenter Service. No action will be performed.


The host cannot be subscribed, because the vCenter is not connected to the SV vCenter Service. No action will be performed.


**Invoke Test Event**

1. Click this icon to request the host to send a test event (see "Integration in the event management of the vSphere Client" on page 107).


**Export Data** ...

1. Click this icon to open a frame where you can choose data to be exported:

   **Host information**
   Via CIM or Redfish.

   

   If the action item is started from the **Actions** menu (see "Starting a FUJITSU PRIMERGY Action" on page 91), the availability of the interfaces cannot be checked. Both choices are displayed, regardless of their availability.

   **Update information**
   Via Update Services and IPMI.

   **System Event Log** information
   Entries from the System Event Log.

   

   System Event Log information is not available via Redfish.

   

   If you choose all System Event Log entries, the retrieval of data will take some time. There is a **Cancel** button for leaving this frame without action. As long as the export process is running, it cannot be stopped and the buttons are locked.

When the requested data has been retrieved, a new window opens showing the data, with the option to save it to a file. When the files are saved, the default file name includes the communication interface (CIM or Redfish) that was chosen.

The icon is displayed if an iRMC address is available.

## 6.3 Storage view

The **Storage** view offers an overview of the RAID controllers found on the host and details of their logical drives and physical disks.

For ESXi 7.x and older: In regular operation, the SV Plug-in generally shows the values of a host system provided by the ServerView ESXi CIM Provider.

For ESXi 7.x and older: You can also use the values of a host system provided by the Redfish interface of its iRMC for monitoring, provided the iRMC has a suitable firmware version. It is also possible to monitor most of the storage values via IPMI. Redfish and IPMI are only available if the iRMC credentials are configured (see "Configure iRMC credentials: 'IPMI configuration'" on page 59). If all protocols are available, you can toggle between CIM, Redfish and IPMI communication interfaces. Be aware that not all the values are available via IPMI.

For ESXi as of 8.0: You can ony use Redfish and IPMI.

Via IPMI the **Storage** view offers a list of the physical disks and their status.

## 6.3.1 Prerequisites - information provider for the Storage view

To ensure the optimum supply of RAID information, it is recommended to install on the host:

- ServerView RAID Core Provider

The information shown in the **Storage** view is provided by **ServerView ESXi CIM Provider**, Redfish, or IPMI and you will see a icon above the Storage Details list on the right.

1. Click the icon above the **Storage Details** list on the right to gather information from the **Device Control Tree**.

You can save the gathered information to a JSON file.

## 6.3.2 Information on the Storage view

**Storage Details**

Overview of the RAID controllers found. This information includes:

Status of the controller shown as an icon, name of the controller, SAS ports to which the controller is connected, number of physical disks attached to the controller, number of logical drives configured on the controller, status of the BBU if available, textual status of the controller.

The entry for a controller can be expanded to view details about the controller as well as its logical drives and physical disks:

1. Click the arrow in front of a controller entry to get more detailed information.

An expanded controller entry is displayed. There are three tabs; the **Controller** tab is open:

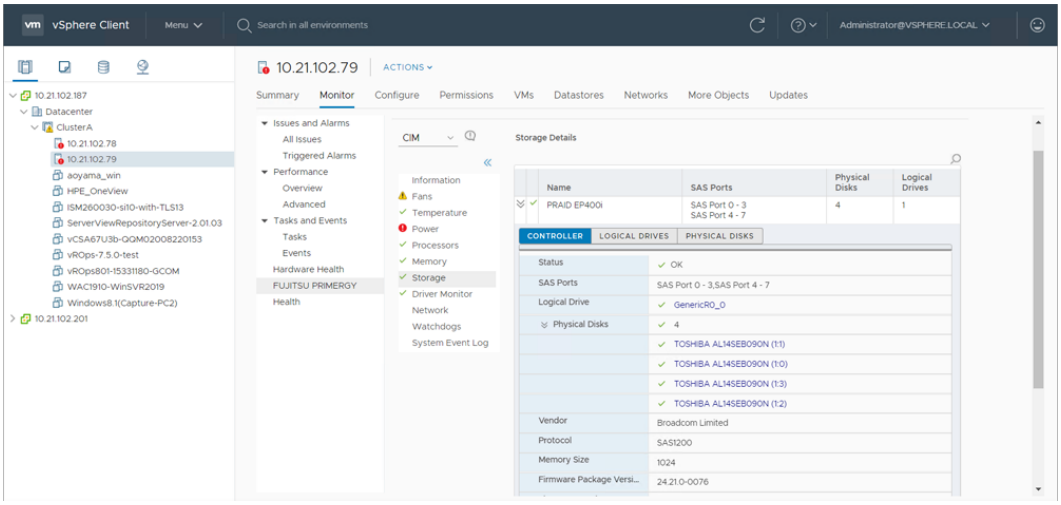


Figure 35: Storage view of the SV Plug-in - expanded controller entry, Controller tab

### Storage Details - Controller tab

Information shown here includes:

Vendor, protocol, memory size, firmware package version, firmware version, BIOS version, driver version, patrol read iterations, vendor/device ID, subvendor/device ID, PCI bus/device/function numbers, number and status of the logical drives (can be expanded), number and status of the physical drives (can be expanded).

### Logical Drives tab

1. Click the **Logical Drives** tab in an expanded controller entry view (**Storage Details** view).

An overview of the logical drives of the selected controller is displayed.

