|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | |  |
| **Huawei FusionDirector Integrator for VMware vCenter**  **V0.2.3** | | |
| **User Guide** | | |
| **Issue** | **01** | |
| **Date** | **2020-05-06** | |
|  | | | | |
|  | HUAWEI TECHNOLOGIES CO., LTD. | |  |  |

|  |
| --- |
| **Copyright © Huawei Technologies Co., Ltd. 2020. All rights reserved.**  No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.  **Trademarks and Permissions**  and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.  All other trademarks and trade names mentioned in this document are the property of their respective holders.  **Notice**  The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.  The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. |

|  |  |
| --- | --- |
| Huawei Technologies Co., Ltd. | |
| Address: | Huawei Industrial Base  Bantian, Longgang  Shenzhen 518129  People's Republic of China |
| Website: | <https://e.huawei.com> |
|  |  |

About This Document

Purpose

This document describes the functional modules of the Huawei FusionDirector Integrator for VMware vCenter (FDIVV) and the functions of the FusionDirector for vCenter plug-in.

Intended Audience

This document is intended for:

* Technical support engineers
* System maintenance engineer

Symbol Conventions

The symbols that may be found in this document are defined as follows.

| Symbol | Description |
| --- | --- |
|  | Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury. |
|  | Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury. |
|  | Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury. |
|  | Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results.  **NOTICE** is used to address practices not related to personal injury. |
|  | Calls attention to important information, best practices, and tips.  **NOTE** is used to address information not related to personal injury, equipment damage, and environment deterioration. |

Change History

Changes between document issues are cumulative. The latest document issue contains all changes made in earlier issues.

| Issue | Release Date | Description |
| --- | --- | --- |
| 01 | 2020-05-06 | The issue is the first official release. |

Contents

[About This Document ii](#_Toc39677226)

[1 Overview 1](#_Toc39677227)

[2 Deploying FDIVV 2](#_Toc39677228)

[2.1 System Requirement 2](#_Toc39677229)

[2.2 Installing FDIVV 2](#_Toc39677230)

[2.3 Configuring the Network 6](#_Toc39677231)

[3 FDIVV WebUI 8](#_Toc39677232)

[4 Configuring FDIVV 10](#_Toc39677233)

[4.1 Logging In to the FDIVV WebUI 10](#_Toc39677234)

[4.2 System Configuration 11](#_Toc39677235)

[4.2.1 Configuring the Device and Network 11](#_Toc39677236)

[4.2.2 Configuring NTP and Time 14](#_Toc39677237)

[4.3 vCenter Server Management 17](#_Toc39677238)

[4.3.1 Adding a vCenter Server 17](#_Toc39677239)

[4.3.2 Modifying a vCenter Server 22](#_Toc39677240)

[4.3.3 Deleting a vCenter Server 22](#_Toc39677241)

[4.4 FusionDirector Management 25](#_Toc39677242)

[4.4.1 Adding a FusionDirector System 25](#_Toc39677243)

[4.4.2 Modifying a FusionDirector System 28](#_Toc39677244)

[4.4.3 Deleting a FusionDirector System 29](#_Toc39677245)

[5 Functions of the FusionDirector for vCenter Plug-in 30](#_Toc39677246)

[5.1 Introduction to the FusionDirector for vCenter Plug-in 30](#_Toc39677247)

[5.2 Checking the FusionDirector for vCenter plug-in Version 31](#_Toc39677248)

[5.3 Configuring vCenter 31](#_Toc39677249)

[5.4 Configuring FDIVV 32](#_Toc39677250)

[5.5 Server Management 34](#_Toc39677251)

[5.5.1 Viewing Server Information 34](#_Toc39677252)

[5.5.2 Configuring Servers 35](#_Toc39677253)

[5.5.2.1 Setting BIOS Parameters 38](#_Toc39677254)

[5.5.2.2 Setting RAID Parameters 52](#_Toc39677255)

[5.5.2.3 Setting NTP Parameters 54](#_Toc39677256)

[5.5.2.4 Setting DNS Parameters 56](#_Toc39677257)

[5.5.2.5 Setting LDAP Parameters 57](#_Toc39677258)

[5.5.3 Deploying an OS 60](#_Toc39677259)

[5.5.3.1 OS Image 60](#_Toc39677260)

[5.5.3.2 Creating an OS Deployment Template 62](#_Toc39677261)

[5.5.3.3 OS Deployment 63](#_Toc39677262)

[5.5.4 Upgrading Firmware and Drivers 65](#_Toc39677263)

[5.5.4.1 Version Repository Management 65](#_Toc39677264)

[5.5.4.1.1 Uploading an Update Package 65](#_Toc39677265)

[5.5.4.1.2 Customizing a Baseline 68](#_Toc39677266)

[5.5.4.2 Update Schedule Management 70](#_Toc39677267)

[5.5.4.2.1 Creating an Update Schedule 70](#_Toc39677268)

[5.5.4.2.2 Viewing the Update Schedule 73](#_Toc39677269)

[5.5.4.3 Checking Device Version and Status 74](#_Toc39677270)

[5.5.5 Configuring and Using Proactive HA 75](#_Toc39677271)

[5.5.5.1 Adding a Host to a Cluster 75](#_Toc39677272)

[5.5.5.2 Configuring Proactive HA 80](#_Toc39677273)

[5.5.5.3 Using Proactive HA 84](#_Toc39677274)

[5.5.6 Viewing Server Alarms and Events 86](#_Toc39677275)

[6 Other Functions of FDIVV 90](#_Toc39677276)

[6.1 System Operations 90](#_Toc39677277)

[6.1.1 Set Session 90](#_Toc39677278)

[6.1.2 Downloading Logs 92](#_Toc39677279)

[6.1.3 Shutting Down the VM 92](#_Toc39677280)

[6.1.4 Restarting the VM 93](#_Toc39677281)

[6.2 Logging Out 95](#_Toc39677282)

[6.3 Changing the Login Password 95](#_Toc39677283)

[6.4 Certificate Management 96](#_Toc39677284)

[6.4.1 Server Certificate 96](#_Toc39677285)

[6.4.2 FusionDirector Certificate 100](#_Toc39677286)

[6.4.3 vCenter Server Certificate 100](#_Toc39677287)

[7 FAQs 102](#_Toc39677288)

[7.1 How to Add a Server ESXi System to a vCenter Cluster 102](#_Toc39677289)

[7.2 FusionDirector for vCenter Icon Is Not Displayed on the vCenter Shortcuts Page 103](#_Toc39677290)

[7.2.1 Plug-in Icon Is Not Displayed After I Log In to vCenter Again 103](#_Toc39677291)

[7.2.2 Plug-in Icon Is Not Displayed After the vCenter Server Is Deleted and Added Again 107](#_Toc39677292)

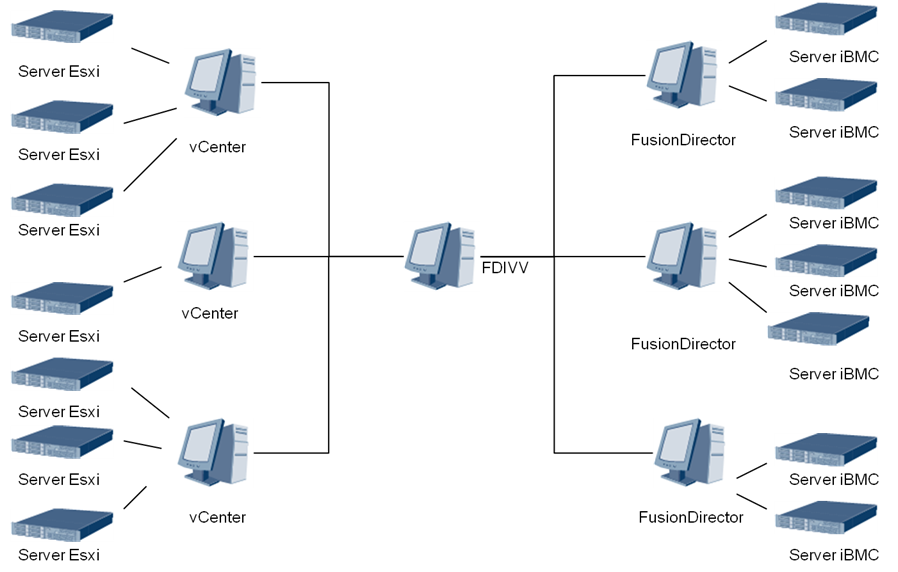
[7.3 How to Change the Default Password Used for the Communication Between the FusionDirector for vCenter Plug-in and FDIVV 111](#_Toc39677293)

# Overview

FDIVV is the software developed by Huawei that functions as a bridge between FusionDirector and VMware vCenter. When adding VMware vCenter to FDIVV, you can integrate the FusionDirector for vCenter plug-in into vCenter to implement OS deployment, server configuration, firmware upgrade, and server monitoring for Huawei servers. Figure 1-1 shows the networking between FDIVV, VMware vCenter, and FusionDirector.

FDIVV supports the installation of plug-ins in FLEX mode on vCenter 6.5 and the installation of plug-ins in HTML5 mode on vCenter 6.7.

Network diagram



# Deploying FDIVV

[2.1 System Requirement](#_EN-US_TOPIC_0184730436)

[2.2 Installing FDIVV](#_EN-US_TOPIC_0184730373)

[2.3 Configuring the Network](#_EN-US_TOPIC_0187445947)

## System Requirement

FDIVV is installed on the VMware ESXi VM. ESXi 5.5, 6.0, 6.5, and 6.7 are supported.

## Installing FDIVV

Prerequisites

The VMware ESXi VM for installing FDIVV is available.

Installing FDIVV

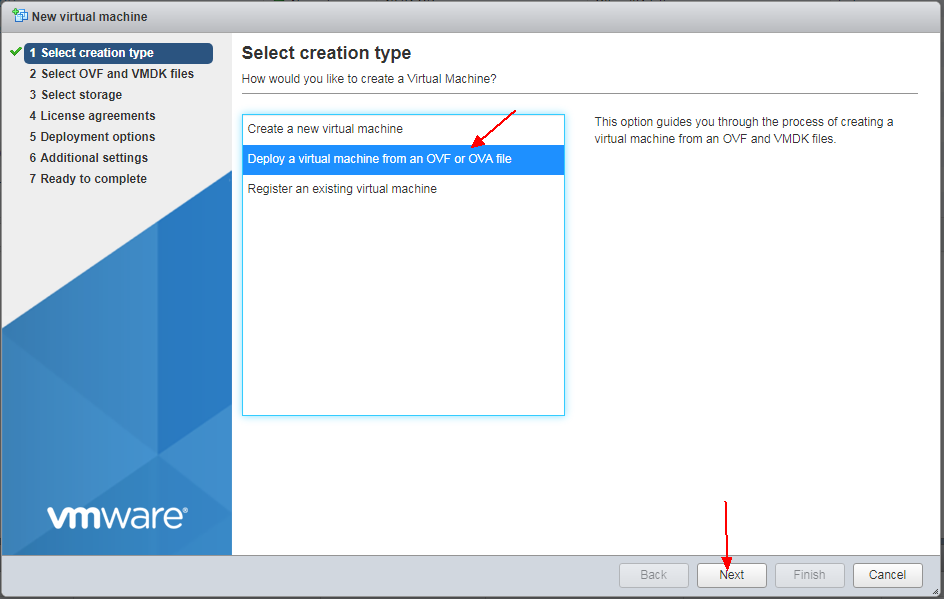
The following uses the VMware ESXi VM of version 6.5.0 as an example.

Log in to the VMware ESXi VM.

On the home page of the VMware ESXi VM, click **Create/Register VM**.

On the displayed **Select creation type** page, choose **Deploy a virtual machine from an OVF or OVA file**, as shown in Figure 2-1.

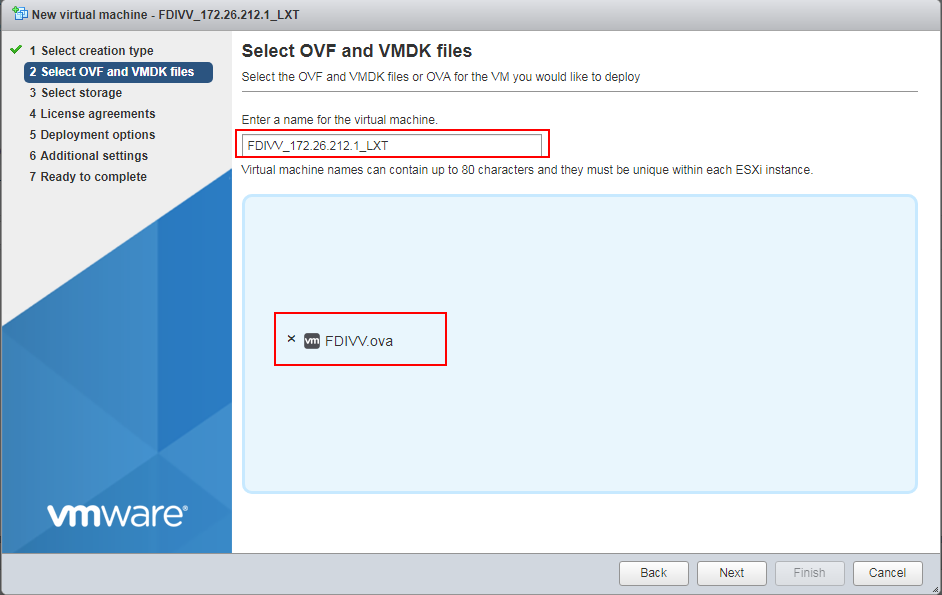
Select creation type page



Click Next. The **Select OVF and VMDK files** page is displayed.

Enter the VM name and select the OVF and VMDK files or the OVA file for the VM to be deployed, as shown in Figure 2-2.

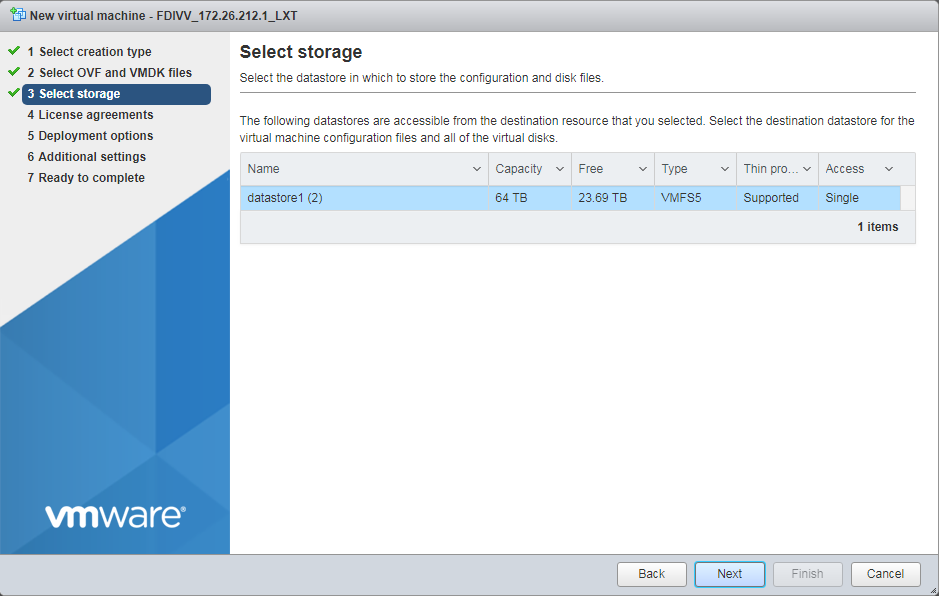
Select OVF and VMDK files page



Click **Next**. The **Select storage** page is displayed.

Retain the default settings, as shown in Figure 2-3.

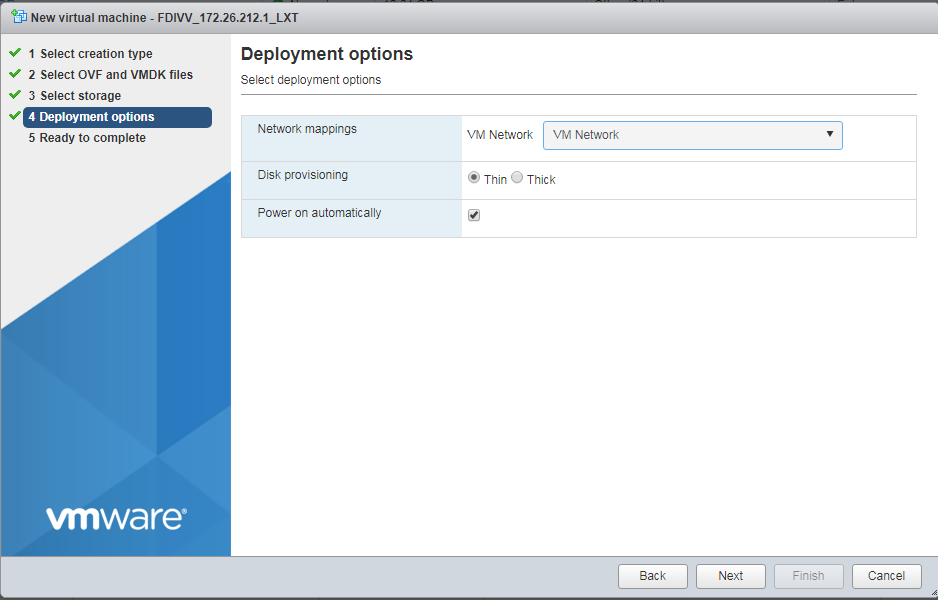
Select storage page



Click **Next**. The **Deployment options** page is displayed.

Set **VM Network** to **VM Network** and **Disk provisioning** to **Thin**. You can select **Power on automatically**, as shown in Figure 2-4.

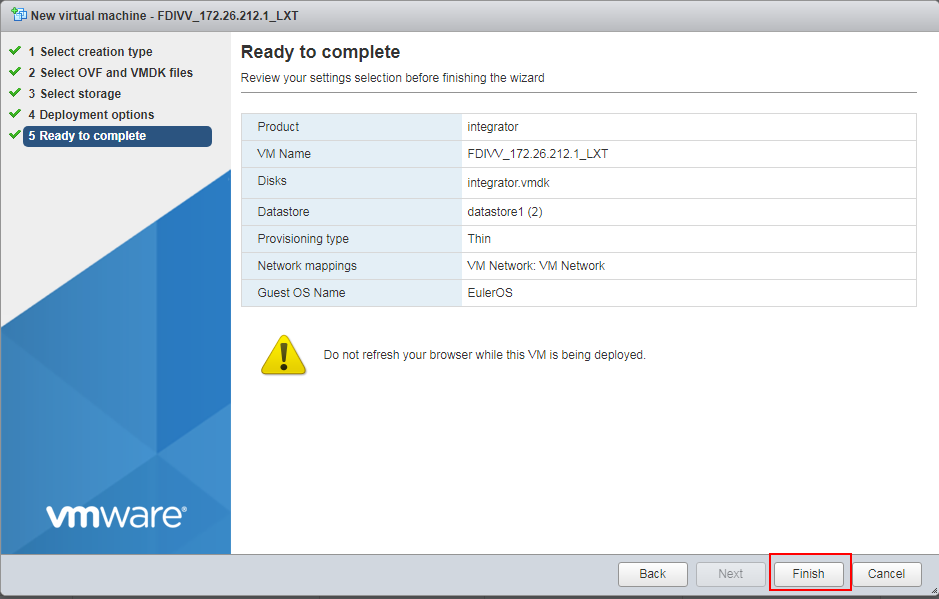
Deployment options page



Click **Next**. The **Ready to complete** page is displayed.

Click **Finish**. The VM is created, as shown in Figure 2-5.

Ready to complete page



----End

## Configuring the Network



* The IP address of the default eth0 of the VM is 192.168.251.251. To modify the network configuration of eth0, perform the following steps.
* If two network interface cards (NICs) are configured, the IP address of eth1 is obtained in DHCP mode by default.
* The network segment of the vCenter service must be the same as that of the eth0 NIC of the FDIVV.

On the VMware ESXi home page, click **Virtual Machines** on the left.

You can view the list of created VMs.

Click the name of the VM for which the network is to be configured. The VM home page is displayed.

Click to open the browser console of the VM.

On the console page, enter the user name and password to log in to the VM.



The default user name and password are **root** and **Huawei@SYS3** respectively.

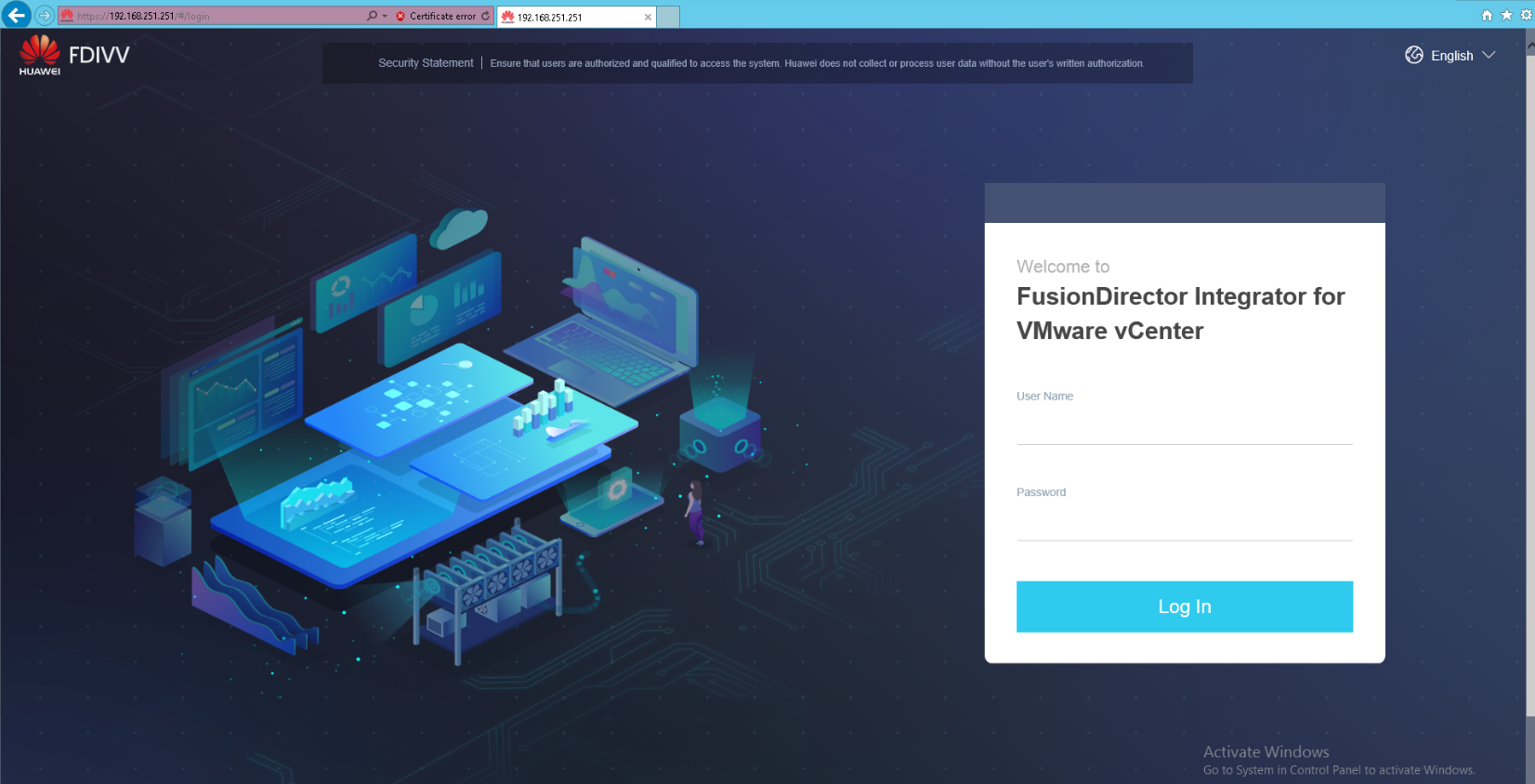
In the address box of the browser, enter **https://192.168.251.251** and press **Enter**.

The FDIVV WebUI login page is displayed, as shown in Figure 2-6.



The network segment for logging in to the environment must be the same as that of the default eth0 of the VM.

FDIVV WebUI login page



Enter the user name and password for logging in to the FDIVV WebUI.

The FDIVV home page is displayed.

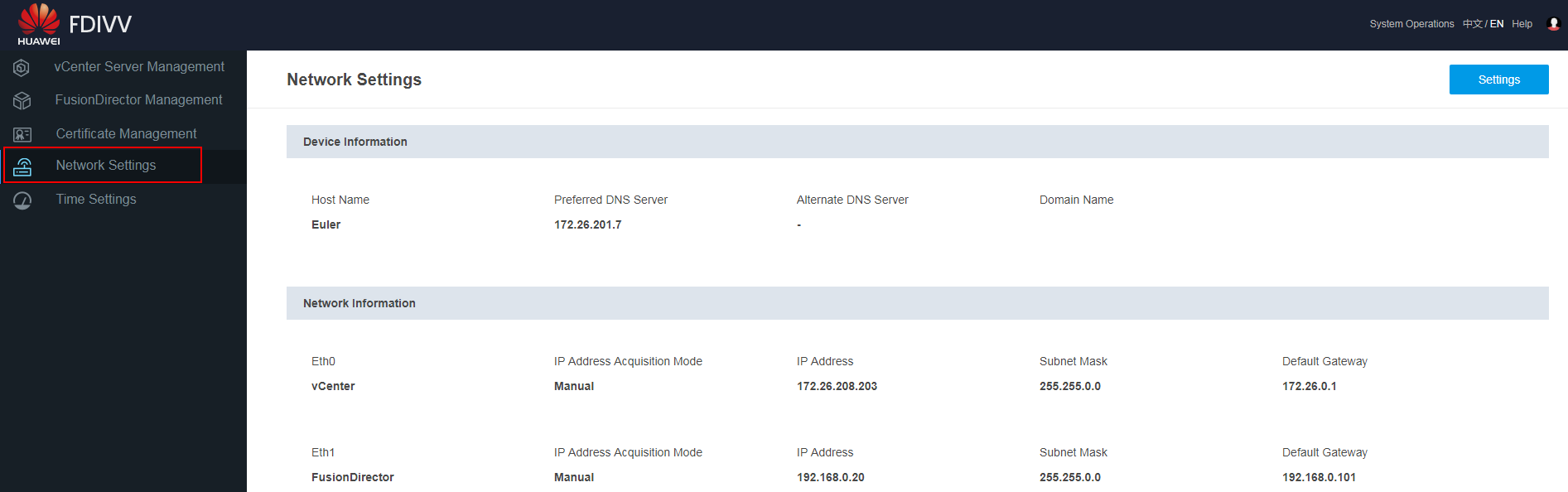


The default user name and password of FDIVV are **Administrator** and **Admin@9000** respectively.

On the FDIVV WebUI, choose **Network Settings**.

The **Network Settings** page is displayed, as shown in Figure 2-7.

Network Settings page



Modify the network settings on the **Network Settings** page. For details, see 4.2.1 Configuring the Device and Network.

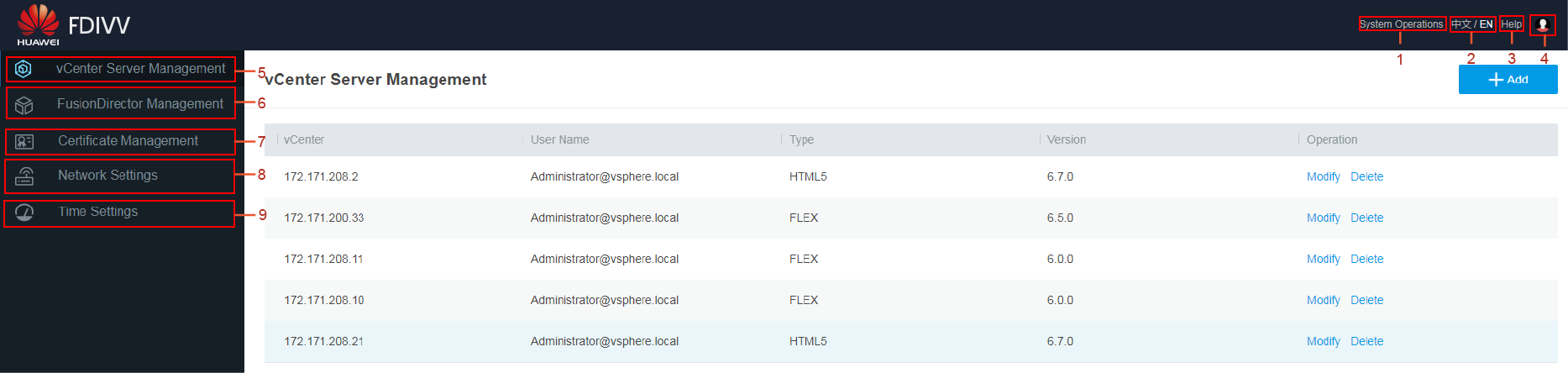
After the network settings are modified, you can use the new IP address to log in to the FDIVV WebUI. For details about how to log in to the FDIVV WebUI, see 4.1 Logging In to the FDIVV WebUI.

----End

# FDIVV WebUI

Figure 3-1 shows the areas of the FDIVV WebUI. Table 3-1 describes the functions of the areas.

FDIVV WebUI



Elements of the home page of the FDIVV WebUI

| No. | Element | Description |
| --- | --- | --- |
| 1 | System Operations | Provides entries for setting session, downloading logs, powering off the system, and restarting the system. For details, see 6.1 System Operations. |
| 2 | 中文 / EN | Switches the language between simplified Chinese and English. |
| 3 | Help | Provides online help for GUI information, operations, and shows FDIVV version information. |
| 4 |  | Displays information about the current user and the last user, and provides entries for logging out of the system and changing the password. For details, see 6.2 Logging Out and 6.3 Changing the Login Password. |
| 5 | vCenter Server Management | Displays the list of added vCenter servers and provides entries for adding, modifying, and deleting vCenter servers. For details, see 4.3 vCenter Server Management. |
| 6 | FusionDirector Management | Displays the list of added FusionDirector systems and provides entries for adding, modifying, and deleting FusionDirector systems. For details, see 4.4 FusionDirector Management. |
| 7 | Certificate Management | Displays the information about the server certificate, vCenter server certificate, and FusionDirector certificate, and provides entries for modifying the certificates. For details, see 6.4 Certificate Management. |
| 8 | Network Settings | Displays the current device and network information and provides entries for configuring the device and network. For details, see 4.2.1 Configuring the Device and Network. |
| 9 | Time Settings | Displays the current NTP and time information and provides entries for configuring NTP and time. For details, see 4.2.2 Configuring NTP and Time. |

# Configuring FDIVV

[4.1 Logging In to the FDIVV WebUI](#_EN-US_TOPIC_0184730485)

[4.2 System Configuration](#_EN-US_TOPIC_0184730509)

[4.3 vCenter Server Management](#_EN-US_TOPIC_0184730353)

[4.4 FusionDirector Management](#_EN-US_TOPIC_0184730541)

## Logging In to the FDIVV WebUI

Prerequisites

You have obtained the IP address, user name, and password for logging in to FDIVV.

The default user name is **Administrator**, and the default password is **Admin@9000**.

Procedure

Open a browser on the maintenance terminal.



FDIVV supports the following browsers: Google Chrome, Mozilla Firefox, Internet Explorer (IE), Microsoft Edge, and Sarafi.

In the address box of the browser, enter **https://***XXX.XXX.XXX.XXX* and press **Enter**.



