# FusionSphere Lab Guide

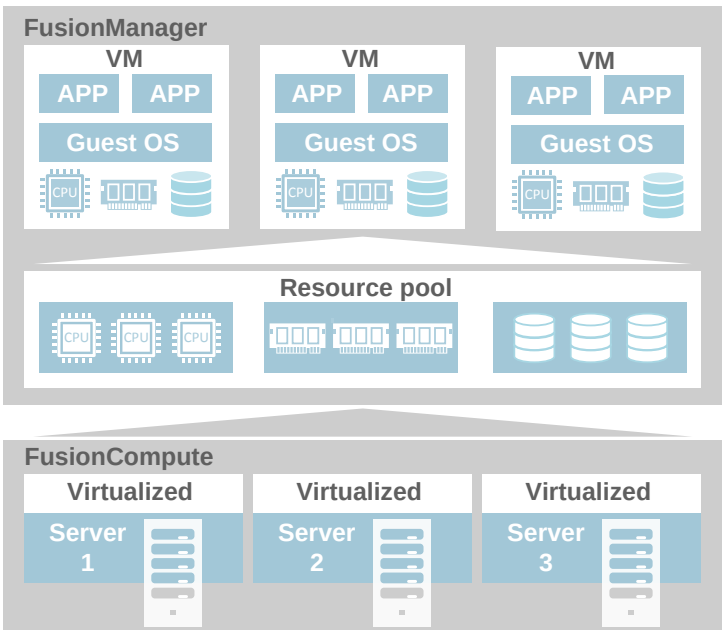
Issue: 01
Date: 2015-07

## Introduction to FusionSphere

The FusionSphere solution consists of the cloud OS software FusionCompute and cloud management software FusionManager.

- FusionCompute is deployed on physical servers to virtualize the server hardware resources, including CPUs, memory, and network interface cards (NICs).
- FusionManager schedules and manages computing, network, and storage resources in the underlying resource pools in a centralized manner. On FusionManager, users can create VMs for tenants, allocate resources for the VMs, and manage the VMs based on the service requirements.

FusionSphere improves hardware resource utilization, shortens the service launch period, simplifies maintenance, and reduces the maintenance costs.




## Objectives

This document illustrates how to quickly install and configure FusionSphere and provision services using FusionSphere. There are some tasks label as optional, which means trainees can skip this task. However, the instructor must prepare those tasks earlier.

# 1 Background

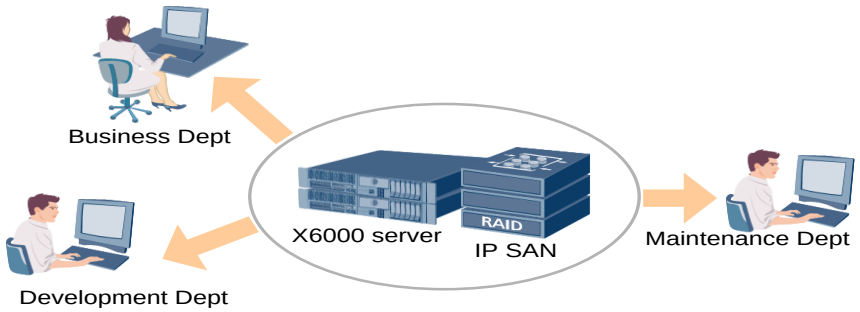
Resource utilization of traditional servers is mostly 5% to 25%, which swells a company's operating expenditure with the increase of servers required by the growing services of the company. This is a common problem challenging most companies nowadays.

Using virtualization technologies, FusionSphere enables one physical server to function as multiple or even hundreds of isolated virtual servers providing the same functions as a traditional server. Besides, FusionSphere is able to pool and dynamically manage the CPU, memory, disk, and NIC resources of these virtual servers in a centralized manner, thereby improving resource utilization and helping companies reduce hardware investment costs as well as operating expenditures.

**Example Scenario**

Company A has three departments: Business, Development, and Maintenance. Business Department is responsible for product sales; Development Department is responsible for product development; and Maintenance Department is responsible for after-sales services.

The company has an X6000 server and an IP SAN storage device deployed in the equipment room to support services of all these three departments.




With the growth of services, the three departments apply for new servers to handle new services. The server requirements of the three departments are as follows.

| Department | Server Requirements |
|---|---|
| Business Dept | One server to deploy a website system for showcasing products and handling online orders. The server is required to be accessible to public network users. |
| Development Dept | • One server to deploy databases<br>• One server to serve as the file server |
| Maintenance Dept | One server to serve as the file server |

The Company A is facing the following problems:

- Resource utilization of the existing servers is low, while purchasing new servers requires additional capital investment.
- Servers, storage devices, and switches cannot be managed in a centralized manner, resulting in slow service response and low maintenance efficiency.

Therefore, Company A expects to optimize service deployment of its three departments by improving the resource utilization of its existing servers.

FusionSphere is able to virtualize physical resources to enable a physical server to run multiple VMs that carry different servers. This solution improves the server utilization and reduces the hardware investment cost. Moreover, FusionSphere is able to manage both physical and virtual resources to improve the company's maintenance efficiency and service response capability.

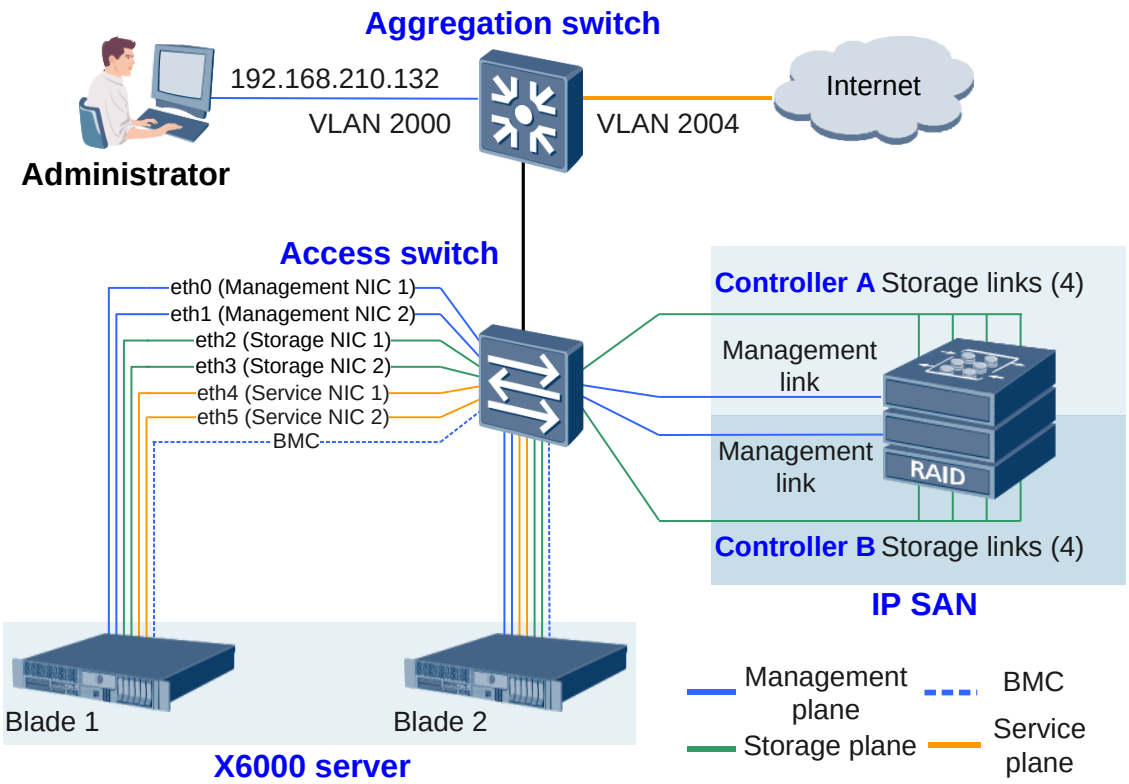
Next, we are going to show how to deploy FusionSphere on Company A's existing servers and use FusionSphere to allocate resources and provision service VMs to the company's three core departments.

# 2 Preparations

## 2.1 Deployment Plan

**1. Physical Device Networking**

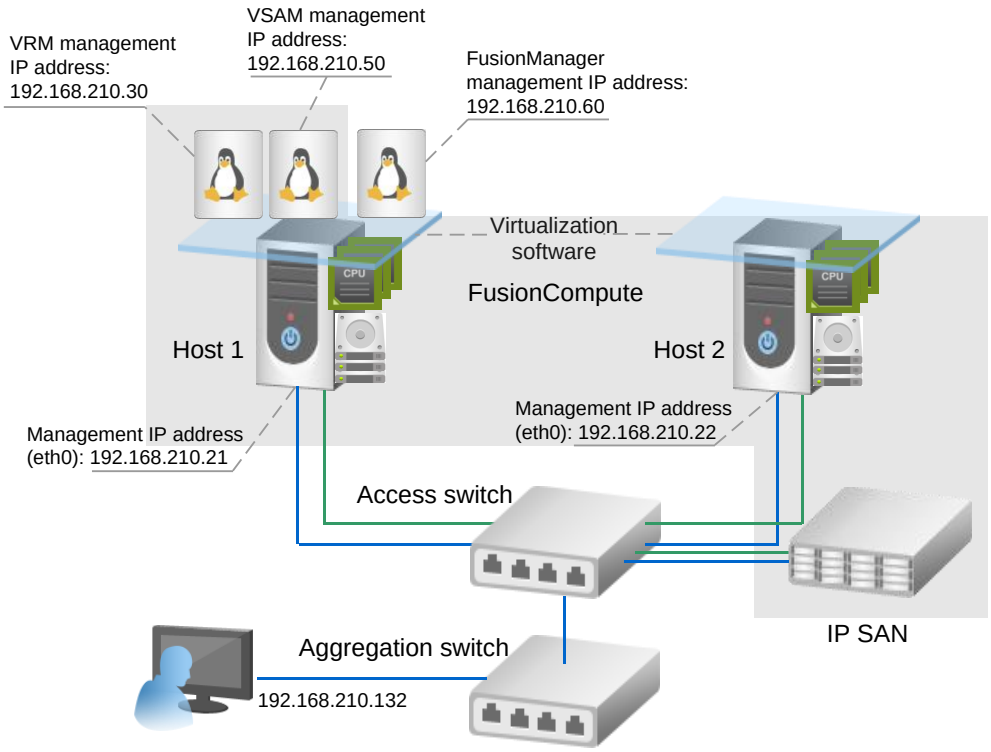
Company A's network devices include an aggregation switch and an access switch. Servers and the IP SAN storage device are connected to the access switch over their network ports to allow data access to the switch from the management, storage, and service planes of the devices.




| Network Plane | Configuration Information | Remarks |
|---|---|---|
| Management plane | VLAN 2000<br>Subnet: 192.168.210.0/24 | The company's management plane network.<br>You can set the host IP addresses and management node IP addresses in the FusionSphere system in the management plane. |
| BMC | VLAN 13<br>Subnet: 192.168.13.0/24 | Server BMC plane, which communicates with the management plane.<br>X6000 blade 1 BMC IP address: 192.168.13.105<br>X6000 blade 2 BMC IP address: 192.168.13.106 |
| Storage planes | Network segments, VLANs, and subnet masks applicable to the storage planes:<br>172.20.0.0 – VLAN 4 – 255.255.0.0<br>172.30.0.0 – VLAN 5 – 255.255.0.0<br>172.40.0.0 – VLAN 6 – 255.255.0.0<br>172.50.0.0 – VLAN 7 – 255.255.0.0 | The storage IP addresses on the four storage planes are:<br>172.20.100.100<br>172.30.100.100<br>172.40.100.100<br>172.50.100.100 |
| Service planes | 2004~2019 | • Subnet 192.168.214.0/24 under VLAN 2004 can directly connect to the Internet.<br>• VLANs 2011 to 2019 can be used for service provisioning. |

## 2. Installation Plan Description

Install FusionCompute virtualization software on the servers in the system so the servers become hosts providing virtual resources in the FusionCompute hypervisor. Then, install the FusionSphere management components, including Virtualization Resource Management (VRM), Virtual Service Appliance Management (VSAM), and FusionManager on Host 1, as shown in the following figure.




| Component | Description | Data Plan |
|---|---|---|
| Host | Two blades in the X6000 server function as two hosts in the FusionCompute hypervisor after having the FusionCompute software installed. | ● Host 1<br>✓ Name: Host01<br>✓ Management IP address: 192.168.210.21<br>✓ **root** user password: Admin@1234<br>● Host 2<br>✓ Name: Host02<br>✓ Management IP address: 192.168.210.22<br>✓ **root** user password: Admin@1234 |
| VRM | Management component in the FusionCompute hypervisor.<br>VRM can be deployed in either standalone or active/standby mode. In this example task, VRM is deployed on only one host (Host01) in standalone mode, and the VRM management IP address is configured to the management plane IP address.<br>📖 **Notes:** In active/standby mode, the management node is deployed on two physical servers or VMs. If the active node is faulty, the system rapidly switches services to the standby node to ensure service continuity. Therefore, the active/standby mode provides high service reliability. | ● Management IP address: 192.168.210.30<br>● Subnet mask: 255.255.255.0<br>● Gateway: 192.168.210.1 |
| FusionManager | Cloud management component, which can be deployed in either standalone or active/standby mode to manage and maintain physical resources, virtual resources, and services in a centralized manner.<br>In this example task, less than 200 VMs are required. Therefore, only one FusionManager node is needed. It is deployed on a VM on Host01, and its management IP address is configured to the management plane IP address. | VM name: FM01<br>Node name: FMN<br>Management IP address: 192.168.210.50<br>Subnet mask: 255.255.255.0<br>Gateway: 192.168.210.1 |

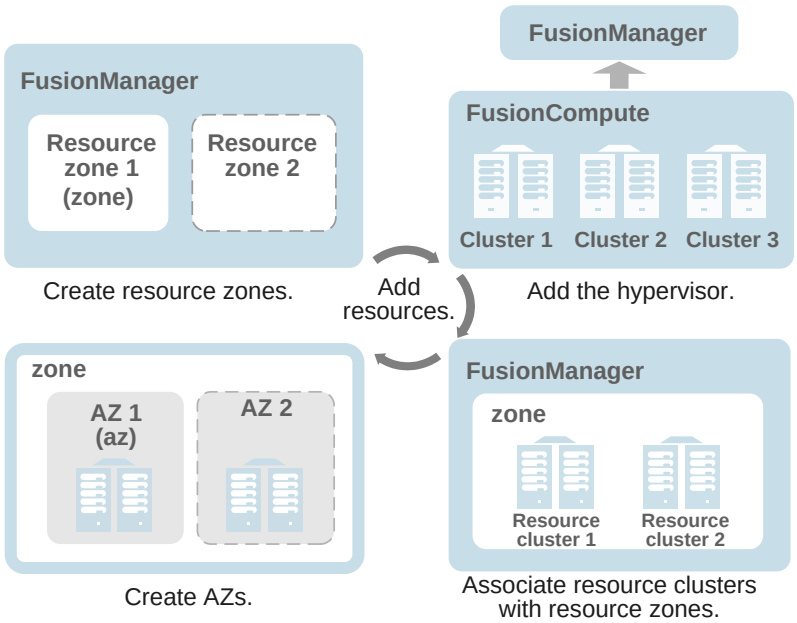
| Component | Description | Data Plan |
| --- | --- | --- |
| VSAM | The Virtual Service Appliance (VSA) management component, which is deployed on a VM to automatically configure and manage system service VMs that provide software router, virtual load balancer (VLB), and Dynamic Host Configuration Protocol (DHCP) functions.<br>After VSAM is deployed in the system, users can apply for software routers, bind a public IP address to a VM, and configure access control list (ACL) rules to improve network access security.<br>In this example task, VSAM is deployed on a single VM on Host01, and its management IP address is configured to a management plane IP address. | VM name: VSAM01<br>Node name: VSAM<br>Management IP address: 192.168.210.60<br>Subnet mask: 255.255.255.0<br>Gateway: 192.168.210 |
| Storage device | The storage device is connected to hosts through the switch storage plane network to provide virtualized storage resources for the VMs running on the hosts. | The host storage port names and IP addresses for communicating with the storage devices:<br>StoragePort1 172.20.123.123<br>StoragePort2 172.30.123.123<br>StoragePort3 172.40.123.123<br>StoragePort4 172.50.123.123 |
| Switch | Connect servers to the storage device to enable intercommunication among different planes in the FusionSphere system. | N/A |

## 2.2 Service Deployment Plan

**1. Add resources to FusionManager.**

After installing FusionSphere, add the FusionCompute hypervisor to FusionManager, so that FusionManager can manage clusters and hosts resources in the FusionCompute hypervisor and provide virtualized resources for users.

The following figure shows the process of adding virtualized resources to FusionManager.




1. Create resource zones in FusionManager.
   A resource zone in the FusionManager system is a logical zone to manage all resources in an independent layer 2 network in the system. All resources in the system must belong to one or multiple resource zones.
2. Add the FusionCompute hypervisor to FusionManager.
   Add the FusionCompute hypervisor to FusionManager to provide virtualized resources in the FusionManager system. A hypervisor contains all the cluster resources managed by a set of VRM system in FusionCompute.

**3. Associate resource clusters with resource zones in FusionManager.**

After adding the hypervisor to FusionManager, associate resource clusters in the hypervisor with the resource zones in FusionManager, then the resources in the clusters can be automatically added to the resource pools in the zones.

**4. Create availability zones (AZs) in FusionManager.**

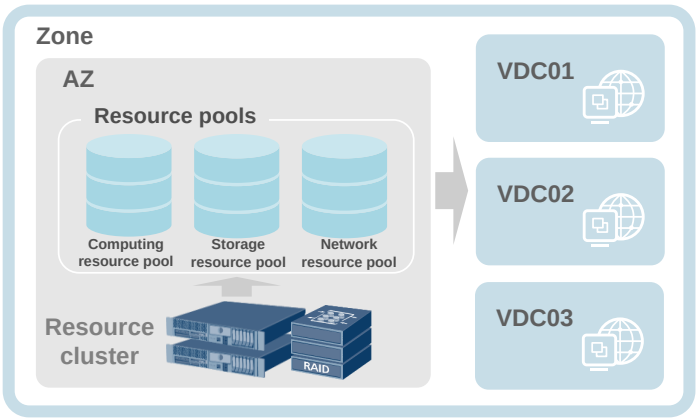
An AZ is a collection of resources available to users in a resource zone. If a resource zone contains multiple resource clusters, you can create multiple AZs to accommodate different resource clusters. An AZ can contain one or multiple resource clusters. By selecting an AZ for a user, you can specify the source of resources available to the user.

In this step, you need to plan data for the following objects.

| Object | Description | Data Plan |
| --- | --- | --- |
| Resource zone | Plan the following information for each resource zone:<br>● Name: identifies a resource zone.<br>● Location: identifies the location of the physical resources in the resource zone. | Name: zone<br>Location: HT2 |
| Hypervisor | Plan the names of the FusionCompute hypervisor and the VSAM node. | Hypervisor name: FC<br>VSAM name: VSAM |
| AZ | Plan the names of the AZs to be created. | AZ name: az |

**2. Configure resource pools and divide resources into VDCs.**

After adding resources to FusionManager, resource pools in each resource zone have available virtual resources. Then, the administrator can include resources in the resource pools into different virtual data centers (VDCs) and allocate the resources to organizations by VDC.



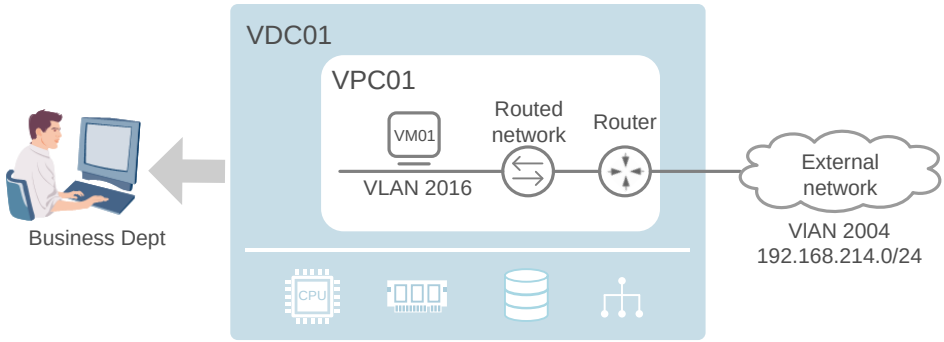

1. Configure resource pools.
   Resource pools are classified into computing resource pools, storage resource pools, and network resource pools. Resources in the resource pools are from the resource clusters virtualized by the hypervisor.
   - Computing resource pool: contains virtual CPU and memory resources on the hosts in the resource clusters.
   - Storage resource pool: contains data store resources in the resource clusters.
   - Network resource pool: contains distributed virtual switches created in the hypervisor. The virtual local area networks (VLANs) used for creating service networks on FusionManager must also be added to the network resource pool for creating external networks and the VSA management network.
2. Create VDCs.
   VDC is the unit for using virtual resources in the resource pools. For example, to provide virtual resources for three departments of a company, you can create a VDC for each department, with each VDC containing isolated computing, storage, and network resources required for the VMs used by each department.

   In this step, you need to plan data for the following objects.

| Object | Description | Data Plan |
|---|---|---|
| VLAN pool | Plan the start VLAN ID and end VLAN ID for the service networks.<br>All VLANs must be allowed to pass through the service plane ports on the switch. | VLAN pool name: VLAN_pool<br>Start VLAN ID: 2004<br>End VLAN ID: 2019 |
| External network | Plan Company A's existing network that can connect to the Internet as the external network, and add the external network to the company's network resource pool to provide IP addresses for the VMs to access public networks. | External network name: external_network01<br>VLAN: 2004<br>Subnet IP address: 192.168.214.0<br>Subnet mask: 255.255.255.0<br>Gateway: 192.168. 214.1 |
| VSA management network | The VSA management network assigns management IP addresses for software routers. The configuration requirements are as follows:<br>• The VSA management network must be configured on the aggregation switch to communicate with the network (VLAN 2000) of the management components at layer 3.<br>• The VLAN planned for the VSA management network cannot be added to FusionManager VLAN pools. | VSA management network name: VSAnet<br>VLAN: 2001<br>Subnet IP address: 192.168.214.0<br>Subnet mask: 255.255.255.0<br>Available IP addresses: 192.168.211.101-192.168.211.150<br>Gateway: 192.168. 214.1 |
| VDC | Plan an independent VDC each for the Business Department, Development Department, and Maintenance Department.<br>Resources in each VDC are managed by the administrator of the VDC respectively. | VDC names:<br>• Business Dept: VDC01<br>• Development Dept: VDC02<br>• Maintenance Dept: VDC03<br>VDC quotas: 12 CPUs, 12 GB memory, and 300 GB storage for each department<br>VDC administrator names: VDC01_admin; VDC02_admin; VDC03_admin |

**3. Deploy services.**

After creating VDCs, create a network in each VDC and provision VMs for users in the VDC. The following figure uses the VDC (VDC01) for the Business Department as an example.



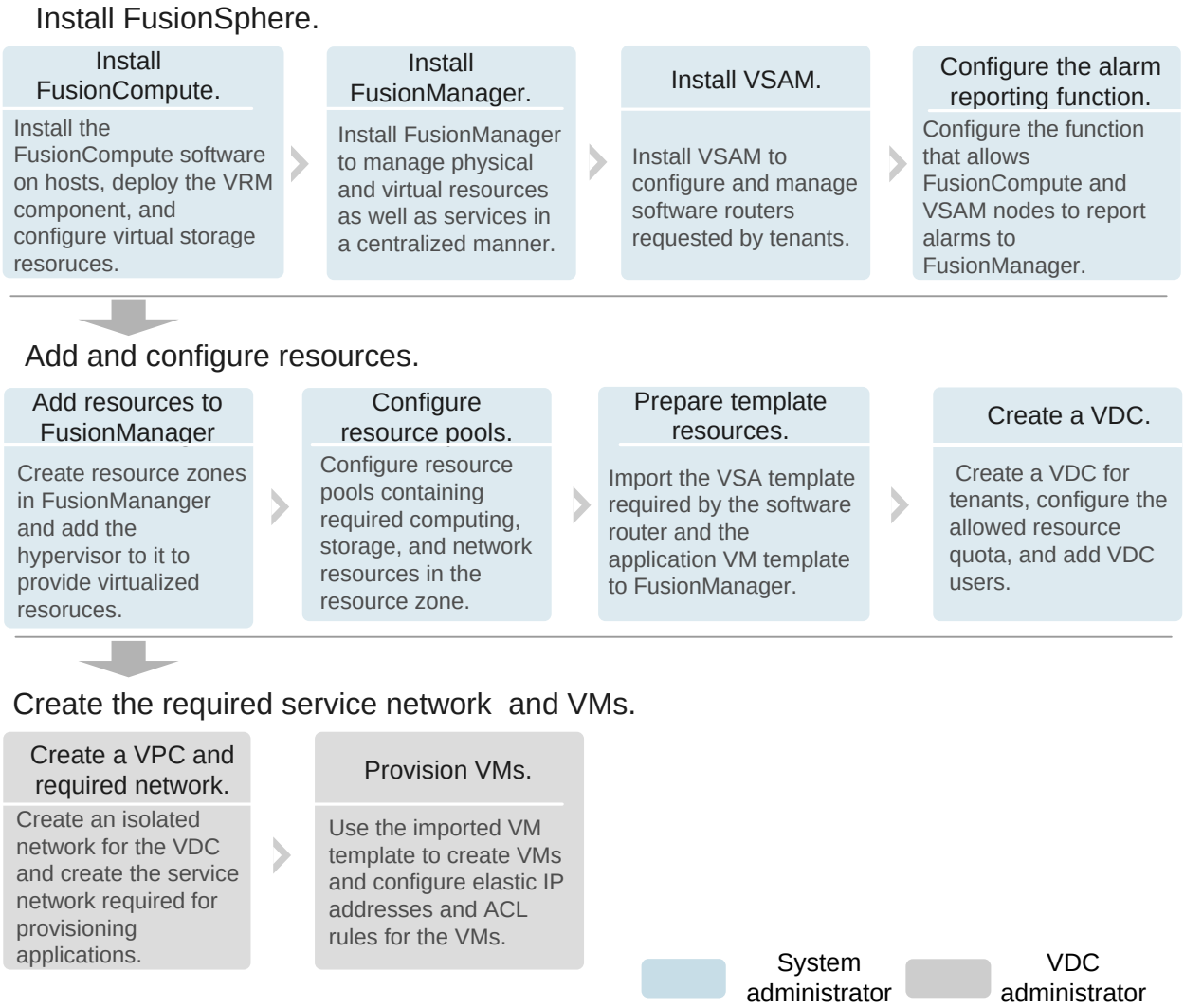

The VDC administrator can create a network and required VMs in the VDC based on the CPU, memory, storage, and network resources allocated to the VDC.

In this step, you need to plan data for the following objects.

| Object | Description | Data Plan |
|---|---|---|
| VPC01 | Plan a virtual private cloud (VPC) for creating secure service networks for the VDC. | VPC name: VPC01 |
| Router | Apply for a software router in VPC01.<br>A software router can be used to bind an elastic IP address to a VM so the VM can connect to the public network. The router also supports the ACL function, which allows the system to use ACL rules to control data packets to be sent to the VMs. | N/A |
| Routed network | Create a routed service network in VPC01.<br>Select a VLAN, for example, VLAN 2016, for the routed network from the service plane VLAN pool. The subnet IP address can be specified by the VDC administrator as desired. | Routed network name: Route_network01<br>VLAN 2016<br>Subnet IP address: 192.168.16.0<br>Subnet mask: 255.255.255.0<br>Gateway: 192.168.16.1 |
| VM | Create a VM for deploying the website system in the routed network.<br>The VM can be created using a VM template that has been published on FusionManager. | VM name: VM001 |

## 2.3 Process Overview

Use FusionSphere to deploy services for the Business Department involves three phases: install FusionSphere, add and configure resources, and create the network and VMs. The entire process is as follows.



## 2.4 Software Preparation

Obtain the following software files for installing FusionSphere.

| Software Type | Software Package | How to Obtain |
|---|---|---|
| FusionCompute host OS | FusionCompute V100R005C00SPC100_CNA.iso | Visit http://support.huawei.com and choose **Enterprise** > **Software** > **IT** > **FusionCloud** > **FusionSphere** > **FusionCompute** > V100R005C00SPC100. |
| FusionCompute installation wizard | FusionCompute V100R005C00SPC100_Tools.zip | |
| VRM VM template file | FusionCompute V100R005C00SPC100_VRM.zip | |
| FusionManager installation file | FusionManager V100R005C00SPC200_SV.zip | Visit http://support.huawei.com and choose **Enterprise** > **Software** > **IT** > **FusionCloud** > **FusionSphere** > FusionManager > V100R005C00SPC200. |
| VSAM VM template file | FusionCompute V100R005C00SPC100_VSAM.zip | Visit http://support.huawei.com and choose **Enterprise** > **Software** > **IT** > **FusionCloud** > **FusionSphere** > FusionCompute > V100R005C00SPC100. |

Obtain the following software files for provisioning services using FusionSphere.

| Software Type | Description | How to Obtain |
|---|---|---|
| OS image file | Used to install an OS on a VM. This task uses the SUSE Linux Enterprise Server 11 OS as an example. | Provided by the lab administrator. |
| Application software | Application software to be installed on VMs, for example:<br>• MySQL<br>• WinRAR<br>• Apache | Provided by the lab administrator. |
| Tools | FusionCompute V100R005C00SPC100_GuestOS Drivers.zip | Visit http://support.huawei.com/enterprise, choose **Software** > **IT** > **FusionCloud** > **FusionSphere** > **FusionCompute** > **V100R005C00SPC100** and download **FusionCompute V100R005C00SPC100_GuestOSDrivers.zip**. |
| VSA VM template | FusionCompute V100R005C00SPC100_VSA.zip | Visit http://support.huawei.com/enterprise, choose **Software** > **IT** > **FusionCloud** > **FusionSphere** > **FusionCompute** > **V100R005C00SPC100** and download **FusionCompute V100R005C00_VSA.zip**. |

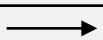
Obtain the following tools before installing FusionSphere:

| Tool Type | Tool Name | How to Obtain |
|---|---|---|
| Cross-platform remote access tool | PuTTY | http://www.putty.org |
| File decompression tool | 7-Zip | http://sparanoid.com/lab/7z/ |

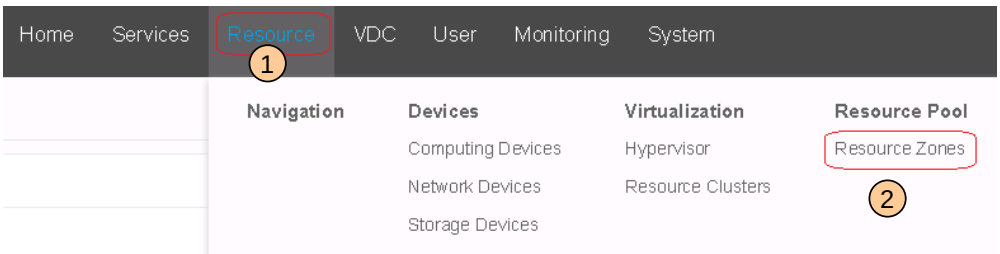
Ensure that the local PC used for installing FusionSphere software meets the following requirements:

| Item | Requirement |
|---|---|
| Hardware | ● Uses 32-bit CPUs with a minimum of 2 GB memory.<br>● The system disk has a minimum of 1 GB free space, and one another service disk has a minimum of 30 GB free space. |
| OS | ● 32-bit Windows XP or Windows 7<br>● Windows firewall is disabled. |
| Network | The PC can communicate with the planned management plane and the host BMC plane properly. |

In the following operation instruction slides, **the left column provides the procedure, and the right column provides the operation background, principle, and other related information**. The following table explains the icons used in the provisioning process. It is recommended that you familiarize yourself with the icon descriptions before proceeding.

| Icon | Description |
|---|---|
|  | Operation sequence |
|  | Transition between different sections of the web interface |
|  | |
|  | Skip to step |

Example:



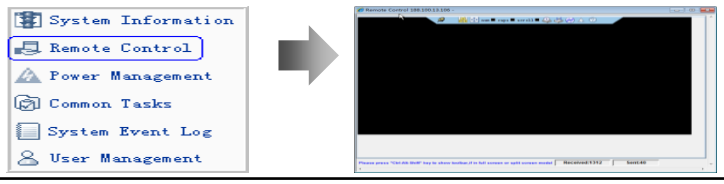
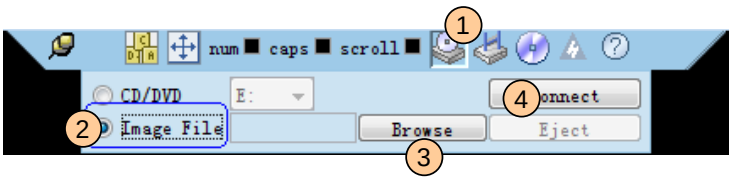

Step 1: Click **Resource**.
Step 2: Click **Resource Zones**.

**NOTE: The screenshots in the steps below include sample parameter values, which may vary from the actual parameter values onsite.**

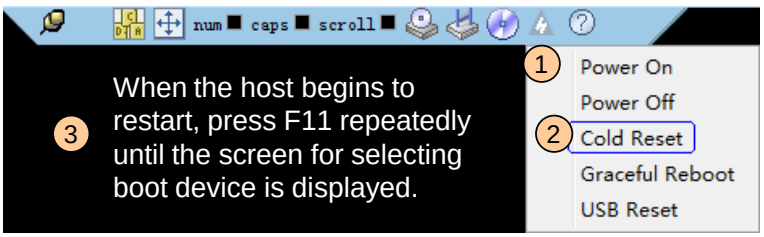
# 3 Install FusionCompute(Optional Task)

## 3.1 Install an OS on the Host

### Step 1: Mount an ISO file to the host.

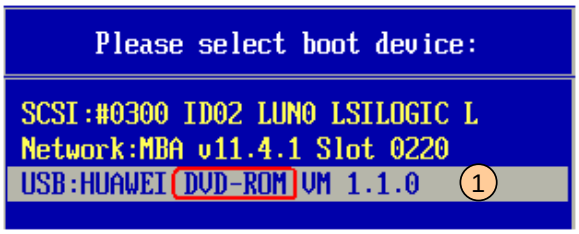
| | |
|---|---|
| 1. Set the local PC to ensure that the PC can ping the host where FusionCompute is to be installed.<br>Ensure that the IP address of the PC is in the same network segment as the host management IP address, and the PC IP address can ping the host BMC system. | Connect the PC and the host to the same switch. |
| 2. Open a web browser on the PC, then enter the BMC IP address into the address bar to access the host BMC system. | First configure the first blade of the X6000 server. |
| 3. Log in to the BMC system using an administrator account.<br>  | Administrator **root** is used as an example in this task. |
| 4. Open the **Remote Control** window.<br>  | You may need to click **Remote Virtual Console** (requiring JRE) on the **Remote Control** page of some Huawei server BMCs. |
| 5. Mount an ISO image to the host.<br>  | ③ Select **FusionCompute V100R005C00SPC100_CNA.iso**.<br>④ When **Connect** turns to **Disconnect**, the ISO file is mounted to the host successfully, |

### Step 2: Upload the OS installation file.

| | |
|---|---|
| 1. Restart the host after the ISO file is mounted to it.<br>  | **Note**<br>The host BIOS password may be required during the restart. Obtain the password in advance.<br>● The default BIOS password for Huawei RH-series rack servers, X-series high-density servers, and E6000 blade server is **uniBIOS123**.<br>● The default BIOS password for Huawei Tecal E9000 blade server is **Huawei12#$** or **uniBIOS123**. |

## Step 2: Start to install the OS on the host.

2. Set DVD-ROM as the boot device.



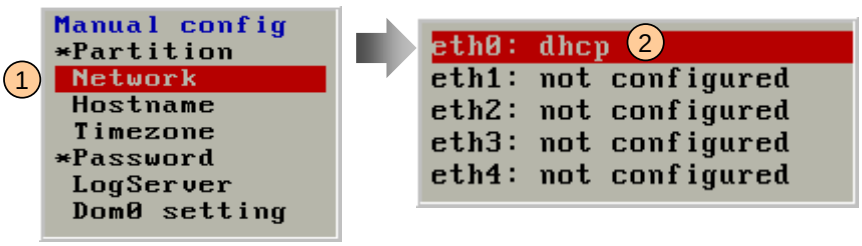

**Note**
The DVD-ROM name and the configuration screen may vary depending on the server used.

3. Select **Install**.


The system begins automatic data loading, which takes about 2 minutes.

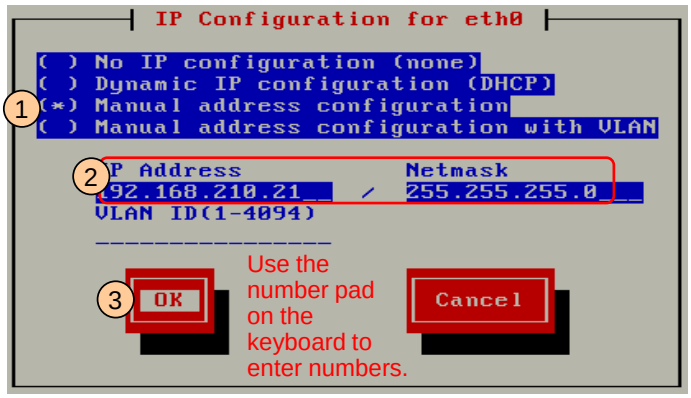
## Step 3: Configure host information.

1. Select **Network**, then select a management plane port, for example, **eth0**.



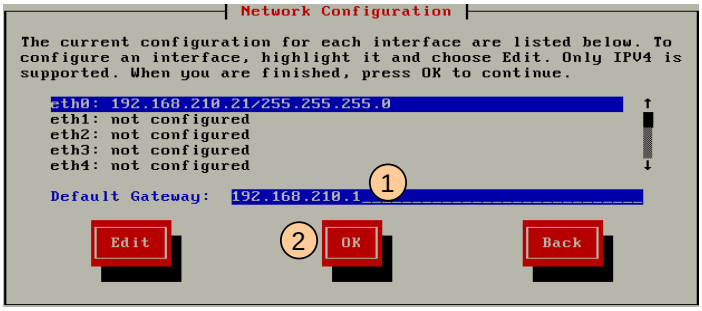

**Tip**
When configuring host data on the configuration screen:
- Press **Tab** or the up and down arrow keys to move the cursor.
- Press **Enter** to expand or execute the highlighted item.
- Press the space bar to toggle between options.

2. On the **IP Configuration for eth0** screen, configure the IP address and subnet mask for the management plane network port.




**Note:** The management plane VLAN must be set to the tagged type on the switch port to which the management network port is connected.

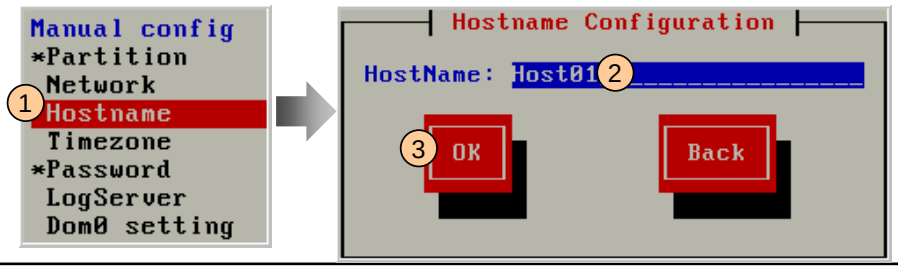
3. On the **Network Configuration** screen, configure the management plane gateway.




N/A

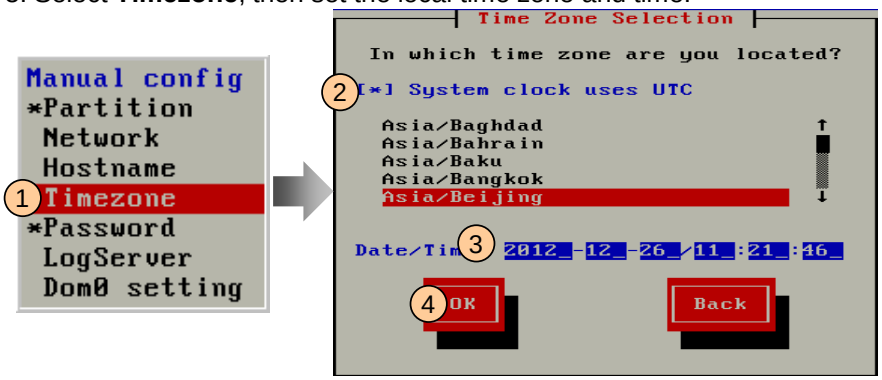
## Step 3: Configure host information.

4. Select **Hostname**, then set the host name.




N/A

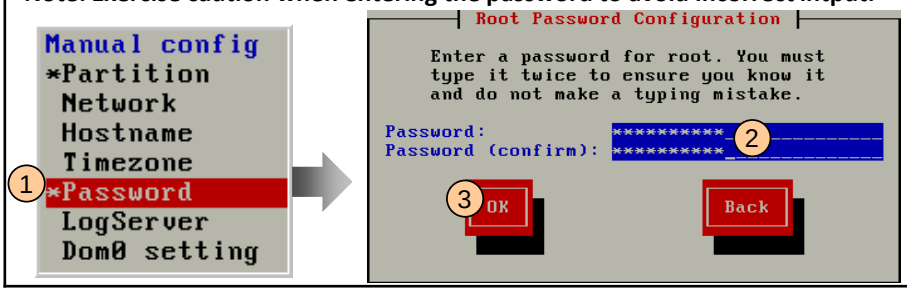
5. Select **Timezone**, then set the local time zone and time.




N/A

6. Select **Password**, then set the password for user **root.**

**Note: Exercise caution when entering the password to avoid incorrect intput.**



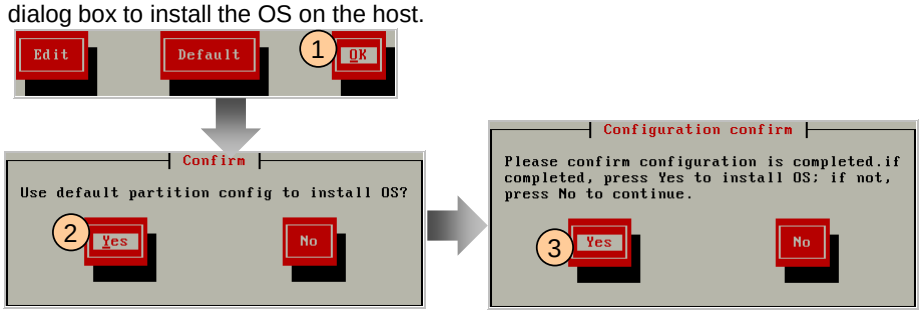

**NOTE**

The password must contain at least:

- Eight characters
- One space or one of the following special characters: ` ~ ! @ # $ % ^ & * ( ) - _ = + \ | [ { } ] ; : ' " , < . > / ?
- At least two of the following: lowercase letters, uppercase letters, and numbers.

## Step 4: Install the host OS.

1. Select **OK** in the bottom right corner of the screen, then select **Yes** in the displayed dialog box to install the OS on the host.




2 Ensure that the OS is installed on the default disk partition.

3 Confirm the configuration, then select **Yes** to install the OS.
The installation takes about 10 minutes.
After the installation is complete, the host automatically restarts.

2. Repeat the above procedure to install OSs on additional hosts.
When the OS installation progress bar for a host is displayed, you can begin installing an OS on the other host.

N/A

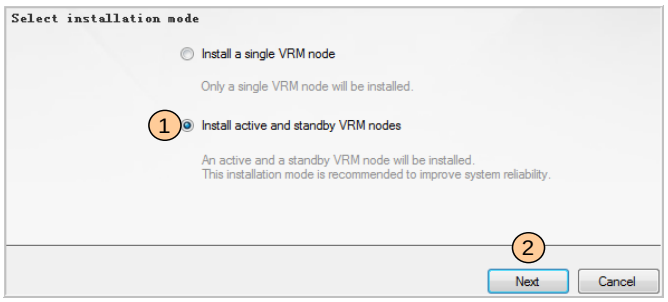
3. If the host running the VRM node is also planned to carry service VMs and the service VMs need to use Huawei storage area network (SAN) devices, use commands to switch the multipathing mode of the VRM host to Huawei multipathing mode after installing the OS on the two hosts.
You can also switch the multipathing mode for the non-VRM host on the FusionCompute web client.

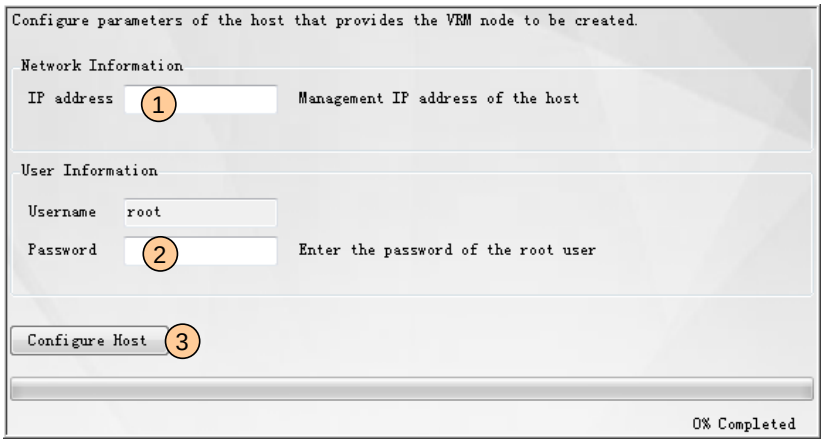
**TIP**

After installing the OS on Host01, you can immediately start to install the VRM node on Host01. During VRM installation, you can install the OS on the other host at the same time.

