FUJITSU Limited

PRIMERGY Plug-in for VMware vCenter

User Guide V6.0

PRIMERGY Plug-in for VMware vCenter is FUJITSU’s Hardware Support Manager simplifying lifecycle management of VMware vSphere clusters. This guide explains how to setup and use it.

December 2024

Contents

1. Preface ... 5
2. Product Summary ... 8
3. Introduction ... 9
3.1. Overview ... 9
3.2. Architecture ... 9
3.3. Firmware Management ... 10
4. Known Issues and Restrictions ... 12
5. Requirements ... 14
5.1. Resources Requirements of the Virtual Appliance ... 14
5.2. Center Server Requirements ... 14
5.3. vSphere Cluster and ESXi Node Requirements ... 14
5.4. Update Repository Requirements ... 15
5.5. Network Requirements ... 15
5.6. Supported Browsers ... 16
6. Configuration Data ... 18
7. Deployment ... 19
7.1. Checking the Prerequisites ... 19
7.2. Deploying the Virtual Appliance ... 19
7.2.1. Downloading the OVA ... 19
7.2.2. Deploying the VM ... 19
7.3. Configuring the Virtual Appliance ... 21
7.3.1. NTP Settings ... 21
7.3.2. Login to the Web Interface ... 22
7.3.3. Time Zone Settings ... 22
7.3.4. vCenter Server Connectivity ... 23
7.3.5. Registering the Plug-In ... 24
7.3.6. Repository URL and Proxy ... 26
7.3.7. iRMC Repository and Proxy ... 27
7.3.8. Rebooting the Plug-In VA ... 28
7.3.9. Component update mode ... 29
7.3.10. File Depot (HSP Upload) ... 29
8. Operation ... 32
8.1.1. iRMC Configuration of the Cluster Nodes ... 32

8.1.2. Managing the iRMC Credentials via REST API ... 36
8.2. Connecting the Plug-In to a Single Image in vLCM ... 37
8.3. Custom Version Selector ... 40
8.4. Custom Version Template Manager ... 44
8.5. Troubleshooting collecting data related to hosts inventories ... 45
8.6. Interpreting the Plug-in’s Compliance States ... 46
8.7. List of registered hosts ... 48
8.8. Backup ... 48
8.9. Host Monitoring ... 49
8.10. Appliance update ... 51
8.11. Troubleshooting Remediation ... 53
9. Maintenance ... 56
9.1. Adding New Host to a Cluster ... 56
9.2. Removing a Host from a Cluster ... 56
9.3. Changing the Plug-in VA’s Password ... 56
9.4. Updating Changed iRMC Passwords ... 56
9.5. Using custom user to login to vCenter ... 56
9.6. Changing vCenter User Password ... 56
9.7. Updating the Hardware Support Package (HSP) ... 57
9.8. Updating the Plug-In Virtual Appliance ... 57
9.9. Changing Network Address Settings of the Plug-in VA ... 58
9.10. Updating changed IP Address of an iRMC ... 59
9.11. Changing the IP Address of the vCenter Server ... 59
9.12. Removing custom selected version for component ... 59
Appendix A: Compliance Status ... 60
A.1. Firmware Component Compliance Status ... 60
A.2. Host Compliance Status ... 61
A.3. Staging ... 61
Appendix B: Checking and Cleaning up Plug-In Registration ... 62
Appendix C: Configuring vSphere Lifecycle Manager ... 64
C.1. Configuring Proxy Settings (if required) ... 64
C.2. Downloading Patches from the Online Depot ... 65
C.3. Defining the Image ... 66
C.4. Enabling Fully Automated Remediation ... 68
C.5. Performing Remediation ... 69
Appendix D: FAQ ... 71
D.1. What logs to include in a trouble ticket? ... 71

D.2. Plug-in Installation ends with an error 71

D.3. Plug-in Registration page loads incomplete. 72

D.4. Not able to select HSM. 73

D.5. Not able to select HSP. 74

D.6. iRMC address not filled automatically in Configure iRMC... 75

D.7. Firmware compliance check not working. 75

D.8. Firmware compliance Image Version Unknown 76

D.9. Firmware compliance Host Version Unknown 76

D.10. Host remediation failed with Unknown message. 77

D.11. vSphere Client does not show/works very slowly after multiple plugin installation/uninstallation/registration/deregistration. 78

D.12. iRMC session details when performing updates. 78

9.13. Backup 79

9.14. Host Monitoring 79

9.15. Appliance update 81

D.13. Unknown error when saving vLCM Image. 83

D.14. Custom Version Selector collecting inventory task is not getting finished and list of components is not being shown in the UI 84

D.15. Privileges for custom user 84

1. Preface

Purpose

This user guide describes the prerequisites, installation, and configuration as well as the usage of the PRIMERGY Plug-in for VMware vCenter.

⚠ Note	All diagrams and pictures included in this document are used as examples for refence purposes only and may contain data not directly relevant to your individual configuration.

Intended Readers

This guide is intended for system administrators, network administrators, administrators of VMware vSphere virtualized system platforms and related service providers.
General knowledge of hardware, software, and networking is assumed.

Related Documents

Document Name	Notation in This Document	Description
PRIMERGY Plug-in for VMware vCenter	User Guide	This document.
FUJITSU Hardware Support Package (HSP) Readme	HSP Readme	Included in the download of the HSP file: Lists the supported hardware, firmware, and software versions.
FUJITSU Software ServerView Suite ServerView Repository Server Installation and User Guide	ServerView Repository Server	Describes the deployment of a ServerView Repository Server.

For the documents above and further referenced documentation, refer to the following websites:

- FUJITSU Technical Support Pages
  If no pop-up window asks you to select a product, click on [Select a new Product]. On the pop-up window, select [Browse For Product], then product line [Software] and product group [Infrastructure Manager (ISM)]. From [Downloads] - [Continue] - [Selected operating system], select [VMware ESXi 7.0]. On the [Documents] tab, you find the related documents then.
- VMware vSphere Documentation
  There are sections in this document that refer to VMware's technical information and documents. Please make sure that you use the documentation that matches the software version you are using.

Notation in this Guide

This document uses the following notational conventions:

- Textboxes with important or helpful information.

ℹ Tip	Indicates information that may prove useful in the understanding of concepts and operation.

⚠ Note	Indicates cautionary information regarding the understanding of concepts and operation.

❗ Warning	Indicates that incorrect use may result in minor or moderate personal injury or damage to the product itself and/or the property of other users.

- <variable>
  Variables represent numeric values or text strings that you must replace in your input according to your environment.
  Example: <IP address>
- [label]
  Labels in square brackets represent designations on user interfaces or keystrokes.
  If several labels are concatenated by '-', the equally named elements on the user interface are to be selected one after the other in the given order.
  Example: [Inventory] - [<cluster name>] – [Updates]
  If several items are concatenated by '+', this indicates that the keys must be pressed simultaneously.
  Example: [Ctrl]+[c]

High Risk Activity

The Customer acknowledges and agrees that the Product is designed, developed and manufactured as contemplated for general use, including without limitation, general office use, personal use, household use, and ordinary industrial use, but is not designed, developed and manufactured as contemplated for use accompanying fatal risks or dangers that, unless extremely high safety is secured, could lead directly to death, personal injury, severe physical damage or other loss (hereinafter "High Safety Required Use"), including without limitation, nuclear reaction control in nuclear facility, aircraft flight control, air traffic control, mass transport control, medical life support system, missile launch control in weapon system. The Customer shall not use the Product without securing the sufficient safety required for the High Safety Required Use. In addition, Fujitsu (or other affiliate's name) shall not be liable against the Customer and/or any third party for any claims or damages arising in connection with the High Safety Required Use of the Product.

Trademarks

VMware, ESXi, vSphere, and vCenter are trademarks or registered trademarks of VMware Corporation in the United States, other countries, or both.

All other company and product names are trademarks or registered trademarks of the respective companies.

This document does not necessarily use the trademark symbols (™ and ®) to indicate system, product or other names as trademarks.

Copyright

Copyright Fujitsu Limited 2024 All rights reserved.
This manual shall not be reproduced or copied without the permission of Fujitsu Limited.

2. Product Summary

With PRIMERGY Plug-in for VMware vCenter, FUJITSU helps customers save time and increase accuracy in updating the firmware and drivers of PRIMERGY servers in their VMware vSphere clusters.

VMware's vSphere Lifecycle Manager (vLCM) maintains the hardware and software according to a desired state model: For each vSphere cluster, the user can define a desired image consisting of the ESXi version, vendor addons and firmware and drivers. In this way, it can be ensured that a remediation provides all servers of the cluster with identical software, firmware, and driver levels.

The PRIMERGY Plug-in for VMware vCenter implements the Hardware Support Manager (HSM), through which vLCM gets access to a FUJITSU-specific repository with the Hardware Support Package (HSP), firmware and drivers. The HSP includes FUJITSU software and data required on the ESXi nodes (PRIMERGY servers) to assist in the firmware and driver update process.

Users can manually choose a custom version to which they wish to update their drivers for each supported (by HSP) component of their ESXi nodes.
From vLCM version 2.2 users are having access to a feature allowing them to quickly manage iRMC credentials of their hosts using new API.

For further details, refer to VMware vSphere Lifecycle Manager.

The PRIMERGY Plug-in for VMware vCenter is deployed using a Virtual Appliance (VA), i.e., a pre-configured Virtual Machine (VM) to run on the VMware vSphere platform. The prerequisites, deployment, usage, and maintenance are described in this manual.

3. Introduction

With PRIMERGY Plug-in for VMware vCenter, Fujitsu helps customers save time and increase accuracy in updating the firmware and drivers of PRIMERGY servers used with VMware vSphere.

This chapter describes the integration with VMware vSphere Lifecycle Management and the plug-in components and their purpose.

3.1. Overview

VMware's vSphere Lifecycle Manager (vLCM) maintains the hardware and software according to a desired state model: For each vSphere cluster or standalone host, the user can define a desired image (also called single image) consisting of the ESXi version, vendor addons and firmware and drivers. Especially for clusters, this ensures that all included servers are supplied with an identical software, firmware, and driver version.

The PRIMERGY Plug-in for VMware vCenter implements the Hardware Support Manager (HSM), through which vLCM gets access to a Fujitsu-specific repository with the Hardware Support Package (HSP), firmware and drivers. The HSP includes Fujitsu software and data required on the ESXi nodes (PRIMERGY servers) to assist in the firmware and driver update process.

For general information on vLCM and HSM, refer to VMware vSphere Lifecycle Manager.

3.2. Architecture

The PRIMERGY Plug-in for VMware vCenter is deployed as a Virtual Appliance (VA), i.e., a pre-configured Virtual Machine (VM) to run on the VMware vSphere platform.

This plug-in VA is intended to centrally manage the global configuration information of the plug-in. It connects to the Fujitsu-specific firmware repository as well as to the vCenter Server.

ℹ Tip	Further information about the firmware repository can be found in section "3.3 Firmware Management" below.

Along with the related configuration data (e.g., network addresses, user credentials and proxy information), also the HSP files are stored on the plug-in VA.

ℹ Tip	The HSP file specifies the supported hardware, i.e., the PRIMERGY server models and their components. As it also specifies a firmware version for each supported component, it represents a firmly defined permissible combination of firmware versions which can be used as a desired state for the servers managed with it. Fujitsu regularly publishes new versions of the HSP file on the Fujitsu Technical Support Pages, from where they must be transferred to the plug-in VA manually.

From the plug-in VA, a vCenter plug-in named "PRIMERGY Plug-in for VMware vCenter" is deployed to the vCenter Server. This plug-in implements the HSM API of the vLCM to manage the firmware updates of the PRIMERGY servers.

The following diagram illustrates the relationships:

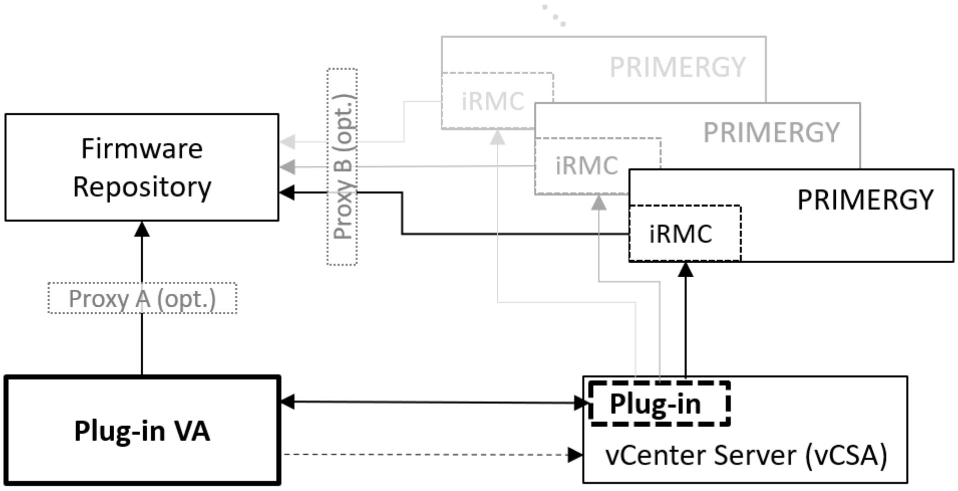


Figure 1- Architecture

The vCenter plug-in establishes a connection to the plug-in VA and needs to be configured to connect to the PRIMERGY iRMCs.

The graphical user interface of the vSphere Client is extended by the following functionality:

- The context menu of each ESXi host includes a menu item to configure its iRMC.
  For each PRIMERGY server to be managed by the plug-in, the credentials of an iRMC account with the Administrator role must be registered via this menu item or the also provided REST API. The specified account is used by the plug-in to configure and operate the iRMC's embedded Lifecycle Management (eLCM) functionality. For example, the proxy and the firmware repository location settings defined on the VA are transferred to the iRMC and the firmware updates are initiated from there.

- When creating or editing a vLCM image, the plug-in and an HSP can be selected as the Firmware and Drivers Addon.
  For each standalone host or cluster whose lifecycle management is to be performed with the plug-in's support, the Firmware and Drivers Addon of the corresponding vLCM image must refer to one of the HSP files provided on the plug-in VA.

- The provided Custom Version Selector allows you to assign a specific firmware version to each host component of each host in order to override the standard rules. Further details can be found in the section "3.3 Firmware Management" below.

If vLCM initiates a staging or remediation process for a host for which the plug-in (actually its HSP) is assigned as the Firmware and Drivers Addon, this starts the corresponding procedure of the plug-in. The plug-in instructs the iRMC to download the required firmware from the assigned repository to the server's eLCM SD card. Afterwards, while the server is being rebooted, the iRMC installs the new firmware.

3.3. Firmware Management

The firmware repository required by the plug-in can be either the Fujitsu GlobalFlash repository on the Internet or a local ServerView Repository Server. While the Fujitsu GlobalFlash repository is centrally managed and updated daily by Fujitsu, a local ServerView repository allows you to manage its content according to individual needs, e.g., to distribute only pre-tested firmware.

Regardless of which repository is used, the actual firmware version to be installed depends also on the following:

- The HSP file, which includes a firmly defined permissible combination of firmware versions for all supported components. Each standalone host or cluster managed by the plug-in can be assigned one of the available HSP files.
  However, the version information of the HSP can be overridden by the two control options below.
- The “Component Update Mode” setting in the plug-in VA, which decides whether the versions from the used HSP or the always newest versions (those with the highest version number) from the firmware repository are to be used. This setting applies globally to all hosts managed with the plug-in.
- The "Custom Version Selector", which allows you for every server managed by the plug-in to specify the desired firmware version for each of its hardware components.

In each case, you must decide whether you want to maintain your own firmware repository and which Component Update Mode setting should apply. The following table shows the possible combinations and their respective advantages and disadvantages:

Repository	Component Update Mode Setting	Advantages / Disadvantages / Recommendations
Fujitsu GlobalFlash repository	HSP	+ Firmly defined permissible combination of firmware versions. - Hosts require Internet access. - Dependence on the HSP file in terms of content and release cycle. Default setting that offers the least possible effort with good operational reliability.
	Repository (=newest available firmware version)	+ Always the latest firmware. - Hosts require Internet access. - The target firmware version of each component can change at any time, resulting in an increasing risk of inadmissible firmware combinations. This combination is typically only acceptable for test environments.
Locally managed ServerView repository	HSP	+ Firmly defined permissible combination of firmware versions can be retained as long as desired. + Hosts do not require Internet access. - Effort to maintain the repository.
	Repository (=newest provided firmware version)	+ Maximum flexibility. + Hosts do not require Internet access. - Effort to maintain the repository. This combination is particularly worthwhile for environments with many ESXi hosts or when particularly high demands in terms of operational reliability must be fulfilled.

Regardless of which combination you choose, you can use the Custom Version Selector to define exceptions for individual components of each server.

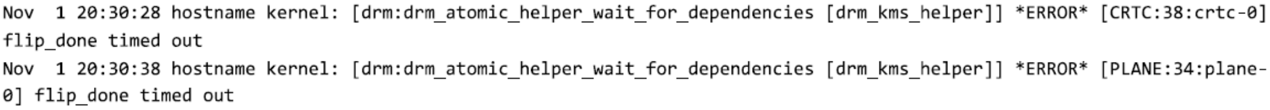
4. Known Issues and Restrictions

Restrictions for PRIMERGY Plug-in for VMware vCenter v6.0:

1. When using the plug-in for firmware update, the prerequisites and restrictions described for the individual firmware update apply as usual. You should carefully read the documentation of the respective firmware release.
2. The plug-in is for use with iRMC S6 (revision 2.42S or higher) or iRMC S5 (revision 1.25F or higher) or S4 (revision 9.08F or higher).
3. Only PRIMERGY Plug-in for VMware vCenter can be installed in one vCenter Server.
4. Configuration of the iRMCs on cluster level (bulk configuration) may lead to error “iRMC address not found” during compliance check. Please use single host configuration when configuring the iRMCs for the first time.
5. When remediation failed on ESXi versions prior to 7.0U2, an "Unknown message" is returned instead of more specific information (bug on VMware’s side).
6. In the host compliance report of vSphere Client, the full image comparison results are currently not shown for host while the overall host compliance status is compliant.
7. Currently the plug-in does not provide a possibility to change the credentials of the used vCenter Server account without the need of a re-registration. Proceed as described in section “9.5 Using custom user to login to vCenter

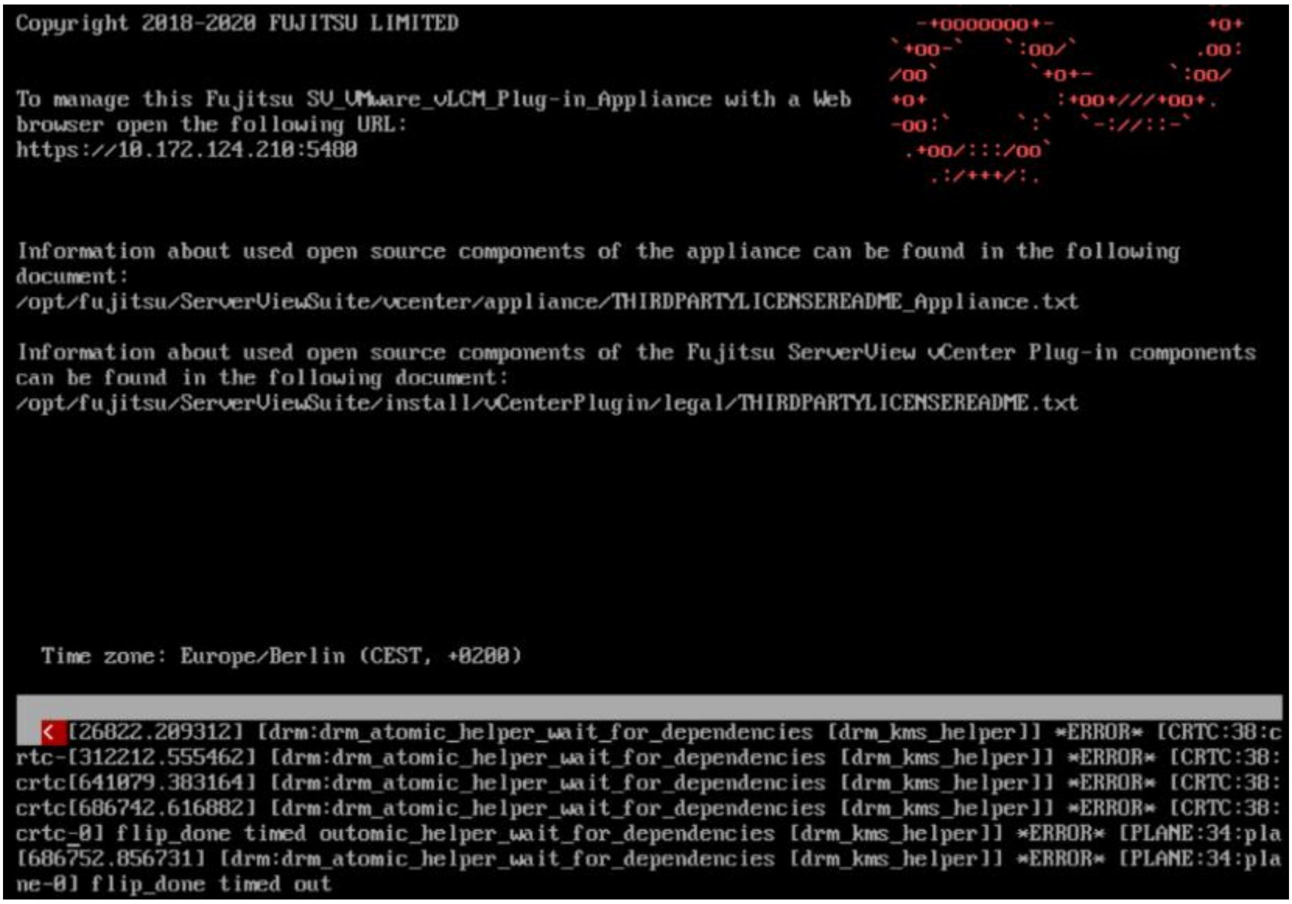
While using administrator account is possible to register plug-in, it’s not recommended for safety reason. New user for vCenter can be created, used roles from appendix D.15 from this manual.

8. Changing vCenter User Password”.
9. Do not use the “WebUI proxy settings” provided on the user interface of the plug-in VA, they are not supported.
10. For Custom Version Selector to work properly, it is required to have connected hosts with valid configured iRMC credentials.
11. In case of an issue where the Custom Version Selector is loading components for its hosts and does not proceed (observed around 80% of progress), please ensure the following: Ensure your browser is updated to the latest version, check for any network configuration issues, disable browser extensions, clear your cache and cookies. Trying incognito mode might resolve the issue, as it incorporates some of the previously mentioned suggestions. If the issue persists, collect data from your browser's developer tools, specifically the console tab and network tab with a filter set to 'Fetch/XHR.' Focus on the outputs from at least the last 5 calls related to getting the task status, which can be easily identified as they start with the prefix “task-“. After collecting this data, please contact your support center for further assistance in investigating and resolving the issue.
12. In the Plug-in VM you can sometimes experience following error:



```
Nov  1 20:30:28 hostname kernel: [drm:drm_atomic_helper_wait_for_dependencies [drm_kms_helper]] *ERROR* [CRTC:38:crtc-0]
flip_done timed out
Nov  1 20:30:38 hostname kernel: [drm:drm_atomic_helper_wait_for_dependencies [drm_kms_helper]] *ERROR* [PLANE:34:plane-
0] flip_done timed out
```

According to VMware engineering team this issue is harmless, and it’s connected to difference between hardware GPU and virtual GPU that is used in VMware virtual machine. This log can be found on Plugin virtual machine:



```
Copyright 2018-2020 FUJITSU LIMITED


To manage this Fujitsu SV_VMware_vLCM_Plug-in_Appliance with a Web
browser open the following URL:
https://10.172.124.210:5480



Information about used open source components of the appliance can be found in the following
document:
/opt/fujitsu/ServerViewSuite/vcenter/appliance/THIRDPARTYLICENSEREADME_Appliance.txt

Information about used open source components of the Fujitsu ServerView vCenter Plug-in components
can be found in the following document:
/opt/fujitsu/ServerViewSuite/install/vCenterPlugin/legal/THIRDPARTYLICENSEREADME.txt









  Time zone: Europe/Berlin (CEST, +0200)


  < [26822.209312] [drm:drm_atomic_helper_wait_for_dependencies [drm_kms_helper]] *ERROR* [CRTC:38:c
rtc-[312212.555462] [drm:drm_atomic_helper_wait_for_dependencies [drm_kms_helper]] *ERROR* [CRTC:38:
crtc[641079.383164] [drm:drm_atomic_helper_wait_for_dependencies [drm_kms_helper]] *ERROR* [CRTC:38:
crtc[686742.616882] [drm:drm_atomic_helper_wait_for_dependencies [drm_kms_helper]] *ERROR* [CRTC:38:
crtc-0] flip_done timed outomic_helper_wait_for_dependencies [drm_kms_helper]] *ERROR* [PLANE:34:pla
[686752.856731] [drm:drm_atomic_helper_wait_for_dependencies [drm_kms_helper]] *ERROR* [PLANE:34:pla
ne-0] flip_done timed out
```

5. Requirements

This chapter describes the requirements to be fulfilled in order to install, configure and operate the PRIMERGY Plug-in for VMware vCenter.

5.1. Resources Requirements of the Virtual Appliance

The following table shows the resource requirements of the deployed virtual machine (VM):

Resource	Minimal Requirement	Recommended Value
CPU	1 vCPU	2 vCPU
Memory	2 GB	4 GB
Storage	40 GB	40 GB

5.2. Center Server Requirements

The vCenter Server, on which this plug-in is to be registered, must meet the following prerequisites:

- vCenter Server version 7.0u3, 8.0, 8.0u1, 8.0u2, 8.0u3.
- vSphere Client user account having the privileges described in "vSphere Lifecycle Manager Privileges For Using Images" at least. For instance, any user account having the Administrator role can be used. However, it is recommended to create a specific account for such technical purpose, not using the default account Administrator@<vsphere-domain>.

⚠ Note	Be aware of the impact when changing the account password, see "9.5 Using custom user to login to vCenter While using administrator account is possible to register plug-in, it's not recommended for safety reason. New user for vCenter can be created, used roles from appendix D.15 from this manual. Changing vCenter User Password".

5.3. vSphere Cluster and ESXi Node Requirements

The vSphere cluster to be managed with the help of this plug-in must use a vLCM single image for lifecycle management, not baselines. The appropriate prerequisites must be fulfilled.
The cluster must consist of supported FUJITSU ESXi hosts only. Please refer to the "HSP Readme" for a complete list of the supported server models and ESXi versions. The document also contains a list of currently supported system components. Unsupported components may be installed, but they are ignored, and their firmware must be maintained otherwise. Please keep in mind that the Custom Version Selector view also won't display any components and/or ESXi hosts that are not supported in the HSP file. This means that the user won't be able to manually select a version for upgrading firmware of those components and/or ESXi hosts.

The Integrated Remote Management Controller (iRMC) of the hosts must meet the following requirements:

- Running firmware iRMC S6 (revision 2.42S or higher) or iRMC S5 (revision 1.25F or higher) or S4 (revision 9.08F or higher)
- ServerView embedded Lifecycle Management (eLCM) enabled (license and SD card installed)
- User account with and Redfish access enabled. Both conditions are met by default for the admin login. However, it is recommended to create a specific account for such technical purpose.

⚠ Note	Be aware of the impact when changing the account password, see "9.4 Updating Changed iRMC ".

5.4. Update Repository Requirements

This plug-in requires a repository providing the required firmware updates. That can be one of the following:

- The FUJITSU GlobalFlash Web Server on the Internet or
- a ServerView Repository Server which downloads the updated from the FUJITSU GlobalFlash Web Server.

⚠ Note	Please keep in mind that if the user specifies a version for each controller/system on the Custom Version Selector view, selected version will be installed regardless of selection.

Regardless of which option is selected, the connection can optionally be routed through a proxy server.

If a new ServerView Repository Server needs to be deployed, refer to the manual "ServerView Repository Server".

5.5. Network Requirements

The virtual appliance requires its own IP address in a network intended for management traffic. The hostname/IP should be registered in the (local) DNS and forward and backward resolvable.

It depends on the individual usage scenario whether access to other networks or to the Internet is needed. In addition to an appropriate gateway, the firewall (if available) must also be configured to enable the necessary communication.

Access to the following systems and services is required and needs to be considered in this regard:

- DNS server
- NTP server
- vSphere Client (vCenter Server)
- PRIMERGY update repository server; see "5.4 Update Repository Requirements". Beside the virtual appliance, also the iRMC of each ESXi host in the vSphere cluster needs access to the repository server. It is possible to configure a proxy for this.

The following table lists only the network connections that are required additionally due to the plug-in use. It is intended to assist in enabling communication between those components, for example through firewalls. However, be aware that it only shows the ports that are commonly used. Most of them are configurable and may differ in the individual customer environment.

Source System	Target System	Port	Purpose
PRIMERGY Plug-in for VMware vCenter	DNS server(s)	53/TCP, 53/UDP	Domain Name Service
	NTP server(s)	123/TCP, 123/UDP	Network Time Protocol
	vCenter Server	443/TCP	vCenter HTTPS port used for registration of the plug-in
	FUJITSU Update Repository (GlobalFlash) or ServerView Repository Server	443/TCP [1)]	Download of firmware and drivers Note: A proxy can be used with it.
	iRMC of each cluster node	443	Configuration of repository and proxy settings
vCenter	PRIMERGY Plug-in for VMware vCenter virtual appliance	3169/TCP and 3170/TCP	Retrieve configuration data and information about the available firmware (HSP).
	iRMC of each cluster node	443/TCP	Configure iRMC.
iRMC of each cluster node	FUJITSU Update Repository (GlobalFlash) or ServerView Repository Server	443/TCP [1)]	Download of firmware and drivers Note: A proxy can be used with it.
Client terminals for Management (Operating)	PRIMERGY Plug-in for VMware vCenter virtual appliance	5480/TCP	Web UI of the plug-in VA.

[1)] Optionally the traffic can be tunneled through a proxy.

5.6. Supported Browsers

The following browsers can be used to configure and operate this plug-in through its Web interface:

Browser	Minimum Version
Internet Explorer	11

Firefox	58
Chrome	63

6. Configuration Data

The following table is intended to collect the data needed during the deployment.

Scope	Setting	Value
PRIMERGY Plug-in for VMware vCenter virtual appliance	Name of the VM	
	Datastore name	
	Network name	
	Hostname (FQDN)	
	root password	
	IP address	
	Netmask	
	Gateway	
	DNS server(s)	
	NTP server(s)	
vCenter Server	vCenter FQDN	
	vCenter IP address	
	vCenter HTTPS port	
	vSphere domain	
	vCenter user	
	vCenter user password	
Update Repository (GlobalFlash)	Globalflash URL	https://support.ts.fujitsu.com/DownloadManager/globalflash [1]
	Proxy A (optional) [2]	
	Proxy A port	
	Proxy A user	
	Proxy A password	
iRMC Repository	iRMC Repository URL	https://support.ts.fujitsu.com [1]
	Repository Catalog	DownloadManager/globalflash/GF_par_tree.exe [1]
	Proxy B (optional) [3]	
	Proxy B port	
	Proxy B user	
	Proxy B password	

[1] To be replaced by the URL of a ServerView Repository Server if required.

[2] Proxy used by the plug-in VA to communicate with the firmware repository server.

[3] Proxy used by the iRMCs to communicate with the firmware repository server.

7. Deployment

This chapter explains the deployment of the PRIMERGY Plug-in for VMware vCenter.

Unless otherwise specified, the described tasks are mandatory. Perform them in the order of the subsections below.

7.1. Checking the Prerequisites

Make sure all prerequisites described in section “5 Requirements” are fulfilled. Especially ensure the following:

- The vSphere cluster is usable, shows no errors and provides the necessary resources.
- IP and hostname of the plug-in VA are registered in DNS.
- The repository providing the firmware is available.
- Proxies and firewalls are configured properly.
- Proper user accounts are provided on vCenter Server and on each node’s iRMC.

7.2. Deploying the Virtual Appliance

An Open Virtualization Appliance (OVA) file is used to deploy the PRIMERGY Plug-in for VMware vCenter virtual appliance to a vSphere cluster.

7.2.1. Downloading the OVA

Proceed as follows to download the OVA file:

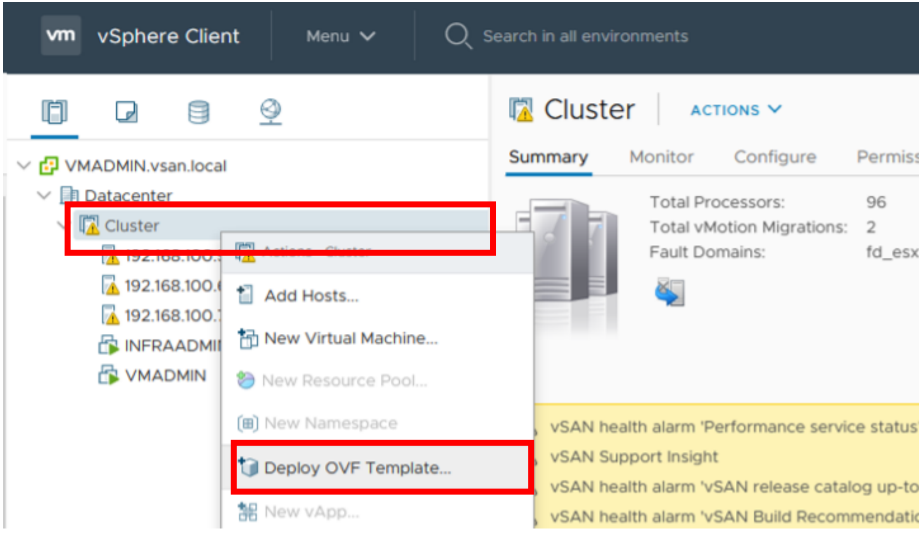
1. Open the FUJITSU Product Support Pages.
2. Click the [**Select a new Product**] button.
3. On the pop-up window, select [**Browse for product**], then [**Software**] – [**Infrastructure Manager (ISM)**].
4. Select [**Downloads**] – [**Continue**] and then [**VMware ESXi 7.x**] as the operating system.
5. From the [**Applications**] tab, expand [**Plugins**] and download the following: "**FUJITSU Software Infrastructure Manager SV Plug-in for VMware vLCM (HSM)**"

7.2.2. Deploying the VM

This section describes how to use the downloaded OVA file to deploy the PRIMERGY Plug-in for VMware vCenter Virtual Appliance into an existing vSphere cluster.

Proceed as follows:

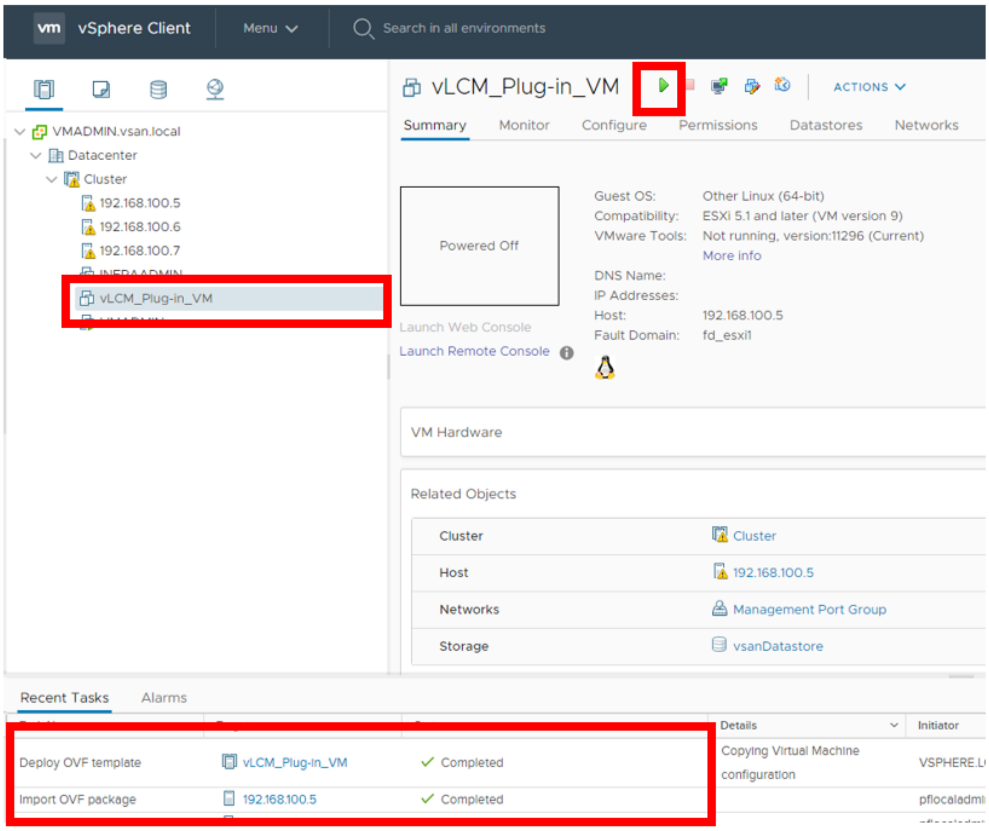
1. Login to the vSphere Client as a user having the privileges to deploy a new VM.
2. In the [**Inventory**] - [**Hosts and Clusters**] view, right-click the cluster name of the cluster to which you want to deploy the VM and chose [**Deploy OVF Template**] then.



3. On the [**Select OVF Template**] screen, check [**Local file**] and click the [**UPLOAD FILES**] button.
4. Upload the OVA file and click the [**NEXT**] button.
5. On the [**Select Name and Folder**] screen, enter the [**Virtual machine name**], select the name of the data center as its location and click the [**Next**] button.
6. On the [**Select a compute resource**] screen, select the desired ESXi node and click the [**Next**] button.
7. On the [**Review details**] screen, click the [**Next**] button.
8. On the [**License agreements**] screen, review the contents. Check [**I accept all license agreements.**] and click the [**Next**] button.
9. On the [**Select storage**] screen, select the intended datastore for VMs of the management software stack and click the [**Next**] button.
10. On the [**Select networks**] screen, select the intended network for management and click the [**Next**] button.
11. On the [**Customize template**] screen, enter the following settings:
    - [**Hostname**] (<Hostname>.<Domain Name>)
    - [**root Password**] (<root password)
    - [**Default gateway**] (<Gateway>)
    - [**DNS**] (<DNS server(s)>)
    - [**Network 1 IP Address**] (<IP address>)
    - [**Network 1 Netmask**] (<Netmask>)

    The values in "(<..>)" are specifying the names of the corresponding PRIMERGY Plug-in for VMware vCenter VA settings listed in section "6 Configuration Data".
    Click the [**Next**] button.
12. Review the values on the [**Ready to complete**] screen and click the [**FINISH**] button.

13. On the [**Recent Tasks**] list of the vSphere Client, monitor the tasks [**Deploy OVF template**] and [**Import OVF package**]. After both are completed, power on the new VM.



Guest OS: Other Linux (64-bit)
Compatibility: ESXi 5.1 and later (VM version 9)
VMware Tools: Not running, version:11296 (Current)
More info
DNS Name:
IP Addresses:
Host: 192.168.100.5
Fault Domain: fd_esxi1

Cluster	Cluster
Host	192.168.100.5
Networks	Management Port Group
Storage	vsanDatastore

			Details	Initiator
Deploy OVF template	vLCM_Plug-in_VM	✓ Completed	Copying Virtual Machine configuration	VSPHERE.L
Import OVF package	192.168.100.5	✓ Completed		pflocaladmi

7.3. Configuring the Virtual Appliance

Before the plug-in can be used by vLCM, some basic settings need to be applied on the plug-in appliance. Mainly the connectivity to all services and between the involved components, vCenter Server, firmware repository and the iRMCs of cluster nodes must be configured.

Perform the required tasks in the order of the subsections.