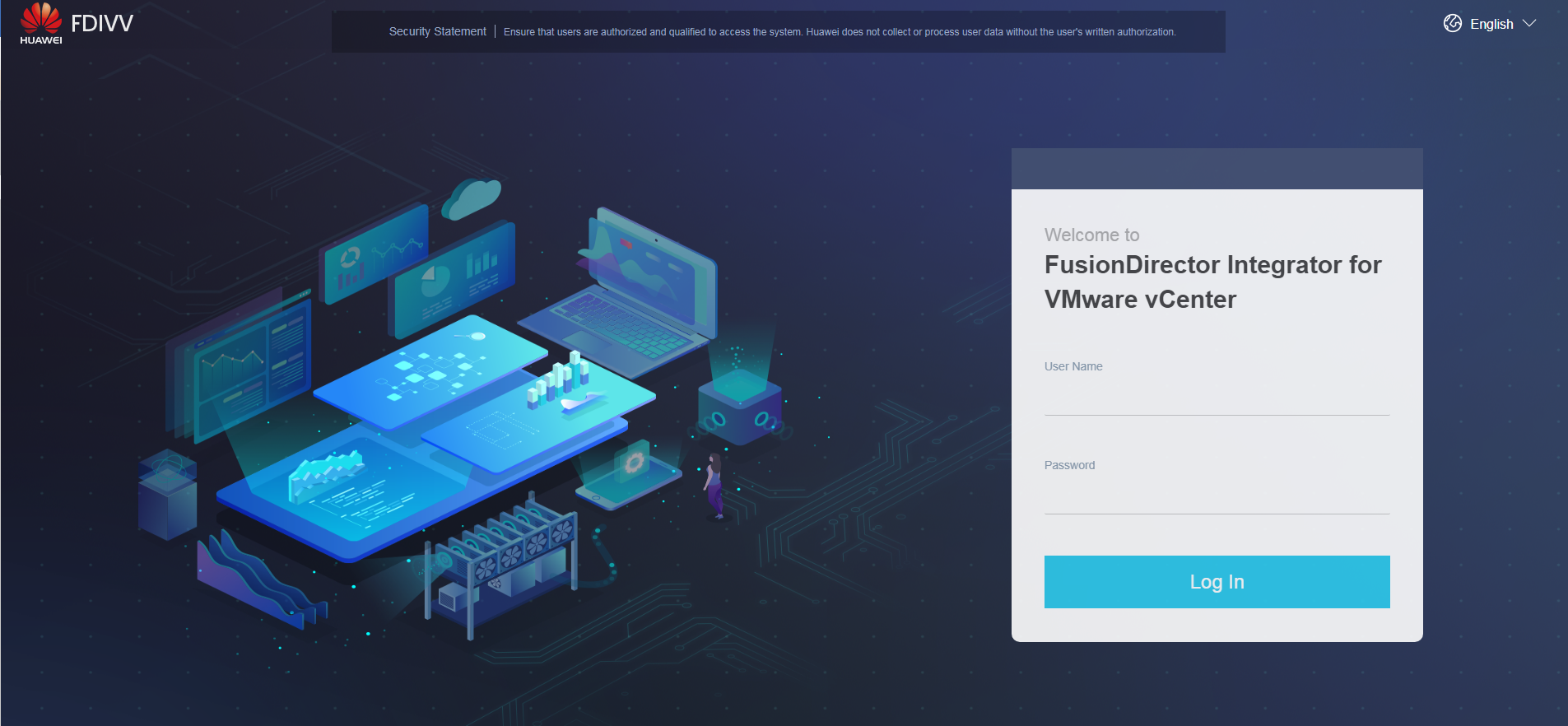
*XXX.XXX.XXX.XXX* indicates the FDIVV WebUI IP address (the same as the IP address configured for FDIVV) or DNS domain name.

Enter the user name and password.



If you enter an incorrect user name or password for three consecutive times, the user will be automatically locked. You can log in again 5 minutes later.

FDIVV login page



Click **Log In** to log in to FDIVV.



If you log in to FDIVV for the first time, the system prompts you to change the initial password after the login. For security purposes, change the initial password upon the first login and periodically change the password.

----End

## System Configuration

### Configuring the Device and Network

On the FDIVV WebUI, choose **Network Settings**.

The **Network Settings** page is displayed.

Click **Settings** in the upper right corner of the page.

The **Settings** dialog box is displayed, as shown in Figure 4-2.

Configuring the device and network



Set the following parameters:

In **Device Settings** area:

* **Host Name**: host name of the device to be configured
* **Domain Name**: domain name of the device to be configured

In **Network Settings** area:

* **IP Address Acquisition Mode**: mode for configuring the IP address used for the communication between the vCenter server or FusionDirector system and FDIVV
* **Subnet Mask**: subnet mask used for the communication between the vCenter server or FusionDirector system and FDIVV
* **IP Address**: IP address used for the communication between the vCenter server or FusionDirector system and FDIVV
* **Default Gateway**: default gateway address used for the communication between the vCenter server or FusionDirector system and FDIVV
* **Preferred DNS Server**: preferred DNS server of the device to be configured. When the preferred and alternate DNS servers are configured, the preferred DNS server is preferentially used for communication.
* **Alternate DNS Server**: alternate DNS server of the device to be configured. When the preferred DNS server is abnormal, the alternate DNS server automatically takes over services from the preferred DNS server.



If the vCenter server and the FusionDirector server are on the same network, you can use Eth0 to connect the vCenter and FusionDirector servers. If the vCenter server and the FusionDirector server are on different network, you can use Eth0 to connect the vCenter server and Eth1 to connect the FusionDirector server.

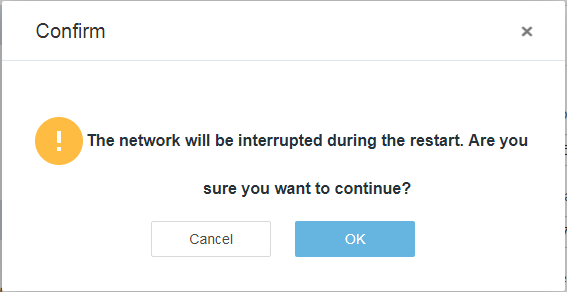
Click **OK**.

* In the **Device Settings** area:

The message "Operation successful." is displayed, indicating that the device configuration is complete.

* In the **Network Settings** area:
  1. The **Confirm** dialog box is displayed, as shown in Figure 4-3.

Confirm dialog box

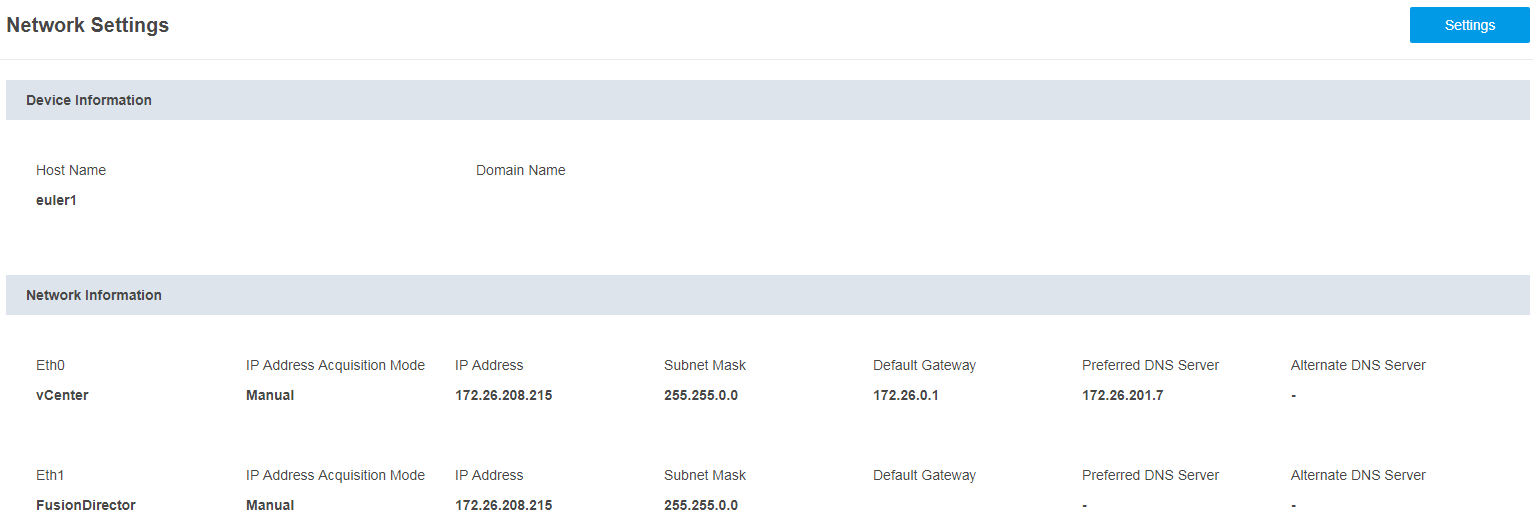


* 1. Click **OK**.

The network automatically restarts and the network configuration is complete.

You can view the device and network configuration on the **Network Settings** page, as shown in Figure 4-4.

Viewing the device and network configuration



----End

### Configuring NTP and Time

On the FDIVV WebUI, choose **Time Settings**. The **Time Settings** page is displayed, where you can configure NTP and time.

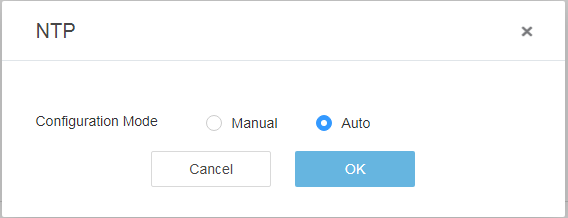
Configuring NTP

On the **Time Settings** page, click on the right of **NTP**.

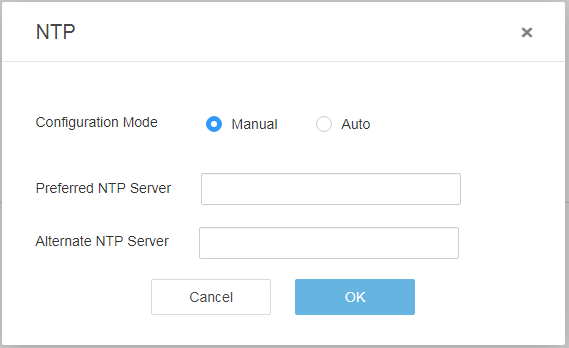


The **NTP** dialog box is displayed, as shown in Figure 4-5 and Figure 4-6.

Configuring NTP (Auto)



Configuring NTP (Manual)



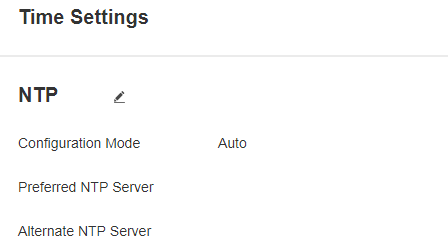
Select **Manual** or **Auto** as required.

Click **OK**.

The message "The NTP server configured successfully." is displayed, indicating that the NTP configuration is complete.

You can view the NTP configuration on the **Time Settings** page, as shown in Figure 4-7.

Viewing the NTP configuration



----End

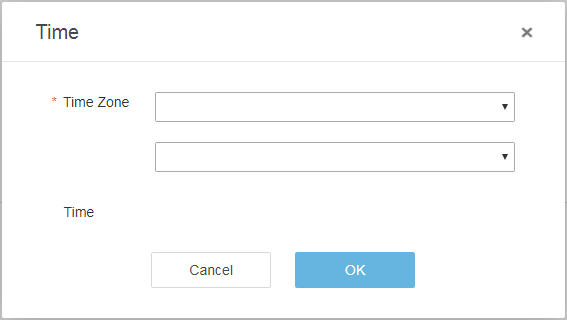
Configuring time

on the **Time Settings** page, click on the right of **Time**.



The **Time** dialog box is displayed, as shown in Figure 4-8.

Configuring time



Select a time zone.

Click **OK**.

The message "The time zone is configured successfully." is displayed, indicating that the time configuration is complete.

You can view the time configuration on the **Time Settings** page, as shown in Figure 4-9.

Viewing the time configuration



----End

## vCenter Server Management

On the FDIVV WebUI, choose **vCenter Server Management**. The **vCenter Server Management** page is displayed, where you can view, add, modify, and delete vCenter servers.

### Adding a vCenter Server



After a vCenter server is added, the system automatically installs and registers the plug-in to the vCenter server. This plug-in interacts with FusionDirector to implement unified monitoring and management of servers.

* When you add a vCenter 6.7, the FusionDirector for vCenter plug-in in HTML5 mode is installed.
* When you add a vCenter 6.5, the FusionDirector for vCenter plug-in in FLEX mode is installed.

For details about the functions of the FusionDirector for vCenter plug-in, see 5 Functions of the FusionDirector for vCenter Plug-in.

The following uses vCenter 6.7 as an example.

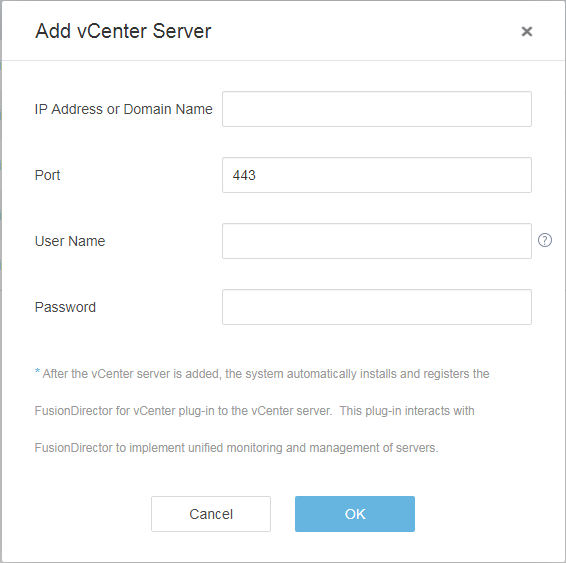
On the FDIVV WebUI, choose **vCenter Server Management**.

The **vCenter Server Management** page is displayed.

Click **Add** in the upper right corner of the page.

The **Add vCenter Server** dialog box is displayed, as shown in Figure 4-10.

Add vCenter Server dialog box



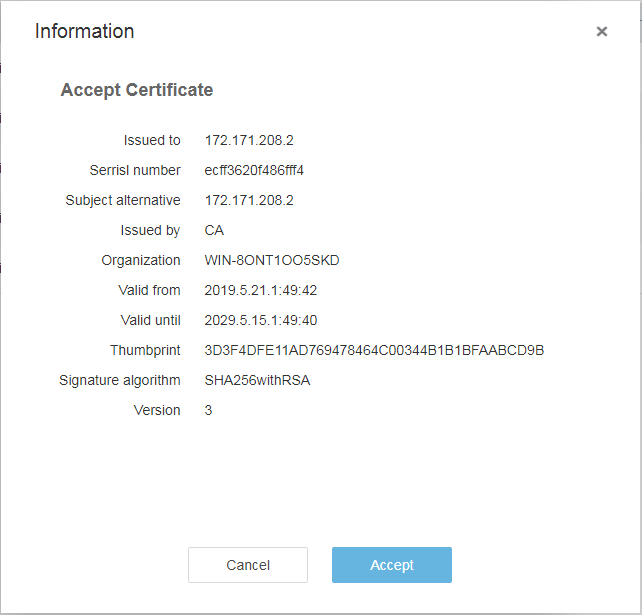
Enter the following parameters:

* **IP Address or Domain Name**: IP address or domain name of the vCenter server to be added.
* **Port**: port number of the vCenter server to be added. The default value is **443**.
* **User Name**: user name for logging in to the vCenter server to be added. The default value is **Administrator@vsphere.local**.
* **Password**: password for logging in to the vCenter server to be added.

Click **OK**.

The **Accept Certificate** dialog box is displayed, as shown in Figure 4-11.

Accept Certificate dialog box

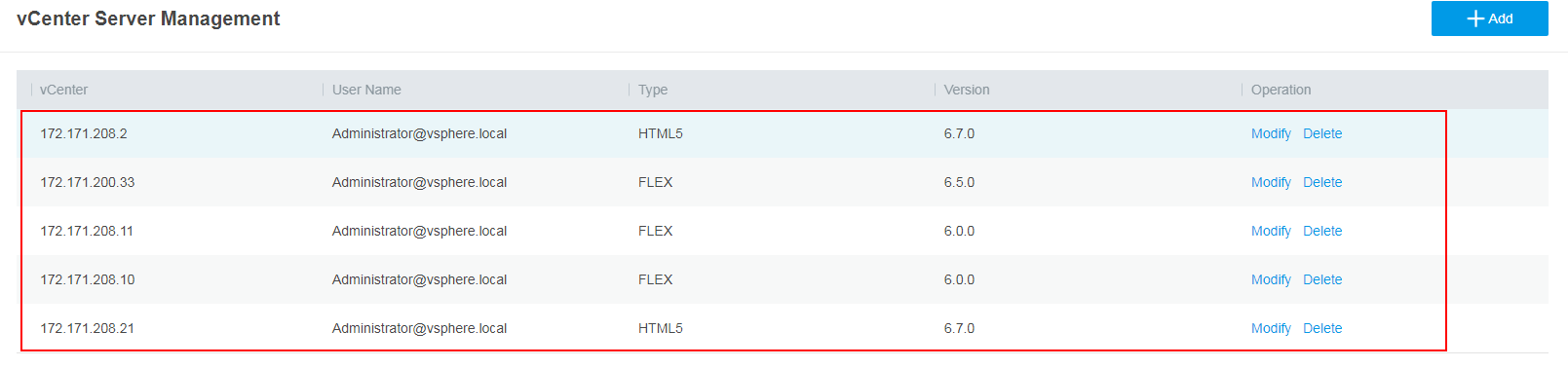


Click **Accept**.

The message "Operation successful." is displayed, indicating that the vCenter server is added.

You can view the added vCenter servers on the **vCenter Server Management** page.

Viewing the added vCenter servers



Restart the vCenter service.

* Restart vCenter on Windows
  1. Access the Windows CLI.
  2. Run the following command to stop the vCenter service:

"C:\Program Files\VMware\vCenter Server\bin\service-control.bat" --stop --all

* 1. Run the following command to start the vCenter service:

"C:\Program Files\VMware\vCenter Server\bin\service-control.bat" --start --all

* Restart vCenter on Linux
  1. Access the Linux CLI as user **root** using the SSH tool.
  2. Run the following command to stop the vCenter service:

service-control --stop --all

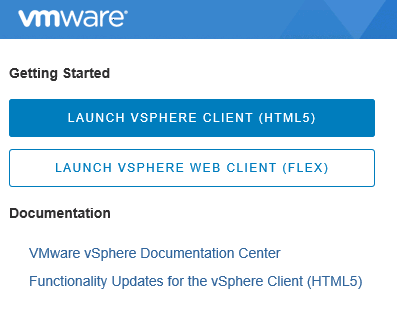
* 1. Run the following command to start the vCenter service:

service-control --start --all

Open the browser on the local PC, enter **https://*vCenter IP address*** in the address box, and press **Enter**.

Select **HTML5** to open the vCenter login page.

vCenter login page



Enter the vCenter user name and password, and click **Login**.

The vCenter home page is displayed.

When you access the vCenter home page for the first time, a message will be displayed, indicating that the deployment of the vCenter plug-in needs to be enabled by refreshing the browser, as shown in Figure 4-14.

Click **REFRESH BROWSER**.

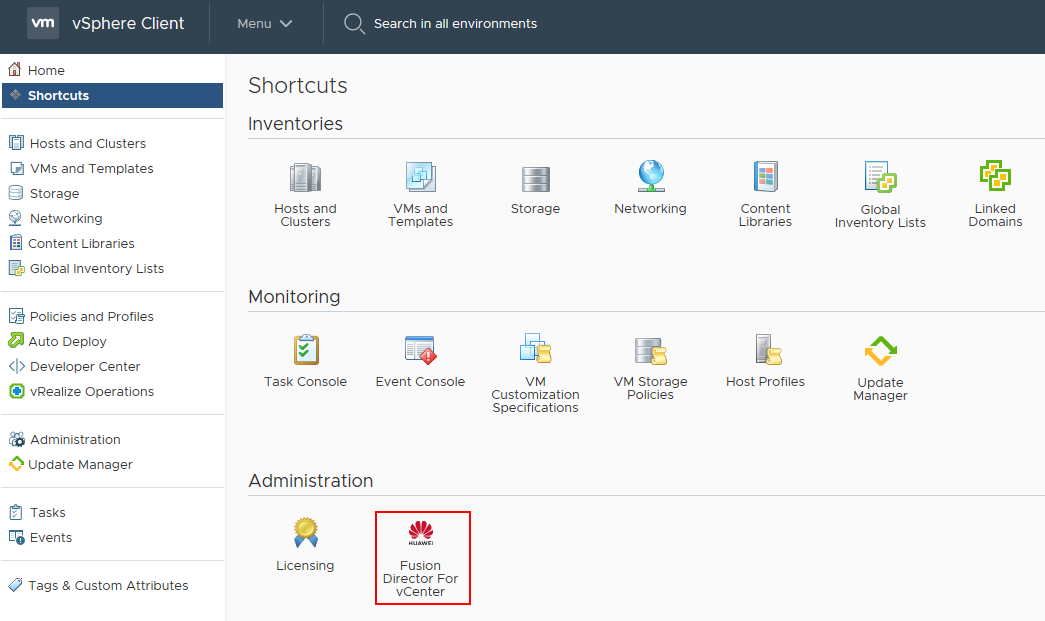
vCenter home page



Choose **Menu** > **Shortcuts**.

If the icon in the red box shown in Figure 4-15 is displayed, the FusionDirector for vCenter plug-in is successfully installed.

Shortcuts page



If you have logged in to vCenter, you need to log out and then log in again to view the **FusionDirector for vCenter** icon.

----End

### Modifying a vCenter Server

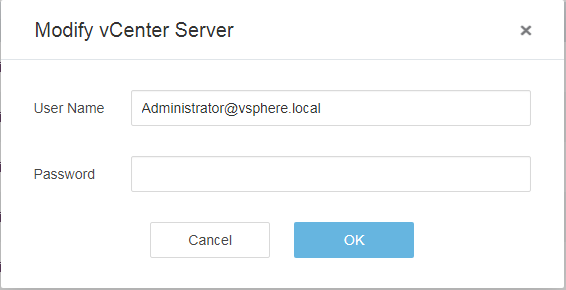
On the FDIVV WebUI, choose **vCenter Server Management**.

The **vCenter Server Management** page is displayed.

Click **Modify** in the **Operation** column of the vCenter server to be modified.

The **Modify vCenter Server** dialog box is displayed, as shown in Figure 4-16.

Modify vCenter Server dialog box



Change the user name or password.

* **User Name**: new user name of the vCenter server.
* **Password**: new password of the vCenter server.

Click **OK**.

The vCenter server is modified.

----End

### Deleting a vCenter Server



After the vCenter server is deleted, the system automatically uninstalls the plug-ins installed on the vCenter server, which affects server management on the vCenter server. Exercise caution when performing this operation.

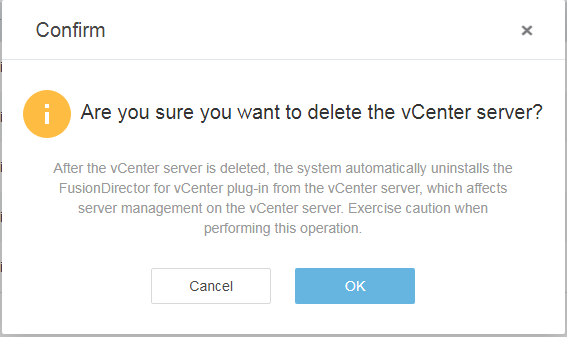
On the FDIVV WebUI, choose **vCenter Server Management**.

The **vCenter Server Management** page is displayed.

Click **Delete** in the **Operation** column of the vCenter server to be deleted.

The message "Are you sure you want to delete the vCenter server?" is displayed, as shown in Figure 4-17.

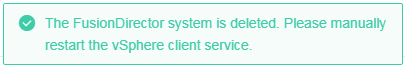
Confirm dialog box



Click **OK**.

A message is displayed, indicating that the deletion is successful and asking you to manually restart the vSphere Client service, as shown in Figure 4-18.

Restarting the vSphere Client service



Restart the vCenter service.

* Restart vCenter on Windows
  1. Access the Windows CLI.
  2. Run the following command to stop the vCenter service:

"C:\Program Files\VMware\vCenter Server\bin\service-control.bat" --stop --all

* 1. Run the following command to start the vCenter service:

"C:\Program Files\VMware\vCenter Server\bin\service-control.bat" --start --all

* Restart vCenter on Linux
  1. Access the Linux CLI as user **root** using the SSH tool.
  2. Run the following command to stop the vCenter service:

service-control --stop --all

* 1. Run the following command to start the vCenter service:

service-control --start --all

Open the browser on the local PC, enter **https://*vCenter IP address*** in the address box, and press **Enter**.

The vCenter login page is displayed.

Enter the vCenter user name and password, and click **Login**.

Check whether the plug-in icon is deleted from the **Shortcuts** page.

* If yes, no further action is required.
* If no, perform [Step 7](#s10) to [Step 8](#s11) to clear the browser cache and open the browser again.

Clear the browser cache.

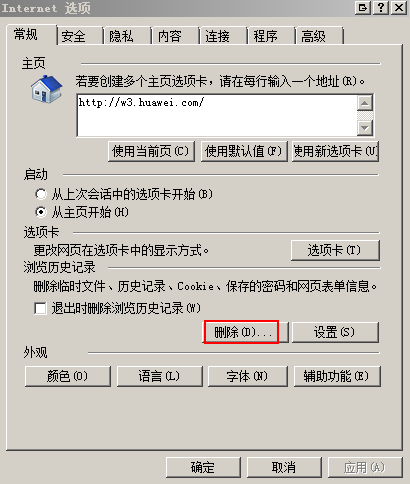
Internet Explorer 11.0 is used as an example.

1. Select **Internet Options**.

The **Internet Options** dialog box is displayed.

1. Click **Delete**, as shown in Figure 4-19.

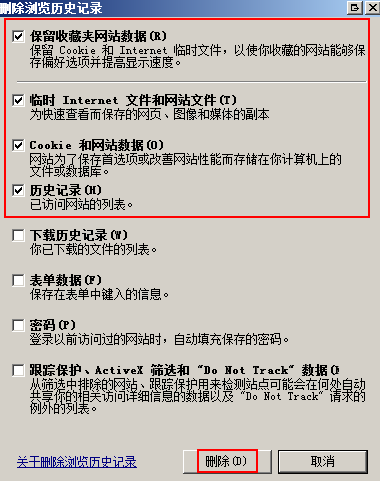
Internet Options dialog box



The **Delete Browsing History** dialog box is displayed.

1. Select the options shown in Figure 4-20, and click **Delete**.

Delete Browsing History dialog box



1. Click **Apply** > **OK**.

Open the browser again, log in to vCenter, and check whether the plug-in icon is deleted.

* If yes, no further action is required.
* If no, contact technical support.

----End

## FusionDirector Management

On the FDIVV WebUI, choose **FusionDirector Management**. The **FusionDirector Management** page is displayed, where you can view, add, modify, and delete FusionDirector systems.

### Adding a FusionDirector System

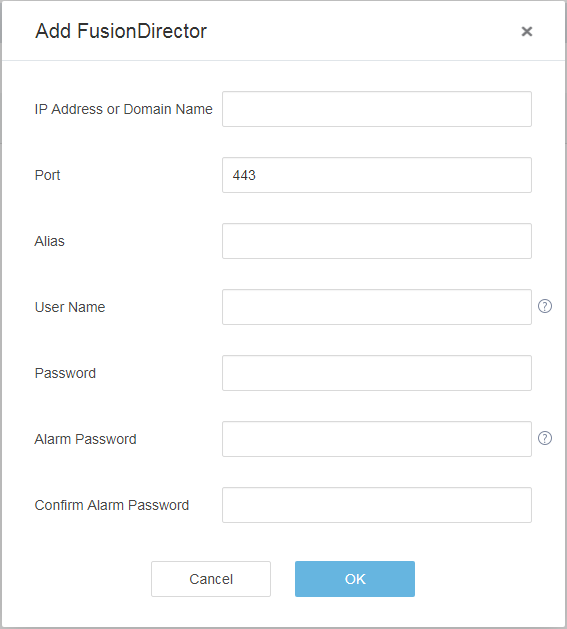
On the FDIVV WebUI, choose **FusionDirector Management**.

The **FusionDirector Management** page is displayed.

Click **Add** in the upper right corner of the page.

The **Add FusionDirector** dialog box is displayed, as shown in Figure 4-21.

Add FusionDirector dialog box



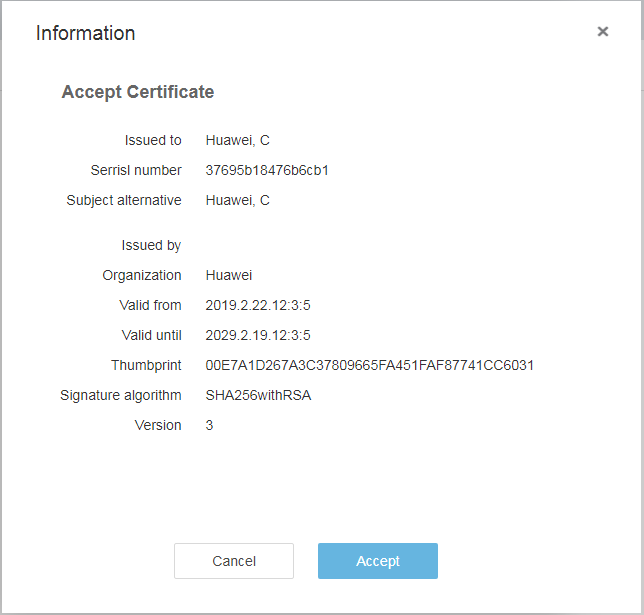
Enter the following parameters:

* **IP Address or Domain Name**: IP address or domain name of the FusionDirector system to be added.
* **Port**: port number of the FusionDirector system to be added. The default value is **443**.
* **Alias**: name of the FusionDirector system to be added.
* **User Name**: user name for logging in to the FusionDirector system to be added. The default value is **rootRedfish**.
* **Password**: password for logging in to the FusionDirector system to be added. The default value is **Machine@123**.
* **Alarm Password**: alarm password for authentication when the FusionDirector sends alarms to the vCenter.
* **Confirm Alarm Password**: enter the alarm password again.

Click **OK**.

The **Accept Certificate** dialog box is displayed, as shown in Figure 4-22.

Accept Certificate dialog box



Click **Accept**.

The message "Operation successful." is displayed, indicating that the FusionDirector system is added.

You can view the added FusionDirector systems on the **FusionDirector Management** page, as shown in Figure 4-23.

Viewing the added FusionDirector systems



----End

### Modifying a FusionDirector System

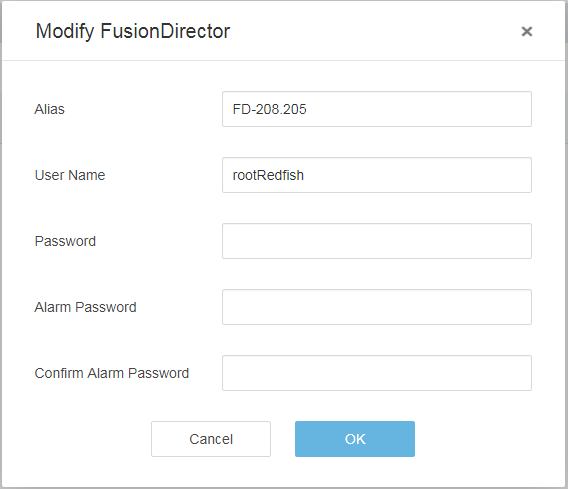
On the FDIVV WebUI, choose **FusionDirector Management**.

The **FusionDirector Management** page is displayed.

Click **Modify** in the **Operation** column of the FusionDirector system to be modified.

The **Modify FusionDirector** dialog box is displayed, as shown in Figure 4-24.

Modify FusionDirector dialog box



Modify the parameters.

* **Alias Name**: name of the FusionDirector system.
* **User Name**: user name for logging in to the FusionDirector system.
* **Password**: password for logging in to the FusionDirector system.
* **Alarm Password**: alarm password for authentication when the FusionDirector sends alarms to the vCenter.
* **Confirm Alarm Password**: enter the alarm password again.

Click **OK**.

The FusionDirector system is modified.

----End

### Deleting a FusionDirector System



After the FusionDirector system is deleted, the FusionDirector for vCenter plug-in cannot obtain server information or perform configurations. Exercise caution when deleting FusionDirector.

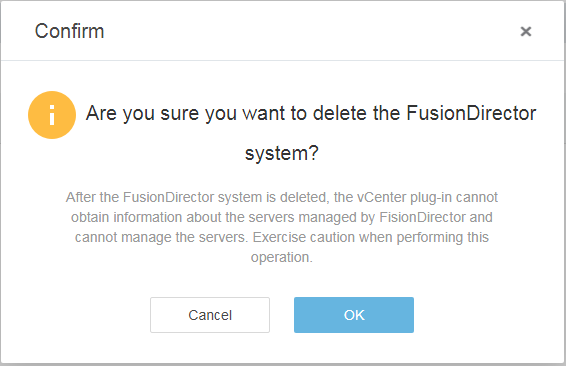
On the FDIVV WebUI, choose **FusionDirector Management**.