# 3.2 Install VRM

| Step 1: Decompress the software packages. | |
|---|---|
| 1. Decompress **FusionCompute V100R005C00SPC100_Tools.zip** onto the PC to obtain the **Installer**, **ModCNABFileTool**, **PlugIn**, **ToDPS**, and **HostInstaller** folders. | N/A |
| 2. Decompress **FusionCompute_V100R005C00SPC100_VRM.zip** into a new folder to obtain two VRM VM template files whose file name extensions are .ovf and .vhd, respectively. | N/A |

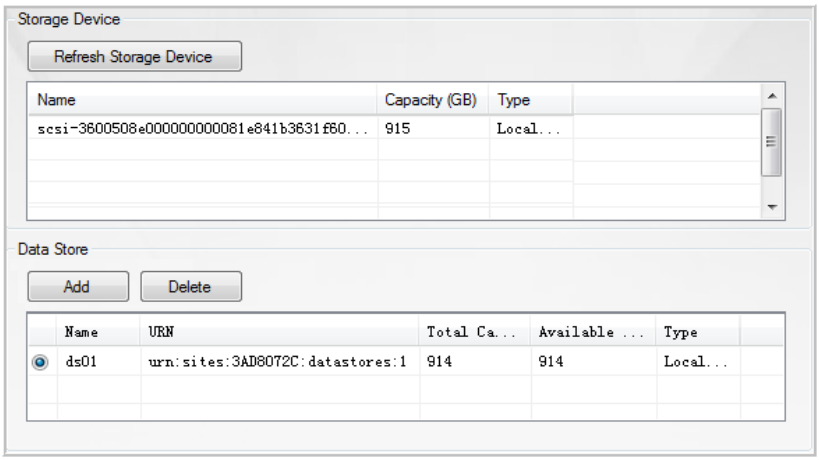
| Step 2: Initialize the installation wizard. | |
|---|---|
| 1. Run **FusionComputeInstaller.exe** in the **Installer** folder. | The installation wizard is opened.<br>**Note**<br>If an error is displayed indicating that the .net Framework program is not installed, run **dotNetFx40_Full_x86_x64.exe** in the **PlugIn** folder. Then manually restart the local PC. |
| 2. Select a language. | N/A |
| 3. Select an installation mode.<br>  | The system begins to install system components, which takes about 30 seconds. |
| 4. Click **Next** after the components are installed. | The **Configure Host** page is displayed. |

| Step 3: Configure the host. | |
|---|---|
| 1. Configure the **host** where the VRM VM is deployed, then click **Next**.<br>  | 1 Enter the management IP address you set during host installation.<br>2 Enter the password (not the host BMC password) you set during host installation.<br>**Note**<br>If a message is displayed indicating that the host is unreachable, ensure that the IP address set in 1 is correct and can be pinged from the local PC. |

## Step 4: Configure a data store.

1. Select **Local disk/FC SAN**, then click **Next**.

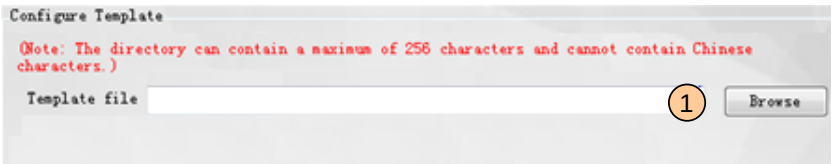
2. The storage devices are automatically refreshed, and the system adds the storage device in the first row as the data store by default.




You are advised to use local disks to install VRM.
A VRM node requires 80 GB space on the local disk.
If local disks are used, the active and standby VRM nodes use different disks, which provide higher reliability.
You are advised to select disks that constitute RAID 1 to enhance reliability.
The length of a RAID 1 disk is generally twice as that of common disks.
For details about VM storage working principles, see Appendix 2.

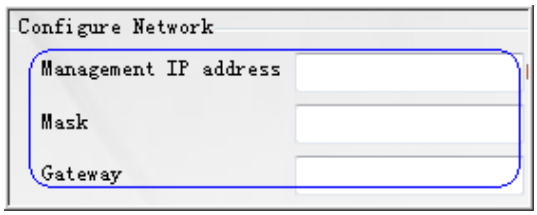
## Step 5: Configure VRM VM information.

1. Configure VRM VM template information.



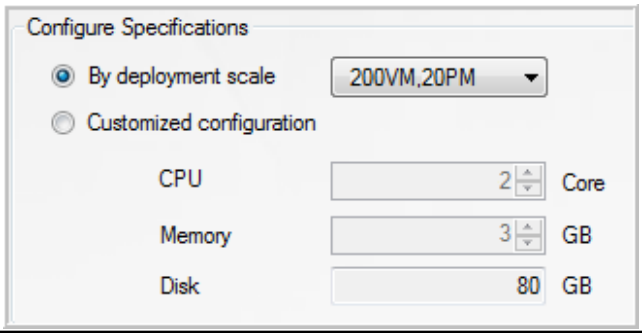

① Select **FusionCompute_V100R005C00SPC100_VRM.ovf**.

2. Set the VRM VM management IP address.




N/A

3. Set VRM VM specifications.

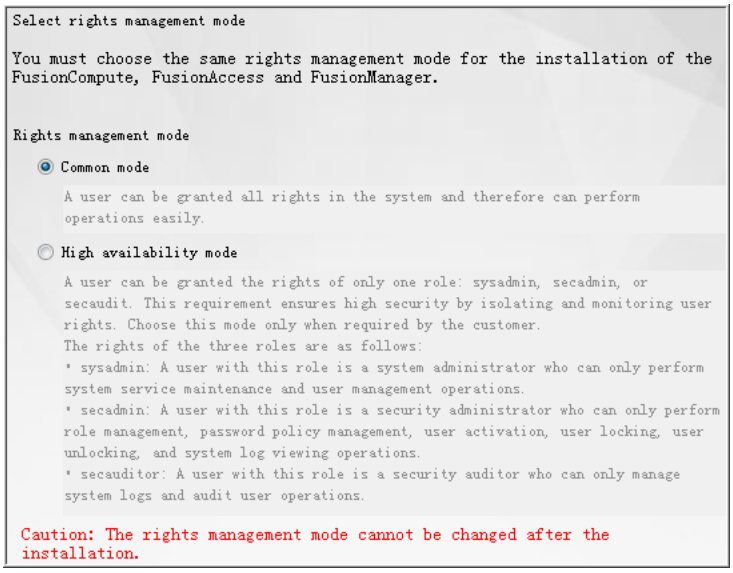



You can set the specifications based on the deployment scale or customize the specifications. **VM** to the right of **By deployment scale** indicates the number of VMs required. **PM** refers to the number of hosts deployed.

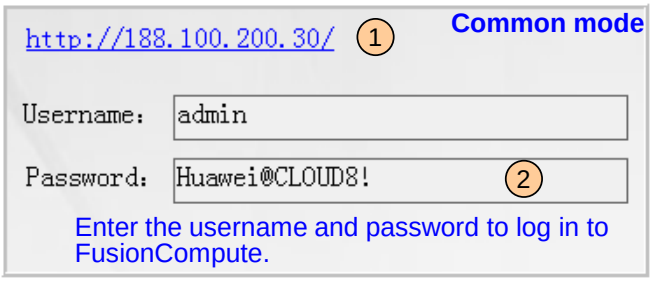
4. Click **Verify Configuration** and click **Next** after the verification succeeds.

N/A

## Step 6: Configure the rights management mode.

| | |
|---|---|
| 1. Select a rights management mode as instructed.<br>  <br> | N/A |

## Step 7: Install the VRM VM.

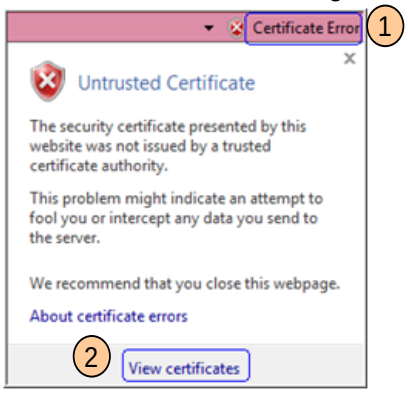
| | |
|---|---|
| 1. Click **Next** to start installing the VRM VM. | The installation takes about 50 minutes. |
| 2. After the installation is complete, click the link on the displayed page and log in to FusionCompute.<br>  <br> | Enter **http://VRM management IP address** in the address bar of the browser, and enter the username and password to log in to FusionCompute.<br>The default username and password are shown in the figure on the left. |
| 3. Click **Finish** to finish the VRM VM installation. | |

# 4 Configure FusionCompute

## 4.1 Log in to the FusionCompute Web Client.

- **To use Internet Explorer➔ Step 1: Configure the Internet Explorer browser.**
- **To use Mozilla Firefox ➔ Step 2: Configure the Mozilla Firefox browser.**

### Step 1: Configure the Internet Explorer browser.

| | |
|---|---|
| 1. Enter http://VRM floating IP address, for example, http://188.100.4.30/, in the address bar of the browser, press **Enter**, and select **Continue to this website (not recommended)**. | Internet Explorer 9 is recommended. |
| 2. In the upper right corner of the browser, click **Certificate Error**, and click **View certificates** in the dialog box displayed.<br>  | After the certificate is installed, FusionCompute will be recognized as a secure site so users do not need to install this certificate again for subsequent logins. |
| 3. Click **Install Certificate** and click **Next** in the dialog box displayed. | N/A |
| 4. Import the certificate to the system as the following figures instruct.<br>  | |

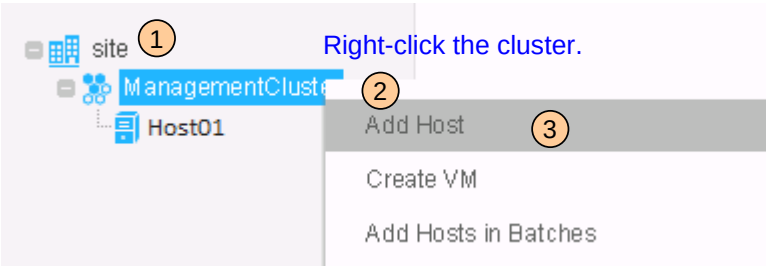
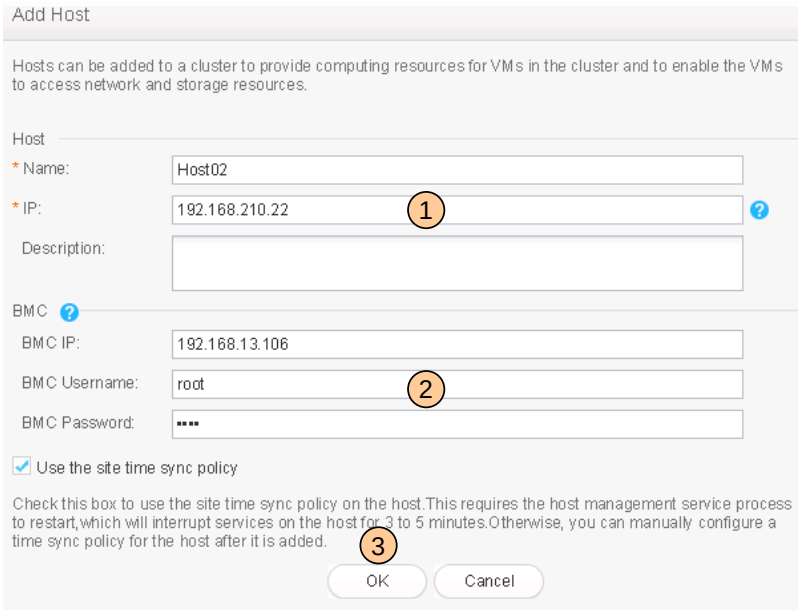
| | |
|---|---|
| 5. Click **Finish**, then click **Yes** in the dialog box displayed. A message is displayed indicating that the import is successful. | N/A |
| 6. Click **OK** to close the certificate dialog box. | |
| 7. Hold down and press **Shift+Ctrl+Delete.** | After the historical records are deleted, restarting the browser will make the previous settings take effect. |
| 8. Select the following options and click **Delete** to delete historical records.<br>● Preserve Favorites website data<br>● Temporary Internet files<br>● Cookies<br>● History | |
| 9. Click **Close** to close Internet Explorer and open it again. | |
| 10. Go to Step 3: Log in to the **FusionCompute Web Client.** | N/A |

| **Step 2: Configure the Mozilla Firefox browser.** | |
|---|---|
| 1. Enter http://VRM floating IP address, for example, http://188.100.4.30/ , in the address bar of the browser, press **Enter**, and select **Continue to this website (not recommended)**. | With this setting configured, the FusionCompute Web Client login page can directly display when you intent to log in to the client the next time. |
| 2. Expand **I Understand the Risks** and click **Add Exception**. | |
| 3. Click **Permanently store this exception** in the dialog box displayed and click **Confirm Security Exception**. | |

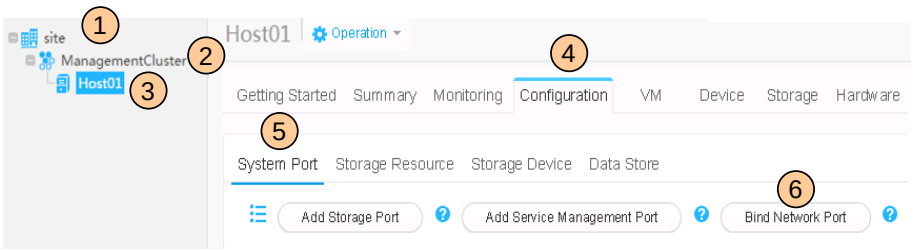
| **Step 3: Log in to the FusionCompute Web Client.** | |
|---|---|
| 1.Enter http://VRM floating IP address in the address bar of the browser and press **Enter.** | N/A |
| 2. Enter the **admin** username and its password to log in to the Web Client. The system asks you to change the initial password upon your first log in to the system. | |

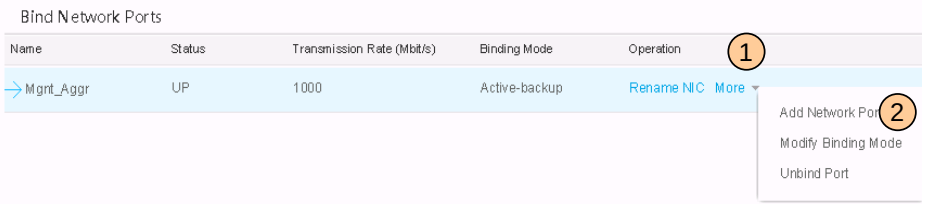
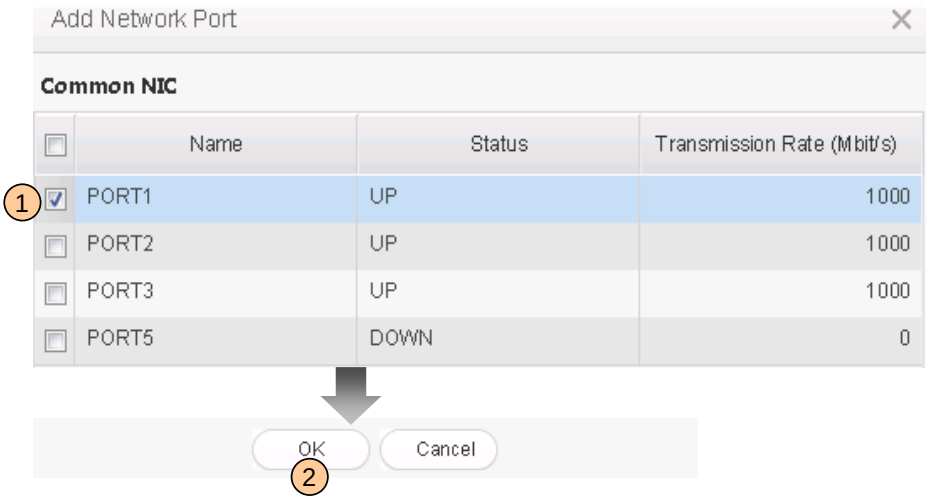
## 4.2 Add Hosts to the Cluster of Host01

### Step 1: Add hosts.

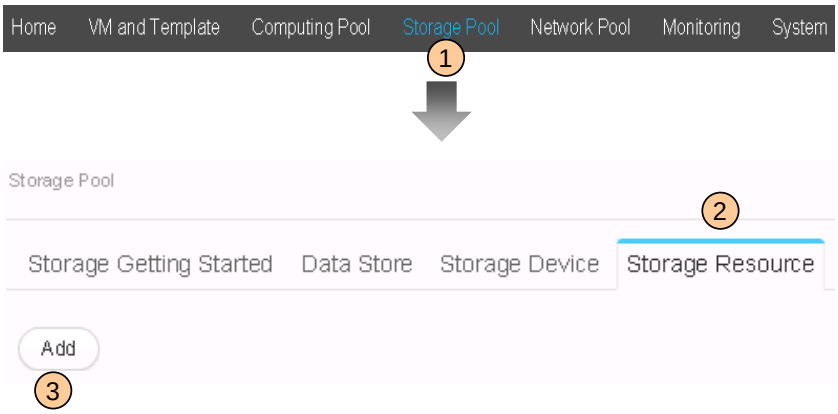
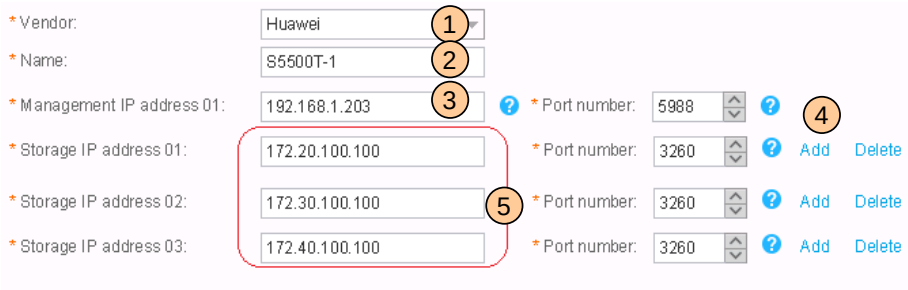
| | |
|---|---|
| 1. On the FusionCompute web client, select **Computing Pool**. | Add all hosts other than the host running the VRM VM to clusters. |
| 2. Go to the **Add Host** page.<br>  | N/A |
| 3. Set the host parameters, then click **OK** to complete the adding.<br>  | After you set the host BMC information, you can power on or off the host on FusionCompute. |

### Step 2: Bind host management ports.

| | |
|---|---|
| 1. Go to the **Bind Network Port** page.<br>  | If ports eth0 and eth1 are both common ports on the management plane of the host, bind them in active/standby mode to improve network reliability. |

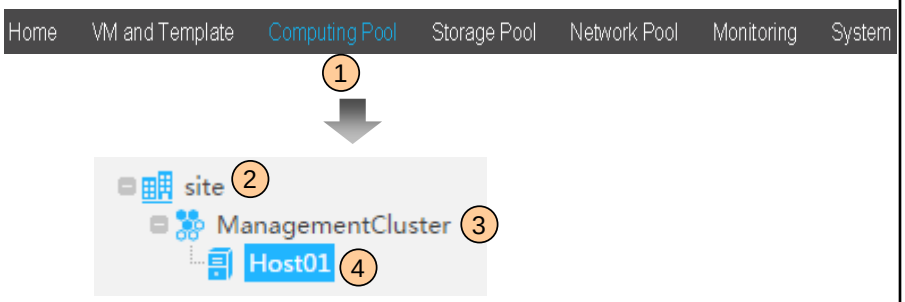
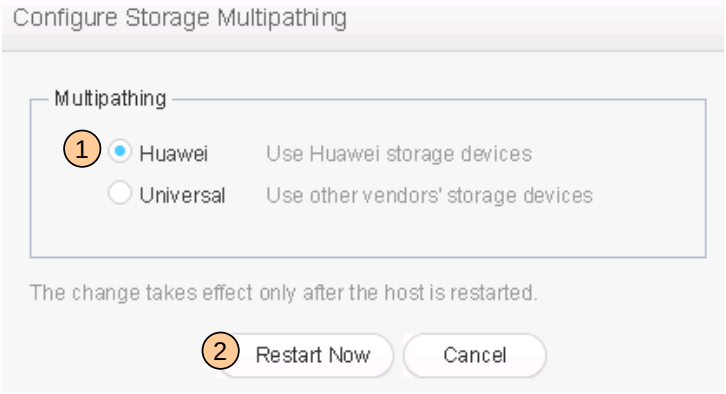
| | |
|---|---|
| 2. Locate the row that contains **Mgnt_Aggr**, then open the **Add Network Port** dialog box.<br>  | **Mgnt_Aggr** is a bound port automatically created during host OS installation that contains the management port **eth0** you configured. Select another management port **eth1** and bind it to **eth0** as **Mgnt-Aggr** to improve network reliability. |
| 3. Select the port name for eth1 to bind it to the management plane network port **PORT*X*** in the displayed port list represents the network port **eth*x*** on the host.<br>  | N/A |
| 4. Click **OK** on the **Bind Network Port** page. | |
| 5. Bind **eth0** and **eth1** on the other host. For details, see **1** to **4**. | |

## 4.3 Add Storage Resources to a Site (SAN Storage)

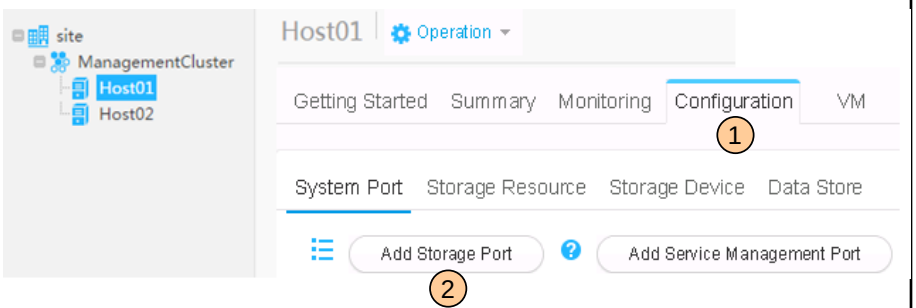
<table>
<tr><td>1. Open the Add Storage Resource dialog box.<br> 
</td><td rowspan="2">For details about network communication between hosts and storage devices, see Appendix 3.</td></tr>
<tr><td>2. Set the storage resource type to IP SAN, then click Next.</td></tr>
<tr><td>3. Set the storage device parameters, then click Add.<br> 
</td><td>3 The management IP address specifies the storage device.<br>4 5 An IP storage area network (SAN) device connects to a host through multiple storage links. Enter the information for all links at one time.</td></tr>
<tr><td>4. Click Next.</td><td rowspan="3">N/A</td></tr>
<tr><td>5. Select the host to be connected to, then click Next.</td></tr>
<tr><td>6. Obtain the generated world wide name (WWN), then click Finish.</td></tr>
</table>

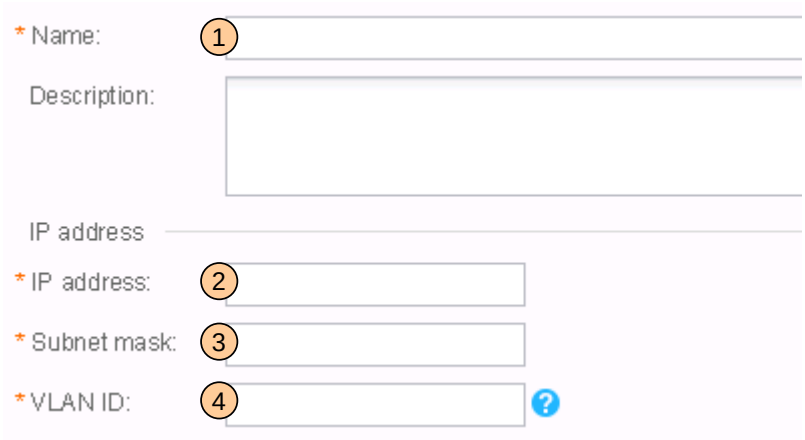
## 4.4 Add a Data Store to the Host (SAN Storage)

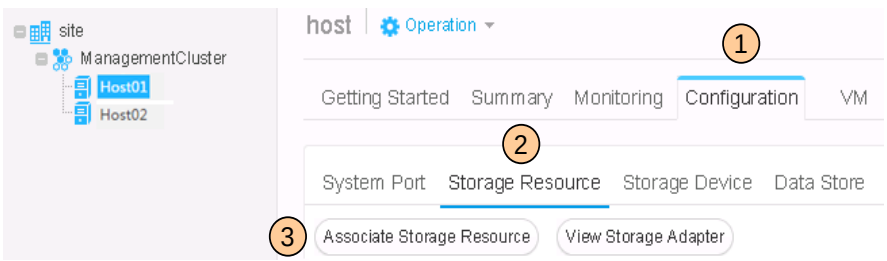
### Step 1: Change the host multipathing mode.

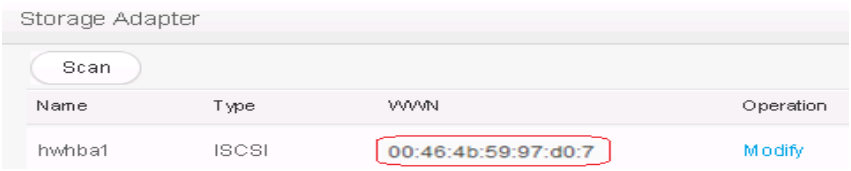
| | |
|---|---|
| 1. Go to the **Getting Started** page of the host.<br>  | The default multipathing mode for FusionCompute is **Universal**. If a Huawei IP SAN device is deployed, change the mode to **Huawei** to improve storage performance. If non-Huawei storage devices are deployed, skip this step. |
| 2. Open the **Configure Storage Multipathing** dialog box. | N/A |
| 3. Select **Huawei**.<br>  | Restart the host for the settings to take effect. The restart process takes about 3 minutes.<br>You can ping the IP address of the host to check whether the host has restarted. If the host can be pinged, the host has successfully restarted. |

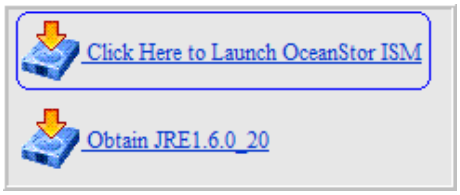
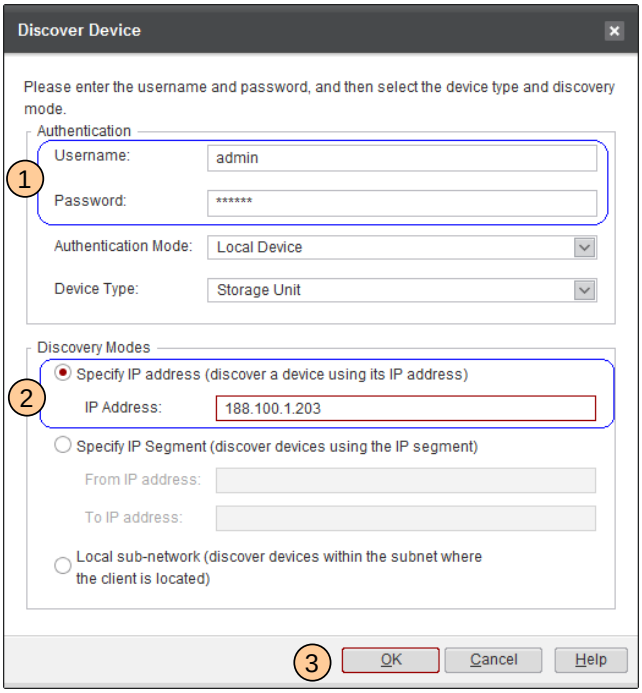
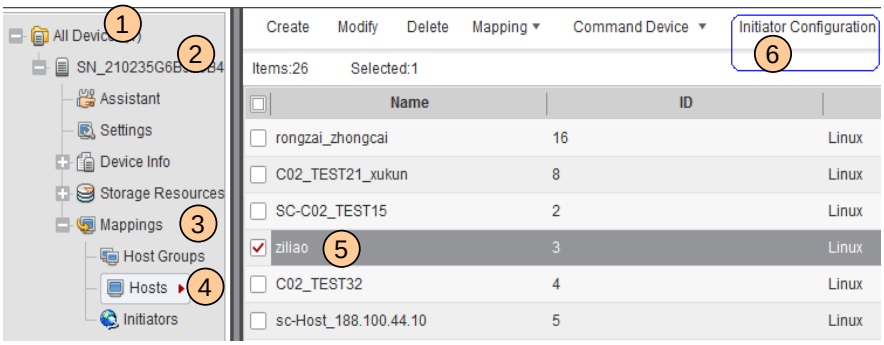
### Step 2: Add storage ports to the host.

| | |
|---|---|
| 1. Go to the **Add Storage Port** page of the host.<br>If you changed the multipathing mode of the host, perform this step after the host restarts.<br>  | After storage ports are added to the host, the host can communicate with the IP SAN device. |

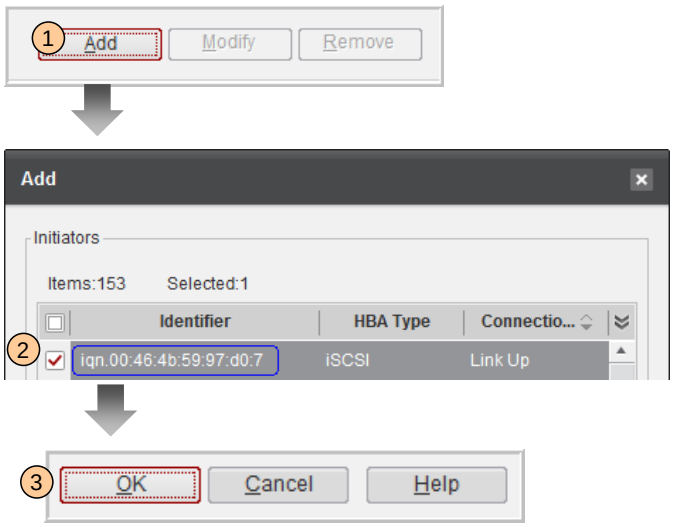
| | |
|---|---|
| 2. Select the host storage plane network , then click **Next**.<br>**PORTX** indicates the network port **ethX** on the host. | The page for connection configuration is displayed. |
| 3. Set the storage port parameters, then click **Next**.<br>  | The page for information conformation is displayed. The IP address is used to communicate with the storage device. Set it to an idle IP address on the storage plane. |
| 4. Confirm the information, then click **Add**. | The **Finish** page is displayed, indicating that the port has been added to the host. |
| 5. If multipathing mode is selected, click **Continue** and repeat **2** to **4** to add multiple storage ports to the host. Click **Close** on the **Finish** page after all ports are added. | N/A |

| **Step 3: Associate storage resources with the host.** | |
|---|---|
| 1. Go to the **Associate Storage Resource** page of the host.<br>  | After a storage device is associated with a host, the host can discover all storage resources on the device. |
| 2. Select the added storage resources, click **Association**, then click **OK** on the displayed dialog box. | The storage resource is associated with the host. After association, all associated storage resources are displayed on the **Storage Resource** page. |

| **Step 4: Configure the initiator.** | |
|---|---|
| 1. Choose **Configuration** > **Storage Resource** and record the host WWN displayed in the bottom right corner of the page.<br>  | Storage devices identify a host using the WWN of the host. |

| | |
|---|---|
| 2. Enter the storage device management IP address in the address bar of the browser, then press **Enter** to load the storage device management software.<br>  | **NOTE**<br>The initiator can be configured only on the management interface of the storage device. |
| 3. Select a language, then click **OK**. | The storage device management software is open. |
| 4. Click **Discover Device**. | N /A |
| 5. Enter the administrator username and password to scan the storage device.<br>  | 2 Enter the management IP address of the storage device. |
| 6. Enter logical host view, then click **Initiator Configuration**.<br>  | 5 Select the logical host that matches the logical unit number (LUN). The selected host in the figure is only an example. |

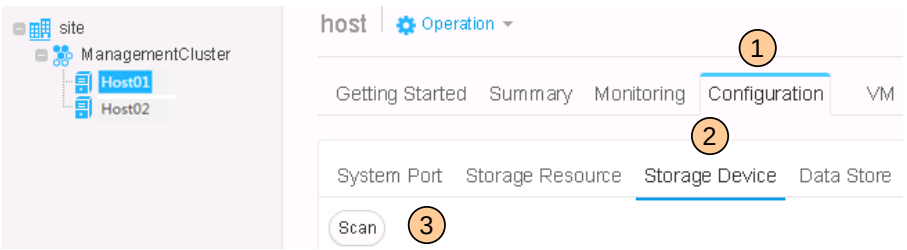
7. Add the host WWN to the initiator.




2 Select the host WWN you have recorded.

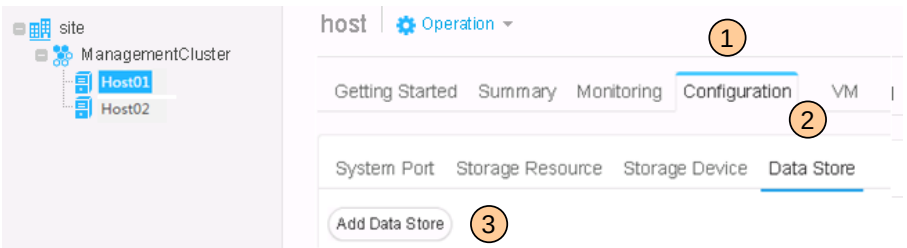
## Step 5: Add a data store.

1. Switch to FusionCompute and scan storage devices available to the host.



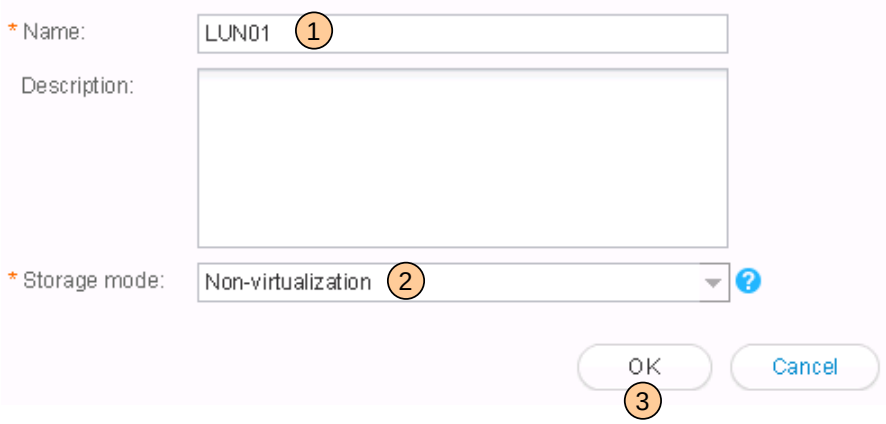

A data store is used to create user disks on VMs. You can view the task progress on the **Task Tracing** page.

2. After the scan is complete, go to the **Add Data Store** page of the host.




N/A

3. Select a SAN device and add it to the host as a data store.

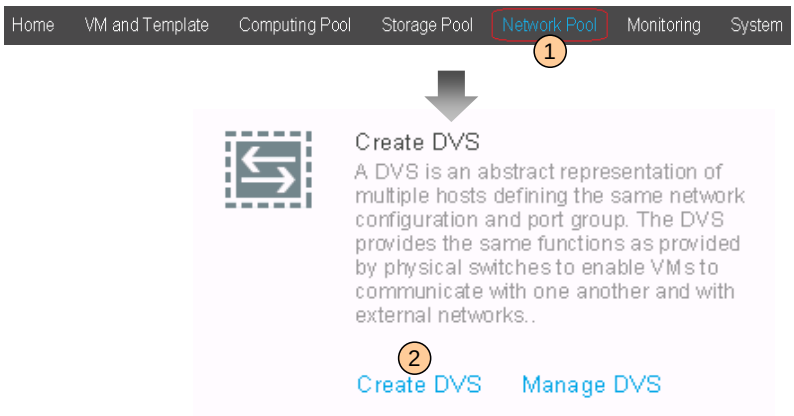
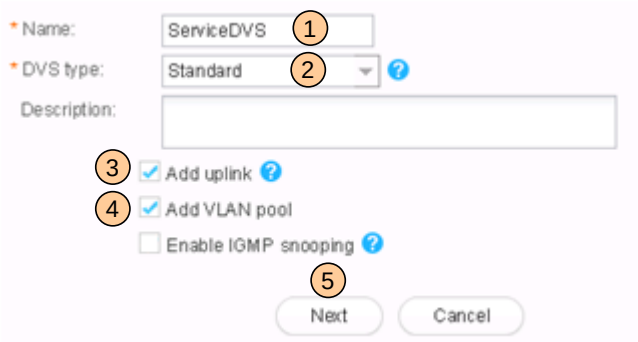
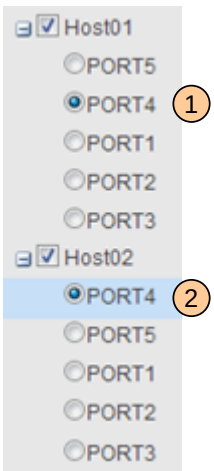


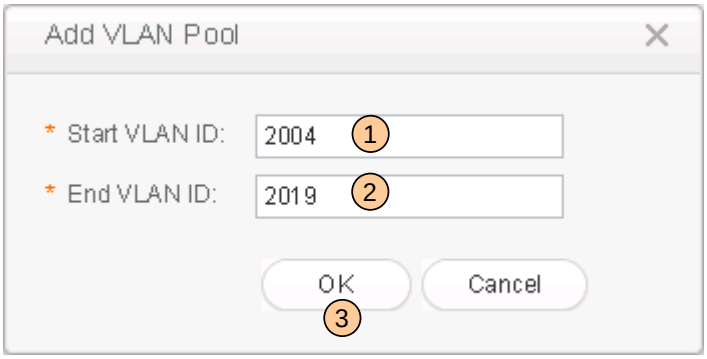

2 A virtualized SAN storage device supports advanced storage features, such as thin provisioning, snapshots, and live storage migration, and provides high resource utilization. However, disk creation on it is slow.
If you set this parameter to **Virtualization**, you can select whether to format the data store. When a data store is added to the host the first time, the data store must be formatted.

# 4.5 Add Virtual Network Resources to the Site

**NOTE:** If the service plane and the management plane are deployed on the same network plane, no service plane distributed virtual switch (DVS) is required. Instead, you only need to add a service plane VLAN pool to the management plane DVS.

## Step 1: Create a DVS.

| | |
|---|---|
| 1. Go to the **Create DVS** page.<br>  | Create a DVS that connects to the service plane to provide network resources for user VMs. A DVS named **ManagementDVS** for the management plane has been automatically created during VRM installation, the bound network port **Mgnt_Aggr** has been added to the uplink group on the DVS, and a management plane port group **managePortgroup** has been created.<br>For details about VM network access, see Appendix 1. |
| 2. Set the DVS name, then check the boxes next to **Add uplink** and **Add VLAN pool**.<br>  | N/A |
| 3. Select a service port for each host on the **Add uplink** page.<br>  | An uplink is a physical port on a host that connects to a DVS. VMs connect to the network through the physical ports on the host.<br>Add all the hosts in a cluster to the same uplink group on a DVS. This allows VMs in the cluster to have the most migration options if a fault occurs. |
| 4. Click **Next.** | N/A |
| 5. Click **Add.** | |

| | |
|---|---|
| 6. Set a VLAN pool on the DVS.<br>  <br> | A VLAN pool defines the allowed VLAN range for a DVS.<br>During service provisioning, create port groups on the DVS for each service. This allows each port group to use VLANs from different VLAN pools.<br>The VLAN pool set on the DVS must be the same as the VLANs set on the physical switch to which the host connects. |
| 7. Click **Next**. | N/A |
| 8. Click **Create**. | |

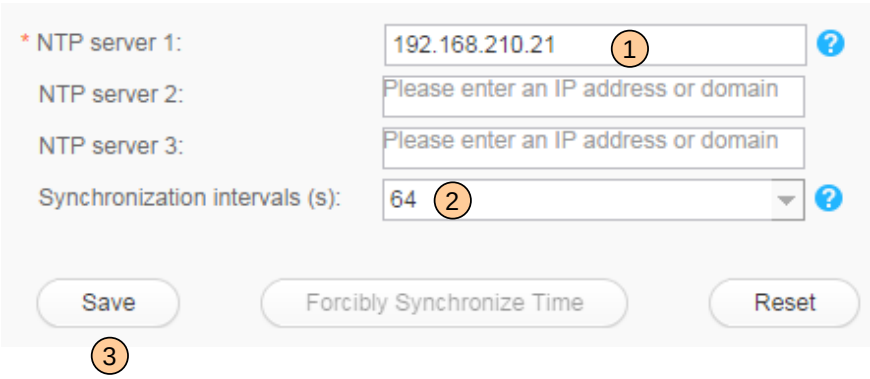
## 4.6 Configure the NTP Clock Source and Time Zone

### Step 1: Configure the Network Time Protocol (NTP) clock source.

1. On FusionCompute, click **System**.

2. Choose **System Configuration** > **Time Management**.

3. Set the NTP server information.

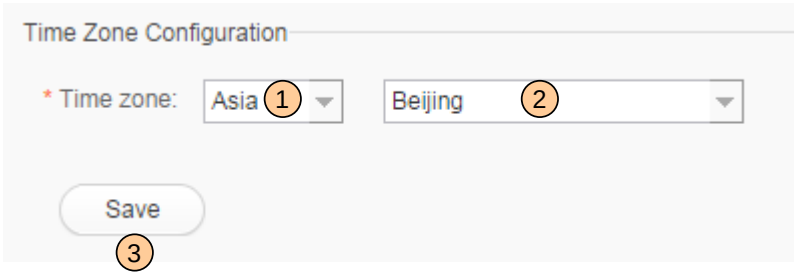



After an NTP clock source is set, the time on all nodes in the system is the same.
If multiple NTP servers are to be deployed, ensure that all the NTP servers use the same upper-layer clock source to ensure time consistency.
This configuration requires a restart of the FusionCompute service process, which interrupts services for about 2 minutes. After the restart, log in to FusionCompute and continue to the next step.
For details about time synchronization, see Appendix 4.

### Step 2: Configure the time zone.

1. On the **System page**, choose **System Configuration** > **Time Zone.**

2. Configure the time zone settings.

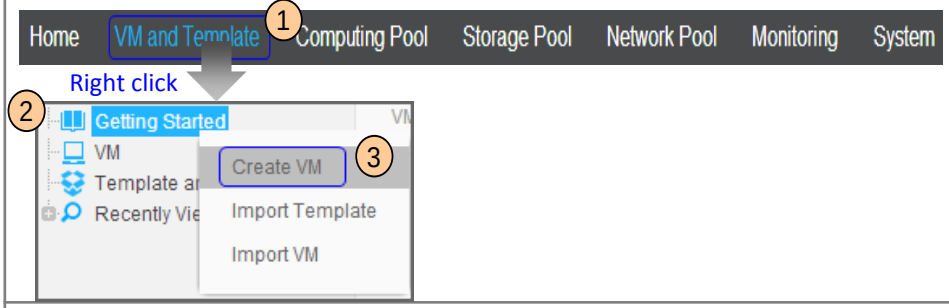



N/A

# 4.7 Create a Bare VM

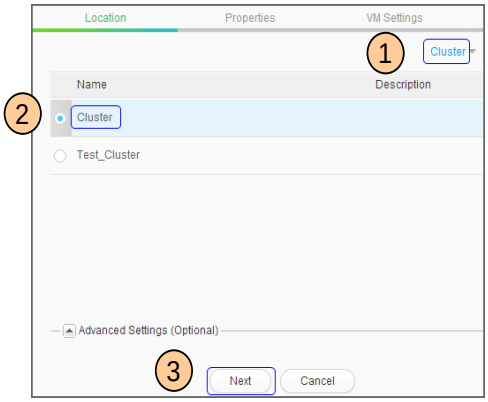
## Step 1: Select a VM Location

1. Go to the **Create VM** page.




-

2. Select the location at which to create the VM.



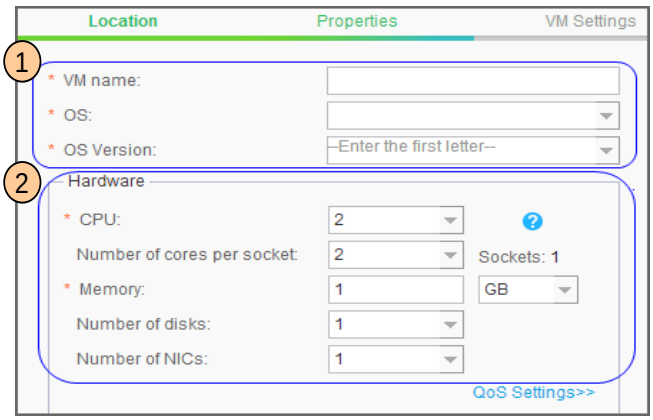

A cluster is a group of hosts.

- If there are no specific requirements for the location of a VM host, select **Cluster**. The system will select a suitable host in the cluster to create the VM on.
- To deploy the VM on a specified host, select **Host**. You can also check the box next to **Bind to Host** to bind the VM to the host.

After the VM is bound to a host, the VM can only run on this host and cannot be migrated to another host.

## Step 2: Configure the VM Attributes

1. Configure the VM attributes in the figure below based on the planned data. All other VM attributes use the default configuration.