7.3.1. NTP Settings

If the plug-in VA is unable to reach the default NTP servers provided by the pool.ntp.org project directly on the Internet, you need to apply a reachable NTP server to the configuration.
Proceed as follows to adjust the NTP server setting:

1. Establish an SSH connection to the root account of the plug-in VA.
2. Open the file `/etc/chrony.conf` in an editor (e.g., vi) and comment out the useless pool setting
   ```
   # pool 2.cloudlinux.pool.ntp.org iburst
   ```
   Instead insert one or more lines specifying the FQDN or IP address of reachable NTP servers. Example:
   ```
   server time1.domain.local iburst
    server time2.domain.local iburst
   ```
   Save the file and close the editor.
3. Restart the chronyd service to load the modified settings.

```
[root@hsm ~]# systemctl restart chronyd
```

4. Check success.

```
[root@hsm ~]# chronyc sources
```

5. Close the SSH session.

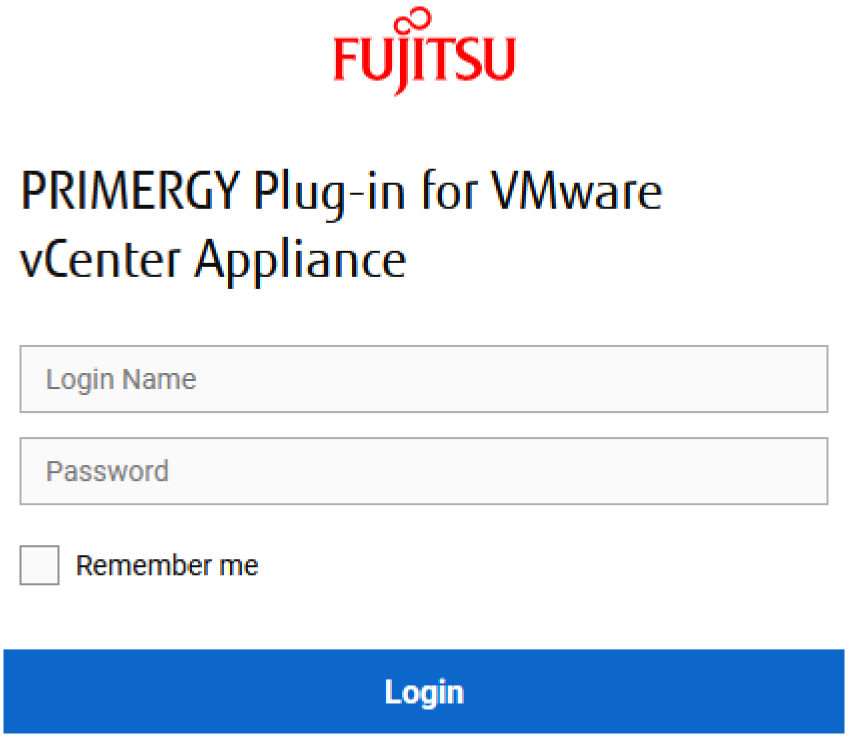
```
[root@hsm ~]# exit
```

7.3.2. Login to the Web Interface

Connect your browser to the Web interface of the Plug-in VA at

https://<FQDN of PRIMERGY Plug-in for VMware vCenter VA>:5480

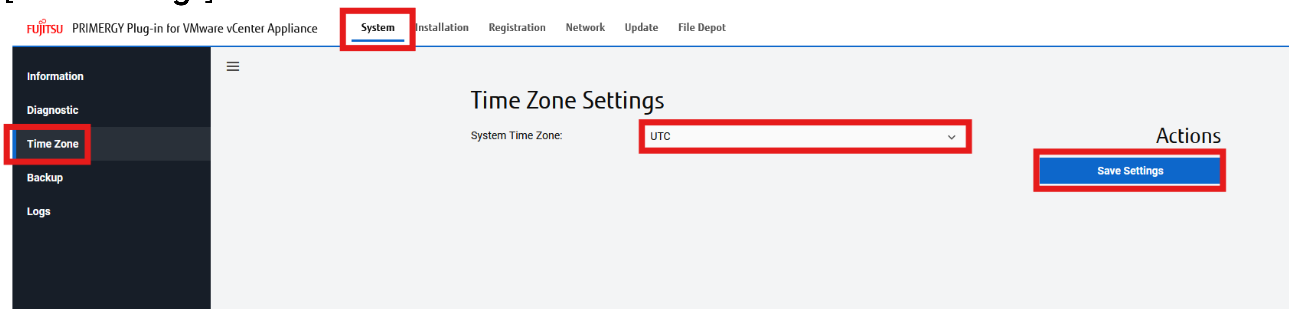
(make sure to specify https and the correct port!)



Log in with the root credentials.

7.3.3. Time Zone Settings

On the [**System**] tab – [**Time Zone**], adjust the [**System Time Zone**] to the local one and click [**Save Settings**].



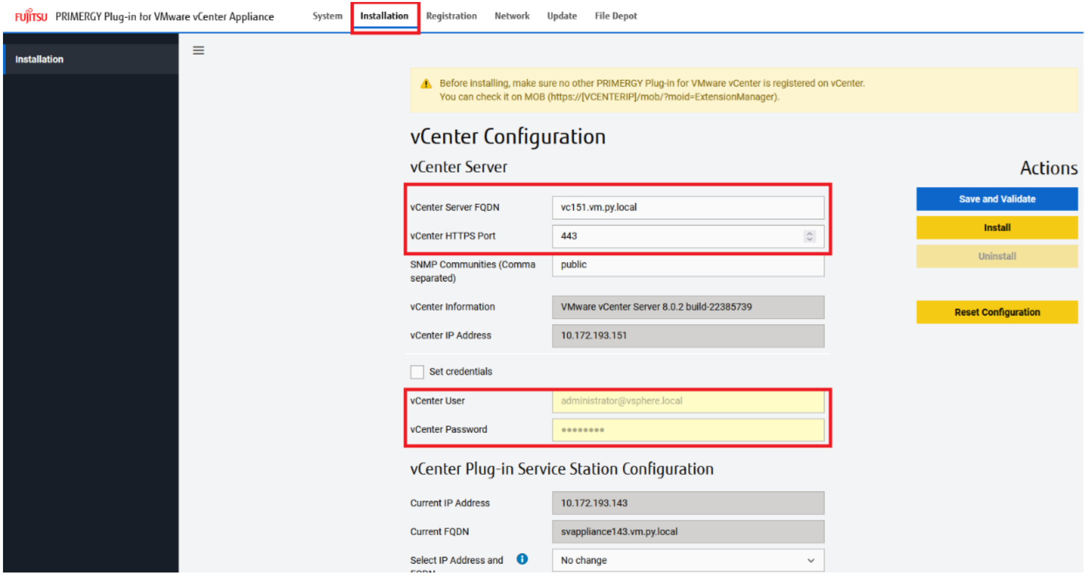
System Time Zone: UTC

7.3.4. vCenter Server Connectivity

Before the plug-in can be registered to vCenter Server, the network connectivity needs to be established.

Proceed as follows:

1. Navigate to the [**Installation**] tab to enter the information about the vCenter Server.



Before installing, make sure no other PRIMERGY Plug-in for VMware vCenter is registered on vCenter.
You can check it on MOB (https://[VCENTERIP]/mob/?moid=ExtensionManager).

vCenter Configuration

vCenter Server

vCenter Server FQDN	vc151.vm.py.local
vCenter HTTPS Port	443
SNMP Communities (Comma separated)	public
vCenter Information	VMware vCenter Server 8.0.2 build-22385739
vCenter IP Address	10.172.193.151

□ Set credentials

vCenter User	administrator@vsphere.local
vCenter Password	••••••••

vCenter Plug-in Service Station Configuration

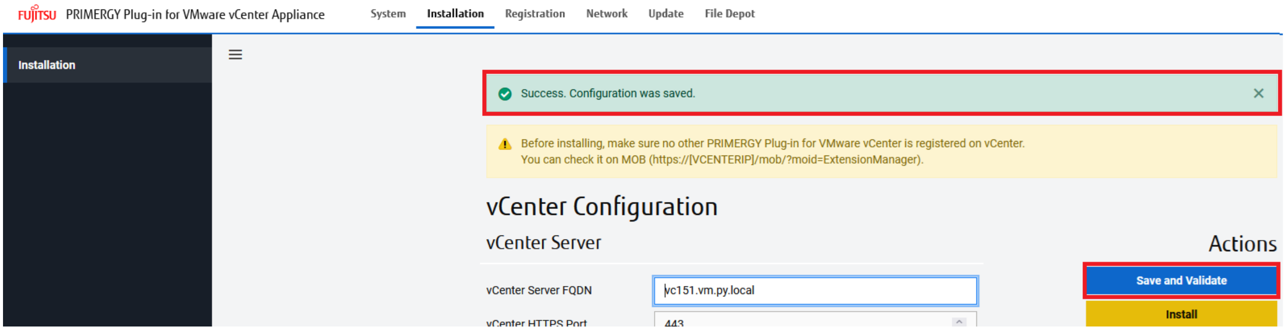
Current IP Address	10.172.193.143
Current FQDN	svappliance143.vm.py.local
Select IP Address and FQDN	No change

Under [**vCenter Configuration**], fill in the following fields:

- [**vCenter Server FQDN**] (<vCenter FQDN>)
  The IP address or network name of the vCenter Server to which the Plug-in is intended to be registered to.
- [**vCenter HTTPS port**] (<vCenter HTTPS port>)
  The HTTPS port of the above vCenter Server (default: 443).
- [**SNMP communities**]
  For future use, do not modify.
- Check [**Set credentials**] to enable the fields used to specify the credentials required to access vCenter Server and register the plug-in on it.
- [**vCenter User**] (<vCenter user>)
  The login requires user with certain privileges. Those will be attached in further section of this manual.
- [**vCenter Password**] (<vCenter user password>)
  The password of the above login.
- [**Select IP Address and FQDN**]
  From the dropdown-list, select a network name or IP address which is known to be usable by the vCenter Server to communicate with the plug-in VA. Consider the DNS registration, a possibly used proxy server and the firewall if one is in place.

The values in "(<..>)" are specifying the names of the corresponding vCenter Server settings listed in section "5 Configuration Data".
Click the [**Save and Validate**] button.

2. Verify that the [**Success. Configuration was saved.**] message appeared and click the [**Install**] button then.



Success. Configuration was saved.

Before installing, make sure no other PRIMERGY Plug-in for VMware vCenter is registered on vCenter.
You can check it on MOB (https://[VCENTERIP]/mob/?moid=ExtensionManager).

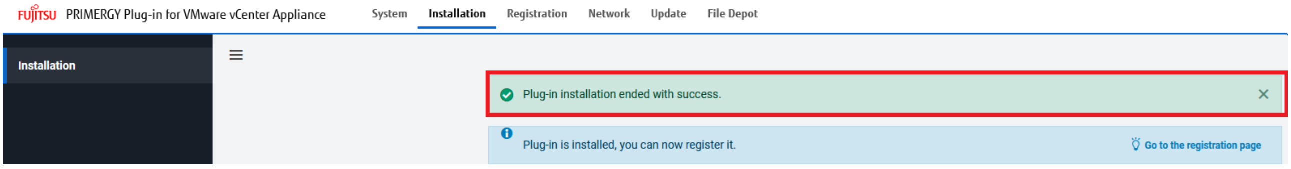
vCenter Configuration

vCenter Server

vCenter Server FQDN: vc151.vm.py.local

vCenter HTTPS Port: 443

3. Wait a few minutes until the [**Plug-in installation ended with success.**] message is shown.


FUJITSU PRIMERGY Plug-in for VMware vCenter Appliance
System
Installation
Registration
Network
Update
File Depot
Installation
Go to the registration page

Plug-in installation ended with success.

Plug-in is installed, you can now register it.

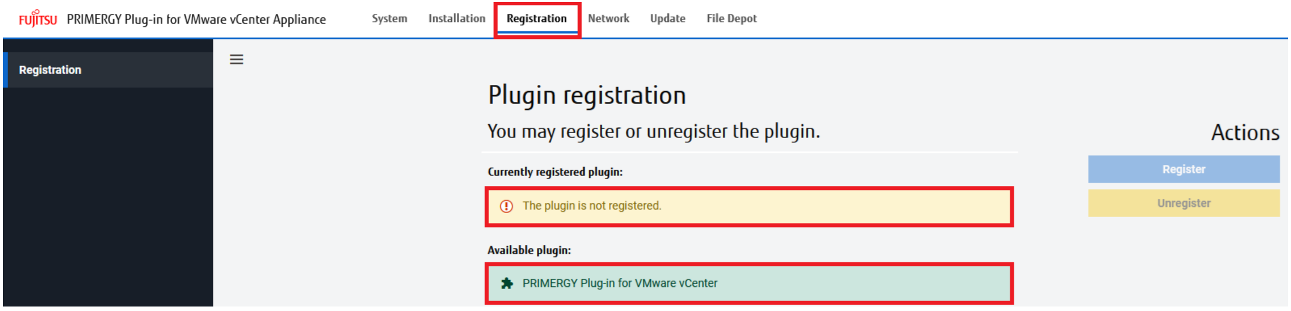
7.3.5. Registering the Plug-In

This section describes how to register the plug-in as an enhancement to the vSphere Client.

Note	If you had already registered the plug-in on the same vCenter Server before, make sure the registration has been completely removed, otherwise the registration will fail. If you are unsure, please check it following the instructions provided in “Appendix B: Checking and Cleaning up Plug-In Registration".

Proceed as follows to register the plug-in:

1. Navigate to the [**Registration**] tab of the PRIMERGY Plug-in for VMware vCenter VA Web interface.
2. If you see a message [**The plugin service is being prepared/setup. Please wait.**], wait some minutes until the messages [**The plugin is not registered.**] and [**PRIMERGY Plug-in for VMware vCenter**] appear.



Plugin registration

You may register or unregister the plugin.

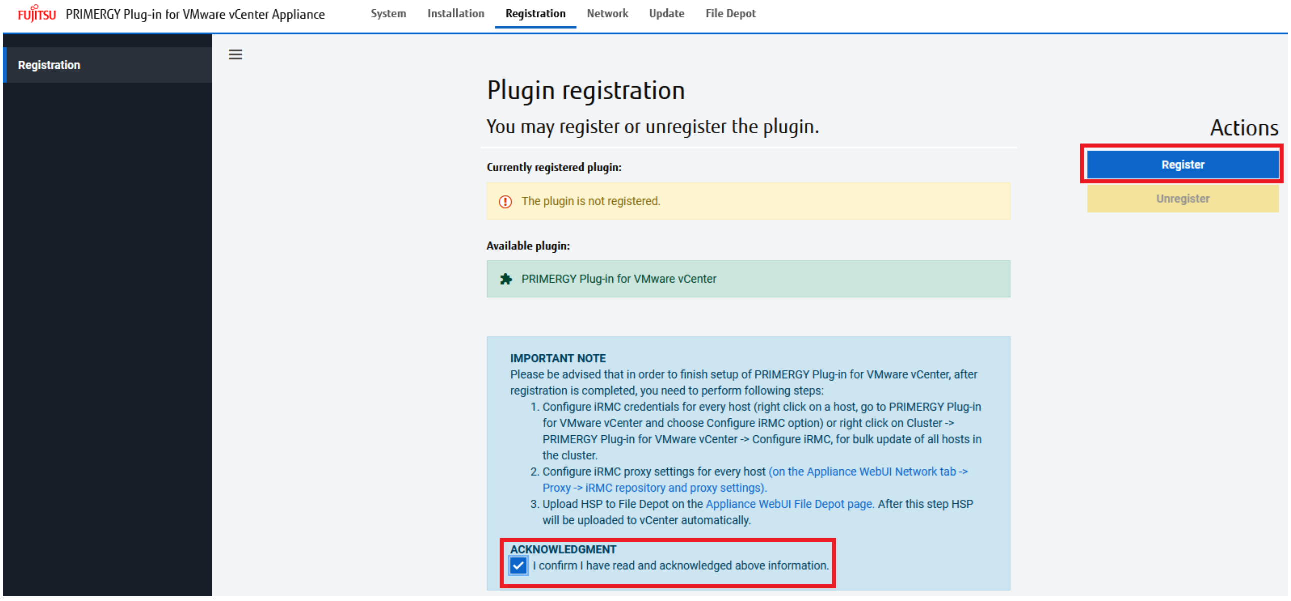
Currently registered plugin:

The plugin is not registered.

Available plugin:

PRIMERGY Plug-in for VMware vCenter

3. Confirm the [**IMPORTANT NOTE**] by checking the box in front of [**I confirm that I have read…**] and click at [**Register**].



Plugin registration

You may register or unregister the plugin.

Currently registered plugin:

The plugin is not registered.

Available plugin:

PRIMERGY Plug-in for VMware vCenter

IMPORTANT NOTE

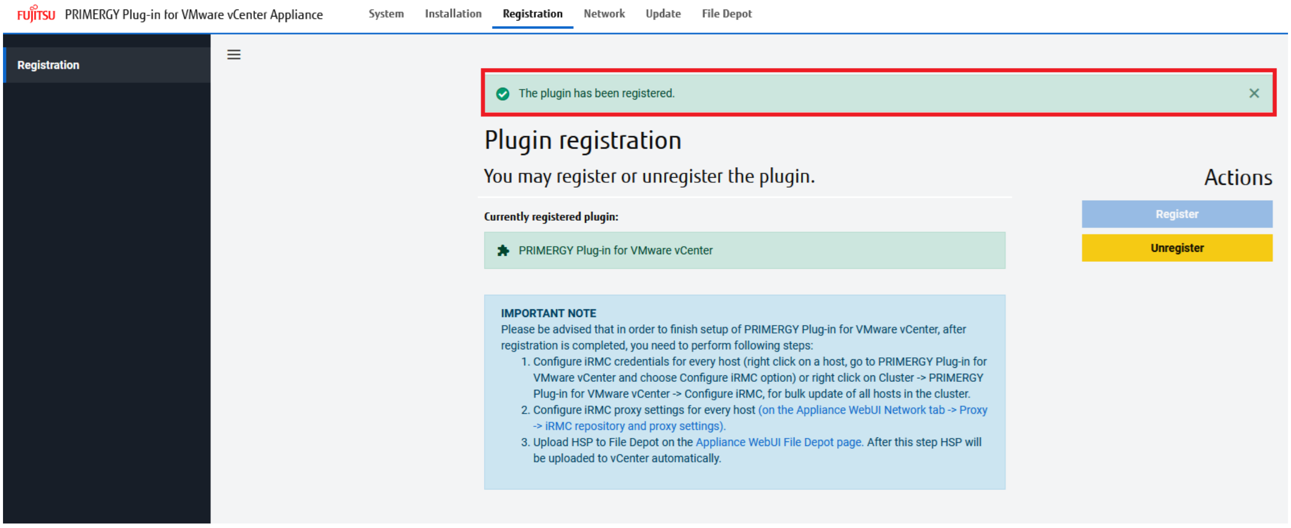
Please be advised that in order to finish setup of PRIMERGY Plug-in for VMware vCenter, after registration is completed, you need to perform following steps:

1. Configure iRMC credentials for every host (right click on a host, go to PRIMERGY Plug-in for VMware vCenter and choose Configure iRMC option) or right click on Cluster -> PRIMERGY Plug-in for VMware vCenter -> Configure iRMC, for bulk update of all hosts in the cluster.
2. Configure iRMC proxy settings for every host (on the Appliance WebUI Network tab -> Proxy -> iRMC repository and proxy settings).
3. Upload HSP to File Depot on the Appliance WebUI File Depot page. After this step HSP will be uploaded to vCenter automatically.

ACKNOWLEDGMENT

☑ I confirm I have read and acknowledged above information.

4. Confirm the dialog [**Register plugin**] by clicking on [**Register**].
5. Wait for the message [**The plugin has been registered**].



The plugin has been registered.

Plugin registration

You may register or unregister the plugin.

Currently registered plugin:

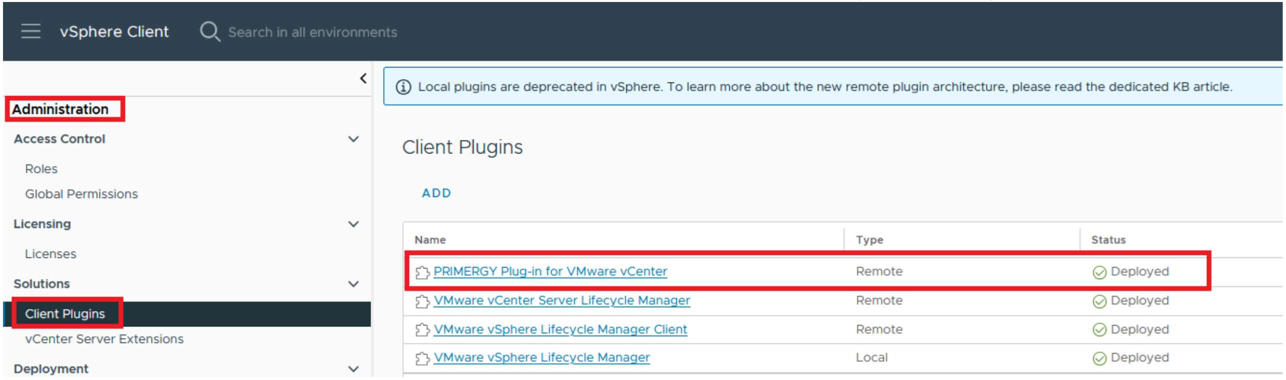
PRIMERGY Plug-in for VMware vCenter

IMPORTANT NOTE

Please be advised that in order to finish setup of PRIMERGY Plug-in for VMware vCenter, after registration is completed, you need to perform following steps:

1. Configure iRMC credentials for every host (right click on a host, go to PRIMERGY Plug-in for VMware vCenter and choose Configure iRMC option) or right click on Cluster -> PRIMERGY Plug-in for VMware vCenter -> Configure iRMC, for bulk update of all hosts in the cluster.
2. Configure iRMC proxy settings for every host (on the Appliance WebUI Network tab -> Proxy -> iRMC repository and proxy settings).
3. Upload HSP to File Depot on the Appliance WebUI File Depot page. After this step HSP will be uploaded to vCenter automatically.

6. In vSphere Client, verify success by checking the visibility of the plug-in in the client plugins list. Note that you might need to refresh your browser window or login to vSphere Client again. Navigate to [**Administration**] – [**Solutions**] – [**Client Plugins**] and verify that [**PRIMERGY Plug-in for VMware vCenter**] and [**FUJITSU ISM SV SV Plug-in for vLCM API**] are present and that the [**Status**] column displays [**Deployed/Enabled**].



Local plugins are deprecated in vSphere. To learn more about the new remote plugin architecture, please read the dedicated KB article.

Client Plugins

ADD

Name	Type	Status
PRIMERGY Plug-in for VMware vCenter	Remote	Deployed
VMware vCenter Server Lifecycle Manager	Remote	Deployed
VMware vSphere Lifecycle Manager Client	Remote	Deployed
VMware vSphere Lifecycle Manager	Local	Deployed

7.3.6. Repository URL and Proxy

Some components require additional information to decide which firmware releases can be installed on them. For instance, for some Intel network adapters, a mapping of so called eTrackIDs to NVM versions is required. This information is provided in files which are stored in the Globalflash or on a ServerView Repository Server.

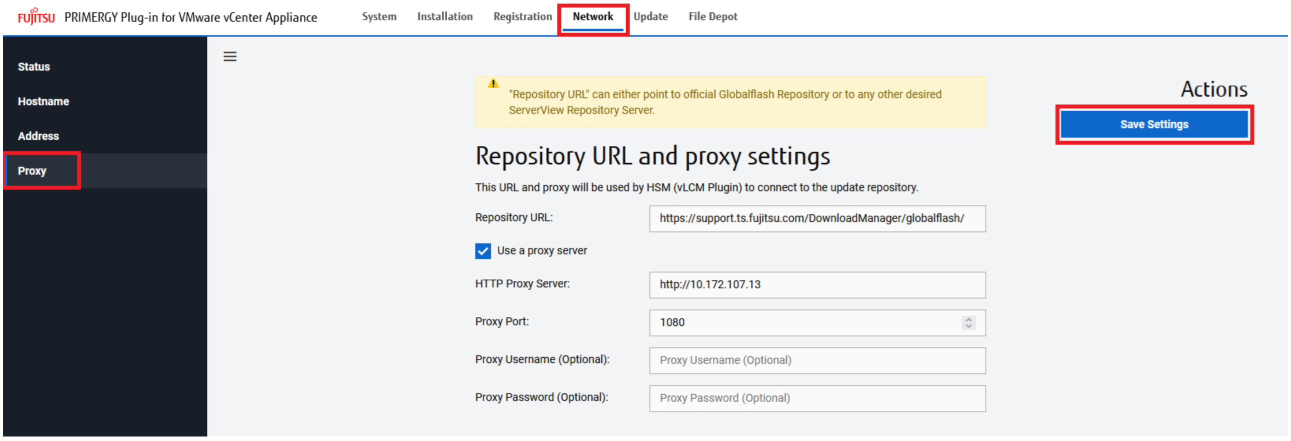
Those files can either be uploaded to the plug-in VA manually (on page [File Depot]), or the plug-in VA can download them using a provided repository URL.

If you need to upload the files manually, e.g., because the plug-in VA has no access to the repository, continue with the next section. The manual file upload will be handled in section “7.3.10 File Depot (HSP Upload)” later.
Otherwise proceed as follows to configure the download from the repository:

1. Navigate to the [**Network**] tab and from the left menu select [**Proxy**] then.
2. Under [**Repository URL and proxy settings**], enter the following settings:
    - **[Repository URL]** (<Repository URL>)
      The URL intended to be used by the plug-in VA to access the Globalflash or a ServerView Repository Server. If you want to use the FUJITSU Globalflash repository on the Internet, click on the ocher colored text [**Click here to enter the default value**].
    - If the plug-in VA needs to use a proxy server to access the specified repository, set the checkmark in front of [**Use a proxy server**].
    - **[HTTP Proxy Server]** (<Proxy A (optional)>)
      FQDN or IP address of the proxy to be used by the plug-in VA to connect to the specified repository.

- **[Proxy Port]** (<Proxy A port>)
  Port to be used to connect to the proxy server.
- [**Proxy Username (Optional)**] (<Proxy A user>)
  If the proxy requires it, specify a user.
- [**Proxy Password (Optional)**] (<Proxy A password>)
  If the proxy requires it, specify the password of the user.

The values in "(<..>)" are specifying the names of the corresponding Update Repository settings listed in section "6 Configuration Data".
After entering the values, click on [**Save Settings**].



"Repository URL" can either point to official Globalflash Repository or to any other desired ServerView Repository Server.

Repository URL and proxy settings

This URL and proxy will be used by HSM (vLCM Plugin) to connect to the update repository.

Repository URL: https://support.ts.fujitsu.com/DownloadManager/globalflash/

☑ Use a proxy server

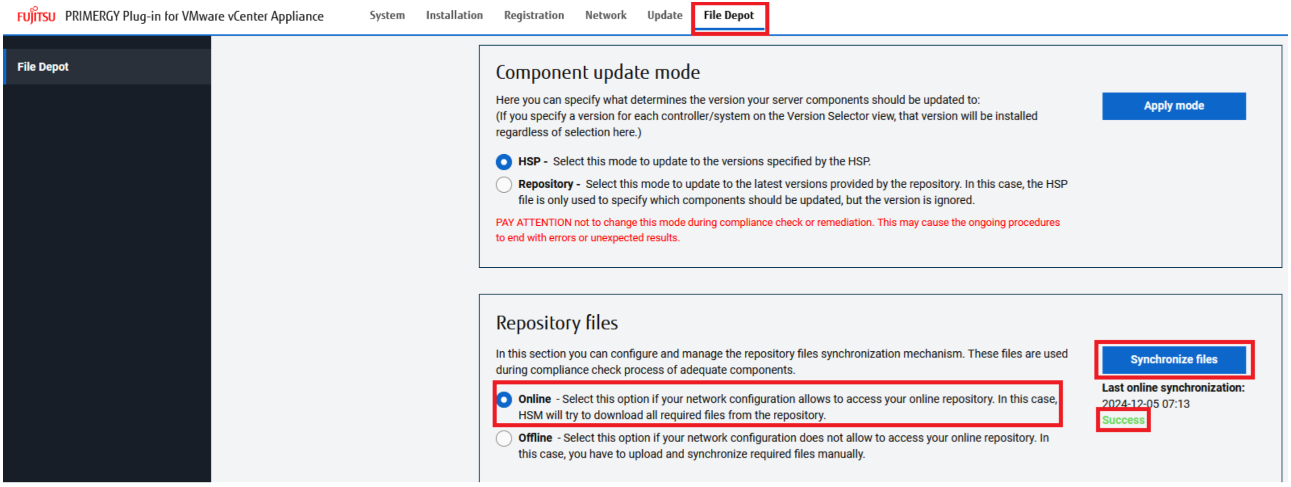
HTTP Proxy Server: http://10.172.107.13

Proxy Port: 1080

Proxy Username (Optional): Proxy Username (Optional)

Proxy Password (Optional): Proxy Password (Optional)

3. To verify success, navigate to the [**File Depot**] page. In the [**Repository files**] frame, select [**Online**] and click the [**Synchronize files**] button. Ensure you see a timestamp and a green [**Success**] message below it then.



Component update mode

Here you can specify what determines the version your server components should be updated to:
(If you specify a version for each controller/system on the Version Selector view, that version will be installed regardless of selection here.)

● **HSP -** Select this mode to update to the versions specified by the HSP.

○ **Repository -** Select this mode to update to the latest versions provided by the repository. In this case, the HSP file is only used to specify which components should be updated, but the version is ignored.

PAY ATTENTION not to change this mode during compliance check or remediation. This may cause the ongoing procedures to end with errors or unexpected results.

Repository files

In this section you can configure and manage the repository files synchronization mechanism. These files are used during compliance check process of adequate components.

● **Online** - Select this option if your network configuration allows to access your online repository. In this case, HSM will try to download all required files from the repository.

○ **Offline** - Select this option if your network configuration does not allow to access your online repository. In this case, you have to upload and synchronize required files manually.

Last online synchronization:
2024-12-05 07:13
Success

7.3.7. iRMC Repository and Proxy

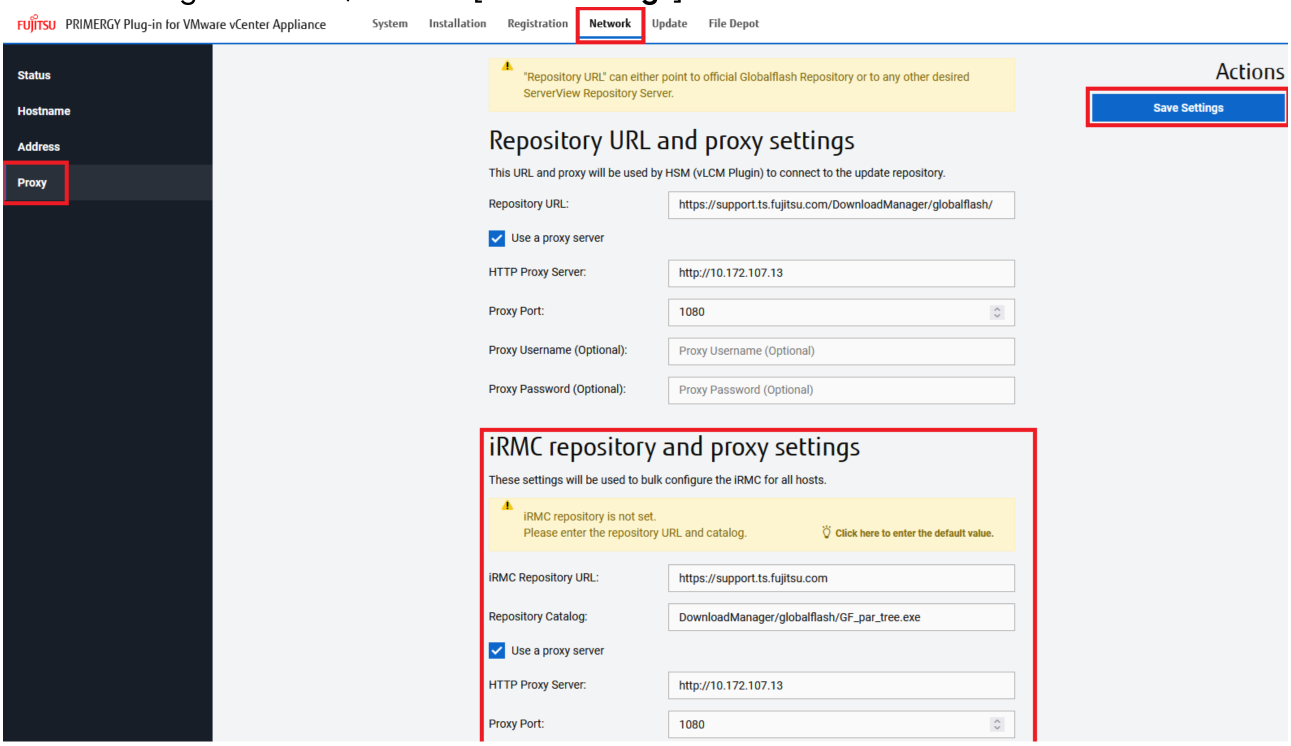
The Web UI of the plug-in VA provides the option to centrally configure the firmware repository which shall be used by all iRMCs handled by this plug-in. With these settings, at the time of the update, possibly existing individual settings on the iRMCs are overwritten.

If you decide not to provide data here, make sure to configure each server's iRMC of the cluster maintained by this plug-in individually.

Proceed as follows to configure the iRMC settings centrally:

1. Navigate to the [**Network**] - [**Proxy**].
2. Under [**iRMC repository and proxy settings**], enter the following settings:
    - **[iRMC Repository URL]** (<iRMC Repository URL>)
      The URL intended to be used by the iRMCs to access the Globalflash or a ServerView Repository Server. If you want to use the FUJITSU Globalflash repository, click on the ocher colored text [**Click here to enter the default value**].
    - **[Repository Catalog]** (<Repository Catalog>)
      Specifies the path of the parameter tree file which is appended to the repository URL.
    - If the iRMCs need to use a proxy server to access the repository, set the checkmark in front of [**Use a proxy server**].
    - **[HTTP Proxy Server]** (<Proxy B (optional)>)
      FQDN or IP address of the proxy to be used by the iRMCs to connect to the specified repository.
    - **[Proxy Port]** (<Proxy B port>)
      Port to be used to connect to the proxy server.
    - [**Proxy Username (Optional)**] (<Proxy B user>)
      If the proxy requires it, specify a user.
    - [**Proxy Password (Optional)**] (<Proxy B password>)
      If the proxy requires it, specify the password of the user.

   The values in "(<..>)" are specifying the names of the corresponding iRMC Repository settings listed in section "6 Configuration Data".
   After entering the values, click on [**Save Settings**].



"Repository URL" can either point to official Globalflash Repository or to any other desired ServerView Repository Server.

Repository URL and proxy settings

This URL and proxy will be used by HSM (vLCM Plugin) to connect to the update repository.

Repository URL: https://support.ts.fujitsu.com/DownloadManager/globalflash/

☑ Use a proxy server

HTTP Proxy Server: http://10.172.107.13

Proxy Port: 1080

Proxy Username (Optional): Proxy Username (Optional)

Proxy Password (Optional): Proxy Password (Optional)

iRMC repository and proxy settings

These settings will be used to bulk configure the iRMC for all hosts.

iRMC repository is not set.
Please enter the repository URL and catalog.
Click here to enter the default value.

iRMC Repository URL: https://support.ts.fujitsu.com

Repository Catalog: DownloadManager/globalflash/GF_par_tree.exe

☑ Use a proxy server

HTTP Proxy Server: http://10.172.107.13

Proxy Port: 1080

7.3.8. Rebooting the Plug-In VA

If you have applied any proxy settings, the plug-in VA requires a reboot to ensure that all services are using the configured proxies.

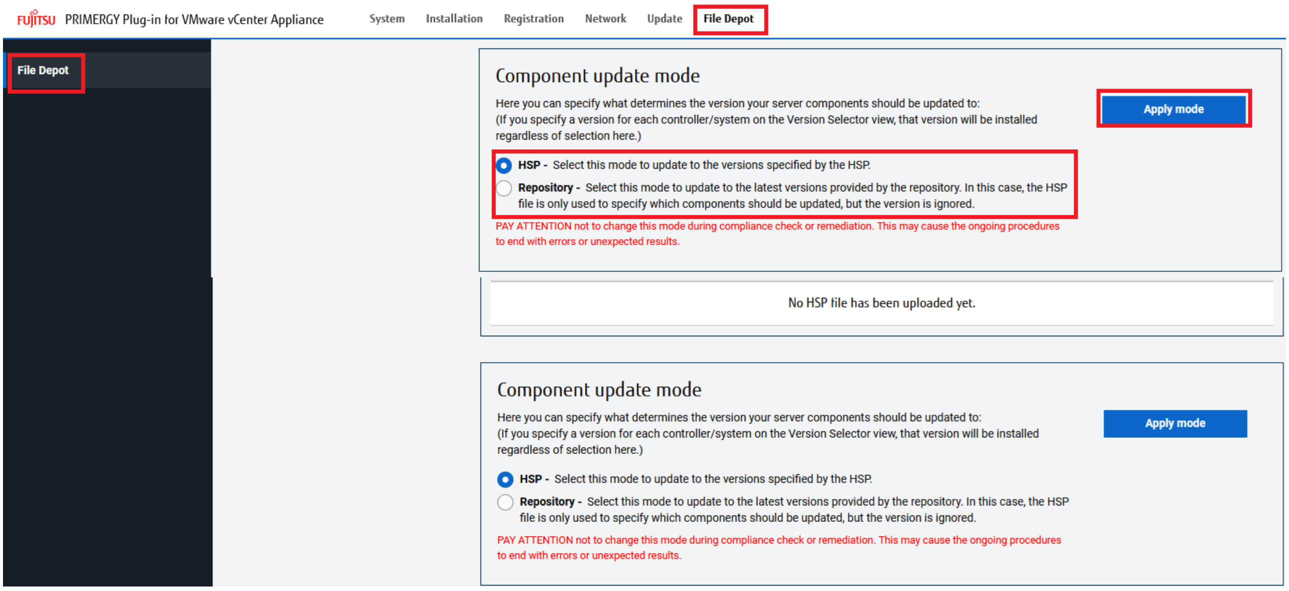
Navigate to [**System**] – [**Information**], click the [**Reboot**] button and click [**Reboot**] to confirm.

Wait a minute until the system is back and login again then.

7.3.9. Component update mode

In this place user can choose one of update components: HSP or latest available by the repository. This applies to all components.

Note	Do not change this option during compliance nor remediation. This may cause the ongoing procedures to end with errors or unexpected results.



Component update mode

Here you can specify what determines the version your server components should be updated to:
(If you specify a version for each controller/system on the Version Selector view, that version will be installed regardless of selection here.)

● **HSP** - Select this mode to update to the versions specified by the HSP.

○ **Repository** - Select this mode to update to the latest versions provided by the repository. In this case, the HSP file is only used to specify which components should be updated, but the version is ignored.

PAY ATTENTION not to change this mode during compliance check or remediation. This may cause the ongoing procedures to end with errors or unexpected results.

Apply mode

No HSP file has been uploaded yet.

Component update mode

Here you can specify what determines the version your server components should be updated to:
(If you specify a version for each controller/system on the Version Selector view, that version will be installed regardless of selection here.)

● **HSP** - Select this mode to update to the versions specified by the HSP.

○ **Repository** - Select this mode to update to the latest versions provided by the repository. In this case, the HSP file is only used to specify which components should be updated, but the version is ignored.

PAY ATTENTION not to change this mode during compliance check or remediation. This may cause the ongoing procedures to end with errors or unexpected results.

Apply mode

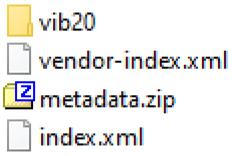
7.3.10. File Depot (HSP Upload)

VMware vLCM requires to provide a Hardware Support Package (HSP) to assist in the firmware and driver update process on the ESXi nodes. This file needs to be downloaded from the FUJITSU Product Support Pages and uploaded to the plug-in VA then.