The **FusionDirector Management** page is displayed.

Click **Delete** in the **Operation** column of the FusionDirector system to be deleted.

The message "Are you sure you want to delete the FusionDirector system?" is displayed, as shown in Figure 4-25.

Confirm dialog box



Click **OK**.

The FusionDirector system is deleted.

----End

# Functions of the FusionDirector for vCenter Plug-in

[5.1 Introduction to the FusionDirector for vCenter Plug-in](#_EN-US_TOPIC_0185510359)

[5.2 Checking the FusionDirector for vCenter plug-in Version](#_EN-US_TOPIC_0184730461)

[5.3 Configuring vCenter](#_EN-US_TOPIC_0184730370)

[5.4 Configuring FDIVV](#_EN-US_TOPIC_0184730377)

[5.5 Server Management](#_EN-US_TOPIC_0184730420)

## Introduction to the FusionDirector for vCenter Plug-in

Supported Servers

Table 5-1 lists the servers supported by the FusionDirector for vCenter plug-in.

Supported servers

| Architecture | Type | Server Model |
| --- | --- | --- |
| x86 | Rack server | 1288H V5 |
| 2288H V5 |
| 2488 V5 |
| 2488H V5 |
| 8100 V5 |
| RH2288 V3 |
| Atlas server | G560 V5 |
| KunLun server | 9008 V5 |
| Arm | Rack server | TaiShan 200 server (model 2280) |

Version Mapping

* Only FusionDirector 1.5.1 or later is supported.
* The following vCenter versions are supported:
* vCenter Server 6.5 and 6.7 on Linux
* vCenter Server 6.5/6.7 for Windows

## Checking the FusionDirector for vCenter plug-in Version

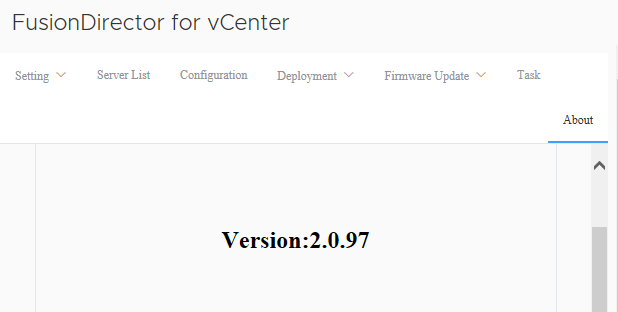
On the vCenter WebUI, choose **Menu** > **Shortcuts** > **Administration** > **FusionDirector for vCenter**.

The **FusionDirector for vCenter** page is displayed.

Click **About** in the upper right corner

The FusionDirector for vCenter plug-in version is displayed, as shown in Figure 5-1.

FusionDirector for vCenter page



----End

## Configuring vCenter



You need to configure vCenter before using the FusionDirector for vCenter plug-in for the first time.

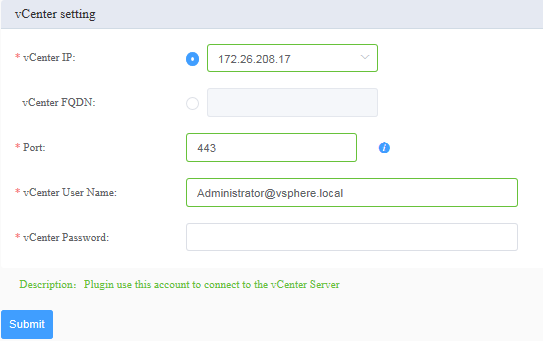
On the vCenter WebUI, choose **Menu** > **Shortcuts** > **Administration** > **FusionDirector for vCenter**.

The **FusionDirector for vCenter** page is displayed.

Choose **Setting** > **vCenter**.

The **vCenter setting** page is displayed, as shown in Figure 5-2.

vCenter setting page



* **vCenter IP**/**vCenter FQDN**: selects the vCenter IP address or enters the vCenter domain name.
* **Port**: indicates the port number configured for the HTTPS service during vCenter installation. The default value is **443**.
* **vCenter User Name**: indicates the user name of the vCenter administrator. The default value is **Administrator@vsphere.local**.
* vCenter Password: indicates the vCenter administrator password.

Click **Submit**.

The **Prompt** dialog box is displayed indicating that the configuration is saved successfully.

Click **OK**.

The vCenter configuration is complete.

----End

## Configuring FDIVV



After the vCenter is configured, the **FDIVV setting** dialog box is displayed.

On the vCenter WebUI, choose **Menu** > **Shortcuts** > **Administration** > **FusionDirector for vCenter**.

The **FusionDirector for vCenter** page is displayed.

Choose **Setting** > **FDIVV**.

The **FDIVV setting** page is displayed, as shown in Figure 5-3.

FDIVV setting page



* **IP or FQDN**: IP address or domain name used for the communication between the FusionDirector for vCenter plug-in and FDIVV. This parameter is automatically set.
* **Port**: port number used for the communication between the FusionDirector for vCenter plug-in and FDIVV. The default value is **443**.
* **User Name**: user name used for the communication between the FusionDirector for vCenter plug-in and FDIVV. The default value is **ApiUser**.
* **Password**: password used for the communication between the FusionDirector for vCenter plug-in and FDIVV. The default value is **Restful@8000**.

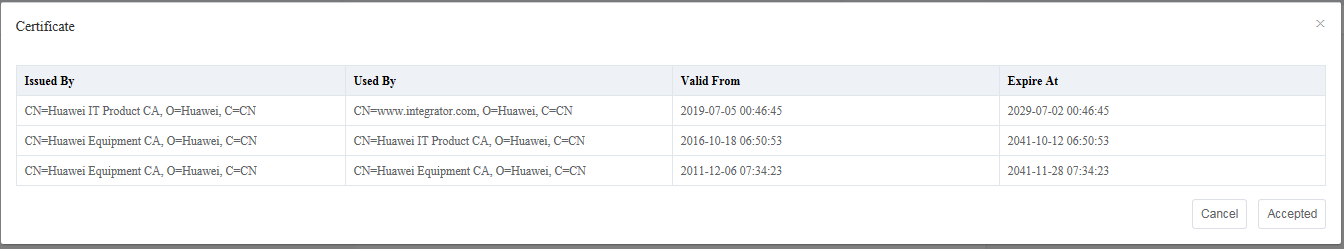


For details about how to change the default password, see 7.3 How to Change the Default Password Used for the Communication Between the FusionDirector for vCenter Plug-in and FDIVV.

Click **Save**.

The **Certificate** dialog box is displayed, as shown in Figure 5-4.

Certificate dialog box



Click **Accepted**.

The FDIVV configuration is complete.

----End

## Server Management

### Viewing Server Information

On the vCenter WebUI, choose **Menu** > **Shortcuts** > **Administration** > **FusionDirector for vCenter**.

The **FusionDirector for vCenter** page is displayed.

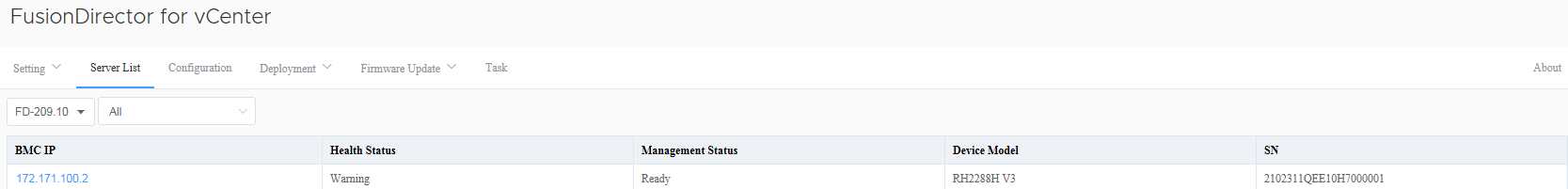
Choose **Server List**.

The **Server List** page is displayed.

View the server information.

1. Select the FusionDirector and server type to view the BMC IP address, health status, management status, device model, and product serial number of all servers of the FusionDirector, as shown in Figure 5-5.

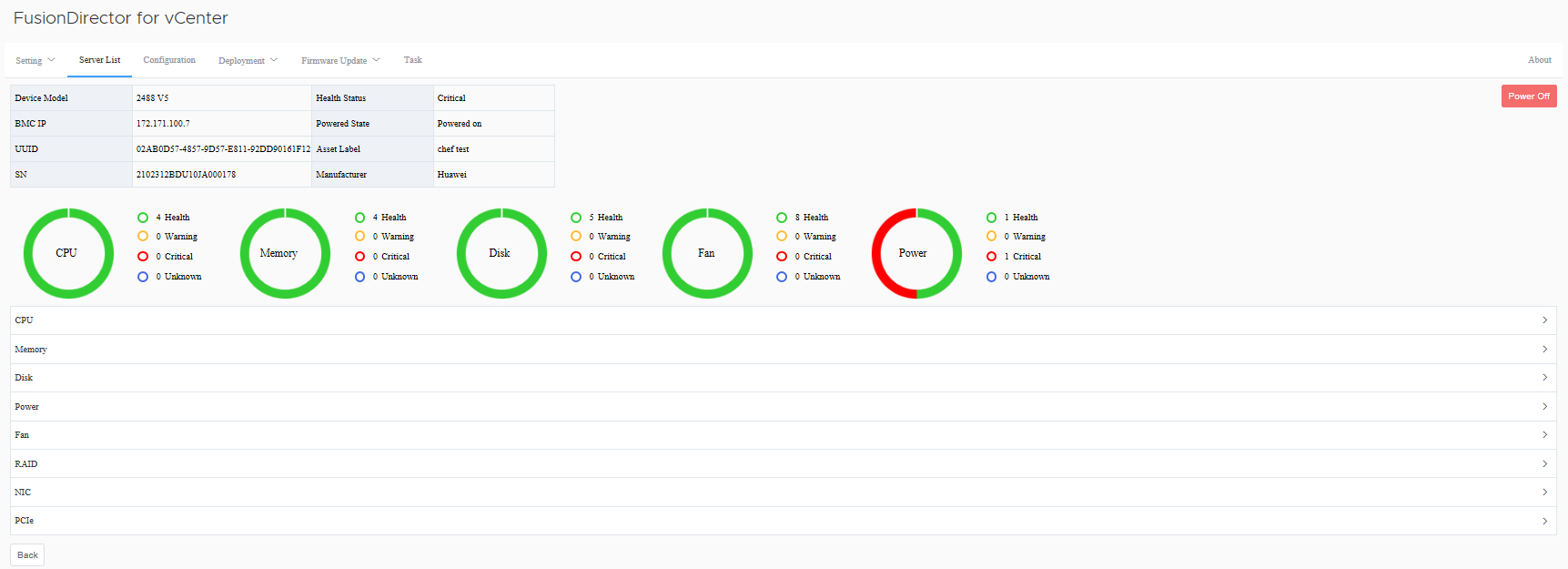
Server List page



1. Click **BMC IP** of a server.

View the basic information, online device status, and CPU, memory, drive, PSU, fan, RAID, NIC, and PCIe information of the server, as shown in Figure 5-6.

Device status



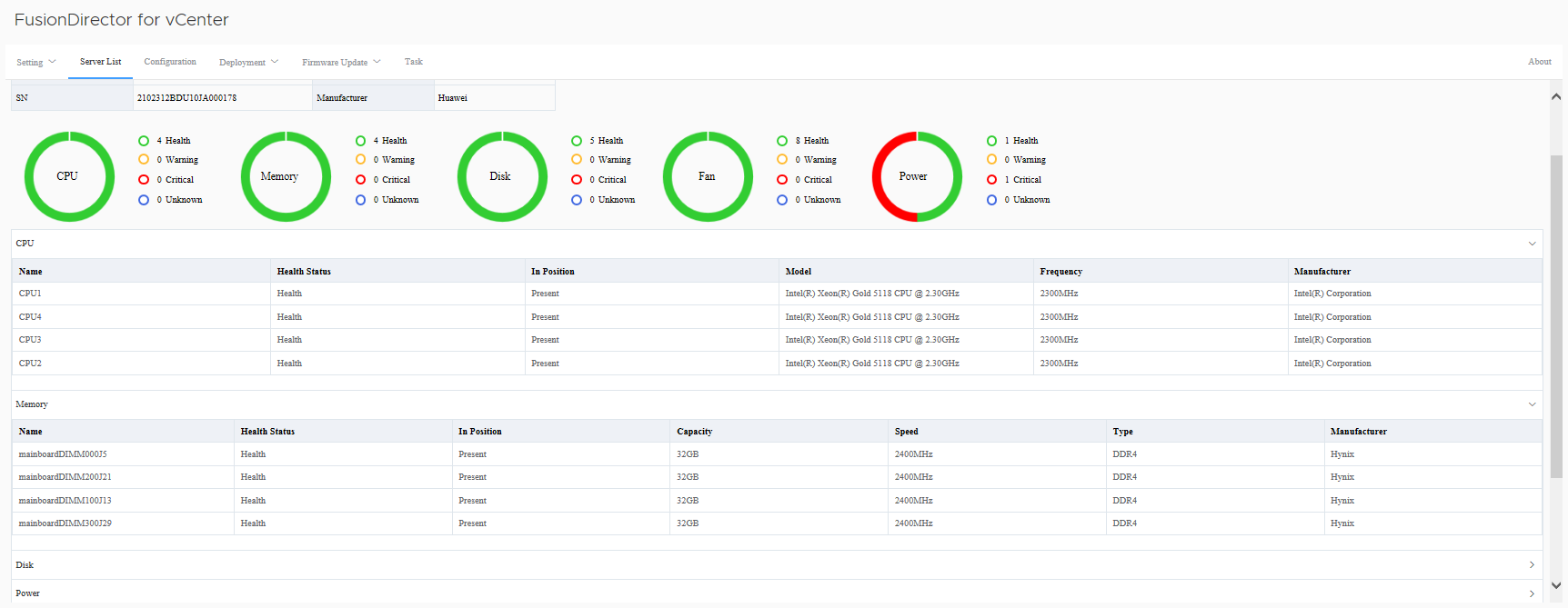
* If **Powered State** is **Powered on**, the **Power Off** button is displayed on the page shown in Figure 5-6. You can click **Power Off** to power off the server.
* If **Powered State** is **Powered off**, the **Power On** button is displayed on the page shown in Figure 5-6. You can click **Power On** to power on the server.

1. Click to view the detailed information about each component.



View the detailed information about the CPU and memory as shown in Figure 5-7.

Detailed information about each component



1. Click **Back**.

The **Server List** page is displayed.

----End

### Configuring Servers

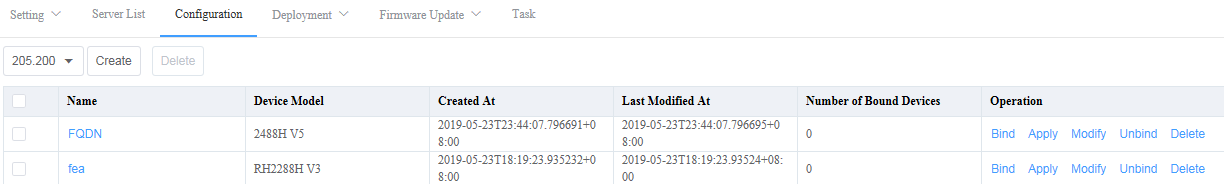
On the vCenter WebUI, choose **Menu** > **Shortcuts** > **Administration** > **FusionDirector for vCenter**.

The **FusionDirector for vCenter** page is displayed.

Choose **Configuration**.

The **Configuration** page is displayed, as shown in Figure 5-8.

Configuration page

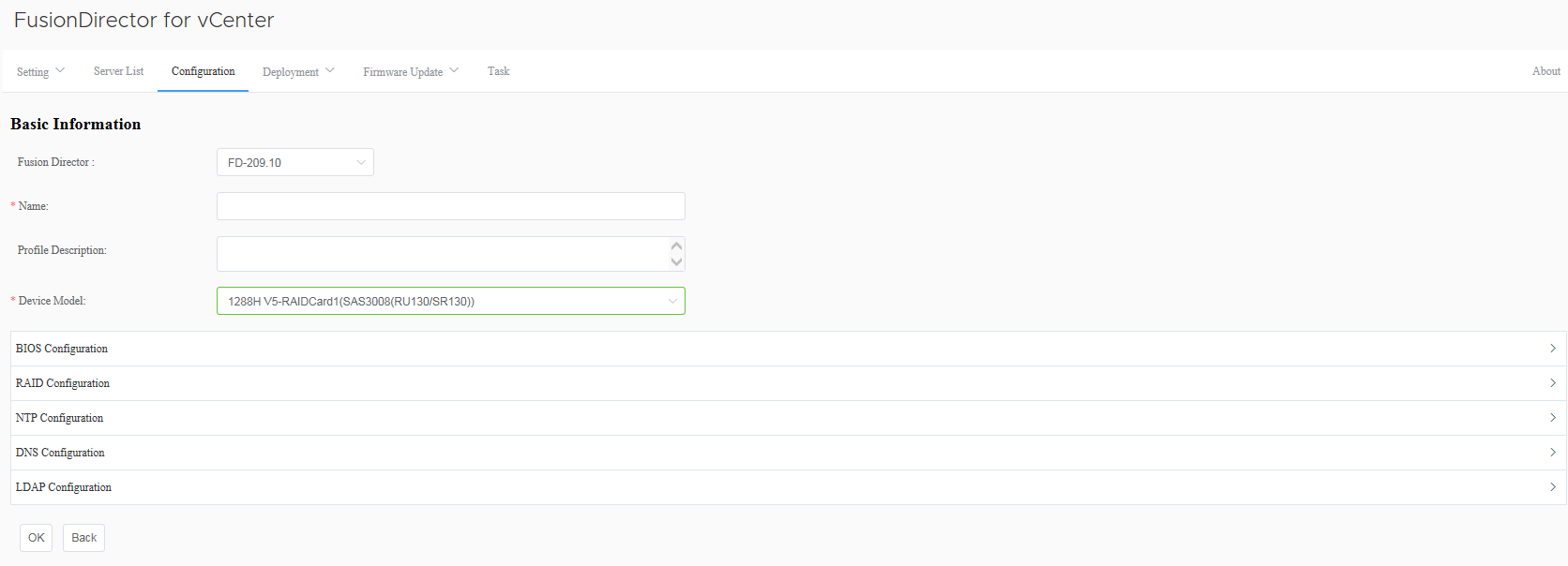


Click **Create**.

The page for creating a template is displayed.

Set the following parameters, as shown in Figure 5-9.

Creating a template



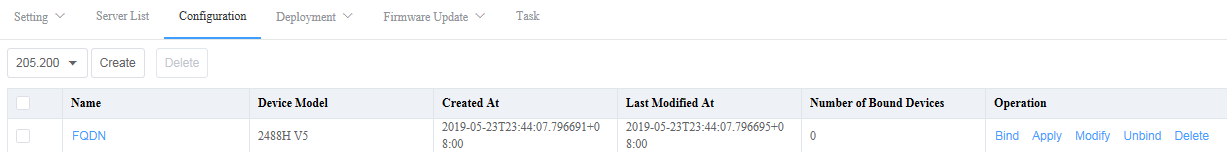
* **Fusion Director**: selects a FusionDirector system.
* **Name**: template name.
* **Profile Description**: (optional) template description
* **Device Model**: selects a server model.
* **BIOS Configuration**: sets BIOS parameters. For details, see 5.5.2.1 Setting BIOS Parameters.
* **RAID Configuration**: sets RAID parameters. For details, see 5.5.2.2 Setting RAID Parameters.
* **NTP Configuration**: sets NTP parameters. For details, see 5.5.2.3 Setting NTP Parameters.
* **DNS Configuration**: sets DNS parameters. For details, see 5.5.2.4 Setting DNS Parameters.
* **LDAP Configuration**: sets LDAP parameters. For details, see 5.5.2.5 Setting LDAP Parameters.

Click **OK**.

The template is created.

On the **Configuration** page, view the created template, as shown in Figure 5-10.

Template



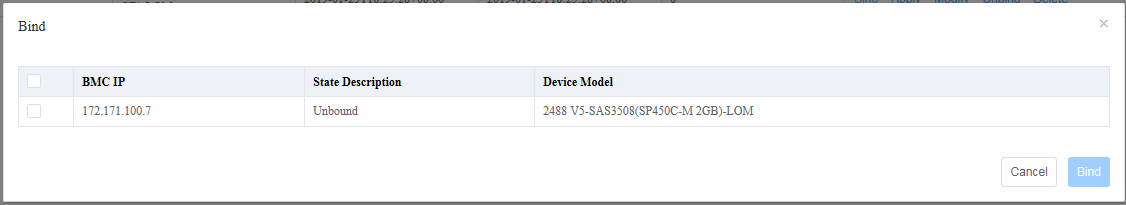
* To view the information of a template, click the template name in the **Name** column.
* To modify a template, click **Modify** in the **Operation** column.
* To delete a template, click **Delete** in the **Operation** column.

Bind the template to the server.

1. Click **Bind** in the **Operation** column.

The **Bind** page is displayed, as shown in Figure 5-11.

Bind page



1. Select the server that needs to use the template and click **Bind**.



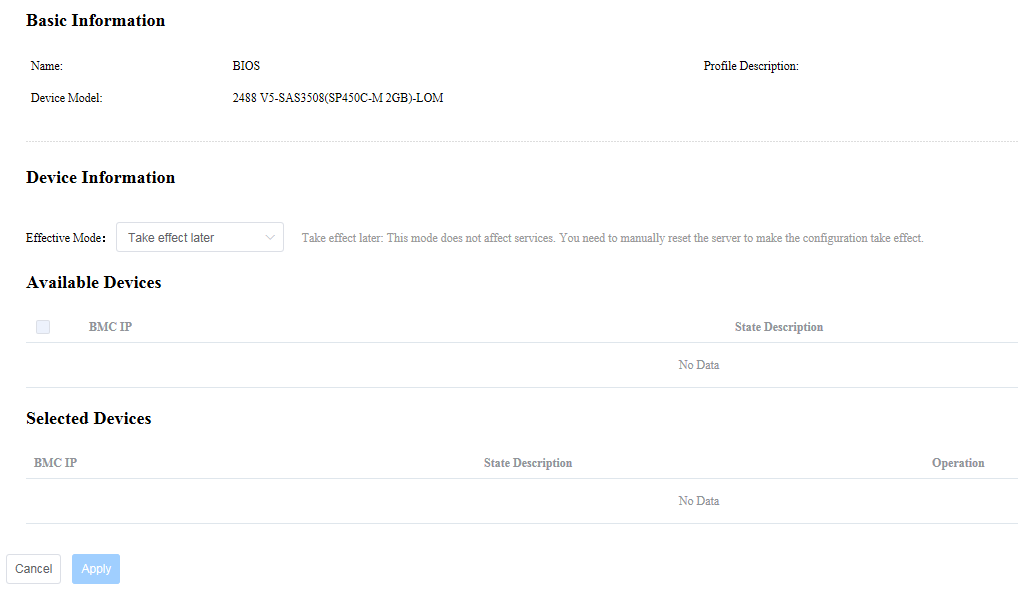
Each server can be bound to only one template. To bind another template to a server, click **Unbind** in the **Operation** column of the bound template to unbind the server from the template.

Apply the template to the server.

1. Click **Apply** in the **Operation** column.

The page for applying the template is displayed, as shown in Figure 5-12.

Applying the template



1. In the **Device Information** area, select **Effective Mode**.

* **Take effect later**: This option does not impact the current services. The configuration takes effect after the server is manually reset.
* **Take effect immediately**: This operation may affect the current services. Exercise caution when performing this operation.

1. In the **Available Devices** area, select the server to be configured.
2. Click **Apply**.

Configuration starts to be delivered.

View the progress and result of the server configuration.

On the **Fusion Director for vCenter** page, choose **Task**.

The **Task** page is displayed, as shown in Figure 5-13.

Task page



----End

#### Setting BIOS Parameters

On the vCenter WebUI, choose **Menu** > **Shortcuts** > **Administration** > **FusionDirector for vCenter**.

The **FusionDirector for vCenter** page is displayed.

Choose **Configuration**.

The **Configuration** page is displayed.

Click **Create**.

The page for creating a template is displayed.

Click **BIOS Configuration**.

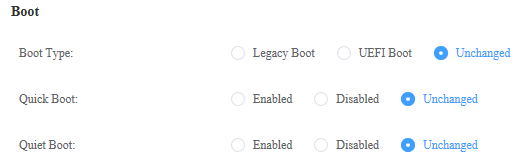
The **BIOS Configuration** area is displayed.



The BIOS configuration varies depending on the server model. The following uses the 2488 V5 as an example.

In the **Boot** area shown in Figure 5-14, set the parameters listed in Table 5-2.

Boot configuration



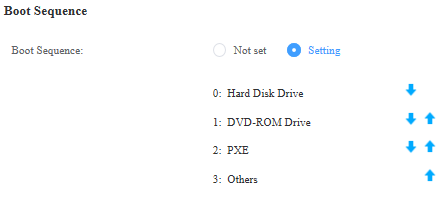
Boot configuration

| Parameter | Function |
| --- | --- |
| Boot Type | Indicates the system boot type. The options are as follows:   * **Legacy Boot**: enables the Legacy boot type. * **UEFI Boot**: enables the UEFI boot type. * **Unchanged**: retains the current configuration. |
| Quick Boot | Specifies whether to enable the quick boot mode. The options are as follows:   * **Enabled**: The memory test is skipped during the server boot process, which shortens the startup time. * **Disabled**: A full memory test is performed during the server boot process, which prolongs the startup time. * **Unchanged**: retains the current configuration. |
| Quiet Boot | Specifies whether to enable the quiet boot mode. The options are as follows:   * **Enabled**: The product log is displayed instead of the POST information during the startup process. * **Disabled**: The POST information is displayed on the screen during the startup process. * **Unchanged**: retains the current configuration. |

In the **Boot Sequence** area, if **Setting** is selected, you can click or to set the system boot sequence, as shown in Figure 5-15.

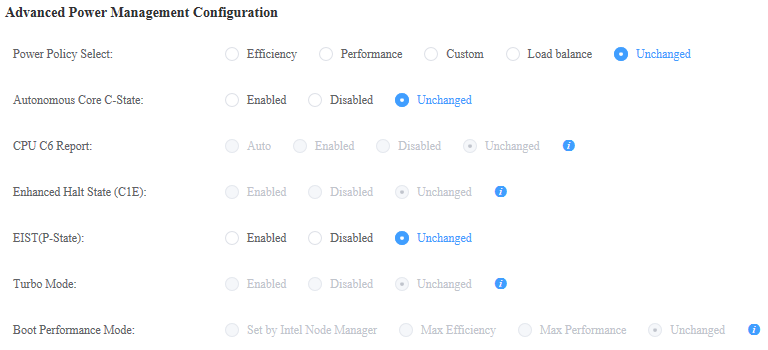


Setting the system boot sequence



In the **Advanced Power Management Configuration** area shown in Figure 5-16, set the parameters listed in Table 5-3.

Advanced power management configuration

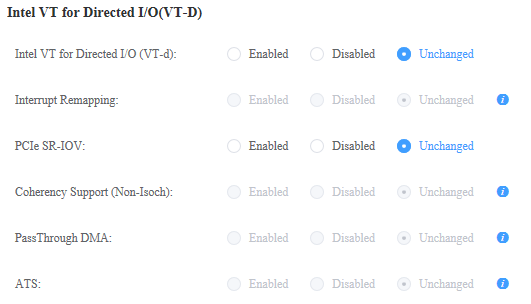


Advanced power management configuration

| Parameter | Function |
| --- | --- |
| Power Policy Select | Indicates the power policy. The options are as follows:   * **Efficiency**: enables the low performance and low power consumption mode. This mode reduces the system power consumption. * **Performance**: enables the high performance and high power consumption mode. * **Custom**: The user can customize the power policy to balance the performance, delay, and power consumption. You are advised to configure the CPU to run at the standard frequency. * **Load Balance**: The system automatically adjusts the server performance based on the service pressure. * **Unchanged**: retains the current configuration. |
| Autonomous Core C-State | Sets the C state of the autonomous core. The options are as follows:   * **Enabled** * **Disabled** * **Unchanged**: retains the current configuration. |
| CPU C6 Report | Sets the C state. This option depends on the setting of the **Autonomous Core C-State** parameter. The options are as follows:   * **Auto** * **Enabled** * **Disabled** * **Unchanged**: retains the current configuration. |
| Enhanced Halt State (C1E) | Sets the C1E configuration. This option depends on the setting of the **Autonomous Core C-State** parameter. The options are as follows:   * **Enabled** * **Disabled** * **Unchanged**: retains the current configuration. |
| EIST (P-State) | Sets the Enhanced Intel SpeedStep Technology (EIST). The options are as follows:   * **Enabled** * **Disabled** * **Unchanged**: retains the current configuration. |
| Turbo Mode | Sets the turbo mode. This option depends on the setting of the **EIST (P-State)** parameter. The options are as follows:   * **Enabled** * **Disabled** * **Unchanged**: retains the current configuration. |
| Boot Performance Mode | Indicates the boot performance. This option depends on the settings of the **EIST (P-State)** and **Power Policy Select** parameters. The options are as follows:   * **Set by Intel Node Manager**: The boot performance is controlled by ME. * **Maximum Efficiency**: The boot performance is set to the maximum efficiency mode. * **Maximum Performance**: The boot performance is set to the maximum performance mode. * **Unchanged**: retains the current configuration. |

In the **Intel VT for Directed I/O(VT-D)** area shown in Figure 5-17, set the parameters listed in Table 5-4.

VT-d configuration

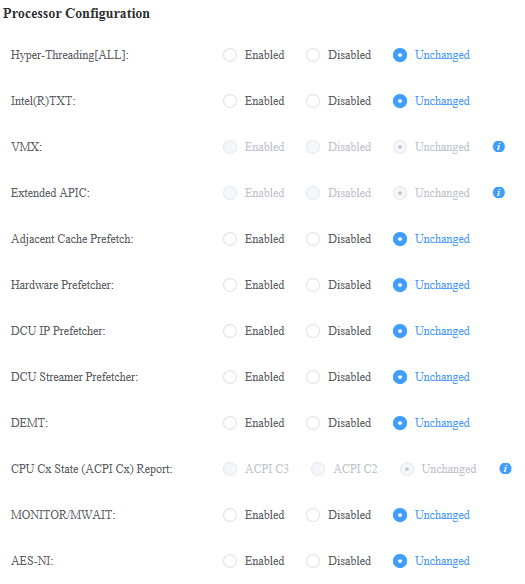


VT-d configuration

| Parameter | Function |
| --- | --- |
| Intel VT for Directed I/O (VT-d) | Sets VT-d. The VT-d feature enables the VMM to manage multiple VMs by using one physical I/O device. The options are as follows:   * **Enabled** * **Disabled** * **Unchanged**: retains the current configuration. |
| Interrupt Remapping | Sets VT-d Interrupt Remapping. You can keep this feature enabled when the feature is not enabled on the management program and OS. This option depends on the setting of the **Intel VT for Directed I/O (VT-d)** parameter. The options are as follows:   * **Enabled** * **Disabled** * **Unchanged**: retains the current configuration. |
| PCIe SR-IOV | Enables or disables SR-IOV for the PCIe card. The options are as follows:   * **Enabled** * **Disabled** * **Unchanged**: retains the current configuration. |
| Coherency Support (Non-Isoch) | Sets the non-isoch coherency. This option depends on the setting of the **Intel VT for Directed I/O (VT-d)** parameter. The options are as follows:   * **Enabled** * **Disabled** * **Unchanged**: retains the current configuration. |
| PassThrough DMA | Sets pass-through DMA. This feature is related to virtualization. This option depends on the setting of the **Intel VT for Directed I/O (VT-d)** parameter. The options are as follows:   * **Enabled** * **Disabled** * **Unchanged**: retains the current configuration. |
| ATS | Sets ATS. This feature is related to virtualization. This option depends on the setting of the **Intel VT for Directed I/O (VT-d)** parameter. The options are as follows:   * **Enabled** * **Disabled** * **Unchanged**: retains the current configuration. |

In the **Processor Configuration** area shown in Figure 5-18, set the parameters listed in Table 5-5.