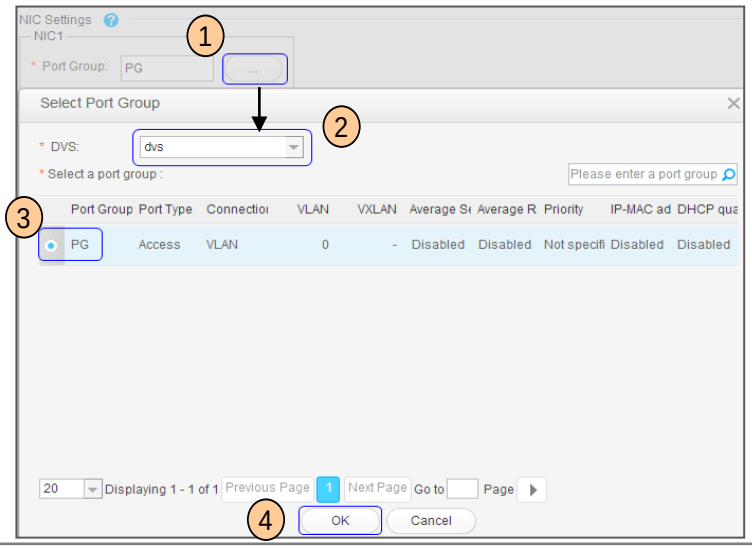

-

2. Click **Next** to go to the **Set VM** page.

-

## Step 3: Configure VM Network Attributes

1. Select a VM NIC port group according to the VM network configuration requirements of the customer.




2. Repeat the above procedure to configure the port groups for other VM NICs.

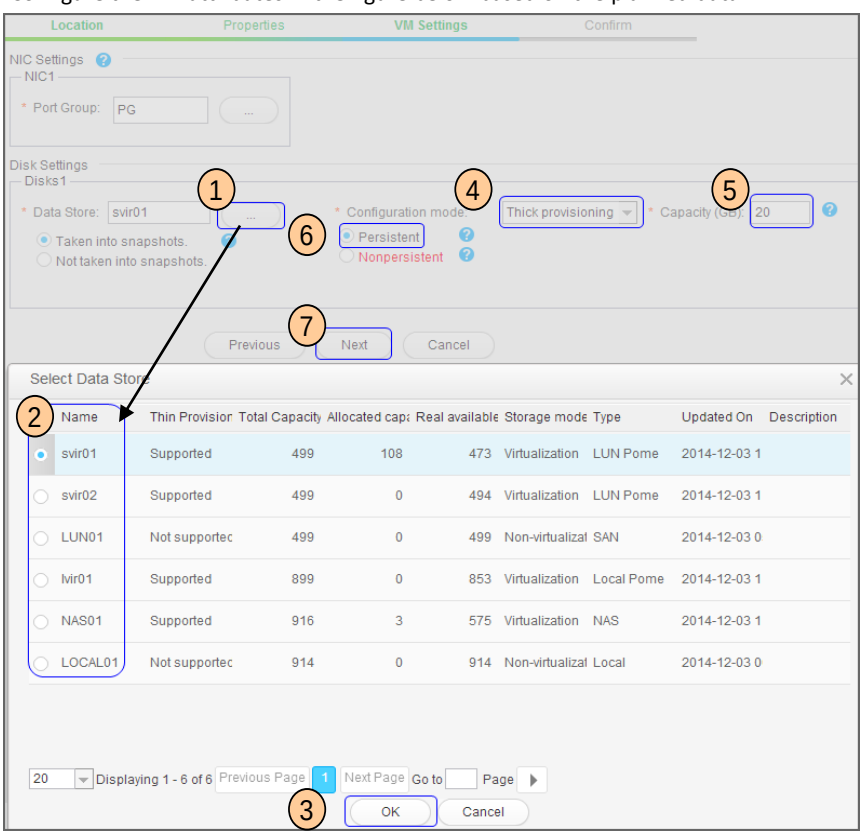
A **DVS** is similar to a switch used for communications on the layer 2 network. The DVS allows the VM to communicate with the physical network.

A **port group** is a logical port of the VM. The port group is used to define the mode the VM NIC uses to connect to the network.

For details, see *Principles of VM Network Access*.

## Step 4: Configure VM Disk Attributes

1. Configure the VM attributes in the figure below based on the planned data.




2. Repeat the above procedure to configure the attributes of other VM disks.

3. After configuring all disks, click **Next**. Confirm the configuration information, then click **Finish**.

-

2 The storage resource pool associated with the host is used as the data store. The data store is used to create VM disks. For details, see *Principles of VM Storage Access*.

4 For virtualized data stores, VM disks can use the following configuration modes:

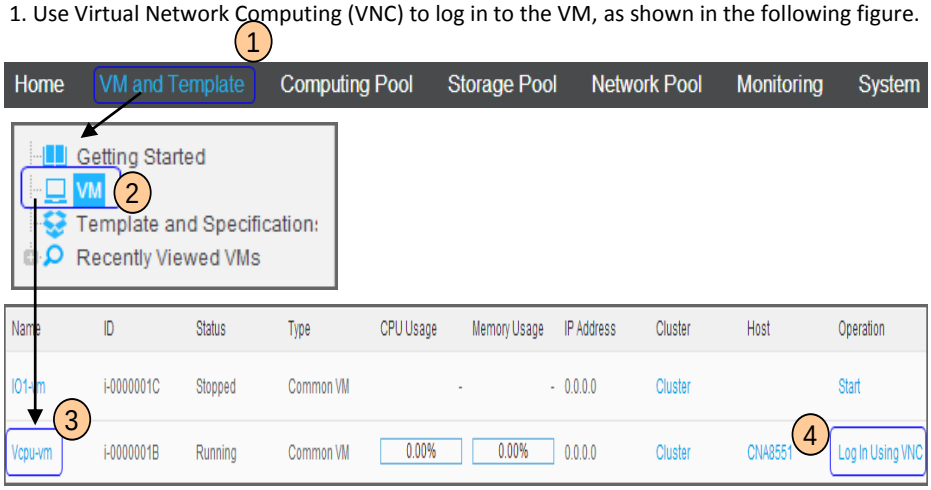
- **Common:** Distributes disk space according to capacity. Immediate disk formatting.
- **Thick provisioning lazy zeroed:** Distributes disk space according to capacity. Delayed formatting. Above average disk creation speed.
- **Thin provisioning:** Distributes disk space according to actual usage.

### Step 5: Confirm VM Creation

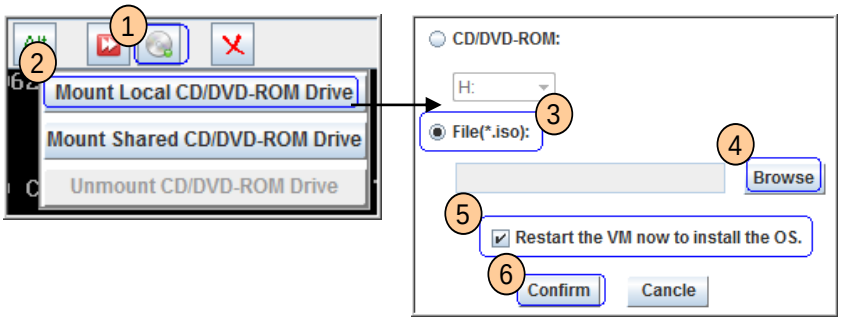
| | |
|---|---|
| 1. Click **Query Task**. Enter the task center and check the progress of VM creation.<br><br>The creation time of a bare VM depends on the VM disk size and disk storage type. The formatting process for thin provisioning disks is relatively slow, please wait a moment. | - |

## 4.8 Install an OS on the VM (Using a Windows VM as an Example)

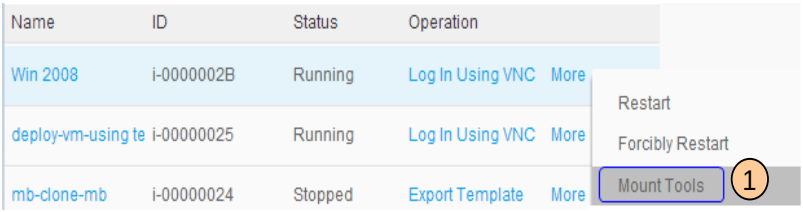
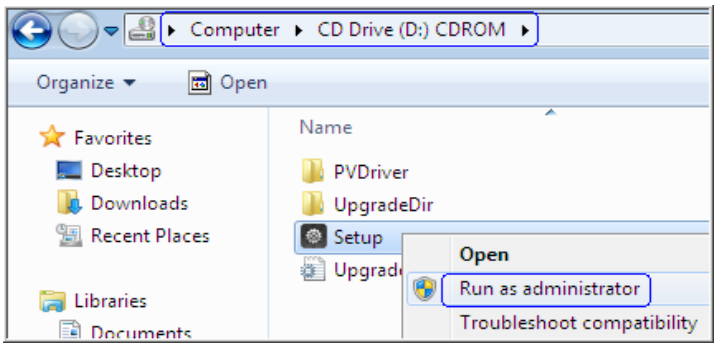
### Step 1: Log In to the VM Using VNC

| | |
|---|---|
| 1. Use Virtual Network Computing (VNC) to log in to the VM, as shown in the following figure.<br>  | VNC login refers to the process of using VNC protocol to remotely access a VM. VNC login allows you to log in to the VM and locate faults through the management plane when the VM network is unavailable. |
| 2. Select **noVNC** in the displayed dialog box.<br>Accept the operation risks as prompted to open to the VNC window.<br>  | - |

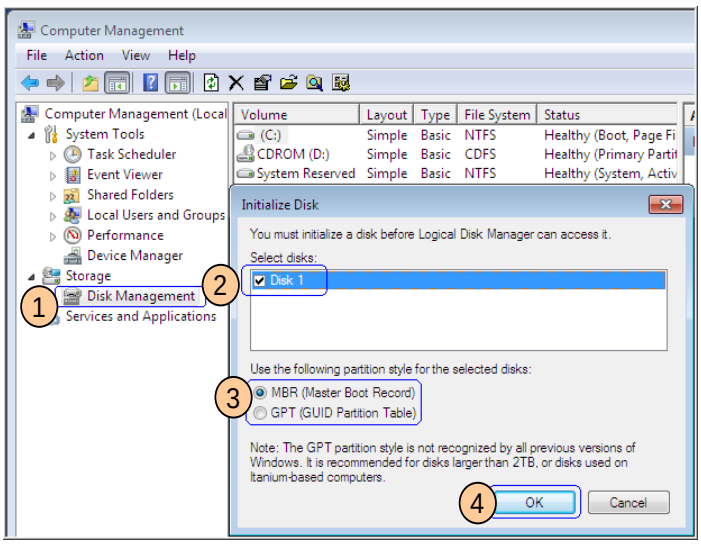
### Step 2: Install an OS on the VM

| | |
|---|---|
| 1. Mount the OS image from the CD/DVD-ROM drive to the VM.<br>  | If only the OS installation disc is available, insert the disc into the CD/DVD-ROM drive, select **CD/DVD-ROM**, and then specify the drive name. |
| 2. Restart the VM, then follow the instructions below to install the OS on the VM.<br><br>**NOTICE** Do not close the VNC window before the OS installation completes. Otherwise, the CD/DVD-ROM drive is automatically unmounted from the VM, which causes the installation to fail. | - |
| 3. After the OS is installed, click  on the top of the VNC window, then select **Unmount CD/DVD-ROM Drive**. | Do not close the VNC window, as it is needed for subsequent operations. |

## Step 3: Install Tools on the VM

| | |
|---|---|
| 1. Locate the row that contains the VM, click **Mount Tools**, then follow the procedure to complete installation.<br>  | Tools contains the paravirtualized (PV) driver for the VM.<br>The PV driver improves I/O processing, hardware monitoring, and other high-level functions on the VM.<br>Mounting Tools mounts a PV driver to the VM. |
| 2. Open the **CD-ROM** drive on the VM. Right-click **Setup**, select **Run as Administrator**, and follow the procedure to complete installation.<br>  | - |
| 3. Restart the VM according to the procedure for Tools to take effect.<br>VMs running Windows Server 2008 must be restarted twice. | - |

## Step 4: Initialize the User Disk

| | |
|---|---|
| 1. On the OS interface on the VM, click **Start**, right-click **Computer**, and click **Manage**. | The user disk refers to a disk drive other than the C drive. If the VM does not have any user disks, skip this step. |
| 2. Initialize the user disk. (**Windows 7** is used as an example below.)<br>  | 3 Select the layout of disk partitions according to the user requirements. |
| 3. Right-click the disk space that has not been distributed, select **New Simple Volume**, and follow the procedure to complete volume creation. | - |

### Step 5: Install Applications

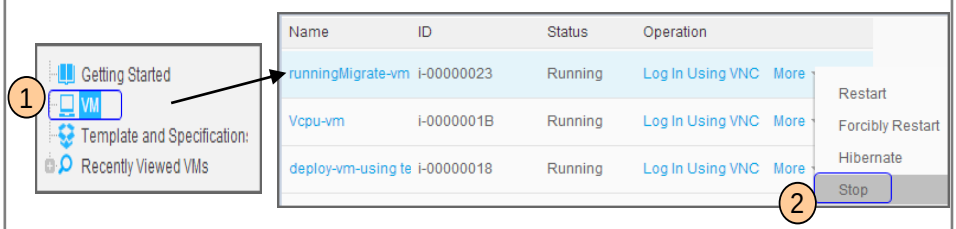
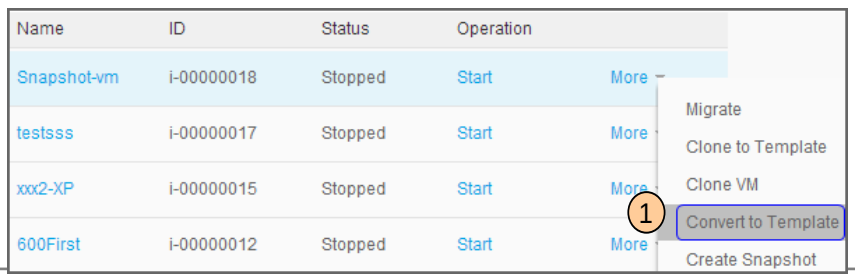
| | |
|---|---|
| 1. If the VM uses VLAN to access the network, configure an IP address for the VM. This allows the VM to intercommunicate with external networks. | - |
| 2. Install applications on the VM.<br>• If the application is an ISO file or on a disc, you must use the CD/DVD-ROM mounting method to install the application.<br>• All other types of installation files must be copied onto the VM before proceeding with installation. | Applications are installed on the VM. |

## 4.9 Create a Template

### Step 1: Select the template creation plan.

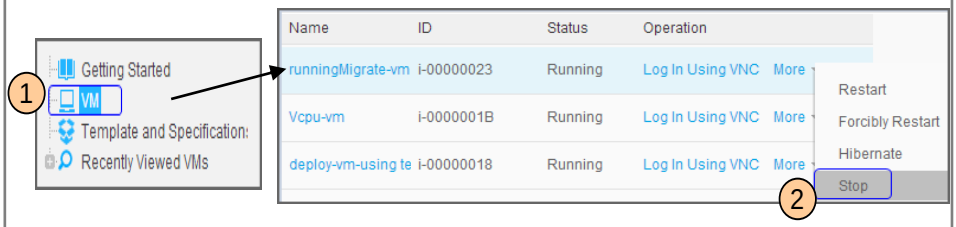
| | |
|---|---|
| 1. Select either of the plans to create a template based on actual requirements:<br>● Convert a VM to a template, select **Plan 1**.<br>● Clone a VM to a template, select **Plan 2**. | NOTE:<br>● Convert a VM to a template: All parameters of the template are from the VM. After a VM is converted to a template, the VM is automatically deleted.<br>● Clone a VM to a template: A copy of the VM is created, and you can customize some parameters to make the template different from the original VM. After the VM is cloned to a template, the original VM can still be used. |

### Plan 1: Convert a VM to a template.

| | |
|---|---|
| 1. Locate the row that contains the VM, and choose **More > Stop** to stop the VM.<br>  | When you convert a VM to a template, the VM must be in the **Stopped** state. |
| 2. Locate the row that contains the VM to be converted to a template and choose **More > Convert to Template**.<br>  | - |
| 3. Click **OK** in the displayed dialog box. | - |
| 4. Click **OK** in the displayed dialog box. | - |
| 5. Check whether the VM is successfully converted to a template on the **Task Center** page. | - |

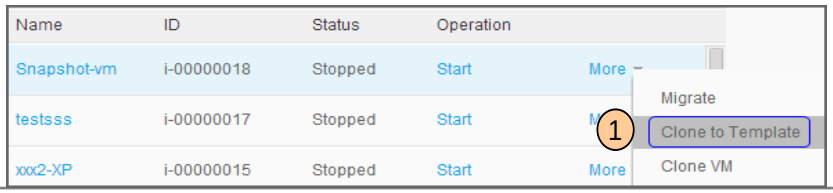
## Plan 2: Clone a VM to a Template

1. Locate the row that contains the VM and choose **More > Stop** to stop the VM.



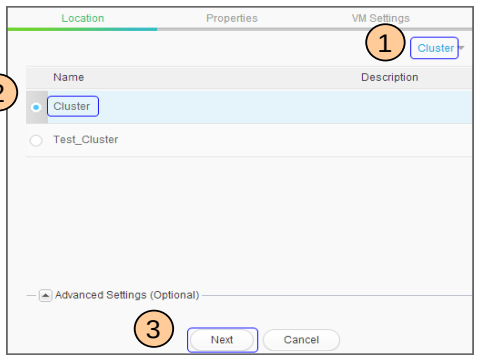

When you clone a VM to a template, the VM must be in the **Stopped** state.

2. Locate the row that contains the VM to be cloned to a template, and choose **More > Clone to Template**.




-

3. Select the template creation location.

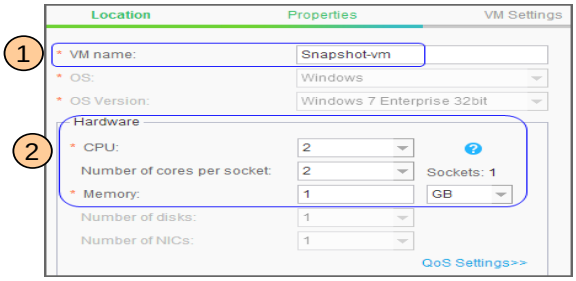



A cluster is a group of hosts.

- If there are no specific requirements for the location of a VM host, select **Cluster**. The system will select a suitable host in the cluster to create the VM on.
- To deploy the VM on a specified host, select **Host**. You can also check the box next to **Bind to Host** to bind the VM to the host.

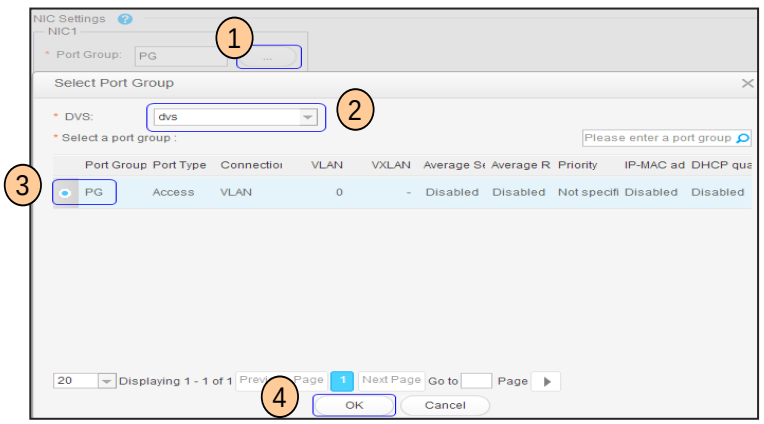
After the VM is bound to a host, the VM can only run on this host and cannot be migrated to another host.

4. Configure the template name and hardware specifications based on the obtained data, and click **Next**.




-

5. Select the port group to which the VM NIC belongs based on customer requirements on the network configuration of the template.

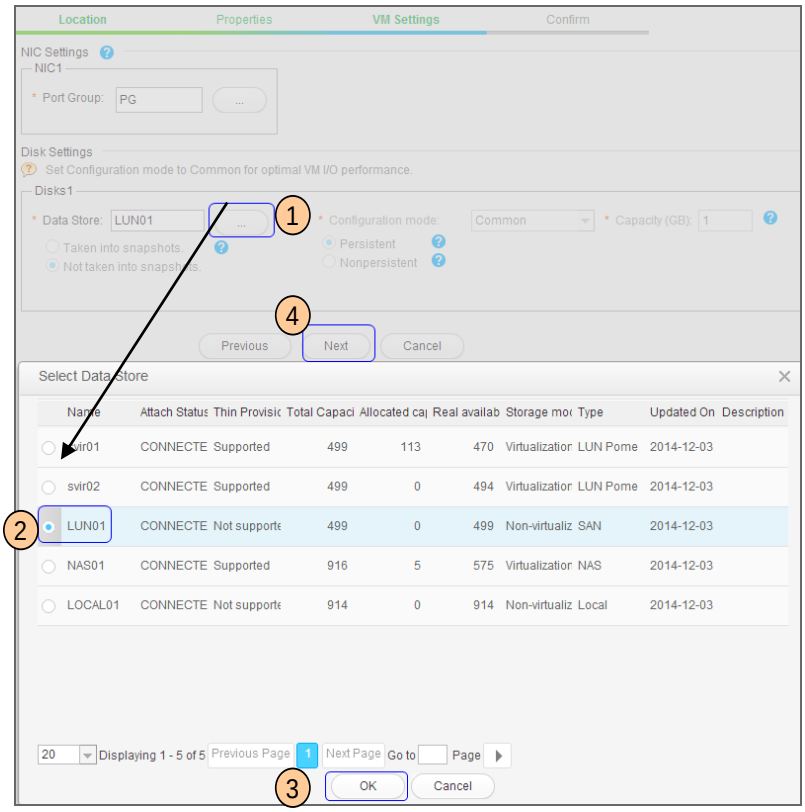



A **DVS** is similar to a switch used for communications on the layer 2 network. The DVS allows the VM to communicate with the physical network.

A **port group** is a logical port of the VM. The port group is used to define the mode the VM NIC uses to connect to the network.

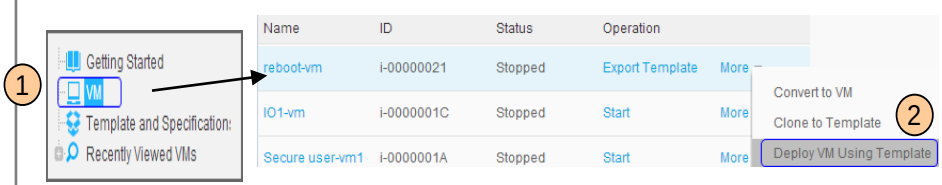
For details, see *Principles of VM Network Access*.

## Plan 2: Clone a VM to a Template

| | |
|---|---|
| 6. Configure disk attributes of the template based on obtained data. The parameters to be configured are shown as follows.<br>  <br> | (2) The storage resource pool associated with the host is used as the data store. The data store is used to create VM disks. For details, see *Principles of VM Storage Access*. |
| 7. Repeat the above procedure to configure attributes of other disks on the template. | |
| 8. Click **Next** after all disks are configured, confirm the configurations, and click **Finish**. | - |
| 9. Check whether the VM is successfully cloned to a template on the **Task Center** page. | - |

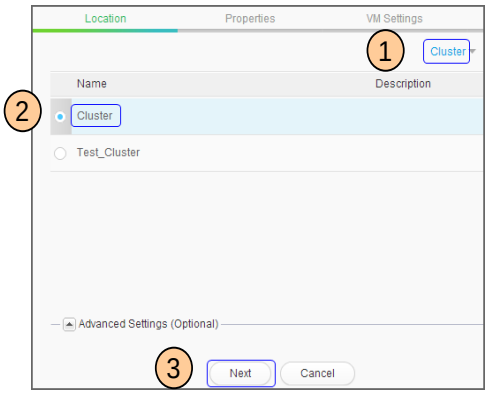
# 4.10 Create a VM Using the Template

## Step 1: Create a VM Using the Template

| | |
|---|---|
| 1. Locate the row that contains the template and choose **More > Deploy VM Using Template**.<br>  <br> | This starts the process of creating a VM using a template. |

## Step 1: Create a VM Using the Template

2. Select the VM creation location.

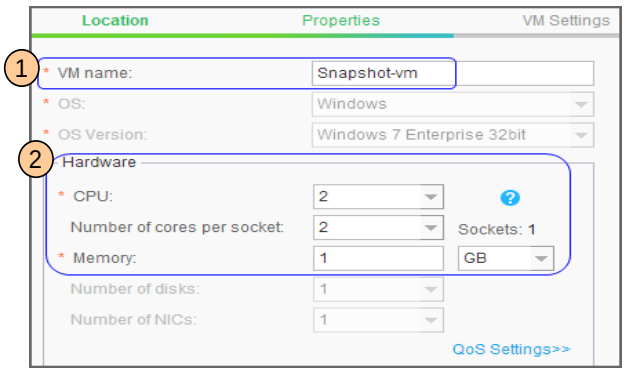



A cluster is a group of hosts.

- If there are no specific requirements for the location of a VM host, select **Cluster**. The system will select a suitable host in the cluster to create the VM on.
- To deploy the VM on a specified host, select **Host**. You can also check the box next to **Bind to Host** to bind the VM to the host.

After the VM is bound to a host, the VM can only run on this host and cannot be migrated to another host.

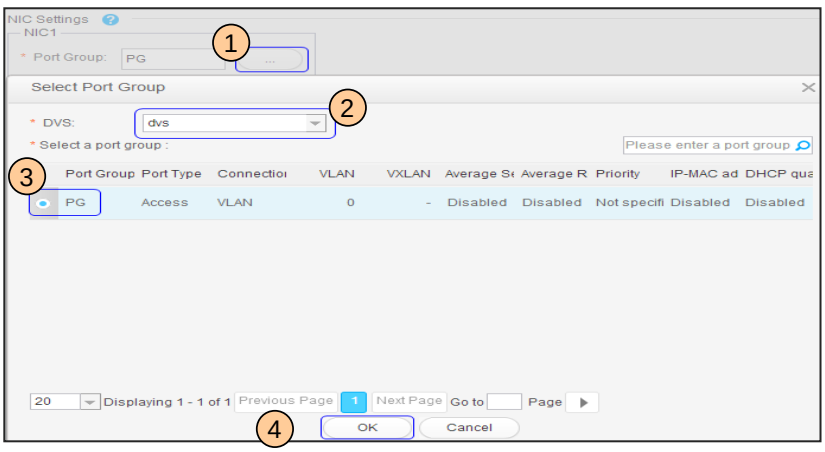
3. Configure the VM name and hardware specifications based on obtained data, and click **Next**.




- Use the default values for all other attributes configurations.
- You cannot set the number of disks or NICs when creating a VM using a template.
- After the VM is created, you can add disks and NICs to it.

## Step 2: Configure VM Network Attributes

1. Select the port group to which the VM NIC belongs based on customer requirements on the VM network configurations.

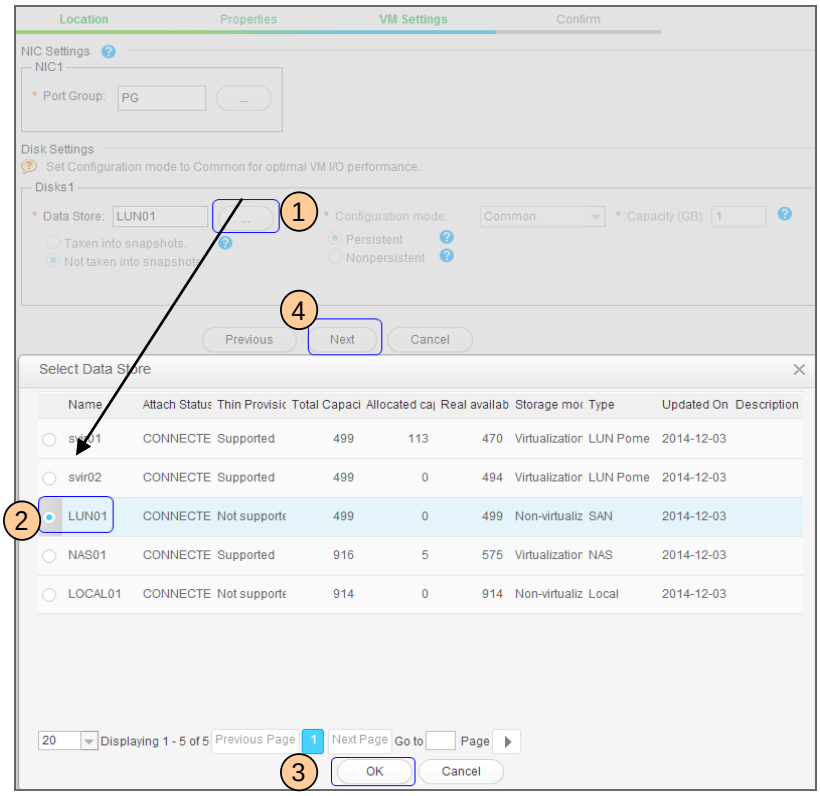



A **DVS** is similar to a switch used for communications on the layer 2 network. The DVS allows the VM to communicate with the physical network.

A **port group** is a logical port of the VM. The port group is used to define the mode the VM NIC uses to connect to the network.

For details, see *Principles of VM Network Access*.

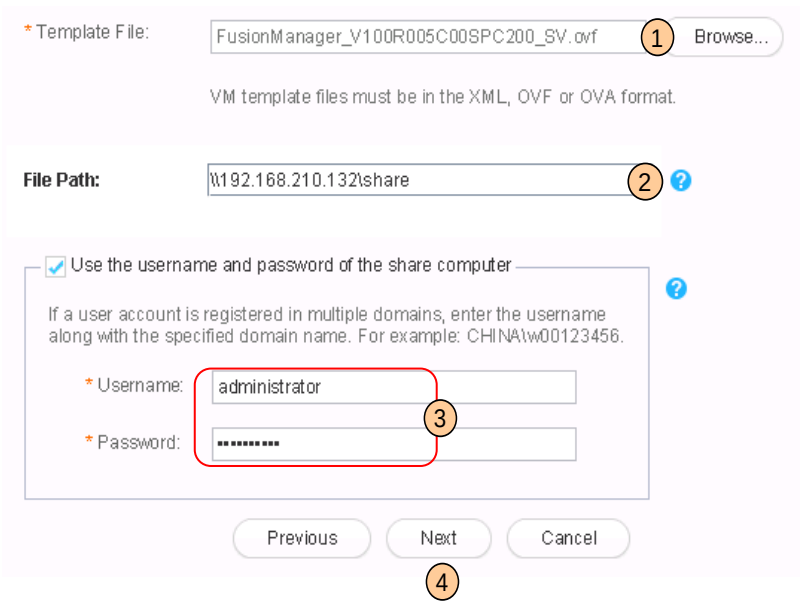
## Step 3: Configure VM Disk Attributes

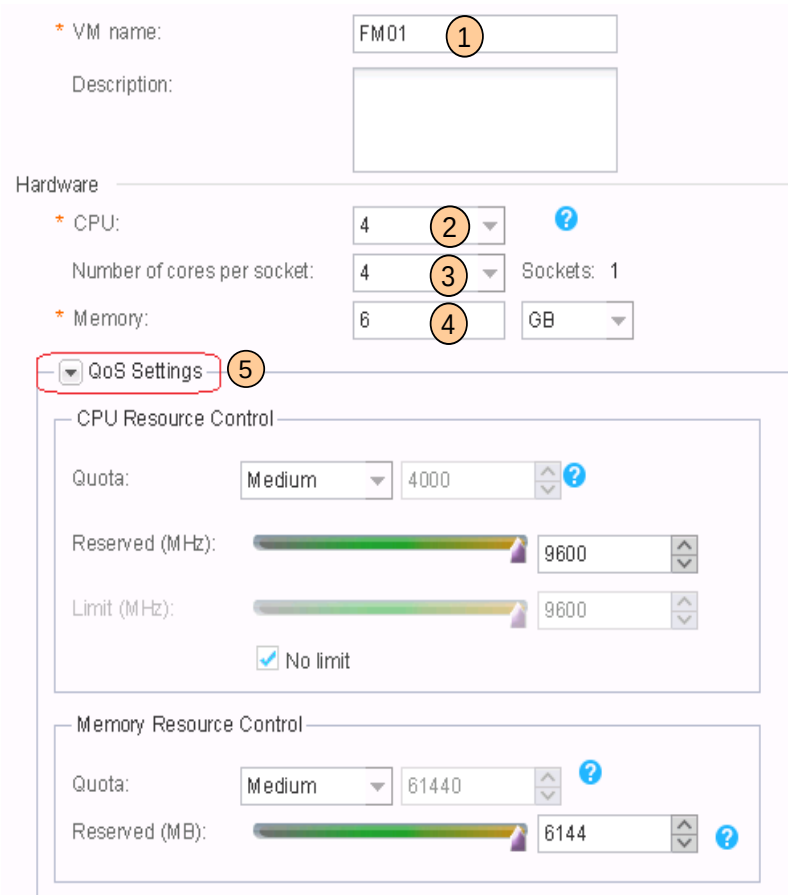
| | |
|---|---|
| 1. Configure the VM disk attributes based on the obtained data. The parameters to be configured are as follows:<br>  <br> | (2) The storage resource pool associated with the host is used as the data store. The data store is used to create VM disks. For details, see *Principles of VM Storage Access*. |
| 2. Repeat the above procedure to configure attributes of other disks on the VM. | |
| 3. Click **Next** after all disks are configured, confirm the configurations, and click **Finish**. | - |
| 4. Check whether the VM is successfully created on the **Task Center** page. | - |

# 5 Install FusionManager(Optional Task)

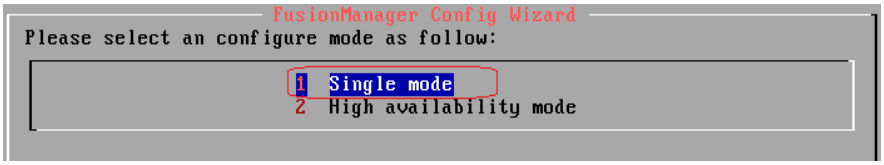
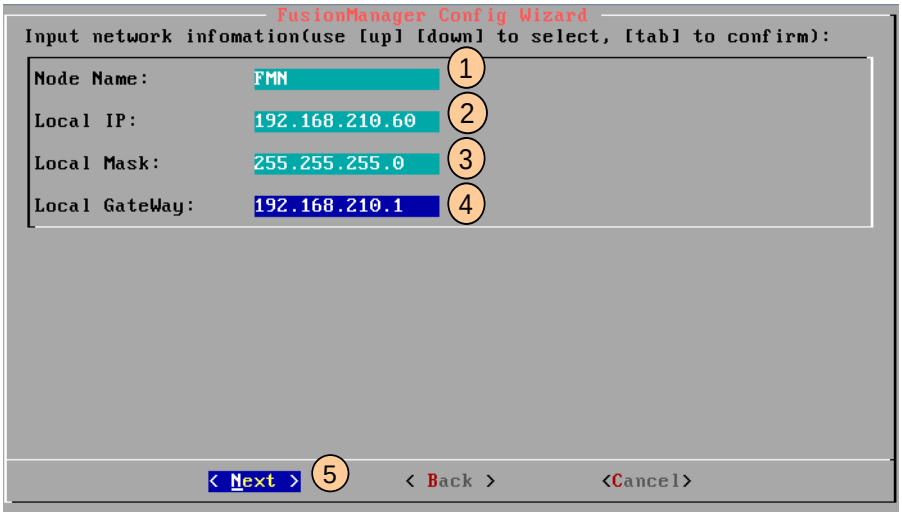
## 5.1 Install FusionManager Using a Template

| Step 1: Decompress the FusionManager installation package. | |
|---|---|
| 1. Create a folder named **share** on the local PC. | Ensure that the folder space is greater than 10 GB. |
| 2.Use 7-Zip to decompress the **FusionManager V100R005C00SPC200_SV.zip** file.<br>The **FusionManager V100R005C00SPC200_SV.7z** file is obtained. | N/A |
| 3. Use 7-Zip to decompress the **FusionManager V100R005C00_SV.7z** file. The following files are obtained:<br>• **FusionManager V100R005C00SPC200_SV.ovf**<br>• **FusionManager V100R005C00SPC200_SV-xvda.vhd** | |
| 4.Move the two files to the **share** folder, and share the folder with the current login user of the local PC. | The shared folder path cannot contain Chinese characters. |

| Step 2: Create a FusionManager VM on FusionCompute. | |
|---|---|
| 1. On FusionCompute, click **VM and Template.** | N/A |
| 2. Click **Import VM**. | |
| 3. Select **Shared directory**, then click **Next**. | |
| 4. Configure template information.<br>  <br> | 2 The path format is \\Local PC IP address\Name of the folder containing the template file.<br>3 If the user account is registered in multiple domains, enter the username with the specified domain name, for example, CHINA\w00123456. |
| 5. Set the creation location to **Host**. | |

| Step 2: Create a FusionManager VM on FusionCompute. | |
|---|---|
| 6. Click **Bind to the selected host** and select **Permanently reserve resources for the VM**. | |
| 7. Bind the FusionManager NIC to the DVS port group of the management plane. | |
| 8. Configure the data store and configuration mode (**Common** or **Thick provisioning lazy zeroed**) for the disk, and select **Persistency**.<br>The options **Persistent** and **Nonpersistent** are available for a VM disk only when the disk type is set to Common and the data store type is set to **Local Pome**, **LUN Pome**, or **NAS**. For such disks, set **Persistency** to **Persistent**. For disks using other types of storage resources, the **Persistency** attribute can only be **Persistent**, which is the default setting and not available for selection. | N/A |
| 9. Configure VM information.<br>  <br> | 3 This parameter is available if the cluster has the GuestNUMA function enabled. The CPUs of a VM can be divided into multiple groups. The one or multiple CPU cores in each group are provided by one or multiple cores of a physical CPU. The number of CPU cores in each group determines the number of CPU cores allowed in a socket. The number of sockets and the number of CPU cores allowed in a socket vary depending on the OS capabilities. Set this parameter based on the actual capability of the in-use OS. The VM CPUs are recommended to be evenly provided by the physical CPU.<br>5 In the **CPU Resource Control** area, move the **Reserved (MHz)** slider to the maximum value. In the **Memory Resource Control** area, move the **Reserved (MB)** slider to the required value. |
| 10. Keep the default values of other parameters, then click **Next**. | N/A |
| 11. Click **Create**.<br>The creation process takes about 40 minutes. | |

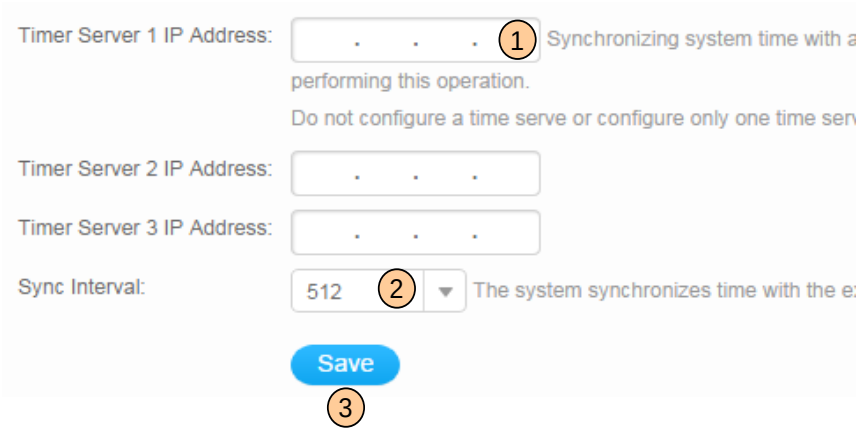
## 5.2 Configure FusionManager

| 1: Configure the FusionManager VM. | |
|---|---|
| 1. On FusionCompute, log in to the FusionManager VM using VNC.<br>The login username is **galaxmanager**, and the default password is **Huawei@CLOUD8**. | N/A |
| 2. Run the following command to disable user logout upon system timeout:<br>**TMOUT=0** | |
| 3. Run the following command to start the configuration wizard:<br>**fmconfig** | |
| 4. Select **OK** to enter the configuration wizard. | |
| 5. Select **Next** to enter the page for selecting the deployment mode. | N/A |
| 6. Select **Single mode**.<br>  | |
| 7. Select **Next**. | |
| 8. Configure FusionManager VM information.<br>  | N/A |
| 9. Confirm that the configuration information is correct, then select Next.<br>The system begins to configure the FusionManager VM. The configuration is successful when the progress reaches 100% and the system displays a **success** message. | If the entered configuration information is incorrect, run **stopALL** to stop the process and perform the configuration procedure again from running the **fmconfig** command. |

# 5.3 Configure Time Synchronization and Time Zone

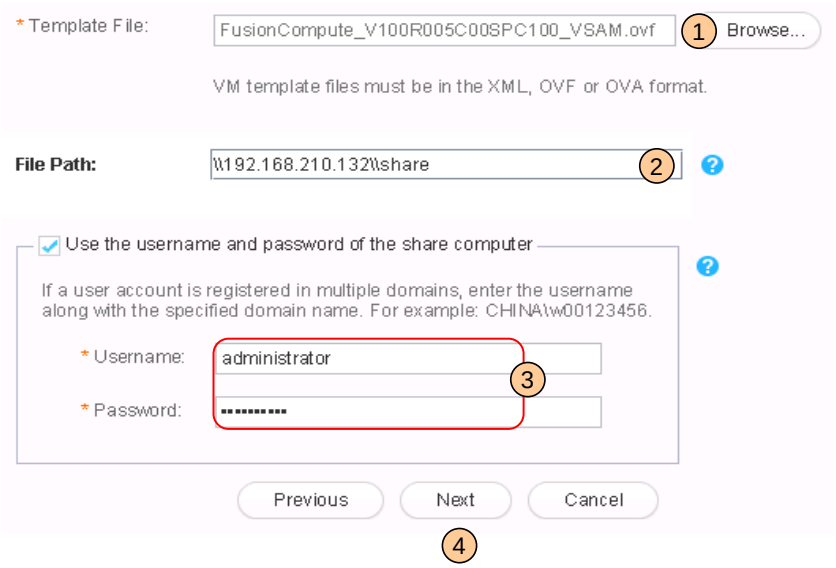
| Step 1: Log in to the FusionManager web client. | |
|---|---|
| 1. Enter the FusionManager management IP address in the address box, then press Enter.<br>The address format is http://FusionManager management node IP address, for example, http://192.168.210.60. | Internet Explorer 9 is recommended. |
| 2. If no security certificate has been installed, click Continue to this website (not recommended). | |
| 3. Enter the username and password. | Default username: admin<br>Default password: Huawei@CLOUD8! |
| 4. Enter the displayed verification code. | |
| 5. Click **Login**.<br>If the system displays a message indicating that the login password must be changed upon the first login or be reset, change the password as prompted. | |

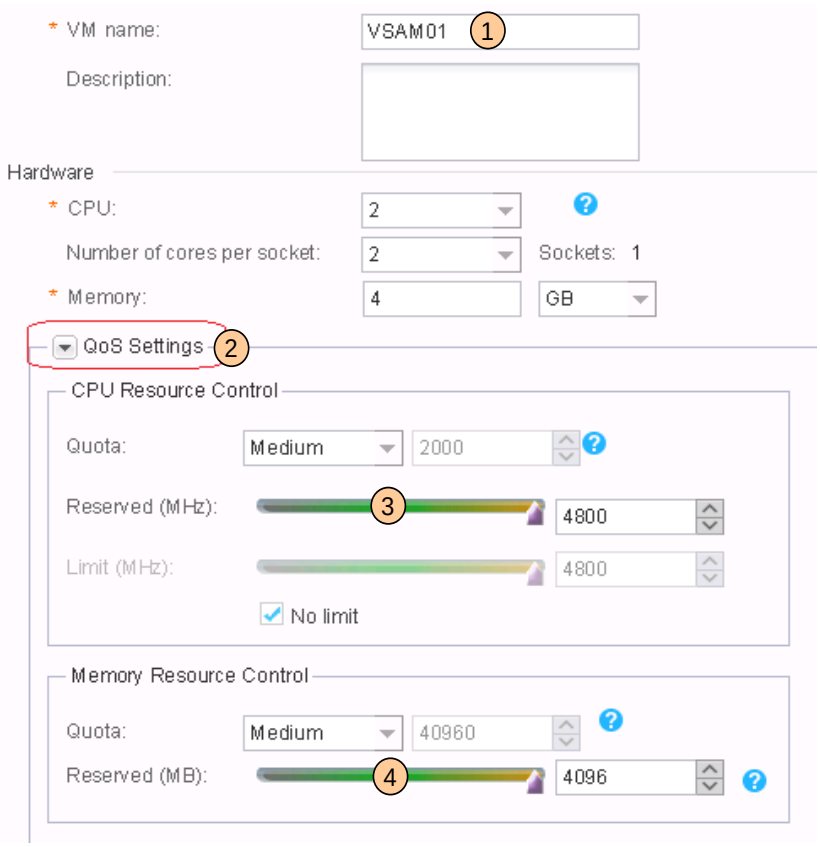
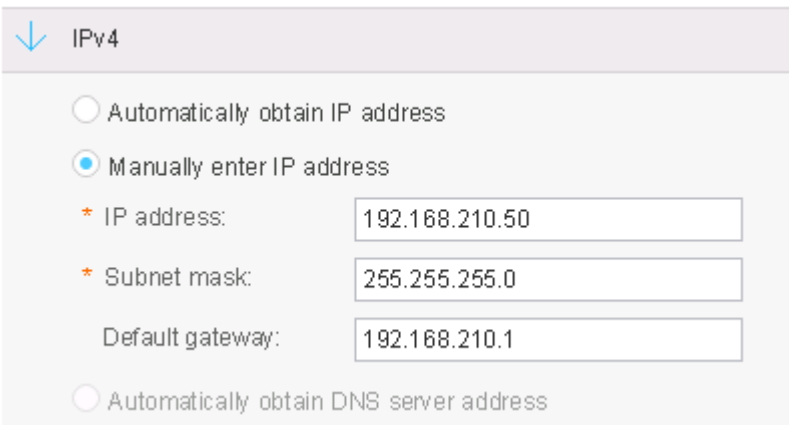
| Step 2: Configure the time zone. | |
|---|---|
| 1. On FusionManager, select **System**. | N/A |
| 2. Choose **System Configuration** > **Time Management**. | |
| 3. In the Time Zone area in the lower part of the page, check whether the current time zone is the same as the local time zone. If different, change the system time zone to the local time zone.<br>  | |

| Step 3: Configure the time server. | |
|---|---|
| 1. Configure the time synchronization function.<br>  | |