The information shown includes:

Status of the drive depicted as an icon, name of the drive, RAID level of the drive, logical size of the drive in MB, number of physical disks configured to this drive, textual status of the drive.

### Logical Drives - details

1. Click the arrow ▸ in front of a logical drive entry to get more detailed information.

The information shown includes:

Stripe size in KB, read mode, write mode, disk cache mode, number and status of the configured physical disks (can be expanded).

### Physical Disks - overview

1. Click the **Physical Disks** tab in an expanded controller entry view (**Storage Details** view).

An overview of the physical disks of the selected controller is displayed.

The information shown includes:

Vendor, model, serial number, firmware version, SAS address, link speed (GB/s), number and status of the logical drives that have configured this disk (can be expanded if more than one logical drive uses this disk).

## 6.4 Driver Monitor view

Not all the values are available via Redfish.

The **Driver Monitor** view is not available via IPMI.

Via the **Driver Monitor** view you can monitor and manage events relating to the components of a monitored host, as listed in the OS event log on the monitored host.

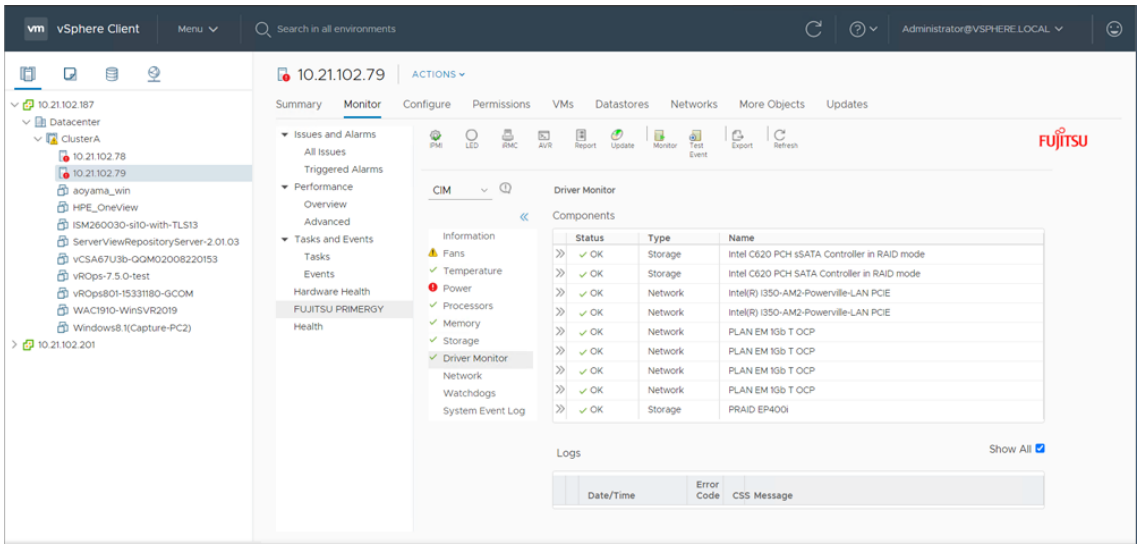


Figure 36: Driver Monitor view of the SV Plug-in

### Requirements

- ServerView ESXi CIM Provider V7.31.06 or later must be installed on the ESXi-based host.
- The ESXi-based host must be subscribed.

### Managing the events

In regular operation the **Driver Monitor** view shows the events of a selected component.

Expand the information.

You can display further information about a component, such as slot, driver or PCI information.

1. Click the arrow in front of a component entry to get more detailed information.

**Show all**

You can display all Driver Monitor events relating to the components of a monitored host, as listed in the OS event log on the monitored host.

1. Click the check-box **Show all** on the right, in the line of the table heading **Logs**.

**Acknowledge**

If a component has the status **Warning** or **Error**, you can confirm this event on the server side and set the status of this component to **ok**.

If a component has the status **Warning** or **Error**, the system status and error lamp also indicates **Warning** or **Error**. If you click the **Acknowledge** button , the system status and error lamp are also turned off.

Confirming all events:

If no component is selected, all events relating to the host will be acknowledged.

Confirming the events relating to an individual component:

Confirming the events relating to an individual component is not possible via Redfish. Via Redfish all events relating to the host will be acknowledged.

If a component is selected, all events relating to this component will be acknowledged.

1. Click the **Acknowledge** button on the right, in the line of the table heading **Components**.

# 6.5 System Event Log view

### Requirements

If an iRMC address is available, the ServerView ESXi CIM Provider later supports the System Event Log view. The entries will be retrieved via CIM.

### System Event Log view of the SV Plug-in

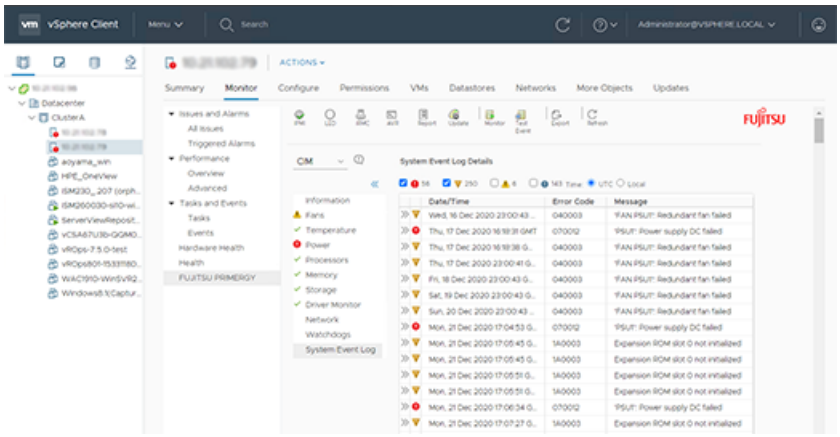


Figure 37: System Event Log view of the SV Plug-in

### Choosing the quantity and severity of entries shown

A host can have many log entries. Therefore the **System Event Log** view starts with only the **Critical** and Major entries showing.