Processor configuration

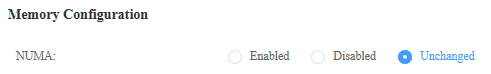


Processor configuration

| Parameter | Function |
| --- | --- |
| Hyper-Threading[ALL] | Sets the hyper-threading function for Intel processors. If this function is enabled, each physical processor core functions as two logical processor cores. If this function is disabled, each physical processor core functions as only one logical processor core. Enabling this function increases the number of logical processor cores and improves system performance. The options are as follows:   * **Enabled** * **Disabled** * **Unchanged**: retains the current configuration. |
| Intel(R)TXT | Sets the Intel Trusted Execution Technology (Intel TXT). The options are as follows:   * **Enabled** * **Disabled** * **Unchanged**: retains the current configuration. |
| VMX | Sets the Virtual Machine Extensions (VMX). When this feature is enabled, virtualization layers or OSs that support this feature can use Intel virtualization capabilities. Some virtualization layers require the Intel virtualization technology. You can keep this feature enabled when the virtualization layer or OS does not support this feature. This option depends on the setting of the **Intel(R)TXT** parameter. The options are as follows:   * **Enabled** * **Disabled** * **Unchanged**: retains the current configuration. |
| Extended APIC | Sets the extended APIC feature. When the total number of CPU cores exceeds 256, you are advised to enable this feature to improve the OS efficiency in CPU multi-core scenarios. This option depends on the settings of the **Intel VT for Directed I/O (VT-d)** and **Interrupt Remapping** parameters. The options are as follows:   * **Enabled** * **Disabled** * **Unchanged**: retains the current configuration. |
| Adjacent Cache Prefetch | Sets the adjacent cache prefetch function. When this feature is enabled, the system regards the data adjacent to the required data is also required, and reads the adjacent data in advance to improve data access performance. When the system uses sequential memory access, this feature improves data access efficiency. When the system uses random memory access, you are advised to disable this feature. The options are as follows:   * **Enabled** * **Disabled** * **Unchanged**: retains the current configuration. |
| Hardware Prefetcher | Sets the hardware prefetching feature. When this feature is enabled, the CPU prefetches instructions or data from the memory to the L2 cache before processing the instructions or data. This feature helps reduce the memory access time and eliminate potential performance bottlenecks. In most environments, this feature needs to be enabled to achieve optimal performance. For some workloads, disabling this option may improve the performance. You can decide whether to enable this feature based on the results of benchmark tests. The options are as follows:   * **Enabled** * **Disabled** * **Unchanged**: retains the current configuration. |
| DCU IP Prefetcher | Sets the DCU IP prefetching feature (enabled by default). This feature may affect system performance depending on the applications running on the server. In most environments, this feature needs to be enabled to achieve optimal performance. For some workloads, disabling this option may improve the performance. You can decide whether to enable this feature based on the results of benchmark tests. The options are as follows:   * **Enabled** * **Disabled** * **Unchanged**: retains the current configuration. |
| DCU Streamer Prefetcher | Sets the DCU streamer prefetching feature (enabled by default). This feature may affect system performance depending on the applications running on the server. In most environments, this feature needs to be enabled to achieve optimal performance. For some workloads, disabling this option may improve the performance. You can decide whether to enable this feature based on the results of benchmark tests. The options are as follows:   * **Enabled** * **Disabled** * **Unchanged**: retains the current configuration. |
| DEMT | Sets the Dynamic Energy Management Technology (DEMT) for the processor based on the processor workload. Selecting this option may have a negative impact on performance, depending on the workload. The options are as follows:   * **Enabled** * **Disabled** * **Unchanged**: retains the current configuration. |
| CPU Cx State (ACPI Cx) Report | Indicates the mapping between the CPU C status and the ACPI C status. This option depends on the setting of the **Autonomous Core C-State** parameter. The options are as follows:   * **ACPI C3**: enables the ACPI C3 mode. * **ACPI C2**: enables the ACPI C2 mode. * **Unchanged**: retains the current configuration. |
| MONITOR/MWAIT | Sets the MONITOR/MWAIT instructions. When this feature is enabled, the system monitors the CPU status to improve the CPU instruction performance. This feature allows some OSs to autonomously adjust energy-saving options. If you want to disable energy saving, disable this feature. The options are as follows:   * **Enabled** * **Disabled** * **Unchanged**: retains the current configuration. |
| AES-NI | Sets the Advanced Encryption Standard New Instructions (AES-NI) function for the CPUs. The options are as follows:   * **Enabled** * **Disabled** * **Unchanged**: retains the current configuration. |

In the **Memory Configuration** area shown in Figure 5-19, set the parameters listed in Table 5-6.

Memory configuration

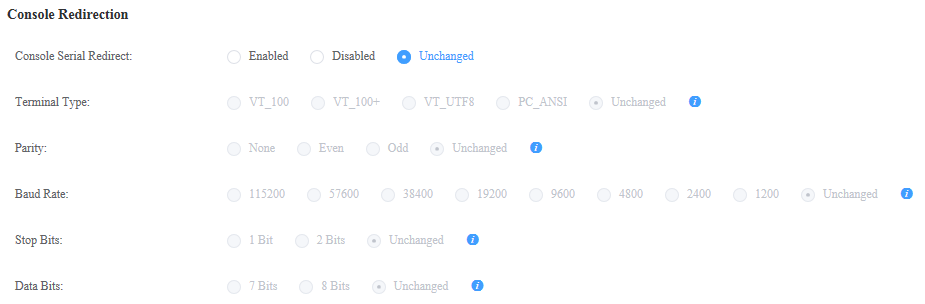


Memory configuration

| Parameter | Function |
| --- | --- |
| NUMA | Sets the non-uniform memory access (NUMA) architecture feature. All OS platforms support NUMA. In most cases, this feature improves the performance of some workloads. Before disabling NUMA, ensure that all nodes have the same memory size. The options are as follows:   * **Enabled** * **Disabled** * **Unchanged**: retains the current configuration. |

In the **Console Redirection** area shown in Figure 5-20, set the parameters listed in Table 5-7.

Console redirection

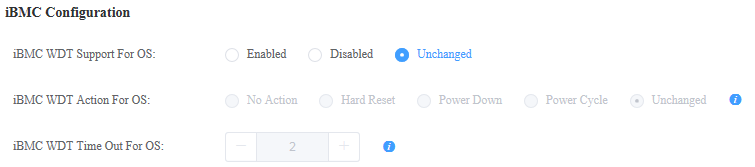


Console redirection

| Parameter | Function |
| --- | --- |
| Console Serial Redirect | Sets the serial port redirection function. When this feature is enabled, the system redirects the data of a specified physical serial port or virtual serial port to a specified system serial port. The options are as follows:   * **Enabled** * **Disabled** * **Unchanged**: retains the current configuration. |
| Terminal Type | Indicates the emulation type in the terminal program. The emulation type selected in the terminal program must be the same as the emulation type in BIOS. This option depends on the setting of the **Console Serial Redirect** parameter. The options are as follows:   * **VT\_100** * **VT\_100+** * **VT\_UTF8** * **PC\_ANSI** * **Unchanged**: retains the current configuration. |
| Parity | Sets the parity check for serial port redirection. This option depends on the setting of the **Console Serial Redirect** parameter. The options are as follows:   * **None**: disables the parity check. * **Even**: sends even bits with regular data bits to detect data transmission errors. * **Odd**: sends an odd bit with regular data bits to detect data transmission errors. * **Unchanged**: retains the current configuration. |
| Baud Rate | Indicates the serial port redirection rate. This option depends on the setting of the **Console Serial Redirect** parameter. The options are as follows:   * **115200** * **57600** * **38400** * **19200** * **9600** * **4800** * **2400** * **1200** * **Unchanged**: retains the current configuration. |
| Stop Bits | Indicates the end of a serial data packet. This option depends on the setting of the **Console Serial Redirect** parameter.   * **1 Bit** * **2 Bits** * **Unchanged**: retains the current configuration. |
| Data Bits | Indicates the length of the data transmitted in serial port redirection. This option depends on the setting of the **Console Serial Redirect** parameter.   * **7 Bits** * **8 Bits** * **Unchanged**: retains the current configuration. |

In the **iBMC Configuration** area shown in Figure 5-21, set the parameters listed in Table 5-8.

iBMC configuration

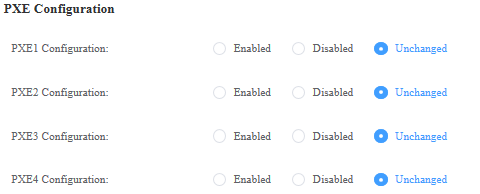


iBMC configuration

| Parameter | Function |
| --- | --- |
| iBMC WDT Support For OS | Sets the watchdog function during OS loading. The options are as follows:   * **Enabled** * **Disabled** * **Unchanged**: retains the current configuration. |
| iBMC WDT Action For OS | Sets the action to be taken when the OS times out. This option depends on the setting of the **iBMC WDT Support For OS** parameter. The options are as follows:   * **No Action**: No action is performed. * **Hard Reset**: resets the system forcibly. * **Power Down**: powers off the system. * **Power Cycle**: powers off and then restarts the system. * **Unchanged**: retains the current configuration. |
| iBMC WDT Time Out For OS | Sets the watchdog timeout duration (in minutes). The value ranges from 2 to 8. This option depends on the setting of the **iBMC WDT Support For OS** parameter. |

In the **PXE Configuration** area shown in Figure 5-22, set the parameters listed in Table 5-9.

PXE configuration

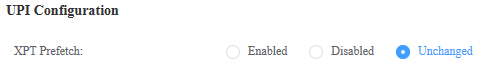


PXE configuration

| Parameter | Function |
| --- | --- |
| PXE1 to PXE4 Configuration | Sets the PXE function for NIC 1 to NIC 4. The options are as follows:   * **Enabled** * **Disabled** * **Unchanged**: retains the current configuration. |

In the **UPI Configuration** area shown in Figure 5-23, set the parameters listed in Table 5-10.

UPI configuration

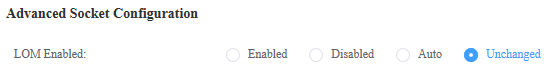


UPI configuration

| Parameter | Function |
| --- | --- |
| XPT Prefetch | Sets the XPT prefetching function. The options are as follows:   * **Enabled** * **Disabled** * **Unchanged**: retains the current configuration. |

In the **Advanced Socket Configuration** area shown in Figure 5-24, set the parameters listed in Table 5-11.

Socket configuration

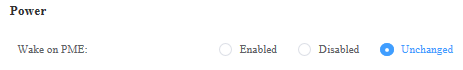


Socket configuration

| Parameter | Function |
| --- | --- |
| LOM Enabled | Indicates whether to enable the LOM. The options are as follows:   * **Enabled** * **Disabled** * **Unchanged**: retains the current configuration. |

In the **Power** area shown in Figure 5-25, set the parameters listed in Table 5-12.

Power configuration

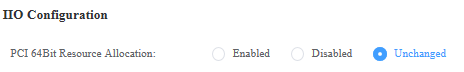


Power configuration

| Parameter | Function |
| --- | --- |
| Wake on PME | Indicates whether to enable the power management event (PME).   * **Enabled** * **Disabled** * **Unchanged**: retains the current configuration. |

In the **IIO Configuration** area shown in Figure 5-26, set the parameters listed in Table 5-13.

IIO configuration



IIO configuration

| Parameter | Function |
| --- | --- |
| PCI 64Bit Resource Allocation | Sets the function of allocating PCI 64-bit resources. The options are as follows:   * **Enabled** * **Disabled** * **Unchanged**: retains the current configuration.   NOTE  If the PCIe devices require resources more than 4 GB, this function will be automatically enabled when the server restarts. |

Click **OK**.

The BIOS configuration template is created.

----End

#### Setting RAID Parameters

On the vCenter WebUI, choose **Menu** > **Shortcuts** > **Administration** > **FusionDirector for vCenter**.

The **FusionDirector for vCenter** page is displayed.

Choose **Configuration**.

The **Configuration** page is displayed.

Click **Create**.

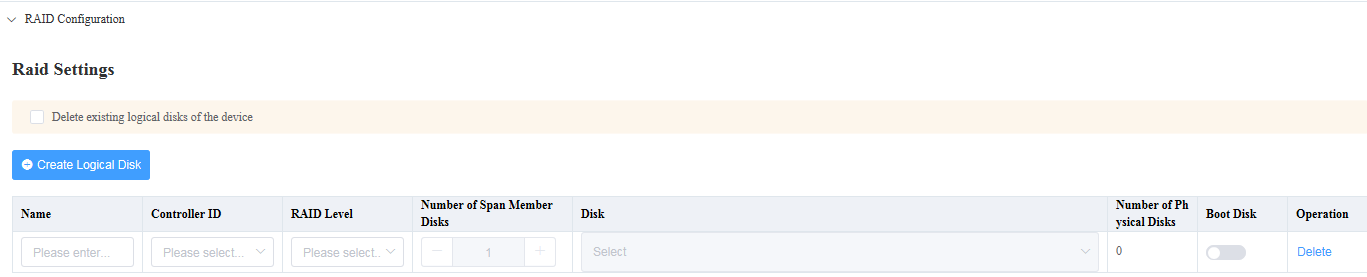
The page for creating a template is displayed.

Click **RAID Configuration**.

The **RAID Configuration** area is displayed.

In the **Raid Settings** area shown in Figure 5-27, set the parameters listed in Table 5-14.

RAID configuration



RAID configuration

| Parameter | | Function |
| --- | --- | --- |
| Delete existing logical disks of the device | | Indicates whether to delete the existing logical disks of the device.  NOTICE  Deleting existing logical disks may cause data loss. Exercise caution when performing this operation. |
| Creating Logical Disk | Name | Indicates the name of the logical disk. |
| Controller ID | Indicates the ID of the controller that controls the logical disk. The value can only be **RAIDStorage0**. |
| RAID Level | Indicates the RAID level of the logical disk. |
| Number of Span Member Disks | Indicates the number of member disks in each span. |
| Disk | Indicates the physical disks of the RAID array.  For RAID 10, the number of physical disks must an even number and must be at least 4. |
| Number of Physical Disks | Indicates the number of added physical disks. |
| Boot Disk | When this option is enabled, the OS boots from the logical disk. Only one logical disk can be set as the boot disk.   * : The logical disk is not set as the boot disk.  * : The logical disk is set as the boot disk. |
| Operation | **Delete**: deletes the created logical disk. |

Click **OK**.

The RAID configuration template is created.

----End

#### Setting NTP Parameters

On the vCenter WebUI, choose **Menu** > **Shortcuts** > **Administration** > **FusionDirector for vCenter**.

The **FusionDirector for vCenter** page is displayed.

Choose **Configuration**.

The **Configuration** page is displayed.

Click **Create**.

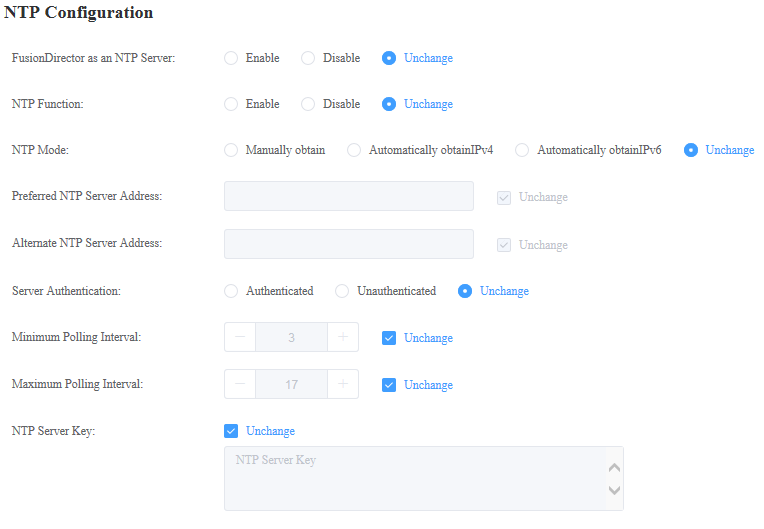
The page for creating a template is displayed.

Click **NTP Configuration**.

The **NTP Configuration** area is displayed.

In the **NTP Configuration** area shown in Figure 5-28, set the parameters listed in Table 5-15.

NTP configuration



NTP configuration

| Parameter | Function |
| --- | --- |
| FusionDirector as an NTP Server | Indicates whether FusionDirector functions as the NTP server and provides the NTP service. The options are as follows:   * **Enabled**: FusionDirector functions as the NTP server. * **Disabled**: FusionDirector does not function as the NTP server. * **Unchanged**: retains the current configuration. |
| NTP Function | Indicates whether the NTP service is enabled on FusionDirector.   * **Enabled** * **Disabled** * **Unchanged**: retains the current configuration. |
| NTP Mode | Indicates the method used to obtain the NTP server address. The options are as follows:   * **Manually obtain**: The user manually configures the IPv4 address, IPv6 address, or domain name of the NTP server.   NOTE  When FusionDirector functions as the NTP server, you do not need to enter the NTP server address.   * **Automatically obtain IPv4**: The system automatically obtains an IPv4 NTP server address. * **Automatically obtain IPv6**: The system automatically obtains an IPv6 NTP server address. * **Unchanged**: retains the current configuration. |
| Preferred NTP Server Address | Indicates the IPv4 address, IPv6 address, or domain name of the alternate NTP server. The address is manually configured by the user. When the preferred and alternate NTP servers are configured, the preferred NTP server is preferentially used for communication. |
| Alternate NTP Server Address | Indicates the IPv4 address, IPv6 address, or domain name of the alternate NTP server. The address is manually configured by the user. When the preferred NTP server is abnormal, the alternate NTP server automatically takes over services from the preferred NTP server. |
| Server Authentication | Indicates whether identity authentication is required when the server communicates with the NTP server. The options are as follows:   * **Authenticated**: enables identity authentication. When this option is selected, you need to configure the NTP server key.   NOTE  When the FusionDirector functions as the NTP server and identity authentication is enabled, you do not need to configure the NTP server key.   * **Unauthenticated**: disables identity authentication. When this option is selected, the NTP server key is not required. * **Unchanged**: retains the current configuration. |
| Minimum Polling Interval | Indicates the minimum interval (minutes) when the server synchronizes time from the NTP server. |
| Maximum Polling Interval | Indicates the maximum interval (minutes) when the server synchronizes time from the NTP server.  NOTE  The system automatically adjusts the synchronization interval based on the network status. When the network is normal, the system sets the synchronization interval to the maximum value. |
| NTP Server Key | When server identity authentication is enabled, you need to upload a key to the server iBMC. The key is used for identity authentication when the server communicates with the NTP server. |

Click **OK**.

The NTP configuration template is created.

----End

#### Setting DNS Parameters

On the vCenter WebUI, choose **Menu** > **Shortcuts** > **Administration** > **FusionDirector for vCenter**.

The **FusionDirector for vCenter** page is displayed.

Choose **Configuration**.

The **Configuration** page is displayed.

Click **Create**.

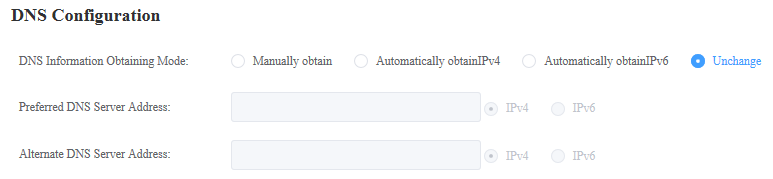
The page for creating a template is displayed.

Click **DNS Configuration**.

The **DNS Configuration** area is displayed.

In the **DNS Configuration** area shown in Figure 5-29, set the parameters listed in Table 5-16.

DNS configuration



DNS configuration

| Parameter | Function |
| --- | --- |
| DNS Information Obtaining Mode | * **Manually obtain**: The user manually configures the DNS server address. * **Automatically obtainIPv4**: The system automatically obtains an IPv4 DNS address. * **Automatically obtainIPv6**: The system automatically obtains an IPv6 DNS address. * **Unchanged**: retains the current configuration. |
| Preferred DNS Server Address | Indicates the IPv4 address or IPv6 address of the alternate DNS server. The address is manually configured by the user. When the preferred and alternate DNS servers are configured, the preferred DNS server is preferentially used for communication. |
| Alternate DNS Server Address | Indicates the IPv4 address or IPv6 address of the alternate DNS server. The address is manually configured by the user. When the preferred DNS server is abnormal, the alternate DNS server automatically takes over services from the preferred DNS server. |

Click **OK**.

The DNS configuration template is created.

----End

#### Setting LDAP Parameters

On the vCenter WebUI, choose **Menu** > **Shortcuts** > **Administration** > **FusionDirector for vCenter**.

The **FusionDirector for vCenter** page is displayed.

Choose **Configuration**.

The **Configuration** page is displayed.

Click **Create**.

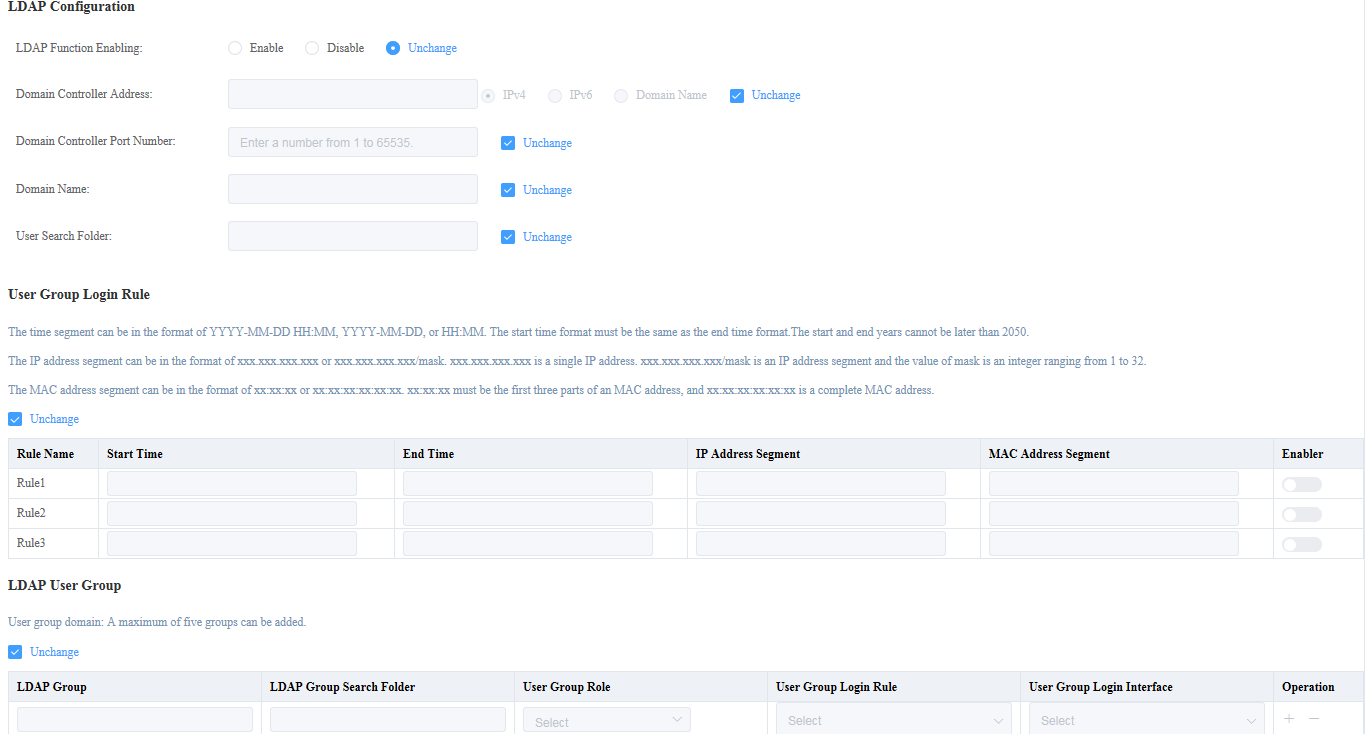
The page for creating a template is displayed.

Click **LDAP Configuration**.

The **LDAP Configuration** area is displayed.

In the **LDAP Configuration** area shown in Figure 5-30, set the parameters listed in Table 5-17.

LDAP configuration



LDAP configuration

| Parameter | | Function |
| --- | --- | --- |
| LDAP Function Enabling | | Sets the LDAP function. The options are as follows:   * **Enabled** * **Disabled** * **Unchanged**: retains the current configuration. |
| Domain Controller Address | | Indicates the address of the LDAP server. The options are as follows:   * **IPv4**, **IPv6**, and **Domain Name** * **Unchanged**: retains the current configuration. |
| Domain Controller Port Number | | Indicates the communication port of the LDAP service.  The value ranges from 1 to 65535. |
| Domain Name | | Indicates the domain of the role group to which the LDAP user defined in the domain controller belongs.  Value length: The value can contain a maximum of 255 characters.  The value can contain letters, digits, and special characters. |
| User Search Folder | | The value must be the same as the name of the search member data folder on the LDAP server, for example, **CN=employee, OU=company** or **OU=department, OU=company**.  Value length: The value can contain a maximum of 255 bytes. The number of bytes occupied by different characters are different. The maximum length of the value can be 64 characters to 255 characters. |
| User Group Login Rule | | Indicates the login rules of the user group members. The settings are as follows:   * Click or to change the status of the rule. indicates that the rule is enabled, and indicates that the rule is disabled.  * **Start Time** and **End Time** of a rule. * **IP Address Segment** and **MAC Address Segment** of a rule. * **Unchanged**: retains the current configuration. |
| LDAP User Group | LDAP Group | Indicates the name of the LDAP group to which the LDAP user belongs.  Value length: The value can contain a maximum of 255 bytes. The number of bytes occupied by different characters are different. The maximum length of the value can be 64 characters to 255 characters. |
| LDAP Group Search Folder | Indicates the name of the application folder to which the LDAP user belongs.  Value length: The value can contain a maximum of 255 bytes. The number of bytes occupied by different characters are different. The maximum length of the value can be 64 characters to 255 characters. |
| User Group Role | Indicates the permission of the group domain to access the server iBMC.   * Administrator * Operator * Common User |
| User Group Login Interface | Indicates the interface types used in LDAP group user login. The options are as follows:   * SSH * Redfish * Web |
| Operation | You can operate the LDAP group by using the following operations.  : adds an LDAP group.  : deletes an LDAP group. |

Click **OK**.

The LDAP configuration template is created.

----End

### Deploying an OS

#### OS Image

Scenarios

You can add, modify, or delete OS image files on this page. Before deploying an OS on a server, you need to add an OS image file.

Prerequisites

The OS compatibility of the server has been confirmed using the [Intelligent Computing Compatibility Checker](http://support.huawei.com/onlinetoolweb/ftca/en), and **Note 79** is present in the **Notes** column.

Procedure

On the vCenter WebUI, choose **Menu** > **Shortcuts** > **Administration** > **FusionDirector for vCenter**.

The **FusionDirector for vCenter** page is displayed.

Choose **Deployment** > **OS Image**.

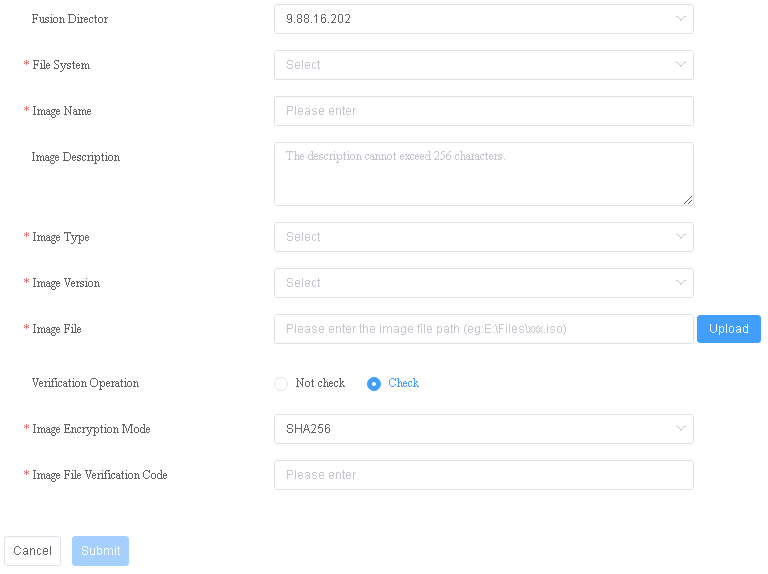
The **OS Image** page is displayed.

Click **Create**.

The page for creating an OS image is displayed.

Set the following parameters, as shown in Figure 5-31.

Adding software source



* **Fusion Director**: selects a FusionDirector system.
* **File type**: selects **Standard**.
* **Image Name**: indicates the OS image file name.
* **Image Description**: (optional) indicates the OS image file description.
* **Image Type**: indicates the OS type. The value is **VMware**.
* **Image Version**: selects an OS version.
* **Image File**: uploads the local OS image file.
* **Verification Operation**: selects **Check** or **Not check** as required.
* **Image Encryption Mode**: indicates the encryption mode. The values can be **SHA256** and **MD5**.
* **Image File Verification Code**: enters the verification code of the image file.

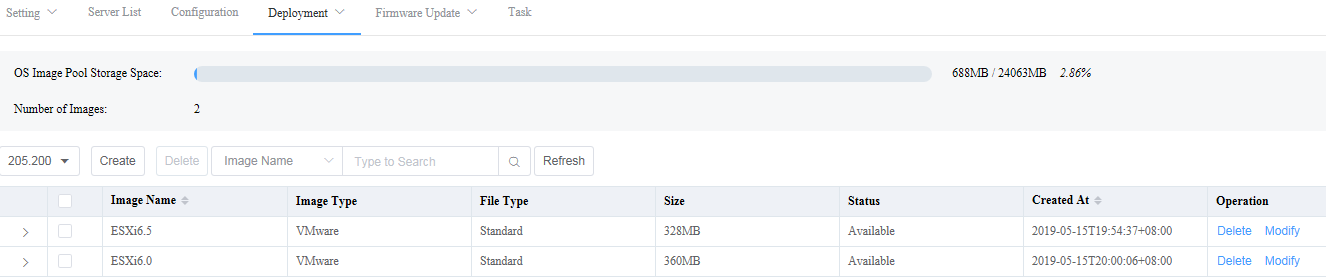
Click **Submit**. The **Prompt** dialog box is displayed.

Click **OK**.

The OS image is created.

You can view the created OS images on the **OS Image** page, as shown in Figure 5-32.

OS image management



* Click to view the basic information about the OS image.



* To modify the description of a created OS image, click **Modify** in the **Operation** column.
* To delete a created OS image, click **Delete** in the **Operation** column.

----End

#### Creating an OS Deployment Template

Procedure

On the vCenter WebUI, choose **Menu** > **Shortcuts** > **Administration** > **FusionDirector for vCenter**.

The **FusionDirector for vCenter** page is displayed.

Choose **Deployment** > **OS Deployment**.

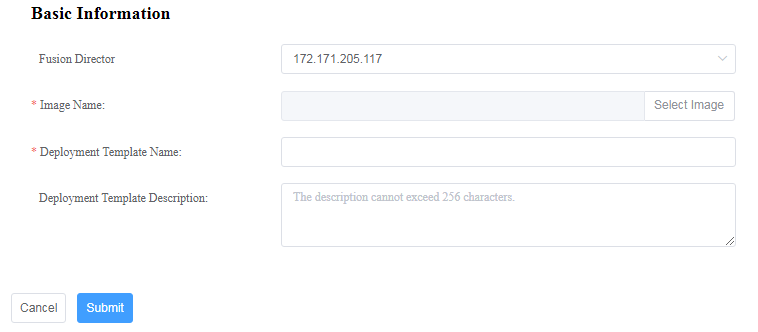
The **OS Deployment** page is displayed.

Click **Create**.

The page for creating an OS deployment template is displayed.

In the **Basic Information** area, set the following parameters, as shown in Figure 5-33.

Basic information



* **Fusion Director**: selects a FusionDirector system.
* **Image Name**: select the OS image created in 5.5.3.1 OS Image.
* **Deployment Template Name**: indicates the OS deployment template name.
* **Deployment Template Description**: (optional) indicates the description of the OS deployment template.

In the **Installation Information** area, set the following parameters and click **Submit**, as shown in Figure 5-33.



The **Installation Information** area is displayed only after you select an OS image in the **Basic Information** area.

Installation information



* **Administrator Password**: indicates the OS administrator password.
* **Confirm Password**: enters the OS administrator password again.