# 6 Install the VSAM VM(Optional Task)

| Step 1: Decompress the VSAM installation package. | |
|---|---|
| 1. Decompress the **FusionCompute V100R005C00SPC100_VSAM.zip** file. The following files are obtained:<br>• **FusionCompute_V100R005C00SPC100_VSAM.ovf**<br>• **FusionCompute_V100R005C00SPC100_VSAM-1.vhd** | N/A |
| 2. Create a folder named **share**, move the two files into the folder, and share the folder with the current login user of the local PC. | |

| Step 2: Create the VSAM VM on FusionCompute. | |
|---|---|
| 1. On FusionCompute, select **VM and Template.** | N/A |
| 2. Click **Import VM**. | |
| 3. Select **Shared directory**, then click **Next.** | |
| 4. Configure template information.<br>  | 2 The path format is \\Local PC IP address\Name of the folder containing the template file.<br>3 If the user account is registered in multiple domains, enter the username with the specified domain name, for example, CHINA\w00123456. |
| 5. Set the creation location to **Host**. | N/A |
| 6. Click **Bind to the selected host** and select **Permanently reserve resources for the VM**. | |
| 7. Configure the FusionManager NIC information on the management plane DVS and port group. | |
| 8. Configure the data store and configuration mode (**Common** or **Thick provisioning lazy zeroed**) for the disk, and select **Persistency**.<br>The options **Persistent** and **Nonpersistent** are available for a VM disk only when the disk type is set to Common and the data store type is set to **Local Pome**, **LUN Pome**, or **NAS**. For such disks, set **Persistency** to **Persistent**.<br>For disks using other types of storage resources, the **Persistency** attribute can only be **Persistent**, which is the default setting and not available for selection. | |

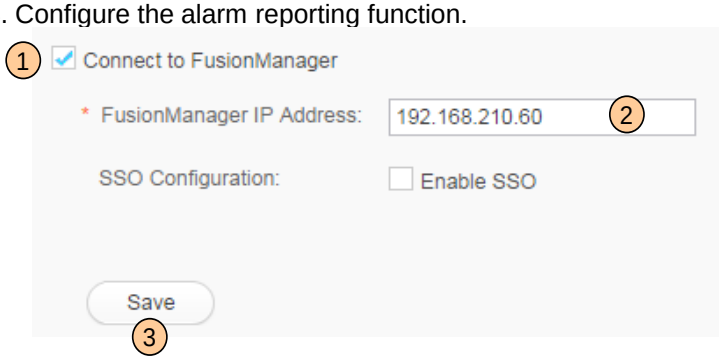
| | |
|---|---|
| 9. Configure VM information.<br>  <br> | 3 In the **CPU Resource Control** area, move the **Reserved (MHz)** slider to the maximum value.<br>4 In the **Memory Resource Control** area, move the **Reserved (MB)** slider to the required value. |
| 10. Keep the default values of other parameters, select **Customize using the Customization Wizard**, then click **Next**. | N/A |
| 11. Enter the VSAM VM name, leave **Save as computer attributes** unchecked, and click **Next**. | |
| 12. Configure VSAM VM NIC information.<br>  <br> | N/A |
| 13. Click **Next**. | N/A |
| 14. Confirm that the entered information is correct, then click **Create**.<br>The creation process takes about 20 minutes. | |

| Step 3: Configure the NTP server and time zone. | |
|---|---|
| 1. On FusionCompute, log in to the VSAM VM as user **root** using VNC.<br>The default **root** user password is **Huawei@CLOUD8!**. | |
| 2. Run the following command to disable user logout upon system timeout:<br>**TMOUT=0** | |
| 3. Run the following command to enter the configuration interface:<br>**python /opt/galax/vsam/tomcat/script/configvsam/ConfigVSAM.py**<br>The following information is displayed:<br>START TO CONFIG VSAM !<br>please input the user gesysman's password[q/Q]:<br>Password: | N/A |
| 4. Enter the **gesysman** user password, which is **GeEnginE@123** by default.<br>The following information is displayed:<br>**********<br>* please choose your operation: *<br>* SET HA : 0 *<br>* SET NTP : 1 *<br>* SET FTP : 2 *<br>* SET Time Zone : 3 *<br>* SHOW ALL : 4 *<br>* SHOW HA : 5 *<br>* SHOW NTP : 6 *<br>* SHOW FTP : 7 *<br>* SHOW Time Zone : 8 *<br>* EXIT : 9 *<br>**********<br>please input your choice[0~9]: | N/A |
| 5. Enter **1**, then press **Enter**. | |
| 6. Enter the NTP server IP address, then press **Enter**.<br>start to config ntp !<br>please input the ntp ip address: | Configure the NTP clock source preferentially to the same external clock source used by both FusionCompute and FusionManager. If no external NTP clock source is available, configure the clock source to the host running the active VSAM VM. |
| 7. Press **Enter**, set the synchronization interval (default: 64s), then press **Enter**. | |
| 8. Enable forcible clock synchronization (which is disabled by default), then press **Enter**. | |
| 9. Configure the NTP network bridge address (which is not configured by default), then press **Enter**. | |
| 10. Confirm that the entered information is correct, then press **Enter**.<br>The system begins to configure the NTP server. | |
| 11. Enter **3** and press **Enter** to configure the time zone.<br>start to config time zone info !<br>please input the time zone info [example:Asia/Hong_Kong]:<br>For more information about time zone, please refer to the following directory :/usr/share/zoneinfo | N/A |
| 12. Enter the time zone, then press **Enter**. | |
| 13. Confirm that the entered information is correct, then press **Enter**. | |

# 7 Configure the Alarm Reporting Function

After installing FusionCompute, FusionManager, and VSAM, configure the function that allows FusionCompute and VSAM to report alarms to FusionManager.

| Step 1: Log in to FusionCompute. | |
|---|---|
| 1. Enter http://*VRM IP address*, for example, http://192.168.210.30, in the address box, then press **Enter**. | Internet Explorer 9 is recommended. |
| 2. Enter the username and password and set the user type and login type. | |
| 3. Click **Login**. | |

| Step 2: Configure the FusionCompute alarm reporting function. | |
|---|---|
| 1. On FusionManager, select **System**. | N/A |
| 2. Choose **Connect To** > **FusionManager**. | |
| 3. Configure the alarm reporting function.<br>  | 2 Set it to the FusionManager management IP address if only one FusionManager VM is deployed. |

**Note:** Before configure the alarm reporting function, enable port 18080 to allow VSAM to report alarms to FusionManager. However, port 18080 is based on the insecure protocol HTTP. Therefore exercise caution when deciding to enable this port.

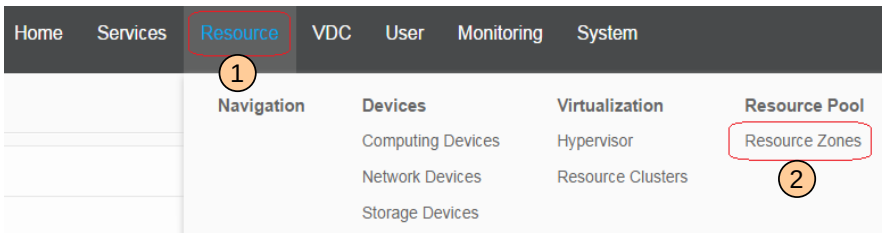
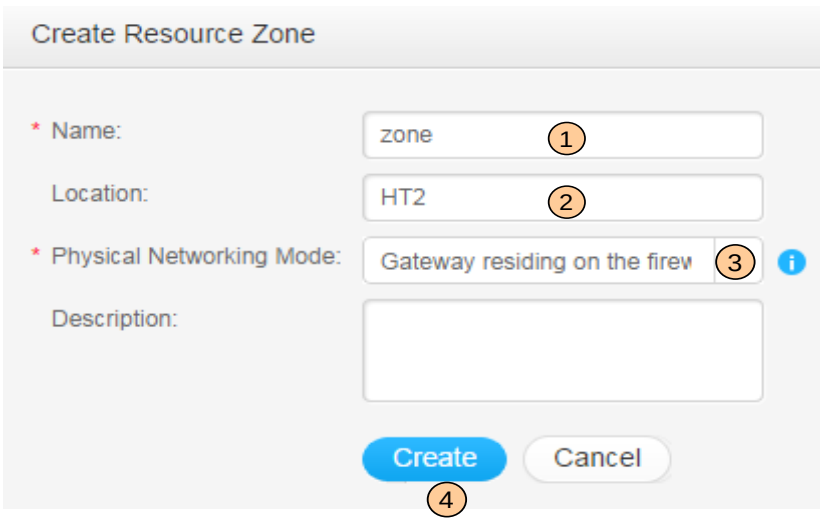
| Step 3: Configure the VSAM alarm reporting function. | |
|---|---|
| 1. On FusionCompute, log in to the VSAM VM as user root using VNC.<br>The default **root** user password is **Huawei@CLOUD8!**. | N/A |
| 2. Run the following command to disable user logout upon system timeout:<br>**TMOUT=0** | |
| 3. Run the following command to query whether port 18080 is disabled.<br>**iptables -S\|grep 18080**<br>If the following command output is displayed, the port is enabled. Go to Step 5.<br>`-A VSAM_INPUT_CONTROL -p tcp -m multiport --dports 18080 -j ACCEPT`<br>If no command output is displayed, the port is disabled. Go to Step 4. | |
| 4. Run the following command to enable port 18080:<br>**sh /opt/galax/vsam/tomcat/script/setVsamHttpPort.sh open**<br>If the following command output is displayed, the port is successfully enabled:<br>`modify config file success` | N/A |
| 5. Run the following command to configure the function that allows VSAM to report alarms to FusionManager in real time:<br>**sh /opt/galax/vrm/om/fms/bin/modGMIp.sh** *FusionManager management IP address*<br>The configuration is successful if the following information is displayed:<br>`modify GM IP Success.....` | N/A |

# 8 Add Resources to FusionManager

## 8.1 Create resource zones.

A resource zone is a logical container of resources virtualized in the hypervisor. Resources in a resource zone belong to an independent layer 2 network and are managed as resource pools, including computing resource pool, storage resource pool, and storage resource pools.

| **Step 1: Log in to the FusionManager .Web Client.** | |
|---|---|
| 1. In the address bar of Internet Explorer, enter http://*FusionManager management IP address*, press **Enter**, then select **Continue to this website (not recommended)** to switch to the FusionManager Web Client login page.<br>For example, enter http://192.168.210.60. | This task uses Internet Explorer 9.0 as an example. |
| 2. Log in to FusionManager as user **admin**.<br>The default password of user admin is **Huawei@CLOUD8!**.<br>After logging in to FusionManager for the first time, you need to change the login password as requested. | N/A |

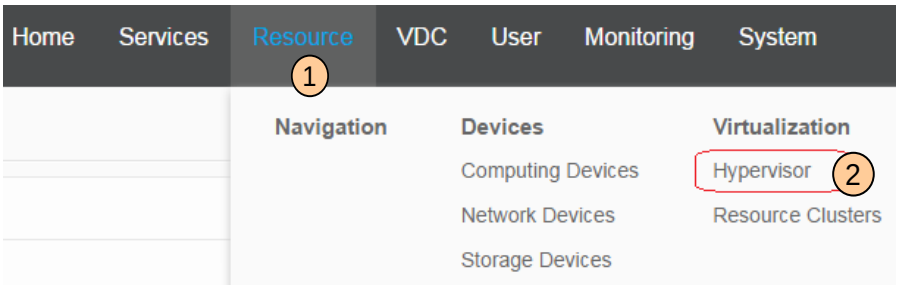
| **Step 2: Create a resource zone.** | |
|---|---|
| 1. On FusionManager, go to the **Resource Zones** page.<br>  | N/A |
| 2. Click **Create** on the displayed page. | |
| 3. Configure zone information.<br>  | (3) In this task, a software VSA node functions as the gateway of the service network, and no physical networking is required. Therefore, use the default physical networking mode. |

## 8.2 Add the Hypervisor to FusionManager

Add FusionCompute and VSAM to FusionManager so FusionManager can manage resources in the hypervisor.

### Step 1: Add the hypervisor to FusionManager.

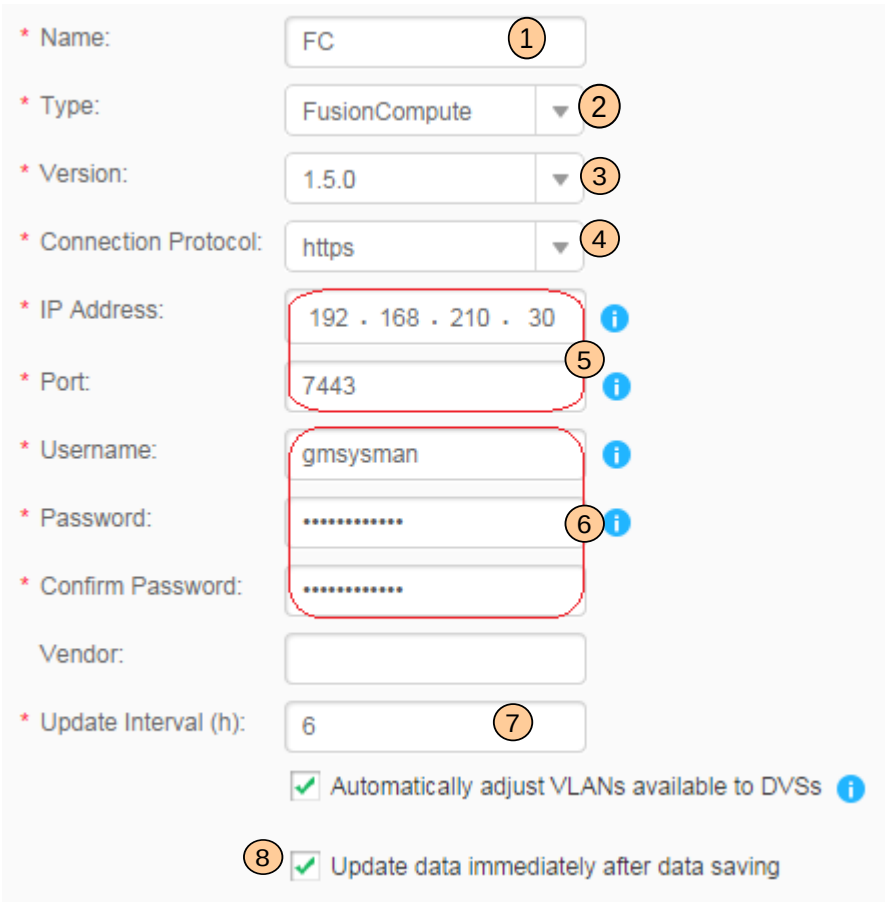
1. Switch to the **Hypervisor** page.




-

2. Click **Add** on the hypervisor page.

3. Configure the hypervisor access information.

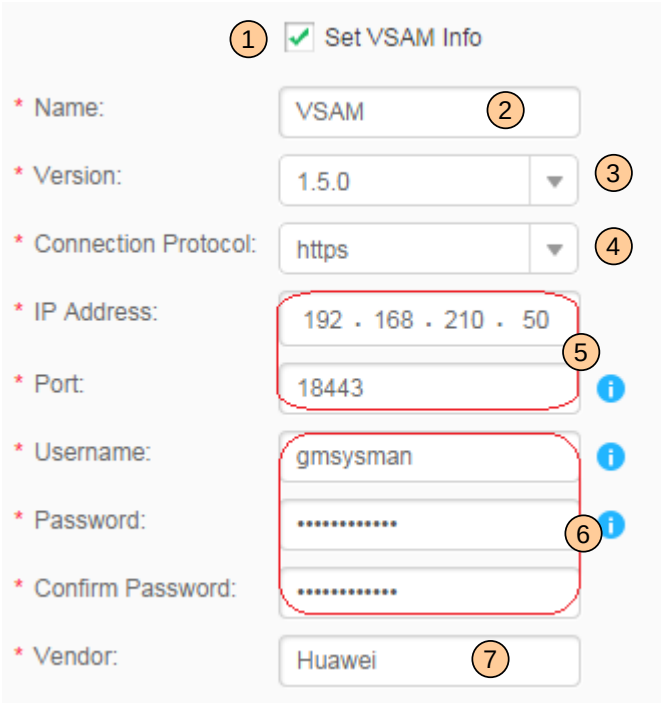



5 If only one VRM node is deployed, enter the VRM management IP address and the default port number 7443.

6 Enter the name for connecting the hypervisor to FusionManager. The default username for connecting the FusionCompute hypervisor is **gmsysman**, and the default password is **GMEnginE@123**.

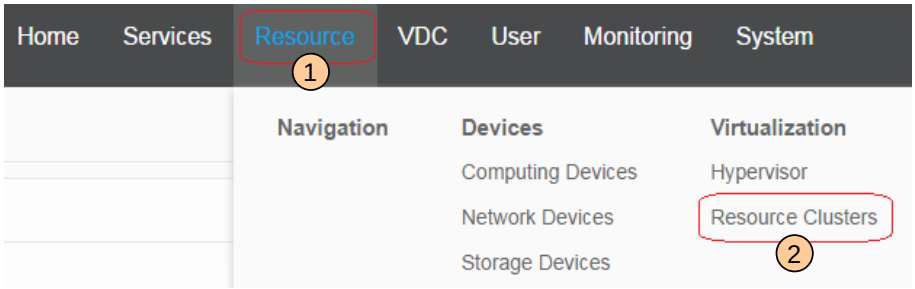
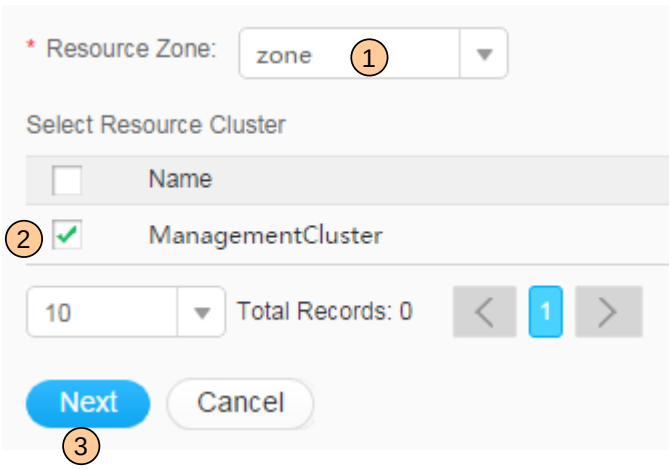
8 If **Update data immediately after data saving** is not checked, the system automatically updates the hypervisor data periodically (every six hours) to ensure data consistency between FusionManager and the hypervisor.

4. Click **Next.**

| Step 2: Add VSAM to FusionManager. | |
|---|---|
| 1. Configure VSAM access information.<br>  <br> | 5 If only one VSAM node is deployed, enter the VSAM management IP address and the default port number 18443.<br>6 The default username for connecting VSAM to FusionManager is **gmsysman**, and the default password is **GMEnginE@123**. |
| 6. Click **Next.** | N/A |
| 7. Confirm that the entered information is correct, then click **Add.** | |

## 8.3 Associate the Resource Cluster with a Resource Zone

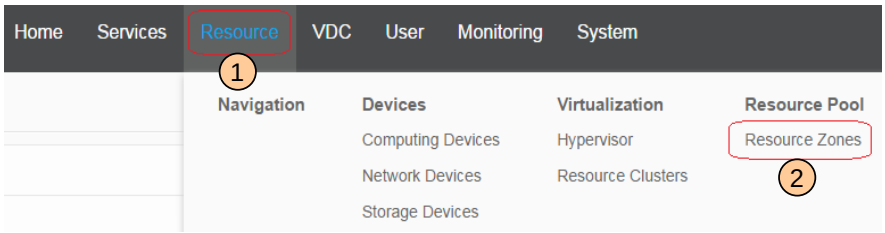
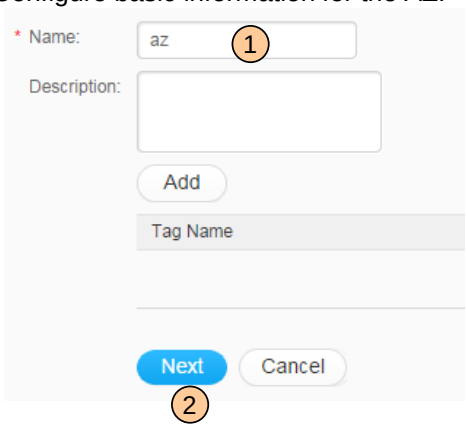
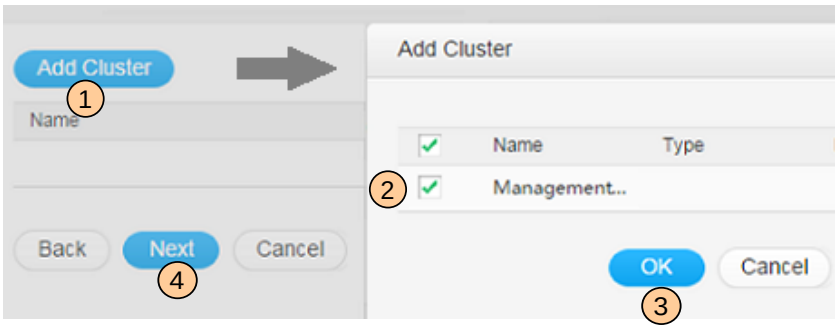
Associate the resource cluster in the added hypervisor with a resource zone in FusionManager, so the computing, storage, and DVS resources virtualized in the hypervisor are added to the computing, storage, and network resource pools in FusionManager, respectively.

| Step 1: Associate the resource cluster with a resource zone in FusionManager. | |
|---|---|
| 1. Go to the **Resource Clusters** page.<br>  | N/A |
| 2. Click **Associate**. | |
| 3. Associate the added resource cluster with a resource zone.<br>  | N/A |
| 4. Click **OK.** | |

## 8.4 Create AZs.

An availability zone (AZ) is a collection of logical resources that can be allocated to users.

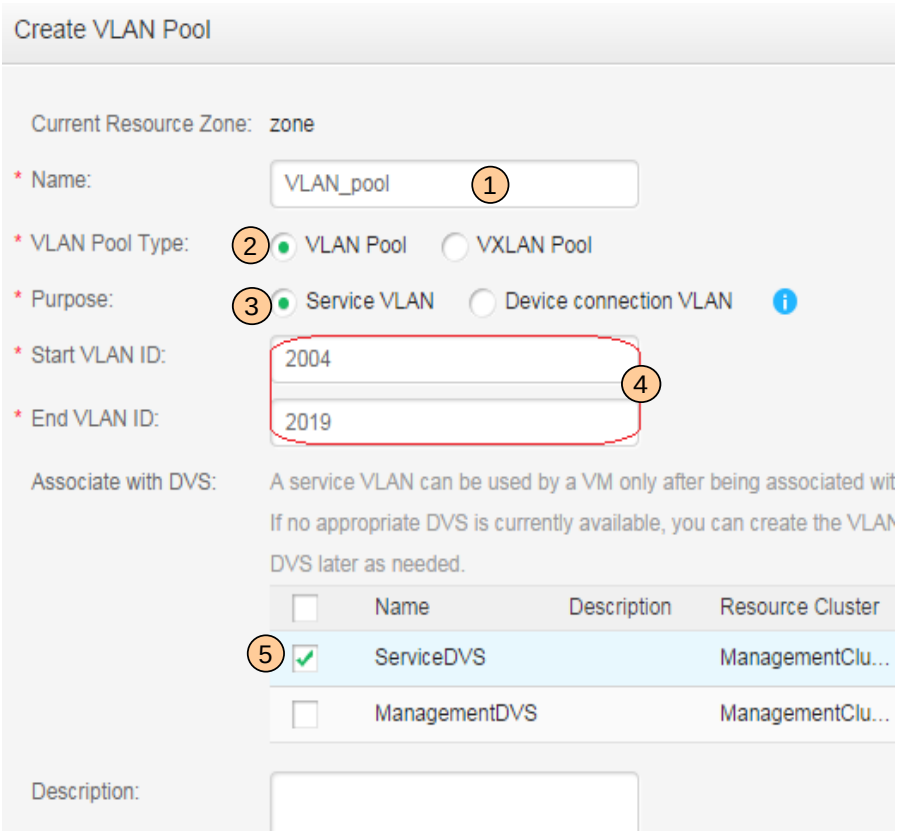
### Step 1: Create an AZ.

| | |
|---|---|
| 1. Go to the **Resource Zones** page.<br>  <br> | N/A |
| 2. Click the name of the target resource zone.<br>The Summary page for the resource zone is displayed. | |
| 3. Select **Availability Zones.** | |
| 4. Click **Create**. | |
| 5. Configure basic information for the AZ.<br>  <br> | N/A |
| 6. Add resource clusters to the AZ.<br>  <br> | The resource clusters contained in an AZ must be provided by the same hypervisor. |
| 7. Confirm that the entered information is correct, then click **Add**. | |

# 9 Configure Resource Pools

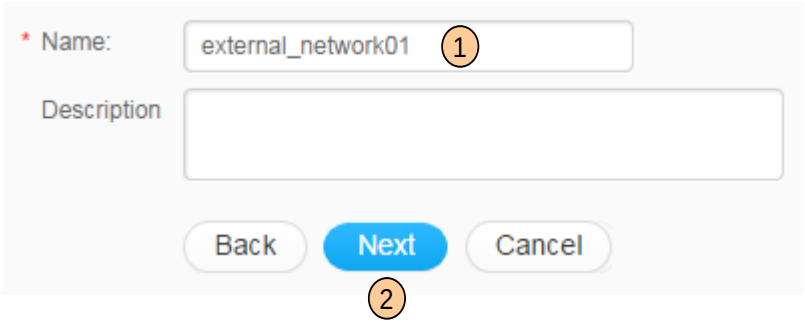
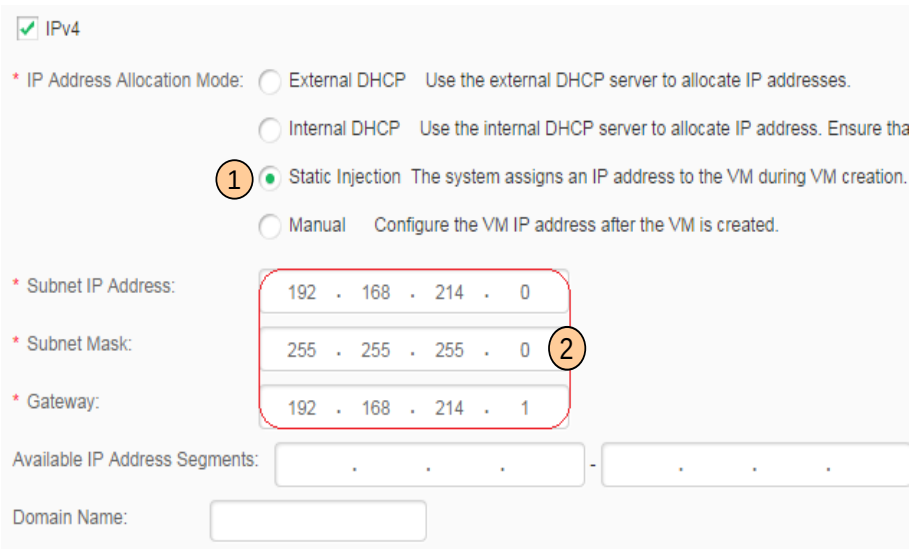
## 9.1 Add a VLAN Pool

To create service networks (external networks, internal networks, and routed networks) on FusionManager, the VLANs used by these networks must be first added to the VLAN pools in FusionManager. Then FusionManager can manage and allocate VLAN resources to the requested service networks in a unified manner. VLAN pools in FusionManager are available only after being associated with the DVSs.

| **Step 1: Add a VLAN pool.** | |
|---|---|
| 1. On FusionManager, choose **Resource** > **Resource Zones**, select a resource zone, then choose **Network Resource Pools** > **VLAN Pools**. | N/A |
| 2. Click **Create**. | |
| 3. Configure the VLAN pool information.<br>  | 4 Enter the service plane VLAN range configured on the switch. |
| 4. Click **Create**. | |

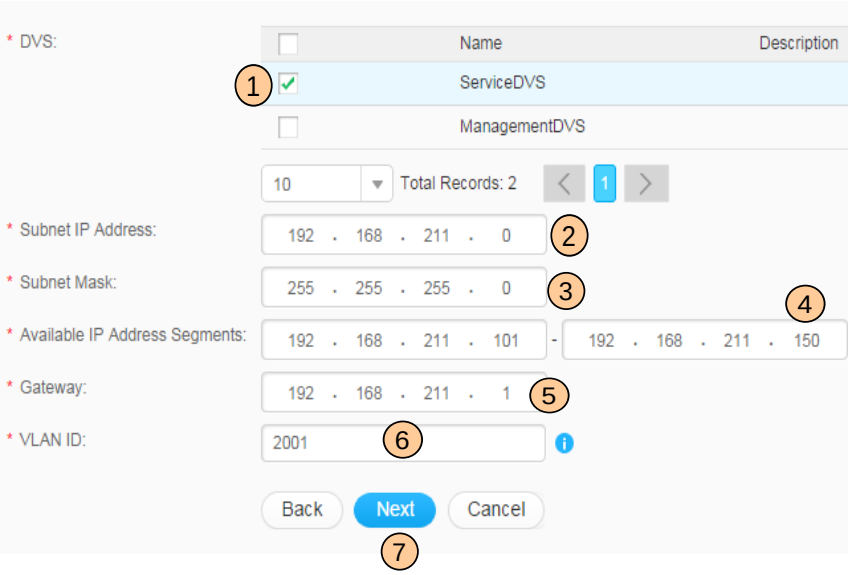
## 9.2 Create an External Network

Add an existing network that is connected to the Internet as the external network. After the external network is added to FusionManager, FusionManager can manage the public IP addresses in the network and provide public IP addresses for VMs to connect to the Internet through the software router.

| Step 1: Create an external network. | |
|---|---|
| 1. On FusionManager, choose **Resource** > **Resource Zones**, select a resource zone, and choose **Network Resource Pools** > **External Networks**. | N/A |
| 2. Click **Create.** | |
| 3. Set **Connection Mode** to **Subnet (common VLAN)** and **Connect to Internet** to **Yes.** | |
| 4. Enter the external network name.<br>  | N/A |
| 5. Select the required DVS, then click **Next.** | Select the DVS with which the external network VLAN is associated. |
| 6. Enter the external network VLAN, then click **Next.** | |
| 7. External subnet information for the external network.<br>  | N/A |
| 8. Click **Next**. | |
| 9. Use the default QoS settings, then click N**ext.** | N/A |
| 10.Confirm that the entered information is correct, then click **Create**. | |

## 9.3 Create a VSA Management Network

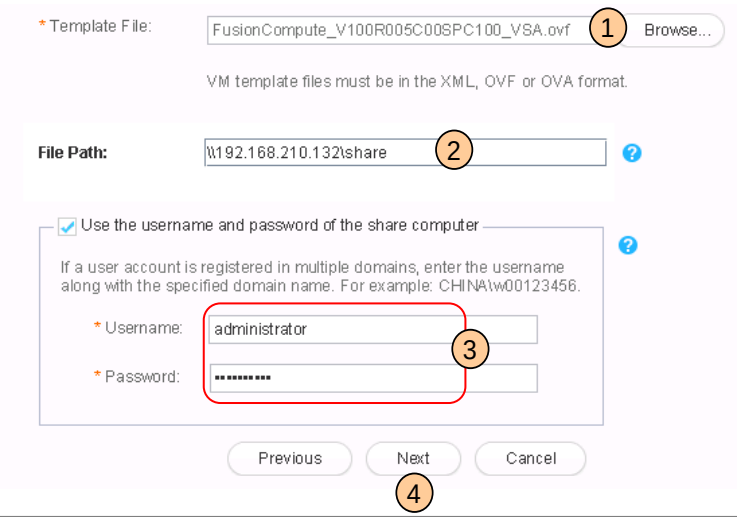
The VSA management network communicates with the system management plane and assigns IP addresses for system service VMs, such as the software router VM and internal DHCP server VM, so the system service VMs can communicate with the VSAM and FusionManager nodes.

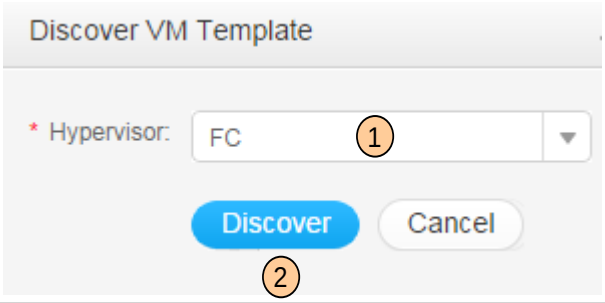
| **Step 1: Add a VSA management network.** | |
|---|---|
| 1.On FusionManager, choose **Resource** > **Resource Zones**, select a resource zone, and choose **Network Resource Pools** > **VSA Network**.<br>2. Click **Create VSA Management Network**. | N/A |
| 4. Enter the external network name.<br>  | N/A |
| 5. Configure the VSA management network.<br>  | 6 Ensure that the VLAN of the VSA management network has been added to the DVS in the hypervisor (FusionCompute) and the VLAN is not contained in the FusionManager VLAN pool. |
| 9. Remain the default settings for network port rate limit, then click **Next**.<br>10. Confirm that the entered information is correct, then click **Create**. | N/A |

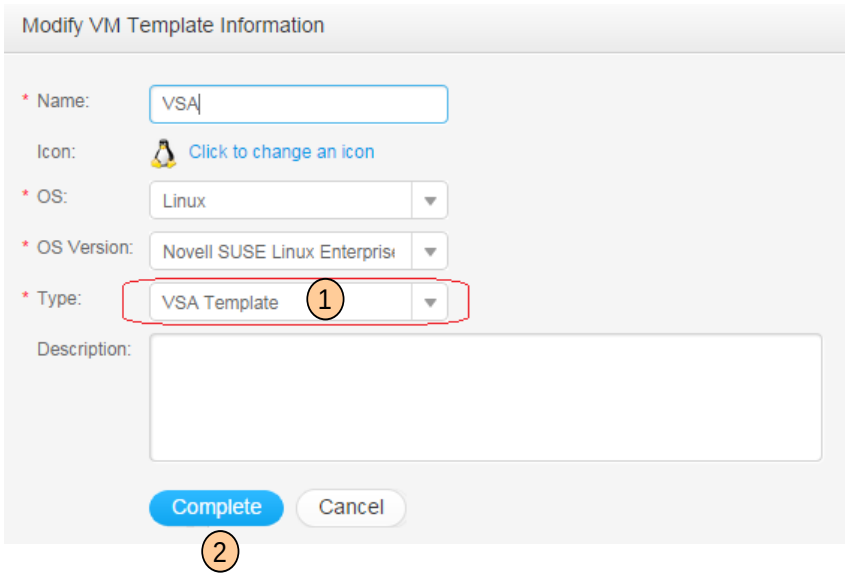
# 10 Prepare a VM Template

## 10.1 Import a VSA VM Template

The VSAM template is a system service VM template. When a tenant applies for a software router, the system uses the imported VSA VM template to automatically create a system service VM functioning as a software router for the tenant.

| Step 1: Import a VSA VM template to FusionCompute. | |
|---|---|
| 1.Decompress **FusionCompute V100R005C00SPC100_VSA.zip** on the local PC.<br>The following files are obtained:<br>• FusionCompute_V100R005C00SPC100_VSA.ovf<br>• FusionCompute_V100R005C00SPC100_VSA-1.vhd | N/A |
| 2.Create a new folder, move the two files to the folder, and share the folder with the current user of the local PC. | |
| 3. Log in to FusionCompute. | |
| 4. On FusionCompute, choose **VM and Template**. | |
| 5. Click **Import Template**. | |
| 6. Select **Shared directory**, then click **Next**. | |
| 7.Configure the template information.<br>  | 3 Enter the username and password for logging in to the local PC. |
| 8. Select the creation location, then click **Next**. | N/A |
| 9.Configure the data store and configuration mode for the VM disks, then select **Persistent**.<br>You are advised to deploy the VSA VM using a shared storage resource. Otherwise, deploying the VSA VM concurrently in multiple clusters may fail. | |
| 10.Remain the default values of other parameters, then click **Next**. | |
| 11.Enter the name of the VSA VM template. | N/A |
| 12.Remain the default values of other parameters, then click **Next**. | |
| 13.Confirm that the entered information is correct, then click **Finish**.<br>The creation process takes about 10 minutes. | |

| Step 2: Discover the VSA template on FusionManager. | |
|---|---|
| 1. Log in to FusionManager. | |
| 2. Choose **Resource** > **VM Templates**. | |
| 3. Click **Discover**. | |
| 4. Discover the VM template available in the hypervisor.<br>  | |
| 5. Click **OK**. | |

| Step 3: Change the VM template type. | |
|---|---|
| 1. Locate the row that contains the discovered VSA template, then choose **More** > **Modify VM Template Information**. | |
| 2. Change the template type.<br>  | |

## 10.2 Create a VM Template

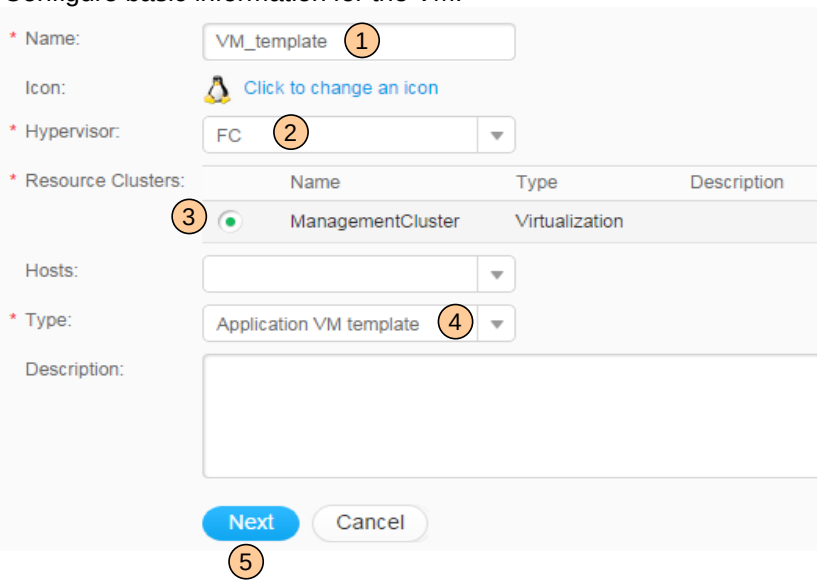
Create a VM template based on the OS type and VM specification requirements of the needed VMs. The template can then be used to create new VMs with the same specifications as the template, which significantly shortens the time for configuring new VMs and installing OSs on them.

### Step 1: Create a VM template.

1. On FusionManager, choose **Resources** > **VM Templates**.

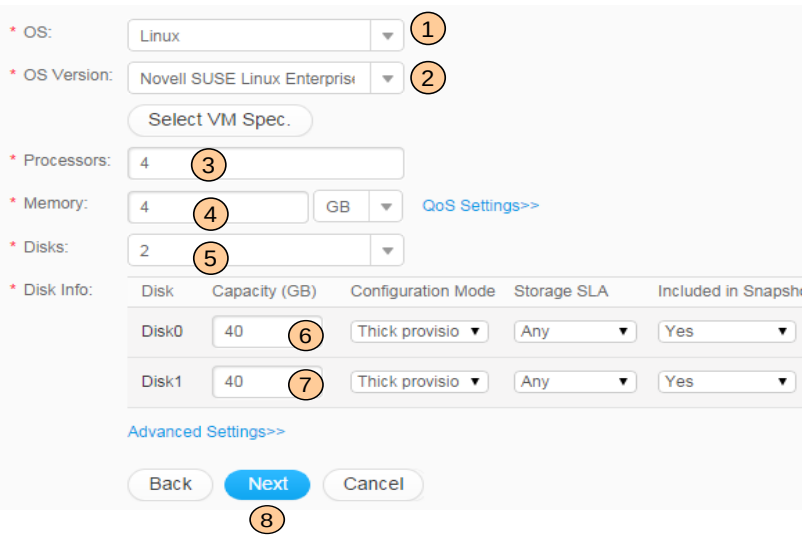
2. Click **Create**.

3. Configure basic information for the VM.



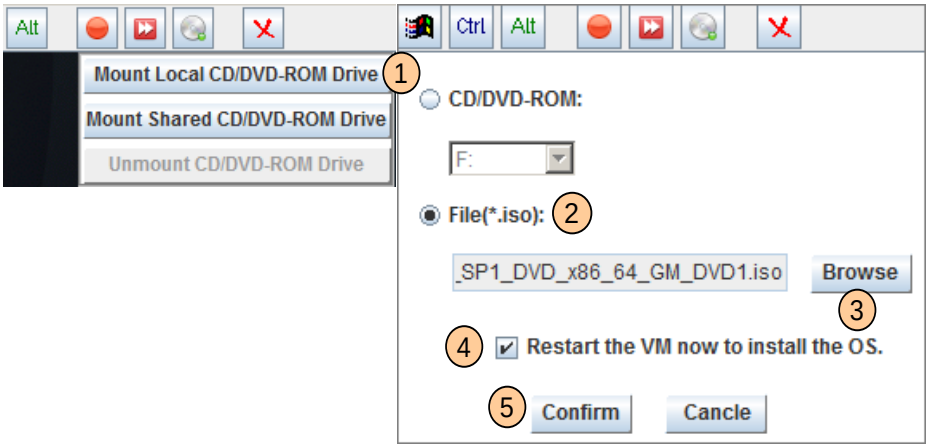

**Note**: FusionManager does not support VM template creation if it uses local disks as storage resources.

4. Configure the VM template specifications.




5. After the VM is created, click **Next**.

The **Install Software** page is displayed. On this page, you can log in to the VM using VNC and install an OS and Tools and configure NICs and disks for the VM.

| Step 2: Install an OS for the VM. | |
|---|---|
| 1. Click  on top of the VNC window and mount the OS CD/DVD-ROM drive or ISO image file to the VM.<br>  | SUSE Linux Enterprise Server 11 is used as an example in this task. |
| 2. After the VM restarts, install the OS on the VM as prompted.<br>The OS installation method for a VM is similar to that for a physical computer. | **Note:** Do not close the VNC login window before OS installation is complete. Otherwise, the CD/DVD-ROM drive is automatically unmounted from the VM |
| 3. After the OS is installed, click  on the top of the VNC window, then select **Unmount CD/DVD-ROM Drive**. | |
| 4. Install the OS patch. The patch file must be mounted to the VM as an ISO file. | N/A |

| Step 3: Disable the firewall on the VM. | |
|---|---|
| 1. Log in to the VM as user **root**. | |
| 2. On the VM desktop, choose **Computer** > **YaST**.<br>The **YaST2 Control Center** window is displayed. | |
| 3. Select **Security and Users** from **Groups** and click **Firewall** in the right pane. The **YaST2** window is displayed. | |
| 4. Select **Disable Firewall Automatic Starting** from **Start-Up** and click **Stop Firewall Now**. | |
| 5. Click **Save Settings and Restart Firewall Now**. | |
| 6. Click **Next**.<br>A confirmation dialog box is displayed. | |
| 7. Click **Yes**.<br>A confirmation dialog box is displayed. | |
| 8. Click **Finish**.<br>The **YaST2** window is closed. | |
| 9. Right-click the VM desktop and choose **Open in terminal** from the shortcut menu.<br>The system switches to the CLI. | |
| 10. Run the **reboot** command to restart the VM. | |

| Step 4: Install Tools. | |
|---|---|
| 1.Decompress the FusionCompute V100R005C00SPC100_GuestOSDrivers.zip software package on the local PC.<br>The **FusionCompute V100R005C00_GuestOS.iso** file is obtained. | |
| 2.Use VNC to log in to the VM as user **root** and mount the ISO image **FusionCompute V100R005C00SPC100_GuestOS.iso** to the VM. | |
| 3.Right-click on the VM desktop and select Open in terminal from the shortcut menu.<br>The system switches to the CLI. | |
| 4.Run the following command to create the **xvdd** directory:<br>**mkdir xvdd** | |
| 5.Run the following command to mount the ISO image to the VM:<br>**mount** *Target directory* **xvdd**<br>For example, run **mount /dev/sr0 xvdd** to mount the ISO file to the **/dev** directory on the VM running SUSE Linux Enterprise Server 11. | |
| 6.Run the following command to switch to the **xvdd/pvDriver/linux** directory:<br>**cd xvdd/pvDriver/linux** | |
| 7.Run the following command to view the required Tools installation package:<br>**ls**<br>The following information is displayed:<br>...<br>uvp-tools-linux-xxx.tar.bz2<br>uvp-tools-linux-xxx.tar.bz2.sha256 | Tools improve I/O processing, hardware monitoring, and other advanced functions on a VM. |
| 8.Run the following commands to copy the Tools installation package to the **root** directory:<br>**cp** *uvp-tools-linux-xxx.tar.bz2* **/root**<br>**cd /root** | |
| 9.Run the following command to decompress the Tools software package:<br>**tar -xjvf** *uvp-tools-linux-xxx.tar.bz2* | |
| 10.Run the following command to switch to the Tools installation directory:<br>**cd** *uvp-tools-linux-xxx* | |
| 11.Run the following command to install Tools:<br>**./install**<br>Tools installation is complete if the following command output is displayed:<br>The PV driver is installed successfully. Reboot<br>the system for the installation to take effect. | |
| 12. Run the following command to restart the VM for Tools to take effect:<br>**reboot** | |
| 13.Use VNC to log in to the VM as user **root** again. | N/A |
| 14.Right-click the VM desktop and choose **Open in terminal** from the shortcut menu. | |
| 15.Run the following command to check whether Tools installation is successful:<br>**ps -ef \| grep uvp-monitor**<br>Tools installation is successful if the command output contains the bold characters as follows:<br>root 4561 1 0 Jun29 ? 00:00:00 **/usr/bin/uvp-monitor**<br>root 4567 4561 0 Jun29 ? 00:00:00 **/usr/bin/uvp-monitor**<br>root 6185 6085 0 03:04 pts/2 00:00:00 grep uvp-monitor | |

| Step 5: Configure the VM NIC. | |
|---|---|
| 1. Run the following command on the VM to view the files in the network rule directory:<br>**ls –l /etc/udev/rules.d** | N/A |
| 2. Run the following commands to delete the rule files whose file names contain **persistent** and **net** in the network rule directory:<br>For example:<br>**rm -r /etc/udev/rules.d/***30*-**net_persistent**-*names*-**.rules**<br>**rm -r /etc/udev/rules.d/***70*-**persistent-net.rules**<br>The italicized content in the command varies depending on the actual service environment | |
| 3. Decompress the software package **FusionCompute V100R005C00SPC100_GuestOSDrivers.zip** on the local PC.<br>The **FusionCompute V100R005C00SPC100_Customization.iso** file is obtained. | |
| 4. Mount **the FusionCompute V100R005C00SPC100_Customization.iso** file to the VM.<br>This file is used to configure the VM to automatically obtain an IP address using the DHCP service. | |
| 5. Copy the **linux** folder in the ISO file to the **/home** directory on the VM. | |
| 6. Run the following command to back up the original NIC configuration file and create a new configuration file for the NIC:<br>**sh /home/linux/autoConfigLinuxNetwork.sh /etc/sysconfig/network**<br>The command is executed successfully if the following information is displayed<br>backup old config files ...<br>create new config files ...<br>done !!! | N/A |
| 7. Run the following command on the VM to switch to the control center:<br>**yast** | N/A |
| 8. Choose **Network Devices** > **Network Settings**. | |
| 9. Hold down **Alt** and press **G** on the **Network Settings** page.<br>The **Global Options** page is displayed. | |
| 10. Hold down **Alt** and press **T,** and select **Traditional Method with ifup**. | |
| 11. Press **F10** to save the configurations and exit the control center. | |

## Step 6: Configure the VM template.

1. Run the following command on the VM to open the **rc** file using the visual interface (vi) editor:
**vi /etc/init.d/rc**

2. Press **i** to enter editing mode.

3. Add a command statement based on the following requirements:
   - If **exit 0** is displayed at the end of the file, add **sh /etc/init.d/setpasswd.sh** in the line before **exit 0**.
   - If **exit 0** is not displayed at the end of the file, add **sh /etc/init.d/setpasswd.sh** at the end of the file.