1. If you wish to see entries of other severities, check/uncheck the boxes at the top of the **System Event Log Details** list:

**Displayed information**

The following information is displayed for each entry:

1. Click the arrow to get more detailed data.

These details can contain different information, such as about the cause of the event or helpful information to solve the problem.

Not all messages have these details.

The severity of the entry is indicated by an icon.

| | |
|---|---|
| **Date/Time** | Date and time either in UTC or local time, depending on the settings seen above the table.<br>1. Change these settings as required. |
| **Error Code** | Defines the type of the entry. |
| **CSS** | Shows whether this entry relates to a CSS (customer self-service) component. |
| (Message) | Details of the message. |

**Column sorting**

The **System Event Log** table allows you to sort by multiple columns.

1. Click a column header to sort.

Use [Ctrl] and click a second column to sort the table by both columns. The first column  cannot be sorted.

## 6.6 Monitoring vCenter or cluster host servers

The SV Plug-in offers lists of the hosts assigned to a vCenter or cluster.

Via this access point the SV Plug-in offers less information on the single host than via the inventory tree item **Hosts** (see "Monitoring ESXi-based hosts" on page 84), but all FUJITSU PRIMERGY Actions are available.

### 6.6.1 Access to the SV Plug-in information of the hosts of a vCenter/cluster

The SV Plug-in information about the hosts of a vCenter or cluster is also displayed if you click the title of an item box of a vCenter/cluster in the **Summary** tab on the home page of the SV Plug-in (see "Summary view" on page 78).

1. In the **Menu** area of the vSphere Client, select **Hosts and Clusters**.
2. Select the desired vCenter or cluster.
3. Click the **Monitor** tab.

   The **Monitor** tab is displayed, with a **Menu** area on the left.

   At the bottom of this menu area you will find the **FUJITSU PRIMERGY** menu item, which opens the views of the SV Plug-in.

   The **FUJITSU PRIMERGY** menu item is only available if two conditions are met:
   - The vendor of the selected host is Fujitsu.
   - The version of the ESXi operating system is at least V5.0.

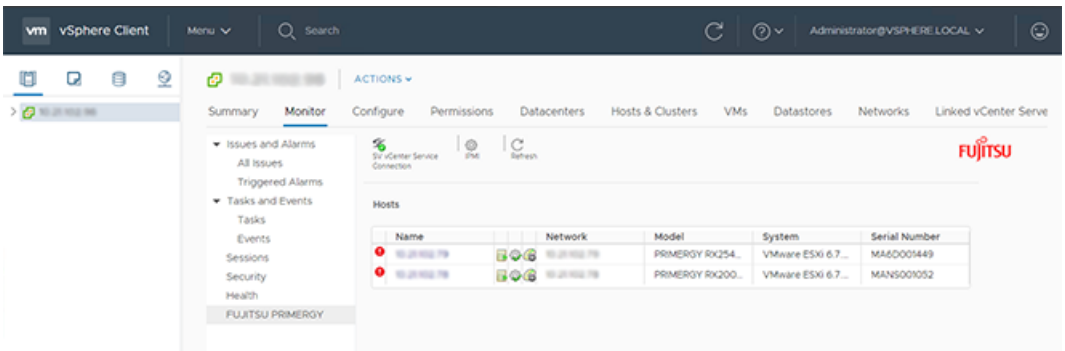


Figure 38: Access to the SV Plug-in information of vCenter servers

4. Click the **FUJITSU PRIMERGY** menu item to display the interface of the SV Plug-in.

   A list of the hosts found in the vCenter/cluster is shown.

**The list gives general information about each host of the vCenter/cluster:**

Status, host name (with a link to the Single System View for the host, if the host is available), SV vCenter Service monitoring status (subscribed/ not subscribed), IPMI Configuration Status, Update Status, network address, model, operating system, serial number

#### 6.6.1.1 Icons

**Status icons**

Each host name is preceded by a status icon:


**ok**


degraded


error


not connected

The host is no longer connected to the vCenter. The current status, monitoring and update status are not available.


not present

If you click this item, no information will be shown to the right of the status item tree.


unknown


retrieving data

**SV vCenter Service Monitoring Status icons**

The first column after the host names indicates the status of the monitoring by the SV vCenter Service:


subscribed


not subscribed

The SV vCenter Service Monitoring Status icons are active: You can click them to toggle the monitoring for events on/off.

**IPMI Configuration Status icons**

The second column after the host names indicates the status of IPMI configuration:


IPMI configured


IPMI not configured

If the IPMI Configuration Status icons are active, you can click them to start the IPMI configuration dialog directly, see "Configure iRMC credentials: 'IPMI configuration'" on page 59.

## 6.6.2 FUJITSU PRIMERGY Actions

### Action icons

The SV Plug-in offers some FUJITSU PRIMERGY Actions, depending on the capabilities of the selected host.

In the main workspace of the SV Plug-in interface, you will see the action icons in the top left.