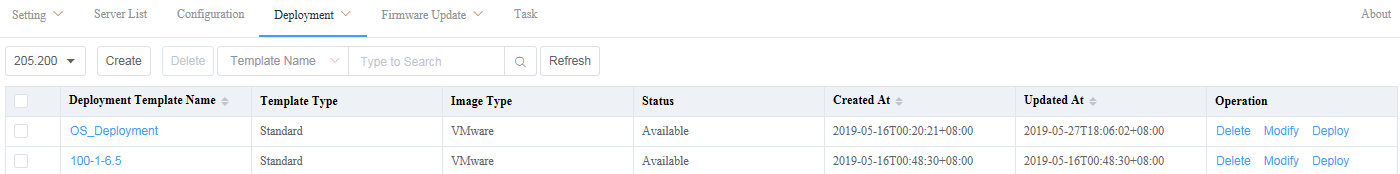
The **Prompt** dialog box is displayed.

Click **OK**.

The OS deployment template is created.

You can view the created deployment templates on the **OS Deployment** page, as shown in Figure 5-35.

OS deployment template



----End

#### OS Deployment



If the iBMC version is later than 3.08, the server supports OS deployment only after obtaining the license authorization. If the OS deployment fails due to the lack of license authorization as prompted, contact [Huawei technical support](https://e.huawei.com/en/) to resolve the license authorization problem.

Procedure

On the vCenter WebUI, choose **Menu** > **Shortcuts** > **Administration** > **FusionDirector for vCenter**.

The **FusionDirector for vCenter** page is displayed.

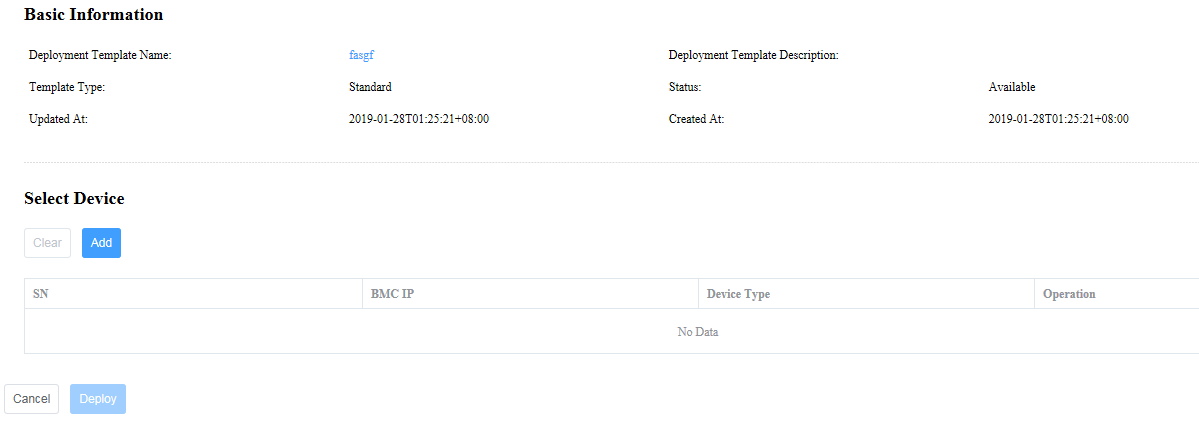
Choose **Deployment** > **OS Deployment**.

The **OS Deployment** page is displayed.

Click **Deploy** in the **Operation** column of the template to be deployed.

The deployment page is displayed, as shown in Figure 5-36.

Deployment



In the **Select Device** area, click **Add**.

The **Add Device** dialog box is displayed.

Select the server where the OS is to be deployed and click **OK**, as shown in Figure 5-37.

Adding a device



On the deployment page, click **Deploy**.

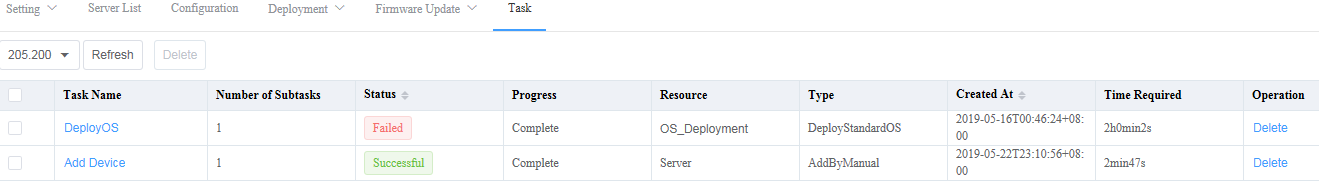
The deployment task is started.

Check the OS deployment status and progress.

On the **Fusion Director for vCenter** page, choose **Task**.

The **Task** page is displayed, as shown in Figure 5-38.

Task



----End

### Upgrading Firmware and Drivers

* Upgrade for the out-of-band firmware BMC, BIOS, and CPLD is supported.
* Upgrade for the in-band firmware RAD controller card and NIC is supported.
* Upgrade for the Smart Provisioning firmware, power supply firmware, and drivers is supported.

#### Version Repository Management

##### Uploading an Update Package

Prerequisites

* To upgrade the in-band firmware, the Smart Provisioning version must be 1.18 or later.
* You have obtained Huawei baseline and firmware packages from [Huawei Online Upgrade Platform (HOUP)](https://houp.huawei.com/download/server/Huawei/).
* You have obtained the software packages and digital signatures from [Huawei Support website](https://support.huawei.com/enterprise/en/category/intelligent-servers-pid-1548148142425?submodel=15791).

Automatically Obtaining an Update Package

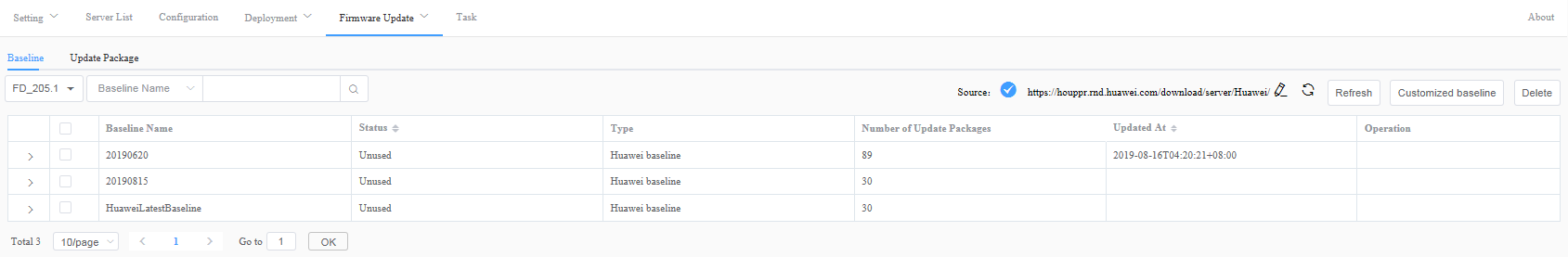
On the vCenter WebUI, choose **Menu** > **Shortcuts** > **Administration** > **FusionDirector for vCenter**.

The **FusionDirector for vCenter** page is displayed.

Choose **Firmware Update** > **Version Repository** > **Baseline**.

The **Baseline** page is displayed, as shown in Figure 5-39.

Baseline

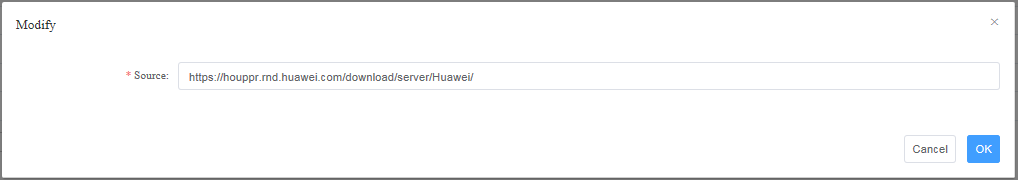


Select a FusionDirector system.

Click and enter the source of the software package, as shown in Figure 5-40.



Source



Click **OK**.

* : indicates that the source fails to be connected. Handle the problem according to the troubleshooting suggestions.



* 1. Check whether the website is correct.
  2. Check whether the DNS or proxy is available.

If the problem persists, contact Huawei technical support.

* : indicates that the source can be accessed. FusionDirector automatically synchronizes the update package and baseline from the source in the background. SCCM automatically obtains the update package and baseline synchronized from FusionDirector.



Click **>** next to a baseline name to view the automatically obtained update package and baseline.

Click the **Update Package** tab. On the **Update Package** page, view the automatically obtained update package.

----End

Manually Uploading an Update Package

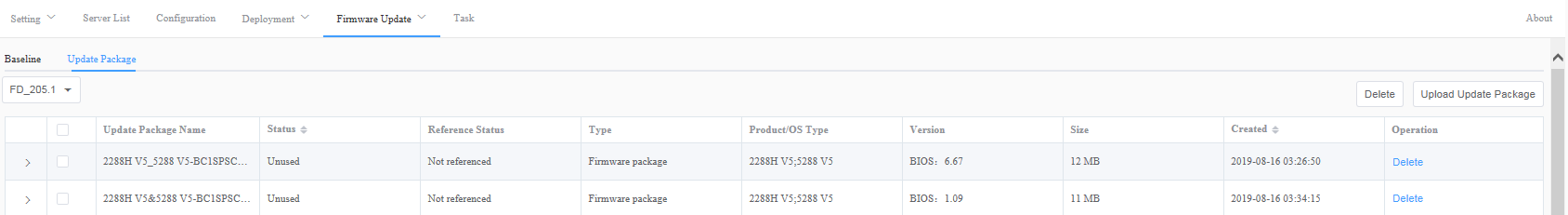
On the vCenter WebUI, choose **Menu** > **Shortcuts** > **Administration** > **FusionDirector for vCenter**.

The **FusionDirector for vCenter** page is displayed.

Choose **Firmware Update** > **Version Repository** > **Update Package**.

The **Update Package** page is displayed, as shown in Figure 5-41.

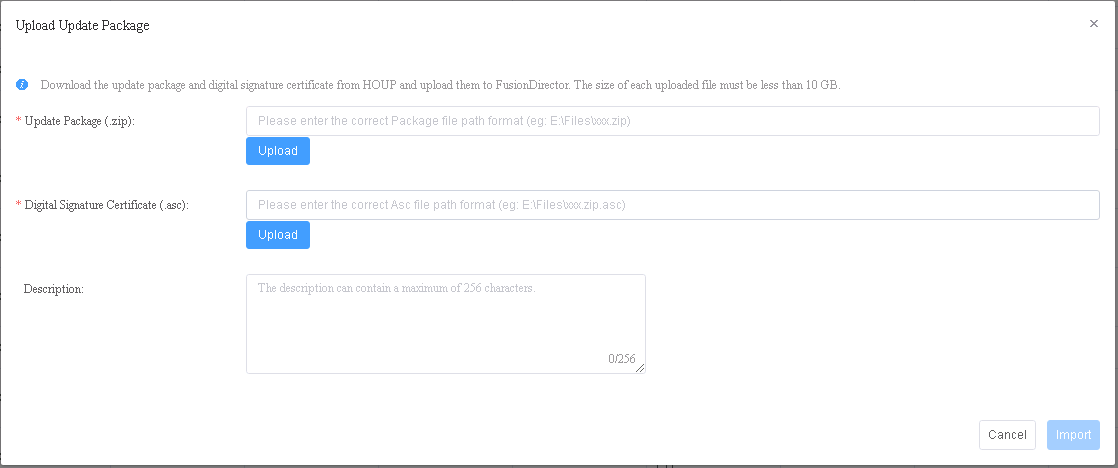
Update package



Click **Upload Update Package**.

The **Upload Update Package** page is displayed. Set the following parameters, as shown in Figure 5-42.

Uploading an update package



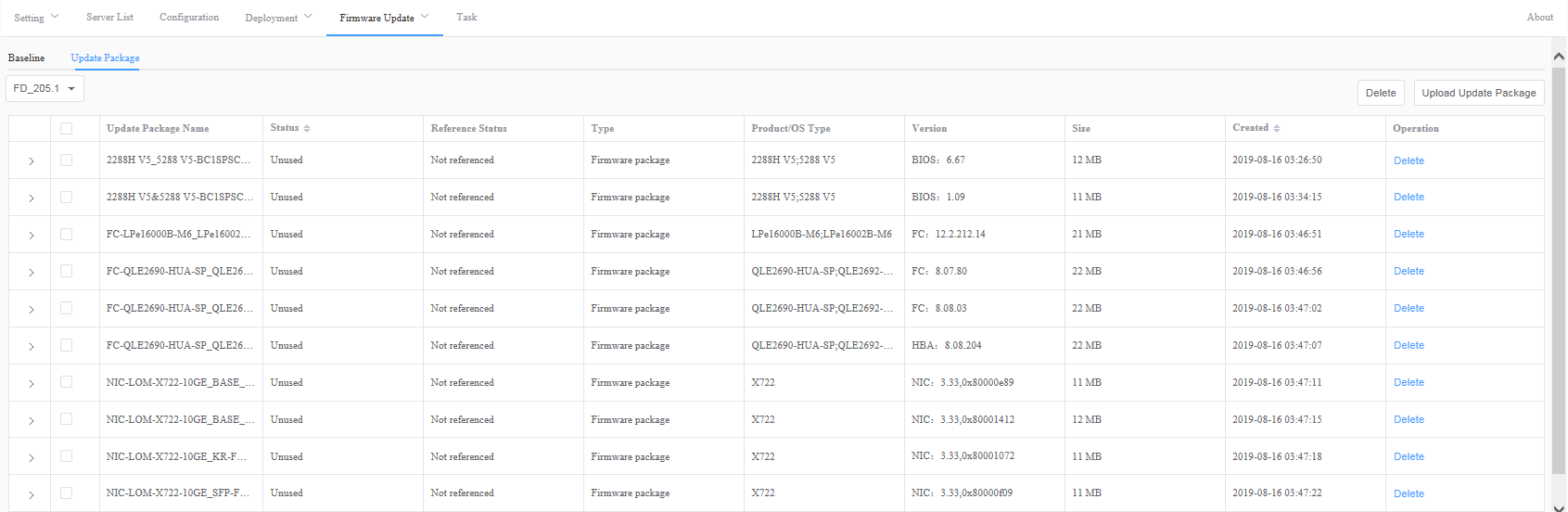
* **Update Package (.zip)**: Enter the path where the local update package is stored and upload the update package in .zip format.
* **Digital Signature Certificate (.asc)**: Enter the path of the local digital signature file and upload the digital signature certificate file in .asc format.
* **Description**: Update package description.

Click **Import**.

The update package is imported.

You can view the uploaded update packages on the **Update Package** page, as shown in Figure 5-43.

Update package



To delete an uploaded update package, click **Delete** in the **Operation** column. The update package that is referenced by the baseline or in use cannot be deleted.

----End

##### Customizing a Baseline

Automatically Obtaining a Baseline

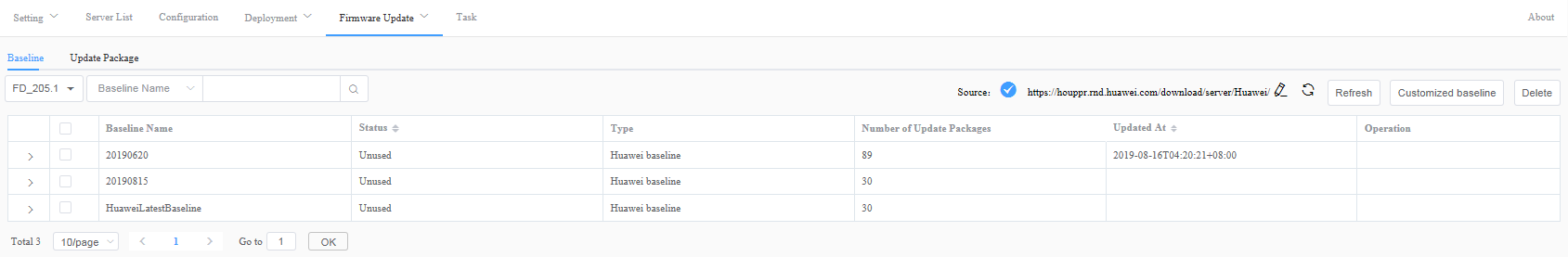
On the vCenter WebUI, choose **Menu** > **Shortcuts** > **Administration** > **FusionDirector for vCenter**.

The **FusionDirector for vCenter** page is displayed.

Choose **Firmware Update** > **Version Repository** > **Baseline**.

The **Baseline** page is displayed, as shown in Figure 5-44.

Baseline

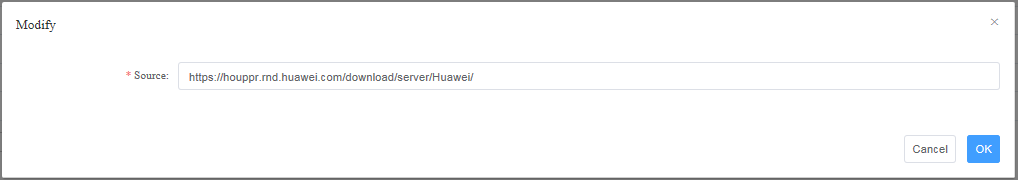


Select a FusionDirector system.

Click and enter the source of the baseline, as shown in Figure 5-45.



Source



Click **OK**.

* : indicates that the source fails to be connected. Handle the problem according to the troubleshooting suggestions.



* 1. Check whether the website is correct.
  2. Check whether the DNS or proxy is available.

If the problem persists, contact Huawei technical support.

* : indicates that the source can be accessed. FusionDirector automatically synchronizes the update package and baseline from the source in the background. SCCM automatically obtains the update package and baseline synchronized from FusionDirector.



Click **>** next to a baseline name to view the automatically obtained update package and baseline.

----End

Manually Customizing a Baseline

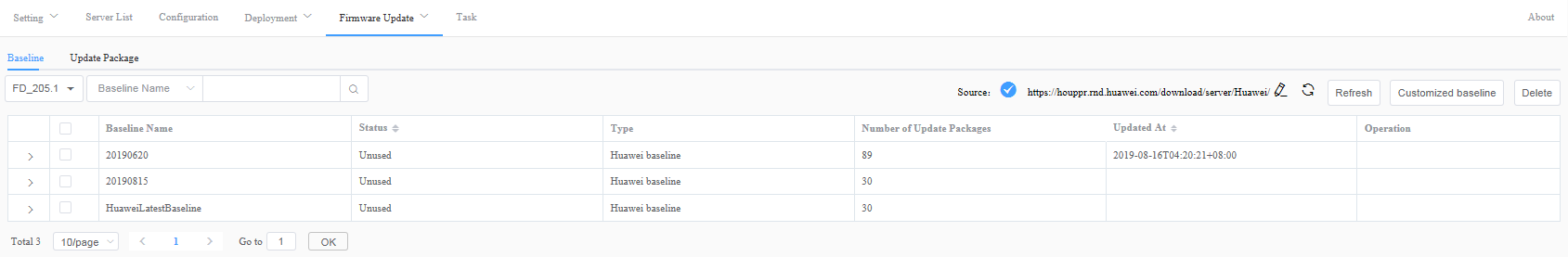
On the vCenter WebUI, choose **Menu** > **Shortcuts** > **Administration** > **FusionDirector for vCenter**.

The **FusionDirector for vCenter** page is displayed.

Choose **Firmware Update** > **Version Repository** > **Baseline**.

The **Baseline** page is displayed, as shown in Figure 5-46.

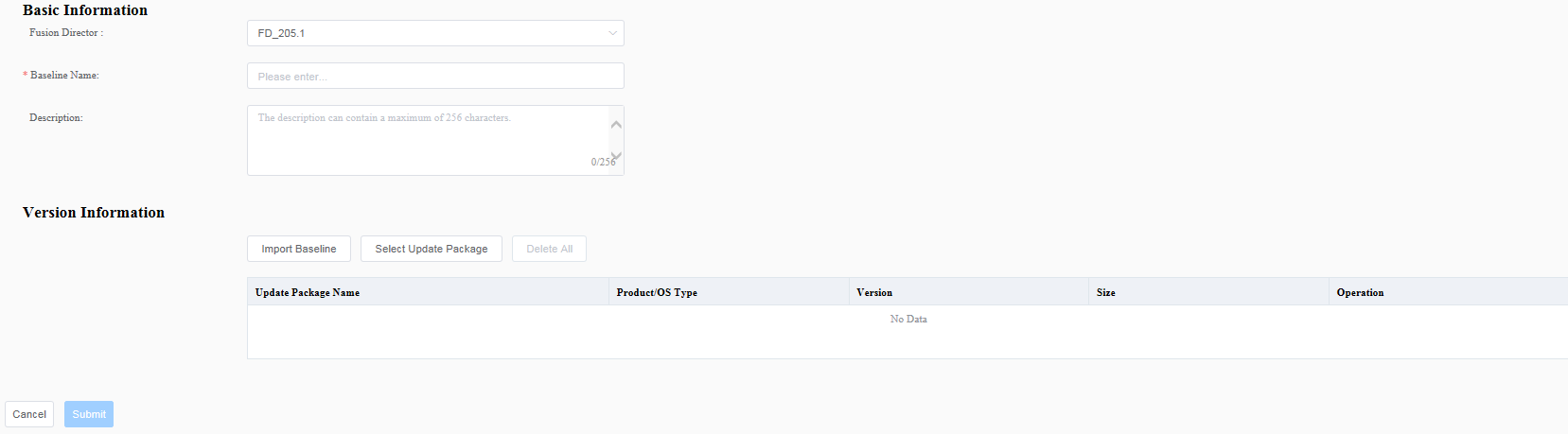
Baseline



Click **Customized baseline**.

The **Customized baseline** page is displayed. Set the following parameters, as shown in Figure 5-47.

Customizing a baseline



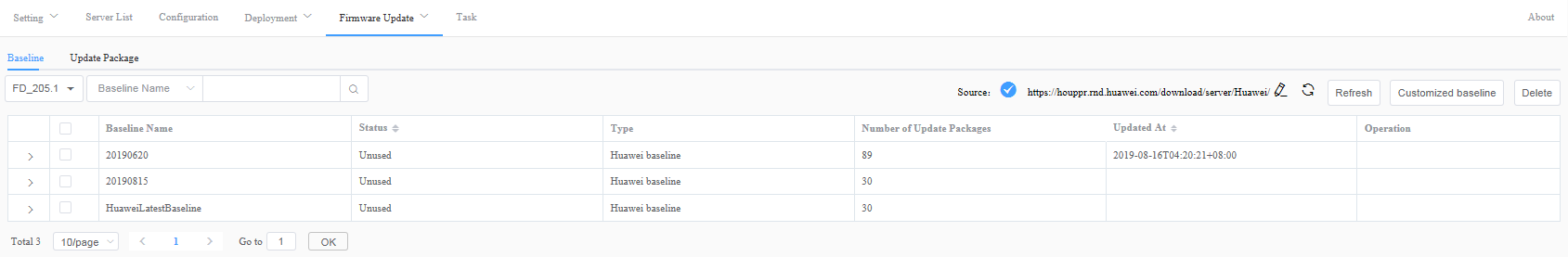
* **Fusion Director**: selects a FusionDirector system.
* **Baseline Name**: indicates the baseline name.
* **Description**: indicates the baseline description.
* **Version Information**: imports an existing baseline or update package.
* **Import Baseline**: selects the created baselines to form an update package for the customized baseline.
* **Select Update Package**: selects the uploaded update packages to form an update package for the customized baseline.

Click **Submit**.

The baseline is created.

You can view the created baselines on the **Baseline** page, as shown in Figure 5-48.

Baseline



----End

#### Update Schedule Management

##### Creating an Update Schedule

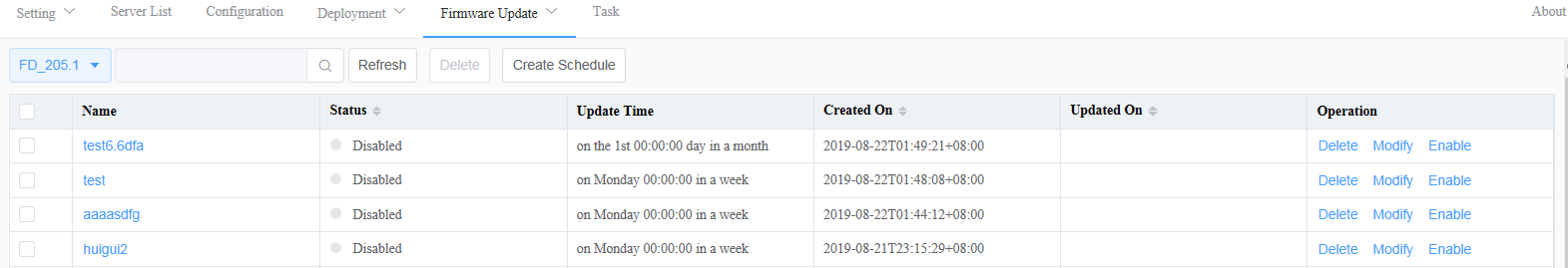
On the vCenter WebUI, choose **Menu** > **Shortcuts** > **Administration** > **FusionDirector for vCenter**.

The **FusionDirector for vCenter** page is displayed.

Choose **Firmware Update** > **Update Schedule**.

The **Update Schedule** page is displayed, as shown in Figure 5-49.

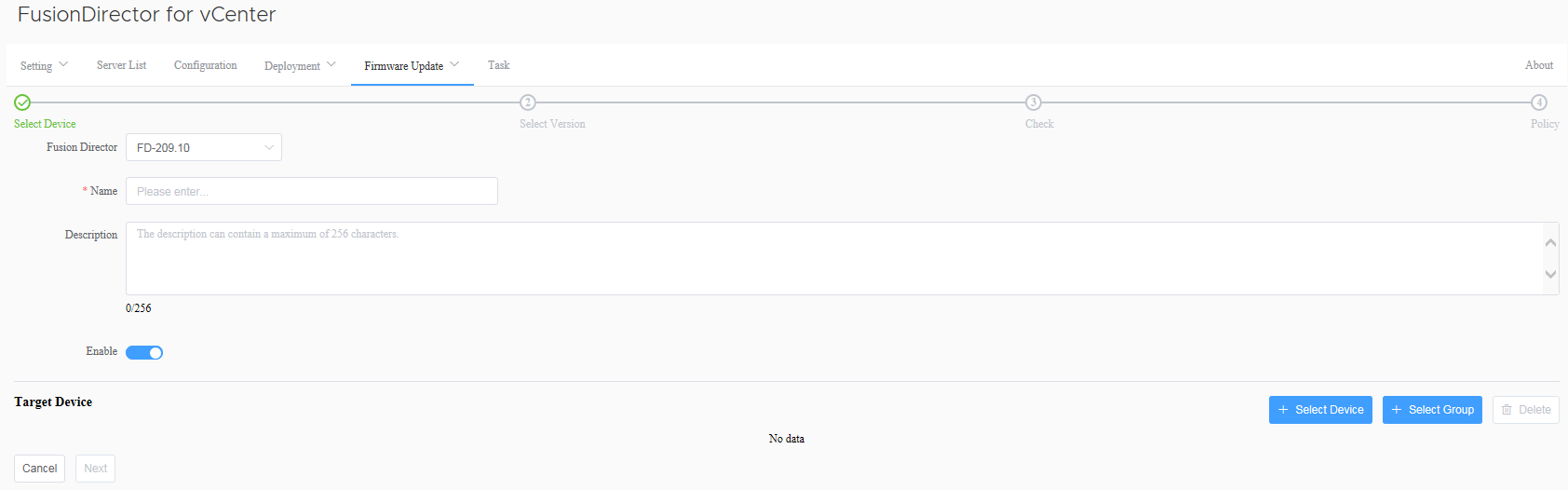
Update schedule



Click **Create Schedule**.

On the **Select Device** page, set the parameters and select groups or devices, as shown in Figure 5-50.

Selecting devices



* **Fusion Director**: selects a FusionDirector system.
* **Name**: indicates the schedule name.



The value can contain 1 to 32 characters, including Chinese characters, letters, digits, hyphens (-), underscores (\_), and dots (.).

* **Description**: indicates the schedule description.
* **Enable**: indicates whether to enable the update schedule. indicates that the schedule is enabled. indicates that the schedule is disabled.



* **Select Device**: You can click to select the device to be updated.



* You can select only one of **Select Device** and **Select Group**.
* To delete a device, click **Delete** on the right.
* **Select Group**: You can click to select the group to be updated.



Private groups created on FusionDirector are invisible on the FusionDirector for vCenter plug-in. To make all groups visible, ensure that all groups are set to non-private groups when they are created.

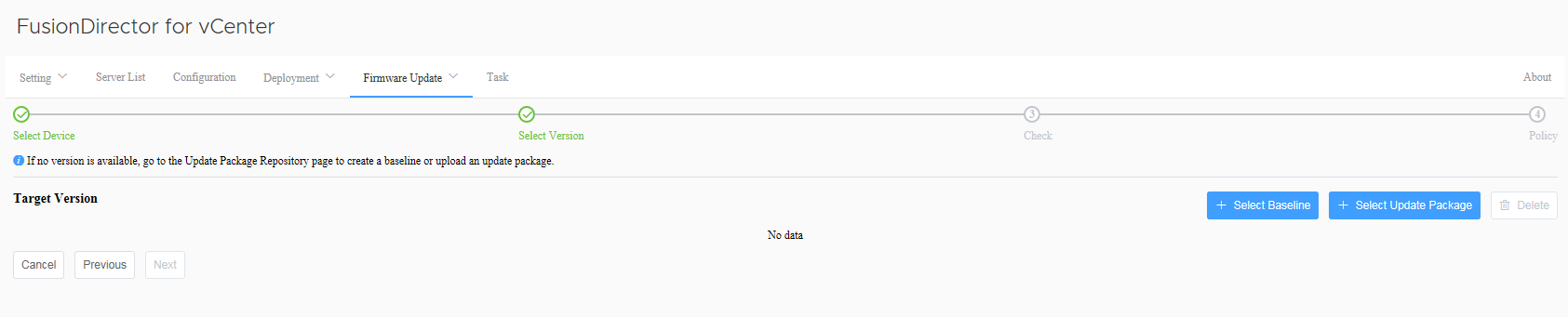


* You can select only one of **Select Device** and **Select Group**.
* To delete a group, click **Delete** on the right.

Click **Next**.

The page for selecting baselines or update packages is displayed, as shown in Figure 5-51.

Selecting baselines or update packages



Click **Select Baseline** or **Select Update Package** to select the required update file.



* You can select only one of **Select Baseline** and **Select Update Package**.
* To delete a baseline or update package, click **Delete** on the right.

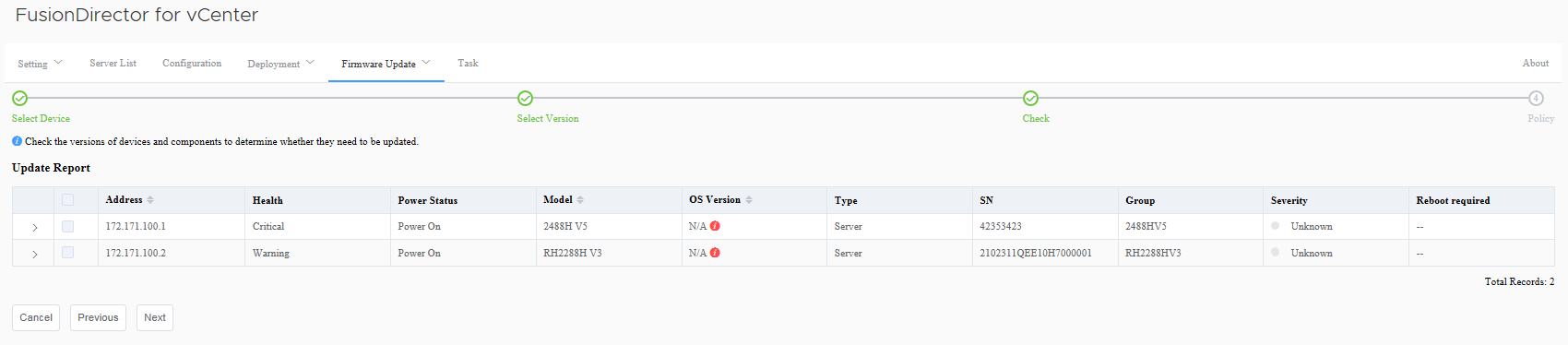
Click **Next**.

On the **Update Report** page, select the device to be updated, as shown in Figure 5-52.



* Click **>** on the left of the update report to view details about each update component.
* By default, the firmware of the same version is not selected for update.
* By default, the in-band firmware and Smart Provisioning firmware is not selected for update.