Download the latest HSP as follows:

1. Open the FUJITSU Product Support Pages.
2. Click the [**Select a new Product**] button.
3. On the pop-up window, select [**Browse for product**], then [**Software**] – [**Infrastructure Manager (ISM)**].
4. Select [**Downloads**] – [**Continue**] and then [**VMware ESXi 7.x**] as the operating system.
5. From the [**Applications**] tab, expand [**Plugins**] and download the following: "**FUJITSU Hardware Support Package (HSP)**"

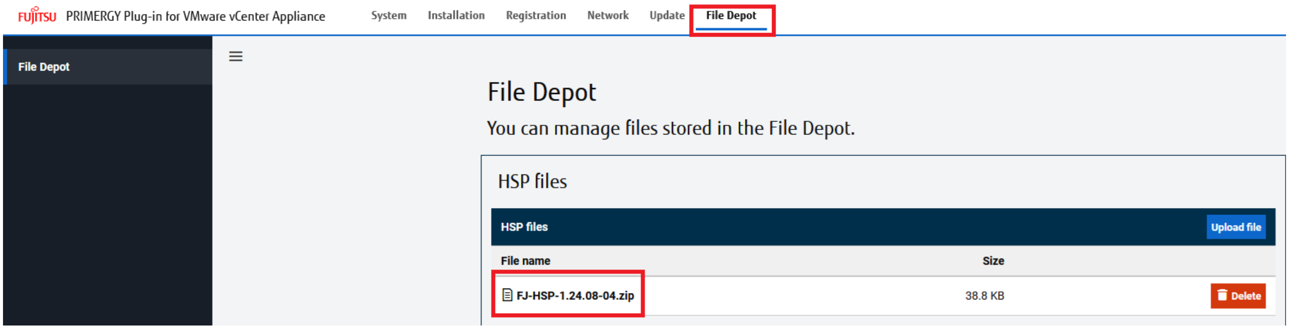
Check the content of the downloaded file and extract the HSP file from it. The HSP file is a zip file with a content similar to this:



vib20
vendor-index.xml
metadata.zip
index.xml

Then upload the extracted HSP zip file to the plug-in VA as follows:

1. On the PRIMERGY Plug-in for VMware vCenter VA Web UI open the [**File Depot**] tab.
2. In the [**HSP files**] frame, click the [**Upload file**] button. This opens a platform-specific file selection dialog on your client device. Navigate to the folder with the **HSP file** which you have downloaded, select it, and confirm to upload it (usually by clicking on [**Open**]).
3. Check whether the uploaded file is listed under [**HSP files**].



File Depot

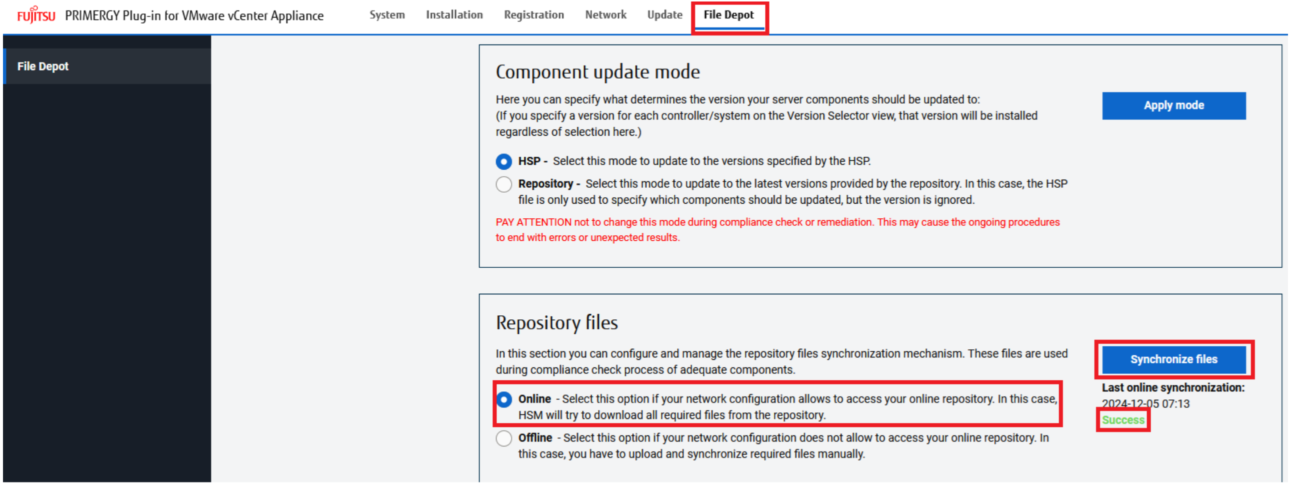
You can manage files stored in the File Depot.

HSP files

File name	Size
FJ-HSP-1.24.08-04.zip	38.8 KB

Note	Please keep in mind that it is possible to upload more than one HSP file but by default, the newest version is going to be used in Custom Version Selector

4. <u>If you have provided a repository URL</u> as described in section “7.3.6 Repository URL and Proxy”, in the [**Repository files**] frame, the [**Online**] method should be already selected. Click on [**Synchronize files**]. Ensure you see a current timestamp and a green [**Success**] message below it then.



Component update mode

Here you can specify what determines the version your server components should be updated to:
(If you specify a version for each controller/system on the Version Selector view, that version will be installed regardless of selection here.)

● **HSP -** Select this mode to update to the versions specified by the HSP.

○ **Repository -** Select this mode to update to the latest versions provided by the repository. In this case, the HSP file is only used to specify which components should be updated, but the version is ignored.

PAY ATTENTION not to change this mode during compliance check or remediation. This may cause the ongoing procedures to end with errors or unexpected results.

Repository files

In this section you can configure and manage the repository files synchronization mechanism. These files are used during compliance check process of adequate components.

● **Online** - Select this option if your network configuration allows to access your online repository. In this case, HSM will try to download all required files from the repository.

○ **Offline** - Select this option if your network configuration does not allow to access your online repository. In this case, you have to upload and synchronize required files manually.

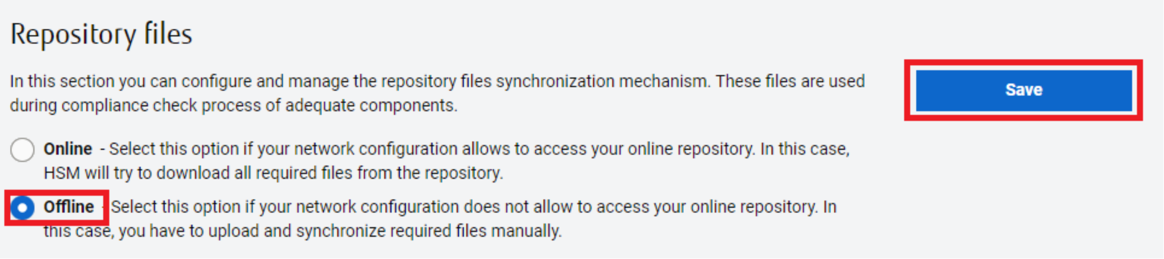
Last online synchronization:
2024-12-05 07:13
Success

5. If you cannot provide a repository URL as described in section “7.3.6 Repository URL and Proxy”, you have to upload the required files “versionAll.txt” and “GF_par_tree.exe” manually.

⚠ Note	The "offline" method described here is explicitly **not recommended**. If possible, you should always use the “online” method, i.e., use a repository as described in section “7.3.6 Repository URL and Proxy”.

First, you need to download the required files to your local device. Open the URL https://support.ts.fujitsu.com/downloadmanager/globalflash/ in your Web browser, right-click on [**versionAll.txt**] and choose your browser’s option to save the linked file (e.g. “Save link as …”). Repeat the same for [**GF_par_tree.exe**].

Next, on the plug-in Web UI, in the [**Repository files**] frame on the [**File Depot**] tab, select [**Offline**] and click on [**Save**].



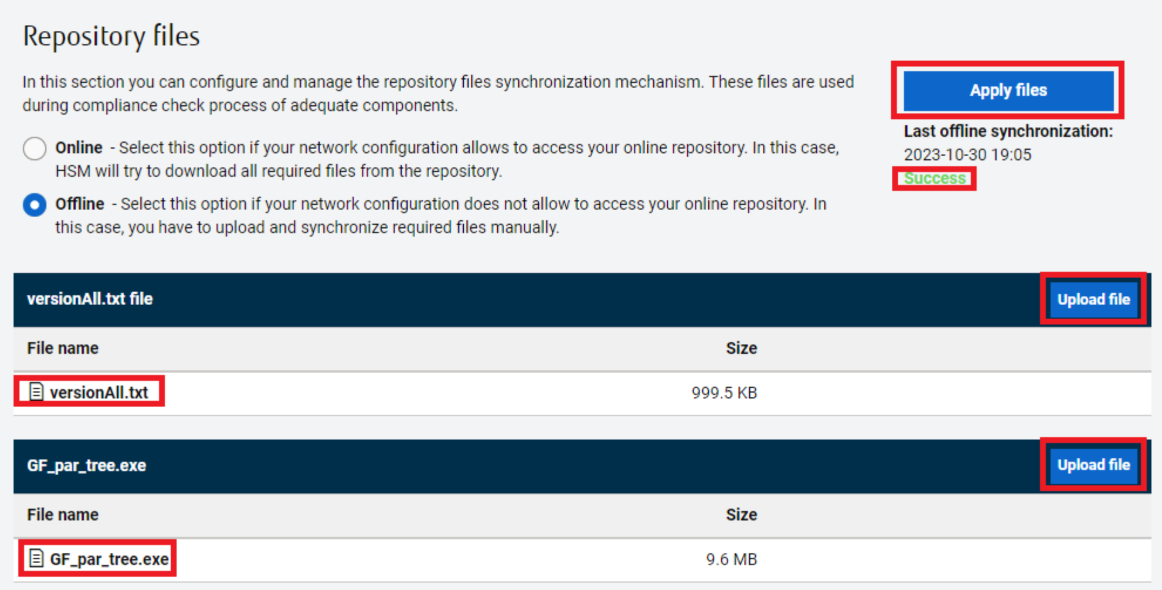
Repository files

In this section you can configure and manage the repository files synchronization mechanism. These files are used during compliance check process of adequate components.

○ **Online** - Select this option if your network configuration allows to access your online repository. In this case, HSM will try to download all required files from the repository.

● **Offline** - Select this option if your network configuration does not allow to access your online repository. In this case, you have to upload and synchronize required files manually.

Now upload both files by clicking on each [**Upload file**] button, selecting and uploading the files, and finally click [**Apply files**]. Ensure you see a current timestamp and a green [**Success**] message below it then.



Repository files

In this section you can configure and manage the repository files synchronization mechanism. These files are used during compliance check process of adequate components.

○ **Online** - Select this option if your network configuration allows to access your online repository. In this case, HSM will try to download all required files from the repository.

● **Offline** - Select this option if your network configuration does not allow to access your online repository. In this case, you have to upload and synchronize required files manually.

Last offline synchronization:
2023-10-30 19:05
Success

versionAll.txt file

File name	Size
versionAll.txt	999.5 KB

GF_par_tree.exe

File name	Size
GF_par_tree.exe	9.6 MB

Now the plug-in is ready to be used by vSphere vLCM as described in the next chapter.

8. Operation

The PRIMERGY Plug-in for VMware vCenter is intended to provide the “Firmware and Drivers Addon” as one part of an image that vLCM uses to manage the lifecycle of a vSphere cluster.

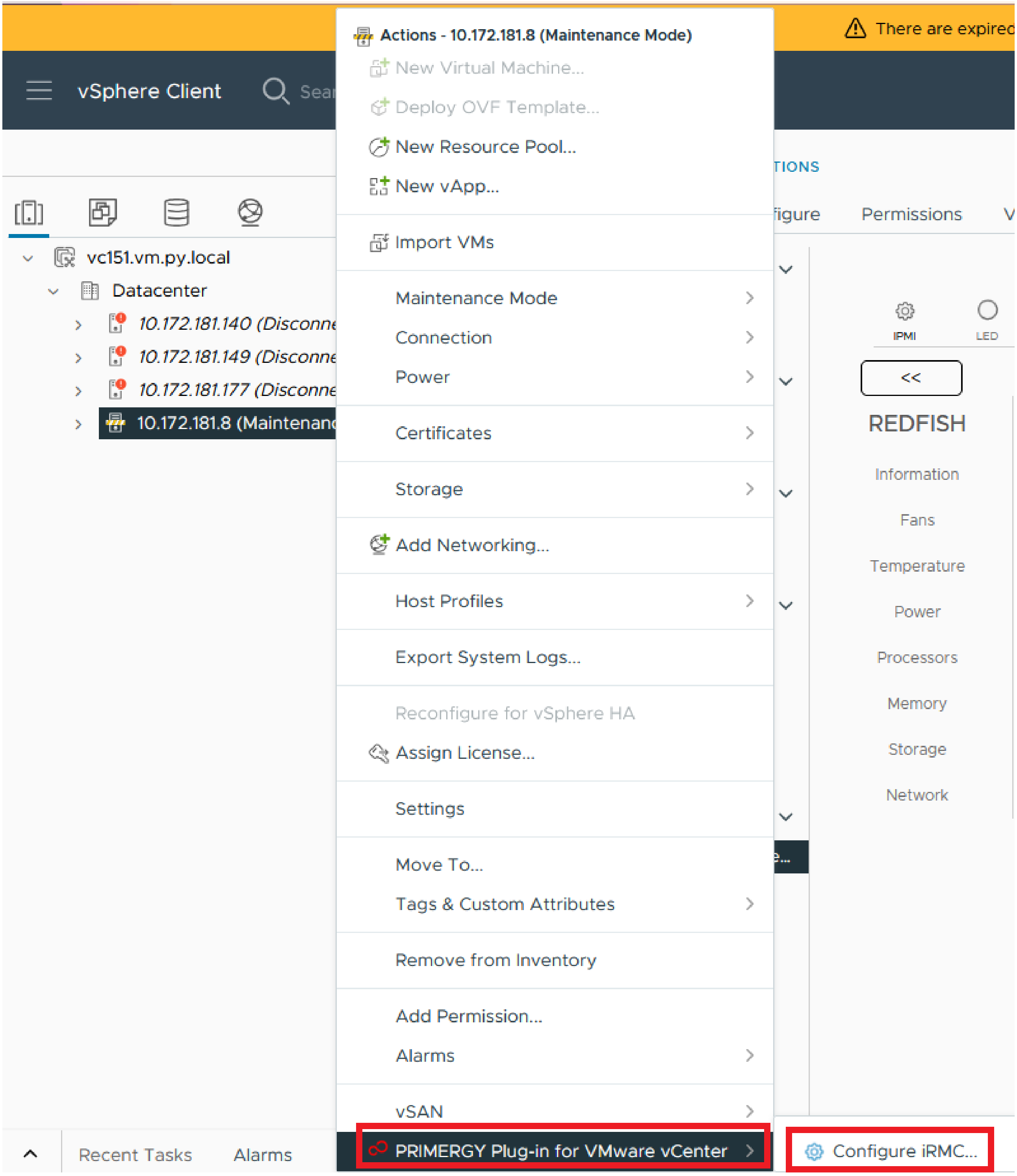
This chapter describes how to connect the plug-in to the vLCM image and how to work with it when maintaining a cluster.

8.1.1. iRMC Configuration of the Cluster Nodes

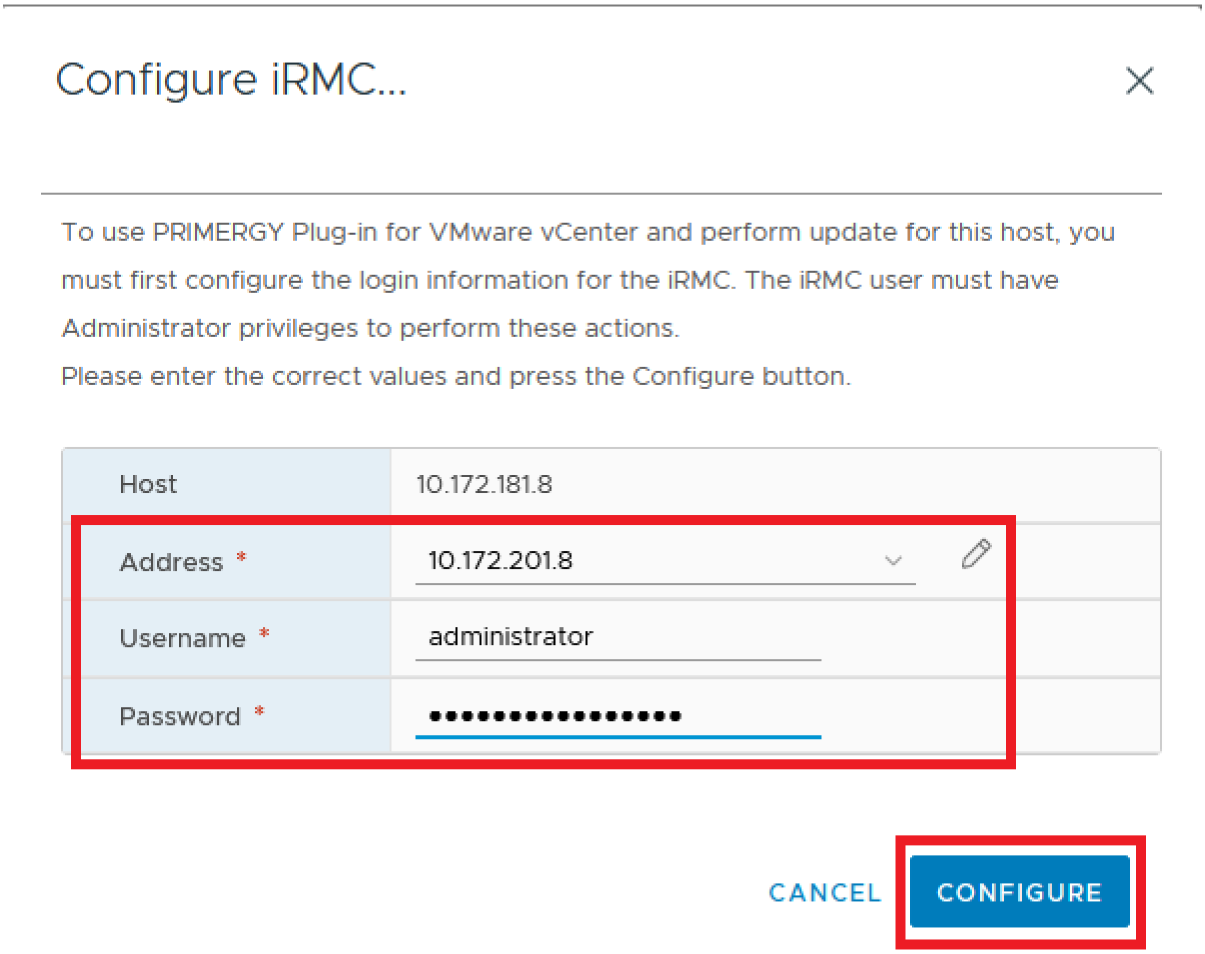
In vSphere Client, the plug-in provides two methods to configure the iRMCs of the cluster nodes: For each node individually or on the cluster level for several at once (bulk configuration).

⚠ Note	When configuring the iRMCs for the first time, even if all iRMCs of the cluster are requiring the same user credentials, you might need to perform the single host configuration. This is because under certain conditions, the bulk configuration is not able to automatically determine the IP address of each iRMC. In case of a later update, e.g., if the password has been changed on several or all nodes, the bulk configuration can be used for it.

- **Single host configuration**
  To configure a single host, right click on the host name, navigate to [**PRIMERGY Plug-in for VMware vCenter**] and choose [**Configure iRMC**].



Then on the opened [**Configure iRMC ...**] dialog, make sure the correct IP address is set behind [**Address**], enter the user credentials to [**Username**] and [**Password**] and click [**CONFIGURE**].



Configure iRMC...

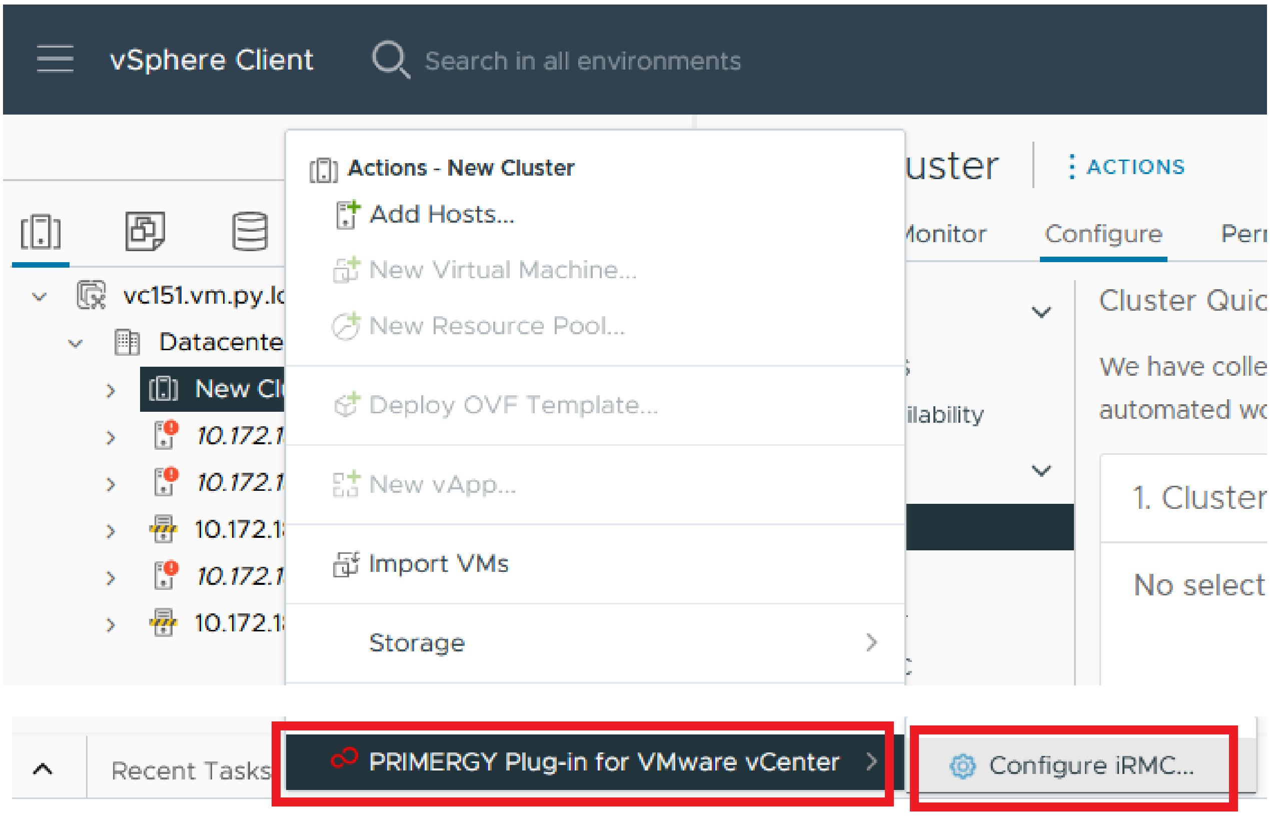
To use PRIMERGY Plug-in for VMware vCenter and perform update for this host, you must first configure the login information for the iRMC. The iRMC user must have Administrator privileges to perform these actions.

Please enter the correct values and press the Configure button.

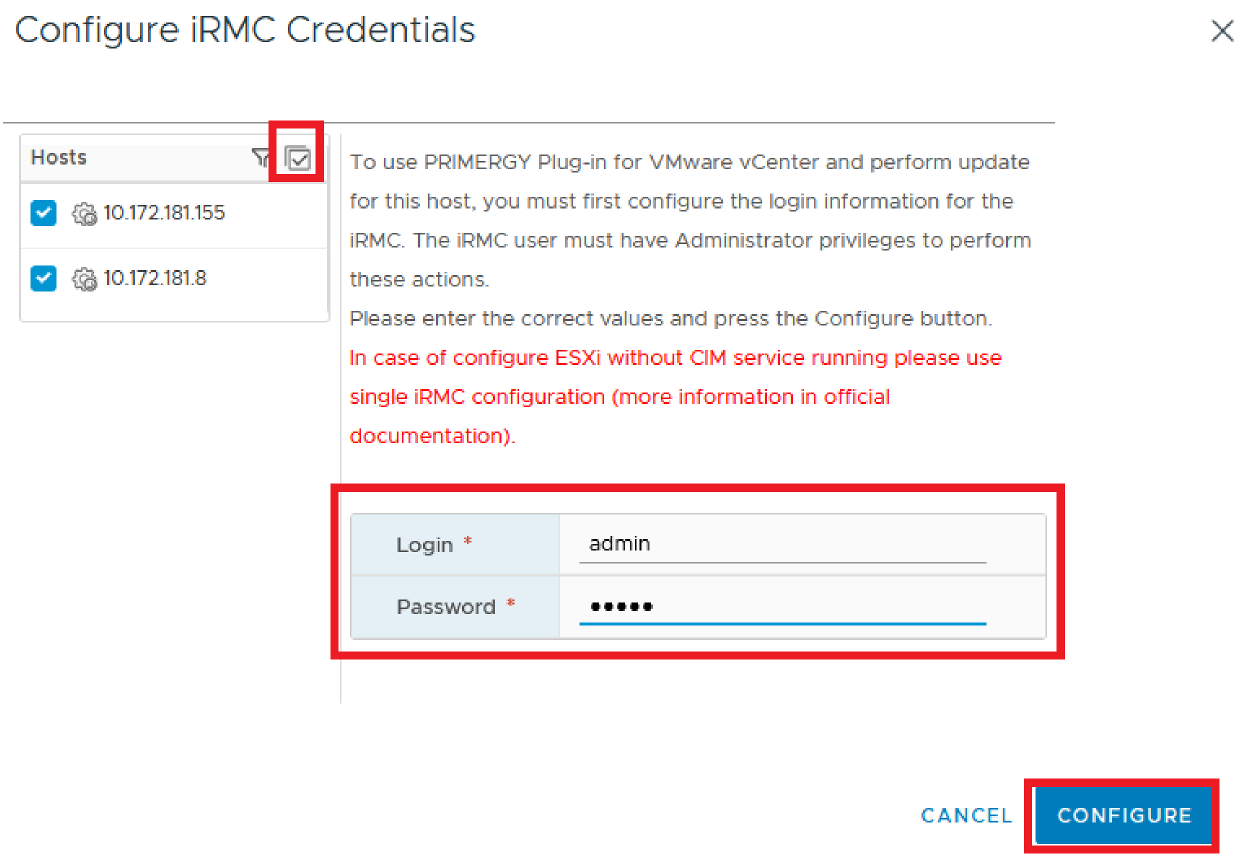
Host	10.172.181.8
Address *	10.172.201.8
Username *	administrator
Password *	●●●●●●●●●●●●●●●●

Wait for the success message and click on [**Close**].
Please note, that due to CIM being dropped from support for ESXi hosts, you might be required to input [**Address**] manually.

- **Bulk configuration**
  To configure multiple hosts at once, right click on the [**cluster name**], navigate to [**PRIMERGY Plug-in for VMware vCenter**] and choose [**Configure iRMC**].



Then on the opened [**Configure iRMC Credentials**] dialog, select the [**Hosts**] to configure, enter the [**Login**] and [**Password**] values and click [**CONFIGURE**].


Configure iRMC Credentials

Hosts
☑ 10.172.181.155
☑ 10.172.181.8

To use PRIMERGY Plug-in for VMware vCenter and perform update for this host, you must first configure the login information for the iRMC. The iRMC user must have Administrator privileges to perform these actions.

Please enter the correct values and press the Configure button.

In case of configure ESXi without CIM service running please use single iRMC configuration (more information in official documentation).

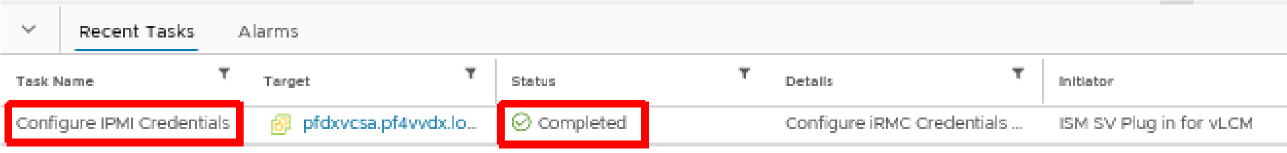
Login * admin

Password * •••••

Confirm the dialog to [**Start the iRMC Configure Task**] by clicking [**OK**].

Also click [**OK**] to close another dialog informing you about the start of the task.

Then monitor it in [**Recent Tasks**] until its [**Status**] is shown as [**Completed**].



Task Name	Target	Status	Details	Initiator
Configure IPMI Credentials	pfdxvcsa.pf4vvdx.lo...	Completed	Configure iRMC Credentials ...	ISM SV Plug in for vLCM

It is possible to perform an iRMC credentials update using designated API endpoint.

Note	Bulk configuration is only available for hosts that have CIM provider installed.

8.1.2. Managing the iRMC Credentials via REST API

As an alternative to the graphical configuration on the vSphere Client, there is an option of using the REST API to register the iRMC credentials of the hosts to be managed.

To do so, a POST request must be sent to the following address:

https://<applianceIp>:<portHsmApi>/hsm_api/configureHostsIrmcCredentials

Description of the variables:

<applianceIp>: The IP address or FQDN of the PRIMERGY Plug-in for VMware vCenter VA.

<portHsmApi>: The HTTPS port number of the “vCenter Plug-in Service Station” (default: 3170). You find the actual configured value on the [**Installation**] tab of the Plug-in VA’s UI, see section “7.3.4 vCenter Server Connectivity”.

Note	This API call requires Basic Auth using credentials used for registering Plug-in. After 5 failed attempts user is getting locked for 10 minutes.

The header of the request must include the following:

- ‘Content-Type: application/json’

Required JSON format body for the request:

```
[
        {
                “irmcAddress”: String,
                “username”: String,
                “password”: String,
                “hostName”: String
        }
]
```

Note	Please keep in mind that the REST API is expecting an array of hosts. Therefore, even if only the credentials of a single host are to be registered or updated, the specification must be made in the form of an array element.

Description of the necessary input:

- <irmcAddress>: The iRMC address of the ESXi host.
- <username>: The iRMC account name to be used (requires the Administrator role!).
- <password>: Password of the specified account.
- <hostName>: The ESXi host IP address or FQDN.

Expected response from the API:

- Response code: 202
- Response body:

```
{
        “taskStatus”: SUCCEEDED / FAILED / PARTLY_SUCCEEDED,
        “failedHostsList”: [String],
        “additionalInfo”: String
}
```

Description of the response:

- <taskStatus>: Status of the task configuring the iRMC credentials of the ESXi hosts:
  - SUCCEEDED: The configuration was successful for all hosts.
  - FAILED: The configuration failed for all the hosts.
  - PARTLY_FAILED: The configuration failed for some of the hosts
- <failedHostsList>: List of hosts (IP addresses) for which the configuration has failed. The list will be empty if <taskStatus> is <SUCCEEDED>.
- <additionalInfo>: Additional information explaining why <taskStatus> is not <SUCCEEDED>. This information will be empty if <taskStatus> is <SUCCEEDED>.

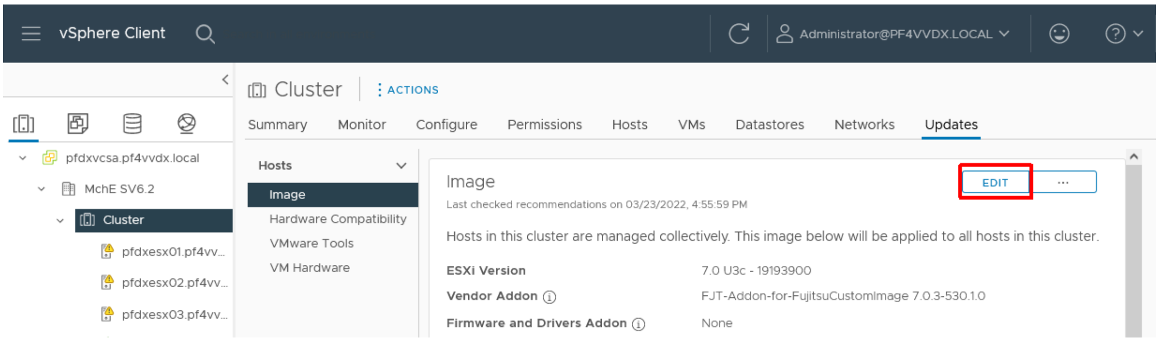
8.2. Connecting the Plug-In to a Single Image in vLCM

It is assumed that the cluster is already configured to be managed by vLCM using a single image. That means the vCenter Server is already prepared to provide latest patches and the FUJITSU Addon.

If you need to prepare the vLCM image from scratch, proceed as described in “Appendix C: Configuring vSphere Lifecycle Manager”.

Perform the following steps to connect this plug-in to an already existing vLCM single image:

1. Login to the vSphere Client as a user having the privileges to configure and use vLCM.
2. In the [**Inventory**], open the [**Host and Clusters**] view, click the [**<cluster name>**], open the [**Update**] tab and click on [**EDIT**].



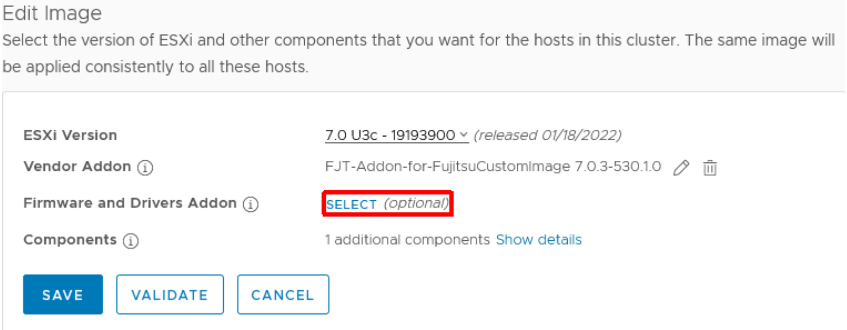
Image

Last checked recommendations on 03/23/2022, 4:55:59 PM

Hosts in this cluster are managed collectively. This image below will be applied to all hosts in this cluster.

ESXi Version	7.0 U3c - 19193900
Vendor Addon	FJT-Addon-for-FujitsuCustomImage 7.0.3-530.1.0
Firmware and Drivers Addon	None

3. On the opened [**Edit Image**] window behind [**Firmware and Drivers Addon**], click [**SELECT**].

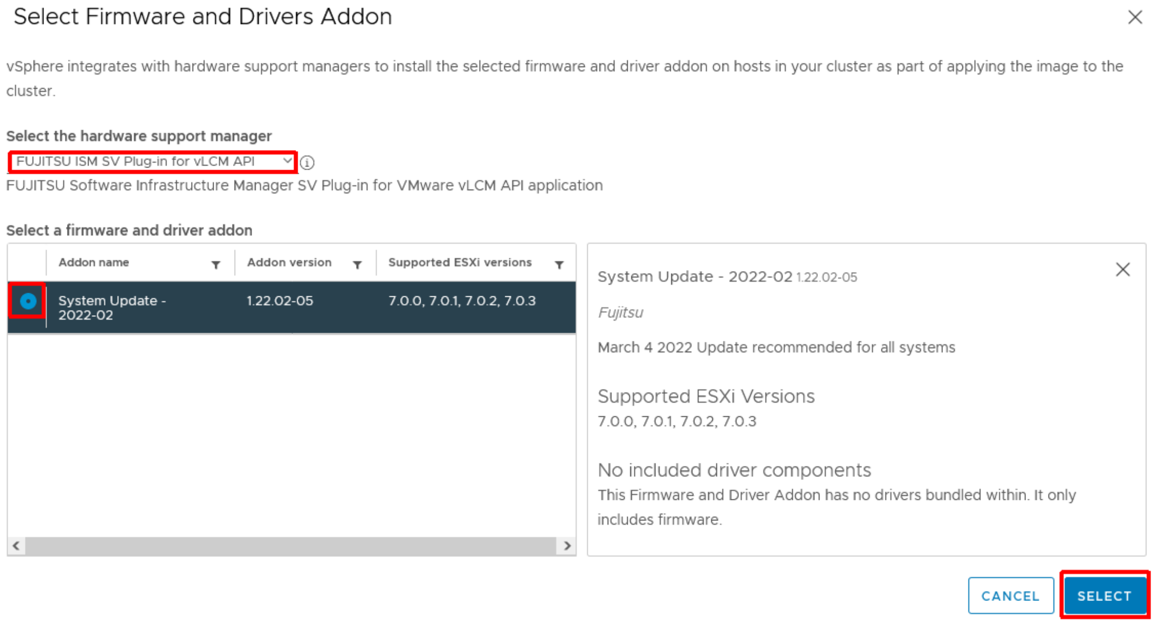


Edit Image

Select the version of ESXi and other components that you want for the hosts in this cluster. The same image will be applied consistently to all these hosts.

ESXi Version	7.0 U3c - 19193900 (released 01/18/2022)
Vendor Addon	FJT-Addon-for-FujitsuCustomImage 7.0.3-530.1.0
Firmware and Drivers Addon	SELECT (optional)
Components	1 additional components Show details

4. On the opened [**Select Firmware and Drivers Addon**] window, from the drop-down box below [**Select the hardware support manager**], select [**PRIMERGY Plug-in for VMware vCenter**]. Then select the matching update from the [**Select a firmware and driver addon**] list, review the details provided on the right window frame and click the [**SELECT**] button.



Select Firmware and Drivers Addon

vSphere integrates with hardware support managers to install the selected firmware and driver addon on hosts in your cluster as part of applying the image to the cluster.

Select the hardware support manager

FUJITSU ISM SV Plug-in for vLCM API

FUJITSU Software Infrastructure Manager SV Plug-in for VMware vLCM API application

Select a firmware and driver addon

Addon name	Addon version	Supported ESXi versions
System Update - 2022-02	1.22.02-05	7.0.0, 7.0.1, 7.0.2, 7.0.3

System Update - 2022-02 1.22.02-05

Fujitsu

March 4 2022 Update recommended for all systems

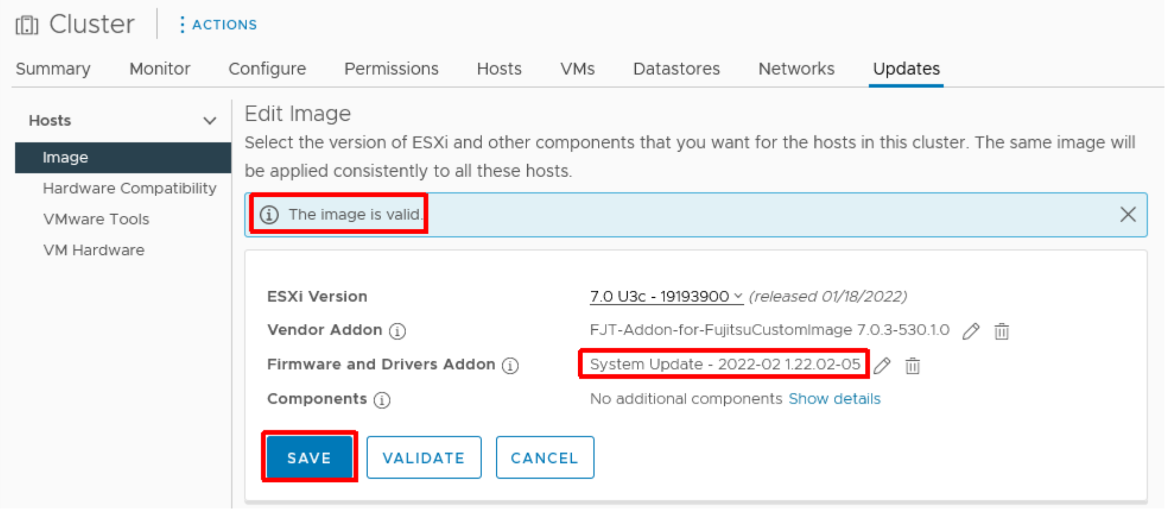
Supported ESXi Versions

7.0.0, 7.0.1, 7.0.2, 7.0.3

No included driver components

This Firmware and Driver Addon has no drivers bundled within. It only includes firmware.