Time of data acquisition: If the SV Plug-in is called, it will retrieve the data from the chosen protocol on the host. Whenever you click the status item tree, the SV Plug-in retrieves the data again. If you click the **Refresh** icon of vSphere  , a new data retrieval cycle will be initiated.


Refresh

1. Click this icon to refresh the current view of the SV Plug-in.

This **Refresh** function only refreshes the views/information of the SV Plug-in - not of the vSphere Client. Therefore, this function is only available among the icons in the top left of the SV Plug-in interface - not in the **Actions** menu.


SVvCenterService Connection

1. Click this icon to start a connection dialog similar to the dialog in the **SV vCenter Service Configuration Overview** (see "SV vCenter Service configuration" on page 56).

If the vCenter is already connected to an SV vCenter Service, you can update the connection or disconnect the vCenter from the SV vCenter Service.

If the vCenter is not connected to an SV vCenter Service, you can connect it to a selected SV vCenter Service.


Actions

This icon will be displayed if a host is selected in the **Monitor** tab view.

1. Click this icon to open the actions context menu (see "Actions in the context menu" on page 104).

### Actions in the context menu

(For how to open this context menu, see "Action icons " on page 103)


**Configure IPMI ...**

1. Click this icon to start the iRMC credentials configuration dialog (see "Configure iRMC credentials: 'IPMI configuration'" on page 59).


**Toggle Identify LED**

1. Click this icon to toggle the Locate LED on and off:

Locate icon is blue: locate LED is on.

Locate icon is gray: locate LED is off.

The icon is displayed if an iRMC address is available.


**Start iRMC**

1. Click this icon to launch the iRMC Web Interface in a new window.

The icon is displayed if an iRMC address is available.

See "Starting iRMC functions with/without single sign-on" on page 67.


**Start Remote Console**

1. Click this icon to launch a remote console (AVR) in a new window.

The icon is displayed if an iRMC address is available.

See "Starting iRMC functions with/without single sign-on" on page 67.


**Start a System Report**

1. Click this icon to start an iRMC system report in a new window.

See "iRMC system report" on page 116.


**Toggle FUJITSU Event Monitoring**

1. Click this icon to turn the subscription of the host to the SV vCenter Service on/off (see "Integration in the event management of the vSphere Client" on page 107).

   This action is depicted in four ways, depending on the current subscription status:

The host is subscribed to the SV vCenter Service. Events will be monitored by the SV vCenter Service and forwarded.

The host is not subscribed to the SV vCenter Service. No events will be monitored by the SV vCenter Service or forwarded.

The subcription status of the host is unknown due to connection problems with the SV vCenter Service. No action will be performed.

The host cannot be subscribed, because the vCenter is not connected to the SV vCenter Service. No action will be performed.


**Invoke Test Event**

1. Click this icon to request the host to send a test event (see "Integration in the event management of the vSphere Client" on page 107).


**Export Data** ...

1. Click this icon to open a frame where you can choose data to be exported:

   **Host information**
   Via CIM or Redfish.

   If the action item is started from the **Actions** menu (see "FUJITSU PRIMERGY Actions" on page 103), the availability of the interfaces cannot be checked. Both choices are displayed, regardless of their availability.

   **Update information**
   Via Update Services and IPMI.

   **System Event Log** information
   Entries from the System Event Log.

   System Event Log information is not available via Redfish.

   If you choose all System Event Log entries, the retrieval of data will take some time. There is a **Cancel** button for leaving this frame without action. As long as the export process is running, it cannot be stopped and the buttons are locked.

When the requested data has been retrieved, a new window opens showing the data, with the option to save it to a file. When the files are saved, the default file name includes the communication interface (CIM or Redfish) that was chosen.

The icon is displayed if an iRMC address is available.

### Opening the Single System View for a host of a vCenter/cluster

The Single System View will be opened if an iRMC address is available.

1. Click the host name of the desired host in the list (see "Access to the SV Plug-in information of the hosts of a vCenter/cluster" on page 101). The Single System View of the desired host is opened.

# 7 Integration in the event management of the vSphere Client

The SV Plug-in includes an SV vCenter Service which routes Fujitsu PRIMERGY-specific events to the vCenter event management to be monitored in the vSphere Client.

In certain situations, some further settings can help you enhance the performance of the SV vCenter Service for events (see "Further helpful service properties for the SV vCenter Service for events" on page 110).

So the Fujitsu PRIMERGY-specific event is shown in the regular **Events** page of the vSphere Client:

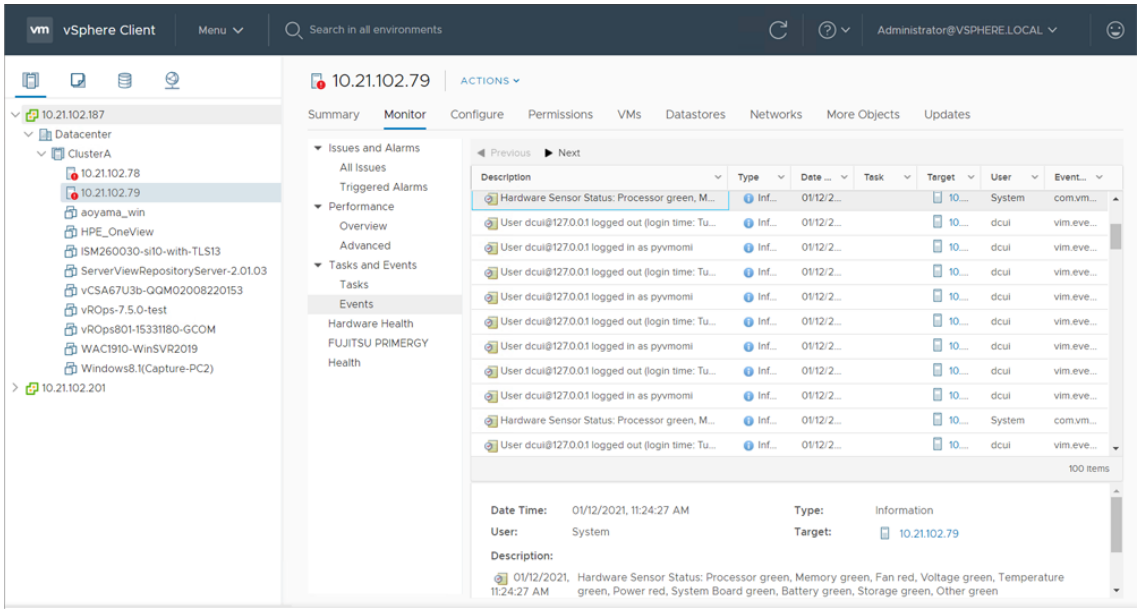


Figure 39: Fujitsu PRIMERGY-specific events in the Events page of the vSphere Client

## 7.1 Requirements for integration in the event management of the vSphere Client

These requirements are only valid for ESXi based hosts with CIM.

vSphere Client

- CIM and SNMP

  ESXi-based host

  ServerView ESXi CIM Provider must be installed on the ESXi-based host whose events are to be displayed in the vSphere Client interface.

- SV vCenter Service must be connected to the vCenter to which the host is assigned (see "SV vCenter Service configuration" on page 56).
- SV vCenter Service must be subscribed to this host (see "Monitoring vCenter or cluster host servers" on page 100). You can find an overview of the hosts subscribed to an SV vCenter Service in the **SV vCenter Configuration Overview** (see "SV vCenter Service Configuration Overview" on page 108).

## 7.2 SV vCenter Service Configuration Overview

You can use this view to manage all the SV vCenter Services installed in your environment.

### 7.2.1 Opening the SV vCenter Configuration Overview

1. In the **Menu** area of the vSphere Client, select the item **Administration**.
2. Select the sub-item **FUJITSU PRIMERGY**.
3. Select the sub-item **SV vCenter Service Configuration**.

In the main workspace of the vSphere Client, the **SV vCenter Service Configuration Overview** opens:

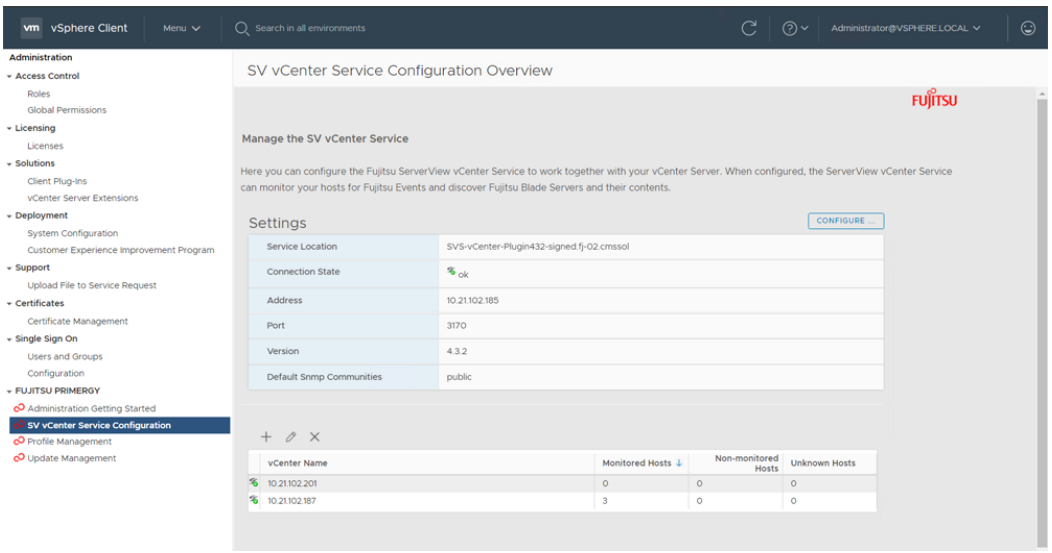


Figure 40: SV vCenter Service Configuration Overview

## 7.2.2 Properties of SV vCenter Services

1. Select an SV vCenter Service in the Service Location selection box.

   The current properties of the selected SV vCenter Service are displayed:

| | |
|---|---|
| **Service Location** | Specifies the FQDN of the virtual machine running the selected SV vCenter Service. |
| **Connection State** | Current status and connection between the vSphere Client and the SV vCenter Service |
| **Address** | Address used for the connection |
| **Port** | Port used for the connection |
| **Version** | Version of the SV vCenter Service |

### 7.2.3 Further helpful service properties for the SV vCenter Service for events

In certain situations, some further settings can help you enhance the performance of the SV vCenter Service for events.

You can set these properties in the **service.properties** file of the service. The file is located on the same system as the service:

**/opt/fujitsu/ServerViewSuite/webserver/conf/svvcenterservice/service.properties**

#### Further service properties

**`trap.forward.limit=30`**

Time limit for event forwarding.

Default value: **30** seconds. Only numeric values.