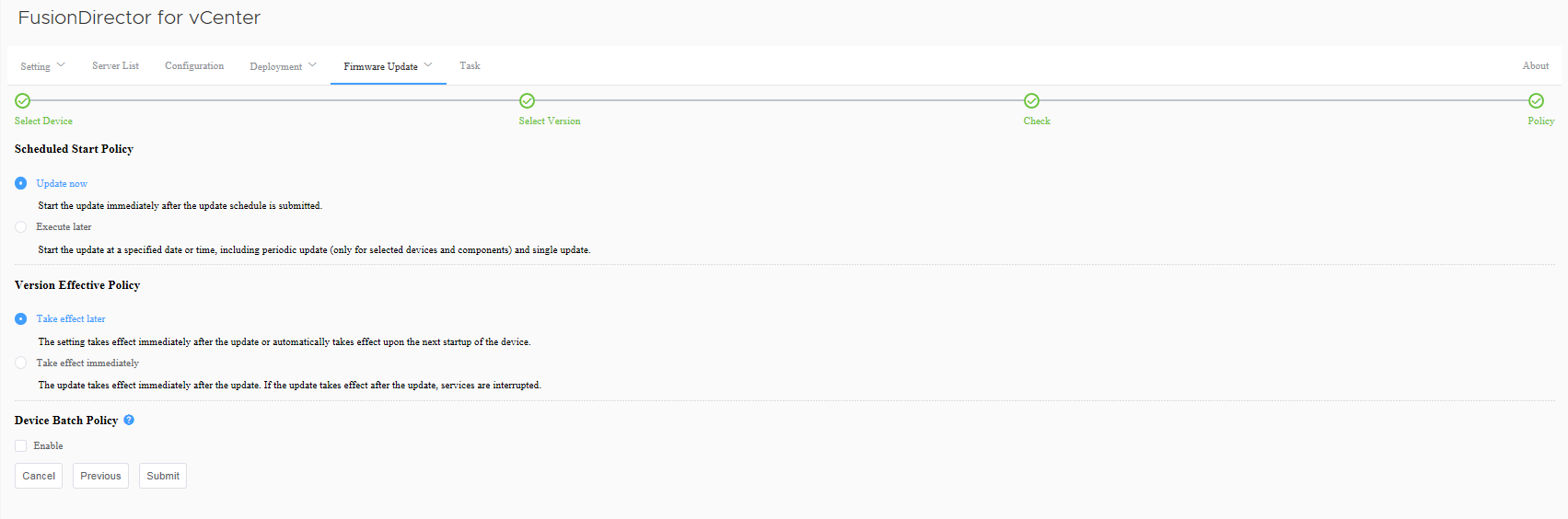
Update report



Click **Next**.

The **Policy** page is displayed, as shown in Figure 5-53.

Update policy



* **Schedule Start Policy**: selects the required scheduled start policy.
* **Update now**: After the schedule is submitted, the system updates the devices immediately.
* **Execute later**: After the schedule is submitted, the system executes the schedule at the specified date/time once or periodically for the selected devices and components. You can specify the week, date, or time for the update.
* **Version Effective Policy**: selects the required version effective policy.
* **Take effect later**: The update takes effect manually or takes effect upon the next startup of the device.



The BMC firmware update takes effect immediately even if you select **Take effect later**.

* **Take effect immediately**: The update takes effect immediately. If activation requires device restart, services will be interrupted
* **Device Batch Policy**: indicates whether to enable the device batch policy.

Click **Submit**.

The update schedule is created.

----End

##### Viewing the Update Schedule

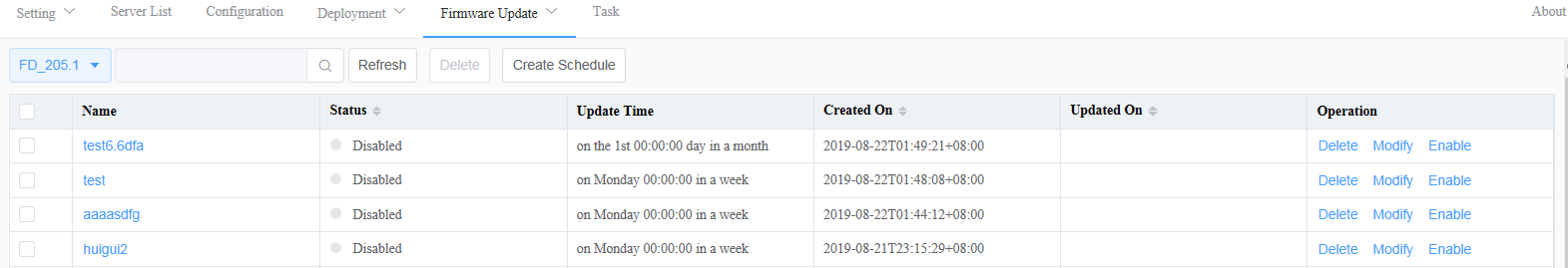
On the vCenter WebUI, choose **Menu** > **Shortcuts** > **Administration** > **FusionDirector for vCenter**.

The **FusionDirector for vCenter** page is displayed.

Choose **Firmware Update** > **Update Schedule**.

The **Update Schedule** page is displayed, as shown in Figure 5-54.

Update schedule



Click the name of the update schedule to view the details, as shown in Figure 5-55.

Detailed update schedule



----End

#### Checking Device Version and Status

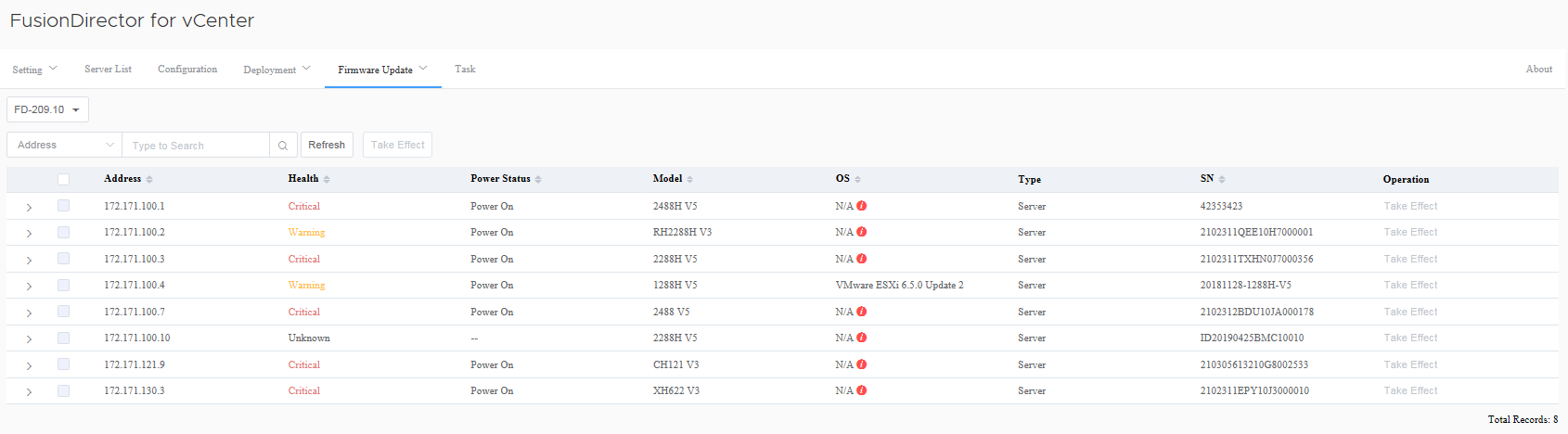
On the vCenter WebUI, choose **Menu** > **Shortcuts** > **Administration** > **FusionDirector for vCenter**.

The **FusionDirector for vCenter** page is displayed.

Choose **Firmware Update** > **Device Version Information**.

The **Device Version Information** page is displayed, as shown in Figure 5-56.

Device version information

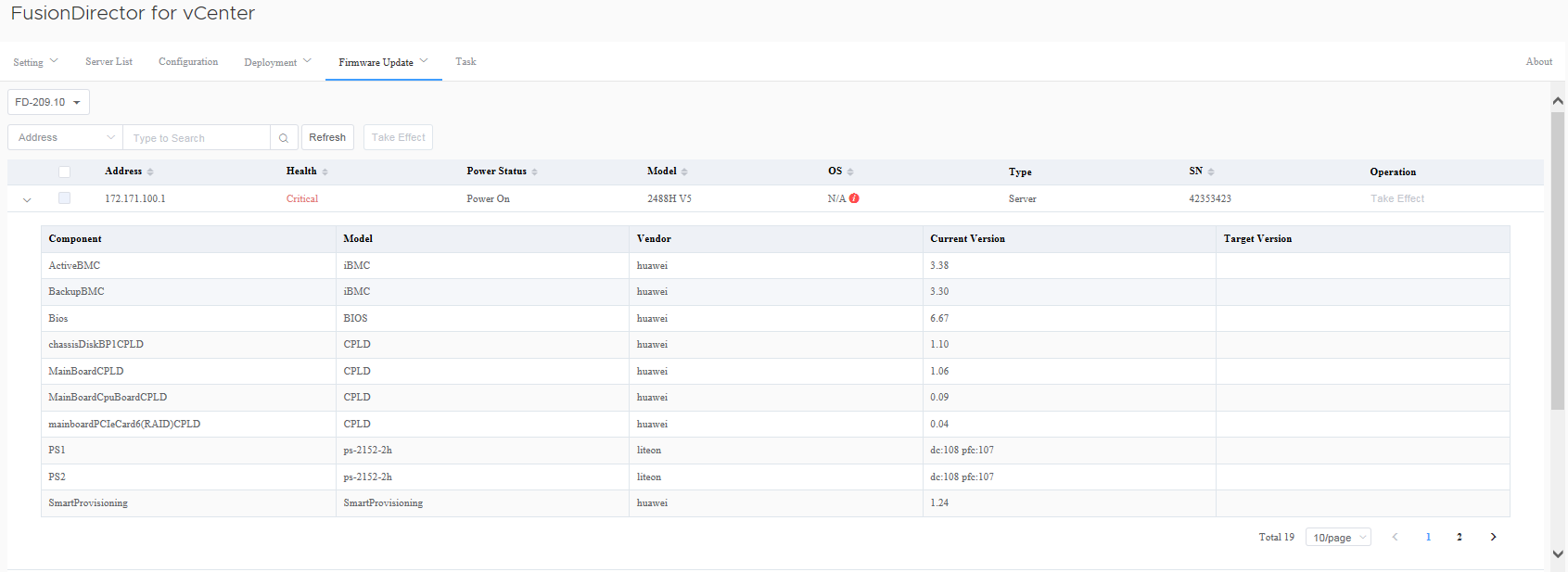


Select a FusionDirector system.

In the server list, click to view the device version information of the server, as shown in Figure 5-57.



Detailed device version information



----End

### Configuring and Using Proactive HA

#### Adding a Host to a Cluster

The following uses the plug-in in HTML5 mode as an example.

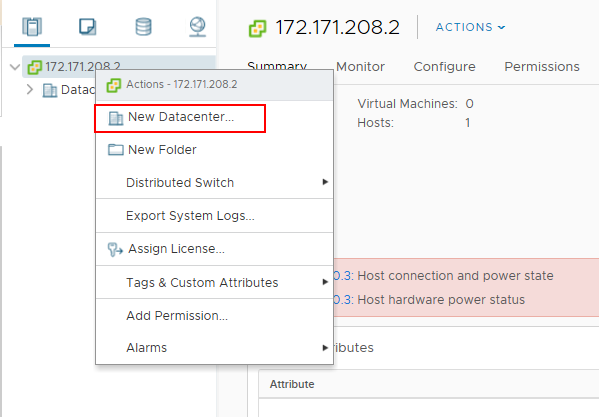
On the vCenter WebUI, choose **Menu**> **Hosts and Clusters**.

The **Hosts and Clusters** page is displayed.

Creating a Data Center

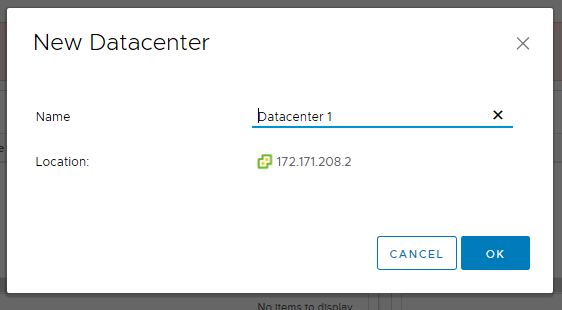
1. Right-click the host name.
2. Choose **New Datacenter**, as shown in Figure 5-58.

Creating a data center 1



1. In the displayed **New Datacenter** dialog box, enter the name of the data center, as shown in Figure 5-59.

Creating a data center 2



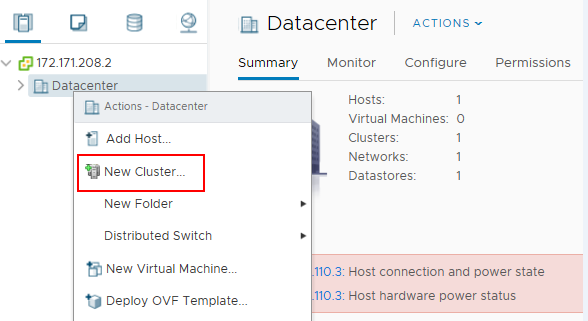
1. Click **OK**.

The data center is created.

Create a cluster.

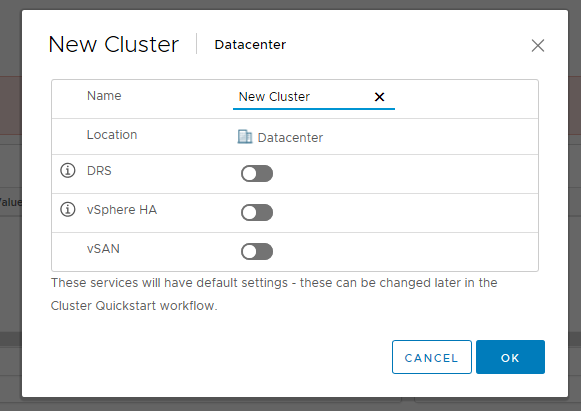
1. Right-click the name of the data center where the cluster is to be created.
2. Choose **New Cluster**, as shown in Figure 5-60.

Creating a cluster 1



1. In the displayed **New Cluster** dialog box, enter the cluster name and enable **DRS**, **vSphere HA**, or **vSAV** as required, as shown in Figure 5-61.

Creating a cluster 2



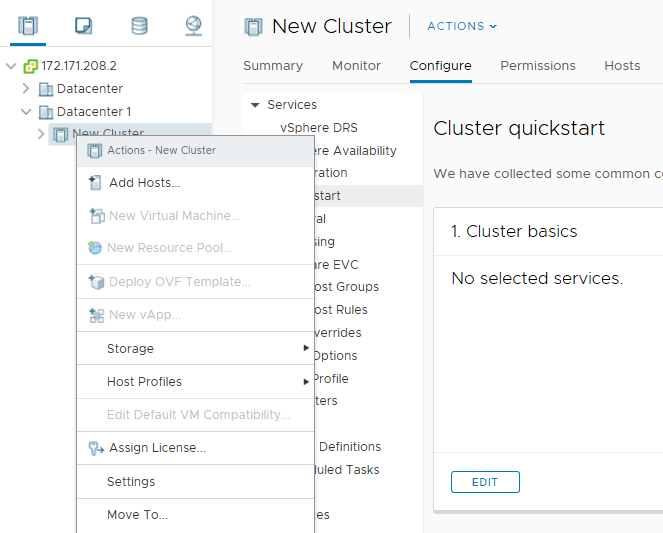
1. Click **OK**.

The cluster is created.

Add a host to a cluster.

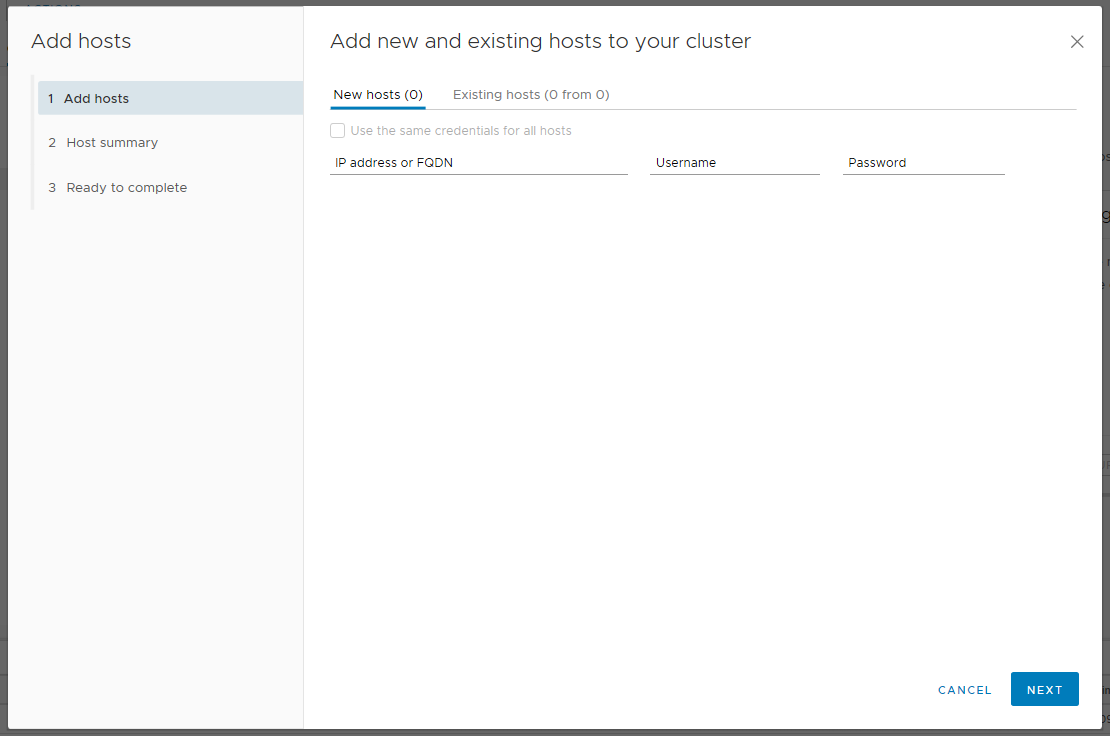
1. Right-click the name of the cluster to which the host is to be added.
2. Choose **Add Hosts**, as shown in Figure 5-62.

Adding a host 1



1. On the displayed **Add new and existing hosts to your cluster** page, choose **New hosts**, as shown in Figure 5-63.

Adding a host 2



1. Enter the following parameters:

* **IP address or FQDN**: IP address or FQDN domain name of the host to be added.
* **Username**: user name of the host to be added.
* **Password**: password for logging in to the host to be added.
* **Use the same credential for all hosts**: You can select this option to use the same credential for all hosts.

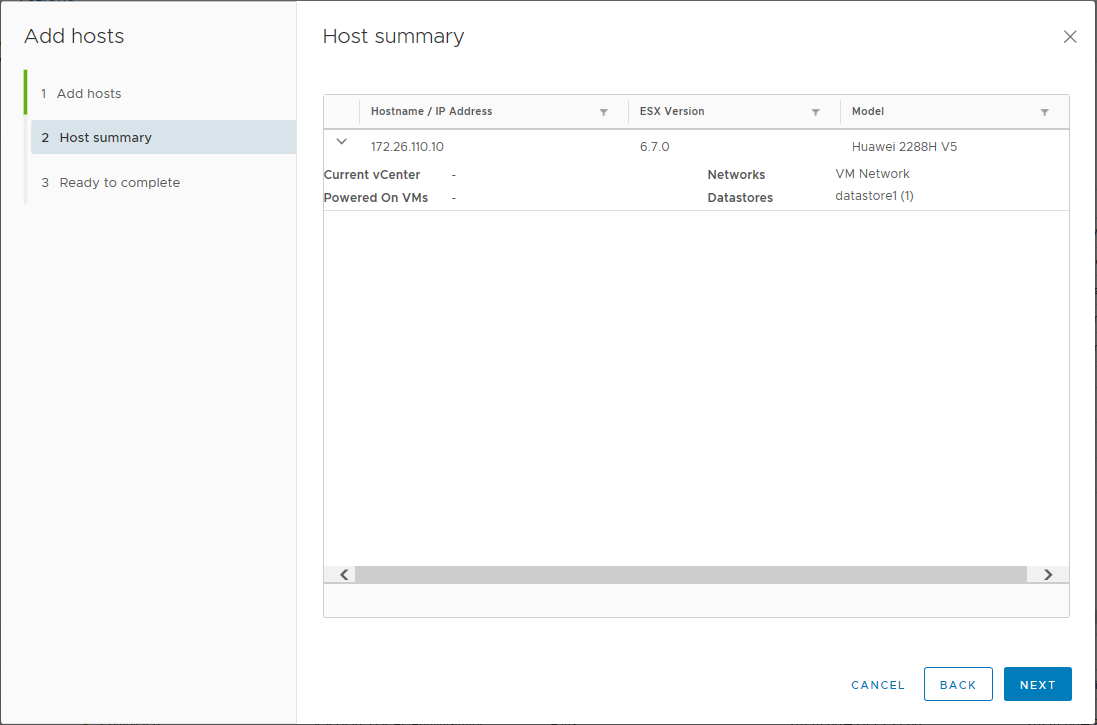
1. Click **Next**.

The **Host summary** page is displayed.

1. In the host list, click to view the details about the host, as shown in Figure 5-64.



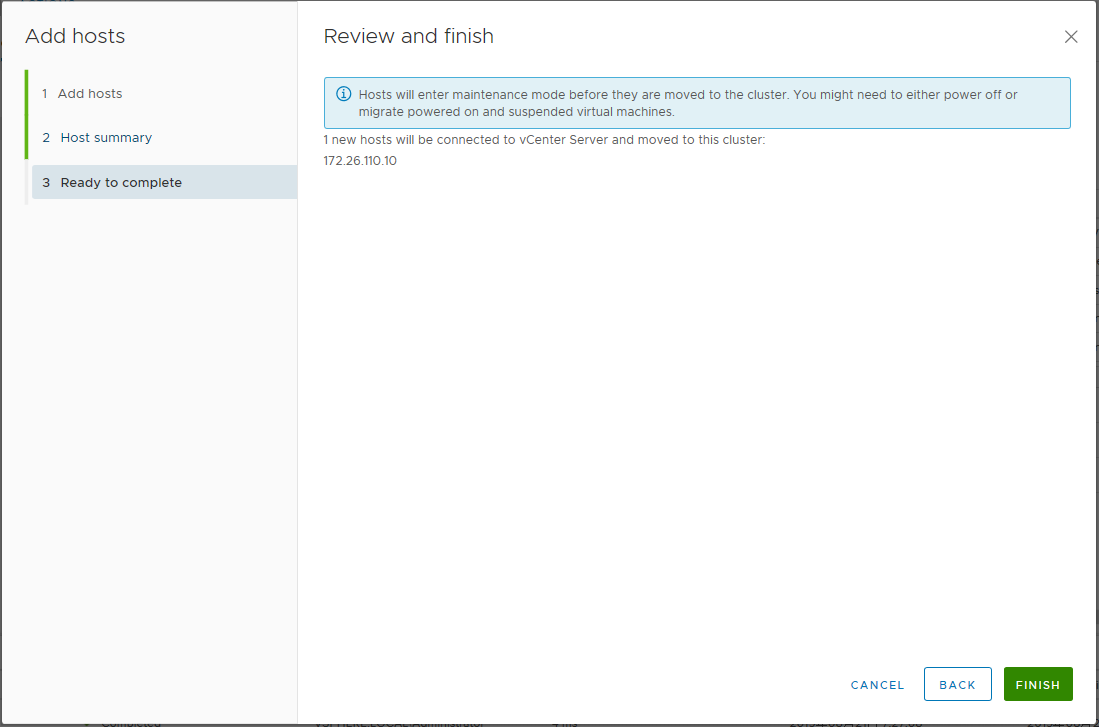
Detailed host information



1. Click **Next**.

The **Review and finish** page is displayed, as shown in Figure 5-65.

Review and finish page

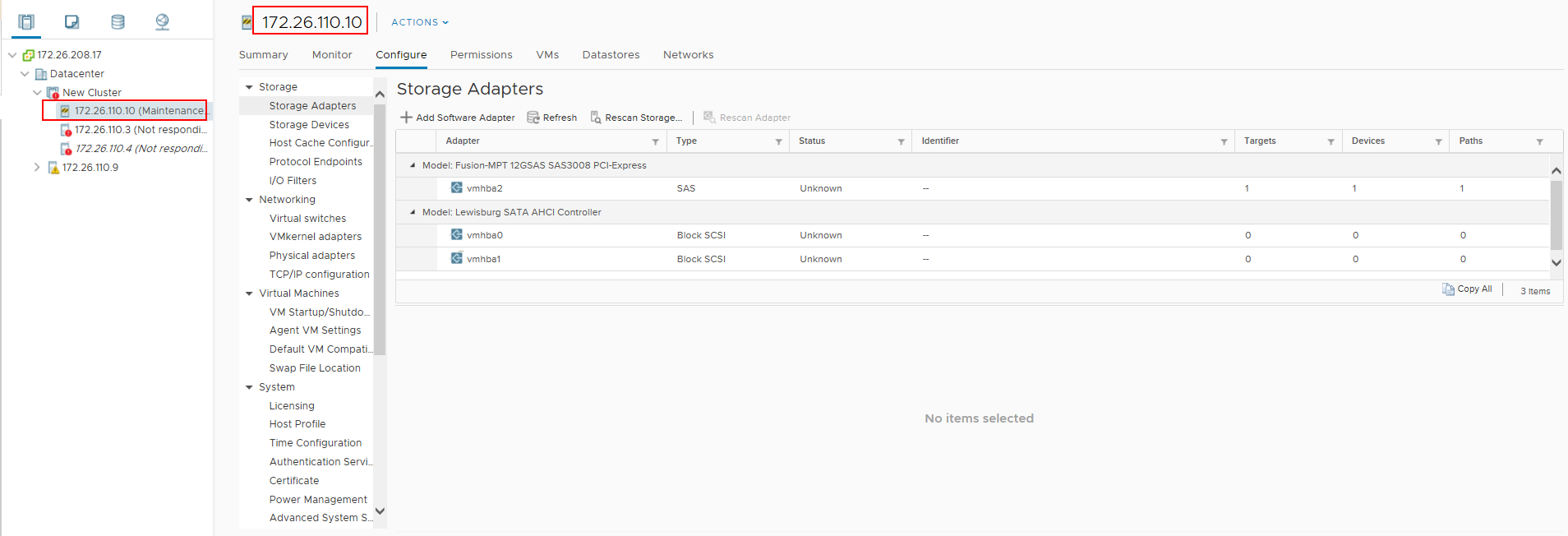


1. Click **Finish**.

The host is added.

You can view the added hosts in the cluster, as shown in Figure 5-66.

Viewing the added hosts



----End

#### Configuring Proactive HA

On the vCenter WebUI, choose **Menu**> **Hosts and Clusters**.

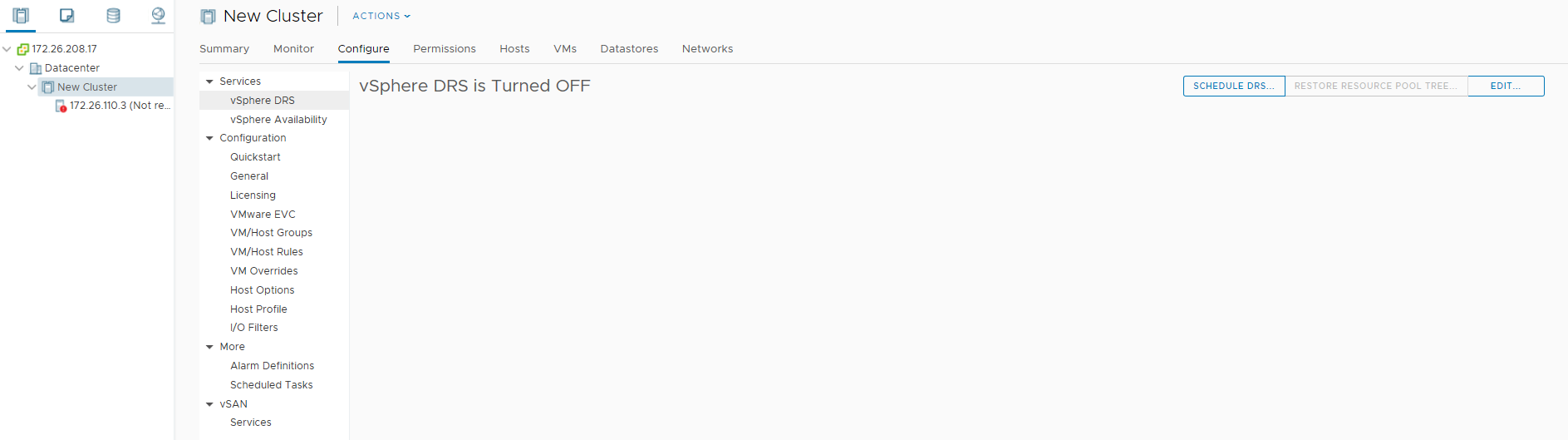
The **Hosts and Clusters** page is displayed.

Enable vSphere DRS.

1. Click the name of the cluster where the target host is located, and then choose **Configure** > **Services** > **vSphere DRS**.

The **vSphere DRS** screen is displayed, as shown in Figure 5-67.

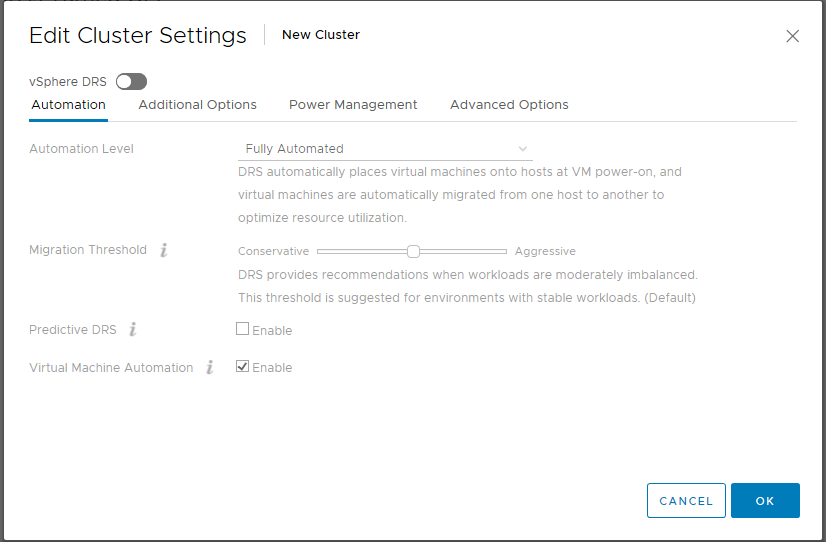
vSphere DRS



1. Click **Edit** in the upper right corner.

The **Edit Cluster Settings** page is displayed, as shown in Figure 5-68.

Editing cluster settings



1. Enable **vSphere DRS** and click **OK**.

Enable **vSphere HA** and **Proactive HA**.

Choose **Configure** > **Services** > **vSphere Availability**.

The **vSphere Availability** page is displayed, as shown in Figure 5-69.

vSphere availability

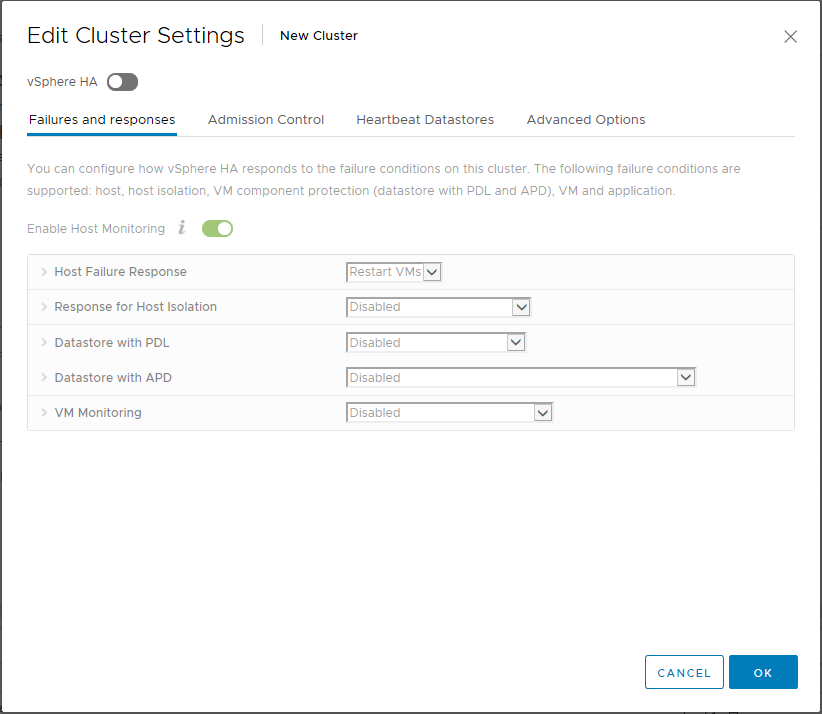


* Enable vSphere HA.