5. Click the [**VALIDATE**] button.
If a message states [**The images is valid**], click the [**SAVE**] button. This will initiate a compliance check implicitly.



Edit Image

Select the version of ESXi and other components that you want for the hosts in this cluster. The same image will be applied consistently to all these hosts.

The image is valid.

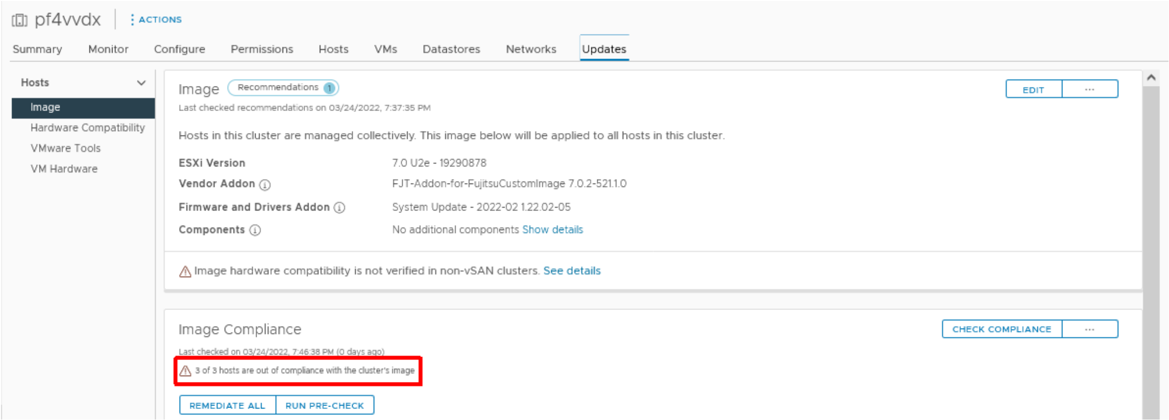
ESXi Version: 7.0 U3c - 19193900 *(released 01/18/2022)*

Vendor Addon: FJT-Addon-for-FujitsuCustomImage 7.0.3-530.1.0

Firmware and Drivers Addon: System Update - 2022-02 1.22.02-05

Components: No additional components Show details

6. Wait until the compliance check completes and check for success. For details refer to VMware's description of the Compliance States. If any host is reported as incompatible, make sure you are using supported hardware and the images uses FUJITSU Addon components supporting the selected ESXi version.



Image

Last checked recommendations on 03/24/2022, 7:37:35 PM

Hosts in this cluster are managed collectively. This image below will be applied to all hosts in this cluster.

ESXi Version	7.0 U2e - 19290878
Vendor Addon ⓘ	FJT-Addon-for-FujitsuCustomImage 7.0.2-521.1.0
Firmware and Drivers Addon ⓘ	System Update - 2022-02 1.22.02-05
Components ⓘ	No additional components Show details

⚠ Image hardware compatibility is not verified in non-vSAN clusters. See details

Image Compliance

Last checked on 03/24/2022, 7:46:38 PM (0 days ago)

⚠ 3 of 3 hosts are out of compliance with the cluster's image

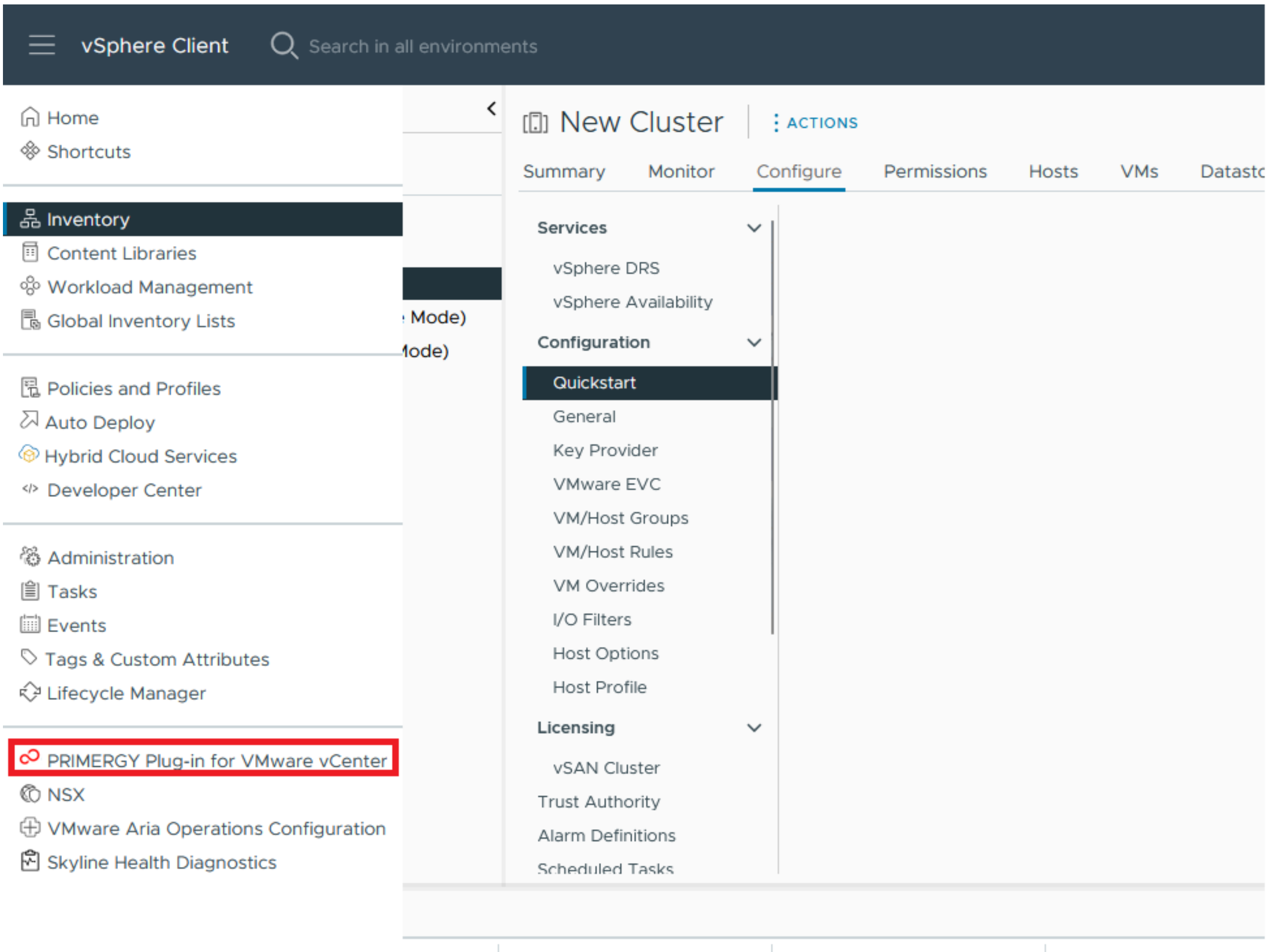
8.3. Custom Version Selector

If the user desires, custom versions for components can be set.

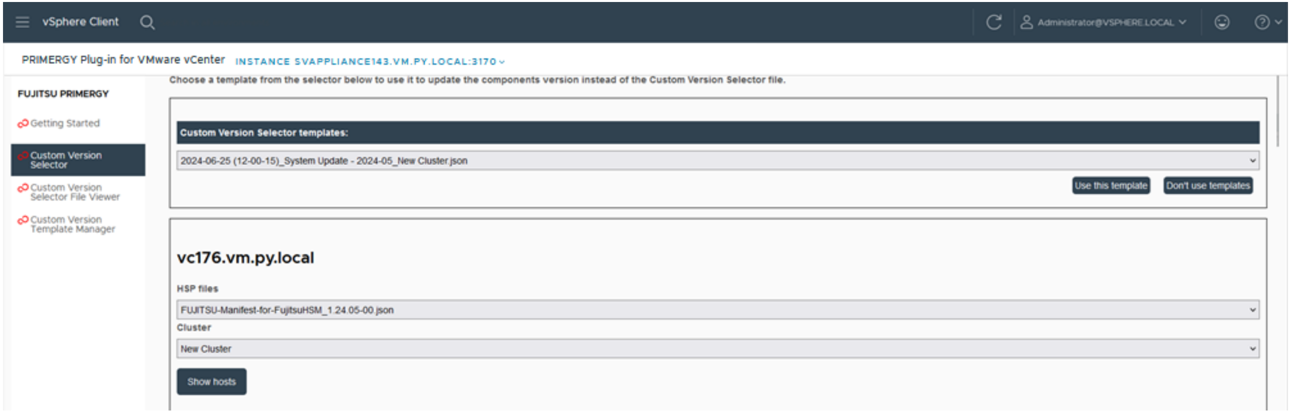
⚠ Note	Please keep in mind that if the user specifies a version for each controller/system on the Custom Version Selector view, selected version will be saved and used as a desired version to be upgraded to until not overwritten

Custom Version Selector allows users to pick a version to which the component could be updated to instead of updating it to HSP or the newest one. For the functionality to work properly the user needs to ensure that a proper configuration has been performed (for that please be sure that all the steps from the point 6. “Deployment” has been properly followed)

Custom Version Selector can be found under **[Main menu]** -> **[PRIMERGY Plug-in for VMware vCenter]**



After opening the Custom Version Selector tab, data regarding clusters, vCenter and uploaded HSP files are getting fetched.


vSphere Client
Administrator@VSPHERE.LOCAL
PRIMERGY Plug-in for VMware vCenter
INSTANCE SVAPPLIANCE143.VM.PY.LOCAL:3170
FUJITSU PRIMERGY
Getting Started
Custom Version Selector
Custom Version Selector File Viewer
Custom Version Template Manager
Use this template
Don't use templates
Show hosts

Choose a template from the selector below to use it to update the components version instead of the Custom Version Selector file.

Custom Version Selector templates:

2024-06-25 (12-00-15)_System Update - 2024-05_New Cluster.json

vc176.vm.py.local

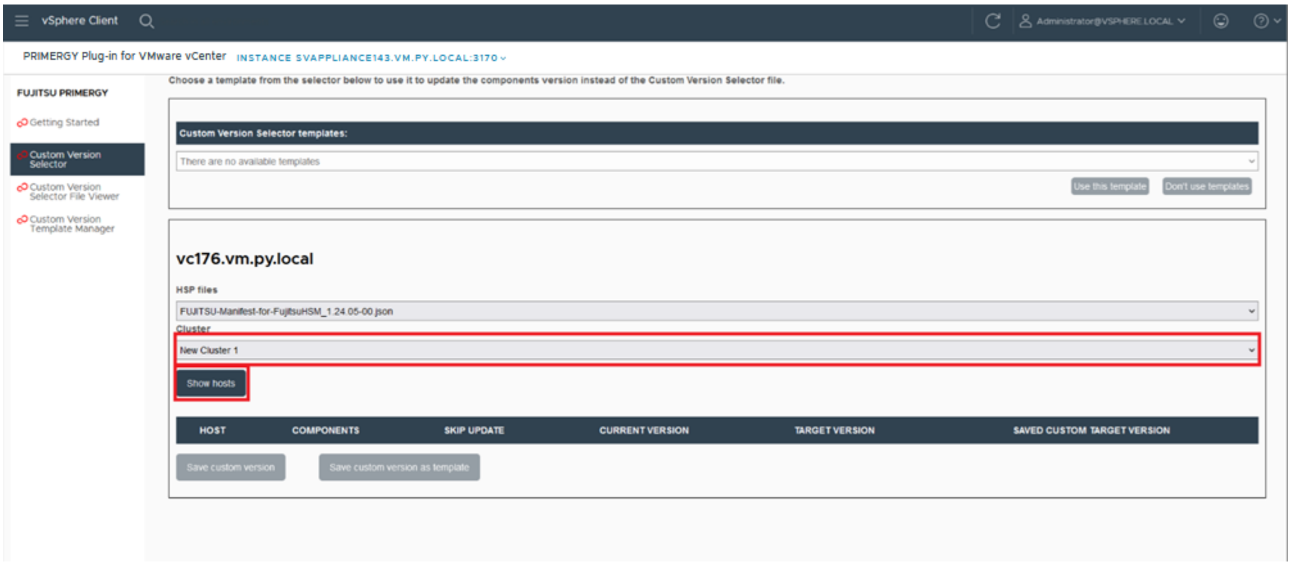
HSP files: FUJITSU-Manifest-for-FujitsuHSM_1.24.05-00.json

Cluster: New Cluster

Tip

As for now, Custom Version Selector is working only with HSP. There is no alternative for Newest Version mode, therefore please remember to set it properly in Plug-in appliance.

When the loading process is complete, the user can select a cluster from which to set a custom firmware version for hosts' components firmware updates. **[Standalone hosts]** option indicates that the user wishes to customize hosts which are not in any cluster.


vSphere Client
Administrator@VSPHERE.LOCAL
PRIMERGY Plug-in for VMware vCenter
INSTANCE SVAPPLIANCE143.VM.PY.LOCAL:3170
FUJITSU PRIMERGY
Getting Started
Custom Version Selector
Custom Version Selector File Viewer
Custom Version Template Manager
Use this template
Don't use templates
Show hosts
Save custom version
Save custom version as template

Choose a template from the selector below to use it to update the components version instead of the Custom Version Selector file.

Custom Version Selector templates: There are no available templates

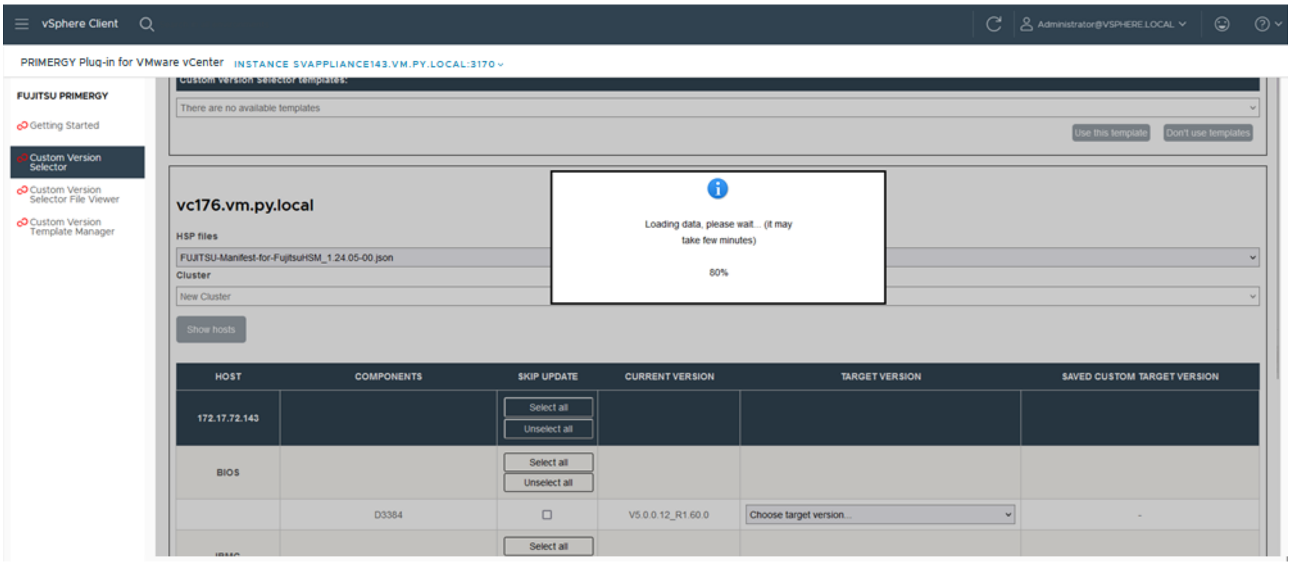
vc176.vm.py.local

HSP files: FUJITSU-Manifest-for-FujitsuHSM_1.24.05-00.json

Cluster: New Cluster 1

HOST	COMPONENTS	SKIP UPDATE	CURRENT VERSION	TARGET VERSION	SAVED CUSTOM TARGET VERSION

After selecting desired option, clicking **[Show hosts]** button starts a process of collecting data related to hosts inventories. Only hosts that are connected, with configured iRMC credentials.


vSphere Client
Administrator@VSPHERE.LOCAL
PRIMERGY Plug-in for VMware vCenter
INSTANCE SVAPPLIANCE143.VM.PY.LOCAL:3170
FUJITSU PRIMERGY
Getting Started
Custom Version Selector
Custom Version Selector File Viewer
Custom Version Template Manager
Use this template
Don't use templates
Show hosts

Custom Version Selector templates: There are no available templates

vc176.vm.py.local

HSP files: FUJITSU-Manifest-for-FujitsuHSM_1.24.05-00.json

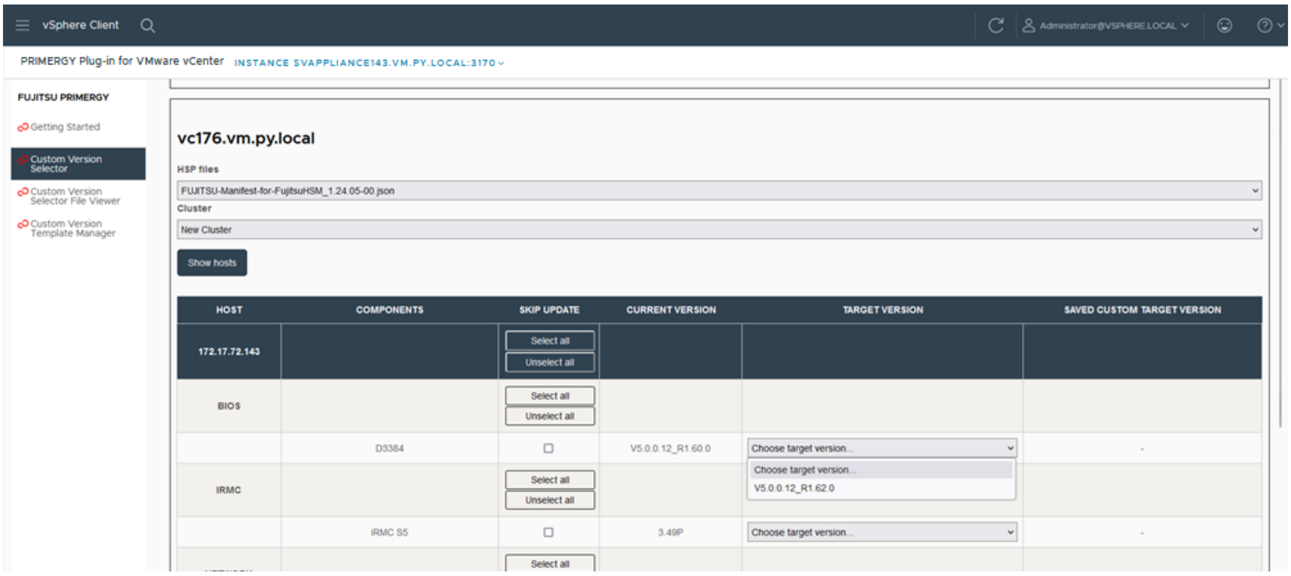
Cluster: New Cluster

Loading data, please wait... (it may take few minutes)

80%

HOST	COMPONENTS	SKIP UPDATE	CURRENT VERSION	TARGET VERSION	SAVED CUSTOM TARGET VERSION
172.17.72.143		Select all Unselect all			
BIOS		Select all Unselect all			
	D3384	□	V5.0.0.12_R1.60.0	Choose target version...	-
iRMC		Select all			

After inventory data collection is finished, user gets a list displayed in the web UI. In the given example below.


vSphere Client
Administrator@VSPHERE.LOCAL
PRIMERGY Plug-in for VMware vCenter
INSTANCE SVAPPLIANCE143.VM.PY.LOCAL:3170
FUJITSU PRIMERGY
Getting Started
Custom Version Selector
Custom Version Selector File Viewer
Custom Version Template Manager
Show hosts
Select all
Unselect all

vc176.vm.py.local

HSP files: FUJITSU-Manifest-for-FujtsuHSM_1.24.05-00.json

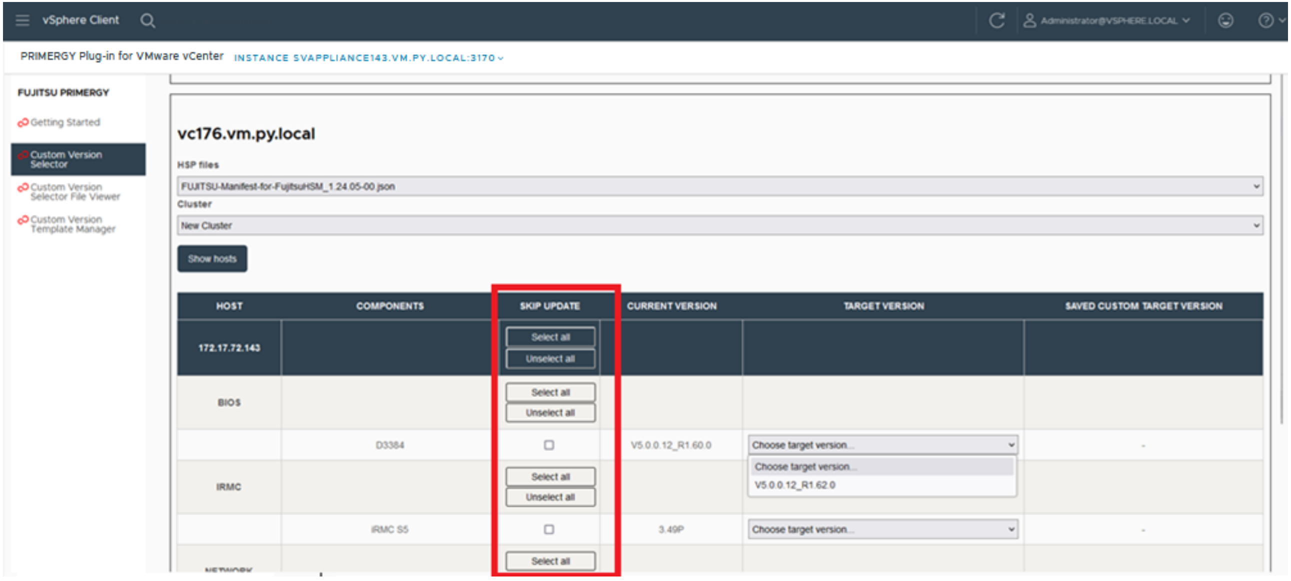
Cluster: New Cluster

HOST	COMPONENTS	SKIP UPDATE	CURRENT VERSION	TARGET VERSION	SAVED CUSTOM TARGET VERSION
172.17.72.143		Select all Unselect all			
BIOS		Select all Unselect all			
	D3384	□	V5.0.0.12_R1.60.0	Choose target version... Choose target version... V5.0.0.12_R1.62.0	-
IRMC		Select all Unselect all			
	IRMC S5	□	3.49P	Choose target version...	-
		Select all			

User can select custom version for each desired component or leave the field in a default option (**[Choose target version]**). If default option will get selected, components won't have a custom version selected and, in case of remediation, will be updated to version defined in HSP.

Tip	Keep in mind that choosing default option is also a way of changing saved custom selected version for component for defined in HSP file or the newest one for the firmware update in case of remediation.

If user is willing not to update host of any of its components, he may want to use "Skip Update" option, where anything ticked won't be updated during remediation.


vSphere Client
Administrator@VSPHERE.LOCAL
PRIMERGY Plug-in for VMware vCenter
INSTANCE SVAPPLIANCE143.VM.PY.LOCAL:3170
FUJITSU PRIMERGY
Getting Started
Custom Version Selector
Custom Version Selector File Viewer
Custom Version Template Manager
Show hosts
Select all
Unselect all

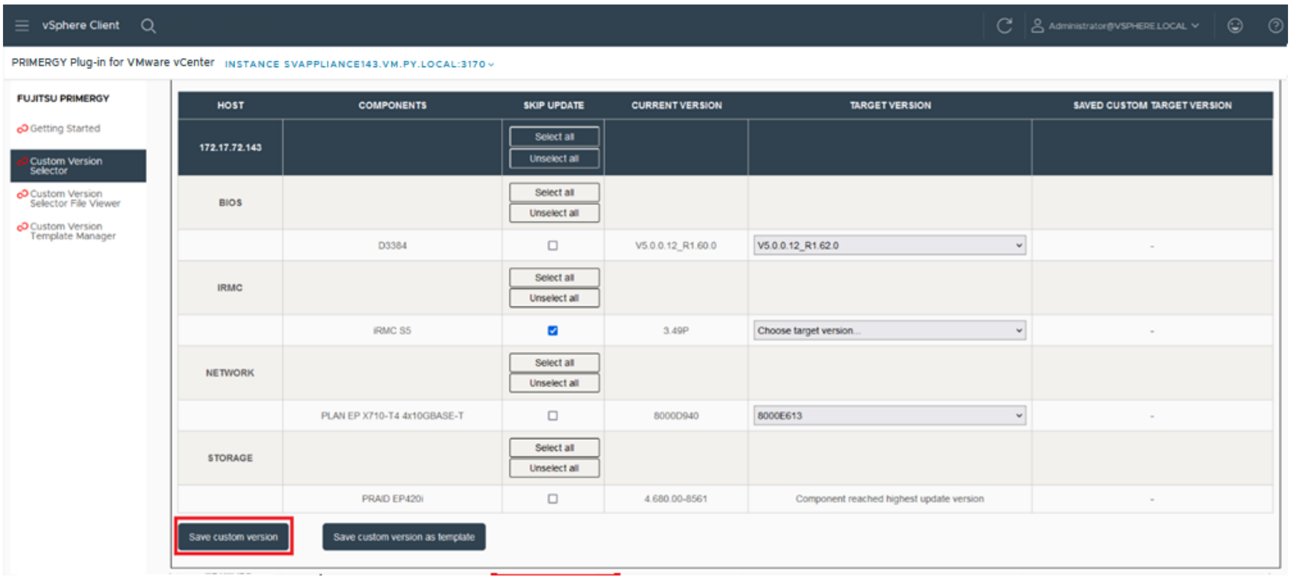
vc176.vm.py.local

HSP files: FUJITSU-Manifest-for-FujtsuHSM_1.24.05-00.json

Cluster: New Cluster

HOST	COMPONENTS	SKIP UPDATE	CURRENT VERSION	TARGET VERSION	SAVED CUSTOM TARGET VERSION
172.17.72.143		Select all Unselect all			
BIOS		Select all Unselect all			
	D3384	□	V5.0.0.12_R1.60.0	Choose target version... Choose target version... V5.0.0.12_R1.62.0	-
IRMC		Select all Unselect all			
	IRMC S5	□	3.49P	Choose target version...	-
		Select all			

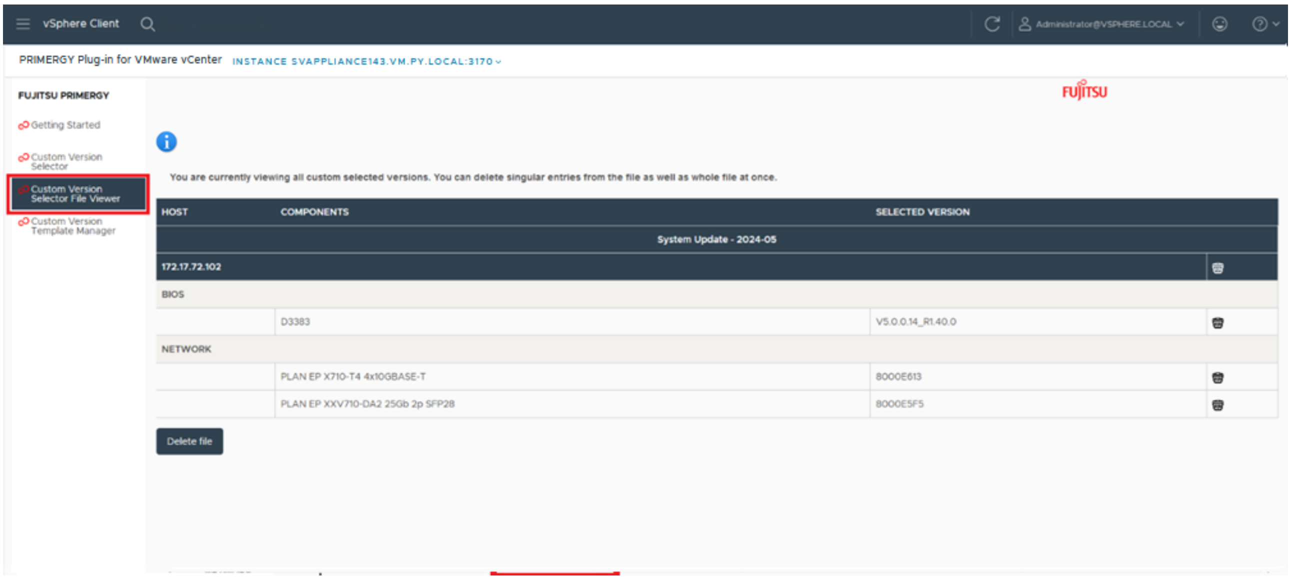
After clicking **[Save custom version]** button, an information appears for the user and new data about custom selected versions for components is being saved. This data is going to be used during compliance check and displayed as a **[Image Version]** for component. During the remediation process, component will be updated to this version.


vSphere Client
Administrator@VSPHERE.LOCAL
PRIMERGY Plug-in for VMware vCenter
INSTANCE SVAPPLIANCE143.VM.PY.LOCAL:3170
FUJITSU PRIMERGY
Getting Started
Custom Version Selector
Custom Version Selector File Viewer
Custom Version Template Manager
Save custom version
Save custom version as template

HOST	COMPONENTS	SKIP UPDATE	CURRENT VERSION	TARGET VERSION	SAVED CUSTOM TARGET VERSION
172.17.72.143		Select all Unselect all			
BIOS		Select all Unselect all			
	D3384	□	V5.0.0.12_R1.60.0	V5.0.0.12_R1.62.0	-
IRMC		Select all Unselect all			
	iRMC S5	☑	3.49P	Choose target version...	-
NETWORK		Select all Unselect all			
	PLAN EP X710-T4 4x10GBASE-T	□	8000D940	8000E613	-
STORAGE		Select all Unselect all			
	PRAID EP420i	□	4.680.00-8561	Component reached highest update version	-

Note	Keep in mind that Custom Version Selector can display versions which are older than currently installed for the component. In case of choosing this option, downgrading won't be performed

After user will save custom versions, they can be viewed and deleted in Custom Version Selector File Viewer.

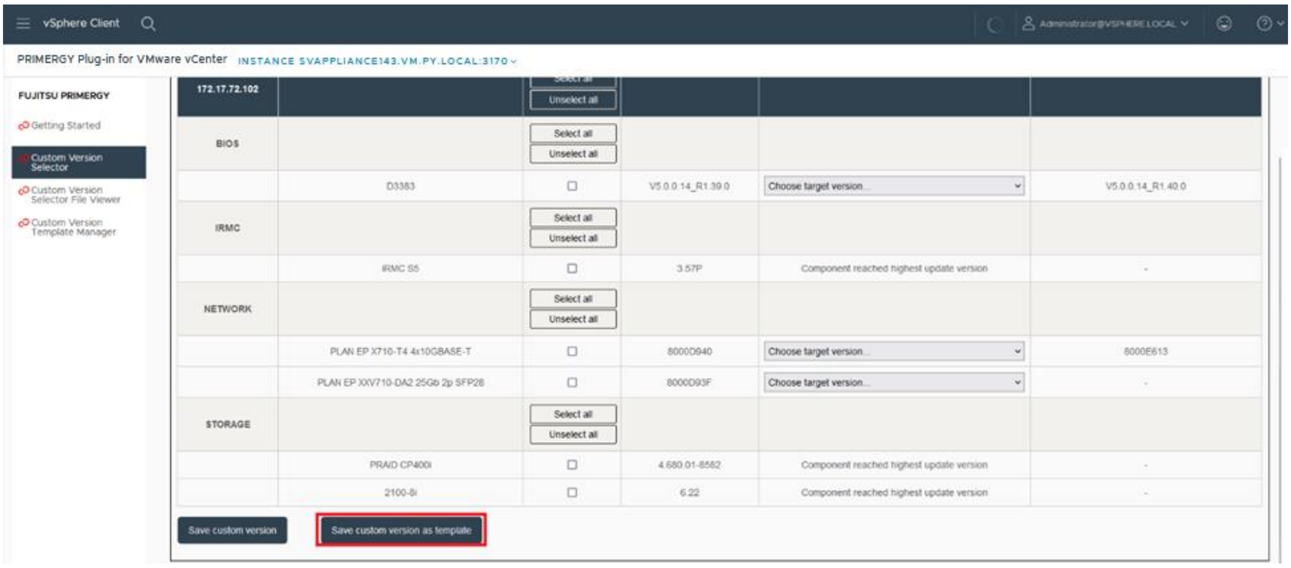

vSphere Client
Administrator@VSPHERE.LOCAL
PRIMERGY Plug-in for VMware vCenter
INSTANCE SVAPPLIANCE143.VM.PY.LOCAL:3170
FUJITSU PRIMERGY
Getting Started
Custom Version Selector
Custom Version Selector File Viewer
Custom Version Template Manager
FUJITSU
Delete file

You are currently viewing all custom selected versions. You can delete singular entries from the file as well as whole file at once.

HOST	COMPONENTS	SELECTED VERSION	
System Update - 2024-05			
172.17.72.102			🗑
BIOS			
	D3383	V5.0.0.14_R1.40.0	🗑
NETWORK			
	PLAN EP X710-T4 4x10GBASE-T	8000E613	🗑
	PLAN EP XXV710-DA2 25Gb 2p SFP28	8000E5F5	🗑

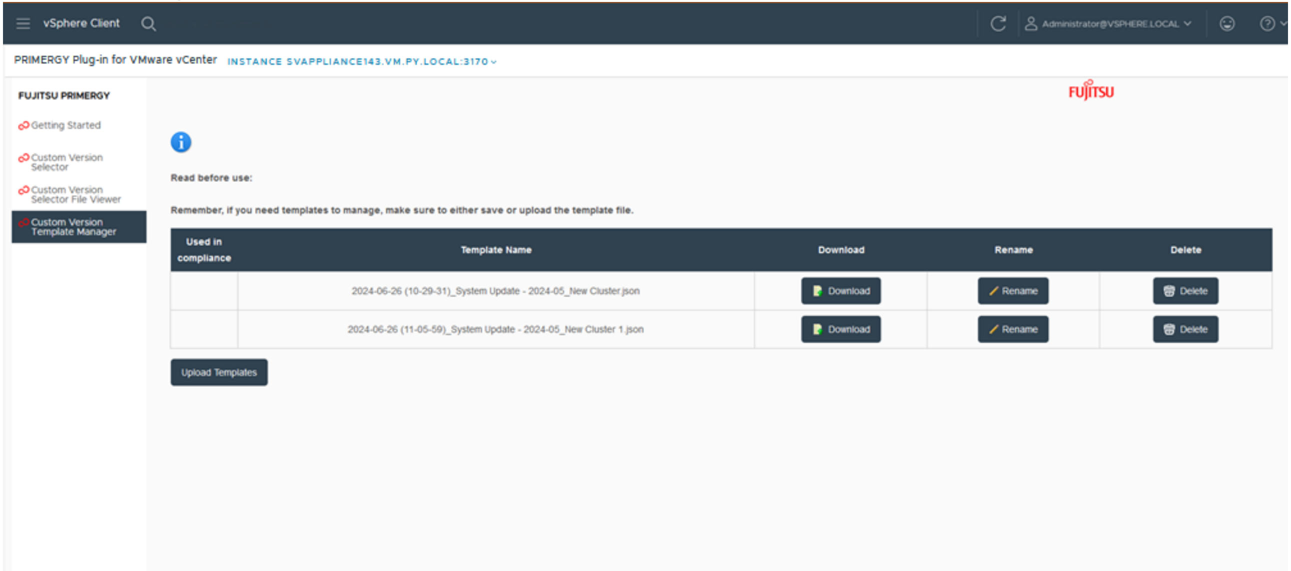
8.4. Custom Version Template Manager

In case when user may want to use variety of custom versions, Custom Version Templates may become handy. After declaring target versions in Custom Version Selector there is button to "Save custom version as template"


vSphere Client
Administrator@VSPHERE.LOCAL
PRIMERGY Plug-in for VMware vCenter
INSTANCE SVAPPLIANCE143.VM.PY.LOCAL:3170
FUJITSU PRIMERGY
Getting Started
Custom Version Selector
Custom Version Selector File Viewer
Custom Version Template Manager
Save custom version
Save custom version as template

172.17.72.102		Select all Unselect all			
BIOS		Select all Unselect all			
	D3383	□	V5.0.0.14_R1.39.0	Choose target version...	V5.0.0.14_R1.40.0
IRMC		Select all Unselect all			
	iRMC S5	□	3.57P	Component reached highest update version	-
NETWORK		Select all Unselect all			
	PLAN EP X710-T4 4x10GBASE-T	□	8000D940	Choose target version...	8000E613
	PLAN EP XXV710-DA2 25Gb 2p SFP28	□	8000D93F	Choose target version...	-
STORAGE		Select all Unselect all			
	PRAID CP400i	□	4.680.01-8582	Component reached highest update version	-
	2100-8i	□	6.22	Component reached highest update version	-

After hitting this button, saved template will be visible at the Custom Version Template Manager. By default, its name is created from using date, time, HSP and cluster names. These can be changed in this view.


vSphere Client
Administrator@VSPHERE.LOCAL
PRIMERGY Plug-in for VMware vCenter
INSTANCE SVAPPLIANCE143.VM.PY.LOCAL:3170
FUJITSU PRIMERGY
Getting Started
Custom Version Selector
Custom Version Selector File Viewer
Custom Version Template Manager
FUJITSU
Upload Templates

Read before use:

Remember, if you need templates to manage, make sure to either save or upload the template file.

Used in compliance	Template Name	Download	Rename	Delete
	2024-06-26 (10-29-31)_System Update - 2024-05_New Cluster.json	Download	Rename	Delete
	2024-06-26 (11-05-59)_System Update - 2024-05_New Cluster 1.json	Download	Rename	Delete

Note	Do not change name of templates manually. If you wish to have other name for this file, please use “Rename” button before exporting it from Plug-in.

8.5. Troubleshooting collecting data related to hosts inventories

In case of an issue where the Custom Version Selector is loading components for its hosts and does not proceed (observed around 80% of progress), please ensure the following:

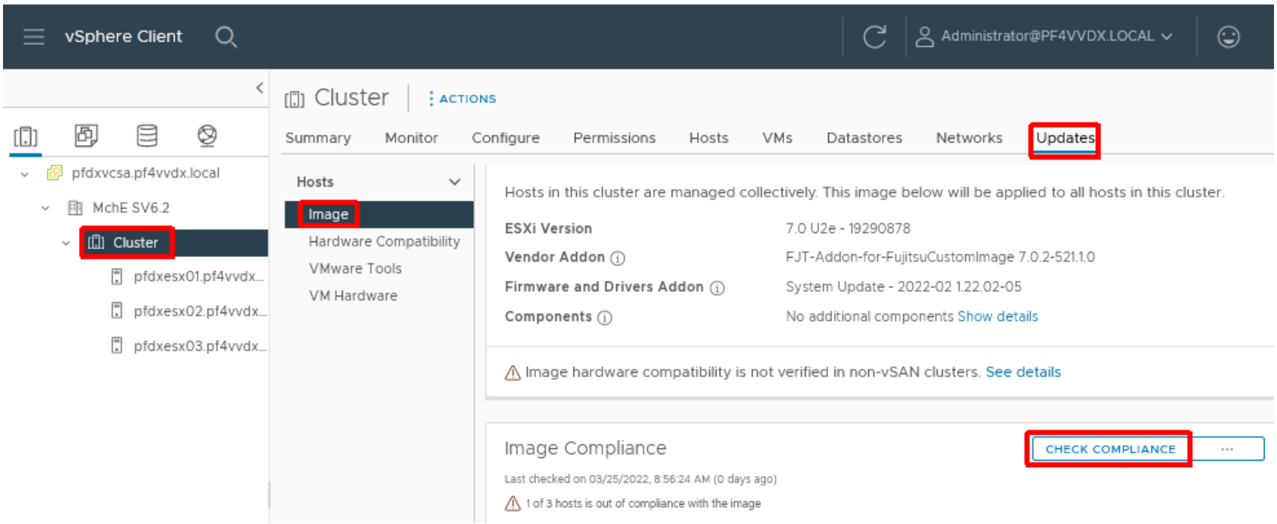
- ensure your browser is updated to the latest version,
- check for any network configuration issues,
- disable browser extensions,
- clear your cache and cookies,
- trying incognito mode might resolve the issue, as it incorporates some of the previously mentioned suggestions,

If the issue persists, collect data from your browser's developer tools, specifically the console tab and network tab with a filter set to 'Fetch/XHR.' Focus on the outputs from at least the last 5 calls related to getting the task status, which can be easily identified as they start with the prefix “task-“.