Note: Sometimes events are sent with high frequency. In this case the same event is sent repeatedly by the same host and generates a significant number of entries in the event management of vSphere Client. The same event sent by the same host during this time limit will not be forwarded to the vCenter event management.

**`cim.client.timeout=3000`**

Timeout value for CIM connections.

Default value: **3000** milliseconds. Only numeric values.

Note: Low connectivity in the network or older versions of CIM providers cause connection timeouts. If you increase this value, there will be fewer connection timeouts but the processing will take longer!

**`snmp.client.timeout=3000`**

Timeout value for SNMP connections.

Default value: **3000** milliseconds. Only numeric values.

Note: Low connectivity in the network or older versions of SNMP agents cause connection timeouts. If you increase this value, there will be fewer connection timeouts but the processing will take longer!

**`cim.health.info.enabled=true`**

Enables/Disables the protocol for health collection.

Default value: **true**. Only string value.

Note: If set to **false**, the protocol will not be used when gathering health information.

**redfish.health.info.enabled=true**

Enables/Disables the protocol for health collection.

Default value: **true**. Only string value.

Note: If set to **false**, the protocol will not be used when gathering health information.

**ipmi.health.info.enabled=false**

Enables/Disables the protocol for health collection.

Default value: **false**. Only string value.

Note: If set to **false**, the protocol will not be used when gathering health information.

**cim.health.info.priority=3**

Priority of the order for health collection.

Default value: **3**. Only numeric values.

Note: Each protocol has its own default priority. The order of protocols tried while gathering health information for a node can be customized.

**redfish.health.info.priority=2**

Priority of the order for health collection.

Default value: **2**. Only numeric values.

Note: Each protocol has its own default priority. The order of protocols tried while gathering health information for a node can be customized.

**ipmi.health.info.priority=1**

Priority of the order for health collection.

Default value: **1**. Only numeric values.

Note: Each protocol has its own default priority. The order of protocols tried while gathering health information for a node can be customized.

**health.info.refresh=60**

Intervals of health collection.

Default value: **60** seconds. Only numeric values.

Note: Health gathering time intervals can be customized.

**`proactive.retries.before.posting=1`**

Retry numbers before posting status.

Default value: **1**. Only numeric values.

Note: The retry mechanism checks update status before posting it. If the update status is not green the process should be repeated. Importantly, the process is repeated not only when the health status update is unknown, but also when health information was successfully collected. Repeating the process prevents sending an invalid process status when the status information is out of order due to breaking the protocols. As default, each health status update can be repeated one time, which means that health status update will be posted on second try.

### 7.2.4 Adding/removing a vCenter to/from the SV vCenter Service

For further information on the following procedures, see "SV vCenter Service configuration" on page 56.

## 7.3 FUJITSU PRIMERGY Predefined Alarm

The SV Plug-in offers a predefined alarm that will be triggered if a warning or error-level event is received by the vSphere Client event management. This alarm is enabled but has no actions defined.

You can define a convenient action for this predefined alarm in the vSphere Client:

**Requirements**

- Required privilege: **Alarms.Create alarm** or **Alarm.Modify alarm**

**Procedure**

After a new or update installation of the SV Plug-in, any changes made to an alarm (e.g. actions) will be lost and you must reconfigure the action as needed.

1. In the **Menu** area of the vSphere Client, select an inventory object.
2. Click the **Configure** tab.
3. Click the **More** - **Alarm Definitions** menu-item.

   The available alarms are listed under **Alarm Name**.
4. Select an alarm listed under **Alarm Name**.
5. Click **Edit** to edit an alarm.

For further information, see the documentation for VMware vSphere.

6. Click **Finish**.

## 7.4 Actions relating to SV vCenter Service

In the vSphere Client views for ESXi-based hosts (see "SV Plug-in information of an ESXi-based host" on page 85 and "FUJITSU PRIMERGY Actions (iRMC-based operations)" on page 91), you will find the following actions relating to the SV vCenter Service:


**Toggle FUJITSU Event Monitoring**

1. Click this icon to turn the subscription of the host to the SV vCenter Service on/off.

   This action is depicted in four ways, depending on the current subscription status:


The host is subscribed to the SV vCenter Service. Events will be monitored by the SV vCenter Service and forwarded.


The host is not subscribed to the SV vCenter Service. No events will be monitored by the SV vCenter Service or forwarded.


The subcription status of the host is unknown due to connection problems with the SV vCenter Service. No action will be performed.


The host cannot be subscribed, because the vCenter is not connected to the SV vCenter Service. No action will be performed.


**Invoke Test Event**

1. Click this icon to request the host to send a test indication.

   The selected host will be requested to send a test indication to its subscribed nodes.

   If the host is not subscribed to the SV vCenter Service (see "SV vCenter Service configuration" on page 56), you will not see the event in the vCenter Event Manager (**Monitor-Events** sub-tab of the vSphere Client).

# 8 Remote Management

The SV Plug-in offers some iRMC-based operations - called FUJITSU PRIMERGY Actions - depending on the capabilities of the selected host.

The FUJITSU PRIMERGY Actions make it very easy for the administrator to connect directly to an ESXi-based host and its iRMC.

To perform the iRMC-based operations (iRMC Web Interface together with single sign-on (SSO), AVR, location button LED , the user name and password for the iRMC credentials must be configured in the vCenter Server (see "Configure iRMC credentials: 'IPMI configuration'" on page 59). Click the 

icon to start the iRMC credentials configuration dialog (see "Configure iRMC credentials: 'IPMI configuration'" on page 59). These IPMI-based actions are always enabled in the context menu, even if the credentials are not configured or the user does not have the privilege to perform the action. In this case an error message will be shown if the action is started.