4. Press **Esc**, enter **:wq**, and press **Enter**.

The system saves the configurations and exits the vi editor.

**Note:**
Back up the **rc** file before editing it.

## Step 7: Initialize the user disk.

1. Run the following command on the VM to query user disk information:
**ll /dev/xvd***

```
brw-rw---- 1 root disk 202, 0 08-15 16:13 /dev/xvda
brw-rw---- 1 root disk 202, 1 08-15 16:13 /dev/xvda1
brw-rw---- 1 root disk 202, 2 08-15 16:13 /dev/xvda2
brw-rw---- 1 root disk 202, 48 08-15 16:13 /dev/xvdd
brw-rw---- 1 root disk 202, 64 08-15 16:13 /dev/xvde
brw-rw---- 1 root disk 202, 65 08-15 16:13 /dev/xvde1
brw-rw---- 1 root disk 202, 66 08-15 16:13 /dev/xvde2
```

**xvda** indicates a system disk, **xvdd** indicates the CD/DVD-ROM drive, and **xvde** indicates a user disk.

2. Run the following command to format the user disk:
**mkfs.ext3 -F /dev/xvde**

3. Run the following commands to attach the user disk to the VM:
**mkdir /usr/xvde**
**mount /dev/xvde /usr/xvde/**

4. Run the following command to query the information about the user disk:
**df –h**
The user disk is successfully attached to the VM if a capacity value is displayed for the xvde disk.

| File System | Capacity | Used | Available | Usage | Mounting Point |
|---|---|---|---|---|---|
| /dev/xvda2 | 19G | 3.1G | 15G | 18% | / |
| devtmpfs | 465M | 108K | 465M | 1% | /dev |
| tmpfs | 465M | 100K | 465M | 1% | /dev/shm |
| /dev/xvde | 20G | 173M | 19G | 1% | /usr/xvde |

N/A

5. Run the following command to open the **fstab** file using the vi editor and enable automatic disk attaching:
**vi /etc/fstab**

6. Move the cursor to the end of the file, press **Enter**, and enter the following line:
**/dev/xvde /usr/xvde/ ext3 defaults 0 0**

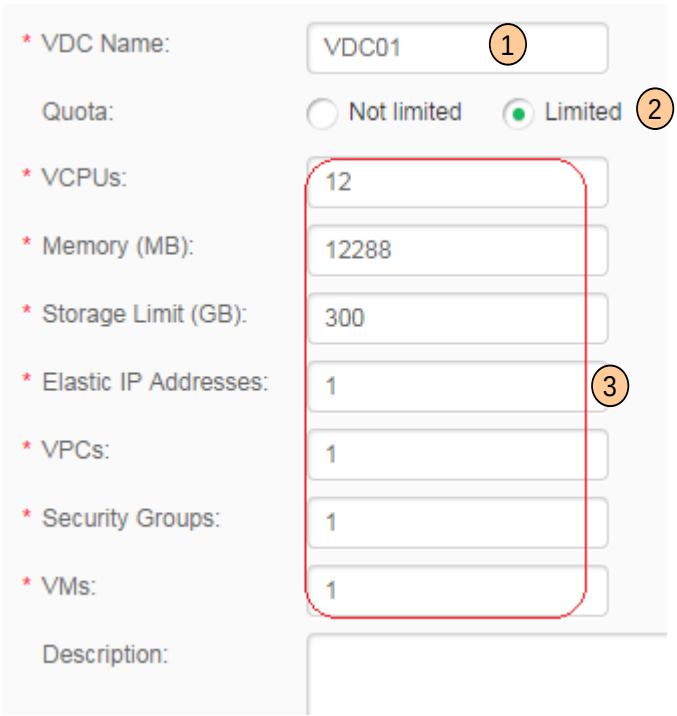
7. Press **Esc**, enter **:wq**, and press **Enter**.
The system saves the configurations and exits the vi editor.

N/A

| Step 8: Complete VM template creation. | |
|---|---|
| 1. FusionManager, choose **Resource** > **Templates and Specs** . | N/A |
| 2. Locate the row that contains the VM template, then choose **More** > **Install Software**.<br>The **Install Software** page is displayed. | |
| 3. Click **Complete**.<br>The **VM Templates** page is displayed., on which the VM template status is Complete. After the VM is created, the CD/DVD-ROM mounted to the VM is automatically unmounted. | |

# 11 Create a VDC

A virtual data center (VDC) is the unit of using virtual resources on FusionManager. Create a VDC for a service department and create a VDC administrator. Then the VDC administrator can manage resources in the VDC and allocate the resources to user VMs in the VDC.

| **Step 1: Create a VDC.** | |
|---|---|
| 1. On FusionManager, choose **VDC** > **VDCs**.<br>The VDC management page is displayed. | |
| 2. Click **Create VDC**. | |
| 3. Configure the VDC information.<br>  | 3 Configure the maximum amount of resources allowed for the VDC. These settings can also be modified after the VDC is created. |
| 4. Click **Next**. | |
| 5. Select an AZ, then click **Next**. | |
| 6. Select an external network, then click **Next**. | |
| 7. Select VDC members, then click **Next**. | |
| 8. Confirm that the entered information is correct, then click **Create**. | |
| 9. Repeat step 2 to step 8 to create VDC02 and VDC03. | |

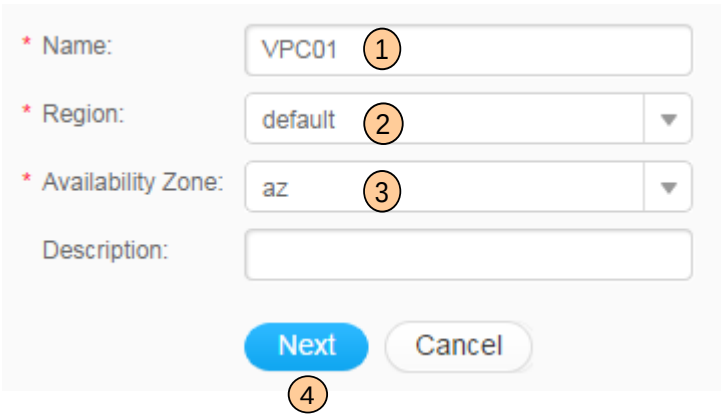
| **Step 2: Create the VDC administrator.** | |
|---|---|
| 1.Locate the row that contains the created VDC, then choose **More** > **Member Management**. | The created VDC administrator can manage the resources available in the VDC. |
| 2. Click **Create User**. | |
| 3. Set the username, password, and role, then click **Create**.<br>To create a VDC administrator, select the **vdcmanager** role. | |

# 12 Create a VPC and Networks

## 12.1 Create a VPC

Create a VPC to provide VDC tenants with a secure and isolated network environment. The VDC administrator can create virtual networks in a VPC to provide VDC tenant VMs with the same network functions as those provided by a traditional network.

| Step 1: Log in to FusionManager. | |
|---|---|
| 1. Log in to FusionManager as the VDC administrator. | After logging in to FusionManager for the first time, you need to change the default login password as requested. |

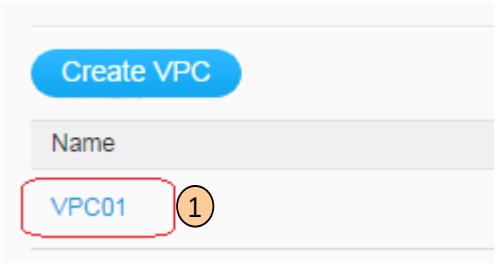
| Step 2: Create a VPC. | |
|---|---|
| 1. Choose **VPC** > **My VPC**. | |
| 2. Click **Create VPC**. | |
| 3. Configure the VPC information.<br>  | |
| 5. choose **Custom**, then click **Next**. | N/A |
| 6. Click **Create**. | |

## 12.2 Apply for a Router

Apply for a router for the VPC so that the router can serve as a gateway for the routed networks created in the VPC. The router also supports the elastic IP address function, which allows an elastic IP address to be bound to the VM so the VM can connect to public networks.

### Step 1: Go to the VPC configuration page.

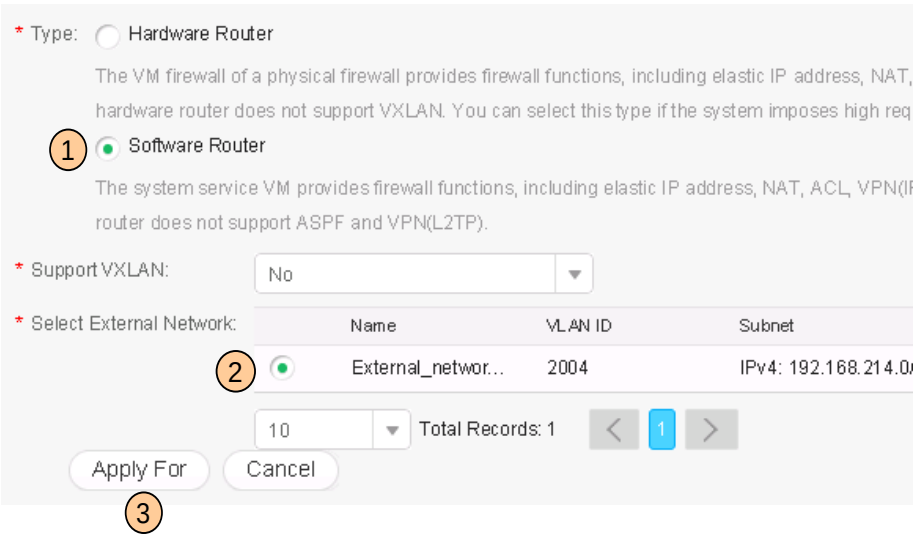
1. Click the name of the created VPC (VPC01).




2. On the displayed VPC01 configuration page, choose **Routers**.

3. Click **Apply for Router**.

4. Apply for a router.




1 A software router is deployed on a VSA VM to provide firewall functions. The administrator can apply for a software router only after creating the VSA management network and importing the VSA template to the system. For details about the software router functions, see Appendix 6.

## 12.3 Create a Routed Network

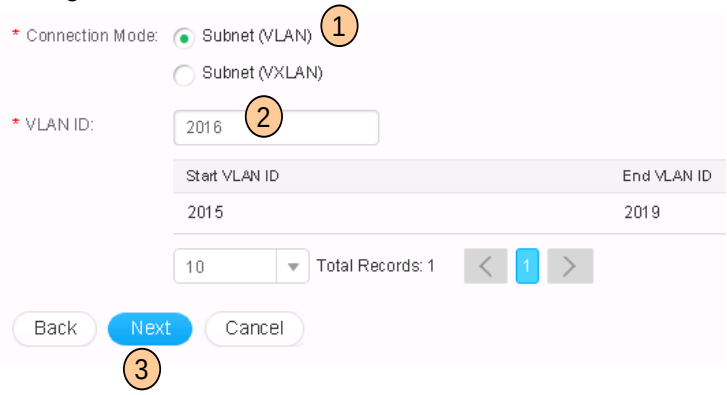
VMs deployed in a routed network can have their private IP addresses bind to an elastic IP address through a router, so the VMs can use the elastic IP address to provide public network access services.

### Step 1: Create a routed network.

1. On the VPC01 page, choose **Network**> **Network**.
2. Click **Create**.
3. Enter the routed network name and set the network type to **Routed Network**.
4. Click **Next**.

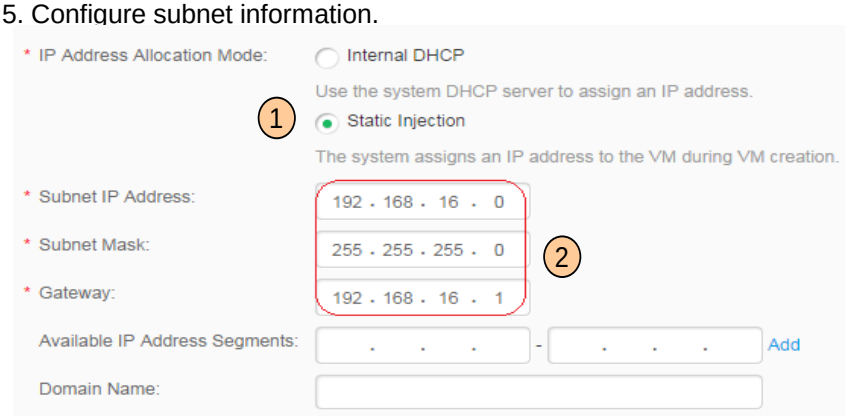
A routed network can provide VMs with elastic IP address and destination network address translation (DNAT) functions through the router. The router also supports configuration of access control list (ACL) rules to control the data traffic inbound to or outbound from the routed network to improve network security.

4. Configure VLAN information for the routed network.




2 Enter a VLAN ID planned for routed networks.

5. Configure subnet information.




2 The VDC administrator can customize the subnet IP address for the routed network.

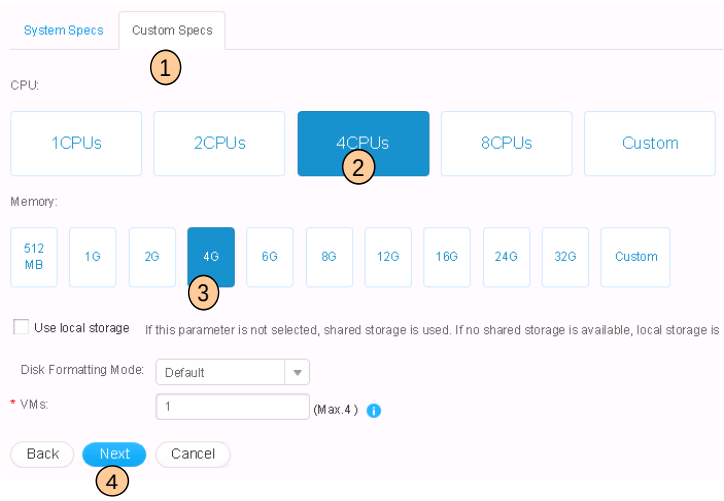
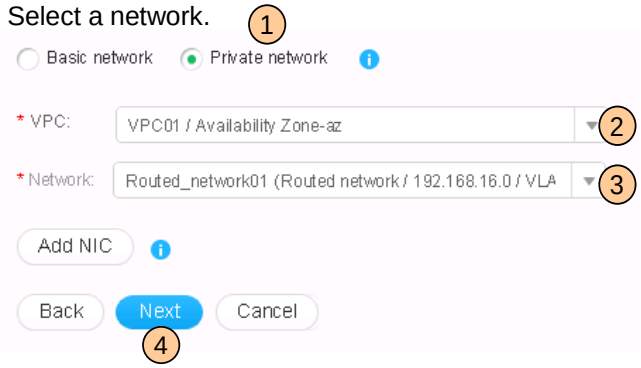
6. Click **Next**.

7. Confirm that the entered information is correct, then click **Create**.

# 13 Provision VM

## 13.1 Create the VM

The VDC administrator can select a created VM template and specify the specifications and network to create a VM with the same configuration as the template.

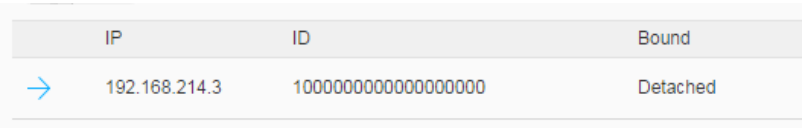
| **Step 1: Create the required VM.** | |
|---|---|
| 1. On the web client page in tenant view, choose **Resources** > Computing > **VMs**. | N/A |
| 2. Click **Create**. | |
| 3. Select a VM template, then click **Next**. | |
| 4. Configure the VM specifications.<br>  | |
| 5. Select a network.<br>  | 3 Add the VM NIC to the routed network created in 11.3. |
| 6. Enter the VM name, then click **Next**. | |
| 7. Confirm that the entered information is correct, then click **Complete**. The system begins to create the VM. | |

| **Step 2: Install the application software.** | |
|---|---|
| 1. Mount the ISO file of the application software to the VM to install the application software on the VM.<br>You can use any ISO image creation tool, such as UltraISO and ISOMaker, to create an ISO file for the desired application software. | |

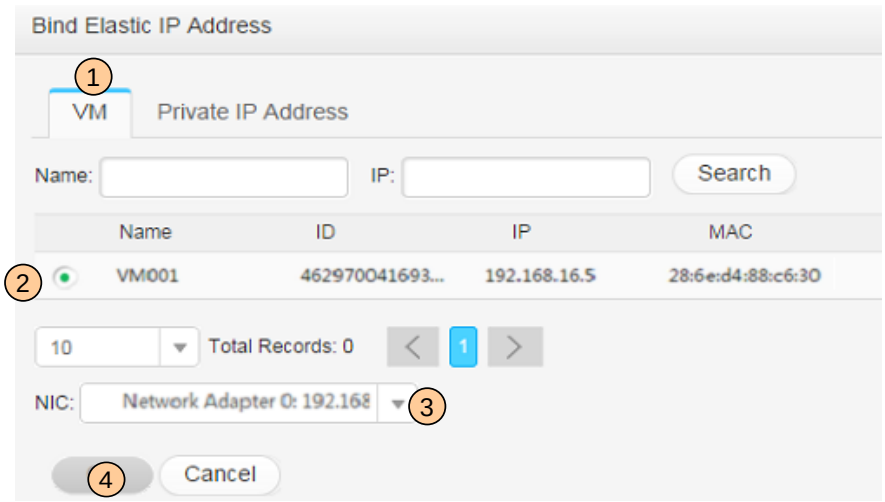
## 13.2 Bind an Elastic IP Address to a VM

Elastic IP address is a public IP address that can be bound to a VM or a private IP address to enable the VM to provide external services using the public IP address. Apply for an elastic IP address before binding the elastic IP address to a VM.

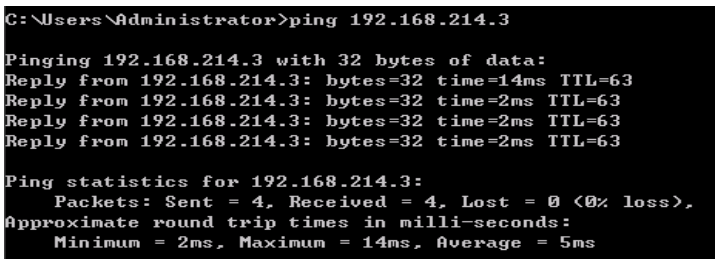
### Step 1: Apply for an elastic IP address.

| | |
|---|---|
| 1. On the VPC01 configuration page, choose **Network** > **Elastic IP Addresses**. | |
| 2. Click **Apply For**.<br>A message is displayed indicating that elastic IP address application is successful. | |
| 3. Click **OK**.<br>The requested elastic IP address is displayed.<br>  | The requested elastic IP address is obtained from a subnet from the created external network. |

### Step 2: Bind the elastic IP address to the VM.

| | |
|---|---|
| 1. Locate the row that contains the obtained elastic IP address, then click **Bind**. | N/A |
| 2. Bind the elastic IP address to the VM.<br>  | |

### Verify the Elastic IP Address Bound to the VM

| | |
|---|---|
| Ping an IP address in the external network using the elastic IP address bound to the VM to check whether the VM can communicate with the external network using the bound elastic IP address.<br>  | |

## 13.3 Add ACL Rules

Add ACL rules in the VPC to allow users to access the web services deployed on a specific VM using only the TCP protocol and port 80. This configuration prevents unauthorized users from accessing the web services and thereby improves network access security.

**Note**: The system allows services access using any supported port and protocol by default. To allow VMs to access services using only the specified protocol and port number, you need to first add an ACL rule that prohibits service access using any protocol or port, and then add another higher-priority ACL rule that specifies the protocol and port number allowed for service access.

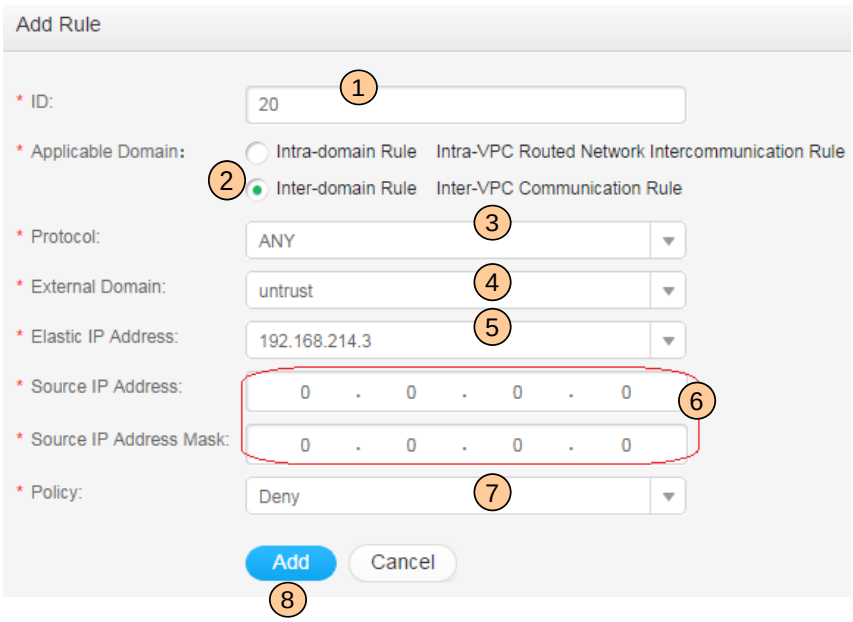
### Step 1: Prohibit access to the web-service-deployed VM using any protocol and port.

1. On the VPC01 configuration page, choose **Security** > **ACLs**.

2. On the **IN** page, click **Add Rule**.

**IN** indicates the control for network packets inbound to the VM. **OUT** indicates the control for network packets outbound from the VM.

3. Configure ACL rules.




1 Set the ACL rule ID representing the rule priority. If multiple ACL rules contain the same rule configuration, the rule with the smaller rule ID takes effect preferentially. You are advised to number two adjacent rules with a step of 10 numbers to facilitate adding more sub-rules in future.

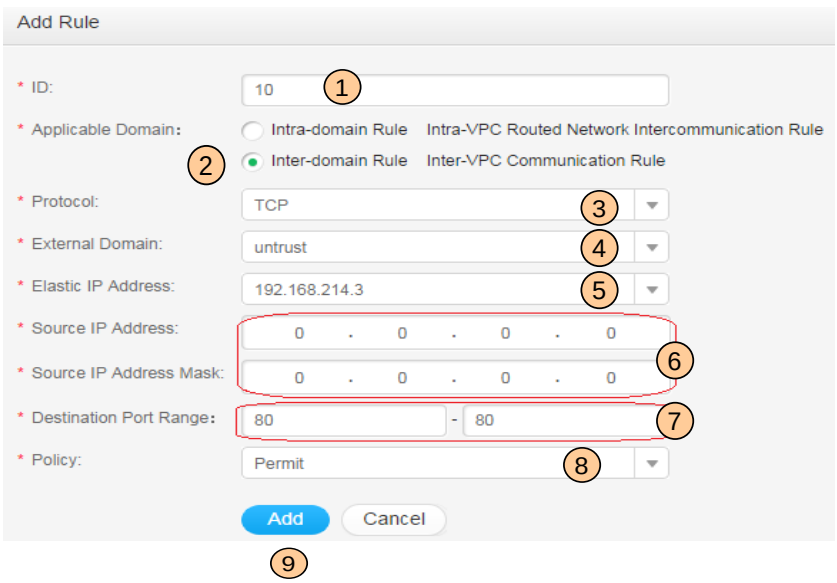
5 Set the elastic IP address bound to the VM on which the configured ACL rule takes effect.

6 Set the IP address of the VMs to access the services. 0.0.0.0 indicates all IP addresses.

### Step 2: Specify the protocol and port number allowed for VM access.

1. On the **IN** page, click **Add Rule**.

2. Configure the ACL rules.

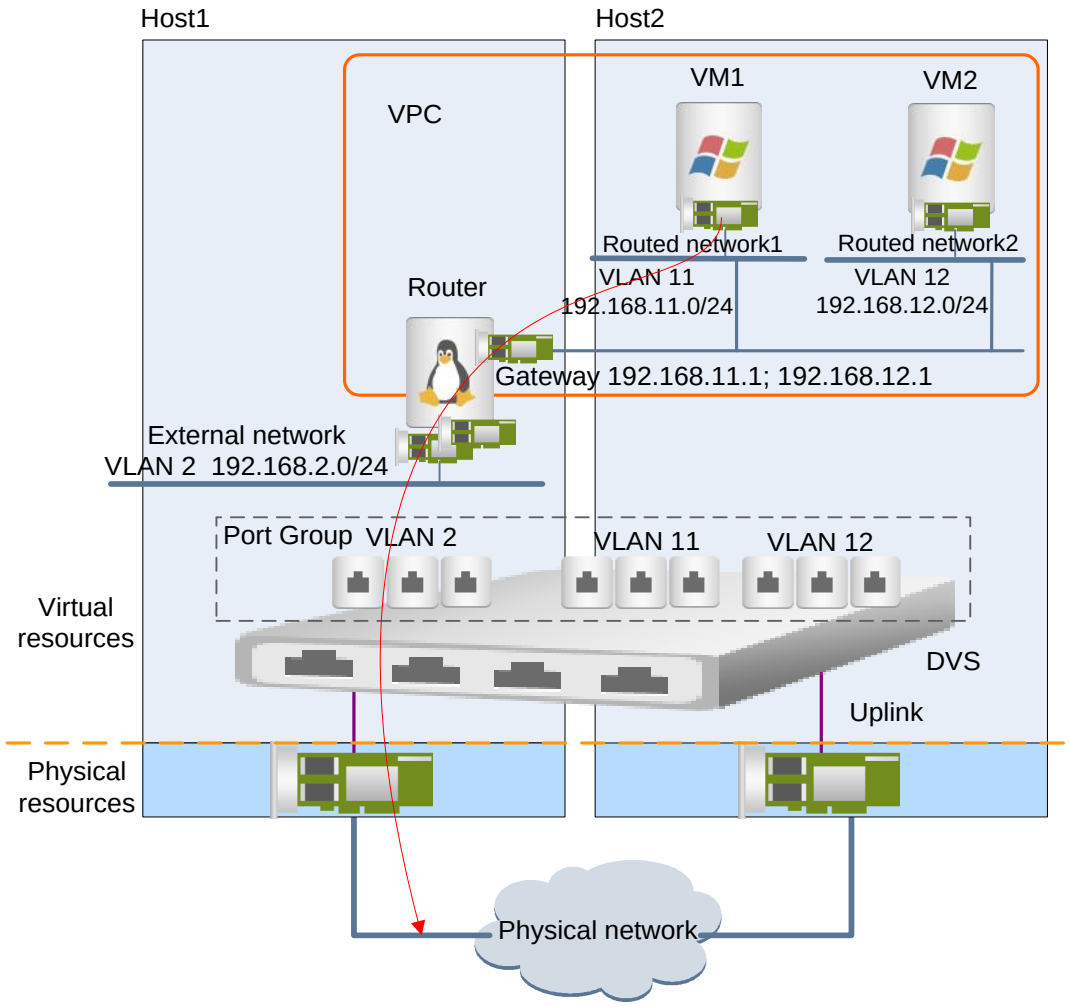



1 The ACL rule configured in the preceding step prohibits the access to the web service VM. The ACL rule to be configured in this step allows access to the VM using the TCP protocol and port number 80. This ACL rule (10) has the higher priority than the ACL rule 20 configured in the preceding step.

# Appendix

## Appendix 1 Principles of VM Network Access

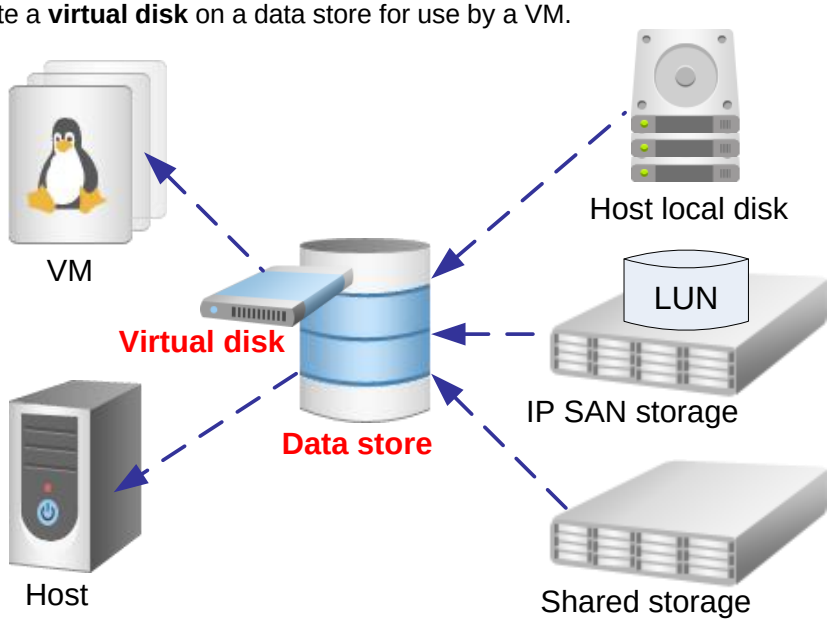
A virtual NIC of a VM communicates with an external network by connecting to the DVS through the port group, then by connecting to the physical NIC of a host through the DVS uplink. These connections are shown in the following figure.




| Network Element | Description |
|---|---|
| Software router | A software router functions as a gateway that enables VMs in a VPC to communicate with VMs in other routed networks. The software router connects to the public network through the external network and therefore provides IP addresses for VMs to access external networks. |
| Port group | A port group is a virtual logical port similar to a template with network attributes. A port group is used to define VM NIC attributes and uses a DVS to connect to the network: Each service network (internal, routed, and external networks) created on FusionManager maps a port group on the DVS. |
| DVS | A DVS provides the same functions as a physical layer 2 switch. A DVS links port groups to VMs and connects to the physical network through uplink channels. |
| Uplink | An uplink connects the DVS to the physical network NIC and therefore can transmit the data from the VMs connected to the DVS to the physical network. |

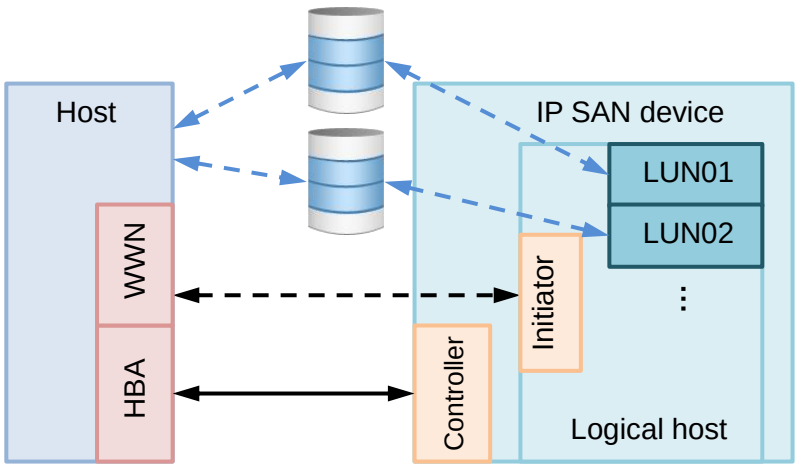
## Appendix 2 Principles of VM Storage Access

A **data store** is a logical storage unit on FusionCompute. A data store is used to universally define all types of storage resources.
You can create a **virtual disk** on a data store for use by a VM.




## Appendix 3 Network Communication Between Hosts and IP SAN Devices

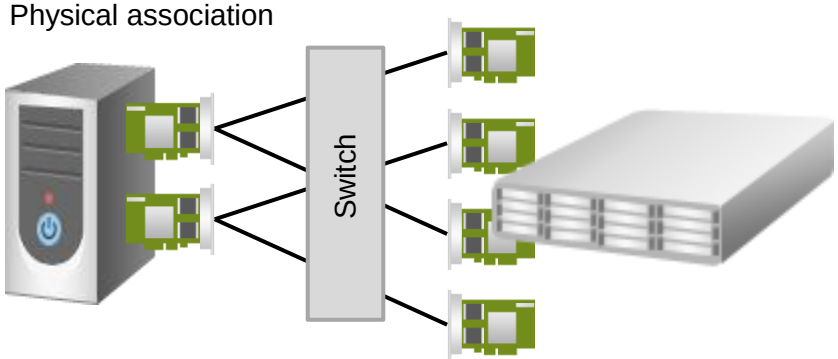
**Logical layer:**
After a storage device is associated with a host, the host bus adapter (HBA) generates a WWN for the host.
After an initiator is added to the logical host on the storage device using the host WWN, the host can access the storage resources (LUNs) that match the logical host on the storage device and add the LUNs as data stores.




Logical association

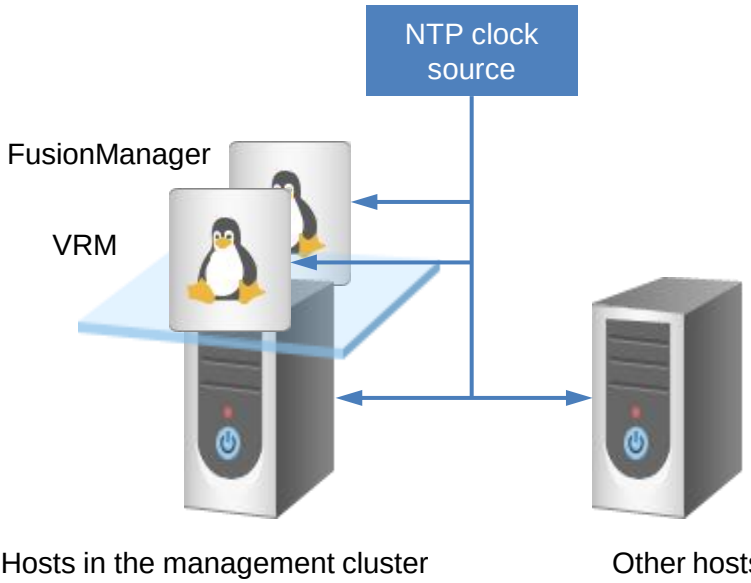
Physical association

**Physical layer:**
A host connects to an IP SAN device through multipathing.
Storage NICs on the host connect to the storage NICs on the storage device controller.



## Appendix 4 Principle of Clock Synchronization

After the NTP clock source is configured, all hosts, VRM VMs, and FusionManager VMs synchronize time from the NTP clock source to ensure system time accuracy.

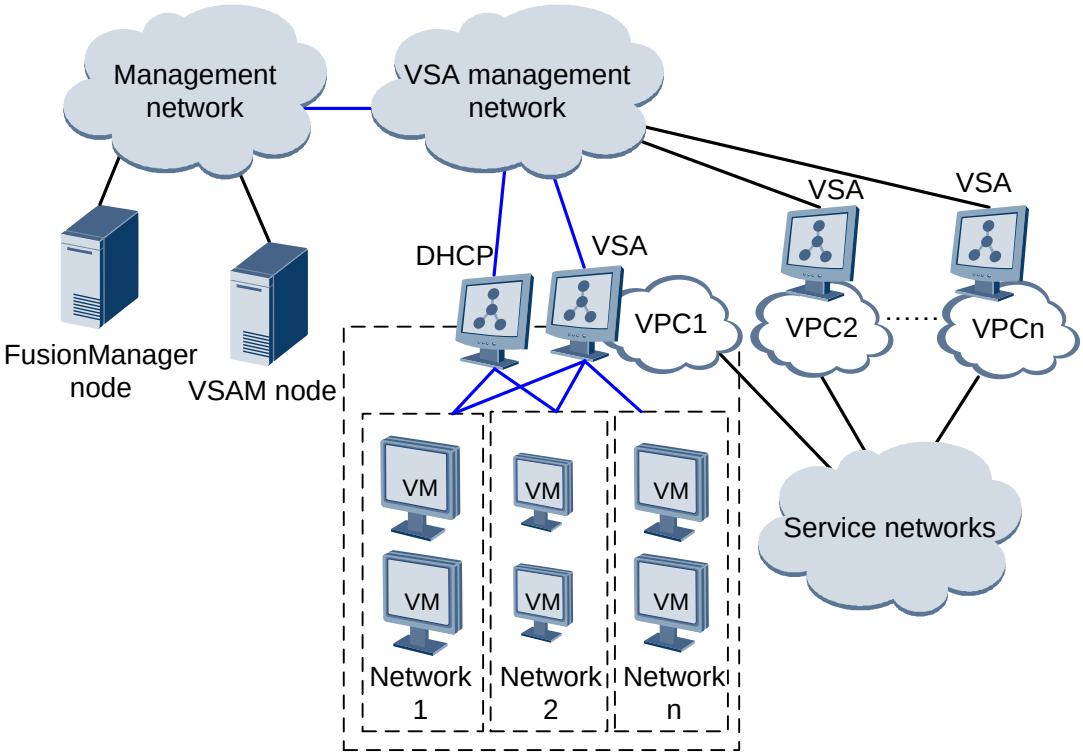



## Appendix 5 Setting Multipathing Mode for a Host Using Commands

| | |
|---|---|
| 1. After the OS is installed on the host and the host restarts, log in to the host as user **root** in the remote control window, and run **TMOUT=0** to disable logout on timeout.<br>`host01 login: root`<br>`Password:`<br>`Authorized users only. All activities may be monitored and reported.`<br>`host01:~ # TMOUT=0`<br>`host01:~ #` | The password of user **root** is the password you set during host OS installation. |
| 2. Run the following command to set the multipathing mode to Huawei mode: **sh /opt/uvp/multipath/change_multipath_mode.sh 1**<br>`host01:~ # sh /opt/uvp/multipath/change_multipath_mode.sh 1`<br>`Enable ultrapath successfully.`<br>The command is executed successfully if the message "**Enable ultrapath successfully**" is displayed. | N/A |
| 3. Run **reboot** to restart the host for the mode to take effect:<br>`host01:~ # reboot`<br>`Broadcast message from root (tty1) (Tue Sep 24 18:16:53 2013):`<br>`The system is going down for reboot NOW!`<br>`INIT: Switching to runlevel: 6`<br>`INIT: Sending processes the TERM signal` | N/A |

# Appendix 6 VSAM and VSA

The VSAM node is deployed on the FusionManager management plane to manage VMs that provide VSA system services, including software router and DHCP.




The VSA management network connects to the management networks of the FusionManager node and the VSAM node to enable communication between VSA VMs and the VSAM node. When a tenant applies for a software router or the DHCP service for a VPC, FusionManager creates a VSA VM using the VSAM node and automatically deploys the virtual firewall or DHCP service on t he VSA VM. A software router functions as a firewall that connects to the Internet-accessible external network to provide public IP addresses for VMs in the VPC to access public networks.

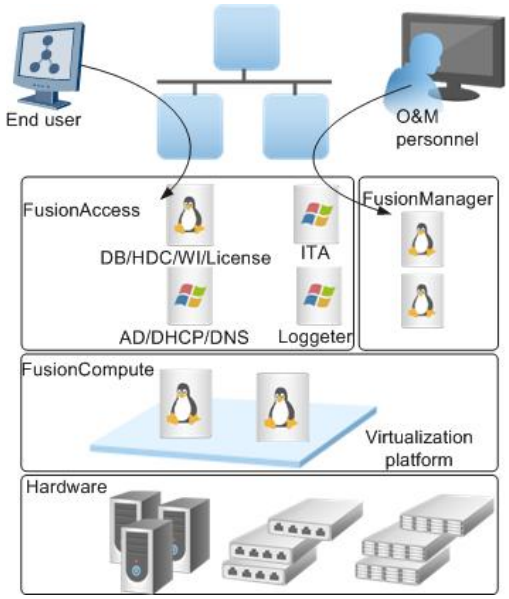
# 02 HCNA-Cloud V2.0
# FusionAccess Installation

Issue: 01
Date: 2015-07

## Introduction to the FusionAccess

Huawei FusionAccess is virtual machine (VM) management software deployed on a virtualization platform. It enables users to access virtual desktops by using networked client devices, such as thin clients (TCs), desktop computers, laptops, and smartphones.

FusionAccess transforms the traditional PC-dominated office model with features such as security, investment, and office efficiency. It is an optimal choice for large- and medium-sized enterprises, government agencies, and mobile offices.

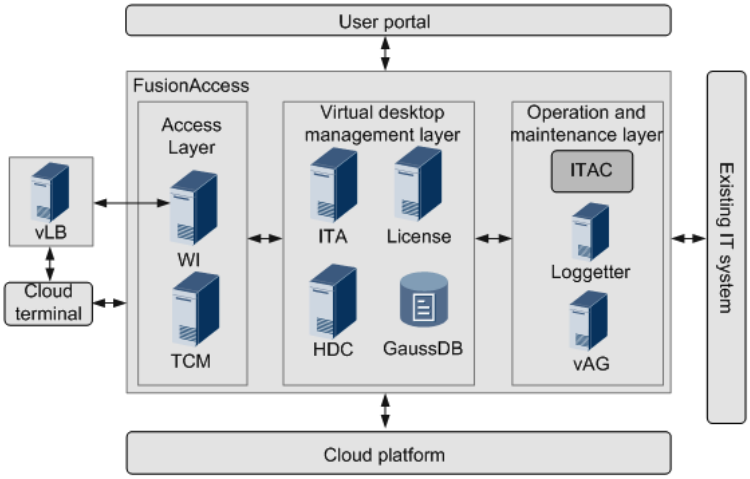



## Objectives

This guide helps you quickly deploy FusionAccess. For more information about the installation and configuration of FusionAccess, see the *FusionCloud Desktop Solution V100R005C20 Software Installation Guide*.

# 1 Overview

FusionAccess consists of the access control layer, virtual desktop management layer, and operation and maintenance (O&M) layer.




**WI**

The WI provides an interface for users to access their VMs.

**ITA**

The IT adapter (ITA) provides an interface for virtual desktop management. The ITA works with the Huawei Desktop Controller (HDC) and the virtualization software FusionCompute to implement functions, such as VM creation and provisioning, VM status and image management, and virtual desktop O&M.

**HDC**

The HDC processes VM registration requests, manages desktop groups, and assigns and unassigns VMs for users.

**License**

The license server manages and distributes licenses for the HDC.

**GaussDB**

The GaussDB stores data for the ITA and HDC.

**Loggetter**

The Loggetter records information about user operations, key points, and information returned during the system installation and operating process. The information helps locate faults.

**vAG/vLB**

The vLB provides the load balancing function and selects a proper WI for end users. The vAG provides an access gateway to ensure the security when end users access VMs, and provides the Virtual Network Computing (VNC) access gateway function. When a VM is faulty, the user can log in to the VM by using VNC.

**TCM**

The thin client manager (TCM) centrally manages TCs, for example, delivering TC certificates and collecting logs. For the TCM installation, see the related TCM documents.