After collecting this data, please contact your support center for further assistance in investigating and resolving the issue.

8.6. Interpreting the Plug-in’s Compliance States

A compliance check for a cluster can be initiated either implicitly by using related vLCM features, such as setting up a new vLCM image, or manually by clicking on [CHECK COMPLIANCE].



Hosts in this cluster are managed collectively. This image below will be applied to all hosts in this cluster.

ESXi Version: 7.0 U2e - 19290878

Vendor Addon ⓘ: FJT-Addon-for-FujitsuCustomImage 7.0.2-521.1.0

Firmware and Drivers Addon ⓘ: System Update - 2022-02 1.22.02-05

Components ⓘ: No additional components Show details

⚠ Image hardware compatibility is not verified in non-vSAN clusters. See details

Image Compliance

Last checked on 03/25/2022, 8:56:24 AM (0 days ago)

⚠ 1 of 3 hosts is out of compliance with the image

Whenever the compliance of a host has been checked, the results received from the PRIMERGY Plug-in for VMware vCenter can be found in the [**Firmware compliance**] section of the hosts. By default, the setting behind [**Show**] is set to [**Only drift comparison**] and the report just shows you which components are currently not compliant and would be updated by a remediation.

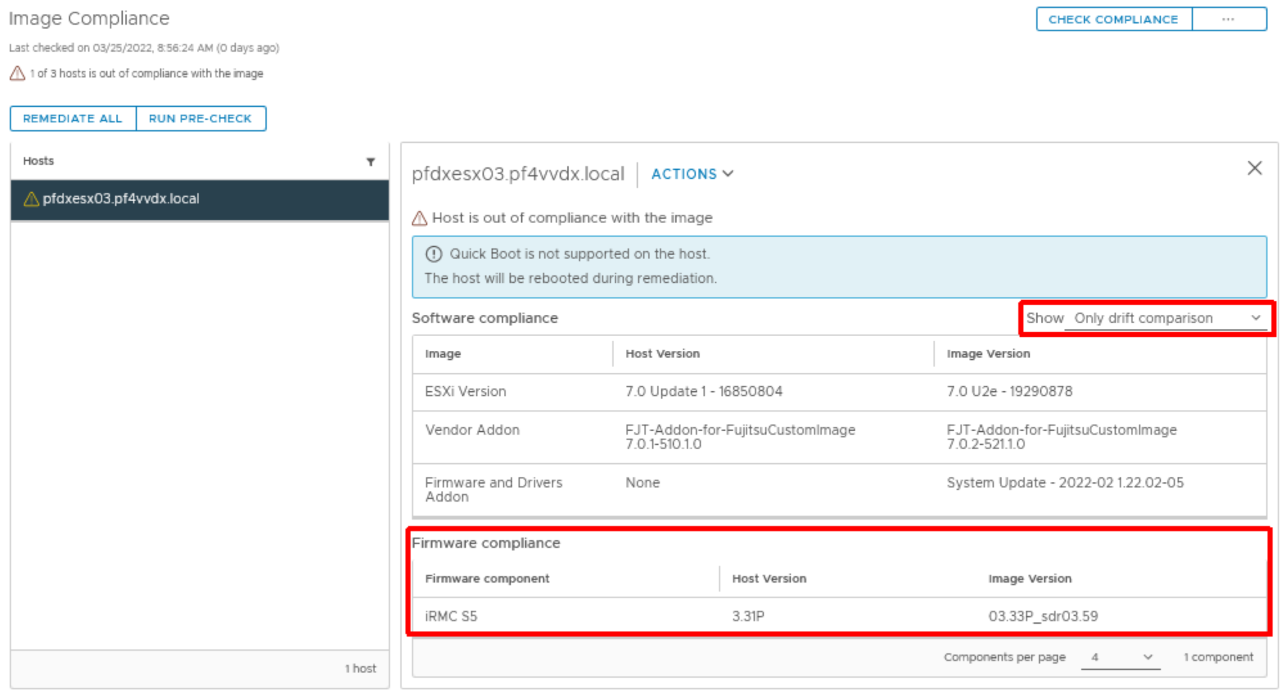


Image Compliance

Last checked on 03/25/2022, 8:56:24 AM (0 days ago)

⚠ 1 of 3 hosts is out of compliance with the image

⚠ Host is out of compliance with the image

ⓘ Quick Boot is not supported on the host.
The host will be rebooted during remediation.

Software compliance

Show: Only drift comparison

Image	Host Version	Image Version
ESXi Version	7.0 Update 1 - 16850804	7.0 U2e - 19290878
Vendor Addon	FJT-Addon-for-FujitsuCustomImage 7.0.1-510.1.0	FJT-Addon-for-FujitsuCustomImage 7.0.2-521.1.0
Firmware and Drivers Addon	None	System Update - 2022-02 1.22.02-05

Firmware compliance

Firmware component	Host Version	Image Version
iRMC S5	3.31P	03.33P_sdr03.59

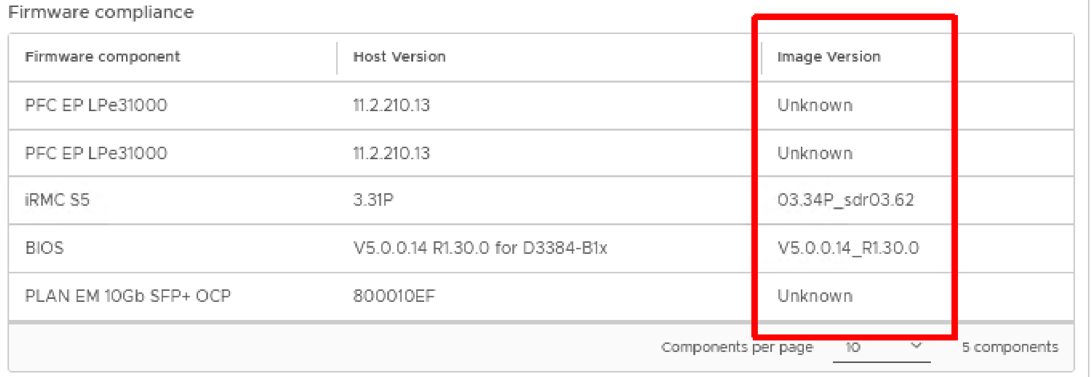
Components per page: 4 — 1 component

Warning	**Components not supported by the used HSP are always handled as compliant!** To ensure that all components are actually up to date and compatible with newly available drivers, you must ensure that all components of the hosts in the cluster are supported by the HSP. Alternatively, the firmware of unsupported components must be maintained otherwise.

To interpret the details of the scan result, set [**Show**] to [**Full image comparison**]. This will show you also the firmware components with matching version numbers and [**Unknown**] versions.

Note	Unfortunately, there is a flaw on the UI: The full image comparison results are currently not shown while the overall host compliance status is compliant.

[Unknown] image version **means, the plug-in does ignore this component** because the component is not (yet) supported by the HSP in use.



Firmware compliance

Firmware component	Host Version	Image Version
PFC EP LPe31000	11.2.210.13	Unknown
PFC EP LPe31000	11.2.210.13	Unknown
iRMC S5	3.31P	03.34P_sdr03.62
BIOS	V5.0.0.14 R1.30.0 for D3384-B1x	V5.0.0.14_R1.30.0
PLAN EM 10Gb SFP+ OCP	800010EF	Unknown

Components per page: 10 — 5 components

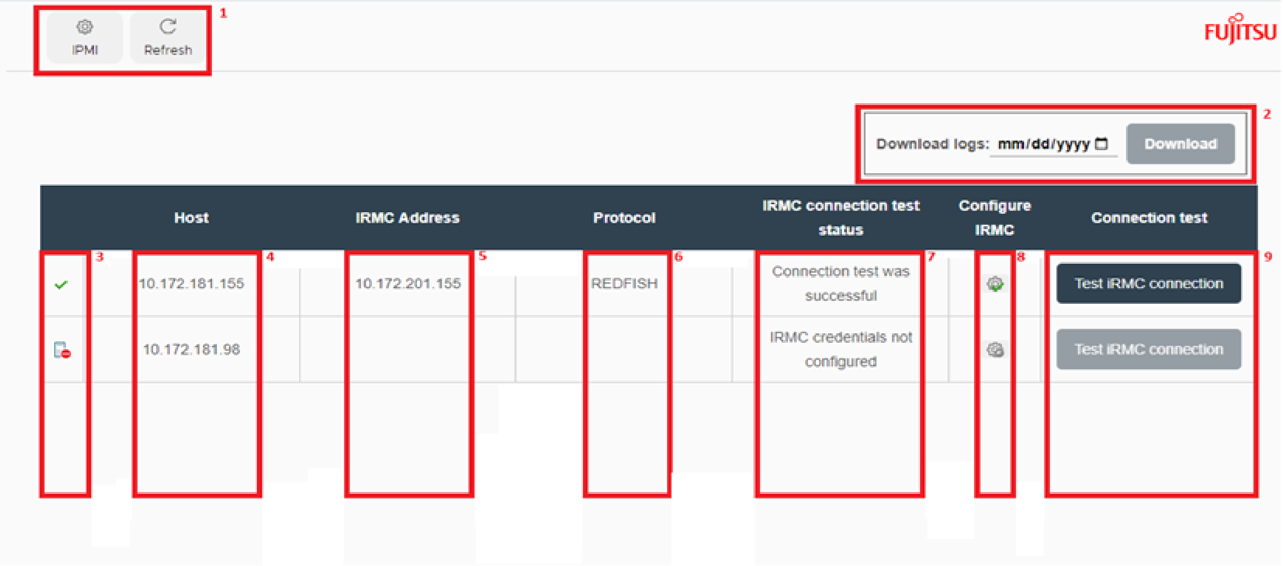
Most components with an unknown image version will have no significance in terms of vSphere support or certification. However, **if relevant components, such as BIOS, HBAs, network adapters, or FC adapters are not supported by the HSP, you must otherwise ensure that they use the correct firmware.** Check the Release Notes, VMware Compatibility Guide and any product-specific Support Matrix. If required, upgrade the firmware of the unsupported components manually or with the help of other tools like the FUJITSU Infrastructure Manager (ISM) or ServerView Update Manager.

Further details about the interpretation of the compliance states are provided in “Appendix A: Compliance Status”.

If not all hosts of a cluster are compliant with the image, you can initiate remediation either on cluster level or for individual hosts. For further details refer to section “C.5 Performing Remediation” in the appendix.

8.7. List of registered hosts

To see a list of contained in certain cluster with all their respective statuses, navigate to this Cluster -> Monitor -> PRIMERGY Plug-in for VMware vCenter and you’ll be greeted with following view:



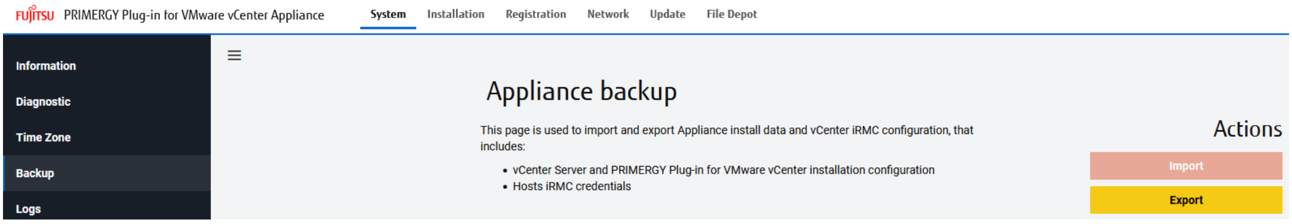
Download logs: mm/dd/yyyy Download

	Host	IRMC Address	Protocol	IRMC connection test status	Configure IRMC	Connection test
✓	10.172.181.155	10.172.201.155	REDFISH	Connection test was successful	⚙	Test iRMC connection
	10.172.181.98			IRMC credentials not configured	⚙	Test iRMC connection

1. IPMI button can register iRMC credentials for hosts, that have CIM. Refresh button will populate whole table with newest data.
2. Log downloader, after choosing proper date, it will generate support bundle. In case of any problems, please attach this file in your case.
3. Connection status icon returns information server connectivity to vCenter.
4. Hostname of server.
5. iRMC address. This field will be only available if server have CIM connection or configured iRMC connection.
6. Protocol by which all information are being downloaded.
7. Connection status text field returns results of tests ran in point 9. Of this list.
8. iRMC connection icon returns information about iRMC configuration. If host have provided proper iRMC credentials, there will be green check over cog. Can be used to configure iRMC.
9. Test button will run basic connection tests – DNS, necessary ports, and ping. The same tests are done every time user refresh this view.

8.8. Backup

In appliance of Plug-in, in System Tab, there is new Backup option. From there user can export his current plugin information such as vCenter login and password, proxy data, iRMC accesses. In case where Plug-in must be reinstalled, this may become handy and save some time for configuration.



Appliance backup

This page is used to import and export Appliance install data and vCenter iRMC configuration, that includes:

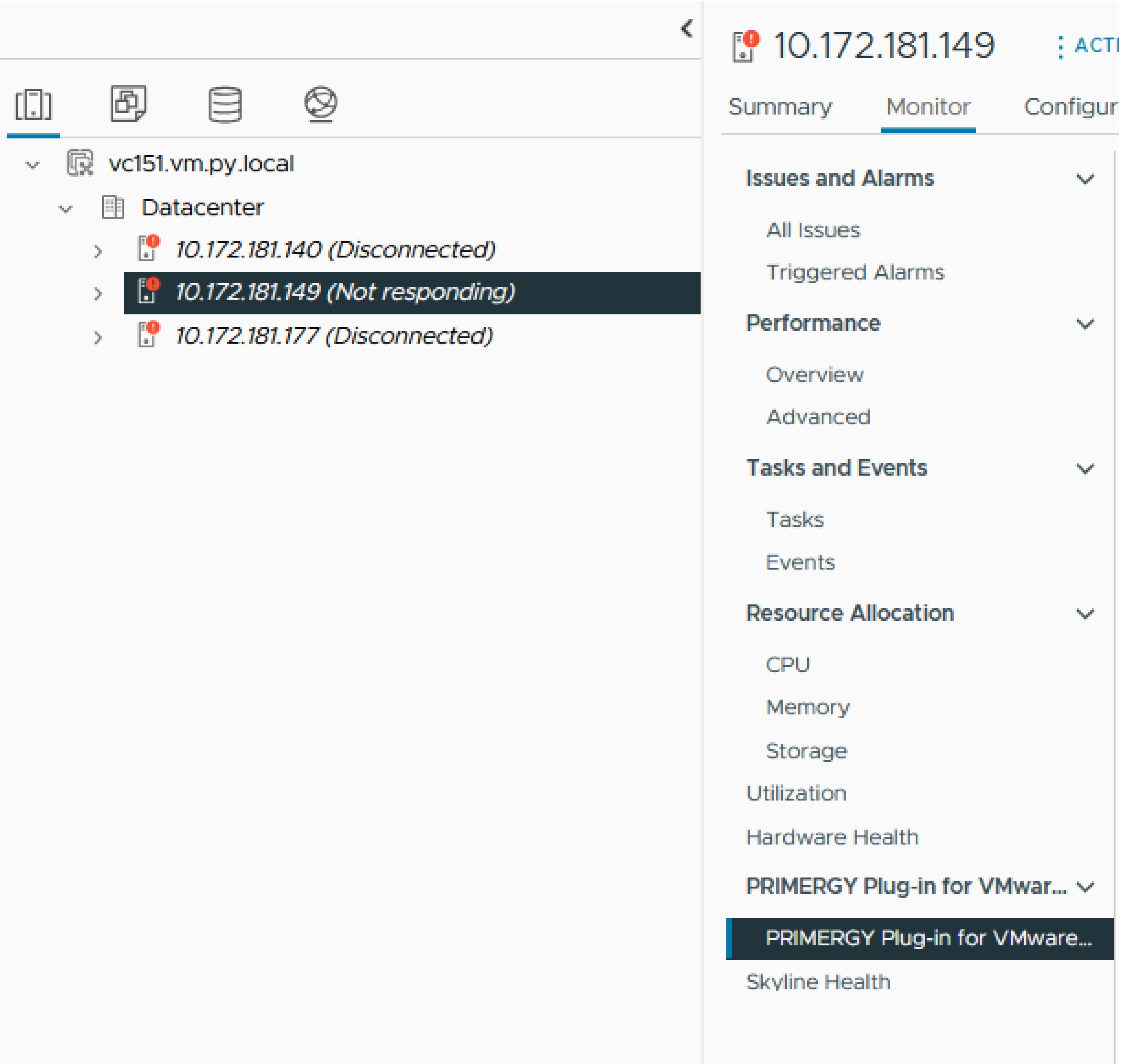
- vCenter Server and PRIMERGY Plug-in for VMware vCenter installation configuration
- Hosts iRMC credentials

All information will be retrieved as zip file, which can be later used in fresh installation of plugin, by choosing Import button. Exported filename should be “ssvexport.zip” and should remain unchanged.

❗ Warning	VM with Plug-in must have the same address and hostname for both instances!
❗ Warning	Please be aware that configuration in new Plug-in instance must be clear. There is “Reset Configuration” Button in case of any information previously saved.

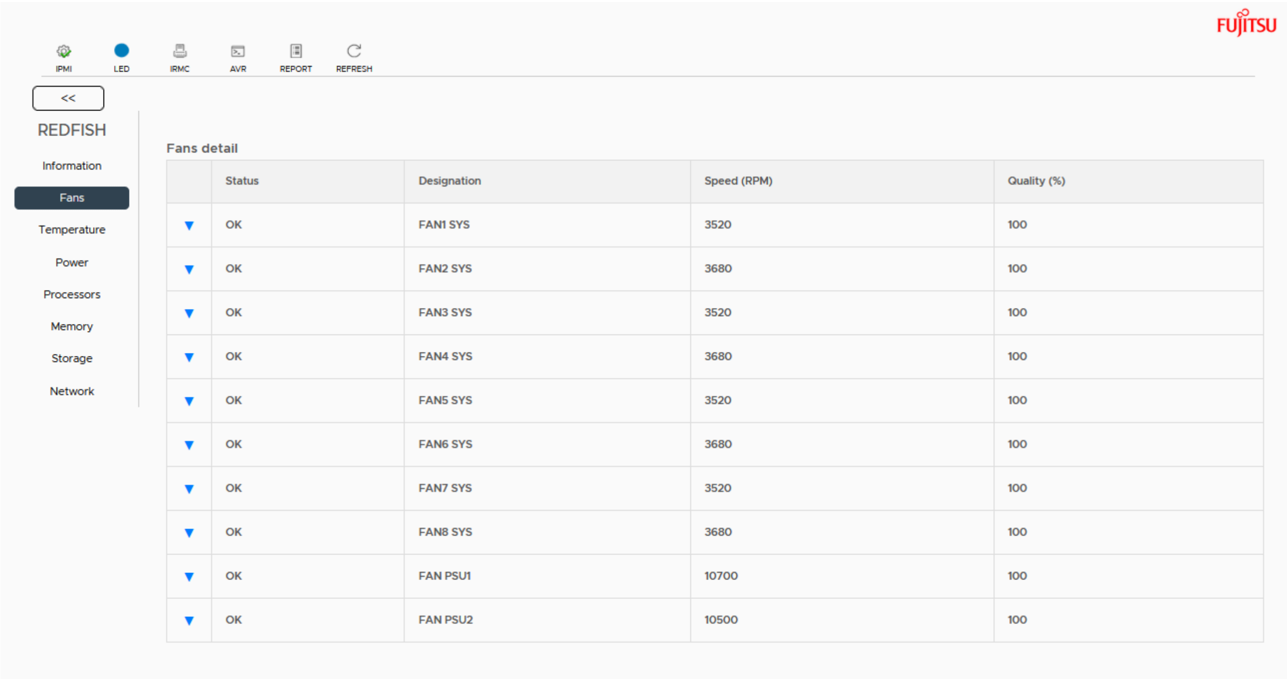
8.9. Host Monitoring

When server is chosen from inventory in vCenter, in “Monitor” tab there is “**PRIMERGY Plug-in for VMware vCenter**” entry available, which can be used to check health statuses for this host components.



If mentioned host have it's iRMC credentials provided, user will be able to collect information via Redfish regarding following data:

- General host information
- Fans
- Temperature
- Power
- Processors
- Memory
- Storage
- Network

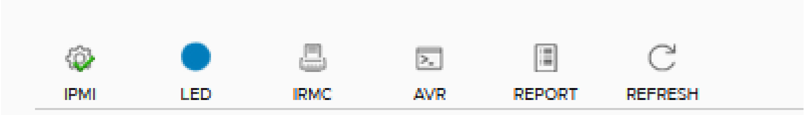


Fans detail

	Status	Designation	Speed (RPM)	Quality (%)
▼	OK	FAN1 SYS	3520	100
▼	OK	FAN2 SYS	3680	100
▼	OK	FAN3 SYS	3520	100
▼	OK	FAN4 SYS	3680	100
▼	OK	FAN5 SYS	3520	100
▼	OK	FAN6 SYS	3680	100
▼	OK	FAN7 SYS	3520	100
▼	OK	FAN8 SYS	3680	100
▼	OK	FAN PSU1	10700	100
▼	OK	FAN PSU2	10500	100

Additionally, at the top of monitor view there are buttons that gives user easy access to iRMC options:

- Configure iRMC credentials
- Turn on/off identification LED
- Open iRMC
- Open AVR
- Generatre report

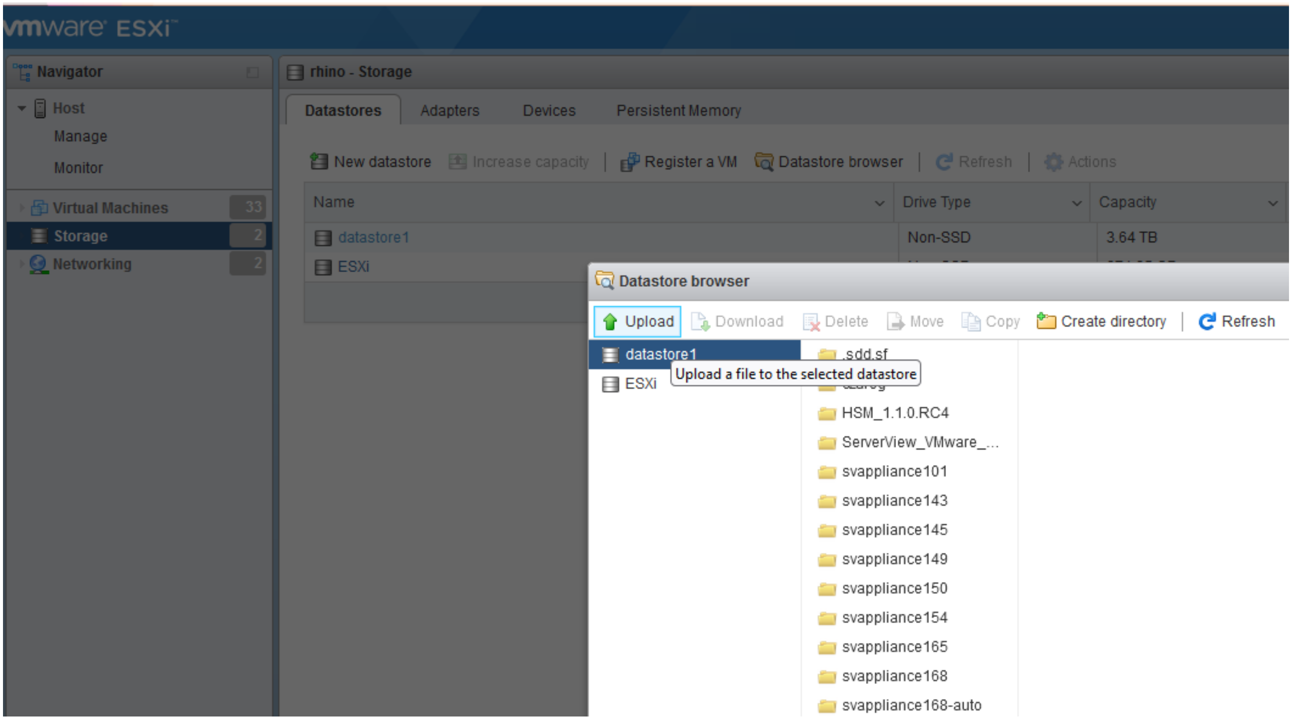


Note	To turn on and off LED on server, iRMC user need to have IPMI privileges set to Administrator or higher.

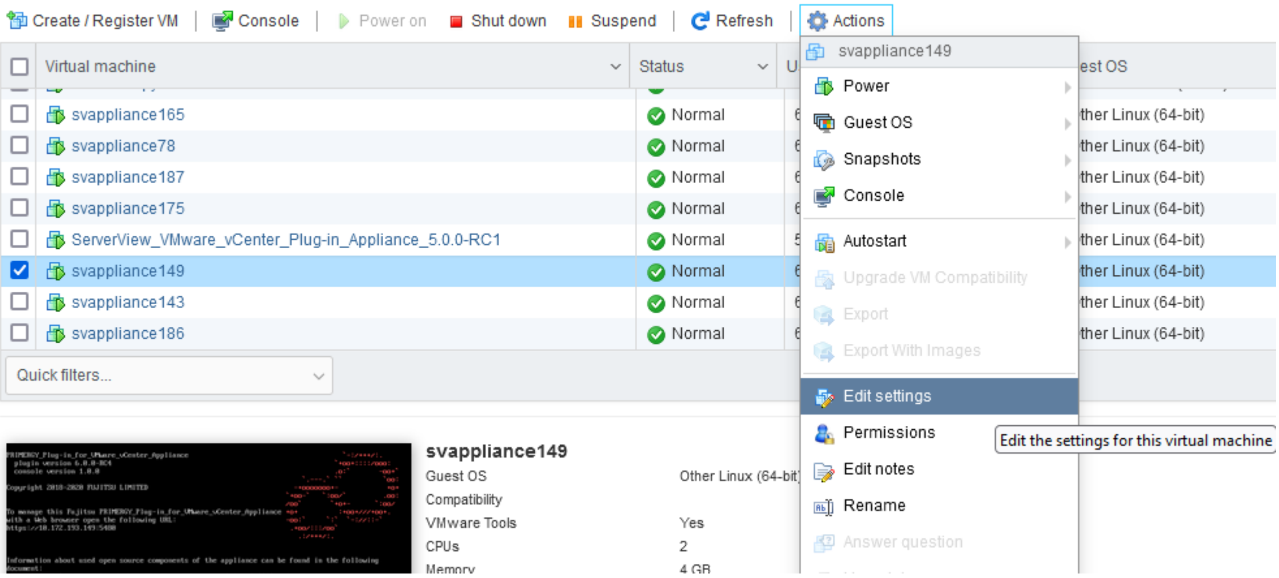
8.10. Appliance update

When new version of appliance is being released, it's possible to use disc image file with updates to get newest version of it without reinstalling it.

Together with OVA file, ISO file will be provided. This must be uploaded to ESXi where plugin is deployed.



Later on, to attach ISO to virtual machine go to its settings

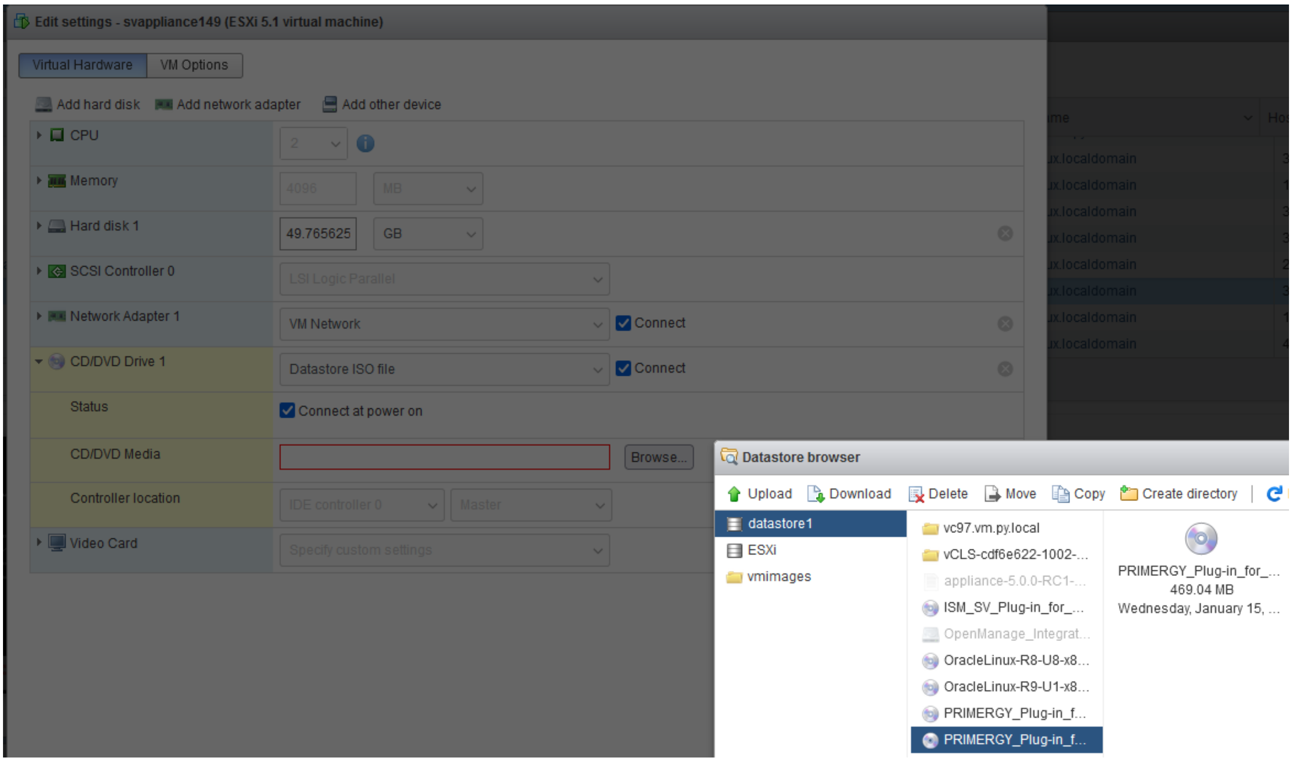


☐	Virtual machine	Status	...est OS
☐	svappliance165	Normal	...ther Linux (64-bit)
☐	svappliance78	Normal	...ther Linux (64-bit)
☐	svappliance187	Normal	...ther Linux (64-bit)
☐	svappliance175	Normal	...ther Linux (64-bit)
☐	ServerView_VMware_vCenter_Plug-in_Appliance_5.0.0-RC1	Normal	...ther Linux (64-bit)
☑	svappliance149	Normal	...ther Linux (64-bit)
☐	svappliance143	Normal	...ther Linux (64-bit)
☐	svappliance186	Normal	...ther Linux (64-bit)

svappliance149

Guest OS	Other Linux (64-bit)
Compatibility	
VMware Tools	Yes
CPUs	2
Memory	4 GB

And under “CD/DVD drive” chose disc image uploaded to server storage



Edit settings - svappliance149 (ESXi 5.1 virtual machine)

CPU: 2

Memory: 4096 MB

Hard disk 1: 49.765625 GB

SCSI Controller 0: LSI Logic Parallel

Network Adapter 1: VM Network ☑ Connect

CD/DVD Drive 1: Datastore ISO file ☑ Connect

Status: ☑ Connect at power on

CD/DVD Media: Browse...

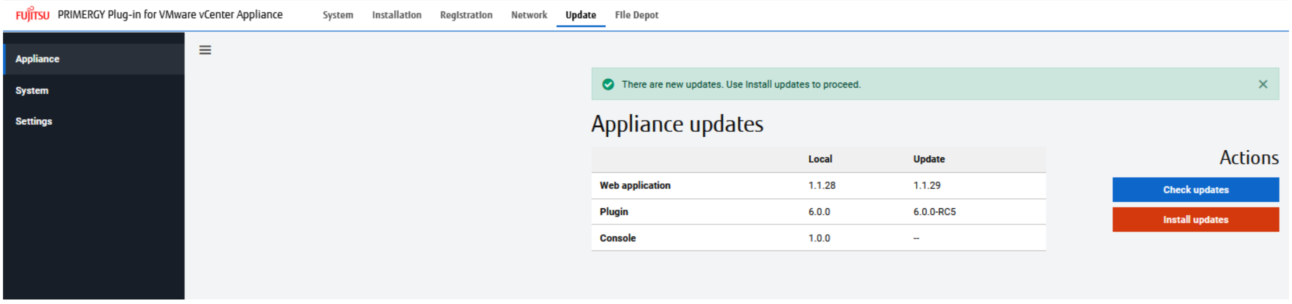
Controller location: IDE controller 0 Master

Video Card: Specify custom settings

Datastore browser

PRIMERGY_Plug-in_for_...
469.04 MB
Wednesday, January 15, ...

When it's connected, you can go to your appliance under "Update" tab and hit "Check for updates" in "Appliance" section



There are new updates. Use Install updates to proceed.

Appliance updates

	Local	Update
Web application	1.1.28	1.1.29
Plugin	6.0.0	6.0.0-RC5
Console	1.0.0	--

Proceed with install and your plugin will be updated.

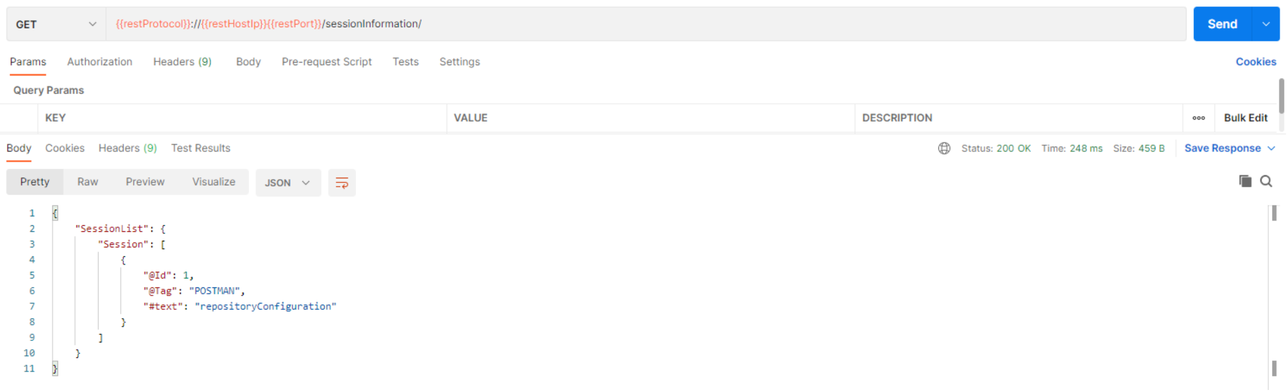
8.11. Troubleshooting Remediation

Usually neither the vSphere Client nor the plug-in VA displays relevant information about performing a firmware upgrade. Instead, logs with more details can be retrieved from the iRMC's session-specific REST API endpoints.

If any error occurs during the update, the error message should include the session ID of a session created and logged on the affected host's iRMC. However, if necessary, the session ID can also be determined via this REST API endpoint:

{irmcRest}/sessionInformation/{sessionId}/sessionInformation

In the example below, just one session with the session ID 1 is reported:



```
{
    "SessionList": {
        "Session": [
            {
                "@Id": 1,
                "@Tag": "POSTMAN",
                "#text": "repositoryConfiguration"
            }
        ]
    }
}
```

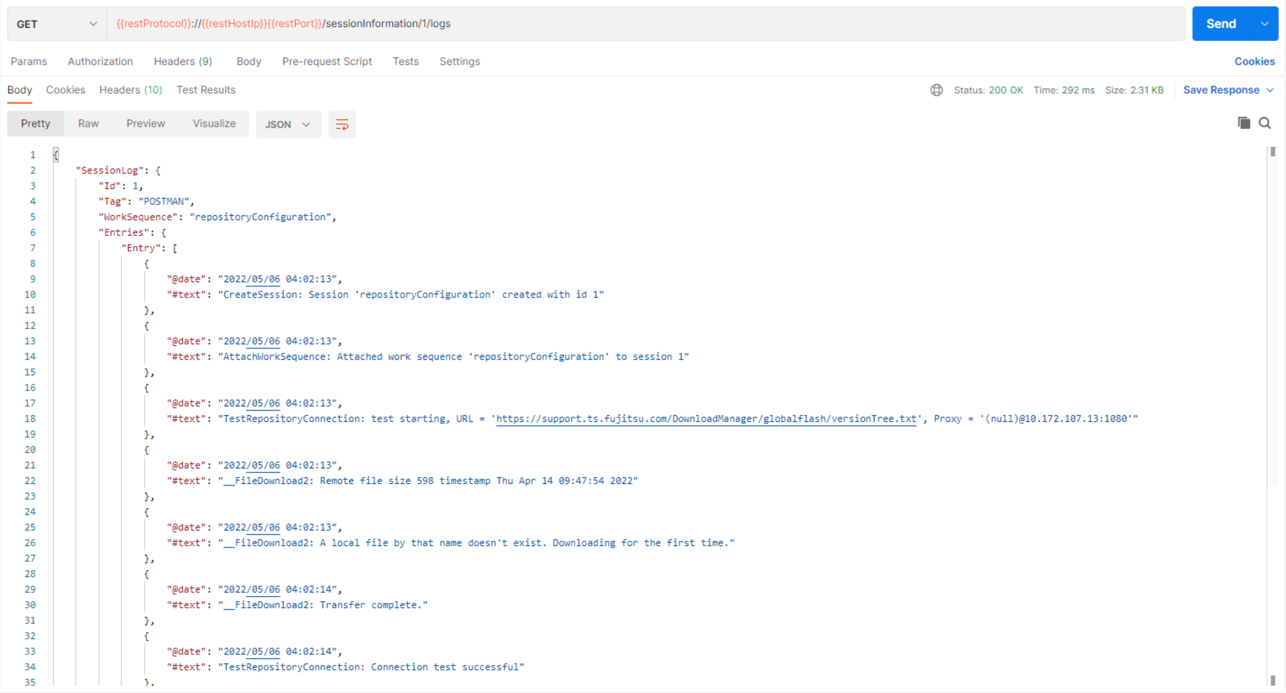
Tip The screenshots of the examples provided in this section were created using the Postman REST Client, but a regular web browser or a curl command would work as well. For more details, please refer to the iRMC's RESTful API documentation.