The single sign-on functionality no longer works in iRMC S5. When calling the iRMC Web Interface from the SV Plug-in, the user will be requested to log in to the iRMC Web Interface.

**Starting one of these iRMC-based FUJITSU PRIMERGY Actions**

ESXi-based host

See "Starting a FUJITSU PRIMERGY Action" on page 91.

vCenter or cluster host server

See "FUJITSU PRIMERGY Actions" on page 103.

## 8.1 LED

To facilitate identification of a system, for instance if it is installed in a fully populated rack, you can activate the identification LED.


**Toggle Identify LED**

1. Click this icon to toggle the Locate LED on and off:

Locate icon is blue: locate LED is on.

Locate icon is gray: locate LED is off.

The icon is displayed if an iRMC address is available.

## 8.2 iRMC Web Interface

iRMC S4/S5 permits system control, diagnosis, configuration and server restarting by remote access via the integrated web interface - even if the operating system or hardware fails.

The iRMC 4 supports Centralized Authentication Service (CAS) configuration, which allows you to configure the iRMC S4/S5 Web Interface for CAS-based single sign-on (SSO) authentication.

The single sign-on functionality no longer works in iRMC S5. When calling the iRMC Web Interface from the SV Plug-in, the user will be requested to log in to the iRMC Web Interface.


**Start iRMC**

1. Click this icon to launch the iRMC Web Interface in a new window.

The icon is displayed if an iRMC address is available.

See "Starting iRMC functions with/without single sign-on" on page 67.

## 8.3 Remote console (AVR)

Advanced Video Redirection (AVR) with iRMC S4/S5 offers the following benefits:

- Operation via a standard web browser (as of FW version 8.05F you can select HTML5).
- System-independent graphical and text console redirection (including mouse and keyboard).
- Remote access for boot monitoring, BIOS administration and control of the operating system.

- Local monitor-off support.
- Low bandwidth support.


**Start Remote Console**

1. Click this icon to launch a remote console (AVR) in a new window.

The icon is displayed if an iRMC address is available.

See "Starting iRMC functions with/without single sign-on" on page 67.

## 8.4 iRMC system report

**Requirements**

- The iRMC must be version S4.
- The iRMC credentials must be configured as follows:
  - The iRMC credentials must be configured with an iRMC user account that has the **Administrator** LAN channel privilege.
  - The vCenter user must have the privileges defined in the **FUJITSU PRIMERGY role FUJITSU PRIMERGY Plug-in Administrator**.

For further information, see "FUJITSU PRIMERGY vCenter role definitions and iRMC single sign-on" on page 65.


**Start a System Report**

1. Click this icon to start an iRMC system report in a new window.

See "iRMC system report" on page 116.

# 9 Proactive HA

## 9.1 Proactive HA - a vCenter cluster feature

**vSphere High Availability – Proactive HA**

vSphere High Availability (HA) now also detects the hardware conditions of the ESXi host and allows you to evacuate the virtual machines before the hardware issues cause an outage to virtual machines, with the help of Proactive HA.

Proactive HA works in conjunction with hardware vendors, monitoring solutions to obtain the health status of the hardware components such as memory, fans and power supplies. Together with a vSphere Client plug-in a Proactive HA Provider is installed and monitors every host in the cluster.

You can configure vSphere HA to respond according to the failure of hardware components. You need to have DRS enabled on the cluster to make use of Proactive HA.

If any hardware component is failed and marked as unhealthy by hardware monitoring, vSphere will classify the affected ESXi host as either moderately or severely degraded, based on the component failure. vSphere will put the affected ESXi host into new state called “Quarantine Mode”.

In Quarantine Mode, DRS will not use the ESXi host for new virtual machine placements and will also attempt to evacuate the host, provided this would not cause performance issues. You can also configure proactive HA to put the degraded ESXi hosts in Maintenance Mode which perform the vMotion of virtual machines to other healthy ESXi hosts in the cluster.

(Source: http://www.vmwarearena.com/vsphere-6-5-high-availability-new-features-proactive-ha/)

**The SV Plug-in supports Proactive HA**

Proactive HA works in conjunction with the SV Plug-in to obtain the health status of the hardware components such as memory, fans and power supplies. The support for the new feature is implemented in SV vCenter Service via the FujitsuHealthProvider, which communicates with vCenter and sends health status updates.

## 9.2 Configuring Proactive HA

The following instruction is based on VMware documentation. For further information see the documentation for VMware vSphere.

1. In the **Menu** area of the vSphere Client, select **Hosts and Clusters**.
2. Select the desired cluster.
3. Click the **Configure** tab.
4. Select **vSphere Availability**.
5. Click **Edit**.
6. Select the check-box **Turn on Proactive HA**.
7. Select the item **Proactive HA Failures and Responses**.

   The **Proactive HA Failures and Responses** view is displayed.
8. Choose one of the possible settings for **Automation Level**:

   **Manual**

   vCenter Server will suggest only the migration recommendations for virtual machines. You must manually migrate the virtual machines out from the degraded hosts.

   **Automated**

   Virtual machines will be migrated to healthy hosts and degraded hosts will be entered into remediation action, in either quarantine or maintenance mode depending on the configured Proactive HA automation level.
9. Choose one of the possible settings for **Remediation** actions for partially failed hosts:

   **Quarantine mode for all failures**

   No new virtual machines are added to the host.