The deployment of the components in a typical desktop cloud scenario is as follows:

| Component | Number of VMs | Software |
|---|---|---|
| AD/DNS/DHCP | 2 | Windows operating system (OS) and AD/DNS/DHCP component software |
| GaussDB/HDC/WI/License | 1 | Linux OS andGauss DB/HDC/WI/License component software |
| DB/HDC/WI | 1 | Linux OS and DB/HDC/WI component software |
| ITA | 2 | Windows OS and ITA component software |
| Loggetter | 1 | Windows OS and Loggetter component software |
| vAG/vLB | 2 | Linux OS and vAG/vLB component software |

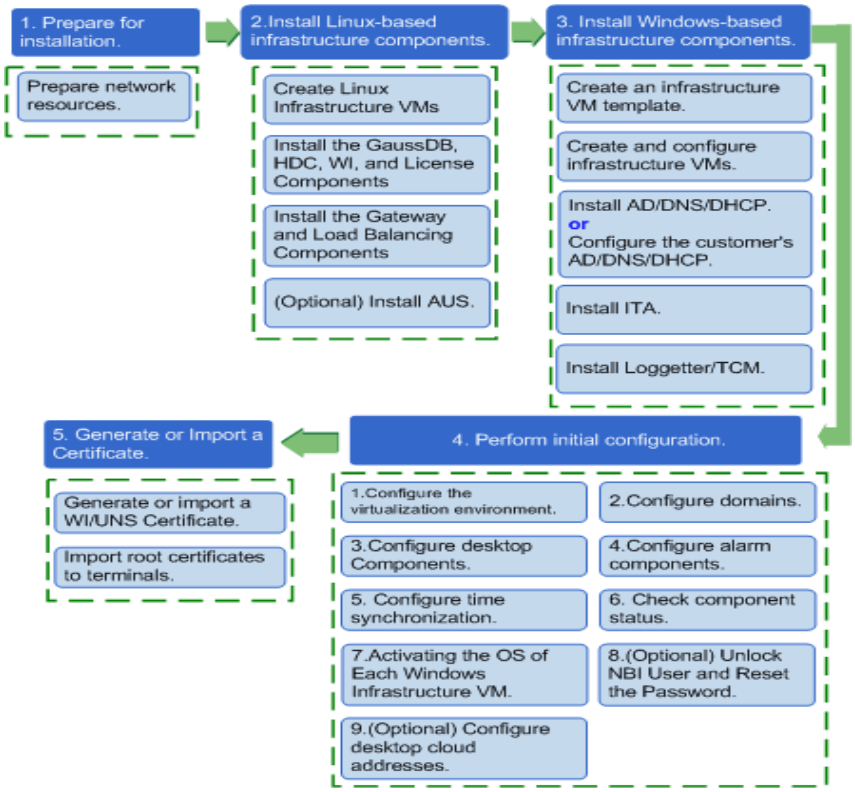
Note: When the vAG does not provide the Huawei Desktop Protocol (HDP) access gateway function, the preceding deployment scheme supports a maximum of 5000 users; when the vAG provides the HDP access gateway function, the preceding deployment scheme supports a maximum of 500 users.

# 2 Installation Process

1. Install FusionCompute.
   During the desktop cloud environment deployment, you need to install and configure the low-layer virtualization platform, that is, FusionCompute. For details about the installation, see the ***(Quick Guide) FusionCompute V100R005C00 Quick User Guide***. The following table describes some data requirements for the FusionCompute Installation.

| Item | Requirement |
|---|---|
| Installation mode | **Install active and standby VRM modes.** |
| Domain 0 specifications | The Domain 0 specifications of the management, and user clusters, and gateway clusters vary with the number of VMs on a host:<br>max_vcpus and reserve_vcpus: 6VCPU<br>mem(MB): 5120 MB<br>mem_for_icache(MB)<br>Common VM: Default 0<br>Linked clones: 12288 |
| VRM VM specification requirements: | • **200 VMs, 20 physical hosts**: 2 VCPUs, 3 GB memory<br>• **1000 VMs, 50 physical hosts**: 4 VCPUs, 5 GB memory<br>• **3000 VMs, 100 physical hosts**: 8 VCPUs, 8 GB memory<br>• **5000 VMs, 200 physical hosts**: 12 VCPUs, 16 GB memory |
| Add **Data Store** | FusionAccess infrastructure VMs must use unvirtualized storage. When adding data storage for a FusionAccess VM, set **Storage mode** to **Non-virtualization**. |
| NTP server of FusionCompute | If the Network Time Protocol (NTP) server is available on the site, set this parameter to the site NTP server.<br>If no NTP server is available on the site, set this parameter to VRM. |

2. Install FusionAccess. Install FusionAccess according to the description in this document. The installation process is as follows:



# 3 Preparations

## 3.1 Obtaining Software Packages

| Document or Software | How to Obtain |
| --- | --- |
| **FusionCompute document**<br>(Quick Guide) FusionCompute V100R005C00 Quick User Guide 01 | **For an enterprise user**, download it from: http://support.huawei.com/enterprise > Product Support > IT > FusionCloud > FusionSphere FusionCompute<br><br>**For a carrier user**, download it from: http://support.huawei.com > Product Support > Carrier IT > FusionCloud > FusionSphere > FusionCompute |
| **FusionCompute software**<br>1. CNA OS software:**FusionCompute V100R005C00SPCxxx_CNA.iso**<br>2. FusionCompute installation wizard tool: **FusionCompute 100R005C00SPCxxx_Tools.zip**<br>3. Virtual Resource Management (VRM) VM template file:**FusionCompute V100R005C00SPCxxx_VRM.zip**<br>4. Intelligent network interface card (iNIC) driver software:**FusionCompute V100R003C10SPCxxx_GuestOSDrivers.zip** | **For an enterprise user**, download it from: http://support.huawei.com/enterprise > Downloads > IT > FusionCloud > FusionSphere > FusionCompute<br><br>**For a carrier user**, download it from: http://support.huawei.com > Software > Carrier IT > FusionCloud > FusionSphere > FusionCompute |
| **FusionAccess software**<br>1.Linux OS component installation software: **FusionAccess_Installer_Linux_V100R005C20SPCxxx.iso**<br>2.Windows OS component installation software: **FusionAccess_Installer_Win_V100R005C200SPCxxx.iso** | **For an enterprise user**, download it from: http://support.huawei.com/enterprise > Software > IT > FusionCloud > FusionAccess > FusionAccess > V100R005C20SPCxxx<br><br>**For a carrier user**, download it from: http://support.huawei.com > Software > Carrier IT > FusionCloud > FusionAccess > FusionAccess > V100R005C20SPCxxx |
| **FusionAccess Tool software**<br>OS installation files:<br>**Windows2008R2SP1_EN.part1.rar**<br>**Windows2008R2SP1_EN.part2.rar**<br><br>Decompress the two files to obtain **Windows2008R2SP1_EN.iso.** | **For an enterprise user**, download it from: http://support.huawei.com/enterprise > Software > IT > FusionCloud > FusionSphere > FusionTool > V100R005C00SPCxxx<br><br>**For a carrier user**, download it from: http://support.huawei.com > Software > Carrier IT > FusionCloud > FusionSphere > FusionTool > V100R005C00SPCxxx |

## 3.2 Local PC Requirements

| Item | Requirement |
|---|---|
| OS | Windows XP or Windows 7 32-bit |
| Hard disk space | The partition for installing the OS must have more than 1 GB free space.<br>Excluding the partition for the OS, at least one partition must have more than 40 GB free space. |
| Network | The local PC can access the network segment of the desktop cloud management plane. |
| Application software | •Internet Explorer 8 or later is installed.<br>•The software used to decompress .rar and .zip packages is installed.<br>•Antivirus software and firewall software are disabled.<br>•The Telnet tool is installed. |

## 3.3 Obtaining a License

**Time required**: 3 to 5 days after application
**Application method**: Huawei technical support engineers apply for the licenses.
**Reference**: FusionCloud Desktop Solution V100R005C10SPCXXX License Usage Guide.
**Download path:** http://support.huawei.com/enterprise > Software > IT > FusionCloud > FusionAccess > FusionCloud Desktop Solution > V100R005C20

## 3.4 Preparing for Required Data

Before the installation, plan the following data with customers:

| Category | Parameter | Example Value and Planned Value |
|---|---|---|
| **A. Network information** | **(A1) VLAN pool**<br>VLAN pool of the infrastructure VM service plane. | *181 to 189*<br>**Planned value:** _____ |
| | **(A2) Port group name and port group**<br>Infrastructure VMs that connect to the same port group belong to the same network and can communicate with each other. This port group is created for the VM service plane. | *Name: VDIPort*<br>*VLAN ID: 181*<br>**Planned value:** _____ |
| | **(A3) Service plane gateway and subnet mask**<br>Service plane gateway and subnet mask of the infrastructure VM, used to configure a VLANIF interface for the VLAN ID used by the infrastructure VM service plane. | *Gateway: 192.168.181.1*<br>*Subnet mask: 255.255.255.0*<br>**Planned value:** _____ |
| **B. VM user disk, IP address, and name** | **(B1) User disk name**<br>Specifies the name of a user disk attached to an infrastructure VM running Windows OS. | *ITA: FA-ITA-DISK*<br>*Loggetter: FA-LOG-DISK*<br>**Planned value:** _____ |

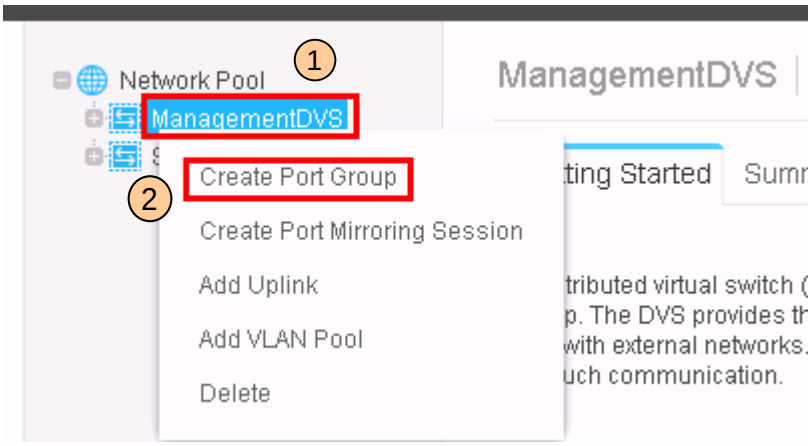
## 3.4 Preparing for Required Data

| Category | Parameter | Example Value and Planned Value | |
|---|---|---|---|
| B. VM user disk, IP address, and name | **(B2) VM names and IP addresses**<br>•AD/DNS/DHCP VM name and service IP address<br>•DB/HDC/WI/License VM name, service IP address, and floating IP address<br>•ITA VM name, management IP address, and service IP address<br>•Loggetter VM name and service IP address<br>•vAG/vLB VM name, service IP address, management IP address, and vLB floating IP address<br>•Service plane mask and gateway<br>•Management plane mask | **Name** | **IP** |
| | | ***FA-AD-1*** | *Service: 192.168.181.66* |
| | | ***FA-AD-2*** | *Service: 192.168.181.67* |
| | | ***FA-DBHDCWILI*** | *Service: 192.168.181.61*<br>*Floating: 192.168.181.60* |
| | | ***FA-DBHDCWI*** | *Service: 192.168.181.63*<br>*Floating: 192.168.181.60* |
| | | ***FA-ITA-1*** | *Service: 192.168.181.62*<br>*Management: 192.168.180.62* |
| | | ***FA-ITA-2*** | *Service: 192.168.181.64*<br>*Management: 192.168.180.64* |
| | | ***FA-Log*** | *Service: 192.168.181.65* |
| | | ***FA-vAGvLB-1*** | *Service: 192.168.181.68*<br>*Management: 192.168.180.68*<br>*Floating: 192.168.181.70* |
| | | ***FA-vAGvLB-2*** | *Service: 192.168.181.69*<br>*Management: 192.168.180.69*<br>*Floating: 192.168.181.70* |
| | | ***Service plane*** | *Mask: 255.255.255.0*<br>*Gateway: 192.168.181.1* |
| | | ***Management plane*** | *Mask: 255.255.255.0* |
| C. OS account | **(C1) Password of the administrator account**<br>Specifies the Windows OS system administrator account. This account has the highest rights. | | *Huawei123*<br>**Planned value:**<br>_____ |
| | **(C2) root user password**<br>Specifies the Linux OS system administrator account. This account has the highest rights. | | *Huawei@123*<br>**Planned value:**<br>_____ |
| D. AD/DNS installation | **(D1) Infrastructure domain name**<br>Specifies the AD domain name. The AD domain manages the accounts of Windows servers and clients. All server and client computers must be added to the domain for management. | | *vdesktop.huawei.com*<br>**Planned value:**<br>_____ |
| | **(D2) DSRM password**<br>In directory services restore mode (DSRM), all domain accounts are unavailable. You must use the DSRM administrator account and the AD DSRM password to log in to the OS. | | *Huawei@123*<br>**Planned value:**<br>_____ |

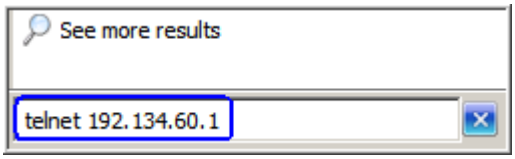
## 3.4 Preparing for Required Data

| Category | Parameter | Example Value and Planned Value |
|---|---|---|
| **D. AD/DNS installation** | **(D3) IP address segment for reverse lookup**<br>Specifies the network segment of the IP address that is translated from the domain name by the DNS. It is the IP address segment of the VM. | *192.168.181*<br>**Planned value:** _____ |
| | **(D4) WI login domain name**<br>Specifies the cloud server address to be entered when a client user tries to log in to the VM. | *fa.vdesktop.huawei.com*<br>**Planned value:** _____ |
| **E. DHCP installation** | **(E1) Scope name**<br>Specifies the DHCP scope name. | *DHCP1*<br>**Planned value:** _____ |
| | **(E2) Start and end IP addresses**<br>Specifies the IP address pool of the service plane. This address pool is used to dynamically assign IP addresses to VMs. | *192.168.181.50 to 192.168.181.100*<br>**Planned value:** _____ |
| | **(E3) Subnet mask and gateway IP address of the address pool**<br>Specifies the subnet mask and gateway IP address of an address pool. | *Subnet mask: 255.255.255.0*<br>*Gateway: 192.168.181.1*<br>**Planned value:** _____ |
| **F. Domain account** | **(F1) Server login account and password**<br>Specifies the login account of each Windows infrastructure VM, except the AD/DNS/DHCP server. | • *ITA: itauser Huawei123!*<br>• *Loggetter: loguser Huawei123*<br>**Planned value:** _____ |
| | **(F2) Domain administrator account and password**<br>Specifies the system administrator of a Linux OS VM. This account has the highest rights for the VM OSs. | *Vdsadmin Huawei123*<br>**Planned value:** _____ |
| | **(F3) Domain account and password of the Tomcat service**<br>Specifies the account for starting the Tomcat service on the ITA server. | *ITAServiceUser Huawei123*<br>**Planned value:** _____ |
| | **(F4) Domain account and password of the log service**<br>Specifies the account for accessing the backup service when the Loggetter server is deployed. | *LogServiceUser Huawei123*<br>**Planned value:** _____ |
| **G. Database information** | **(G1) HDC database name**<br>HDC database instance created on the GaussDB. | *HDCGaussDB01*<br>**Planned value:** _____ |
| | **(G2) ITA database name**<br>ITA database instance created on the GaussDB. | *FusionAccess*<br>**Planned value:** _____ |
| | **(G3) Account for connecting the ITA to the database**<br>Account for ITA server connecting to the database instance and the password. | *Username: ITALoginUser*<br>*Password: Huawei@123*<br>**Planned value:** _____ |

# 4 Preparing Network Resources

| Step 1: Create a port group for the service plane. | |
|---|---|
| 1. In the address box of your browser, enter *http://floating IP address of the VRM* and press **Enter** to log in to the FusionCompute. | Ensure that the local PC can properly communicate with the desktop cloud management plane. |
| 2. On the FusionCompute, choose **Network Pool > Network Pool** | - |
| 3. Create a port group for the infrastructure VM service plane.<br>  | (1) When deploying FusionCompute, determine whether to deploy a service plane distributed switch based on the actual plan.<br>If a service plane distributed switch is created, select the distributed switch of the service plane VLAN.<br>If no service plane distributed switch is created, select the distributed switch of the management plane. |
| 4. Set the port group **Name** (A2), click **Next**. | The port group is used for the service plane NIC communication of infrastructure VMs. |
| 5. Set the VLAN ID (A2).<br>  | (2) The VLAN ID must be in the VLAN pool range of the distributed switch.<br><br>After the distributed switch is selected, the VLAN pool range is displayed in the **Resource Statistics** area on the **Summary** tab page on the right. |
| 6. Confirm the settings and click **Create**. | After the port group is created, close the page. |

# 4 Preparing Network Resources

| **Step 2: Configure the information about the service plane port group on the aggregation switch.** | |
|---|---|
| 1. On the local PC, click **Start**, enter *telnet switch IP address* in the **See more results** dialog box, and press **Enter** to log in to the aggregation switch.<br>  | - |
| 2. On the aggregation switch, run the following commands to configure the gateway and subnet mask (A3) used by the infrastructure VM service plane:<br>**<Quidway>system-view**<br>**[Quidway] interface vlanif** *Service plane vlan id*<br>**[Quidway-Vlanif*vlanid*] ip address** *Service plane gateway Subnet mask*<br>**[Quidway-Vlanif*vlanid*] display this**<br>**[Quidway-Vlanif*vlanid*] quit** | The **display this** command is used to view the gateway and subnet configuration information of the VLANIF interface. |
| 3. Configure that the port for the aggregation switch allows the port group (A2) to pass, tagged.<br>**<Quidway>system-view**<br>**[Quidway] interface GigabitEthernet***0/0/x*<br>**[Quidway-GigabitEthernet***0/0/x***] port hybrid tagged** *vlan-id*<br>**[Quidway] quit**<br>**<Quidway>save** | - |

# 5 Installing Linux Infrastructure Components

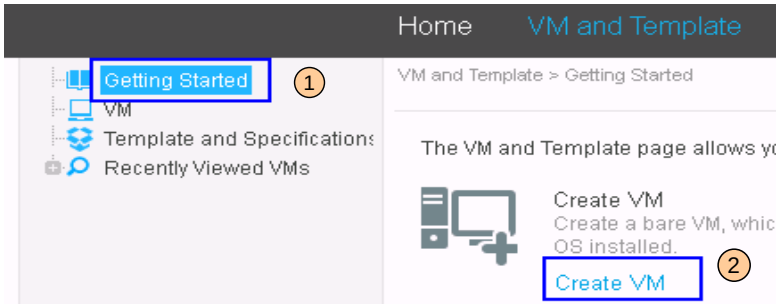
## 5.1 Creating Linux VMs

### Step 1: Create a bare VM.

1. On the FusionCompute portal, choose **VM and Template**.

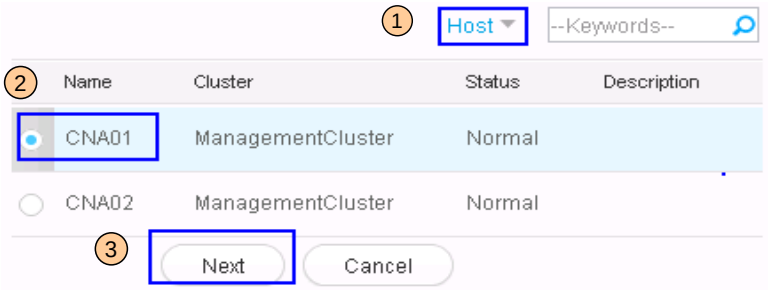
-

2. Create a VM.



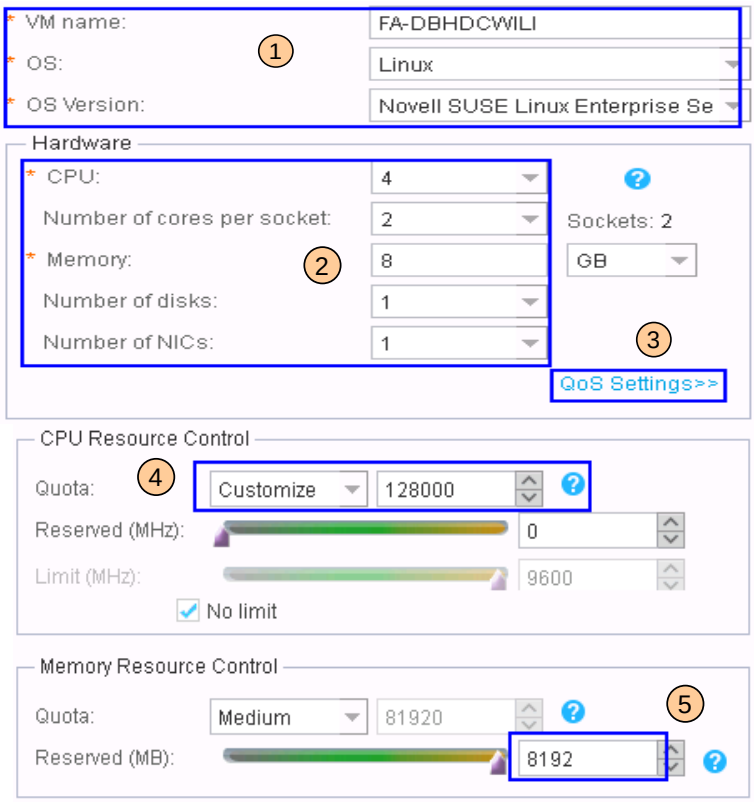

-

3. Select a host.




- The GaussDB/WI/HDC/License VM and GaussDB/WI/HDC VM must be deployed on different hosts.
- The two vAG/vLB VMs must be deployed on different hosts.

4. Set VM properties.




GaussDB/WI/HDC/License VM and GaussDB/WI/HDC VM:

| | | | |
|---|---|---|---|
| 1 | Name:<br>FA-DBHDCWILI<br>FA-DBHDCWI<br>Type:<br>Novell SUSE Linux Enterprise Server 11 SP1 64-bit | | |
| 2 | 4 vCPUs/8 GB memory/1 disk/1 NIC | | |
| 4 | 128000 | 5 | 8192 |

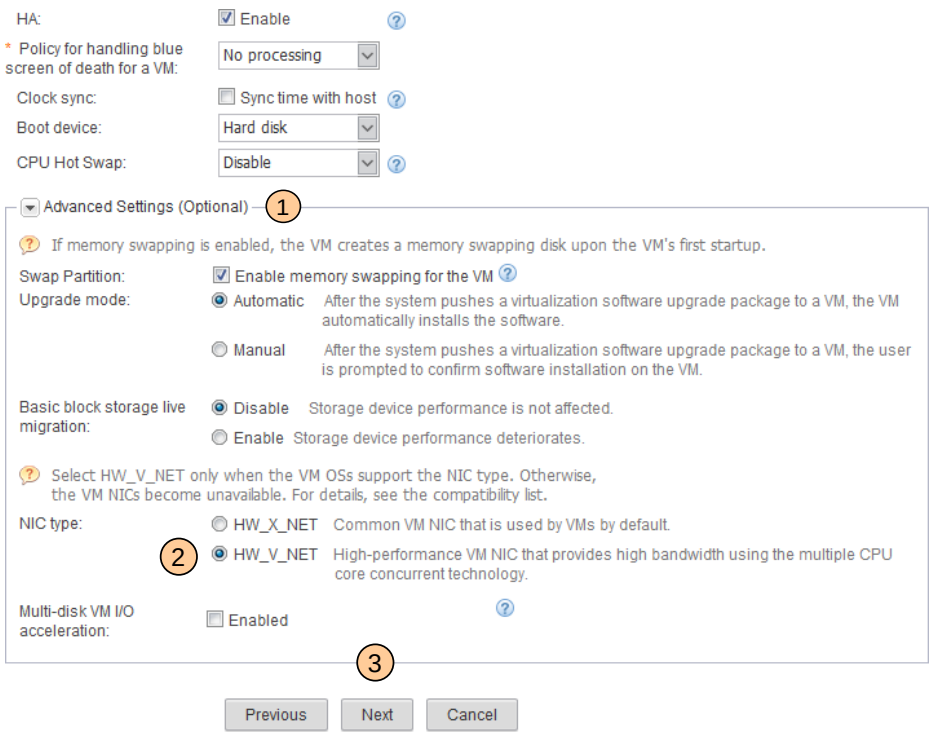
Two vAG/vLB VMs:

| | | | |
|---|---|---|---|
| 1 | Name:<br>FA-vAGvLB-1<br>FA-vAGvLB-2<br>Type:<br>Novell SUSE Linux Enterprise Server 11 SP1 64-bit | | |
| 2 | 4 vCPUs/4 GB memory/1 disk/2 NICs | | |
| 4 | 128000 | 5 | 4096 |

## 5.1 Creating Linux VMs

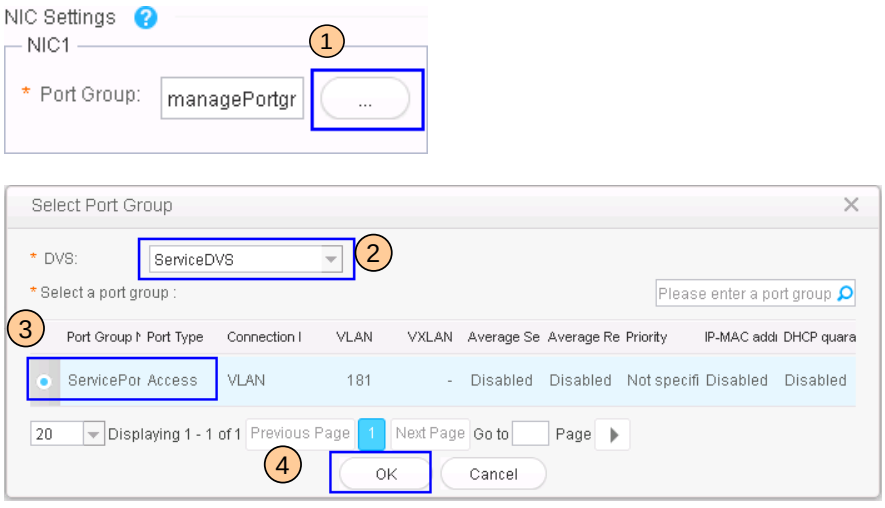
### Step 1: Create a bare VM.

5. (**Only for vAG, vLB, vAG/vLB**) Set 'NIC type' to 'HW_V_NET'.




When create **vAG, vLB, vAG/vLB VMs**, you should set **'NIC type'** to **'HW_V_NET'**.

6. Configure NICs.



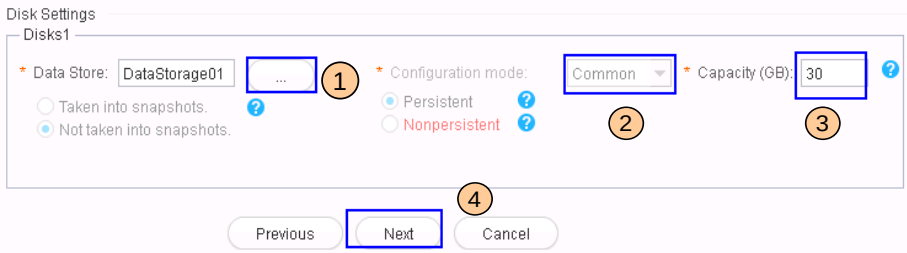
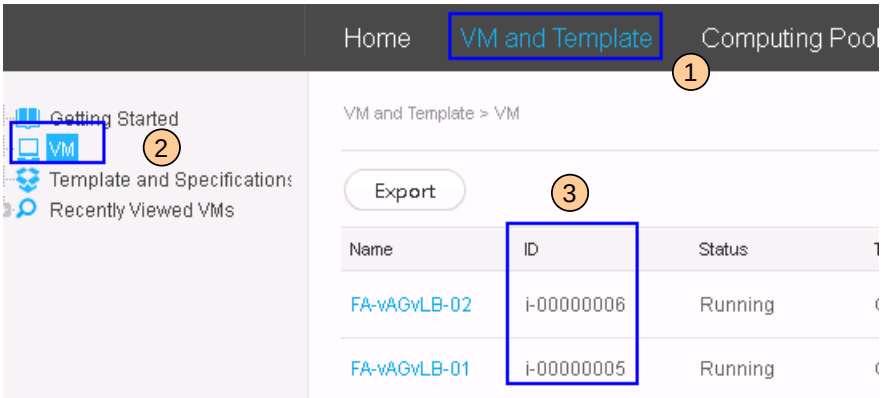

2 Select port groups based on actual plan.

3 Select the service plane port group for the first NIC; Select the management plane port group for the second NIC. **Among the Linux VMs in the scenarios described in this document, only vAG/vLB VMs have management plane NICs.**

7. Click **Next**.

## 5.1 Creating Linux VMs

### Step 1: Create a bare VM.

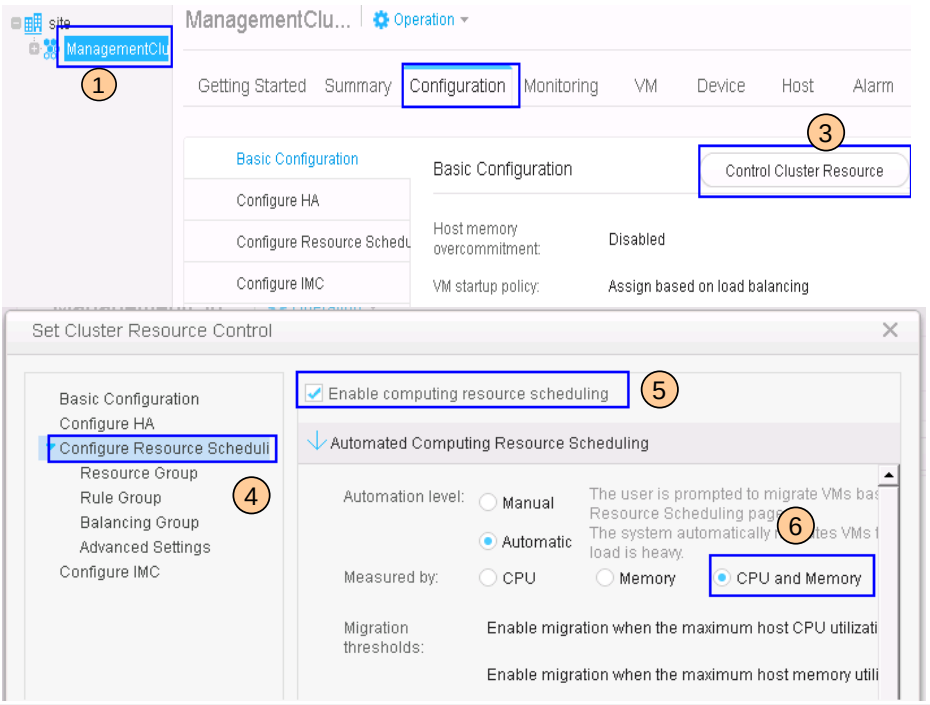
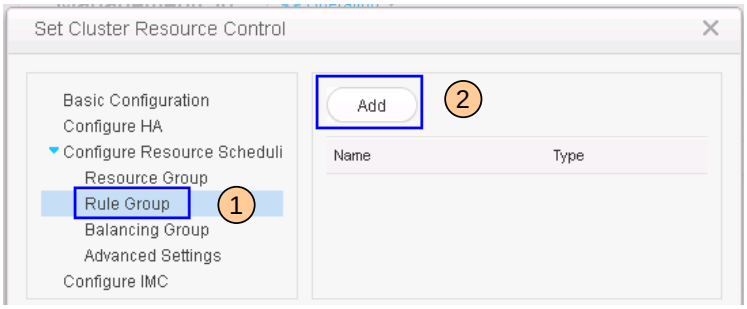
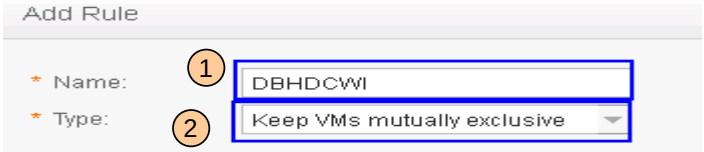
| | |
|---|---|
| 5. Configure disks.<br>  | 1 Select a non-virtualization data store. and set the **Configuration mode** to **Common**.<br>**CAUTION**<br>Select data stores in different RAID groups for the VMs working in active/standby mode.<br>3 30 |
| 9. Confirm the settings, and click **Finish**. Record the VM ID.<br>  | For example: i-0000006 |
| 10. Click **Create Another** and refer to the preceding steps to create the GaussDB/WI/HDC, active and standby vAG/vLB VMs. Record the VM ID. | - |

### Step 2 Set the automatic recovery attribute for Linux infrastructure VMs.

| | |
|---|---|
| 1. Log in to the VRM active node by using **PuTTY** with the **VRM floating IP address**. The login account is **gandalf**. | Default password: **Huawei@CLOUD8** |
| 2. Run the following command to switch to the **root** user.<br>**su – root**<br>**TMOUT=0** | Default password: **Huawei@CLOUD8!** |
| 3. For each newly created **infrastructure VM**, run the following command:<br>**sh /opt/galax/vrm/tomcat/script/modifyRecover.sh *vmId* true**<br>***vmId*** is the ID of the VM. | This command must be run for each infrastructure VM. |
| 4. Restart the VRM process.<br>**service vrmd restart**<br>Run this command only after the previous step is complete on all the VMs. | |
| 5. On the FusionCompute portal, choose **VM and Template**, click the **VM** tab, locate the row that contains the GaussDB/WI/HDC/License VM, choose **More** > **Forcibly stop**. | Stop and restart the VM for the configuration to take effect. |
| 6. After **Status** of the VM changes to **Stopped**, locate the row that contains the VM, choose **Start**. | - |
| 7. Refer to **5** to **6** to stop and start all Linux infrastructure VMs. | - |

## 5.1 Creating Linux VMs

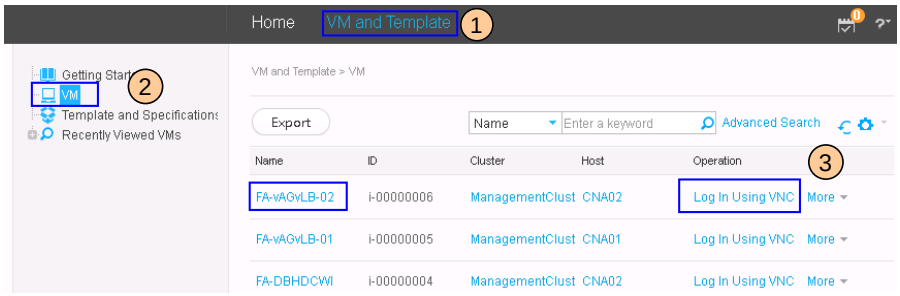
### Step 3 Set VMs to be mutually exclusive.

| | |
|---|---|
| 1. Choose **Computing Pool > Host and Cluster**. | |
| 2. Open the window for setting resource scheduling policies.<br>  | To ensure reliability, set the VMs of the same component to be mutually exclusive so that the VMs are always on different host nodes. When a host is faulty, FusionAccess can continue to work properly. |
| 3. Add a rule.<br>  | - |
| 4. Set **Type** to **Keep VMs mutually exclusive**.<br>  | |
| 5. Add the GaussDB/WI/HDC/License and GaussDB/WI/HDC VMs to **Selected VMs**. | - |
| 6. Click **OK** as prompted to add the rule. | - |
| 7. Refer to **3 to 6** to set vAG/vLB VMs to be mutually exclusive. | - |
| 8. On the lower part of the page, click **OK**. | - |

## 5.1 Creating Linux VMs

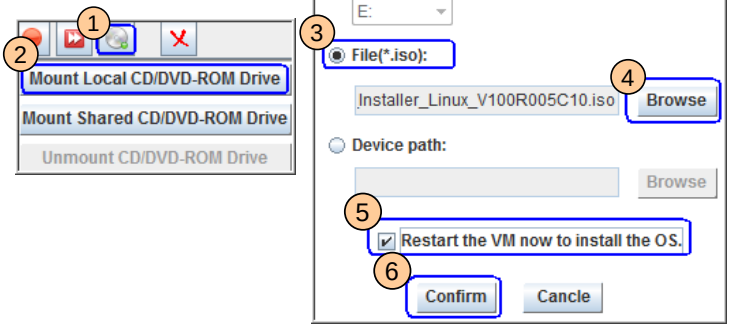
### Step 4 Install the OS.

1. Log in to the GaussDB/WI/HDC/License component VM.




3 Locate the row that contains the VM.

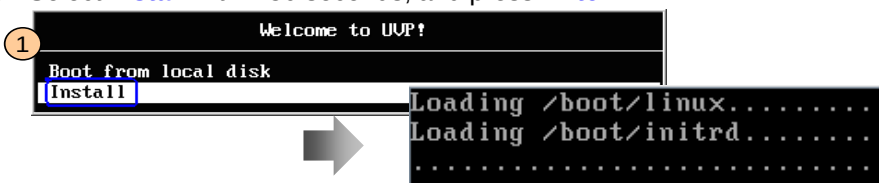
2. Mount a CD-ROM drive.




-

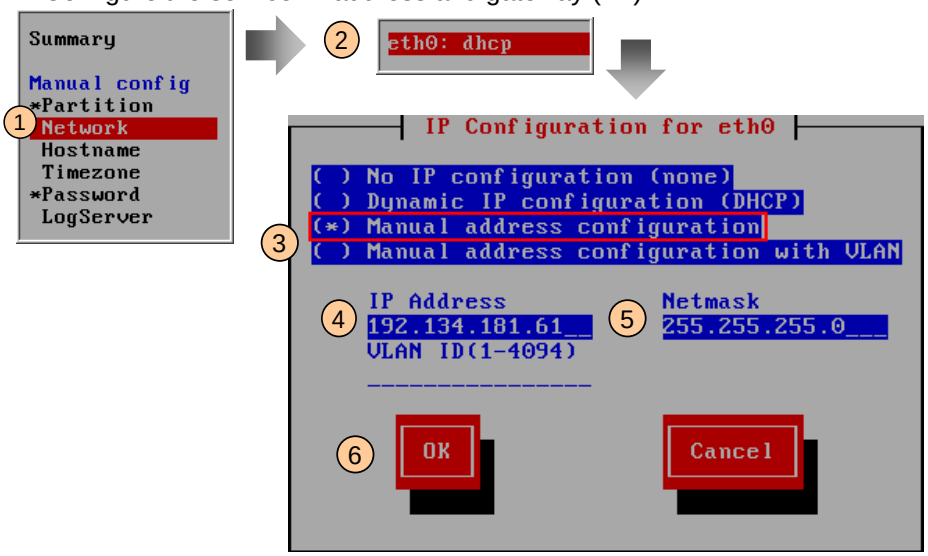
1

3. Select **Install** within 30 seconds, and press **Enter**.




Within 30 seconds

4. Configure the service IP address and gateway (B2).



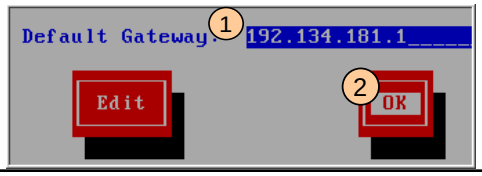
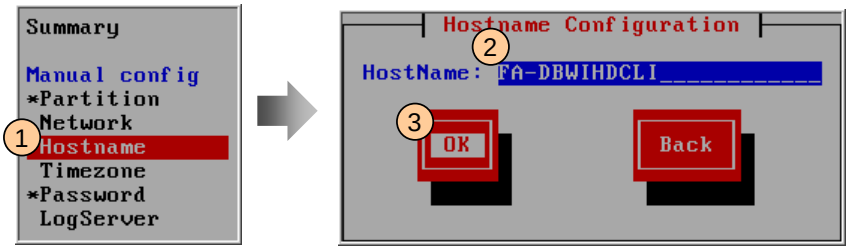
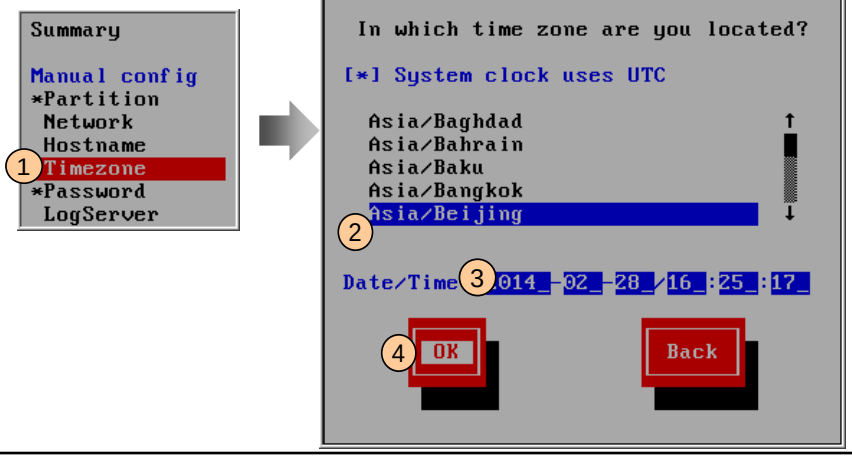

Repeat 2 3 4 5 6 to configure the management IP for the vAG/vLB VM, where 2 is **eth1: not configured**.

**Keyboard operations:**

- Press **Tab, ↑, or ↓** to move the cursor.
- Press **Enter** to select or execute the item that the cursor selects.
- Press the **space key** to select the item selected by the cursor.
- When you enter a **digit**, use the digital keys in the upper part of the **main keyboard area**.