Knowing the session ID, details about the session can be retrieved from these REST API endpoints:

{irmcRest}/sessionInformation/{sessionId}/status (overall status)

{irmcRest}/sessionInformation/{sessionId}/logs (detailed logs)

For example, the session logs for session ID 1:



```
{
    "SessionLog": {
        "Id": 1,
        "Tag": "POSTMAN",
        "WorkSequence": "repositoryConfiguration",
        "Entries": {
            "Entry": [
                {
                    "@date": "2022/05/06 04:02:13",
                    "#text": "CreateSession: Session 'repositoryConfiguration' created with id 1"
                },
                {
                    "@date": "2022/05/06 04:02:13",
                    "#text": "AttachWorkSequence: Attached work sequence 'repositoryConfiguration' to session 1"
                },
                {
                    "@date": "2022/05/06 04:02:13",
                    "#text": "TestRepositoryConnection: test starting, URL = 'https://support.ts.fujitsu.com/DownloadManager/globalflash/versionTree.txt', Proxy = '(null)@10.172.107.13:1080'"
                },
                {
                    "@date": "2022/05/06 04:02:13",
                    "#text": "__FileDownload2: Remote file size 598 timestamp Thu Apr 14 09:47:54 2022"
                },
                {
                    "@date": "2022/05/06 04:02:13",
                    "#text": "__FileDownload2: A local file by that name doesn't exist. Downloading for the first time."
                },
                {
                    "@date": "2022/05/06 04:02:14",
                    "#text": "__FileDownload2: Transfer complete."
                },
                {
                    "@date": "2022/05/06 04:02:14",
                    "#text": "TestRepositoryConnection: Connection test successful"
                },
```

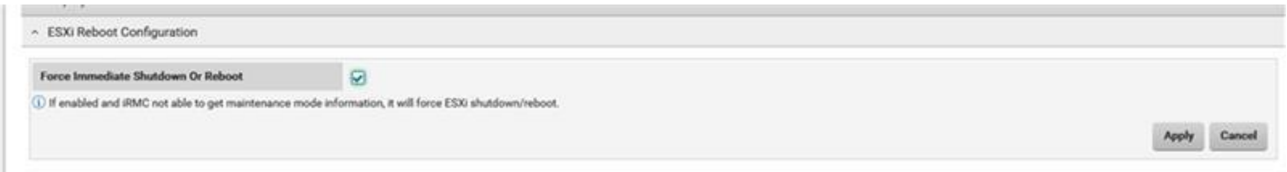
If a host remediation fails with "Unknown message", check the following log files:

- vCenter Server: /storage/log/vmware/vmware-updatemgr/vum-server/vmware-vum-server.log
- Plug-in VA: /opt/fujitsu/ServerViewSuite/webserver/logs/hsm/hsm_api.<current_date>.log

The following log files are required when opening a ticket to request technical support:

- vCenter Server:
  /storage/log/vmware/vsphere-ui/logs/
  /storage/log/vmware/vmware-updatemgr/vum-server/vmware-vum-server.log
  /storage/log/vmware/vmware-updatemgr/vum-server/hwsupportmgrctl.log
  /storage/log/vmware/vmware-updatemgr/vum-server/lifecycle.log
- Plug-in VA:
  /opt/fujitsu/ServerViewSuite/webserver/logs/*
  /var/log/fujitsu/*

In newer iRMC releases, there is an issue with rebooting server after remediation. In settings, there is tick that need to be checked to process it properly.



ESXi Reboot Configuration

Force Immediate Shutdown Or Reboot ☑

ⓘ If enabled and iRMC not able to get maintenance mode information, it will force ESXi shutdown/reboot.

9. Maintenance

In this chapter, maintenance tasks are described.

9.1. Adding New Host to a Cluster

After adding an additional node to the vSphere cluster, the only required task is to register its iRMC to the plug-in as described in “8.1.1 iRMC Configuration of the Cluster Nodes”.

9.2. Removing a Host from a Cluster

The removal of a node from a vSphere cluster requires no action related to the plug-in.

9.3. Changing the Plug-in VA’s Password

Proceed as follows to change the password of the plug-in VA’s root account:

1. Establish an SSH connection to the root account of the plug-in VA.
2. Change the password by executing the passwd command:
   ```
   [root@hsm ~]# passwd
   ```
   Enter the new password twice as requested by the command.
3. Verify success: Access the plug-in VA’s Web interface in your browser and log in to the root account using the new password, see “7.3.2 Login to the Web Interface”.
4. Close the SSH session.
   ```
   [root@hsm ~]# exit
   ```

9.4. Updating Changed iRMC Passwords

If the password of any cluster node’s registered iRMC account is changed, the plug-in’s configuration of that cluster node needs to be updated accordingly. Rerun the iRMC configuration for each affected cluster node as described in section “8.1.1 iRMC Configuration of the Cluster Nodes”.

9.5. Using custom user to login to vCenter

While using administrator account is possible to register plug-in, it’s not recommended for safety reason. New user for vCenter can be created, used roles from appendix D.15 from this manual.

9.6. Changing vCenter User Password

If the password of the vCenter Server account used to install the plug-in (“vCenter User” configured in “7.3.4 vCenter Server Connectivity” should be changed, this currently requires reinstalling and re-registering the plug-in with the new credentials.

First you need to unregister and to uninstall the plug-in from vCenter Server. However, this requires that the registered user credentials are still valid.

⚠ Note	If the password has already been changed on the vCenter Server, you should change it back to the registered one temporarily. Otherwise, you will need to perform additional steps as a workaround, see below.

Proceed as follows:

1. Login to the Web interface of the plug-in VA as the root user.
2. On the [**Registration**] tab, click [**Unregister**].

> Note
>
> If the page loading does not complete and the [Unregister] button stays disabled (greyed-out), most likely the registration was done with meanwhile outdated user credentials. Either make them working again or proceed as follows to work around the problem:
>
> 1. Perform the steps described in "Appendix B: Checking and Cleaning up Plug-In Registration".
> 2. On the [**Installation**] tab, check the [**Uninstall**] button. If it is disabled (greyed-out), initiate a reboot of the VA ([**System**] – [**Information**] – [**Reboot**]). Afterwards, reconnect to the VA's Web interface and continue with the next steps.

3. On the [**Installation**] tab, click [**Uninstall**]. Confirm the appearing dialog by clicking [**Uninstall**].
4. Now, on the vSphere Client, change the password of the account.
5. Execute the configuration steps described in sections "0" to "7.3.10" to re-register the plug-in on vCenter Server and to provide the HSP and firmware repository files once again.
6. Configure the iRMCs of the affected clusters as described in section "8.1.1 iRMC Configuration of the Cluster Nodes".
7. On vSphere Client, check the vLCM image of the affected clusters for the correct assignment of the HSP (Firmware and Drivers Addon). See section "8.2 Connecting the Plug-In to a Single Image in vLCM".
8. Execute a compliance check for each affected cluster to make sure everything is working again.

9.7. Updating the Hardware Support Package (HSP)

The HSP file should be updated regularly performing the following steps:

1. Upload the always newest revision to the plug-in VA as described in section "7.3.10 File Depot (HSP Upload)".
2. Connect the vLCM image of each cluster to the new HSP as described in section "8.2 Connecting the Plug-In to a Single Image in vLCM".

9.8. Updating the Plug-In Virtual Appliance

For now, to update the plug-in version, you must first purge the existing version and then install the new one.

Proceed as follows:

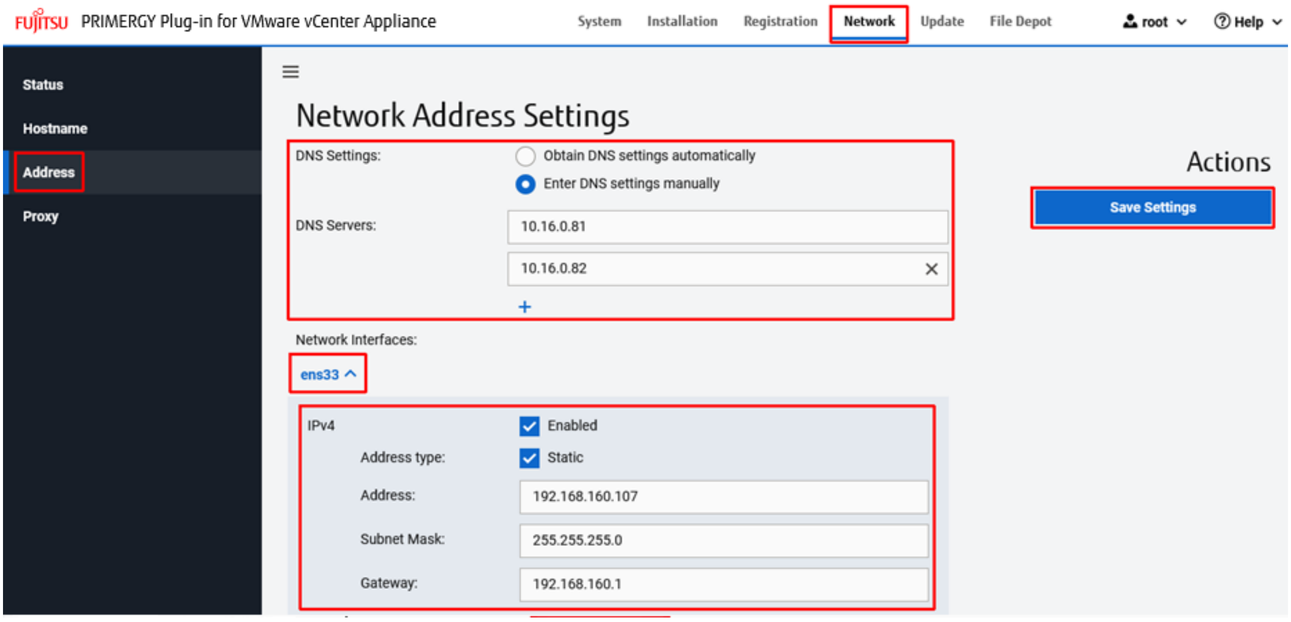
1. Login to the Web interface of the Plug-in VA as the root user.
2. Make sure you have noted all required settings of the plug-in, such as from the [**Installation**] page and the [**Network**] – [**Proxy**] page. A complete list of the required settings can be found in section “6 Configuration Data”.
3. Navigate to [**Registration**] and click on [**Unregister**].
4. Navigate to [**System**] and click on [**Shutdown**].
5. Login to the vSphere Client as an administrator and rename or even delete the plug-in VA.
6. Deploy the new plug-in VA as described in section “7 Deployment”.
7. Configure the iRMCs of the affected clusters as described in section “8.1.1 iRMC Configuration of the Cluster Nodes”.
8. On vSphere Client, check the vLCM image of the affected clusters for the correct assignment of the HSP (Firmware and Drivers Addon). See section “8.2 Connecting the Plug-In to a Single Image in vLCM”.
9. Execute a compliance check for each affected cluster in order to make sure everything is working again.

9.9. Changing Network Address Settings of the Plug-in VA

To change the network settings of the plug-in VA, you need to unregister and to uninstall the plug-in, then to change the IP address of the VA and finally to install and to register the plug-in again.

Proceed as follows:

1. Login to the Web interface of the plug-in VA as the root user.
2. On the [**Registration**] tab, click [**Unregister**].
3. On the [**Installation**] tab, click [**Uninstall**]. Confirm the appearing dialog by clicking [**Uninstall**].
4. On the [**Network**] tab, select [**Address**], make the appropriate network settings and click [**Save Settings**].



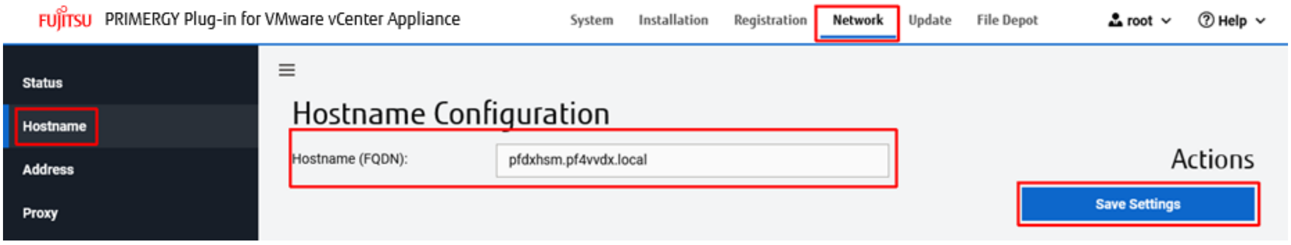
DNS Settings: ○ Obtain DNS settings automatically
● Enter DNS settings manually

DNS Servers: 10.16.0.81
10.16.0.82

Network Interfaces:
ens33

IPv4 ☑ Enabled
Address type: ☑ Static
Address: 192.168.160.107
Subnet Mask: 255.255.255.0
Gateway: 192.168.160.1

5. If required, you can also change the hostname (FQDN). Navigate to [**Network**] – [**Hostname**], enter the new name and click [**Save Settings**].



Hostname Configuration

Hostname (FQDN): pfdxhsm.pf4vvdx.local

6. Navigate to [**System**] – [**Information**], click the [**Reboot**] button and click [**Reboot**] to confirm. Wait a minute until the system is back and login again using the new IP address then.
7. Execute the configuration steps described in sections “0” to “7.3.10” in order to re-register the plug-in on vCenter Server and to provide the HSP and firmware repository files once again.
8. Configure the iRMCs of the affected clusters as described in section “8.1.1 iRMC Configuration of the Cluster Nodes”.
9. On vSphere Client, check the vLCM image of the affected clusters for the correct assignment of the HSP (Firmware and Drivers Addon). See section “8.2 Connecting the Plug-In to a Single Image in vLCM”.
10. Execute a compliance check for each affected cluster in order to make sure everything is working again.

9.10. Updating changed IP Address of an iRMC

If the IP address of an iRMC has been changed, rerun the single host configuration described in “8.1.1 iRMC Configuration of the Cluster Nodes”.

9.11. Changing the IP Address of the vCenter Server

If the IP address of the vCenter Server needs to be changed, you must unregister and uninstall the plug-in prior to the change and then install and register it for the new IP address. If you apply the description in terms of changing the IP address instead of the password, the procedure is the same as described in section “9.5 Using custom user to login to vCenter

While using administrator account is possible to register plug-in, it’s not recommended for safety reason. New user for vCenter can be created, used roles from appendix D.15 from this manual.

Changing vCenter User Password”.

9.12. Removing custom selected version for component

If the user desires to remove custom selected version for the component, it is recommended to follow steps from “7.3 Custom Version Selector”:

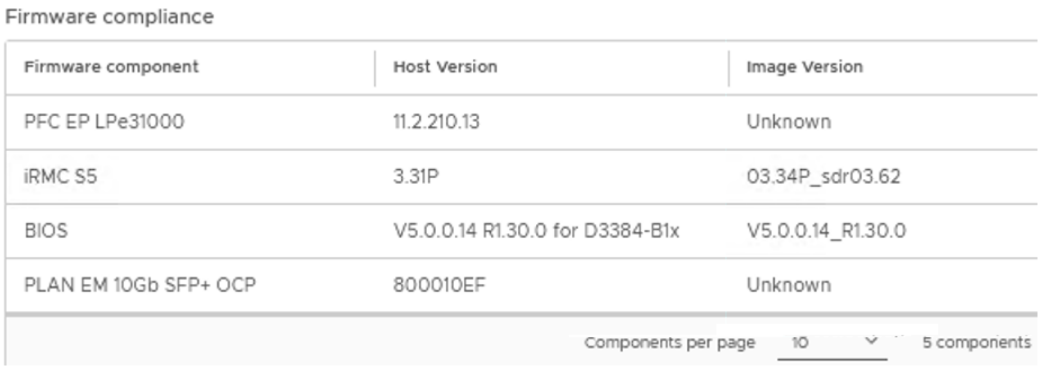
- find desired host and component,
- setup a default value for component,
- save changes.

Appendix A: Compliance Status

This appendix describes how the plug-in determines the compliance state of the individual components and the overall compliance state of the host.

A.1. Firmware Component Compliance Status

On vSphere Client, the image compliance report for each host lists the current firmware version (Host Version) and the target firmware version (Image Version) for each component.



Firmware compliance

Firmware component	Host Version	Image Version
PFC EP LPe31000	11.2.210.13	Unknown
iRMC S5	3.31P	03.34P_sdr03.62
BIOS	V5.0.0.14 R1.30.0 for D3384-B1x	V5.0.0.14_R1.30.0
PLAN EM 10Gb SFP+ OCP	800010EF	Unknown

Components per page 10 5 components

Based on the comparison of the two versions, the plug-in determines the compliance state of each component according to the rules shown in the table below.

Current Version	Target Version	Component Compliance State	Description
<version>	<same or lower version>	COMPLIANT	Current version is newer or matches the target version
<version>	<higher version>	NON_COMPLIANT	Current version is older than target version
<version>	UNKNOWN [2]	COMPLIANT	Component not supported by the HSP
UNKNOWN [1]	<any version>	UNAVAILABLE	Failed to determine current version
UNKNOWN [1]	UNKNOWN [2]	NONE (component ignored)	Failed to determine the current version for a component which is not supported by the HSP

[1] An UNKNOWN status for current version means that it cannot be determined via the Redfish API.

[2] An UNKNOWN status for target version means that it is not supported by the HSP in use.

During remediation, all components with NON_COMPLIANT status will be updated before the software and drivers on the host are updated if required.

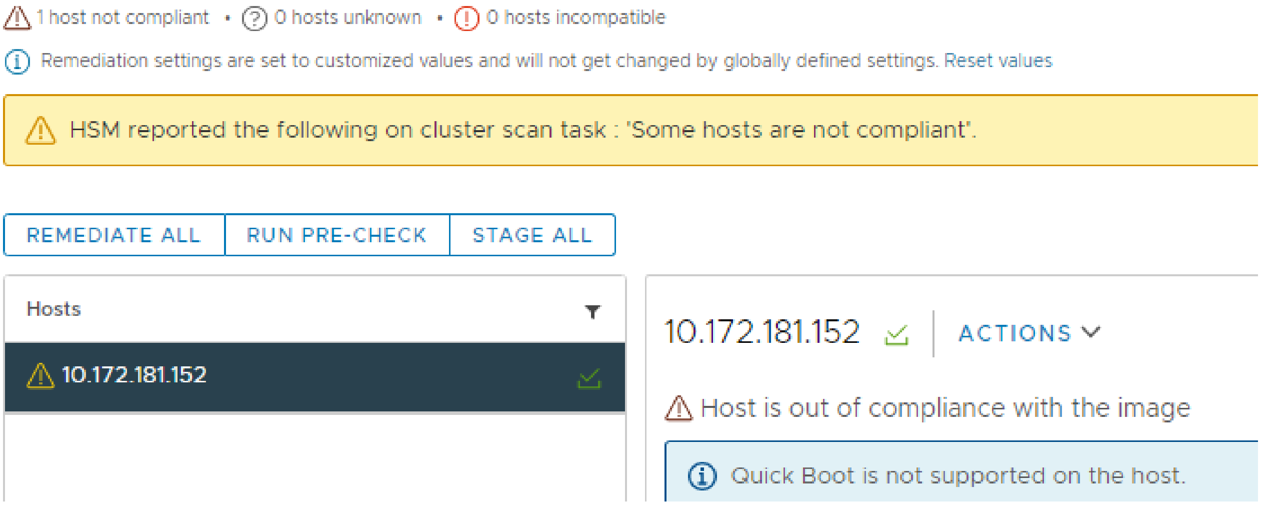
A.2. Host Compliance Status

The overall compliance status of a host is derived from the compliance results of the host's individual components, see previous section.

Components Compliance	Overall Host Compliance Status
All components are COMPLIANT	COMPLIANT
At least one component is NON_COMPLIANT or UNAVAILABLE	NON_COMPLIANT

A.3. Staging

Staging is a new automatic part of compliance remediation that automatically scans compliance and gathers components that could be updated. We can see that host is staged with green check mark next to its name as seen bellow



⚠ 1 host not compliant • ? 0 hosts unknown • ! 0 hosts incompatible

ⓘ Remediation settings are set to customized values and will not get changed by globally defined settings. Reset values

⚠ HSM reported the following on cluster scan task : 'Some hosts are not compliant'.

⚠ Host is out of compliance with the image

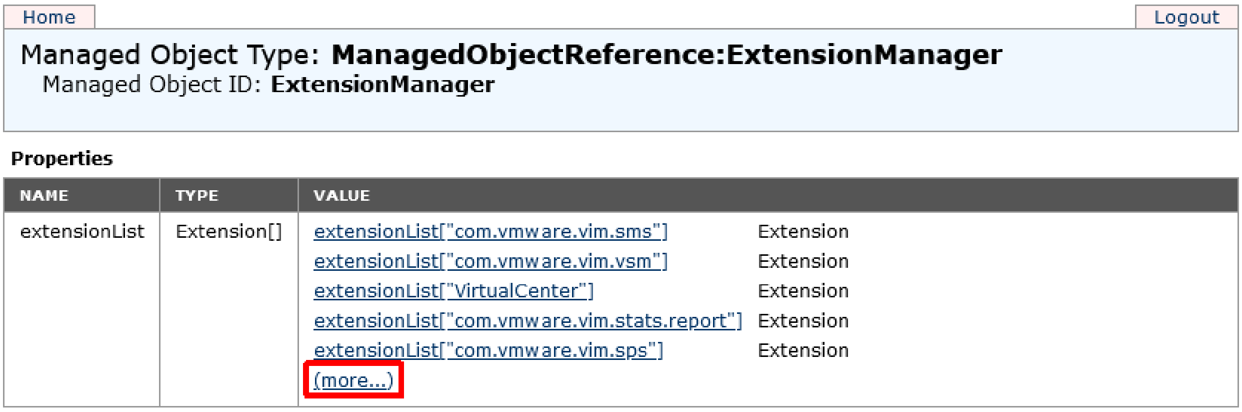
ⓘ Quick Boot is not supported on the host.

Appendix B: Checking and Cleaning up Plug-In Registration

The registration of the PRIMERGY Plug-in for VMware vCenter to a vCenter Server will fail when trying to register it again while a previous registration was not completely removed. For example, you cannot unregister the plug-in after the plug-in VA has been destroyed or replaced or the password of the used account has been changed.

In such case proceed as follows to clean up the registration on the vCenter Server:

1. Connect your browser to the Managed Object Browser (MOB) of the vCenter Server at
   https://<vCenter FQDN>/mob/?moid=ExtensionManager.
2. At the bottom of the **[Properties]** table, click on [**(more...)**].

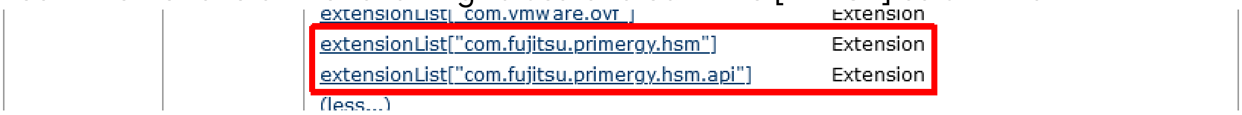


Managed Object Type: **ManagedObjectReference:ExtensionManager**
Managed Object ID: **ExtensionManager**

Properties

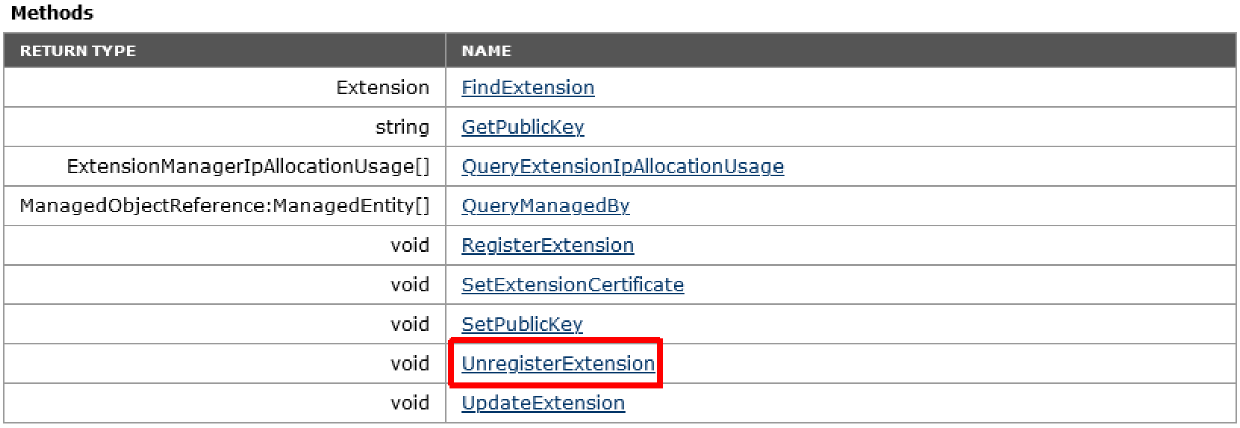
NAME	TYPE	VALUE	
extensionList	Extension[]	extensionList["com.vmware.vim.sms"]	Extension
		extensionList["com.vmware.vim.vsm"]	Extension
		extensionList["VirtualCenter"]	Extension
		extensionList["com.vmware.vim.stats.report"]	Extension
		extensionList["com.vmware.vim.sps"]	Extension
		(more...)	

3. Check whether one of the following values is listed in the [**VALUE**] column now:



		extensionList["com.vmware.ovf"]	Extension
		extensionList["com.fujitsu.primergy.hsm"]	Extension
		extensionList["com.fujitsu.primergy.hsm.api"]	Extension
		(less...)	

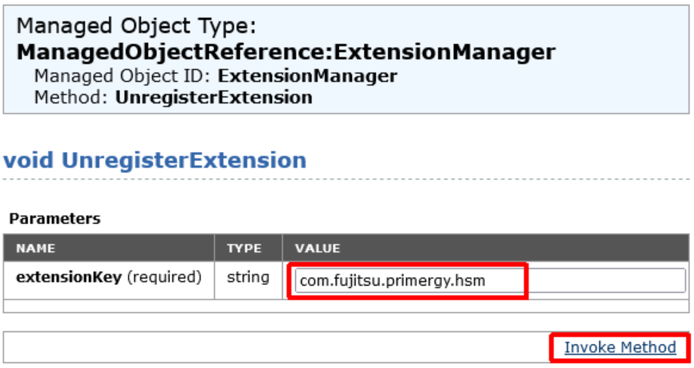
4. If you can't find any of these two values, the plug-in is currently not registered, and you can stop the task at this point. Otherwise, you need to unregister the extension as described in the subsequent steps.
5. Scroll down to the [**Methods**] section and click on [**UnregisterExtension**].



Methods

RETURN TYPE	NAME
Extension	FindExtension
string	GetPublicKey
ExtensionManagerIpAllocationUsage[]	QueryExtensionIpAllocationUsage
ManagedObjectReference:ManagedEntity[]	QueryManagedBy
void	RegisterExtension
void	SetExtensionCertificate
void	SetPublicKey
void	UnregisterExtension
void	UpdateExtension

6. Enter the value [**com.fujitsu.primergy.hsm**] as the [**extensionKey**] and click on [**Invoke Method**].



Managed Object Type: **ManagedObjectReference:ExtensionManager**
Managed Object ID: **ExtensionManager**
Method: **UnregisterExtension**

void UnregisterExtension

Parameters

NAME	TYPE	VALUE
extensionKey (required)	string	com.fujitsu.primergy.hsm

7. A message [**Method Invocation Result: void**] confirms success. Repeat the same for the key [**com.fujitsu.primergy.hsm.api**] then. Now you should be able to register the plug-in again.

Appendix C: Configuring vSphere Lifecycle Manager

To provide the system with updates on a regular basis, vSphere 7 provides the vSphere Lifecycle Manager (vLCM).

vLCM offers several options for the lifecycle management of a vSphere cluster. This description considers only a part of the possibilities, in particular

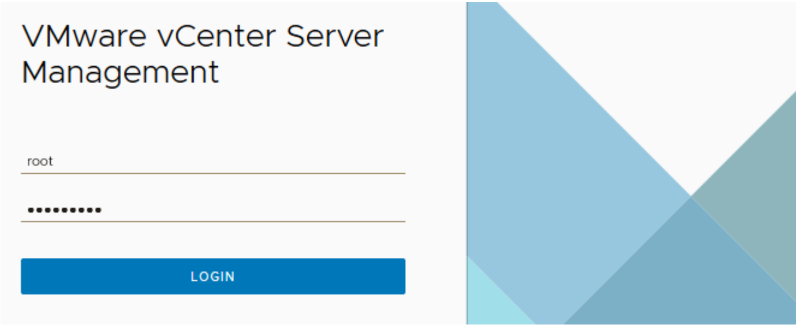
- it discusses only the so called “single image” method, not the “baselines” method and
- it uses the Default VMware Online Depot to receive the patches and FUJITSU addons.

The usage of vLCM is described in detail in VMware’s documentation “Managing Host and Cluster Lifecycle”.

C.1. Configuring Proxy Settings (if required)

To connect to the VMware online depot on the Internet, you may need to configure the proxy settings of the vCenter Server Appliance first.

1. Open the vCSA management at **https://<vCSA IP>:5480** and login to the **root** account.

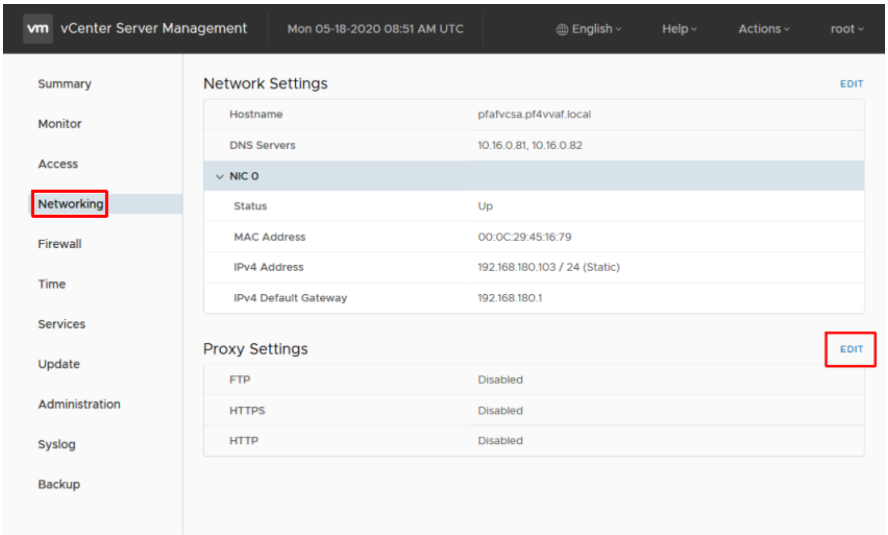


VMware vCenter Server Management

root

•••••••••

2. Select [**Networking**] from the navigation pane on the left side. For [**Proxy Settings**] click the [**EDIT**] button.



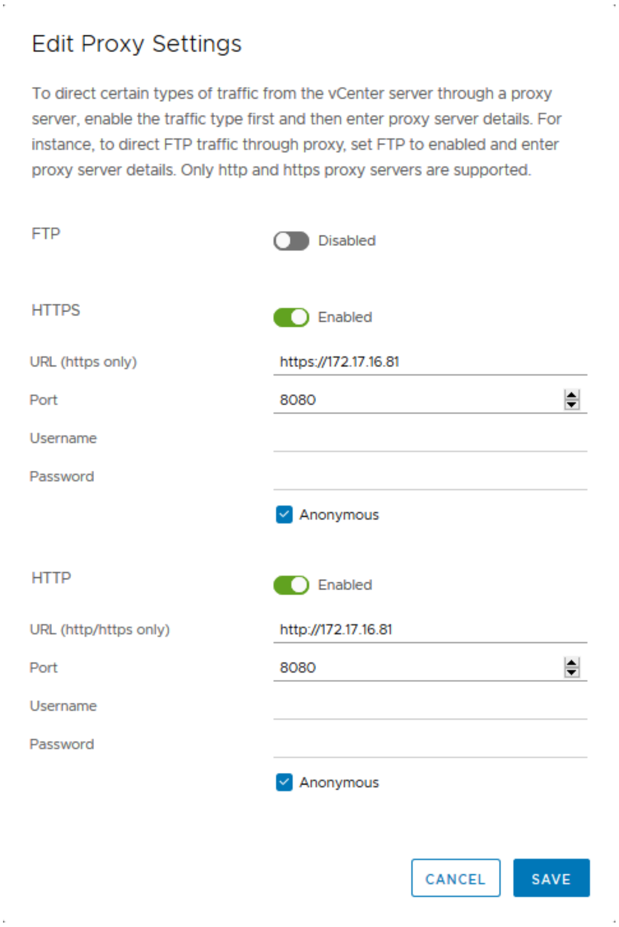
Network Settings

Hostname	pfafvcsa.pf4vvaf.local
DNS Servers	10.16.0.81, 10.16.0.82
NIC 0	
Status	Up
MAC Address	00:0C:29:45:16:79
IPv4 Address	192.168.180.103 / 24 (Static)
IPv4 Default Gateway	192.168.180.1

Proxy Settings

FTP	Disabled
HTTPS	Disabled
HTTP	Disabled

3. Enable the traffic types and enter the [**URL]** and [**Port]** of the proxy. If the proxy requires authentication, uncheck [**Anonymous]**, and provide the [**Username**] and [**Password**]. Click **SAVE**.



Edit Proxy Settings

To direct certain types of traffic from the vCenter server through a proxy server, enable the traffic type first and then enter proxy server details. For instance, to direct FTP traffic through proxy, set FTP to enabled and enter proxy server details. Only http and https proxy servers are supported.

FTP: Disabled

HTTPS: Enabled

URL (https only): https://172.17.16.81

Port: 8080

Username:

Password:

☑ Anonymous

HTTP: Enabled

URL (http/https only): http://172.17.16.81

Port: 8080

Username:

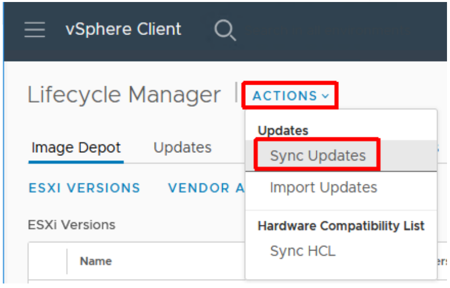
Password:

☑ Anonymous

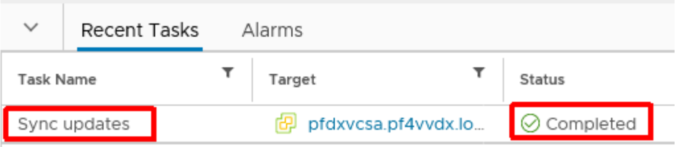
C.2. Downloading Patches from the Online Depot

To load the latest patches and FUJITSU addons into the vLCM image depot, perform the following steps:

1. Login to the vSphere Client as a user having the privileges to configure and use vLCM.
2. Open the **[Lifecycle Manager]**, click on **[Actions]** and select **[Sync Updates]**.



3. On the **[Recent Tasks]** list of the vSphere Client, monitor the task and wait until it has completed succesfully.



Task Name	Target	Status
Sync updates	pfdxvcsa.pf4vvdx.lo...	✓ Completed

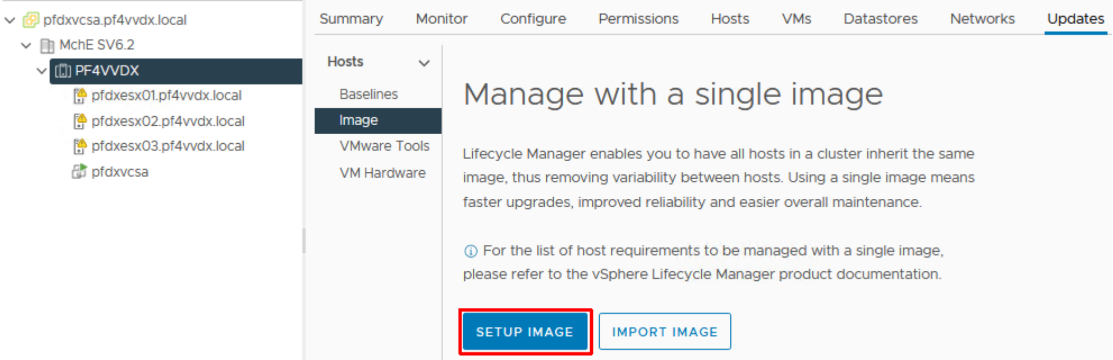
C.3. Defining the Image

This section describes how to setup the vLCM single image to manage the lifecycle of a vSphere cluster with it.

Note	Even though using the image depot is VMware's recommended method for lifecycle management, you should be aware of the related consequences. In particular, please note that the decision to use a single image for update management is irreversible. Once the cluster has been converted for it, as of today you cannot switch back to the baseline method. **If in doubt, do not continue!**

If you decided to perform the **non-reversible procedure** of converting the cluster to single image management, proceed as follows:

1. From the [**Inventory**], select the [**<cluster name>**], open the [**Updates**] tab, click on [**Image**] and click the [**SETUP IMAGE**] button then.

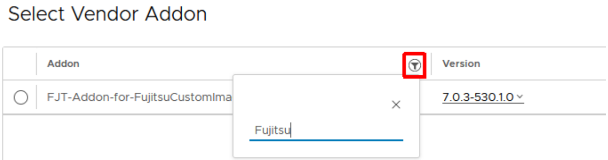


Manage with a single image

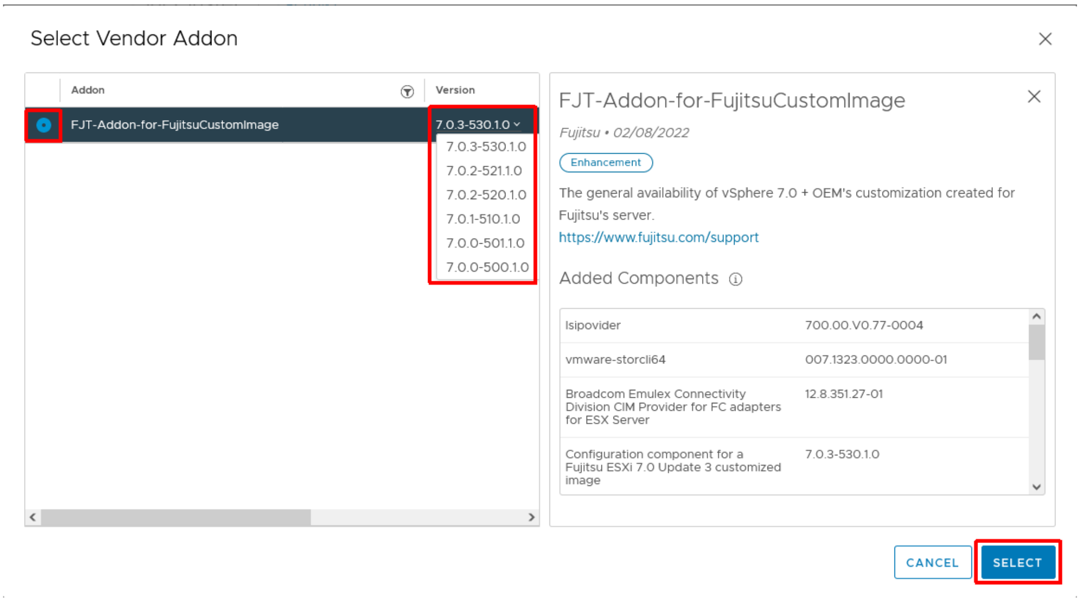
Lifecycle Manager enables you to have all hosts in a cluster inherit the same image, thus removing variability between hosts. Using a single image means faster upgrades, improved reliability and easier overall maintenance.

ⓘ For the list of host requirements to be managed with a single image, please refer to the vSphere Lifecycle Manager product documentation.

2. Define the image in accordance with the requirements for the respective cluster. For instance, it might be necessary to consider requirements described by a Product Support Matrix.
   Make the following assignments:
   - [**ESXi Version**] – Use the drop-down box to select the version matching to the ESXi version(s) currently installed on the cluster's nodes, i.e., the same or a newer one.
   - [**Vendor Addon**] – Click on the pencil icon to open the [Select Vendor Addon] window and select the matching FUJITSU addon. It might be helpful to use the filter to search for it.



Select the matching [**Version**] from the drop-down box, review the details provided on the right window frame and click [**SELECT**].