1. Click **Edit** on the right of **vSphere HA is Turned Off**.

The **Edit Cluster Settings** page is displayed, as shown in Figure 5-70.

Editing cluster settings



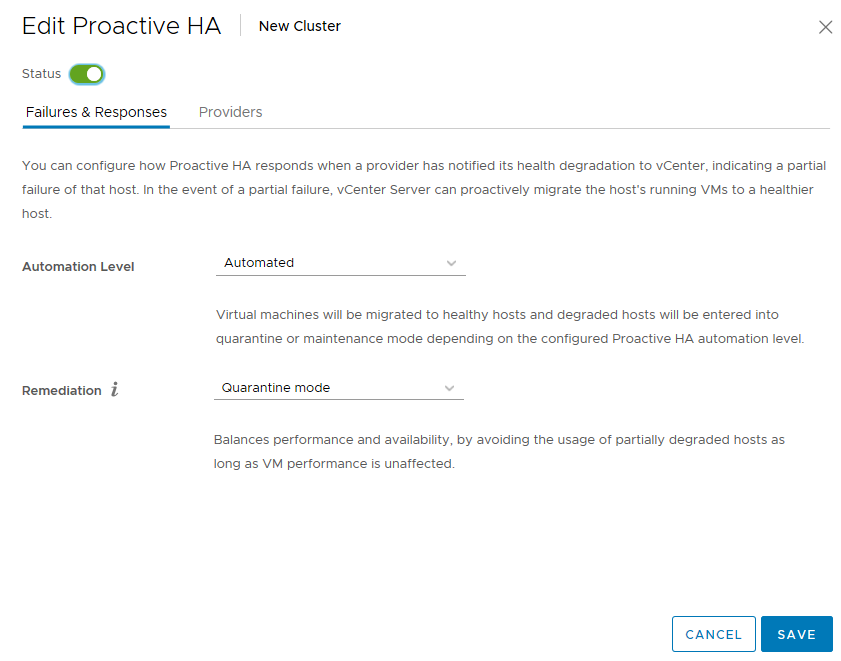
1. Enable **vSphere HA** and **Enable Host Monitoring**, and click **OK**.

* Enable Proactive HA

1. Click **Edit** on the right of **Proactive HA is not available**.

The **Edit Proactive HA** page is displayed, as shown in Figure 5-71.

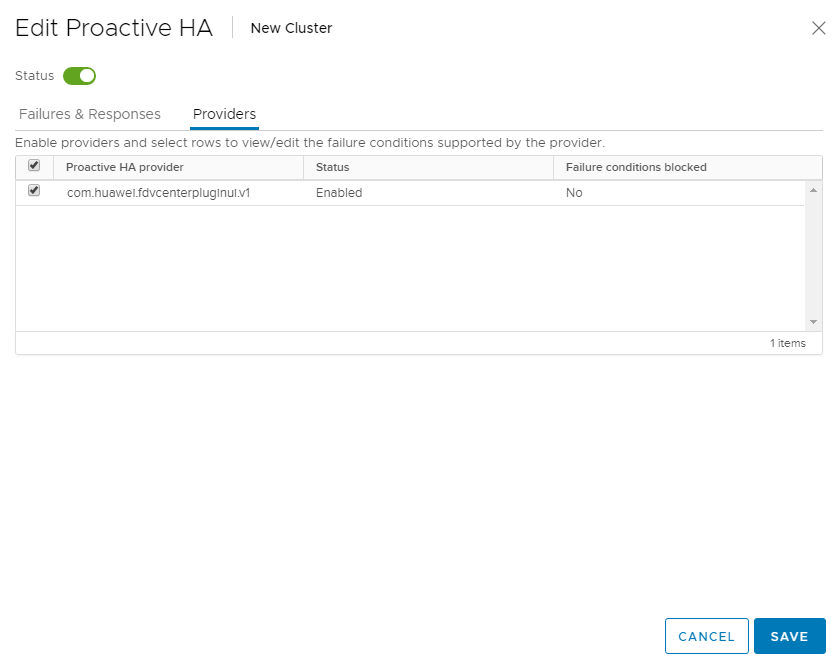
Editing Proactive HA



1. Enable **Status**.
2. Click **Failure & Responses**, and set **Automation Level** and **Remediation** as required.
3. Click **Providers**.

The **Providers** tab page is displayed, as shown in Figure 5-72.

Editing providers



1. Select **com.huawei.fdvcenterpluginui.v1** provided by the Huawei FusionDirector Integrator for VMware vCenter plug-in and click **Save**.

Proactive HA is configured.

----End

#### Using Proactive HA

On the vCenter WebUI, choose **Menu**> **Hosts and Clusters**.

The **Hosts and Clusters** page is displayed.

Choose Datacenter > *Cluster* > *Host*.

The host page is displayed, as shown in Figure 5-73.

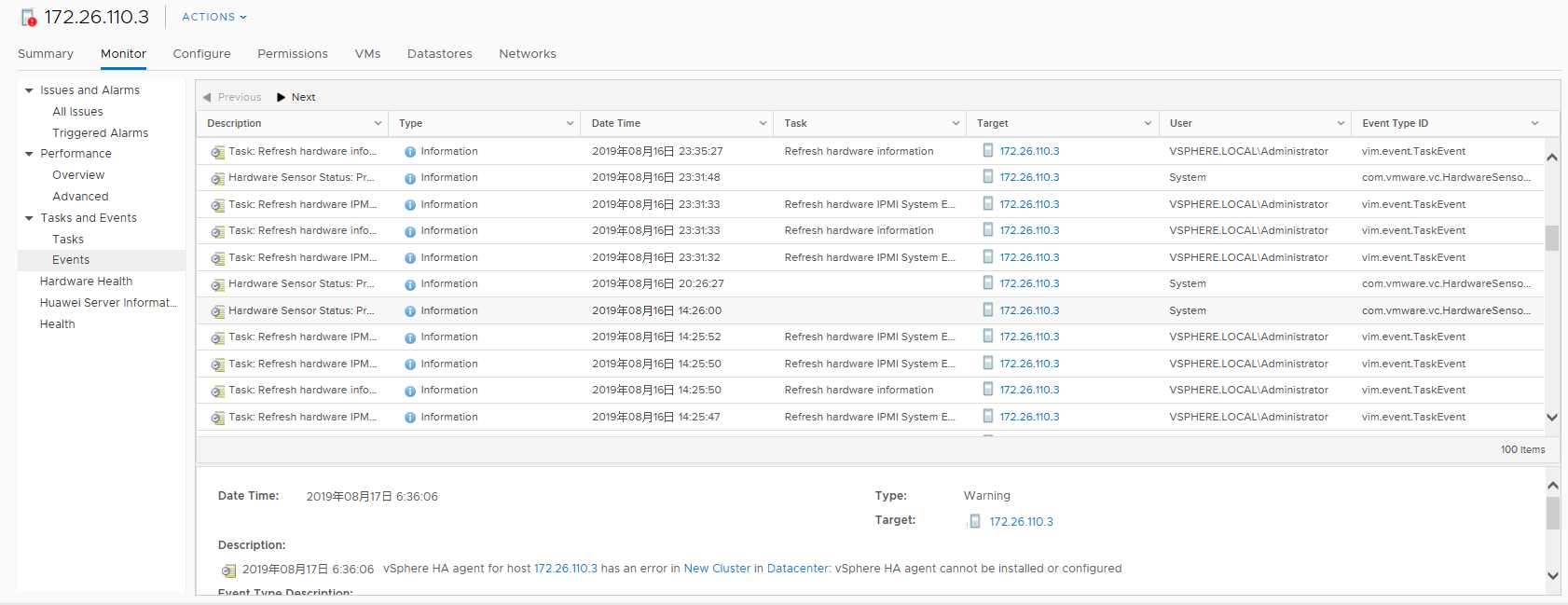
Host



Choose **Monitor** > **Tasks and Events** > **Events**.

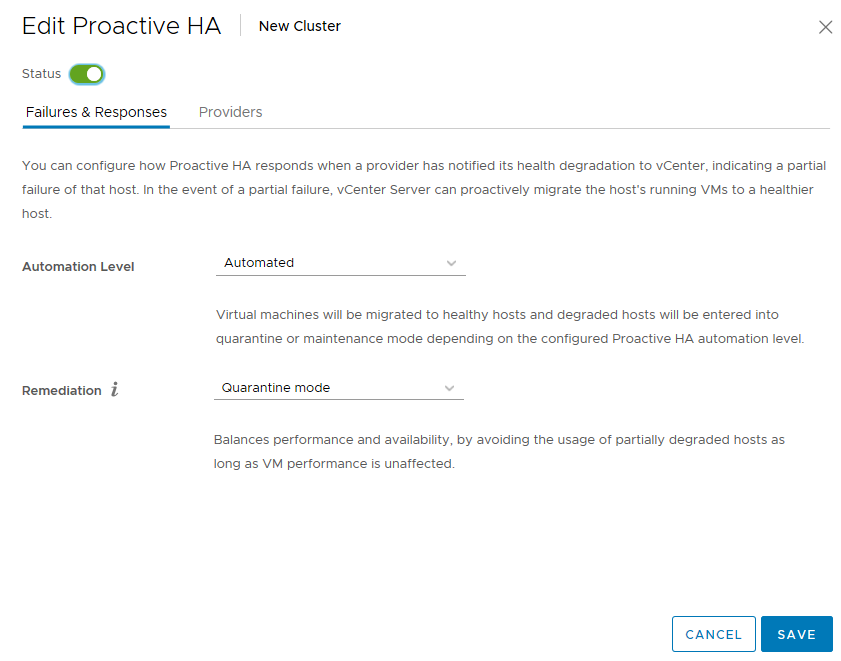
The **Events** page is displayed, as shown in Figure 5-74. You can view the alarms pushed by HA Provider. The alarm description is started with com.huawei.fdvcenterpluginui.v1.

Events



If **Automation Level** and **Remediation** in [Step 3.3](#li179901119135714) of 5.5.5.2 Configuring Proactive HA are set to **Automated** and **Quarantine mode** respectively, as shown in Figure 5-75, vCenter isolates the host when the alarm pushed by the HA Provider is severely degraded.

Configuring Proactive HA



----End

### Viewing Server Alarms and Events

The following uses the plug-in in HTML5 mode as an example.

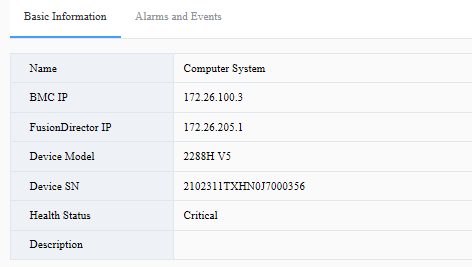
On the vCenter WebUI, choose **Menu**> **Hosts and Clusters**.

The **Hosts and Clusters** page is displayed.

Click the cluster where the target host is located, and choose **Monitor** > **Huawei Server Information**.

The Huawei server information page is displayed, as shown in Figure 5-76.

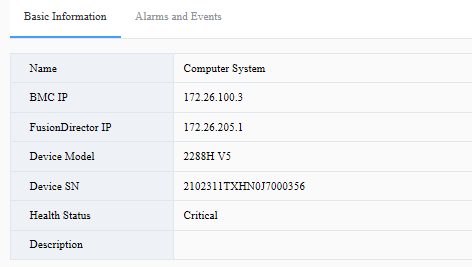
Huawei server information page



Select **Basic Information** or **Alarms and Events** to view the basic information and alarm information about the server where the alarm is generated.

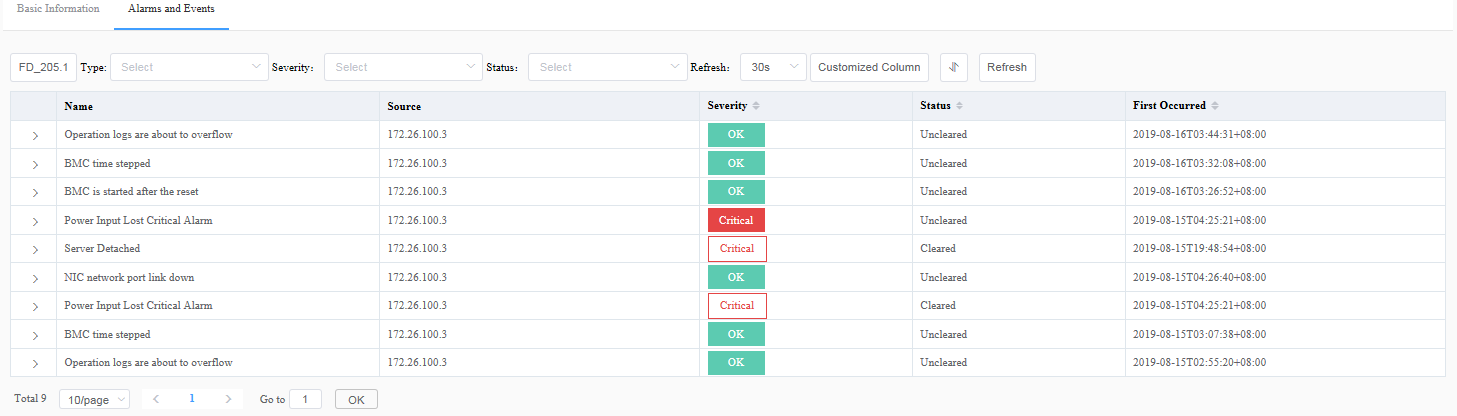
* **Basic Information** page displays the BMC IP address, FusionDirector IP address, device model, serial number, health status, and description of the server, as shown in Figure 5-77.

Basic Information page



* **Alarms and Events** page displays the alarm and event information about the server, as shown in Figure 5-78.

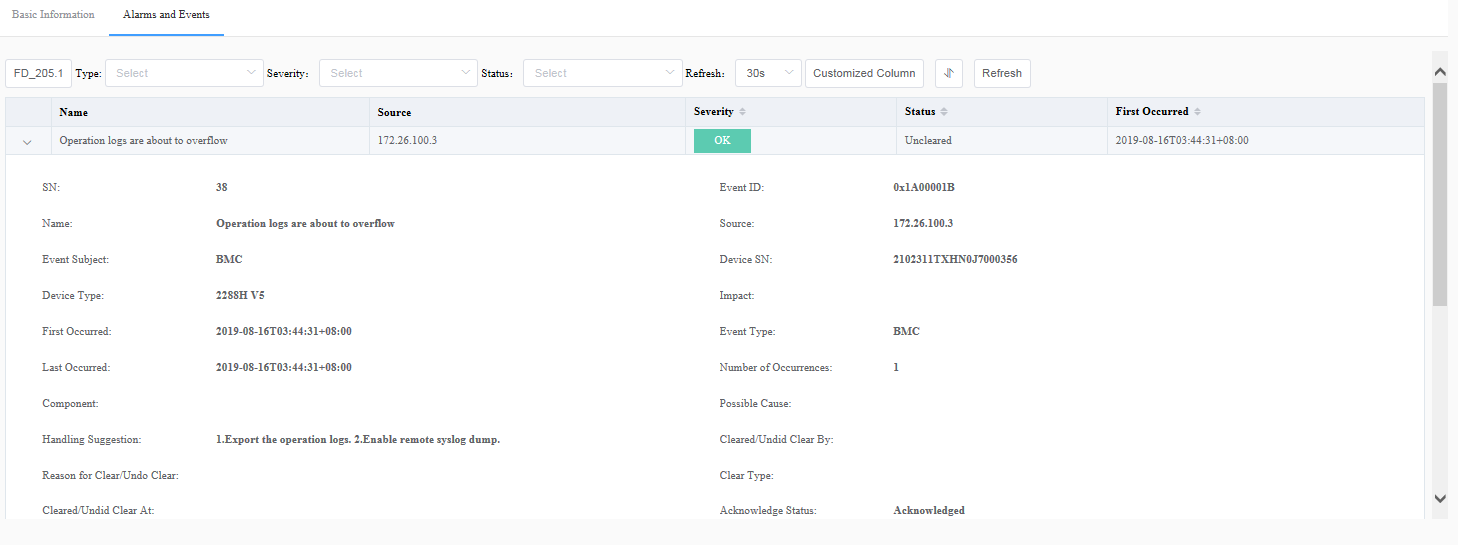
Alarms and Events page



In the alarm and event list, click to view the details about the alarm or event, as shown in Figure 5-79.



Detailed event or alarm information



In the row shown in Figure 5-80, you can set the display of alarms and events. For details, see Table 5-18.

Setting alarm display



Setting alarm display

| Option | Description |
| --- | --- |
| Type | Indicates the type of alarms to be displayed. The options are as follows:   * All * Current Alarm * Historical Alarm * Event * Masked Alarms and Events   NOTE  If no option is selected, the alarms of all types are displayed. |
| Severity | Indicates the severity of alarms to be displayed. The options are as follows:   * All * Warning * Critical   NOTE  If no option is selected, the alarms of all severity are displayed. |
| Status | Indicates the status of alarms to be displayed. The options are as follows:   * All * Cleared * Uncleared   NOTE  If no option is selected, the alarms in all status are displayed. |
| Refresh | Indicates the interval for refreshing the alarm and event list. The default value is **30s**. |
| Customized Column | You can set the columns to be displayed in the alarm and event list.  Click **Customized Column**. In the displayed **Select Column** dialog box, select the alarm information to be displayed and click **OK**. |
|  | Click . In the displayed **Sort** dialog box, set the sorting mode and click **OK**.   * You can set **First Sort Field**, **Second Sort Field**, and **Third Sort Field**. * You can select **Ascending** or **Descending** for each sort. * You must set the sorts in sequence. |

----End

# Other Functions of FDIVV

[6.1 System Operations](#_EN-US_TOPIC_0184730422)

[6.2 Logging Out](#_EN-US_TOPIC_0184730490)

[6.3 Changing the Login Password](#_EN-US_TOPIC_0184730352)

[6.4 Certificate Management](#_EN-US_TOPIC_0184730372)

## System Operations

The **System Operations** tab provides the following options: **Set Session**, **Download Log**, **Shut Down**, and **Restart**.

### Set Session



Modifying session parameters will cause the service to restart. Exercise caution when performing this operation.

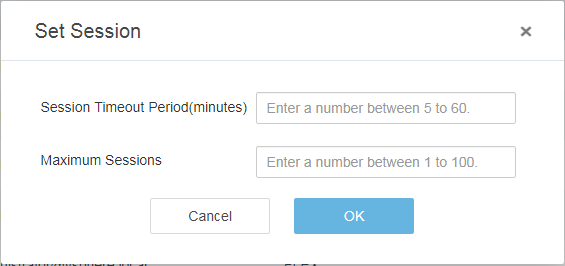
Click **System Operations**.

The user shortcut operation box is displayed.

Click **Set Session**.

The **Set Session** dialog box is displayed, as shown in Figure 6-1.

Set Session dialog box



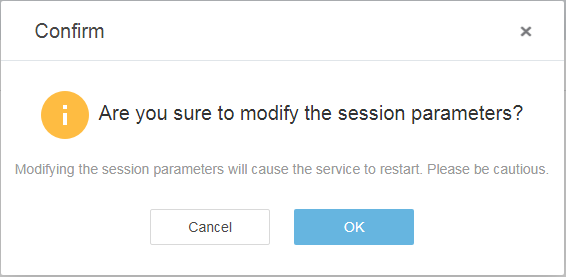
Set the following parameters:

* **Session Timeout Period(minutes)**: If you do not perform any operation within a specified period after login, the account is automatically logged out. The value ranges from 5 to 60 (in minutes). The default value is **5**.
* **Maximum Sessions**: specifies the maximum number of concurrent sessions in the system. The value ranges from 1 to 100. The default value is **100**.

Click **OK**.

The **Confirm** dialog box is displayed, as shown in Figure 6-2.

Confirm dialog box



Click **OK**.

The service restarts automatically, and the session parameter setting is complete.

----End

### Downloading Logs

Procedure

Click **System Operations**.

The user shortcut operation box is displayed.

Click **Download Log**.

The log file starts to be downloaded to the default path on the local PC.

----End

Log File Description

Table 6-1 describes the downloaded log files.

Description of downloaded log files

| File Name | Description |
| --- | --- |
| itergarator.log | FDIVV run log |
| javacore.txt | FDIVV thread information |
| systemLog.zip | System operation log |

### Shutting Down the VM



If FDIVV is shut down, all FusionDirector for vCenter plug-ins cannot work properly. Exercise caution when performing this operation.

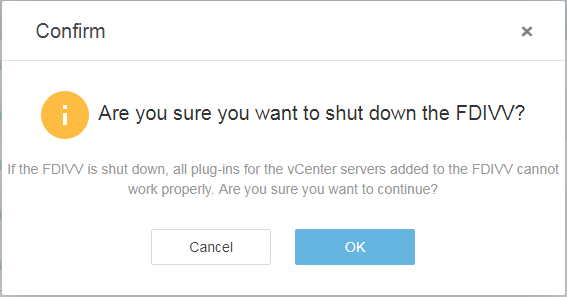
Click **System Operations**.

The user shortcut operation box is displayed.

Click **Shut Down**.

The **Confirm** dialog box is displayed, as shown in Figure 6-3.

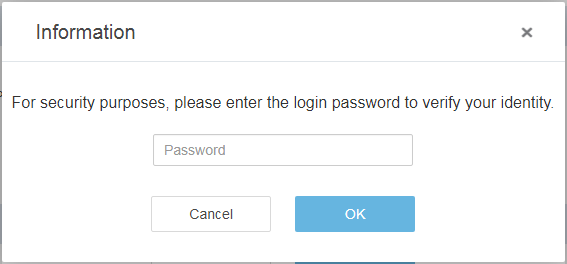
Confirm dialog box



Click **OK**.

The **Information** dialog box is displayed, as shown in Figure 6-4.

Information dialog box



Enter the login password and click **OK**.

The VM starts to be shut down.

----End

### Restarting the VM



Restarting FDIVV will disconnect the current connection. Exercise caution when performing this operation.

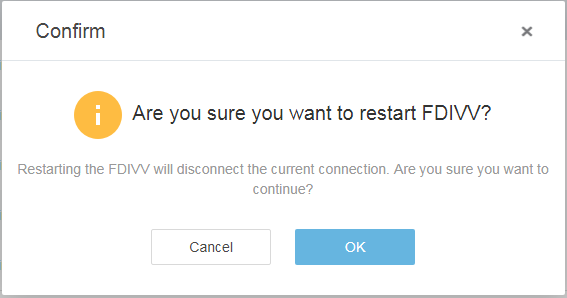
Click **System Operations**.

The user shortcut operation box is displayed.

Click **Restart**.

The **Confirm** dialog box is displayed, as shown in Figure 6-5.

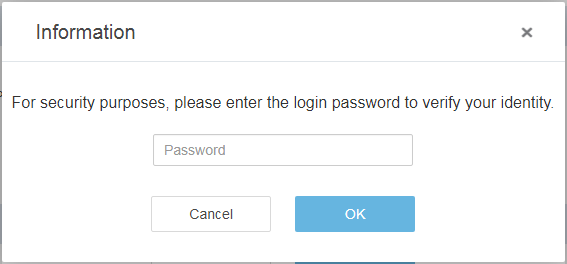
Confirm dialog box



Click **OK**.

The **Information** dialog box is displayed, as shown in Figure 6-6.

Information dialog box



Enter the login password and click **OK**.

The VM starts to be restarted.

----End

## Logging Out

Click .

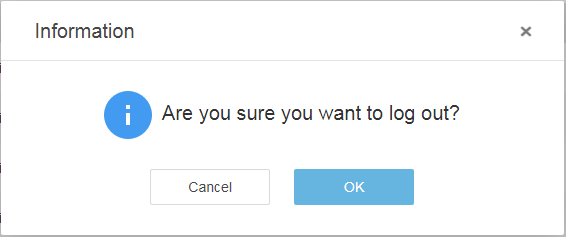


The user shortcut operation box is displayed.

Click **Exit**.

The **Information** dialog box is displayed, as shown in Figure 6-7.

Information dialog box



Click **OK**.

The FDIVV login page is displayed.

----End

## Changing the Login Password

Click .

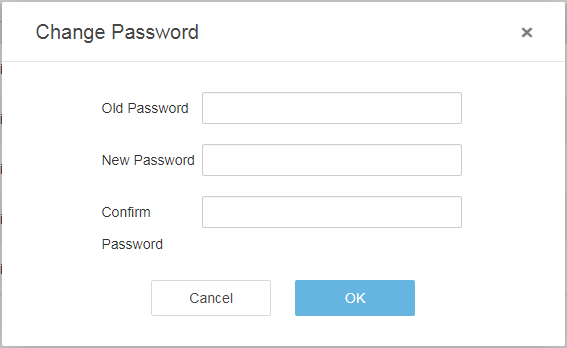


The user shortcut operation box is displayed.

Click **Change Password**.

The **Change Password** dialog box is displayed, as shown in Figure 6-8.

Change Password dialog box



Enter the parameters.



The password is a string of 8 to 32 characters and must contain uppercase letters, lowercase letters, digits, and special characters.

Click **OK**.

The password is changed.

----End

## Certificate Management

On the FDIVV WebUI, choose **Certificate Management**. The **Certificate Management** page is displayed, where you can manage the server certificate, vCenter server certificates, and FusionDirector certificates.

### Server Certificate

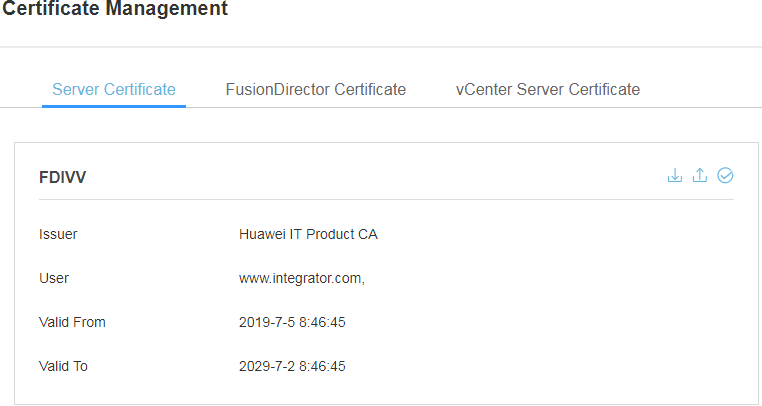
Viewing the FDIVV Certificate

On the FDIVV WebUI, choose **Certificate Management**. The **Certificate Management** page is displayed.

Click **Server Certificate**. The **Server Certificate** tab page is displayed.

You can view the issuer, user, and validity period of the FDIVV certificate, as shown in Figure 6-9.

Viewing the FDIVV certificate



----End

Exporting the FDIVV Certificate

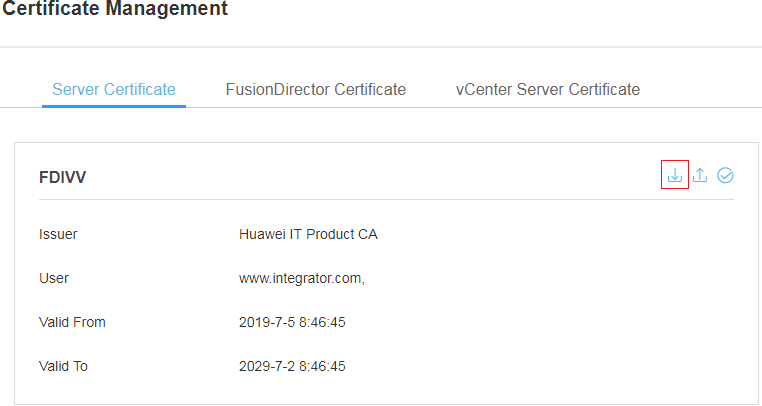
On the FDIVV WebUI, choose **Certificate Management**. The **Certificate Management** page is displayed.

Choose **Server Certificate**. The FDIVV certificate page is displayed.

Click in the upper right corner to export the FDIVV certificate, as shown in Figure 6-10.



Exporting the FDIVV certificate



----End

Importing the FDIVV Certificate

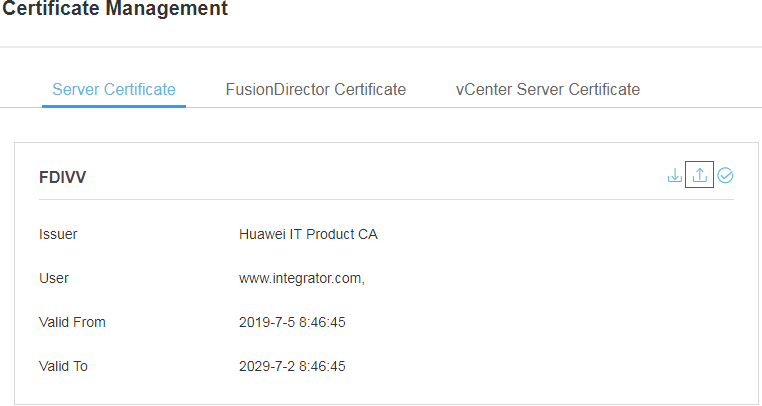
On the FDIVV WebUI, choose **Certificate Management**. The **Certificate Management** page is displayed.

Choose **Server Certificate**. The FDIVV certificate page is displayed.

Click in the upper right corner, as shown in Figure 6-11.

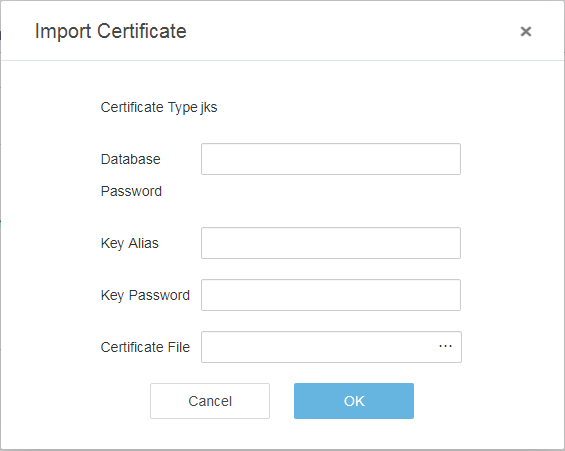


Importing the FDIVV certificate



The **Import Certificate** dialog box is displayed, as shown in Figure 6-12.

Import Certificate dialog box



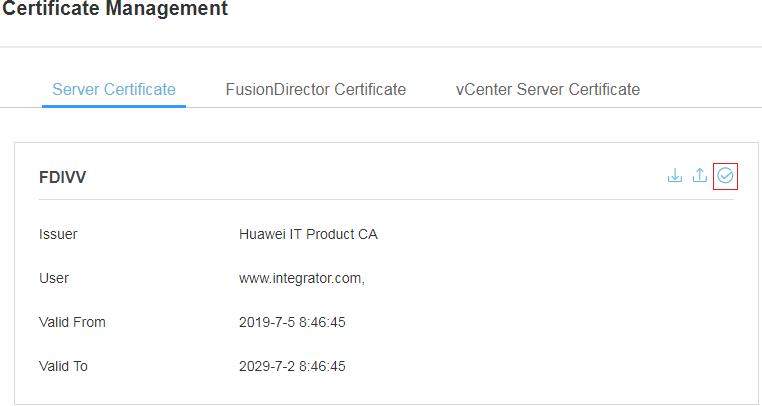
Enter the parameters and click **OK**.

The certificate is imported.

Click in the upper right corner to make the certificate take effect, as shown in Figure 6-13.