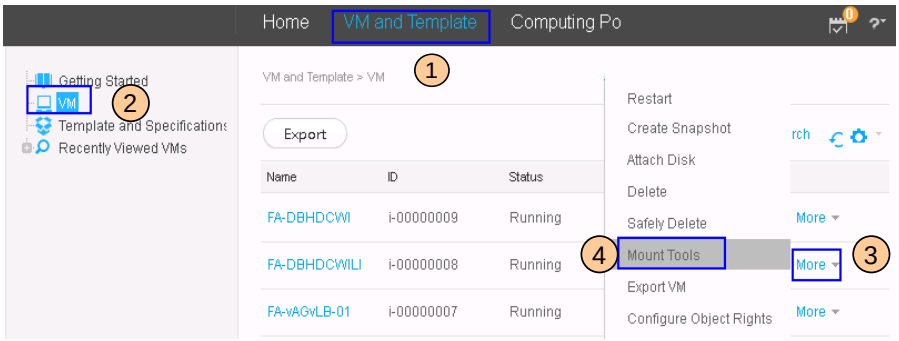
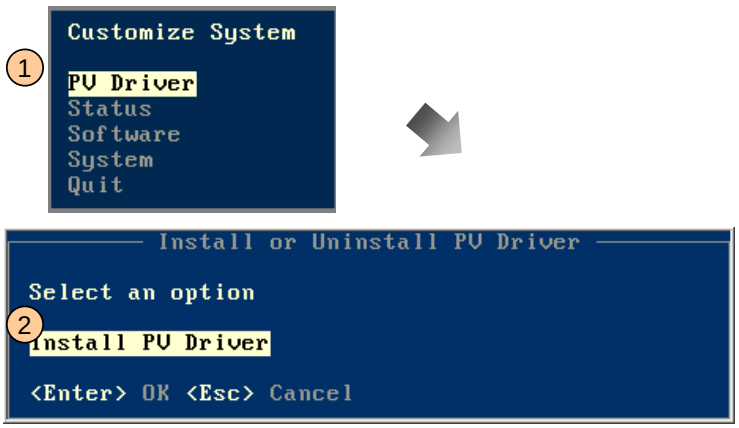
## 5.1 Creating Linux VMs

### Step 4 Install the OS.

| | |
|---|---|
| 5. Configure the gateway.<br>  | 1 Service plane gateway. |
| 6. Configure the host name (B2).<br>  | - |
| 7. Configure the time zone.<br>  | - |
| 8. Configure the password (C2).<br>  | - |
| 9. Press **F12** and press **Enter** twice to start the OS installation. | About 8 minutes. |
| 10. Log in to the VM using the root account and the password configured in step 8. | - |

## 5.1 Creating Linux VMs

### Step 5: Install the PV-Driver.

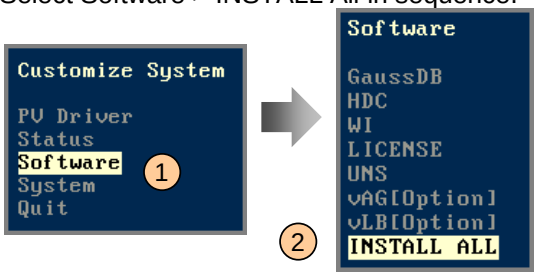
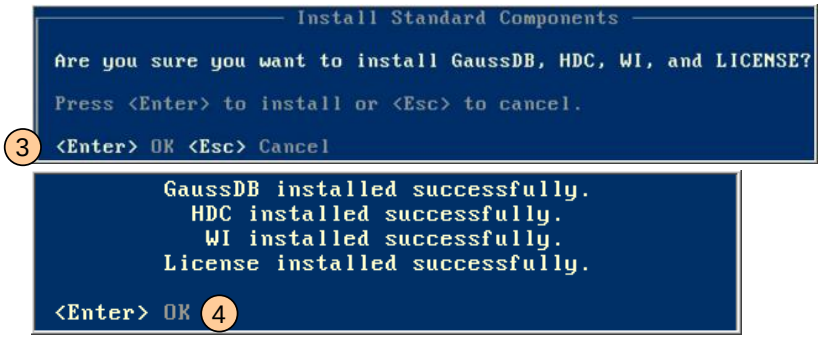
| | |
|---|---|
| 1. On the FusionCompute portal, mount tools on the GaussDB/WI/HDC/License VM.<br>  | (4) Locate the row that contains the GaussDB/WI/HDC/License VM. |
| 2. Click **OK** twice. | - |
| 3. In the VNC window on the VM, install the PV-Driver.<br>  | |
| 4. Press **Enter** twice to install the PV-Driver. | - |
| 5. After the PV-Driver is installed, press **F8** as prompted to restart the VM. | - |
| 6. After the restart, log in to the VM as the **root** user. | - |

### Step 6 Install other VMs.

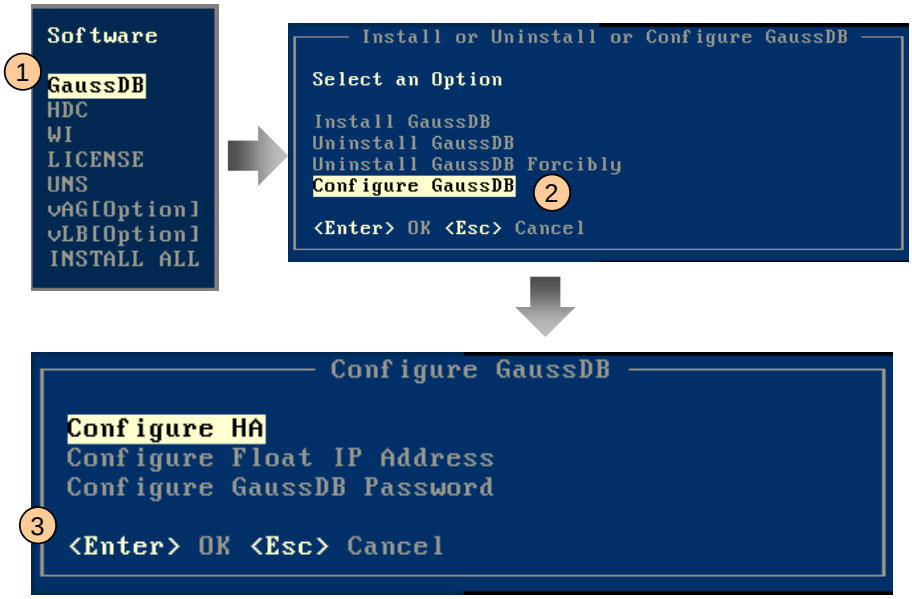
| | |
|---|---|
| 1. Refer to **step 4** to **step 5** in this section to install the following software on the GaussDB/HDC/WI VM and the active and standby vAG/vLB VMs:<br>1. Install the OS.<br>2. Install the PV-Driver. | You can install OS on different VMs at the same time. After OS installation, perform subsequent operation. |

## 5.2 Installing the GaussDB/HDC/WI/License Components

### Step 1 Install components.

| | |
|---|---|
| 1. In the VNC window on the VM, enter **startTools** to start the installation tool. | - |
| 2. Select Software > INSTALL All in sequence.<br>  | - |
| 3. Press **Enter**, after the installation finished and press **Enter**.<br>  | - |

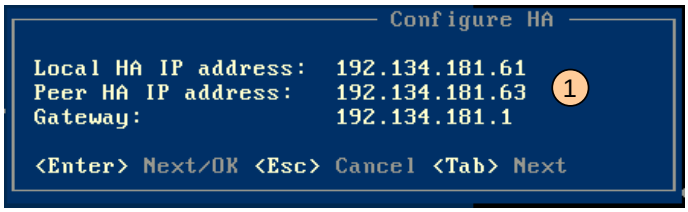
### Step 2 Configure the GaussDB

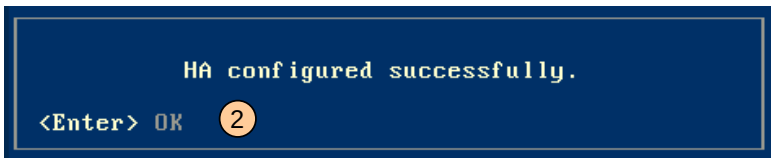
| | |
|---|---|
| 1. Configure HA information (B2).<br>  | - |

## 5.2 Installing the GaussDB/HDC/WI/License Components

### Step 2 Configure the GaussDB

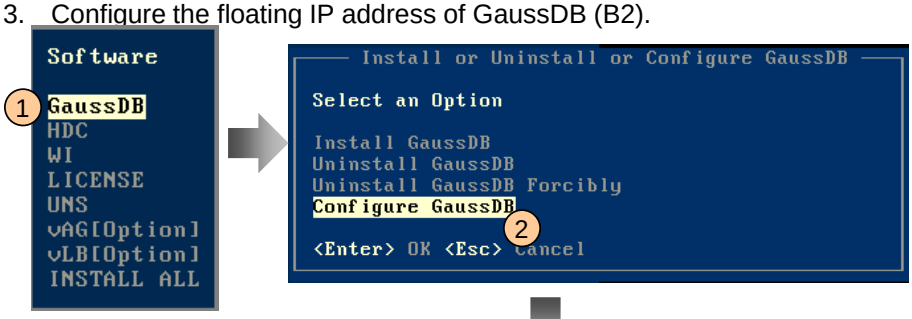
2. Configure HA information (B2).




1
- **Local HA IP Address** is the service plane IP address of this VM.
- **Peer HA IP address** is the service plane IP address of the peer VM that works with this GaussDB in active/standby mode.
- **Gateway:** service plane gateway

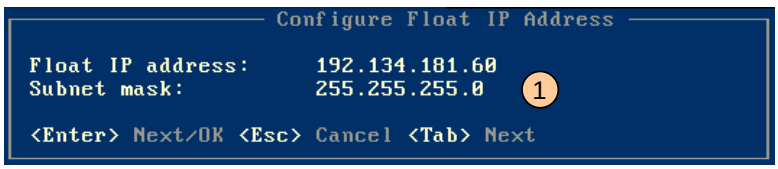
3. Configure the floating IP address of GaussDB (B2).





-

4. Configure the floating IP address of GaussDB (B2).





1
Floating IP address and subnet mask of GaussDB

## 5.2 Installing the GaussDB/HDC/WI/License Components

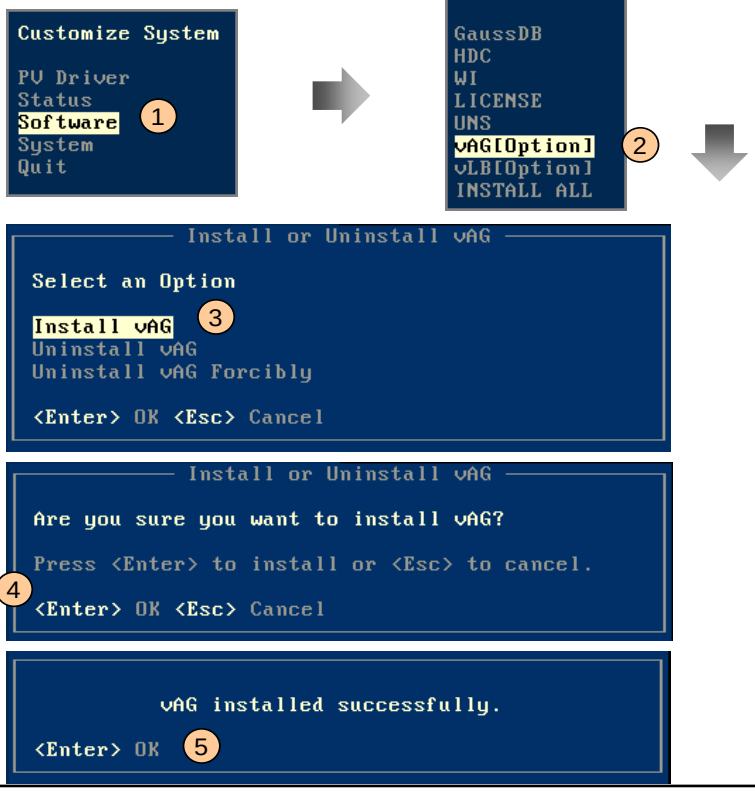
| Step 3 Install the GaussDB/HDC/WI server. | |
|---|---|
| 1. Refer to the previous information in this section, and log in to the GaussDB/HDC/WI component server to perform the following operations:<br>1. Select **install all** to install all components.<br>2. Configure the GaussDB HA information and floating IP address. | • The procedure for installing both the active and standby servers are the same, except for the data planning. You can obtain the data from the data planning table.<br>• The GaussDB components on the two servers work in active/standby mode. If HA is configured, the two servers are peers. |

## 5.3 Installing the vAGvLB Components

### Step 1 Install vAG.

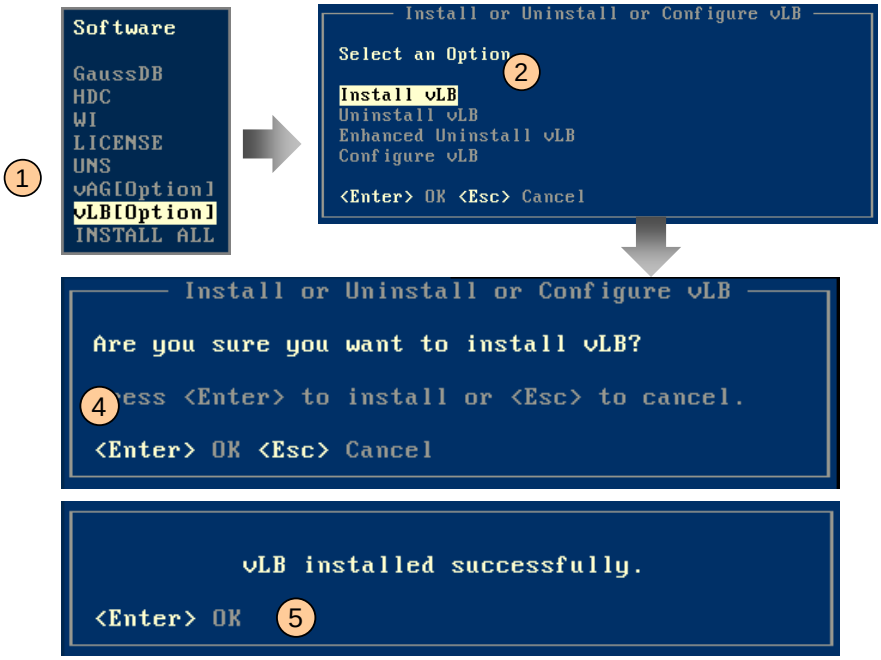
1. In the VNC window on the VM, enter **startTools** to start the installation tool. | -

2. Go to the installation directory.




### Step 2 Install vLB.

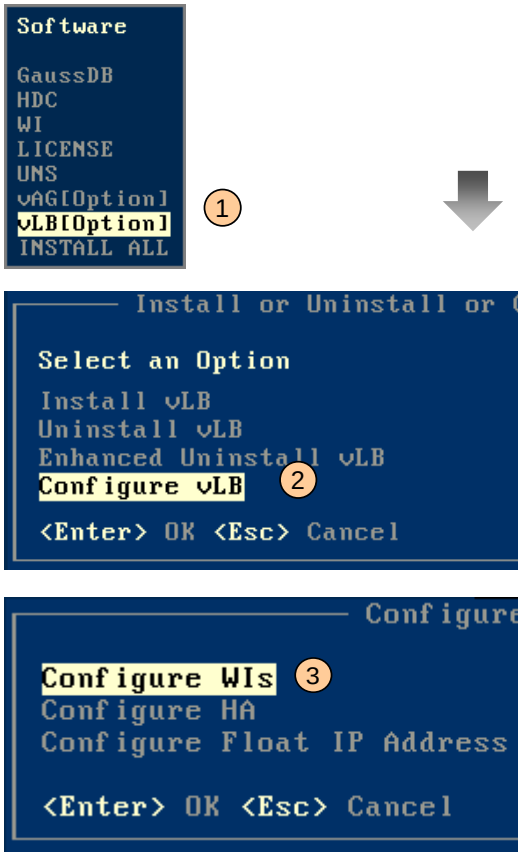
1. Run the installation program. | -



## 5. 3 Installing the vAGvLB Components

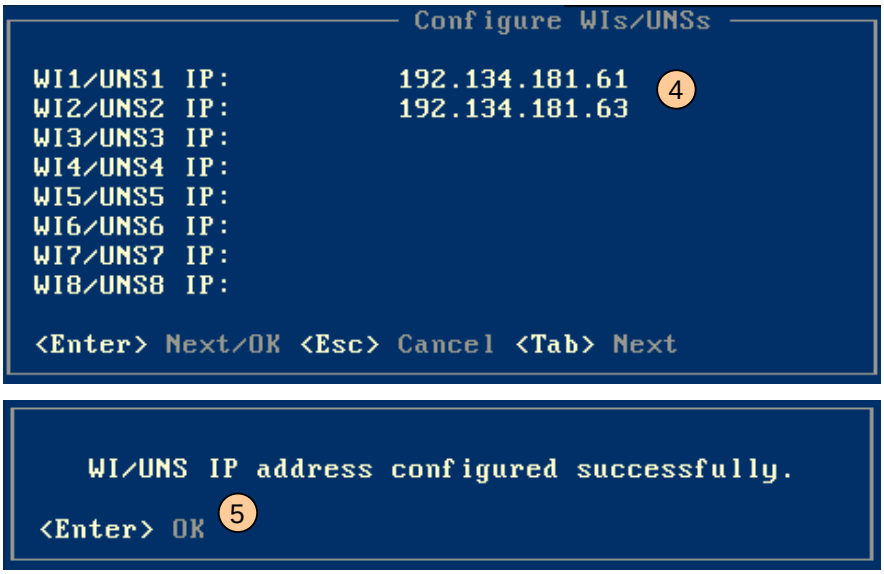
### Step 3 Configure the IP address of the WI/UNS servers.

1. Go to the installation directory.




-

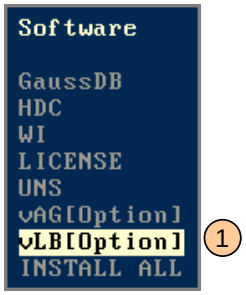
2. Configure the IP address of the WI/UNS servers (B2).

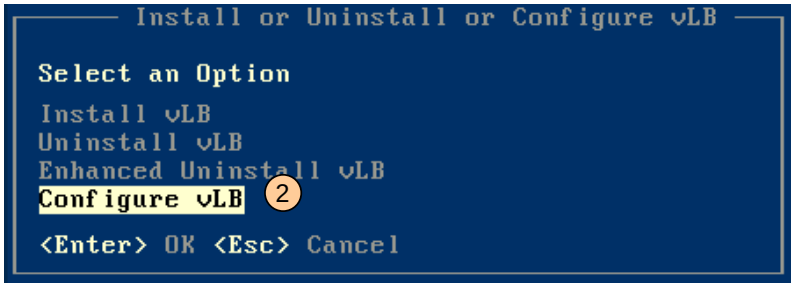


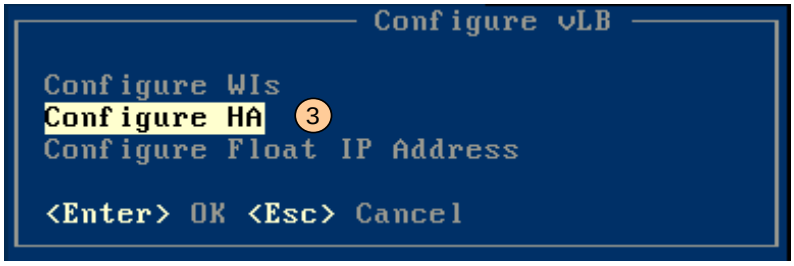

5 Service plane IP addresses of the WI/UNS servers.

## Step 4 Configure the HA of the vLB.

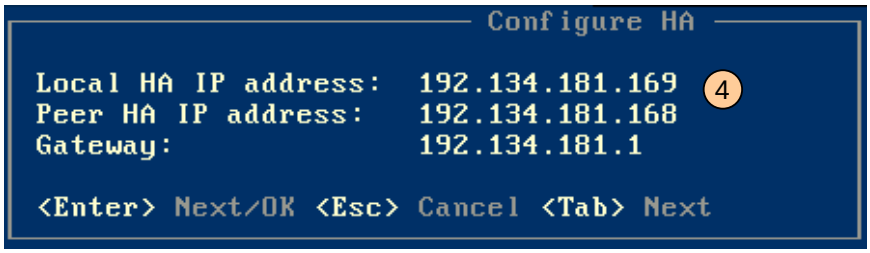
1. Configure the HA of the vLB (B2).

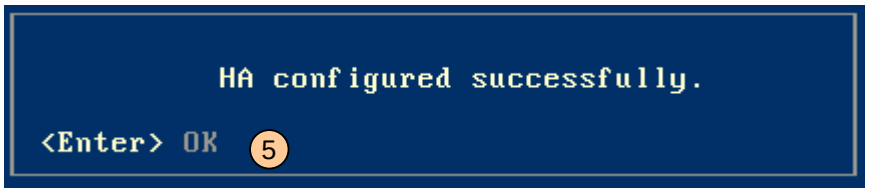



2. Configure the IP address of the HA (B2).




-

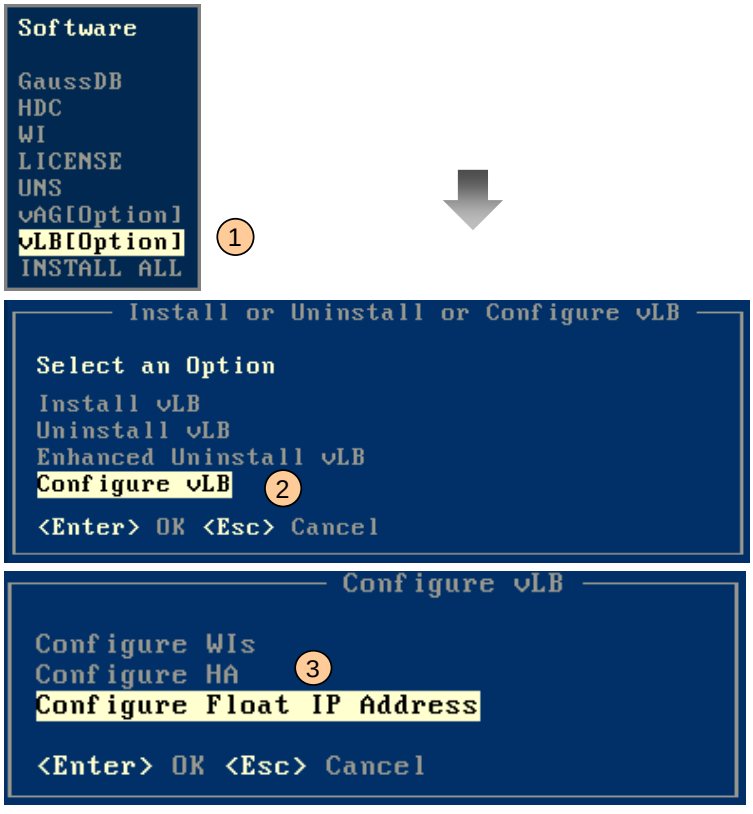
5

•**Local HA IP Address** is the service plane IP address of this VM.
•**Peer HA IP address** is the service plane IP address of the peer VM that works with this vLB in load balancing mode.
•**Gateway:** Service plane gateway

## 5. 3 Installing the vAGvLB Components

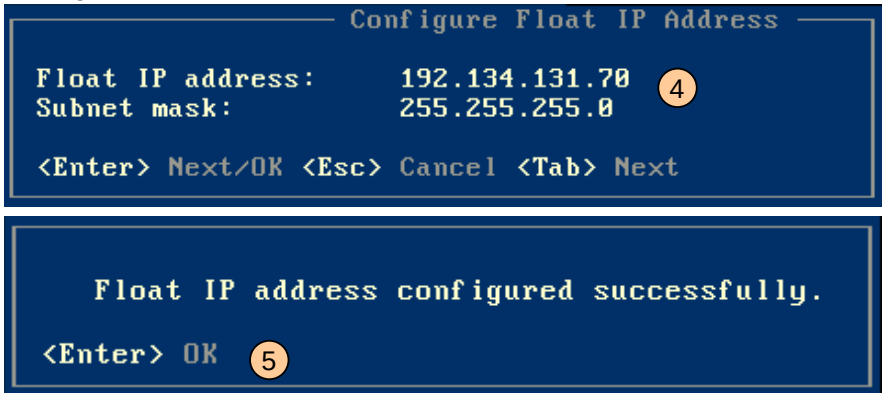
### Step 5 Configure the Float IP addresses for the vLB servers.

1. Go to the installation directory.




-

2. Configure the Float IP addresses for the vLB servers.




Service plane Float IP addresses of the vLB servers.

### Step 6 Install the vAG/vLB servers.

1. Refer to the previous information in this section, and perform the following operations to install the standby vAG/vLB component:
   1. Install the vAG component.
   2. Install the vLB component.
   3. Configure IP addresses for the WI servers.
   4. Configure the HA for the vLB servers.
   5. Configure the floating IP address for the vLB servers.

- The procedure for installing both the active and standby servers are the same, except for the data planning. You can obtain the data from the data planning table.
- The vLB components on the two servers

# 6 Installing Windows OS Infrastructure Components

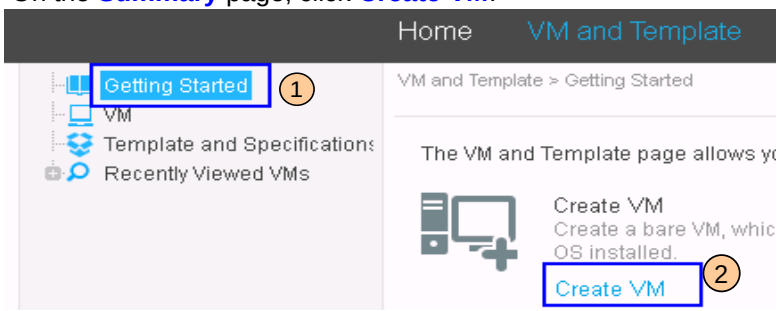
## 6.1 Creating an Infrastructure VM Template

### Step 1 Create a bare VM.

1. On the FusionCompute portal, choose **VDC Management > VM and Template**.

-

2. On the **Summary** page, click **Create VM**.

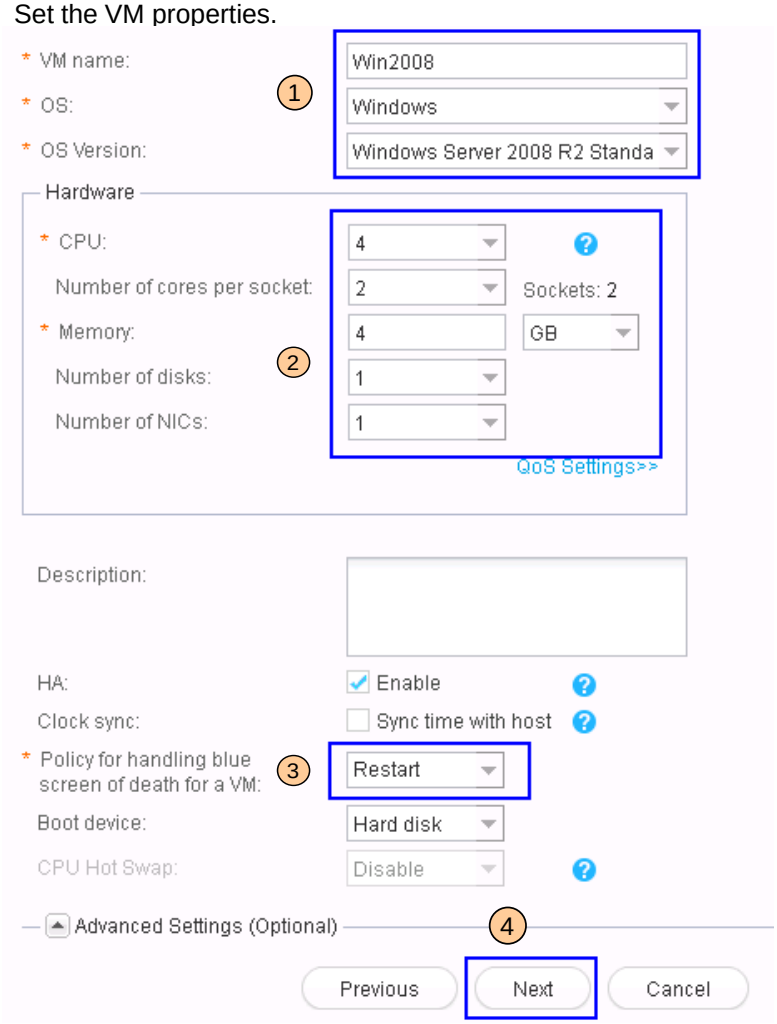



-

3. On the **Create VM** page, click **Next**.

-

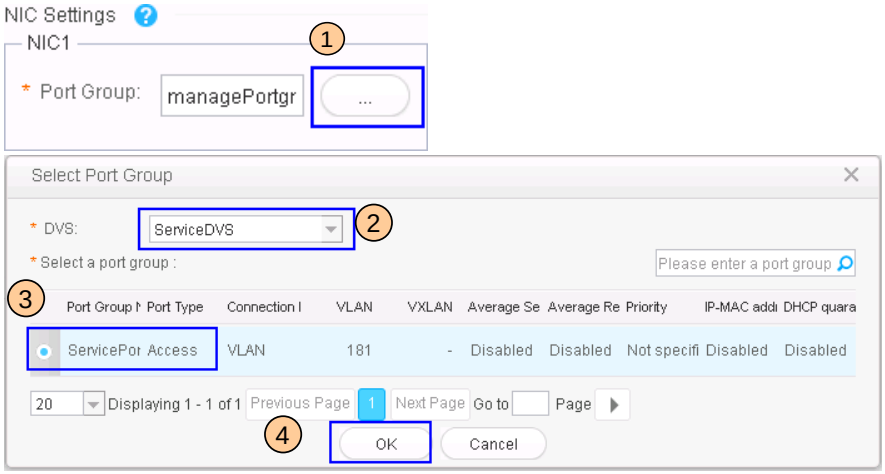
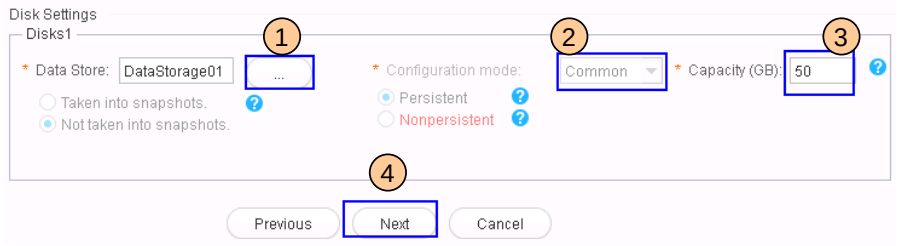
4. Set the VM properties.




| | |
|---|---|
| 1 | **VM name**: Customized<br>**OS version**: Windows Server 2008 R2 Standard 64bit |
| 2 | 4 VCPU/4 GB memory/1 disk/1 NIC |
| 3 | Select **Restart**. |

## 6.1 Creating an Infrastructure VM Template

### Step 1 Create a bare VM.

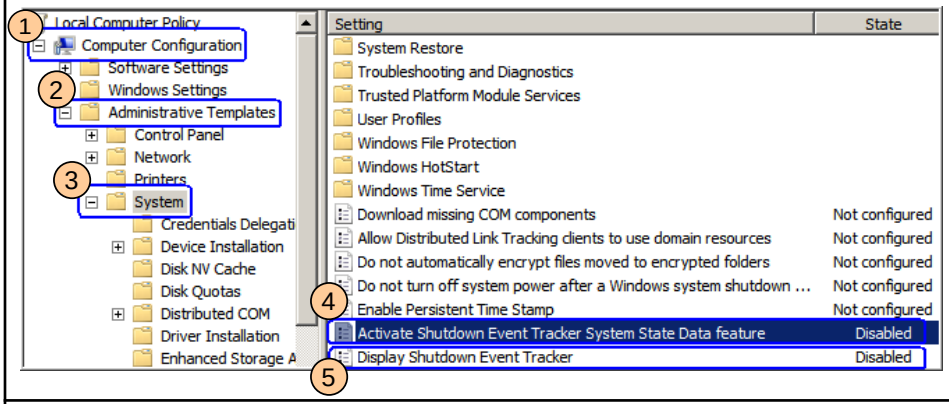
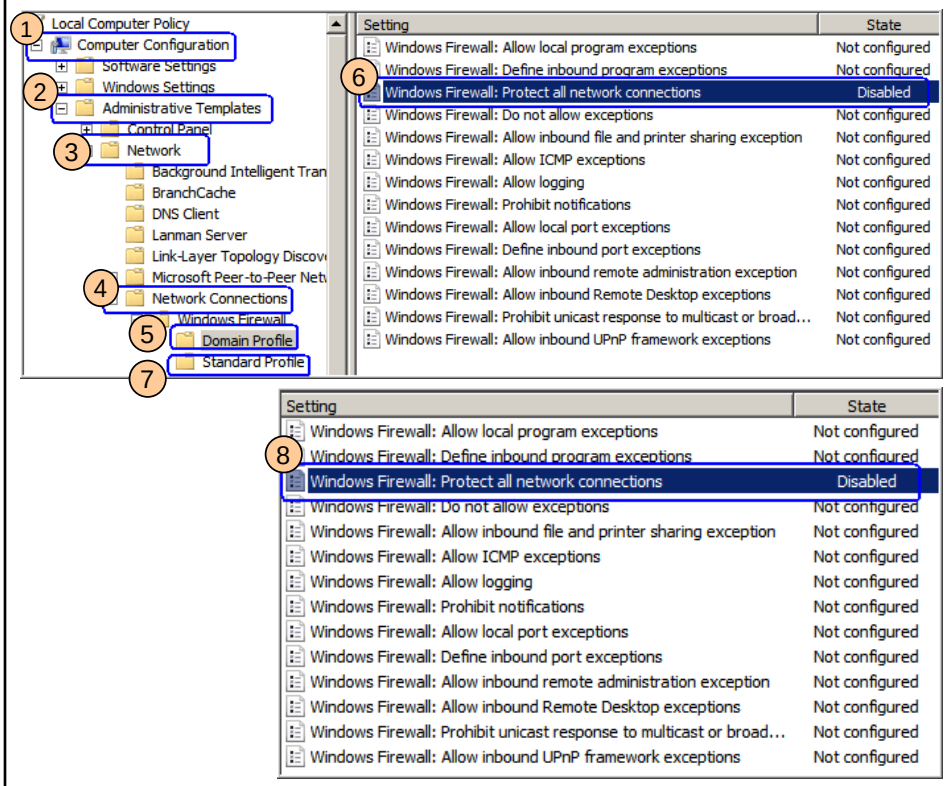
| | |
|---|---|
| 5. Set NICs.<br>  <br> | 2 Select the value based on the data plan.<br><br>3 Select the service plane port group. |
| 6. Set the disk.<br>  <br> | 1 Select a non-virtualization data store. The selected data store must ensure that the configuration mode can be set to **Common**.<br><br>3 Set the disk capacity to 50 GB. |
| 7. Confirm the entered information, and click **Finish**. | - |

### Step 2 Install the OS.

| | |
|---|---|
| 1. Log in to the VM created in step 1 using VNC. | - |
| 2. Mount the Windows Server 2008 ISO file, select **Restart the VM now to install the OS**, and click **OK**. | Windows2008R2SP1_EN.iso |
| 3. Install the OS as promoted, retain the default values of the parameters, set the password of **Administrator**, and log in to the VM. | The installation takes about 50 minutes. |

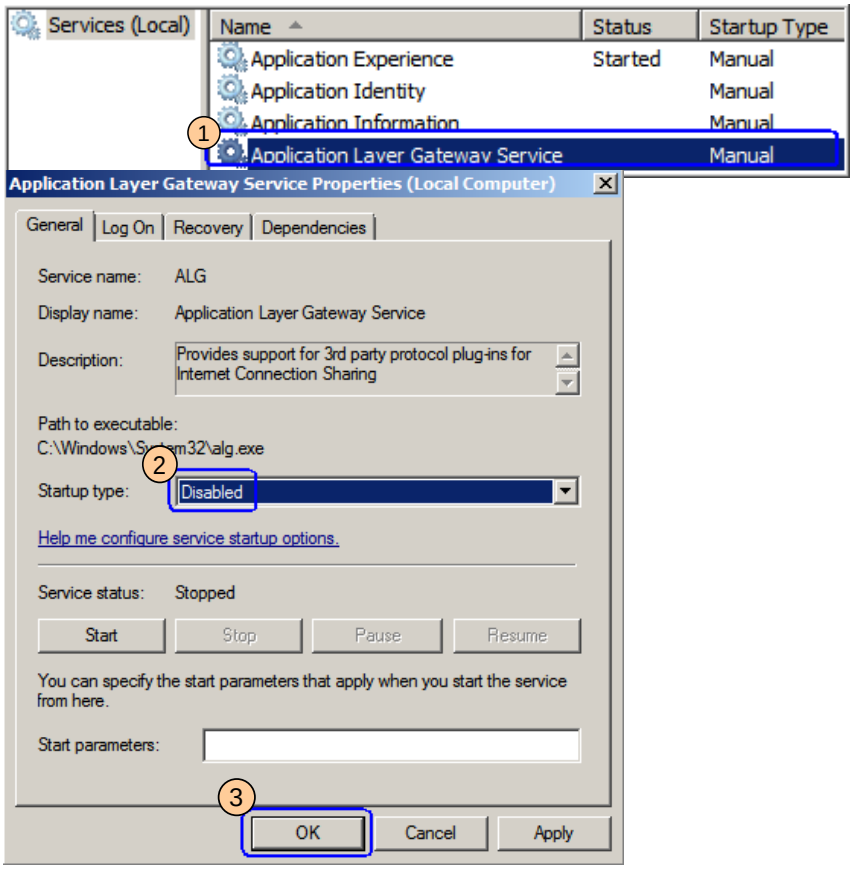
## 6.1 Creating an Infrastructure VM Template

### Step 3 Modify the group policies.

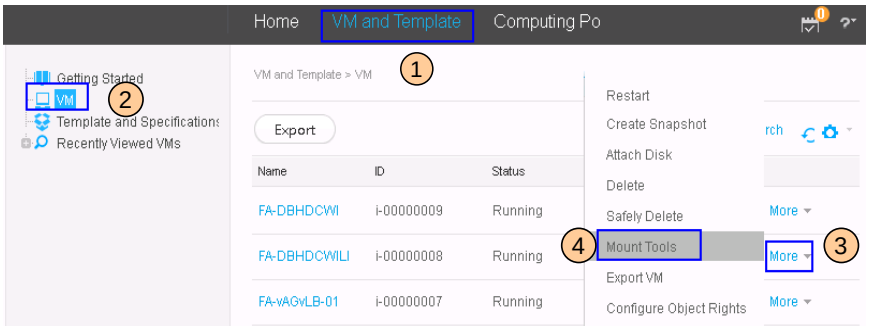
| | |
|---|---|
| 1. Click **Start**, enter **gpedit.msc** in **Search programs and files**, and press **Enter**. | - |
| 2. Disable the services in ④ and ⑤.<br>  | ④ ⑤ Double-click the service and select **Disabled**. |
| 3. Disable the firewall.<br>  | ⑥ ⑧ Double-click the service and select **Disabled**. |
| 4. Close the **Local Group Policy Editor** window. | - |

## 6.1 Creating an Infrastructure VM Template

### Step 4 Disable services.

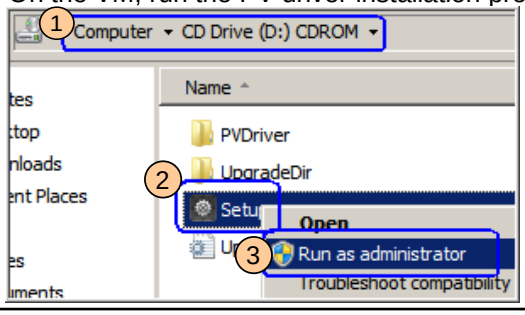
| | |
|---|---|
| 1. Click **Start**, enter **services.msc** in **Search programs and files**, and press **Enter.** | - |
| 2. Disable the Application Layer Gateway Service.<br>  | (1) Double-click the service, select **Disabled** in **Startup type,** and click **OK**. |
| 3. Disable the **Windows Firewall** service in the same way. | - |
| 4. Close the **Services** window. | - |

### Step 5 Install the paravirtualized (PV) driver.

| | |
|---|---|
| 1. On the FusionCompute portal, mount tools to the VM.<br>  | (3) Locate the row that contains the VM. |
| 2. Click **OK** twice. | - |

## 6.1 Creating an Infrastructure VM Template

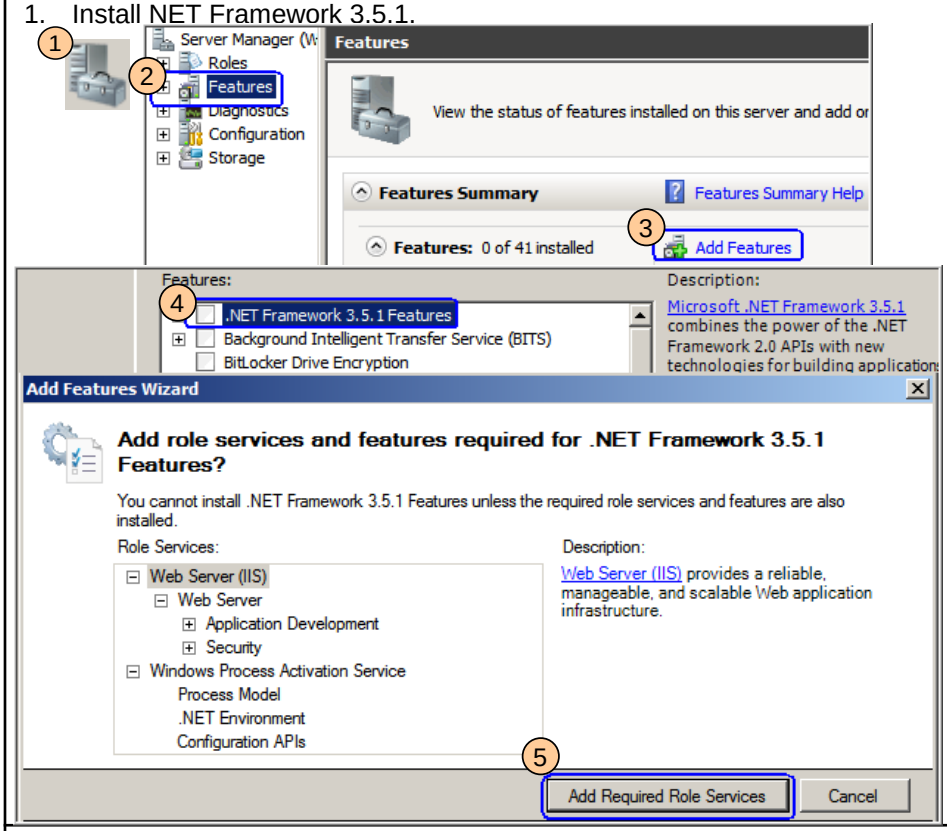
### Step 5 Install the PV driver.

| | |
|---|---|
| 3. On the VM, run the PV driver installation program.<br>  <br> | |
| 4. Install the PV driver as prompted and restart the VM. | The VM restarts twice during the installation. |

### Step 6 Copy the log collecting tool and health check tool.

| | |
|---|---|
| 1. In the VNC login window, mount **FusionAccess_Installer_Win_V100R005C20SPC100.iso**. | Do not select **Restart the VM now to install the OS** |
| 2. Switch to the CD-ROM drive directory and copy the **FusionCare** folder under the **tools** folder to drive C on the VM. | |

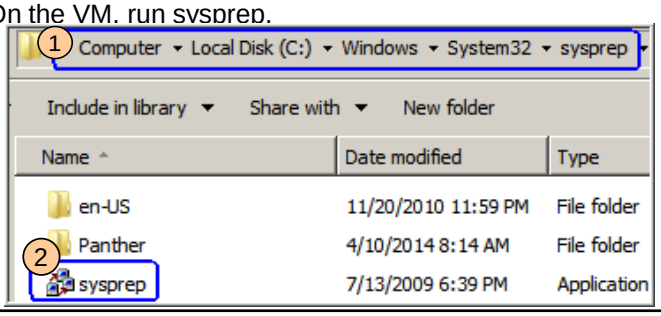
### Step 7 Install .NET Framework 3.5.1.

| | |
|---|---|
| 1. Install NET Framework 3.5.1.<br>  <br> | 1  is displayed in the lower left corner on the VM screen. |
| 2. Click **Next** and complete the installation as prompted. | - |
| 3. Close the **Server Manager** window. | - |

## 6.1 Creating an Infrastructure VM Template

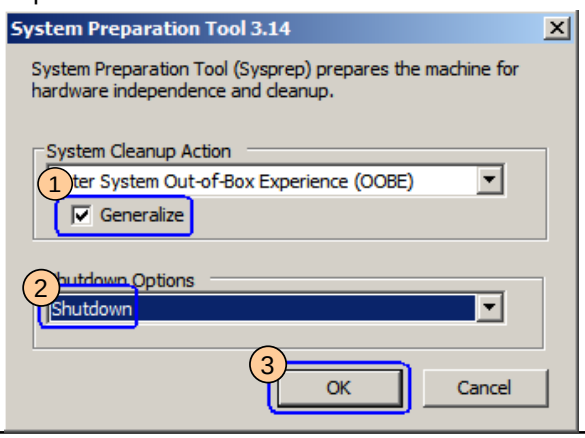
### Step 8 Encapsulate the template.

1. On the VM, run sysprep.




2 Double-click **sysprep**.

2. Set parameters.



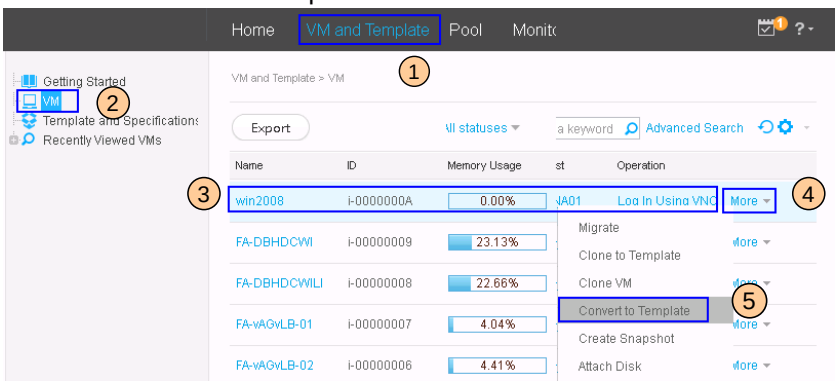

The VM shuts down automatically after **sysprep** is executed.

### Step9 Create an infrastructure template.

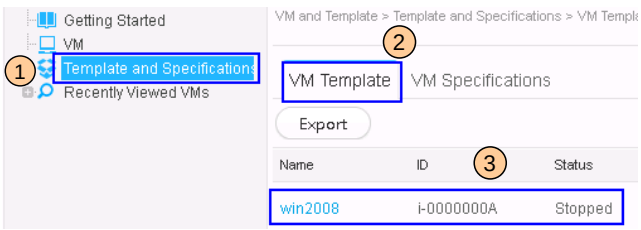
1. On the FusionCompute portal, choose **VM and Template**.

-

2. Convert the VM into a template.




3. Query the template status in the navigation tree.




If the template VM is displayed in **Recently Viewed Templates**, the template VM is converted into a template.