Select Vendor Addon

Addon	Version
● FJT-Addon-for-FujitsuCustomImage	7.0.3-530.1.0

FJT-Addon-for-FujitsuCustomImage

Fujitsu • 02/08/2022

Enhancement

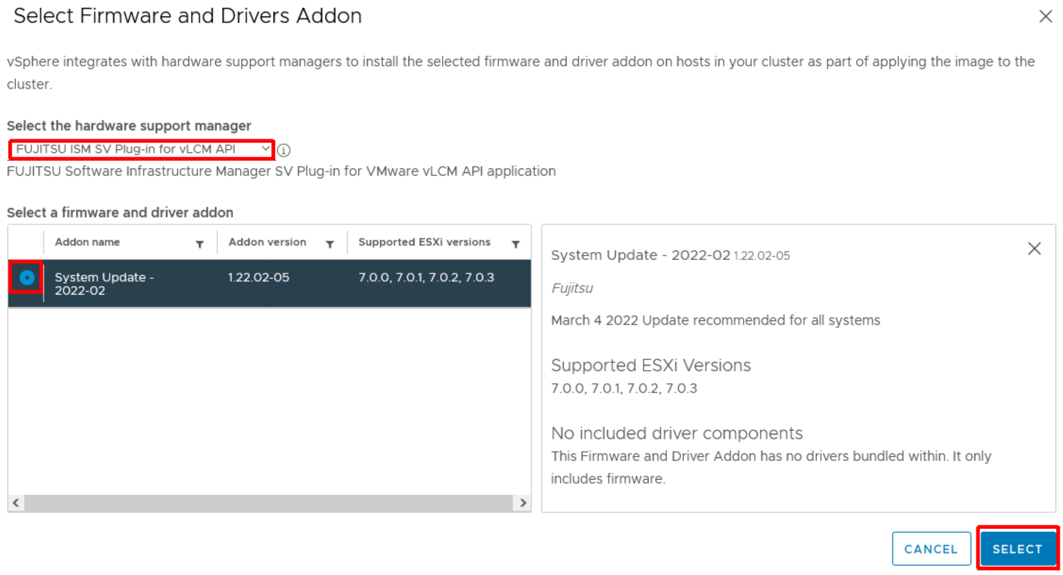
The general availability of vSphere 7.0 + OEM's customization created for Fujitsu's server.

https://www.fujitsu.com/support

Added Components

lsipovider	700.00.V0.77-0004
vmware-storcli64	007.1323.0000.0000-01
Broadcom Emulex Connectivity Division CIM Provider for FC adapters for ESX Server	12.8.351.27-01
Configuration component for a Fujitsu ESXi 7.0 Update 3 customized image	7.0.3-530.1.0

- [**Firmware and Drivers Addon**] – Click on [**SELECT**] to open the [**Select Firmware and Drivers Addon**] window. From the drop-down box below [**Select the hardware support manager**], select [**PRIMERGY Plug-in for VMware vCenter**]. Then select the matching update from the [**Select a firmware and driver addon**] list, review the details provided on the right window frame and click [**SELECT**].



Select Firmware and Drivers Addon

vSphere integrates with hardware support managers to install the selected firmware and driver addon on hosts in your cluster as part of applying the image to the cluster.

Select the hardware support manager

FUJITSU ISM SV Plug-in for vLCM API

FUJITSU Software Infrastructure Manager SV Plug-in for VMware vLCM API application

Select a firmware and driver addon

Addon name	Addon version	Supported ESXi versions
● System Update - 2022-02	1.22.02-05	7.0.0, 7.0.1, 7.0.2, 7.0.3

System Update - 2022-02 1.22.02-05

Fujitsu

March 4 2022 Update recommended for all systems

Supported ESXi Versions

7.0.0, 7.0.1, 7.0.2, 7.0.3

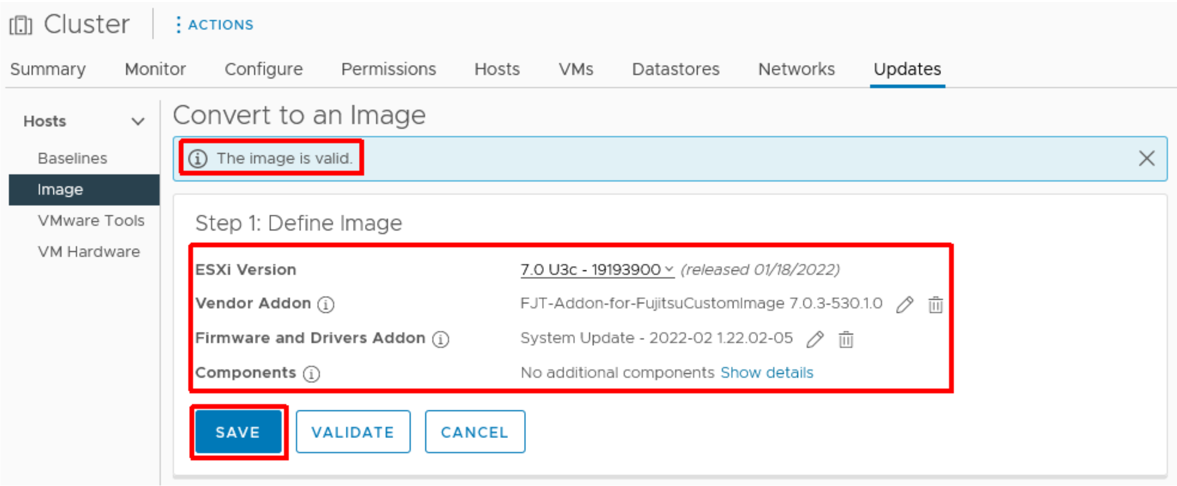
No included driver components

This Firmware and Driver Addon has no drivers bundled within. It only includes firmware.

- [**Components**] - Only required in exceptional cases.

Click on [**Validate**].

A light blue highlighted message [**The image is valid.**] should appear then. Click [**SAVE**].



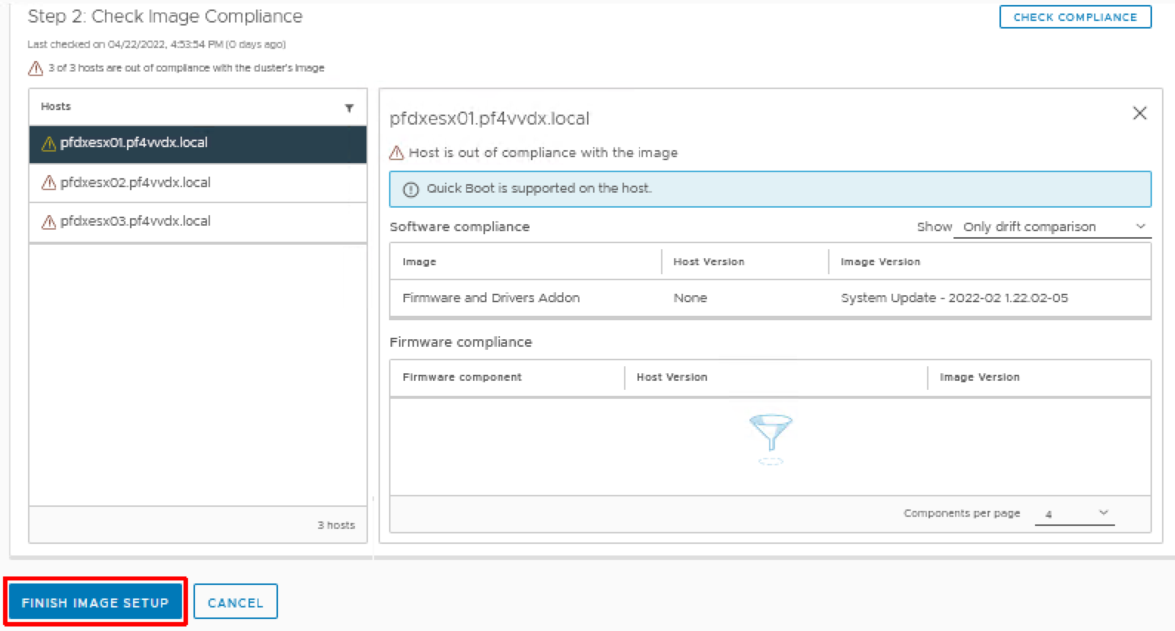
Convert to an Image

The image is valid.

Step 1: Define Image

ESXi Version	7.0 U3c - 19193900 (released 01/18/2022)
Vendor Addon	FJT-Addon-for-FujitsuCustomImage 7.0.3-530.1.0
Firmware and Drivers Addon	System Update - 2022-02 1.22.02-05
Components	No additional components Show details

3. Wait while the image compliance is checked.



Step 2: Check Image Compliance

Last checked on 04/22/2022, 4:53:54 PM (0 days ago)

3 of 3 hosts are out of compliance with the cluster's image

pfdxesx01.pf4vvdx.local
pfdxesx02.pf4vvdx.local
pfdxesx03.pf4vvdx.local

3 hosts

pfdxesx01.pf4vvdx.local

Host is out of compliance with the image

Quick Boot is supported on the host.

Software compliance

Image	Host Version	Image Version
Firmware and Drivers Addon	None	System Update - 2022-02 1.22.02-05

Firmware compliance

Firmware component	Host Version	Image Version

4. Finally, click [**FINISH IMAGE SETUP**] and confirm by clicking [**YES, FINISH IMAGE SETUP**].

This will convert the cluster for the single image management and initiates a compliance check for the hosts.

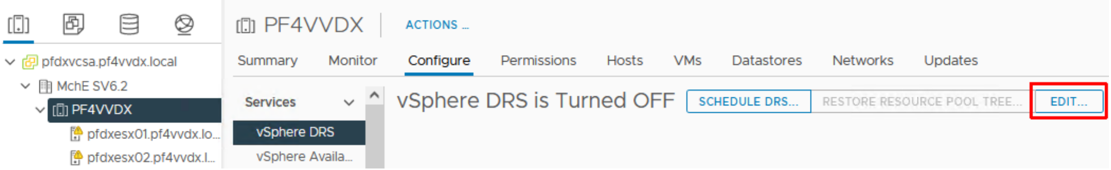
C.4. Enabling Fully Automated Remediation

There are several methods to enable fully automatic remediation, such as disabling HA (be careful!) while it is running or forcing vLCM to handle certain situations by making appropriate vLCM settings. However, usually the best and simplest option is to enable the Distributed Resource Scheduler (DRS) for the cluster.

⚠ Note	DRS can only be used if the evaluation license is still active or if a VMware vSphere Enterprise Plus edition is used.

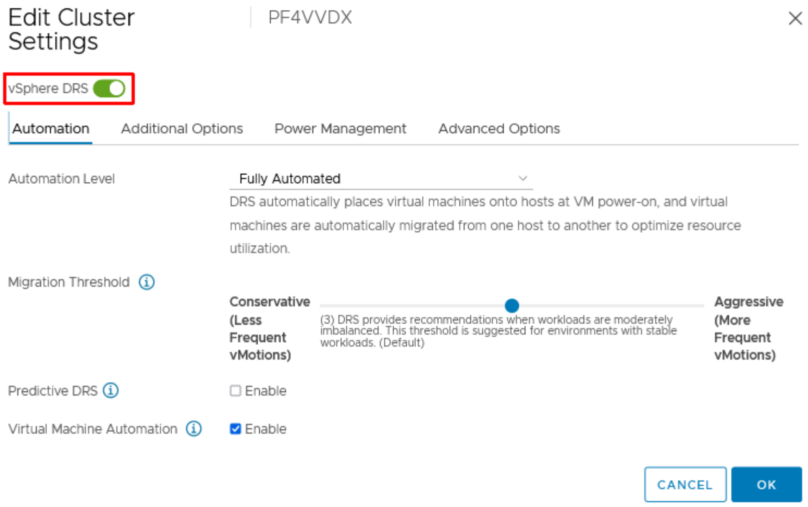
To enable DRS (maybe just temporarily), from the [**Host and Clusters**] view, click the

[**<cluster name>**] and open the [**Configure**] tab. Below [**Services**], select [**vSphere DRS**] and click on [**EDIT...**] then.



vSphere DRS is Turned OFF

On the opening dialog, click on the slider behind [**vSphere DRS**] to turn it on.



Automation Level: Fully Automated

DRS automatically places virtual machines onto hosts at VM power-on, and virtual machines are automatically migrated from one host to another to optimize resource utilization.

Migration Threshold: (3) DRS provides recommendations when workloads are moderately imbalanced. This threshold is suggested for environments with stable workloads. (Default)

Predictive DRS: ☐ Enable

Virtual Machine Automation: ☑ Enable

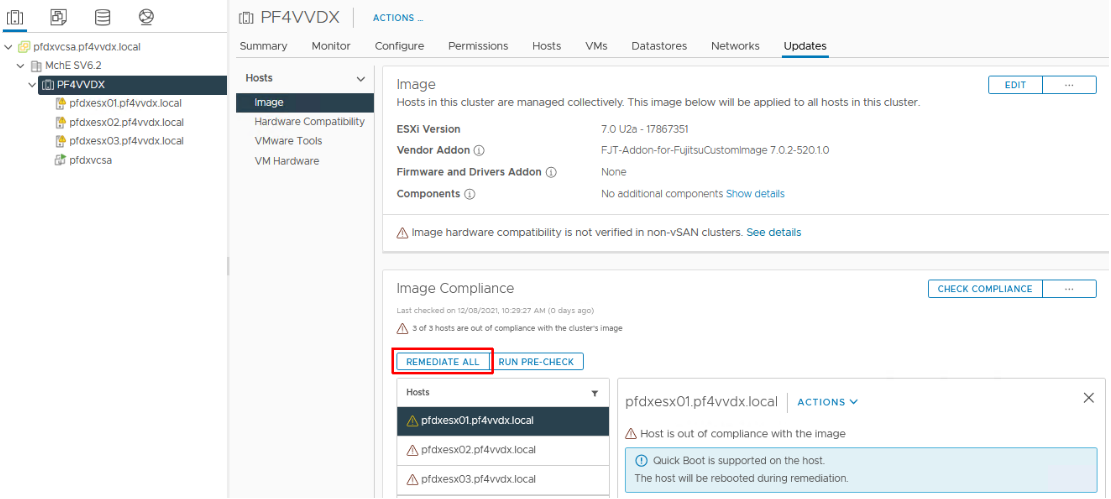
The required setting of [**Automation Level: Fully Automated]** is the default value.

Click [**OK**] to enable DRS.

C.5. Performing Remediation

If not all hosts are compliant with the image, you should run the remediation of the cluster.

From the [**Host and Clusters**] view, click the [**<cluster name>**]. open the [**Update**] tab and click [**Image**].



Image

Hosts in this cluster are managed collectively. This image below will be applied to all hosts in this cluster.

ESXi Version	7.0 U2a - 17867351
Vendor Addon	FJT-Addon-for-FujitsuCustomImage 7.0.2-520.1.0
Firmware and Drivers Addon	None
Components	No additional components Show details

⚠ Image hardware compatibility is not verified in non-vSAN clusters. See details

Image Compliance

Last checked on 12/08/2021, 10:29:27 AM (0 days ago)

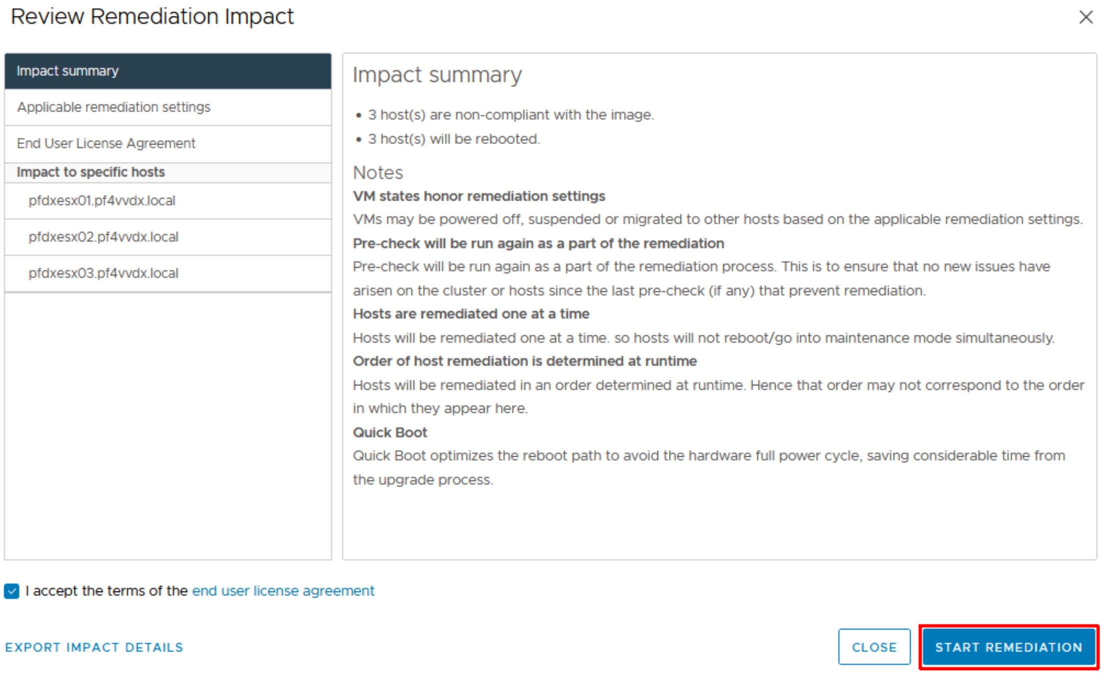
⚠ 3 of 3 hosts are out of compliance with the cluster's image

⚠ Host is out of compliance with the image

Quick Boot is supported on the host.
The host will be rebooted during remediation.

If the [**REMEDIATE ALL**] button is grayed out, either a remediation or a compliance check (e.g., triggered by the activation of DRS) is currently running. If so, wait until it completes.

Clicking on [**REMEDIATE ALL**] (or [**ACTIONS**] > [**Remediate**] for an individual host) will open a dialog which informs you about the impact of the procedure.



Review Remediation Impact

Impact summary

- 3 host(s) are non-compliant with the image.
- 3 host(s) will be rebooted.

Notes

VM states honor remediation settings

VMs may be powered off, suspended or migrated to other hosts based on the applicable remediation settings.

Pre-check will be run again as a part of the remediation

Pre-check will be run again as a part of the remediation process. This is to ensure that no new issues have arisen on the cluster or hosts since the last pre-check (if any) that prevent remediation.

Hosts are remediated one at a time

Hosts will be remediated one at a time. so hosts will not reboot/go into maintenance mode simultaneously.

Order of host remediation is determined at runtime

Hosts will be remediated in an order determined at runtime. Hence that order may not correspond to the order in which they appear here.

Quick Boot

Quick Boot optimizes the reboot path to avoid the hardware full power cycle, saving considerable time from the upgrade process.

☑ I accept the terms of the end user license agreement

Review it, set the checkmark in front of [**I accept the terms…**] and click [**START REMDEDIATION**] to start the remediation. The required tasks will run in the background then.

If vLCM uses its default settings and neither HA is disabled nor DRS is used for the cluster, host remediation may loop (by default 3 times with a delay of 5 minutes) because the host cannot be set to maintenance mode while any VMs are running on it.

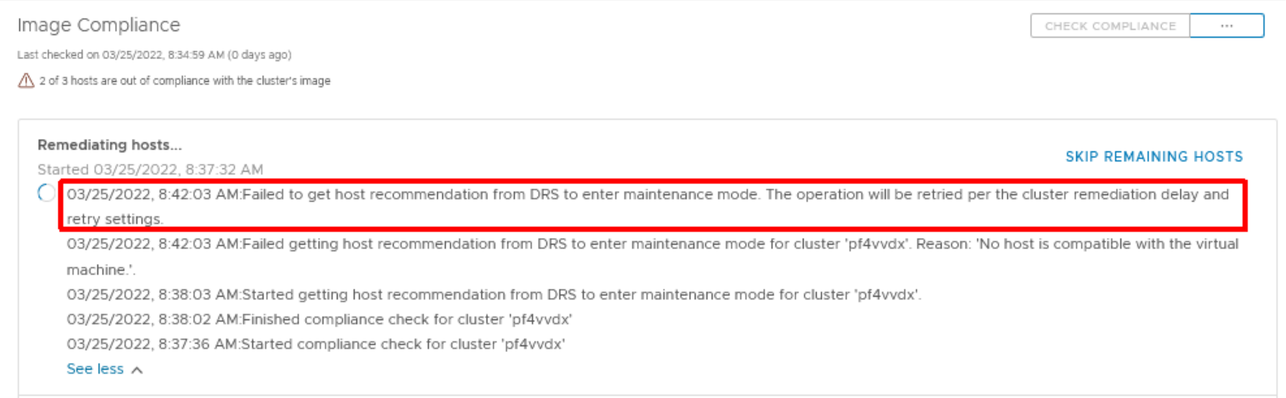


Image Compliance

Last checked on 03/25/2022, 8:34:59 AM (0 days ago)

⚠ 2 of 3 hosts are out of compliance with the cluster's image

Remediating hosts...

Started 03/25/2022, 8:37:32 AM

```
03/25/2022, 8:42:03 AM:Failed to get host recommendation from DRS to enter maintenance mode. The operation will be retried per the cluster remediation delay and retry settings.
03/25/2022, 8:42:03 AM:Failed getting host recommendation from DRS to enter maintenance mode for cluster 'pf4vvdx'. Reason: 'No host is compatible with the virtual machine.'.
03/25/2022, 8:38:03 AM:Started getting host recommendation from DRS to enter maintenance mode for cluster 'pf4vvdx'.
03/25/2022, 8:38:02 AM:Finished compliance check for cluster 'pf4vvdx'
03/25/2022, 8:37:36 AM:Started compliance check for cluster 'pf4vvdx'
```

Either change the approprate HA, DRS or vLCM settings or migrate all VMs from that host manually. The remediation will continue then.

⚠ Note	After remediation has completed, do not forget to enable HA or to disable DRS if you have changed its setting temporarily.

Appendix D: FAQ

D.1. What logs to include in a trouble ticket?

VCenter Server (vCSA):

/storage/log/vmware/vsphere-ui/logs/

/storage/log/vmware/vmware-updatemgr/vum-server/vmware-vum-server.log

/storage/log/vmware/vmware-updatemgr/vum-server/hwsupportmgrctl.log *)

/storage/log/vmware/vmware-updatemgr/vum-server/lifecycle.log *)

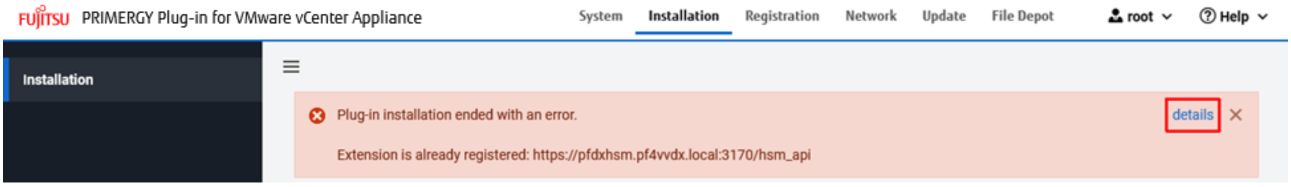
*) File does not exist until a remediation has been performed.

Plug-in appliance:

/opt/fujitsu/ServerViewSuite/webserver/logs/*

/var/log/fujitsu/*

D.2. Plug-in Installation ends with an error



Plug-in installation ended with an error.

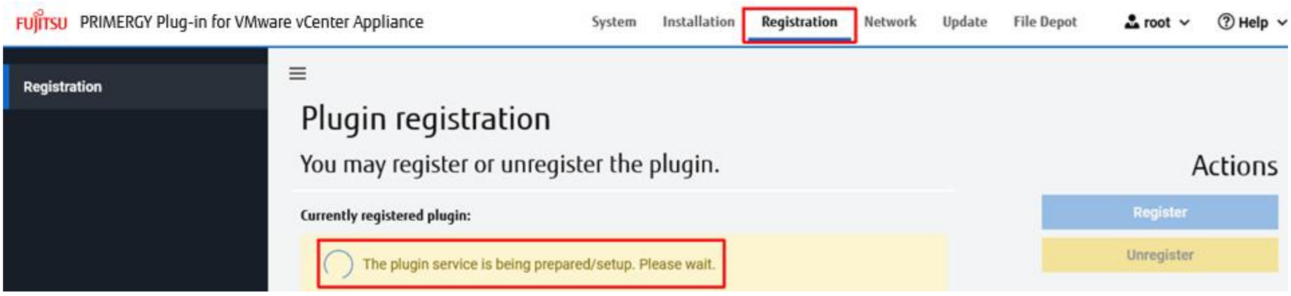
Extension is already registered: https://pfdxhsm.pf4vvdx.local:3170/hsm_api

Solution:

Click on [**details**] to display the message indicating the reason and act accordingly.

For instance, if the message tells you that the “Extension is already registered” as in the example above, the plug-in is already deployed on the vCenter Server, but the connection to the plug-in VA is apparently not working anymore. In such case, you need to remove the plug-in from vCenter Server manually as described in “Appendix B: Checking and Cleaning up Plug-In Registration”.

D.3. Plug-in Registration page loads incomplete.



Plugin registration

You may register or unregister the plugin.

Currently registered plugin:

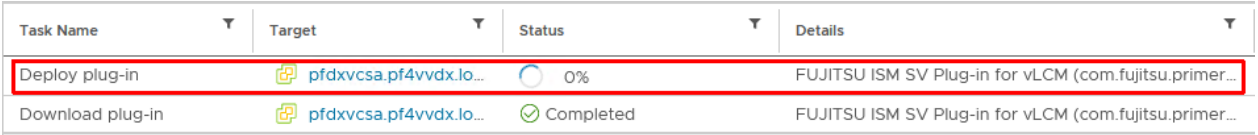
The plugin service is being prepared/setup. Please wait.

Reason:

The connection to the plug-in VA is apparently not working as expected, e.g., caused by downtime of the vCenter Server, networking issues or even a changed password of the account used for the plug-in registration.

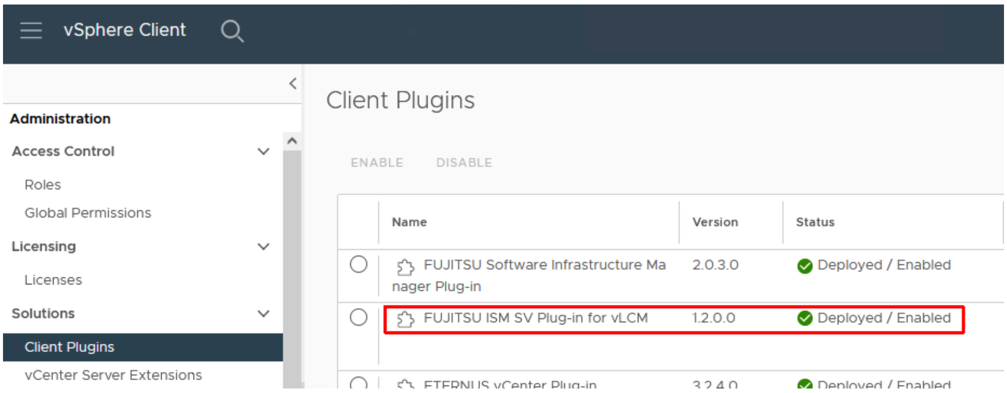
Solution:

If the problem is observed shortly after the plug-in registration, on vSphere Client, check the status of the plug-in deployment task and wait for its completion if necessary.



Task Name	Target	Status	Details
Deploy plug-in	pfdxvcsa.pf4vvdx.lo...	0%	FUJITSU ISM SV Plug-in for vLCM (com.fujitsu.primer...
Download plug-in	pfdxvcsa.pf4vvdx.lo...	✓ Completed	FUJITSU ISM SV Plug-in for vLCM (com.fujitsu.primer...

Otherwise check if the plug-in is really deployed and enabled on the vCenter Server.



Client Plugins

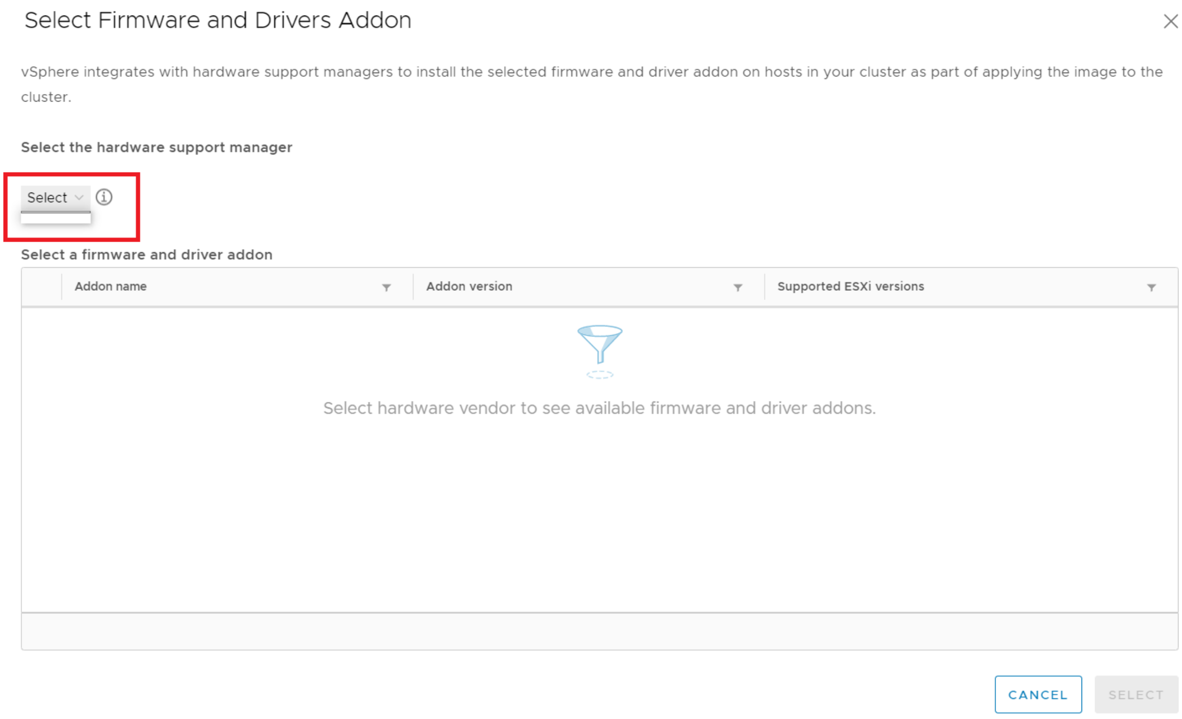
	Name	Version	Status
○	FUJITSU Software Infrastructure Manager Plug-in	2.0.3.0	✓ Deployed / Enabled
○	FUJITSU ISM SV Plug-in for vLCM	1.2.0.0	✓ Deployed / Enabled
○	ETERNUS vCenter Plug-in	3.2.4.0	✓ Deployed / Enabled

If so, make sure the password of the account specified during the plug-in installation is still valid. For further details refer to "9.5 Using custom user to login to vCenter

While using administrator account is possible to register plug-in, it's not recommended for safety reason. New user for vCenter can be created, used roles from appendix D.15 from this manual.

Changing vCenter User Password". The description there may also be helpful if the installation and registration of the plug-in has to be set up from scratch again.

D.4. Not able to select HSM.



Select Firmware and Drivers Addon

vSphere integrates with hardware support managers to install the selected firmware and driver addon on hosts in your cluster as part of applying the image to the cluster.

Select the hardware support manager

Select

Select a firmware and driver addon

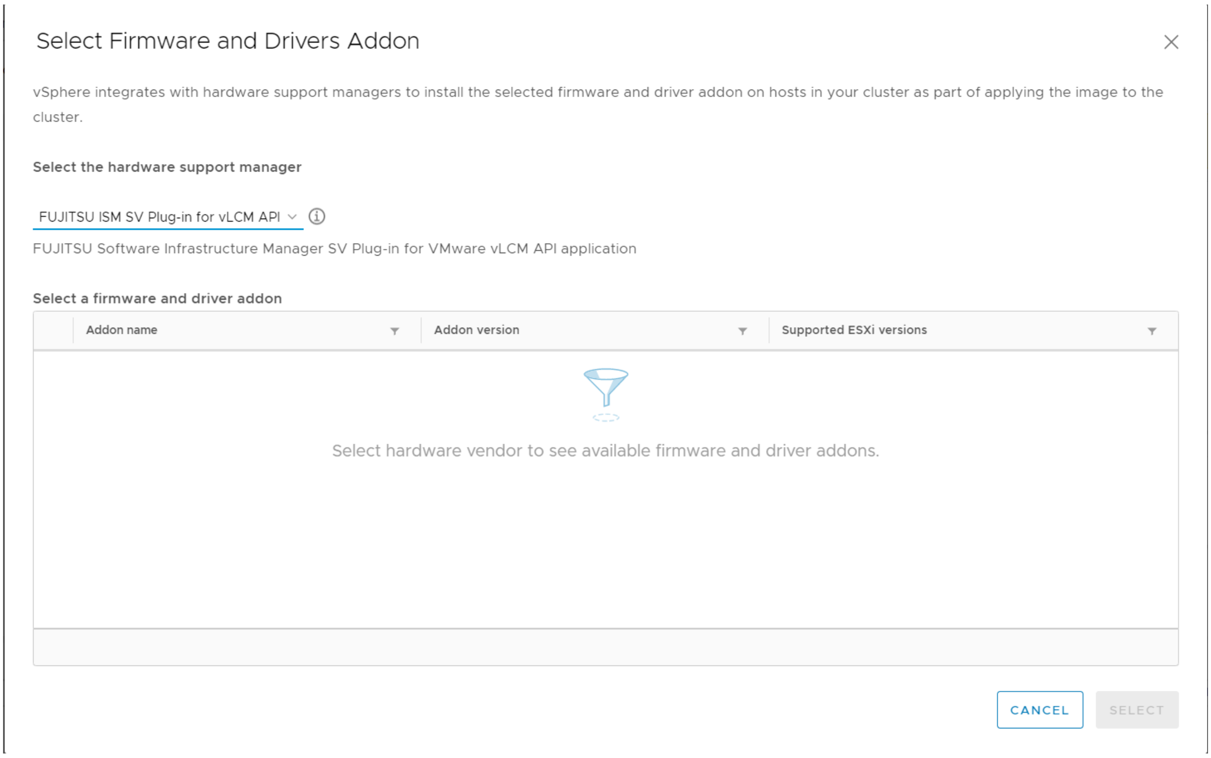
Addon name	Addon version	Supported ESXi versions

Select hardware vendor to see available firmware and driver addons.

Solution:

Register the plug-in as described in section “7.3.5 Registering the Plug-In”.

D.5. Not able to select HSP.



Select Firmware and Drivers Addon

vSphere integrates with hardware support managers to install the selected firmware and driver addon on hosts in your cluster as part of applying the image to the cluster.

Select the hardware support manager

FUJITSU ISM SV Plug-in for vLCM API

FUJITSU Software Infrastructure Manager SV Plug-in for VMware vLCM API application

Select a firmware and driver addon

Addon name	Addon version	Supported ESXi versions

Select hardware vendor to see available firmware and driver addons.

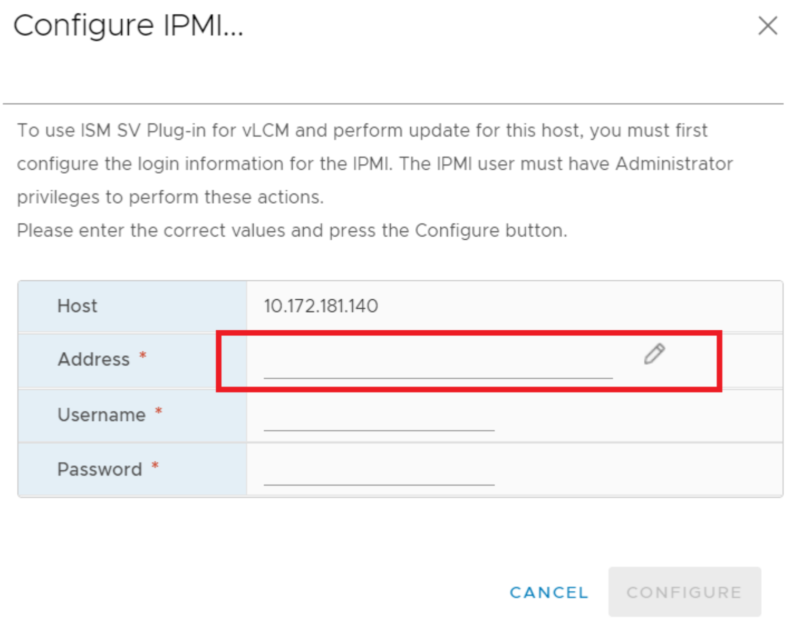
Reason:

Either the plug-in VA is not operable or cannot be reached through the network, or no HSP file has been uploaded to it.

Solution:

Make sure the plug-in VA is operable and at least one HSP has been uploaded, see “7.3.10 File Depot (HSP Upload)”.

D.6. iRMC address not filled automatically in Configure iRMC…


Configure IPMI…

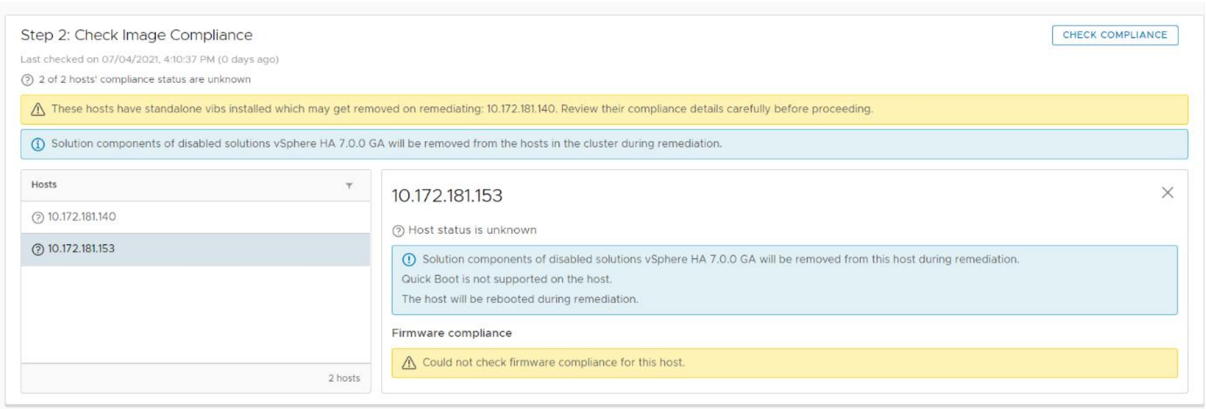
To use ISM SV Plug-in for vLCM and perform update for this host, you must first configure the login information for the IPMI. The IPMI user must have Administrator privileges to perform these actions.
Please enter the correct values and press the Configure button.

Host	10.172.181.140
Address *	
Username *	
Password *	

Solution:

Provide iRMC IP manually.

D.7. Firmware compliance check not working.


Step 2: Check Image Compliance

Last checked on 07/04/2021, 4:10:37 PM (0 days ago)

2 of 2 hosts' compliance status are unknown

These hosts have standalone vibs installed which may get removed on remediating: 10.172.181.140. Review their compliance details carefully before proceeding.

Solution components of disabled solutions vSphere HA 7.0.0 GA will be removed from the hosts in the cluster during remediation.

Hosts
10.172.181.140
10.172.181.153
2 hosts

10.172.181.153

Host status is unknown

Solution components of disabled solutions vSphere HA 7.0.0 GA will be removed from this host during remediation.
Quick Boot is not supported on the host.
The host will be rebooted during remediation.

Firmware compliance

Could not check firmware compliance for this host.