Validating the certificate



----End

### FusionDirector Certificate

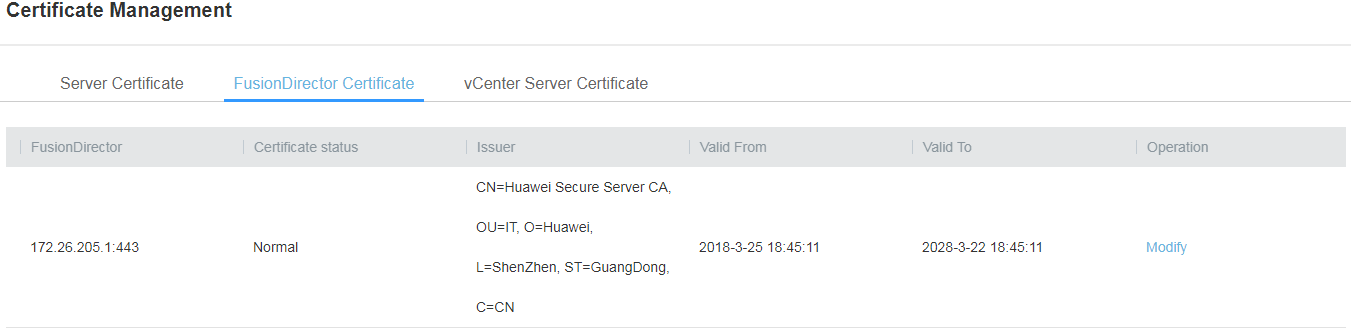
Viewing FusionDirector Certificates

On the FDIVV WebUI, choose **Certificate Management**. The **Certificate Management** page is displayed.

Click **FusionDirector Certificate**. The **FusionDirector Certificate** page is displayed.

You can view the IP address, status, issuer, and validity period of each FusionDirector certificate, as shown in Figure 6-14.

Viewing FusionDirector certificates



----End

Modifying a FusionDirector Certificate

On the FDIVV WebUI, choose **Certificate Management**. The **Certificate Management** page is displayed.

Click **FusionDirector Certificate**. The **FusionDirector Certificate** page is displayed.

Click **Modify** in the **Operation** column of the FusionDirector certificate to be modified.

The **Open** dialog box is displayed.

In the **Open** dialog box, select the required certificate and click **Open**.

The FusionDirector certificate is modified.

----End

### vCenter Server Certificate

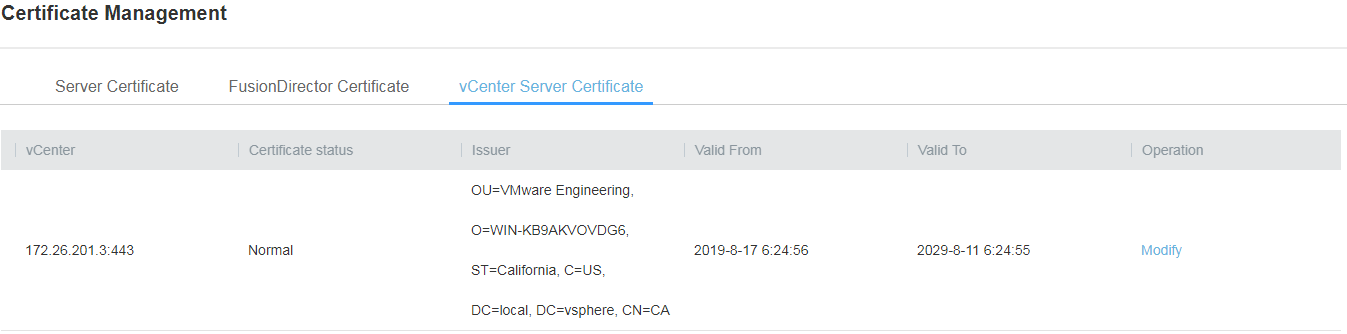
Viewing vCenter Certificates

Choose **Certificate Management**. The **Certificate Management** page is displayed.

Click **vCenter Server Certificate**. The **vCenter Server Certificate** tab page is displayed.

You can view the IP address, status, issuer, and validity period of each vCenter server certificate, as shown in Figure 6-15.

Viewing vCenter certificates



----End

Modifying a vCenter Certificate

On the FDIVV WebUI, choose **Certificate Management**. The **Certificate Management** page is displayed.

Click **vCenter Server Certificate**. The **vCenter Server Certificate** tab page is displayed.

Click **Modify** in the **Operation** column of the vCenter server certificate to be modified.

The **Open** dialog box is displayed.

In the **Open** dialog box, select the required certificate and click **Open**.

The vCenter server certificate is modified.

----End

# FAQs

[7.1 How to Add a Server ESXi System to a vCenter Cluster](#_EN-US_TOPIC_0184730478)

[7.2 FusionDirector for vCenter Icon Is Not Displayed on the vCenter Shortcuts Page](#_EN-US_TOPIC_0184730350)

[7.3 How to Change the Default Password Used for the Communication Between the FusionDirector for vCenter Plug-in and FDIVV](#_EN-US_TOPIC_0231584030)

## How to Add a Server ESXi System to a vCenter Cluster

On the vCenter WebUI, choose **Menu**> **Hosts and Clusters**.

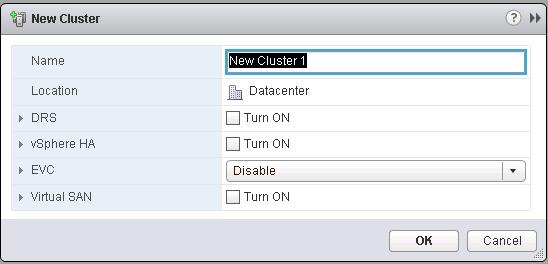
The **Hosts and Clusters** page is displayed.

Choose **Datacenter** from the shortcut menu.

Choose **New Cluster**.

The **New Cluster** page is displayed, as shown in Figure 7-1.

New Cluster page



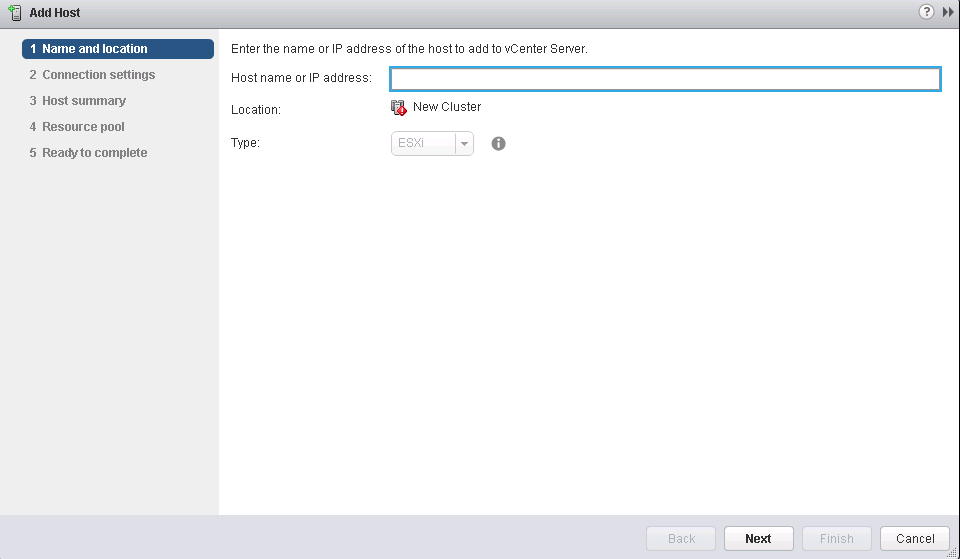
Enter a cluster name in **Name**, and click **OK**.

Right-click the newly created cluster.

Choose **Add Host...**.

The **Add Host** page is displayed, as shown in Figure 7-2.

Add Host page



* On the **Name and location** page, enter the IP address of the server ESXi system.
* On the **Connection settings** page, enter the user name and password of the server ESXi system.

Click **Finish**. The ESXi system is added.

----End

## FusionDirector for vCenter Icon Is Not Displayed on the vCenter Shortcuts Page

### Plug-in Icon Is Not Displayed After I Log In to vCenter Again

Symptom

The FusionDirector for vCenter plug-in is successfully installed. After you log in to vCenter again, the **FusionDirector For vCenter** icon is not displayed on the **Shortcuts** page.

Solution

Check whether a firewall is enabled in the system where the plug-in deployment program is located.

* If the firewall is enabled, disable the firewall.
* If the firewall is disabled, go to [Step 2](#d0e9007).

Restart the vCenter service.

* Restart vCenter on Windows
  1. Access the Windows CLI.
  2. Run the following command to stop the vCenter service:

"C:\Program Files\VMware\vCenter Server\bin\service-control.bat" --stop --all

* 1. Run the following command to start the vCenter service:

"C:\Program Files\VMware\vCenter Server\bin\service-control.bat" --start --all

* Restart vCenter on Linux
  1. Access the Linux CLI as user **root** using the SSH tool.
  2. Run the following command to stop the vCenter service:

service-control --stop --all

* 1. Run the following command to start the vCenter service:

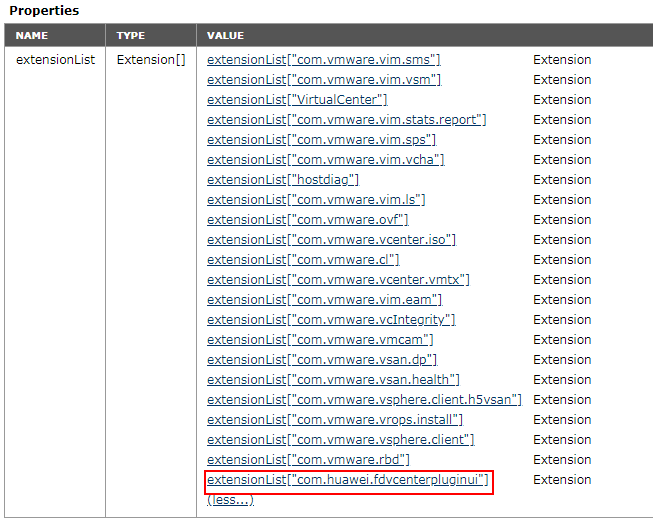
service-control --start --all

Check whether the **FusionDirector for vCenter** icon is displayed on the **Shortcuts** page.

* If the icon is displayed, no further action is required.
* If the icon is not displayed, go to [Step 4](#li81809502184).

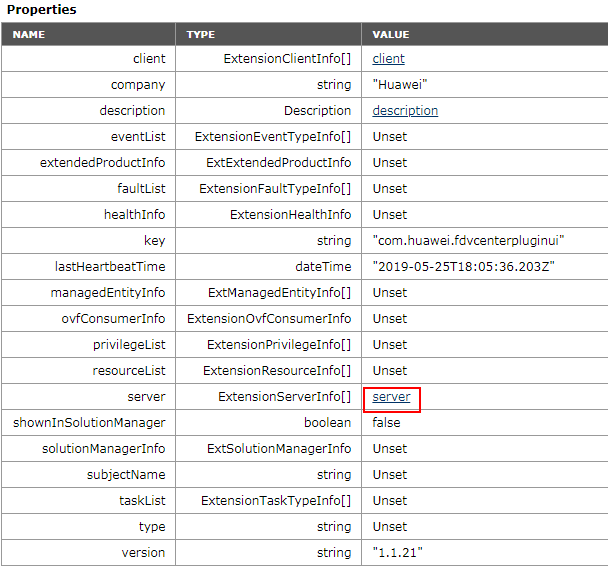
Log in to https://*vCenter IP address*/mob/?moid=ExtensionManager and view the vCenter server information, as shown in Figure 7-3.

vCenter server information



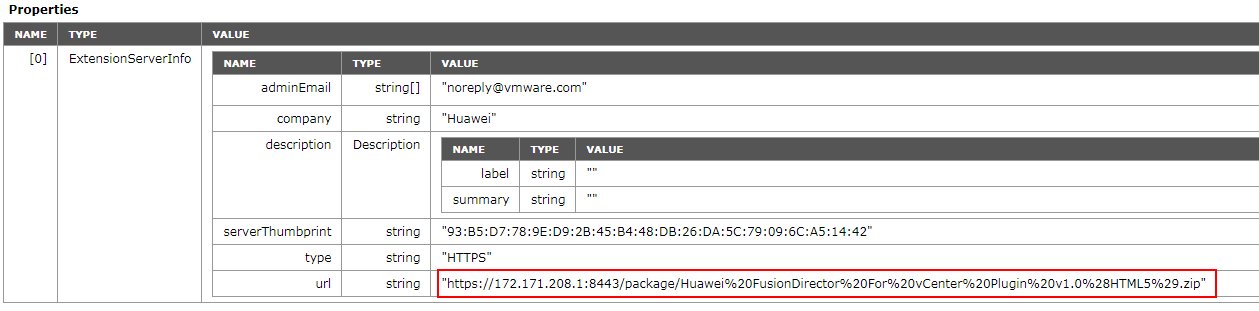
Click **com.huawei.fdvcenterpluginui** to view the plug-in information, as shown in Figure 7-4.

Plug-in information



Click **server** to view the detailed information about the **server** field, as shown in Figure 7-5.

Information of the server field



Check whether the IP address can be connected to vCenter.

* If the connection is normal, go to [Step 8](#li717615498548).
* If the connection is abnormal, modify the network configuration until the IP address is connected to vCenter, and go to [Step 8](#li717615498548).

Reinstall the plug-in.

1. Uninstall the plug-in. For details, see 4.3.3 Deleting a vCenter Server.
2. Install the plug-in. For details, see 4.3.1 Adding a vCenter Server.
3. Log in to vCenter to view the plug-in icon.

----End

### Plug-in Icon Is Not Displayed After the vCenter Server Is Deleted and Added Again

Symptom

After the vCenter server is deleted and added again, the **FusionDirector for vCenter** icon is not displayed on the **Shortcuts** page after you log in to vCenter again.

Solution

Clear the browser cache.

Google Chrome is used as an example.

1. Click in the upper right corner of the browser.

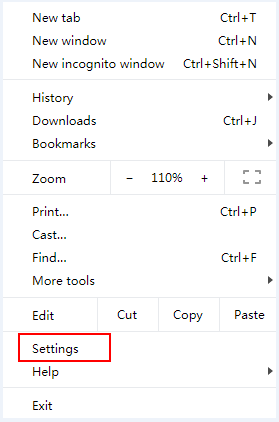


The shortcut operation box is displayed.

1. Choose **Settings**, as shown in Figure 7-6.

The **Settings** page is displayed.

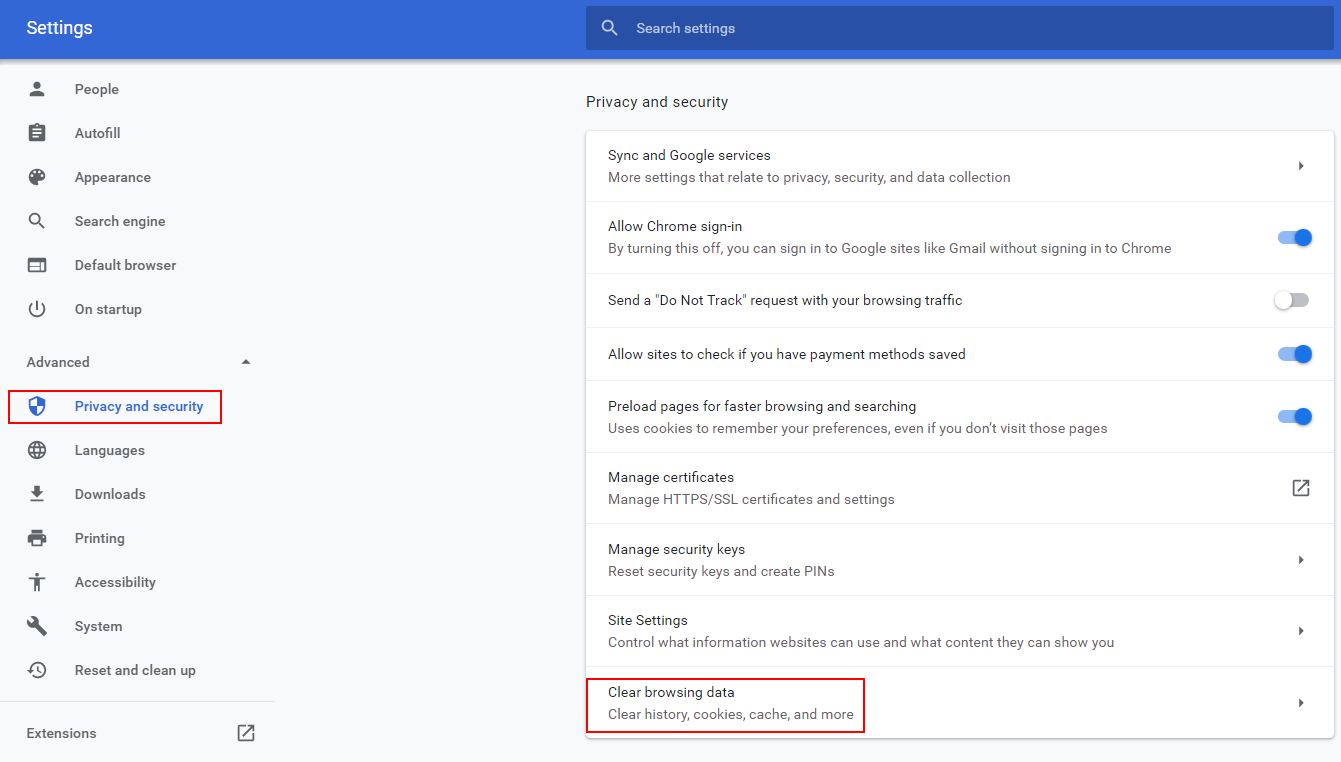
Shortcut operation box



1. Choose **Privacy and security** > **Clear browsing data**, as shown in Figure 7-7.

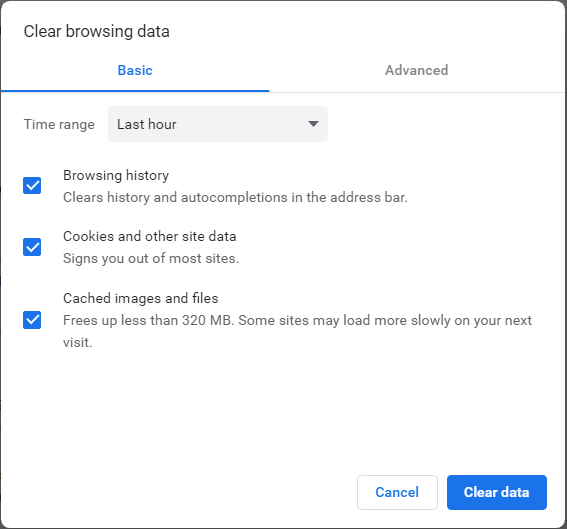
The **Clear browsing data** dialog box is displayed.

Settings page

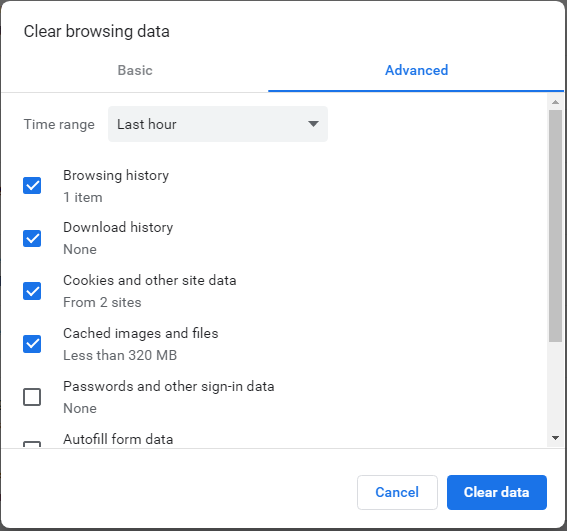


1. In the **Clear browsing data** dialog box, select the data to be cleared on the **Basic** and **Advanced** tab pages, as shown in Figure 7-8 and Figure 7-9.

Basic tab page



Advanced tab page



1. Click **Clear data**.

The cache is cleared.

Restart the vCenter service.

* Restart vCenter on Windows
  1. Access the Windows CLI.
  2. Run the following command to stop the vCenter service:

"C:\Program Files\VMware\vCenter Server\bin\service-control.bat" --stop --all

* 1. Run the following command to start the vCenter service:

"C:\Program Files\VMware\vCenter Server\bin\service-control.bat" --start --all

* Restart vCenter on Linux
  1. Access the Linux CLI as user **root** using the SSH tool.
  2. Run the following command to stop the vCenter service:

service-control --stop --all

* 1. Run the following command to start the vCenter service:

service-control --start --all

Log in to vCenter to view the plug-in icon.

----End

## How to Change the Default Password Used for the Communication Between the FusionDirector for vCenter Plug-in and FDIVV

Prerequisites

The Postman software has been installed.



Postman is third-party software and needs to be prepared by the customer.

Procedure

Open Postman.

Logging In to the FDIVV WebUI

1. Enter **https://***XXX.XXX.XXX.XXX***/SessionService/Login** in the URL text box and press **Enter**, as shown in Figure 7-10.



*XXX.XXX.XXX.XXX* indicates the IP address (same as the configured FDIVV IP address) or DNS domain name for accessing the FDIVV WebUI.

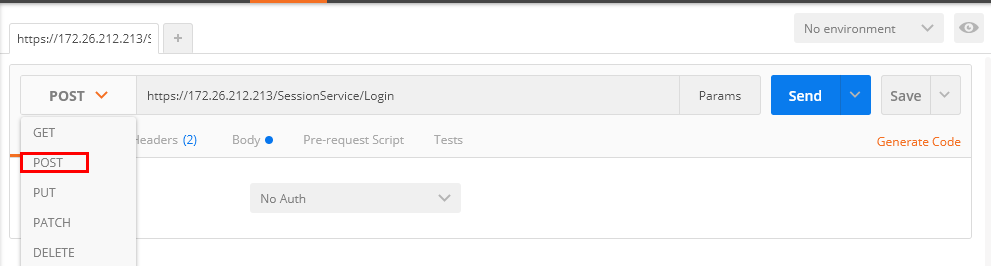
Entering a URL



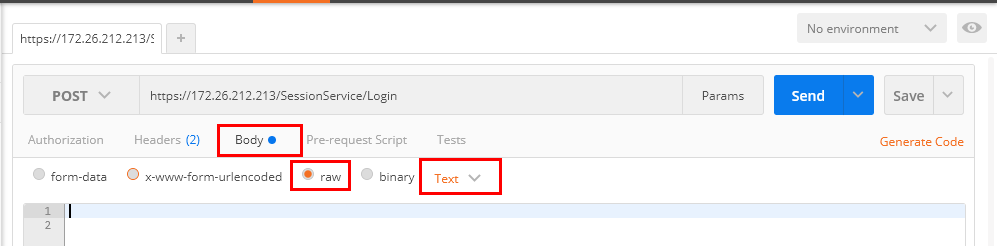
1. Determine the operation to be performed.

Select **POST** from the operation type drop-down list on the left of the URL text box, as shown in Figure 7-11.

Determining the operation to be performed



1. Click the **Body** tab, select **raw**, and set the file type to **Text**, as shown in the following figure.



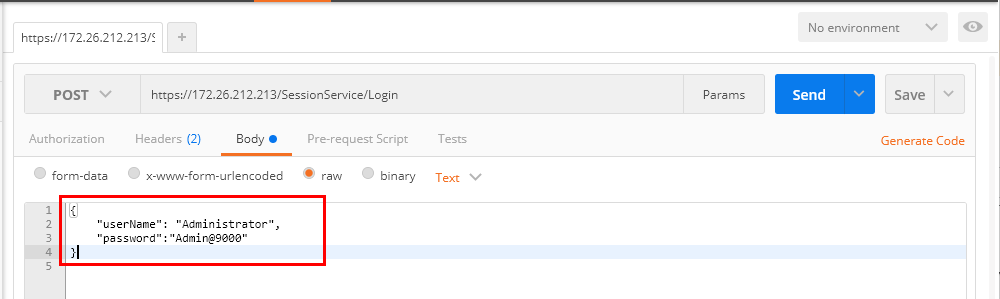
1. Enter the following commands in the command input box, as shown in Figure 7-12.

{   
 "userName": "*xxx*",   
 "password":"*yyy*"   
 }

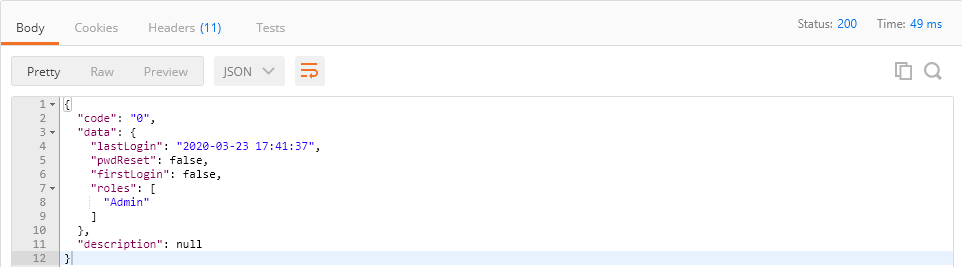
Parameter description:

* **userName**: indicates the user name for logging in to the FDIVV WebUI. The default value is **Administrator**.
* **password**: indicates the password for logging in to the FDIVV WebUI. The default value is **Admin@9000**.

Entering commands



1. Click **Send**. If the following information is displayed, the operation is successful:



Output parameter description:

* **lastLogin**: indicates the last login time.
* **pwdReset**: indicates whether the default password has been reset.
* **firstLogin**: indicates whether it is the first login.
* **roles**: indicates the account type.
* **description**: indicates the error description.

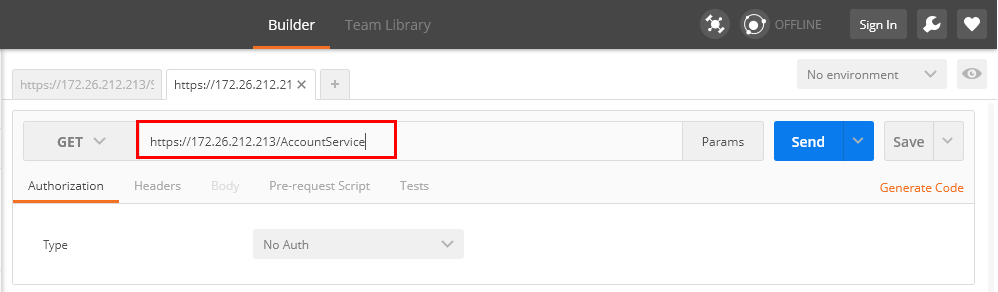
Change the default password used for the communication between the FusionDirector for vCenter plug-in and FDIVV.

1. Click **+** to open a new tab page.
2. Enter **https://***XXX.XXX.XXX.XXX***/AccountService** in the URL text box and press **Enter**, as shown in Figure 7-13.



*XXX.XXX.XXX.XXX* indicates the IP address (same as the configured FDIVV IP address) or DNS domain name for accessing the FDIVV WebUI.

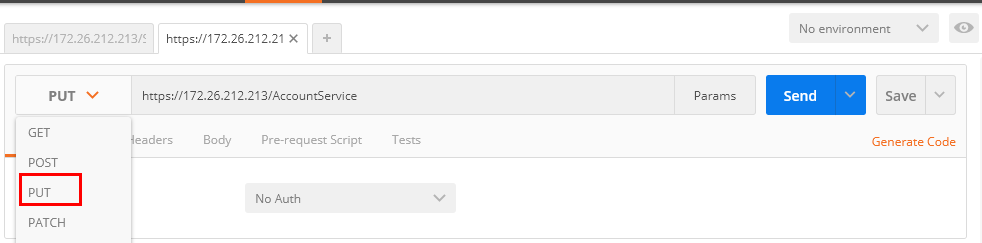
Entering a URL



1. Determine the operation to be performed.

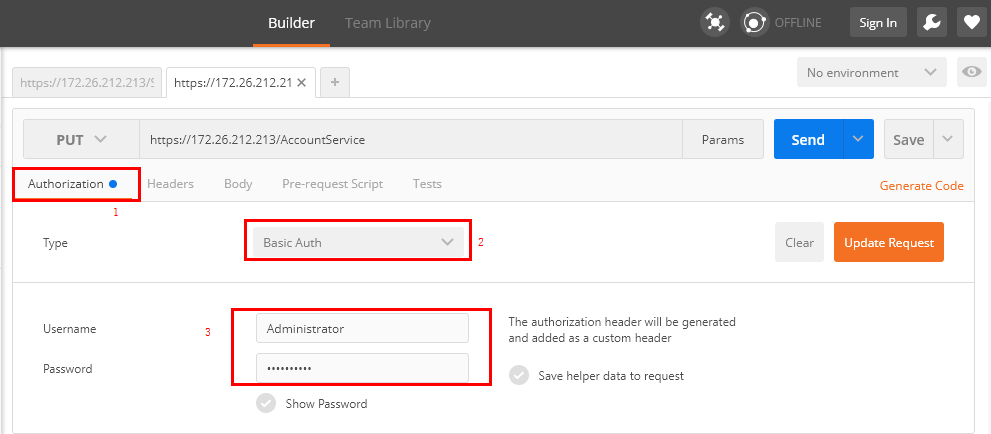
Select **PUT** from the operation type drop-down list on the left of the URL text box, as shown in Figure 7-14.

Determining the operation to be performed



1. Perform basic authorization.
   1. Click the **Authorization** tab and set **Type** to **Basic Auth**, as shown in 1 and 2 in Figure 7-15.

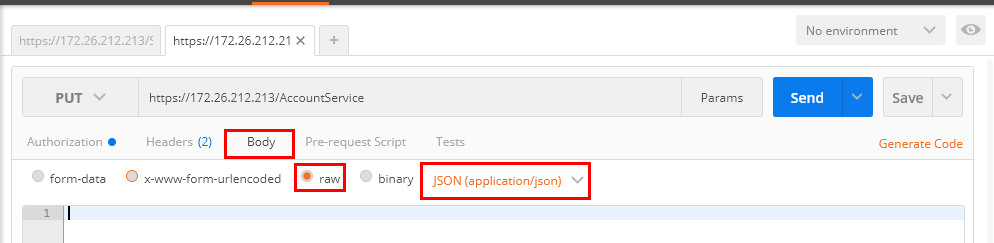
Basic authorization



* 1. Enter the user name (**Administrator** by default) and password (**Admin@9000** by default) for logging in to the FDIVV WebUI, as shown in 3 in Figure 7-15.
  2. Click **Update Request**.

The basic authorization is complete.

1. Click the **Body** tab, select **raw**, and set the file type to **JSON (application/json)**, as shown in the following figure.



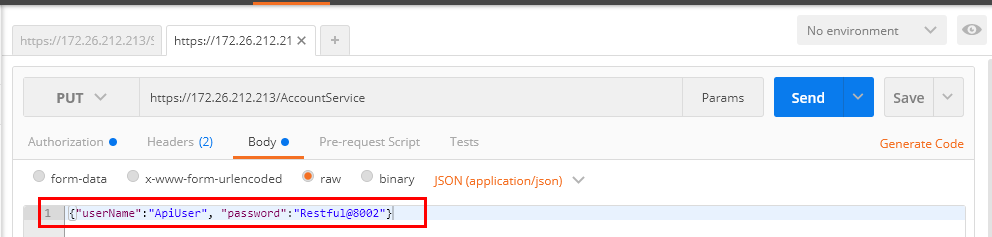
1. Enter the following commands in the command input box, as shown in Figure 7-16.

{"userName":"*xxx*", "password":"*yyy*"}

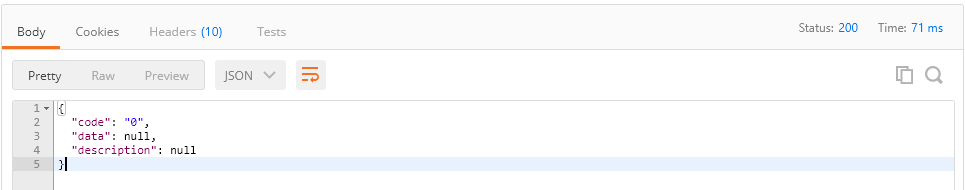
Parameter description:

* **userName**: indicates the user name used for the communication between the FusionDirector for vCenter plug-in and FDIVV. The default value is **ApiUser**.
* **password**: indicates the new password used for the communication between the FusionDirector for vCenter plug-in and FDIVV. The default value is **Restful@8000**.

Entering commands



1. Click **Send**. If the following information is displayed, the password for the communication between the FusionDirector for vCenter plug-in and FDIVV is successfully changed.



Output parameter description:

* **code**: indicates the error code.
* **description**: indicates the error description.

----End