   **Quarantine mode for moderate and Maintenance mode for severe failure (Mixed)**

   Keeps virtual machines running on the host for moderate failure. But will migrate virtual machines for severe failures.

   **Maintenance Mode for all failures**

   Migrates all the virtual machines from the host and puts the ESXi host in maintenance mode.
10. In the bottom section of the **Proactive HA Failures and Responses** view is the table of **Proactive HA providers** for this cluster.

11. Select the check-box in front of the **FujitsuHealthProvider**.

    Click on the **edit** link in the last column of the table to view/edit the failure conditions supported by the provider.

12. Click **OK**.

    The **Edit Cluster Settings** view is closed.

    Now the current information provided by the **FujitsuHealthProvider** is processed by vSphere Client and is displayed in the **Monitor - Tasks** and **Monitor - Events** sub-tabs for the cluster or host (see "Monitoring vCenter or cluster host servers" on page 100).

# 10 Error handling

## 10.1 Time of data acquisition

If the SV Plug-in is called, it will retrieve the data by chosen protocol.. Whenever you click the status item tree (see "Information on the selected host - Status icons, items and views" on page 86), the SV Plug-in retrieves the data of the ServerView ESXi CIM Provider again.

If you click the **Refresh**  icon of vSphere, a new data retrieval cycle will be initiated.

## 10.2 All expanded items are closed

Once a view with expanded items is refreshed, all expanded items are closed.

You will therefore have to expand the desired items again to see the specific data again.

## 10.3 Retrieving data failed

If data retrieval fails, an error icon will be displayed in the bottom right of the SV Plug-in interface.

If loading a content view fails, a message box will open showing the possible cause and the original error text.

## 10.4 An action in the top left of the SV Plug-in interface is disabled

An action in the top left of the SV Plug-in interface will be disabled if the user does not have the required privilege. There will be a tooltip saying **not privileged to start...**.

See "Starting iRMC functions with/without single sign-on" on page 67.

## 10.5 An action in the context menu results in an error message

Requesting an action in the context menu will result in an error message if the user does not have the required privilege.

See "Starting iRMC functions with/without single sign-on" on page 67.

## 10.6 Remote console (AVR) or iRMC Web Client do not work as expected

### 10.6.1 Mismatch in privileges

If the remote console (AVR) or iRMC Web Client are started from vSphere Client, they will be started in the role that matches the current user privileges as previously defined.

If these privilege definitions are not enough to enable the desired functions, AVR and iRMC Web Client will show unexpected behavior.

See "Starting iRMC functions with/without single sign-on" on page 67.

### 10.6.2 Problem when starting iRMC S5 Web Interface

If a problem arises when starting the iRMC S5 Web Interface in Microsoft Edge, you will need to remove the Compatibility Mode in the Internet Explorer Settings.

1. Select **Tools** - **Compatibility View settings**.
2. Uncheck the checkbox **Display internet sites in Compatibility View**.

## 10.7 The same event generates a significant number of entries in the event management

Sometimes events are sent with high frequency. In this case the same event is sent repeatedly by the same host and generates a significant number of entries in the event management of vSphere Client.

The SV Plug-in includes an **SV vCenter Service** which routes Fujitsu PRIMERGY-specific events to the vCenter event management to be monitored in the vSphere Client.

You can set the **`trap.forward.limit`** property of this service to enhance its performance.

See "Further helpful service properties for the SV vCenter Service for events" on page 110.

## 10.8 Repeated connection timeouts

Low connectivity in the network or older versions of ServerView ESXi CIM Provider or SNMP agents cause connection timeouts.

The SV Plug-in includes an **SV vCenter Service**, which routes Fujitsu PRIMERGY-specific events to the vCenter event management to be monitored in the vSphere Client.

You can set the **<cim/snmp>.client.timeout** property of this service to enhance its performance during connection timeouts.

If you increase this value, there will be fewer connection timeouts but the processing will take longer!

See "Further helpful service properties for the SV vCenter Service for events" on page 110.

## 10.9 Executing SVSInstallerGUI.sh results in warnings (remote X Server, e.g. MobaXTerm)

If **SVSInstallerGUI.sh** is executed with a remote X Server (e.g. MobaXTerm), some warnings will be displayed.

Example:

```
QXcbConnection: XCB error: 147 (Unknown), sequence: 161,
resource id: 0, major code: 140 (Unknown), minor code: 20
```

This is a known problem of the Qt libraries which will be solved in future versions of Qt.

You can ignore these warnings and the installer will nevertheless work correctly.

In addition, **SVSInstaller** can be executed without a GUI. Then no warnings will be displayed.

## 10.10 vCenter Server Appliance: Executing SVSInstallerGui.sh failed

**SVSInstallerGui.sh** cannot be executed on the vCenter Server Appliance (based on SLES 11), because there are prerequisites missing.

You must use **SVSInstaller.sh** here.

# 10.11 Single sign-on doesn't work (iRMC Web Interface, AVR, Location button LED)

Single sign-on can be used when starting the iRMC functions as **Administrator**. When starting the iRMC Web Interface, their iRMC LAN channel privilege will be adjusted to match the privilege level of the vCenter user.

The single sign-on functionality no longer works in iRMC S5. When calling the iRMC Web Interface from the SV Plug-in, the user will be requested to log in to the iRMC Web Interface.