Reason:

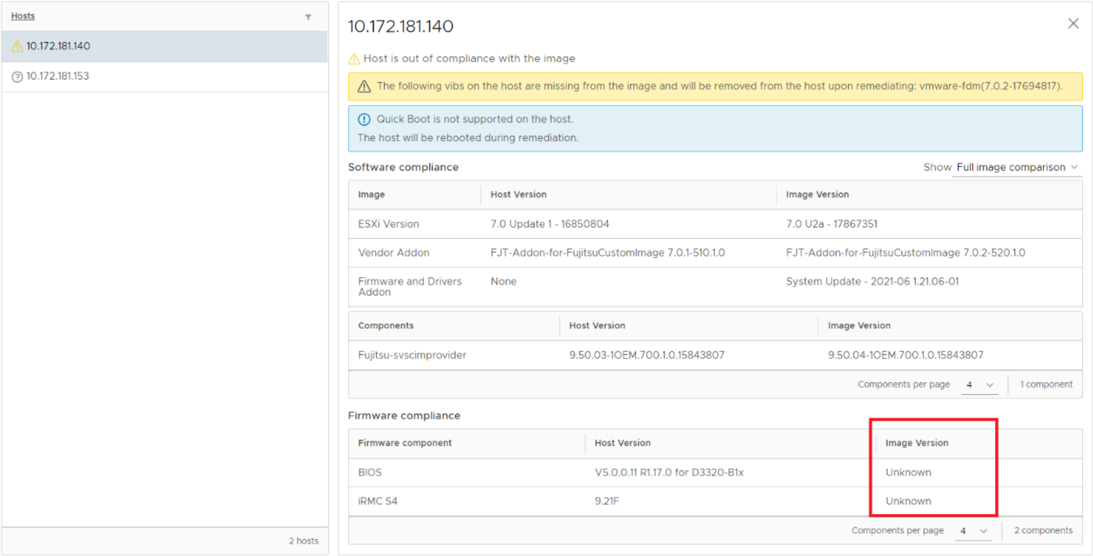
The plug-in is unable to establish a connection to the node's iRMC.

Solution:

Check whether the iRMC is operable. Make sure you have configured valid credentials as described in section "8.1.1 iRMC Configuration of the Cluster Nodes".

If you receive a message "iRMC address not found", you need to perform the configuration for each affected iRMC one by one, i.e. you need to use single-host configuration instead of bulk configuration.

D.8. Firmware compliance Image Version Unknown



Hosts

⚠ 10.172.181.140

? 10.172.181.153

2 hosts

10.172.181.140

⚠ Host is out of compliance with the image

⚠ The following vibs on the host are missing from the image and will be removed from the host upon remediating: vmware-fdm(7.0.2-17694817).

ⓘ Quick Boot is not supported on the host.
The host will be rebooted during remediation.

Software compliance — Show Full image comparison

Image	Host Version	Image Version
ESXi Version	7.0 Update 1 - 16850804	7.0 U2a - 17867351
Vendor Addon	FJT-Addon-for-FujitsuCustomImage 7.0.1-510.1.0	FJT-Addon-for-FujitsuCustomImage 7.0.2-520.1.0
Firmware and Drivers Addon	None	System Update - 2021-06 1.21.06-01

Components	Host Version	Image Version
Fujitsu-svscimprovider	9.50.03-1OEM.700.1.0.15843807	9.50.04-1OEM.700.1.0.15843807

Components per page 4 — 1 component

Firmware compliance

Firmware component	Host Version	Image Version
BIOS	V5.0.0.11 R1.17.0 for D3320-B1x	Unknown
iRMC S4	9.21F	Unknown

Components per page 4 — 2 components

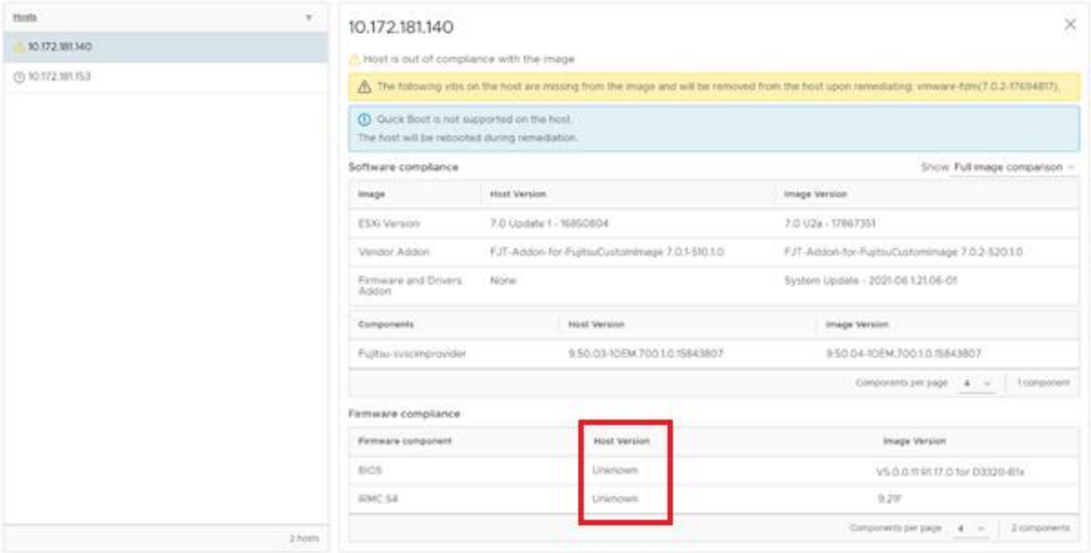
Reason:

The used HSP does not support the affected components.

Solution:

Make sure you are using the newest HSP file published.

D.9. Firmware compliance Host Version Unknown



Hosts

⚠ 10.172.181.140

? 10.172.181.153

2 hosts

10.172.181.140

⚠ Host is out of compliance with the image

⚠ The following vibs on the host are missing from the image and will be removed from the host upon remediating: vmware-fdm(7.0.2-17694817).

ⓘ Quick Boot is not supported on the host.
The host will be rebooted during remediation.

Software compliance — Show Full image comparison

Image	Host Version	Image Version
ESXi Version	7.0 Update 1 - 16850804	7.0 U2a - 17867351
Vendor Addon	FJT-Addon-for-FujitsuCustomImage 7.0.1-510.1.0	FJT-Addon-for-FujitsuCustomImage 7.0.2-520.1.0
Firmware and Drivers Addon	None	System Update - 2021-06 1.21.06-01

Components	Host Version	Image Version
Fujitsu-svscimprovider	9.50.03-1OEM.700.1.0.15843807	9.50.04-1OEM.700.1.0.15843807

Components per page 4 — 1 component

Firmware compliance

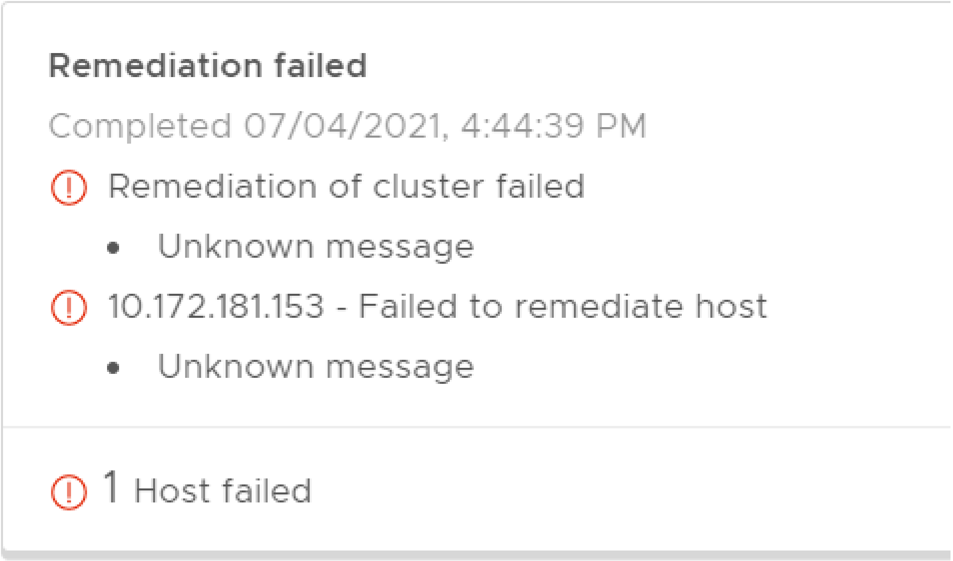
Firmware component	Host Version	Image Version
BIOS	Unknown	V5.0.0.11 R1.17.0 for D3320-B1x
iRMC S4	Unknown	9.21F

Components per page 4 — 2 components

It is possible, especially in case of network cards, that version on the host is defined in a form of an eTrackID. The external global flash files are required to resolve it into normal NVM version.

Please make sure, that the Repository files synchronization was successful., see section “7.3.10 File Depot (HSP Upload)”. If you are using the Offline method, you may need to upload newer copies of the files “versionAll.txt” and “GF_par_tree.exe” manually.

D.10. Host remediation failed with Unknown message.



Remediation failed

Completed 07/04/2021, 4:44:39 PM

ⓘ Remediation of cluster failed

- Unknown message

ⓘ 10.172.181.153 - Failed to remediate host

- Unknown message

ⓘ 1 Host failed

Solution:

Check VCenter Server log:

/storage/log/vmware/vmware-updatemgr/vum-server/vmware-vum-server.log

and plug-in appliance log:

/opt/fujitsu/ServerViewSuite/webserver/logs/hsm/hsm_api.<CURRENT_DATE>.log

D.11. vSphere Client does not show/works very slowly after multiple plugin installation/uninstallation/registration/deregistration.

This problem should only occur in exceptional cases, for instance in evaluation environments.

Solution:

! Warning	If you observe this issue in a production environment, we strongly recommend that you contact FUJITSU support to resolve the issue. The procedure described below should only be used in very exceptional cases. It will lead to downtime of the vSphere Client and mistakes may damage the vCSA.

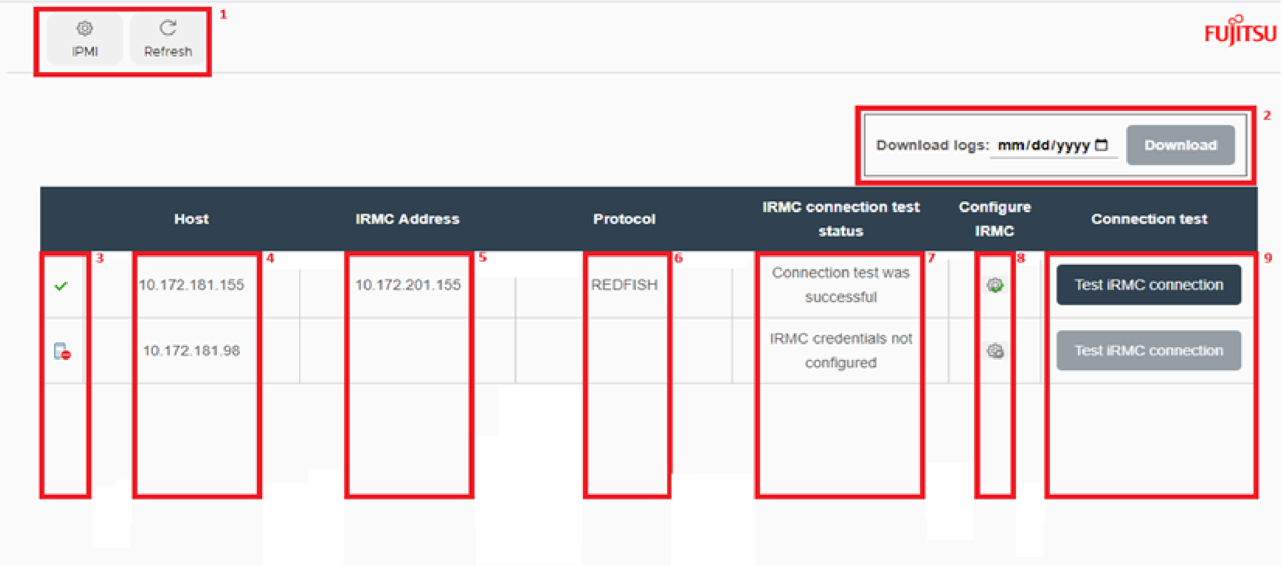
Connect to the vCSA root account using SSH and paste following commands:

```
shell
service-control --stop --all
rm -rf /etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity/com.fujitsu.primergy.hsm-*
service-control --start –all
```

D.12. iRMC session details when performing updates.

Please refer to section “8.7 List of registered hosts

To see a list of contained in certain cluster with all their respective statuses, navigate to this Cluster -> Monitor -> PRIMERGY Plug-in for VMware vCenter and you’ll be greeted with following view:



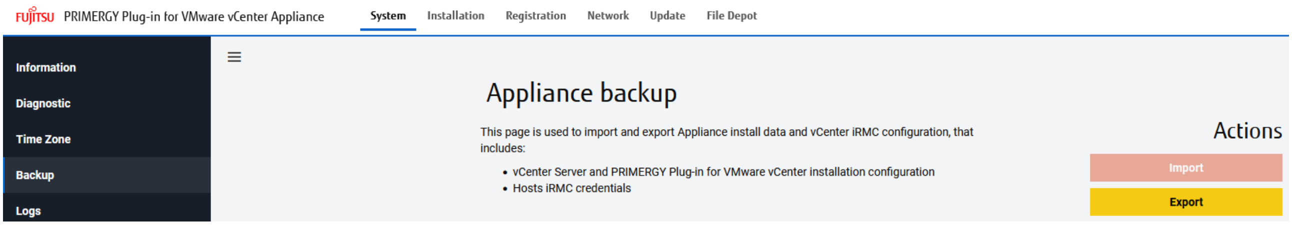
	Host	IRMC Address	Protocol	IRMC connection test status	Configure IRMC	Connection test
✓	10.172.181.155	10.172.201.155	REDFISH	Connection test was successful	⚙	Test iRMC connection
	10.172.181.98			IRMC credentials not configured	⚙	Test iRMC connection

10. IPMI button can register iRMC credentials for hosts, that have CIM. Refresh button will populate whole table with newest data.
11. Log downloader, after choosing proper date, it will generate support bundle. In case of any problems, please attach this file in your case.
12. Connection status icon returns information server connectivity to vCenter.
13. Hostname of server.

14. iRMC address. This field will be only available if server have CIM connection or configured iRMC connection.
15. Protocol by which all information are being downloaded.
16. Connection status text field returns results of tests ran in point 9. Of this list.
17. iRMC connection icon returns information about iRMC configuration. If host have provided proper iRMC credentials, there will be green check over cog. Can be used to configure iRMC.
18. Test button will run basic connection tests – DNS, necessary ports, and ping. The same tests are done every time user refresh this view.

9.13. Backup

In appliance of Plug-in, in System Tab, there is new Backup option. From there user can export his current plugin information such as vCenter login and password, proxy data, iRMC accesses. In case where Plug-in must be reinstalled, this may become handy and save some time for configuration.



Appliance backup

This page is used to import and export Appliance install data and vCenter iRMC configuration, that includes:

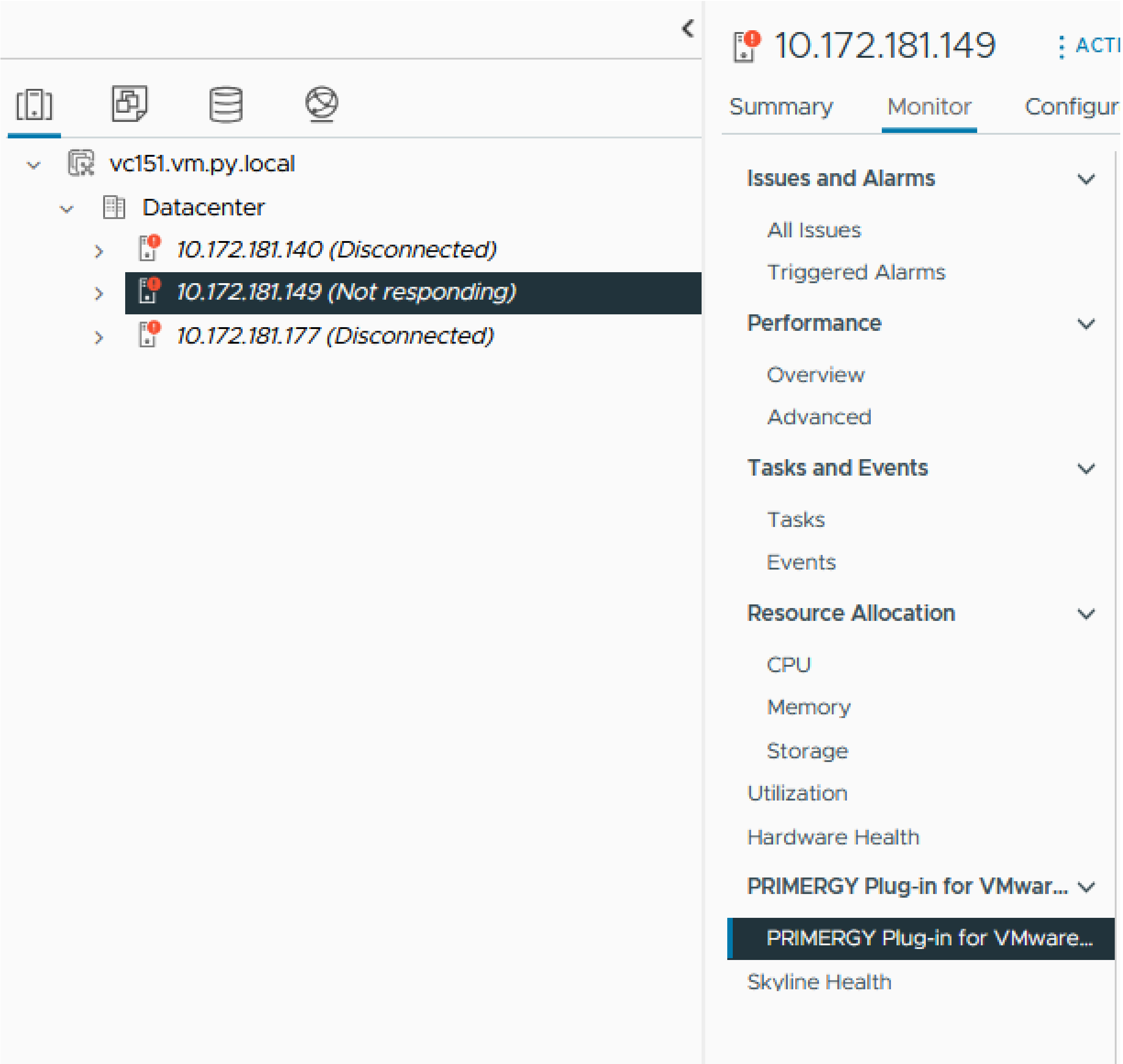
- vCenter Server and PRIMERGY Plug-in for VMware vCenter installation configuration
- Hosts iRMC credentials

All information will be retrieved as zip file, which can be later used in fresh installation of plugin, by choosing Import button. Exported filename should be “ssvexport.zip” and should remain unchanged.

❗ Warning	VM with Plug-in must have the same address and hostname for both instances!
❗ Warning	Please be aware that configuration in new Plug-in instance must be clear. There is “Reset Configuration” Button in case of any information previously saved.

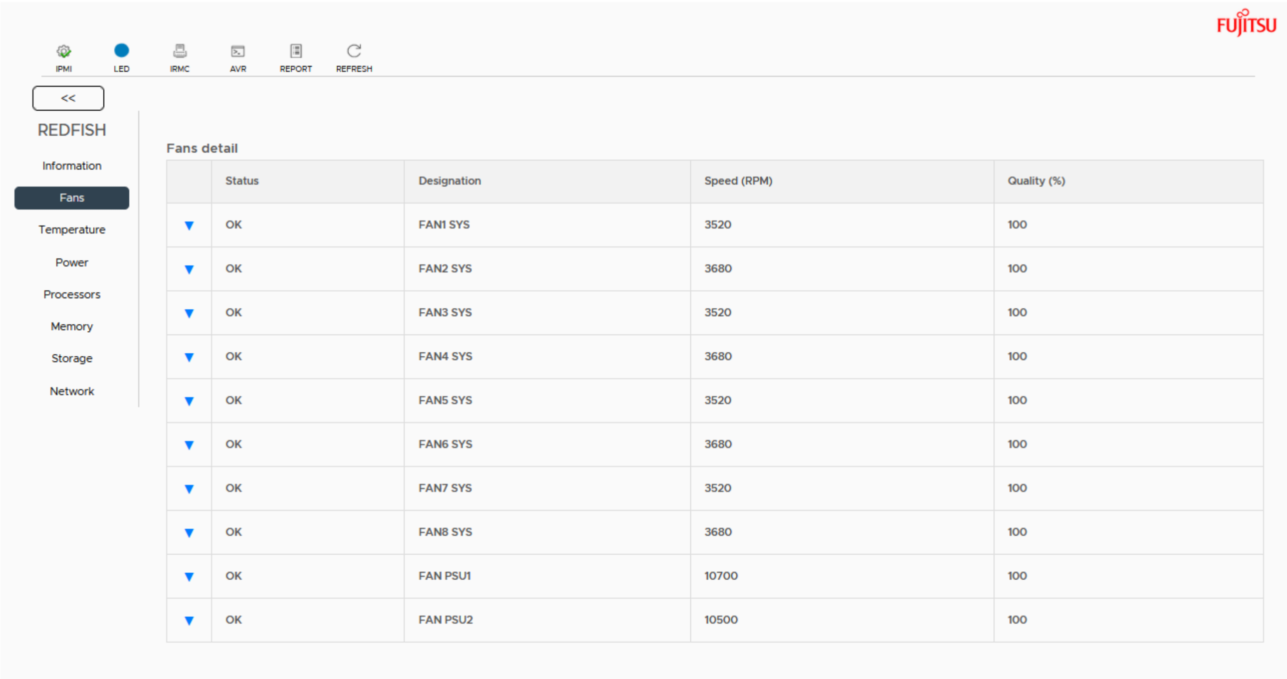
9.14. Host Monitoring

When server is chosen from inventory in vCenter, in “Monitor” tab there is “**PRIMERGY Plug-in for VMware vCenter**” entry available, which can be used to check health statuses for this host components.



If mentioned host have it's iRMC credentials provided, user will be able to collect information via Redfish regarding following data:

- General host information
- Fans
- Temperature
- Power
- Processors
- Memory
- Storage
- Network

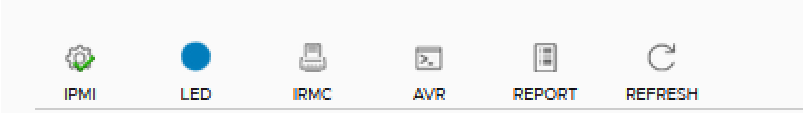


Fans detail

	Status	Designation	Speed (RPM)	Quality (%)
▼	OK	FAN1 SYS	3520	100
▼	OK	FAN2 SYS	3680	100
▼	OK	FAN3 SYS	3520	100
▼	OK	FAN4 SYS	3680	100
▼	OK	FAN5 SYS	3520	100
▼	OK	FAN6 SYS	3680	100
▼	OK	FAN7 SYS	3520	100
▼	OK	FAN8 SYS	3680	100
▼	OK	FAN PSU1	10700	100
▼	OK	FAN PSU2	10500	100

Additionally, at the top of monitor view there are buttons that gives user easy access to iRMC options:

- Configure iRMC credentials
- Turn on/off identification LED
- Open iRMC
- Open AVR
- Generatre report

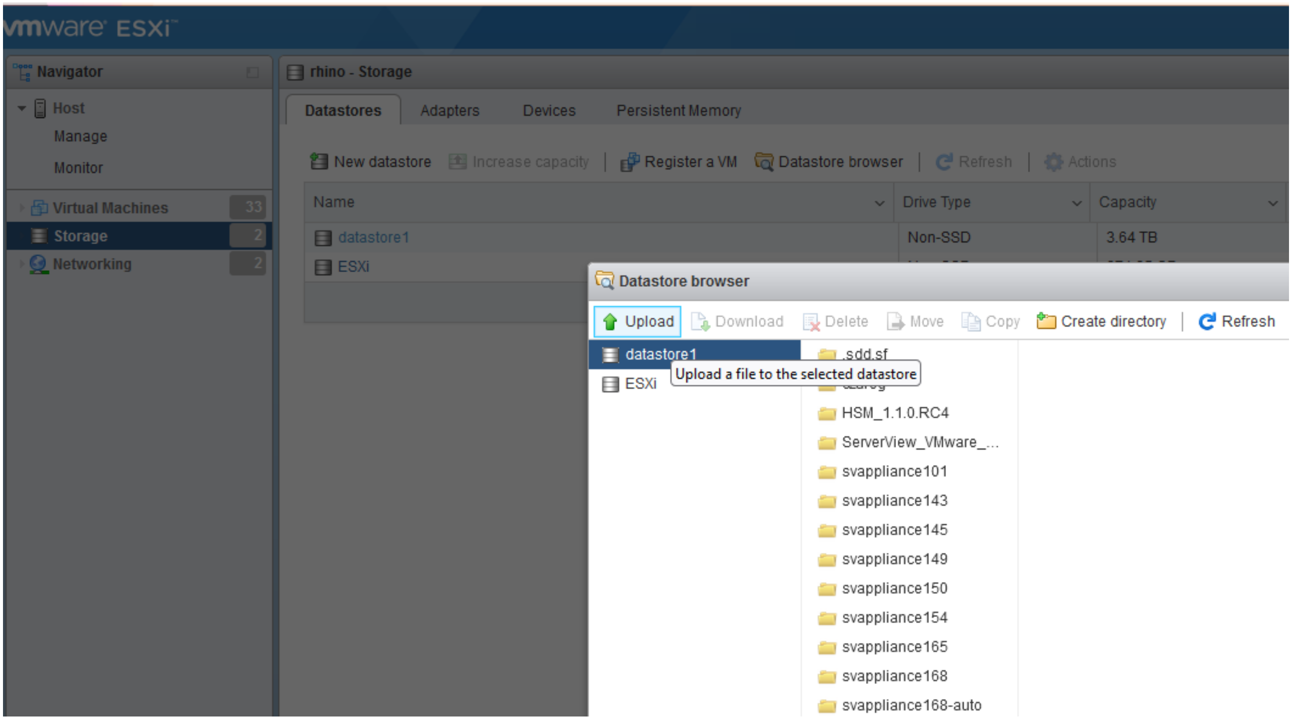


Note	To turn on and off LED on server, iRMC user need to have IPMI privileges set to Administrator or higher.

9.15. Appliance update

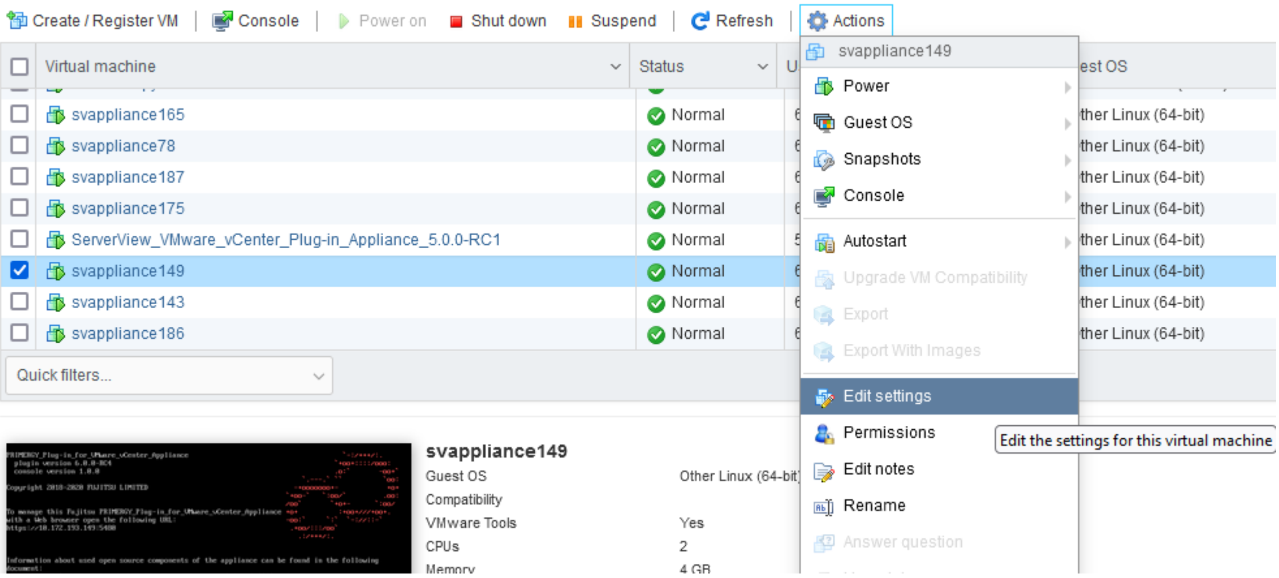
When new version of appliance is being released, it’s possible to use disc image file with updates to get newest version of it without reinstalling it.

Together with OVA file, ISO file will be provided. This must be uploaded to ESXi where plugin is deployed.



Name	Drive Type	Capacity
datastore1	Non-SSD	3.64 TB
ESXi		

Later on, to attach ISO to virtual machine go to its settings

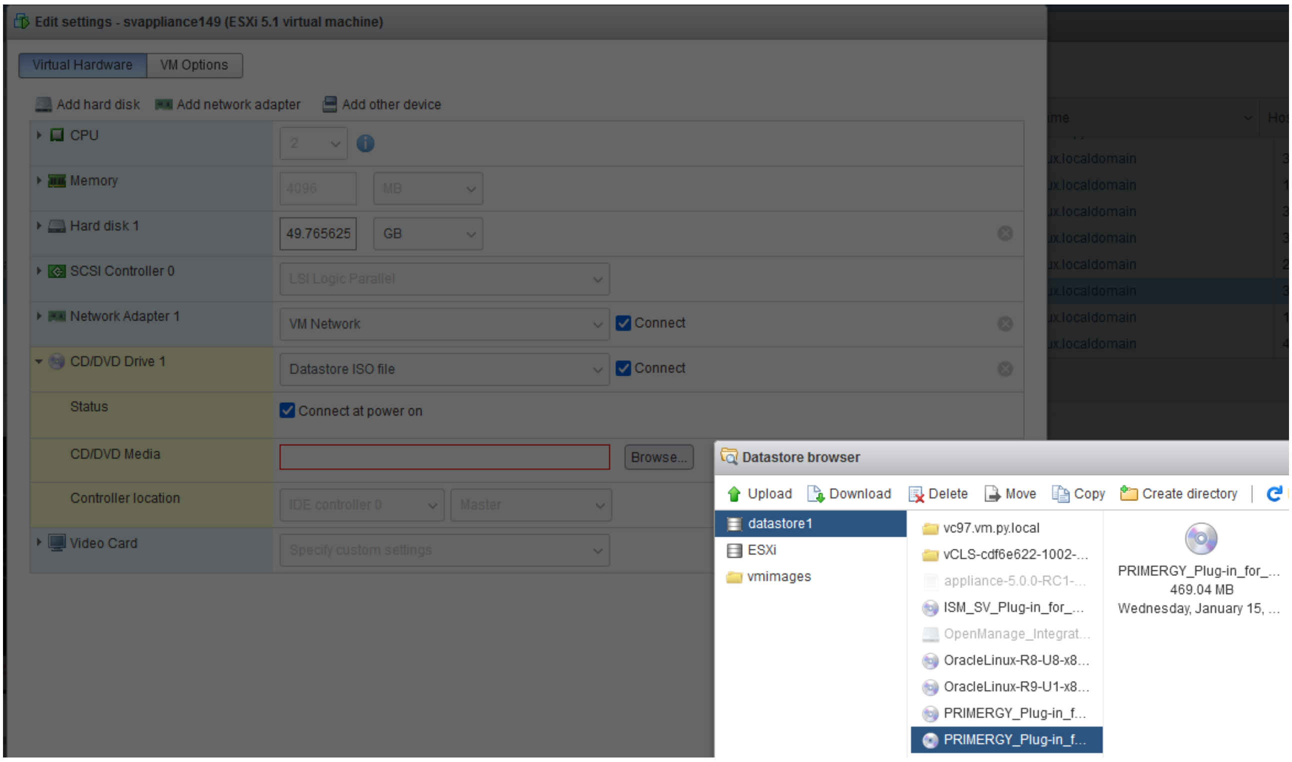


	Virtual machine	Status	est OS
□	svappliance165	Normal	ther Linux (64-bit)
□	svappliance78	Normal	ther Linux (64-bit)
□	svappliance187	Normal	ther Linux (64-bit)
□	svappliance175	Normal	ther Linux (64-bit)
□	ServerView_VMware_vCenter_Plug-in_Appliance_5.0.0-RC1	Normal	ther Linux (64-bit)
☑	svappliance149	Normal	ther Linux (64-bit)
□	svappliance143	Normal	ther Linux (64-bit)
□	svappliance186	Normal	ther Linux (64-bit)

svappliance149

Guest OS	Other Linux (64-bit)
Compatibility	
VMware Tools	Yes
CPUs	2
Memory	4 GB

And under “CD/DVD drive” chose disc image uploaded to server storage



Edit settings - svappliance149 (ESXi 5.1 virtual machine)

CPU: 2

Memory: 4096 MB

Hard disk 1: 49.765625 GB

SCSI Controller 0: LSI Logic Parallel

Network Adapter 1: VM Network ☑ Connect

CD/DVD Drive 1: Datastore ISO file ☑ Connect

Status: ☑ Connect at power on

CD/DVD Media: Browse...

Controller location: IDE controller 0 Master

Video Card: Specify custom settings

Datastore browser

datastore1

ESXi

vmimages

vc97.vm.py.local

vCLS-cdf6e622-1002-...

appliance-5.0.0-RC1-...

ISM_SV_Plug-in_for_...

OpenManage_Integrat...

OracleLinux-R8-U8-x8...

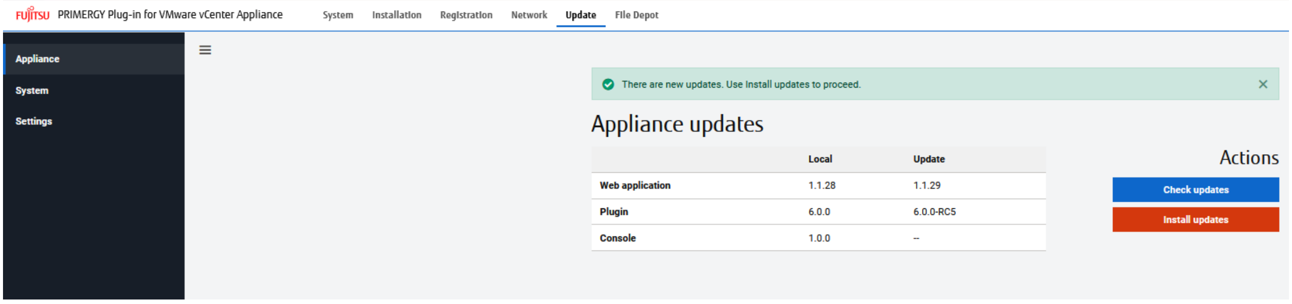
OracleLinux-R9-U1-x8...

PRIMERGY_Plug-in_f...

PRIMERGY_Plug-in_f...

PRIMERGY_Plug-in_for_...
469.04 MB
Wednesday, January 15, ...

When it's connected, you can go to your appliance under “Update” tab and hit “Check for updates” in “Appliance” section



PRIMERGY Plug-in for VMware vCenter Appliance

There are new updates. Use Install updates to proceed.

Appliance updates

	Local	Update
Web application	1.1.28	1.1.29
Plugin	6.0.0	6.0.0-RC5
Console	1.0.0	--

Actions

Proceed with install and your plugin will be updated.

Troubleshooting Remediation”.

D.13. Unknown error when saving vLCM Image.

Issue can be observed in case of vCenter 7.0.1 when saving the vLCM Image. After compliance check, hosts with ESXi version lower than the uploaded Image Offline Bundle or Image ESXi version can present the following message.

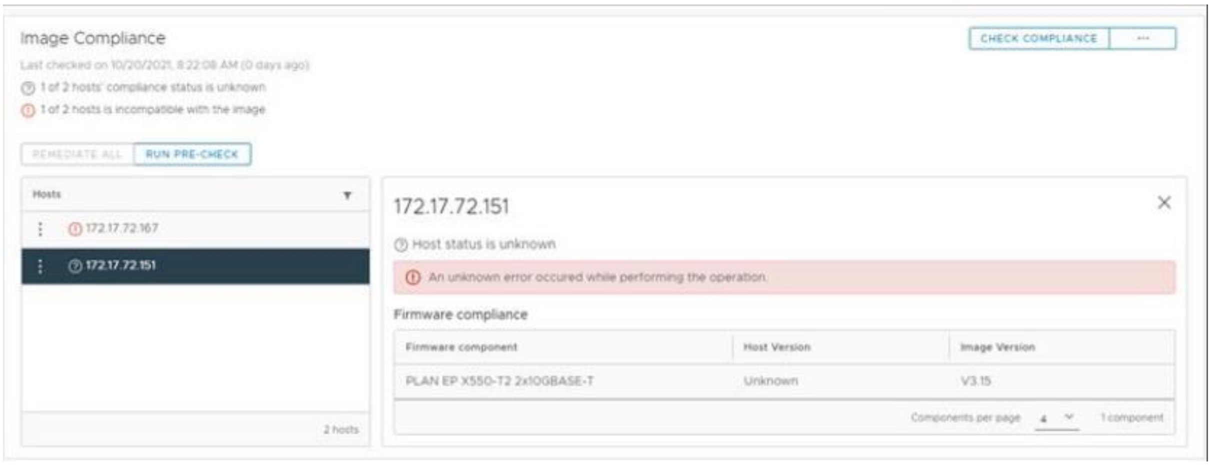


Image Compliance

Last checked on 10/20/2021, 8:22:08 AM (0 days ago)

1 of 2 hosts' compliance status is unknown

1 of 2 hosts is incompatible with the image

Hosts

- 172.17.72.167
- 172.17.72.151

2 hosts

172.17.72.151

Host status is unknown

An unknown error occured while performing the operation.

Firmware compliance

Firmware component	Host Version	Image Version
PLAN EP X550-T2 2x10GBASE-T	Unknown	V3.15

Components per page 4 · 1 component

We recommend using a newer version of vCenter Server – 7.0.2 and higher.

D.14. Custom Version Selector collecting inventory task is not getting finished and list of components is not being shown in the UI

In rare case of an issue where the Custom Version Selector is loading components for its hosts and does not proceed (observed around 80% of progress), please ensure the following:

- ensure your browser is updated to the latest version,
- check for any network configuration issues,
- disable browser extensions,
- clear your cache and cookies,
- trying incognito mode might resolve the issue, as it incorporates some of the previously mentioned suggestions,

If the issue persists, collect data from your browser's developer tools, specifically the console tab and network tab with a filter set to 'Fetch/XHR.' Focus on the outputs from at least the last 5 calls related to getting the task status, which can be easily identified as they start with the prefix “task-“.

After collecting this data, please contact your support center for further assistance in investigating and resolving the issue.

D.15. Privileges for custom user

Minimal roles needed to install vLCM plugin on the new user:

datastore:
  allocate space
  browse datastore
  configure datastore

extension:
  register extension
  unregister extension
  update extension

global:
diagnostics
licenses
settings

Roles needed to set up iRMC credentials for our plugin operations (needed to use for example the CVS or templates)
host:
CIM
CIM interaction
Tasks:
Create task
Update task

Roles needed to configure image, perform compliance check and remediation:

host:
Configuration
Connection
Image configuration
Maintenance

VMware vSphere Lifecycle Manager

Configure
Configure Service
Desired Configuration Management Privileges
Export desired cluster configuration
Modify desired cluster configuration.
Read-only access to desired configuration management platform
Remediate cluster to the desired configuration.
ESXi Health Perspectives
Read
Write
Lifecycle Manager: General Privileges
Read
Write
Lifecycle Manager: Hardware Compatibility Privileges
Access Hardware Compatibility
Write
Lifecycle Manager: Image Privileges
Read
Write
Lifecycle Manager: Image Remediation Privileges
Read
Write
Lifecycle Manager: Settings Privileges
Read

- Write
- Manage Baseline
  - Attach Baseline
  - Manage Baseline
- Manage Patches and Upgrades
  - Remediate to Apply Patches, Extensions, and Upgrades
  - Scan for Applicable Patches, Extensions, and Upgrades
  - Stage Patches and Extensions
  - View Compliance Status
- Upload file
  - Upload upgrade images and offline bundles