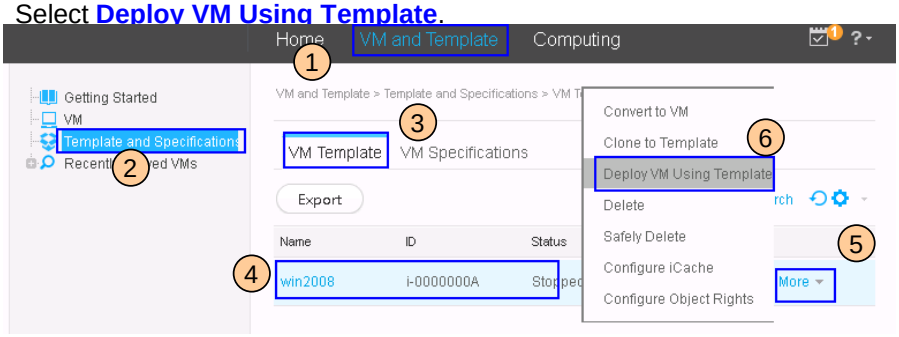
## 6.2 Creating and Setting Infrastructure VMs

### Step 1 Create infrastructure VMs.

1. On the FusionCompute portal, choose **VM and Template> Template and Specifications**.

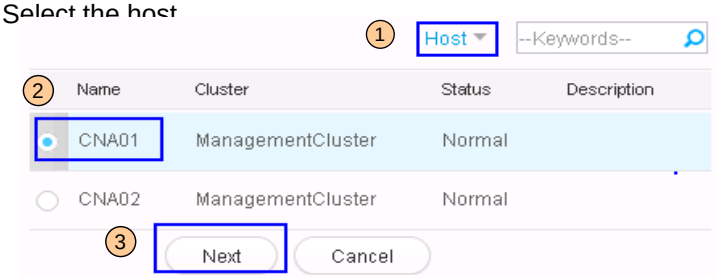
-

2. Select **Deploy VM Using Template**.




3 Select the appropriate template.

3. Select the host

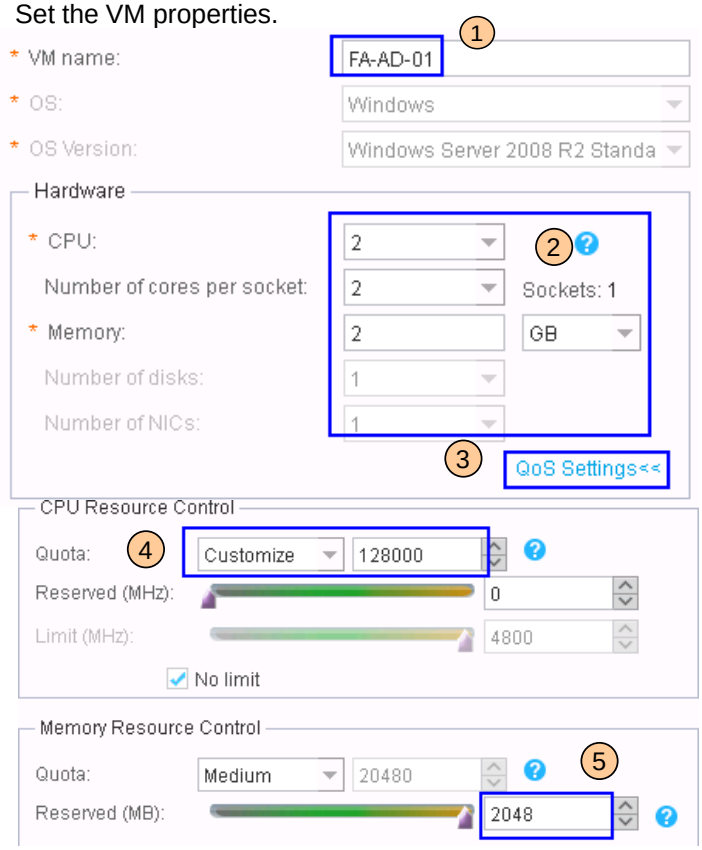



2 The VMs working in active/standby mode must be deployed on different CNAs.

4. On the **Create VM** page, click **Next**.

-

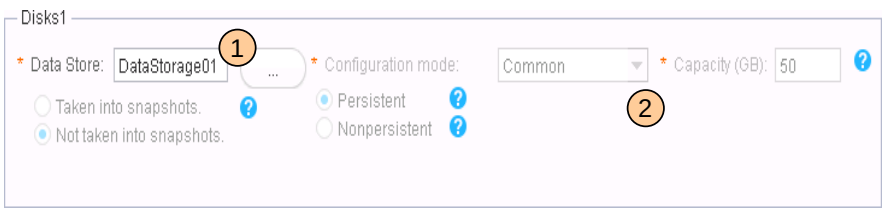
5. Set the VM properties.




| | |
|---|---|
| Two AD/DNS/DHCP VMs: | |
| 1 | FA-AD-1/FA-AD-2 |
| 2 | 2 VCPUs/2 GB memory |
| 4 | 128000 |
| 5 | 2048 |
| Two ITA VMs: | |
| 1 | FA-ITA-1/FA-ITA-2 |
| 2 | 4 VCPUs/4 GB memory |
| 4 | 128000 |
| 5 | 4096 |
| One Loggetter VM: | |
| 1 | FA-LogTCM |
| 2 | 2 VCPUs/2 GB memory |
| 4 | 128000 |
| 5 | 2048 |

## 6.2 Creating and Setting Infrastructure VMs

### Step 1 Create infrastructure VMs.

| | |
|---|---|
| 5. Click **Next**. | - |
| 6. Set the disk.<br>  | **CAUTION**<br>Select data stores in different RAID groups for the VMs working in active/standby mode.<br>1 Select the data store. The selected data store must ensure that the configuration mode 2 can be set to **Common**. |
| 7. Click **Next**, confirm the entered information, and click **Finish**. | |
| 8. Click **Create Another** and create the other infrastructure VMs in the same way. | - |

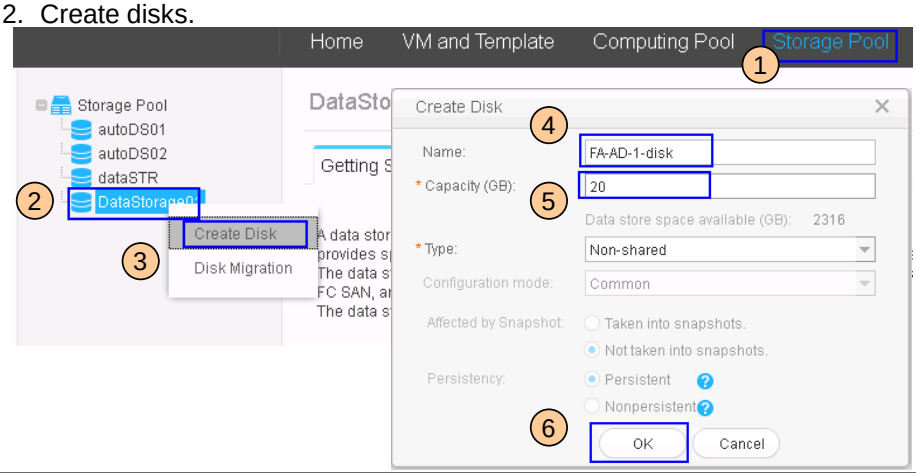
### Step 2 Set the automatic recovery attribute for infrastructure VMs and set VMs to be mutually exclusive.

| | |
|---|---|
| 1. Set the **automatic recovery** for all the Windows infrastructure VMs, and set the following Windows VMs to be **mutually exclusive**:<br>• Set FA-AD-1 and FA-AD-2 to be mutually exclusive.<br>• Set FA-ITA-1 and FA-ITA-2 to be mutually exclusive. | For details, see Set 5.1 Creating Linux VMs.<br>**automatic recovery**: Step 2<br>**Mutually exclusive**: Step 3 |

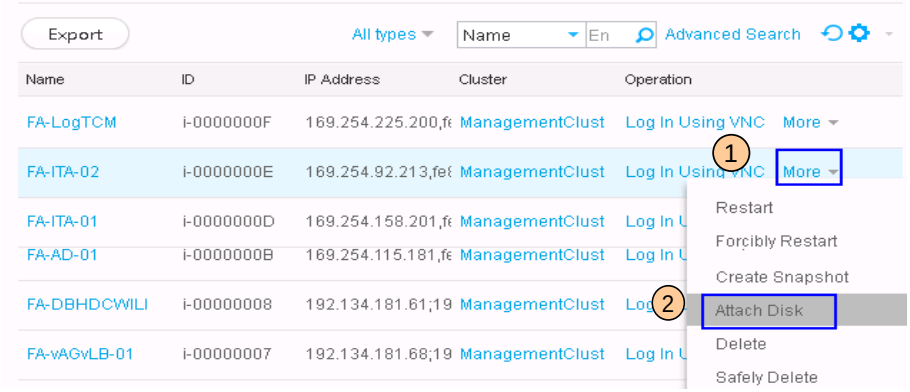
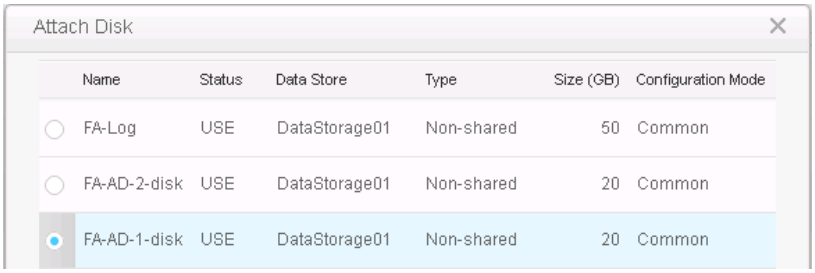
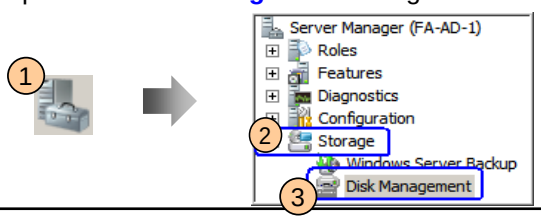
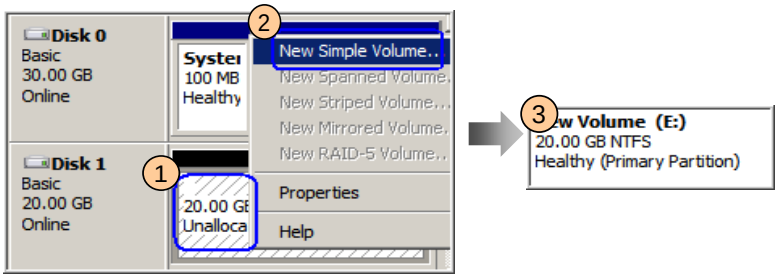
### Step 3 Set basic VM information.

| | |
|---|---|
| 1. Log in to FA-AD-1 using VNC. | - |
| 2. Set the region, time, and keyboard, enter the product key, and reset the administrator password as prompted. | - |
| 3. Set FA-AD-2, FA-ITA-1, FA-ITA-2, and FA-LogTCM in the same way. | - |

### Step 4 Add user disks.

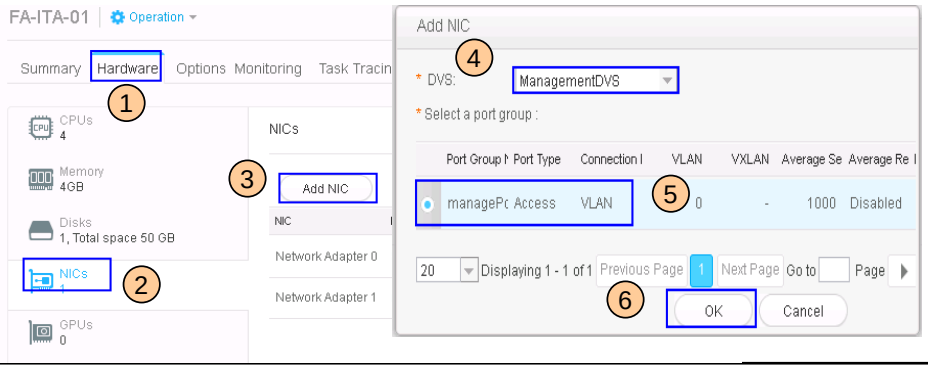
| | |
|---|---|
| 1. Choose **Storage Pool**. | - |
| 2. Create disks.<br>  | 1 Select a data store for the user disk. You can select any type of data store for creating the user disk.<br>Two AD/DNS/DHCP VMs:<br>4 FA-AD-1/FA-AD-2<br>5 20<br>One Loggetter VM:<br>4 FA-LogTCM<br>5 50 |
| 3. Click **OK** continuously and complete the disk creation for the active AD/DNS/DHCP VM. | |

## Step 4 Add user disks.

| | |
|---|---|
| 4. Repeat steps **2 to 4** to create disks for the standby AD/DNS/DHCP VM and Loggetter VM. | - |
| 5. Choose **VM and Template > VM** and click **FA-AD-1** on the **VM** tab. | - |
| 6. Select the VMs.<br>  | |
| 7. Select the disk.<br>  | - |
| 8. Click **OK** to attach the disk to the VM. | - |
| 9. Log in to **FA-AD-1** using VNC. | - |
| 10. Open the **Disk Management** dialog box.<br>  | - |
| 11. Set parameters as prompted. | |
| 12. Format the disk.<br>  | ③ Shows the disk status after formatting. |
| 13. Repeat steps **5 to 12** to bind and format the disks of the standby AD/DNS/DHCP VM and the Loggetter VM. | - |

## 6.2 Creating and Setting Infrastructure VMs

### Step 5 Add NICs.

| | |
|---|---|
| 1. Choose **VM and Template > VM** and click **FA-ITA-1** on the **VM** tab. | - |
| 2. Add NICs.<br>  | 5 Select the distributed switch on the management plane. |
| 3. Add NICs for the standby ITA VM FA-ITA-2 in the same way. | - |

### Step 6 Set the VM time on all VMs. (**Perform this operation on all VMs**.)

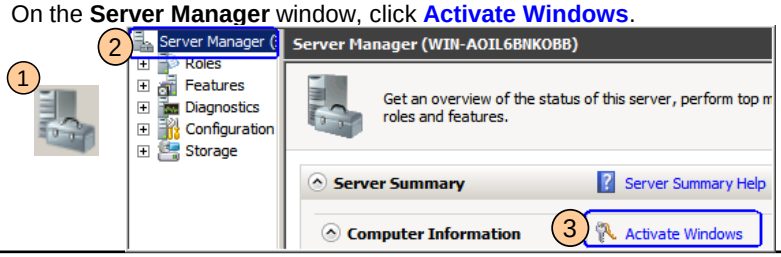
| | |
|---|---|
| 1. Log in to the VM using VNC and set the VM time. | - |
| 2. (Optional) Set the daylight saving time (DST).<br>• If DST is observed by the time zone on Windows, select **Automatically adjust clock for Daylight Saving Time** and set the DST.<br>• If DST is not observed by the time zone on Windows, download **TZEDIT.exe** and set the DST. | Set the VM time based on site requirements. |

### Step 7 Set VM IP addresses on all VMs. (**Perform this operation on all VMs**.)

1. Set IP addresses.

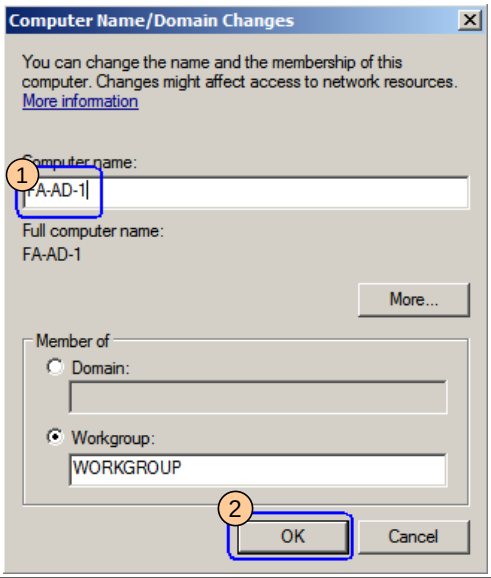
| Address | First NIC (For all VMs) | Second NIC (Only for ITA) |
|---|---|---|
| IP address/subnet mask | Service plane IP address | Management plane IP address |
| Default gateway IP address | Service plane gateway IP address | N/A |
| Primary DNS server | IP address of the active DNS server | N/A |
| Secondary DNS server | IP address of the standby DNS server | N/A |

### Step 8 Activate the VM OS on all VMs. (**Perform this operation on all VMs**.)

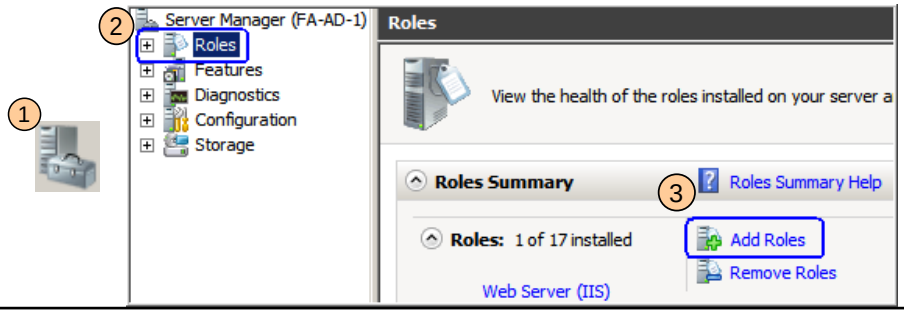
| | |
|---|---|
| 1. On the **Server Manager** window, click **Activate Windows**.<br>  | - |
| 2. Enter the product key and activate the OS as prompted.<br>**CAUTION**<br>Use the correct product key for the OS. If a product key for an OS in the Chinese edition is used to activate an OS in the English edition, the blue screen of death (BSOD) will occur on the infrastructure VM. | |

## 6.3 Installing the AD/DNS Services

### Step 1 Change the AD/DNS server names. **(The operations on the active and standby servers are the same.)**

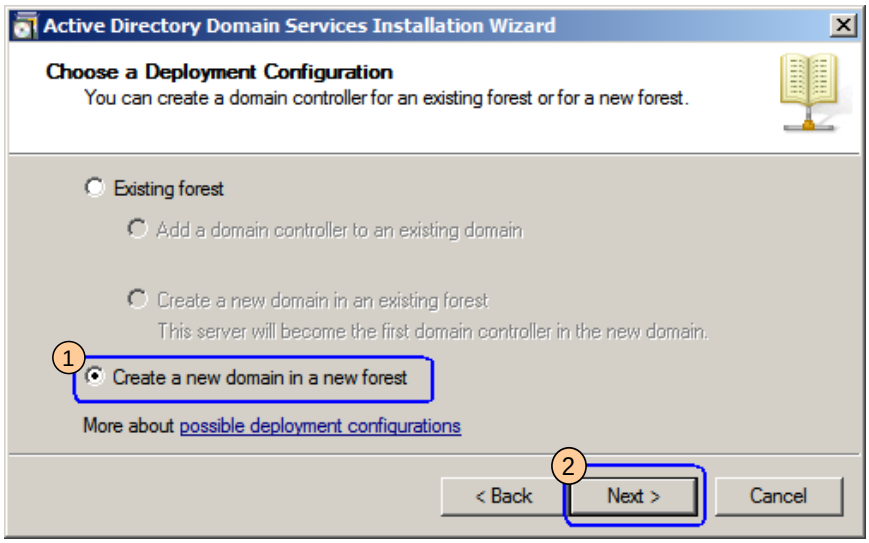
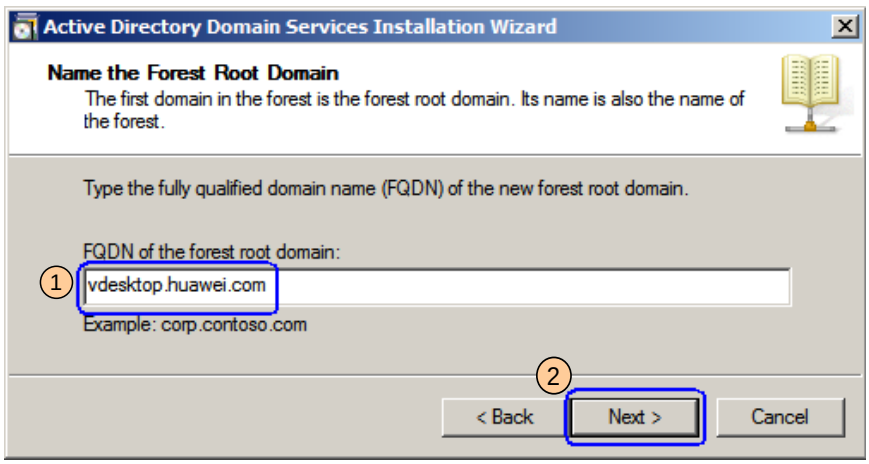
| | |
|---|---|
| 1. Log in to the FA-AD-1 using VNC. | To change the standby server name, log in to the FA-AD-2 VM. |
| 2. Click **Start**, enter **sysdm.cpl** in **Search programs and files**, and press **Enter**. Then, click **Change** in the **System Properties** dialog box. | - |
| 3. Change the computer name for the VM.<br>  | - |
| 4. Restart the VM as prompted. | - |

### Step 2 Add the AD role. **(The operations on the active and standby servers are the same.)**

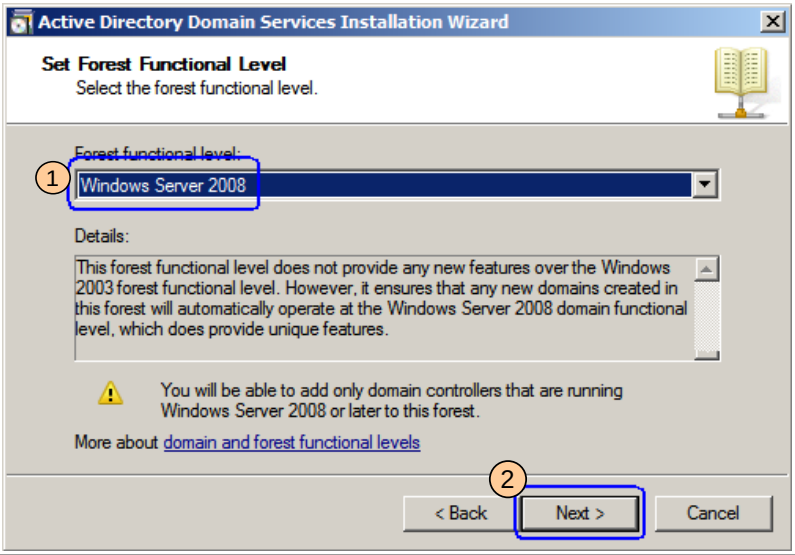
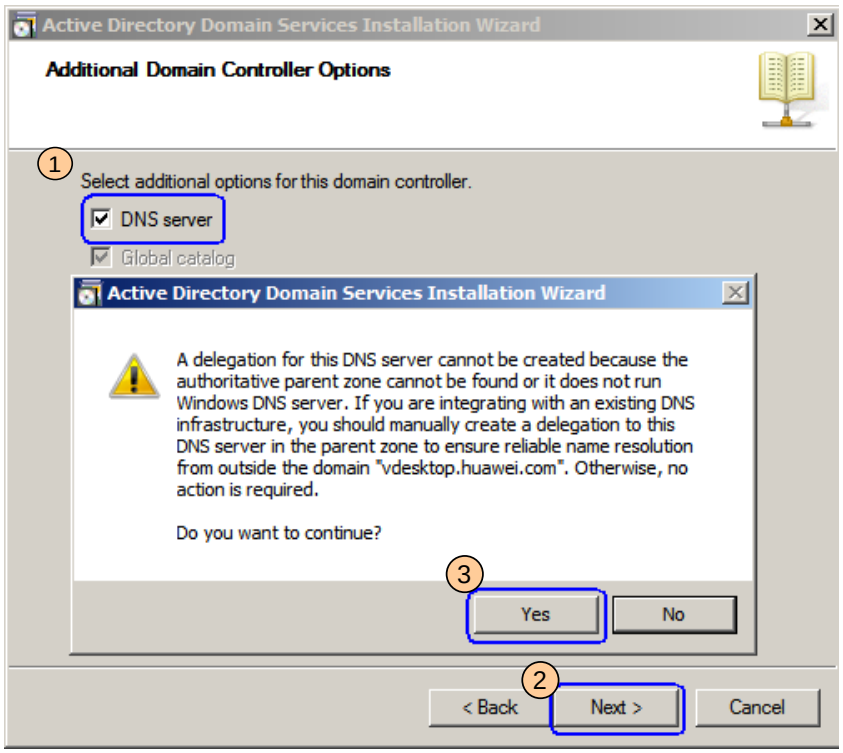
| | |
|---|---|
| 1. Add Roles.<br>  | - |
| 2. Click **Next**. | - |

## 6.3 Installing the AD/DNS Services

| **Step 2 Add the AD role. (The operations on the active and standby servers are the same.)** | |
|---|---|
| 3. Select **Active Directory Domain Services**.<br>  | - |
| 4. Add the AD role as prompted. | - |

| **Step 3 Install the AD/DNS. (The second column describes the different operations on the standby server.)** | |
|---|---|
| 1. Click **Start**, enter **dcpromo.exe** in **Search programs and files**, and press **Enter**. | The operations are the same on the standby server. |
| 2. Retain the default values and go to the following page as prompted.<br>  | Standby server:<br>Select **Existing forest** > **Add a domain controller to an exiting domain** and click **Next**. |
| 3. Set a domain name.<br>  | Standby server:<br>On **Network credentials**, enter the **FQDN of the forest root domain** and click **Set**. Enter the **Administrator account and password of** the active AD server and click **Next**.<br>Proceed as prompted until the dialog box shown in **Step 6** is displayed. |

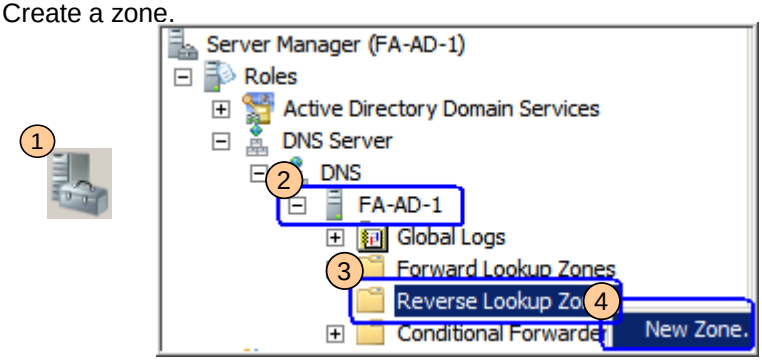
## 6.3 Installing the AD/DNS Services

| **Step 3 Install the AD/DNS. (The second column describes the different operations on the standby server.)** | |
|---|---|
| 4. Set the forest functional level.<br>  | Standby server: No this operation. |
| 5. Set **Forest functional level** to **Windows Server 2008** and click **Next.** | Standby server: No this operation. |
| 6. Add the DNS server.<br>  | The operations on the standby server are the same. |
| 7. Click **Next**. Set the restore Directory Services Restore Mode (DSRM) password, install the services as prompted, and restart the VM. | The operations on the standby server are the same. |

## 6.3 Installing the AD/DNS Services

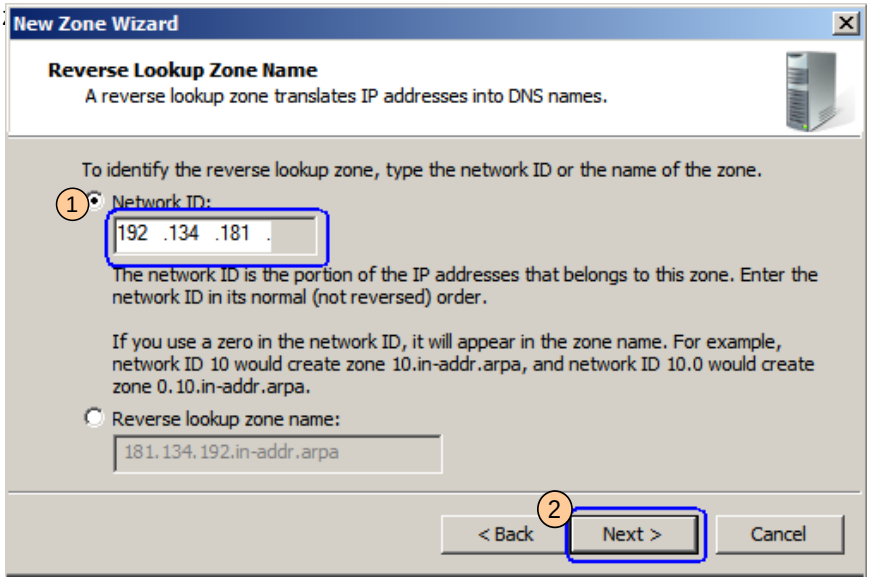
**Step 4 Configure reverse DNS lookup. (Perform this operation only on the active server.)**

1. Create a zone.




-

2. Retain the default values and go to the page for setting the reverse lookup




-

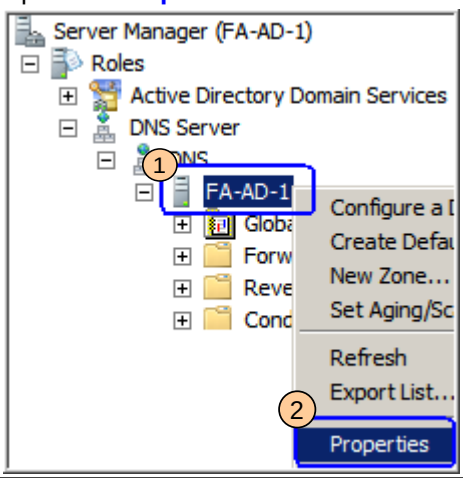
3. Complete the configuration as prompted.

-

## 6.3 Installing the AD/DNS Services

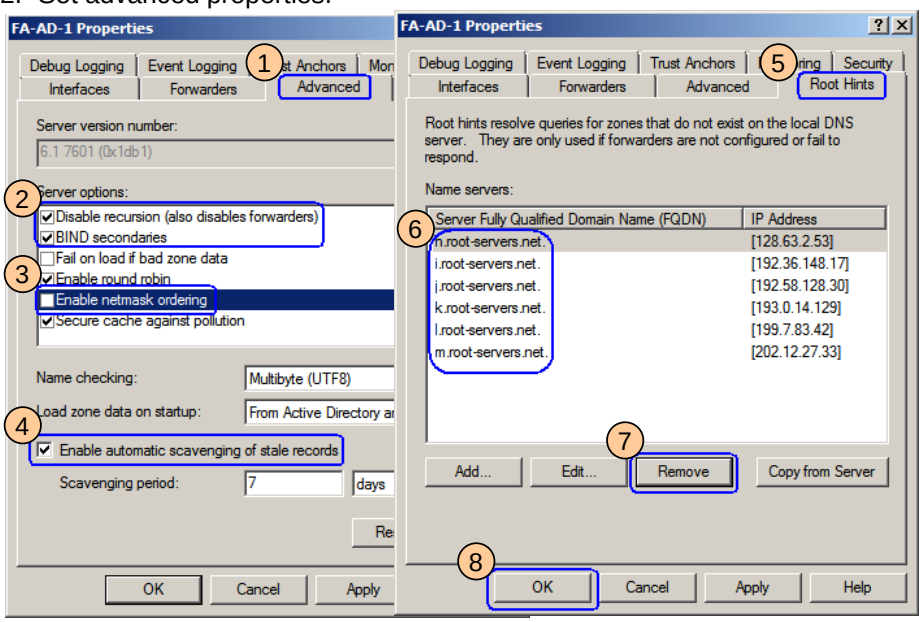
**Step 5 Configure DNS advanced properties. (Perform this operation only on the active server.)**

1. Open the **Properties** window.



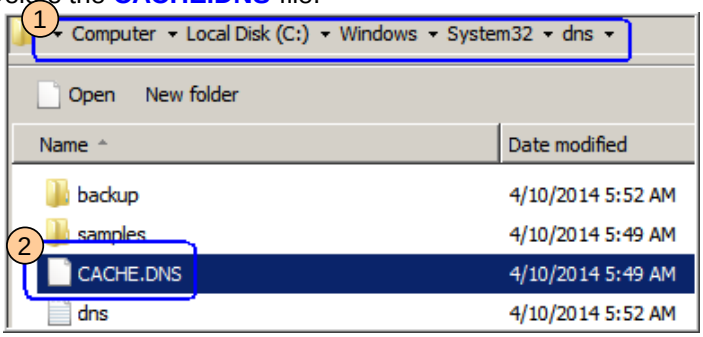

-

2. Set advanced properties.




6 Delete all files named **root-servers.net**.

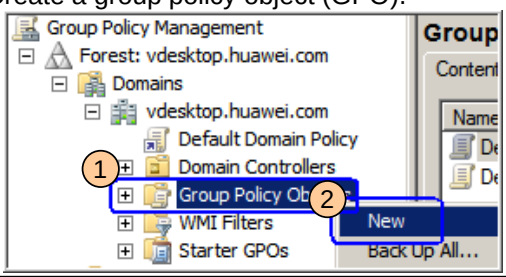
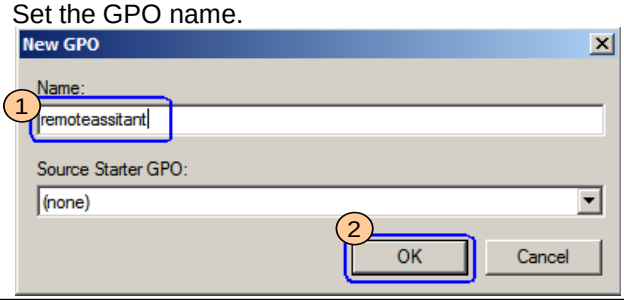
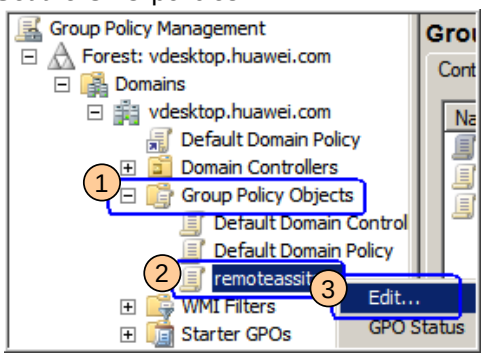
3. Delete the **CACHE.DNS** file.




-

## 6.3 Installing the AD/DNS Services

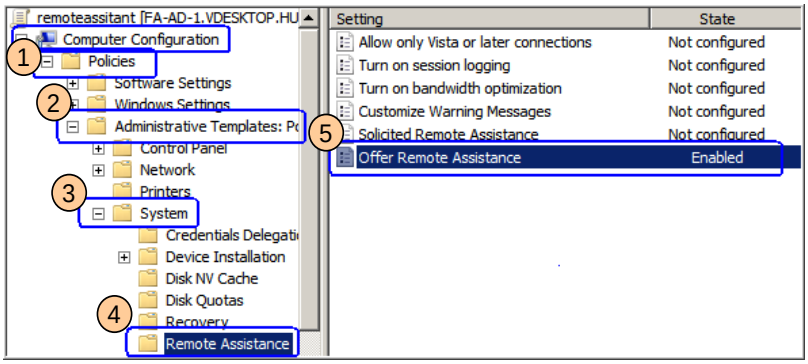
| **Step 6 Configure the winrm service. (The operations on the active and standby servers are the same.)** | |
|---|---|
| 1. On the AD server, click **Start**, enter **cmd** in **Search programs and files**, and press **Enter**. | - |
| 2. Run **winrm qc /q** and view the information displayed.<br>  | - |
| 3. Close the **cmd** window. | - |

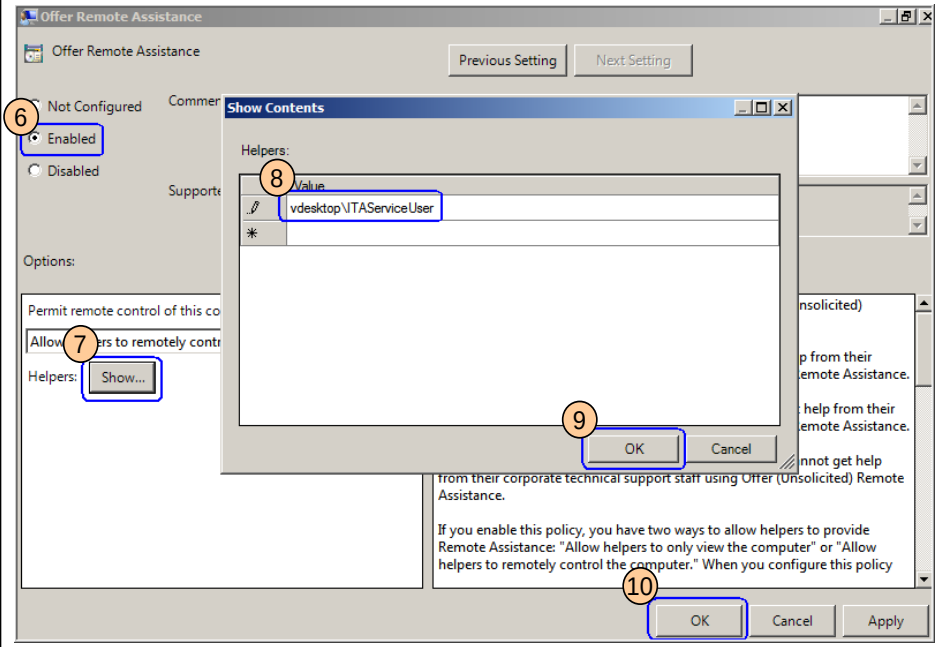
| **Step 7 Configure the remote assistant service. (Perform this operation only on the active server.)** | |
|---|---|
| 1. On the active AD service, click **Start**, enter **gpmc.msc** in **Search programs and file**, and press **Enter**. | - |
| 2. Create a group policy object (GPO).<br>  | - |
| 3. Set the GPO name.<br>  | - |
| 4. Set the GPO policies.<br>  | - |

## 6.3 Installing the AD/DNS Services

### Step 7 Configure the remote assistant service. **(Perform this operation only on the active server.)**

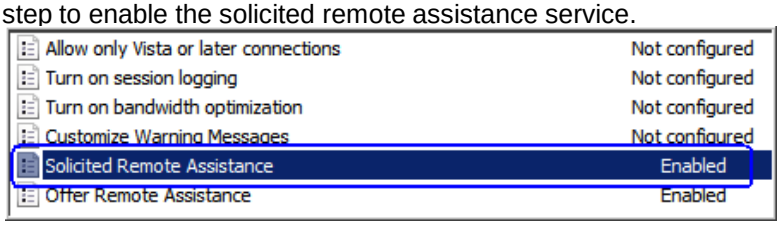
5. Enable **Offer Remote Assistance**.




8 Enter the domain account of the Tomcat service.

6. Enable **Solicited Remote Assistance**. See 5 6 10 in the previous step to enable the solicited remote assistance service.




### Step 8 Install the AD/DNS services on the standby server.

1. Install the AD/DNS services on the standby server.
   For details, see steps 1 to 7 in section ***6.3 Installing the AD/DNS Services***. Pay attention to the information in the **second column**.

-

## 6.4 Installing the DHCP Service

**Step 1 Configure functions of the active DHCP server.**
**(The second column describes the different operations on the standby server.)**

1. Log in to the active AD/DNS/DHCP server using VNC.

Log in to the standby AD/DNS/DHCP server.

2. Add roles.

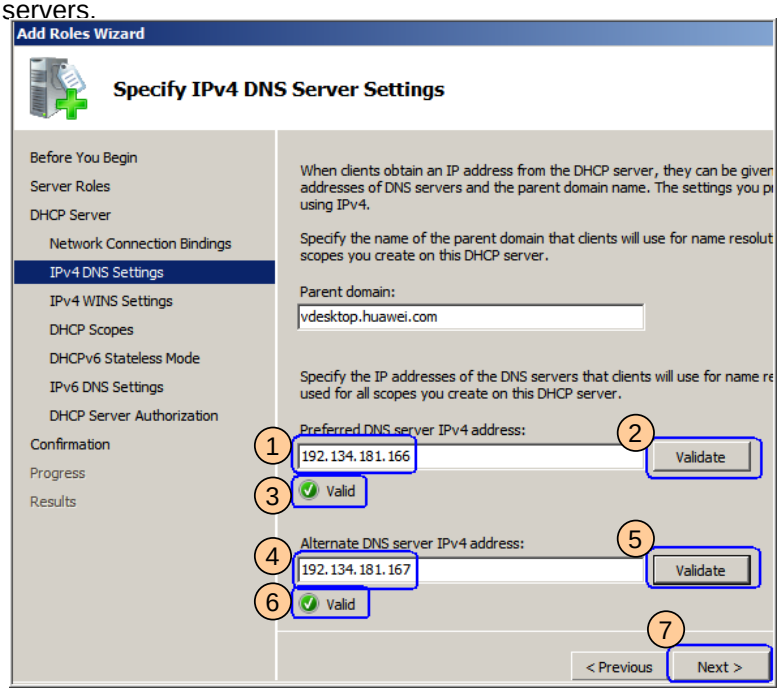

The operations on the standby server are the same.

3. Click **Next**.

4. Select **DHCP Server**.


5. Open the **Specify IPv4 DNS Server** window as prompted.

6. Set the service plane IP addresses for the active and standby DNS servers.



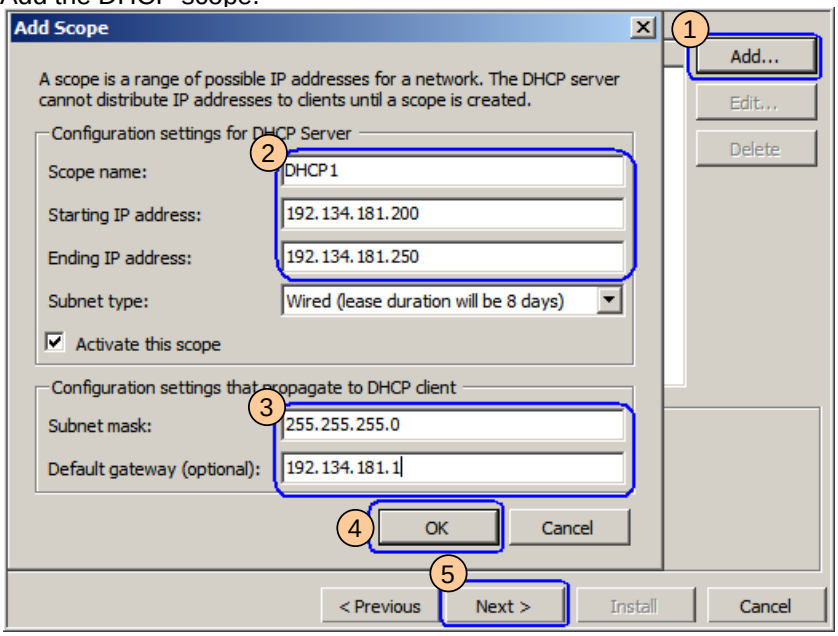
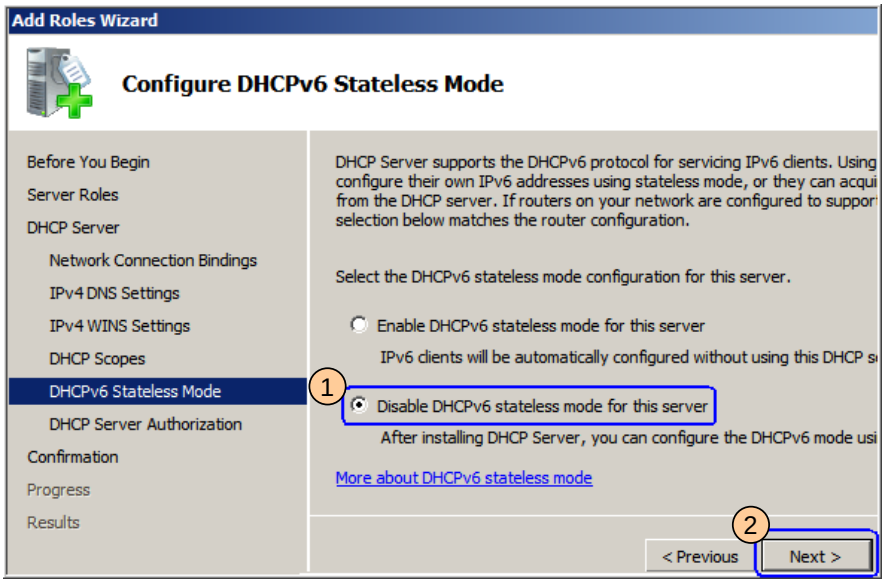

1 Enter the service plane IP address of the active DNS server.

4 Enter the service plane IP address of the standby DNS server.

The operations on the standby server are the same.

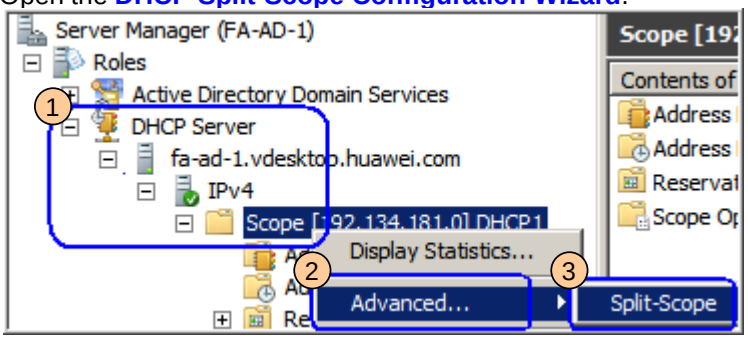
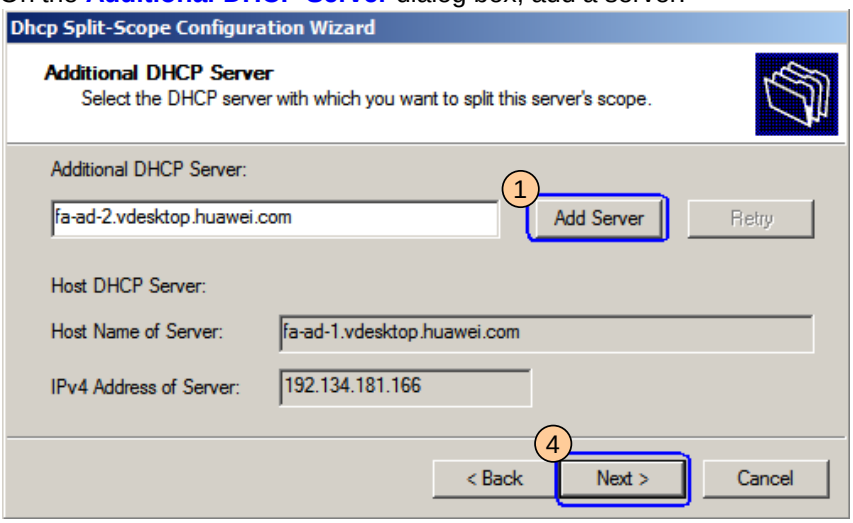
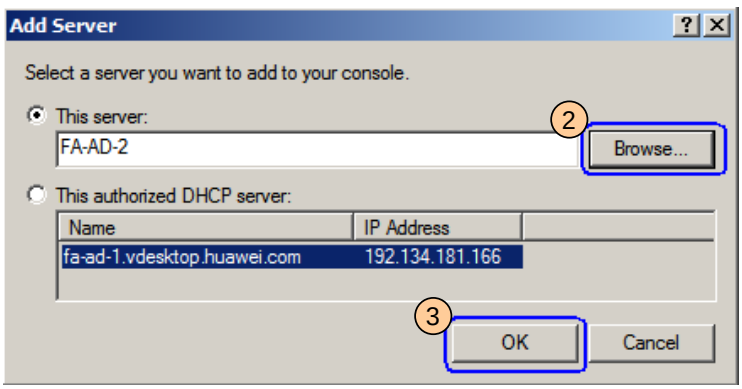
## 6.4 Installing the DHCP Service

**Step 1 Configure functions of the active DHCP server.**
**(The second column describes the different operations on the standby server.)**

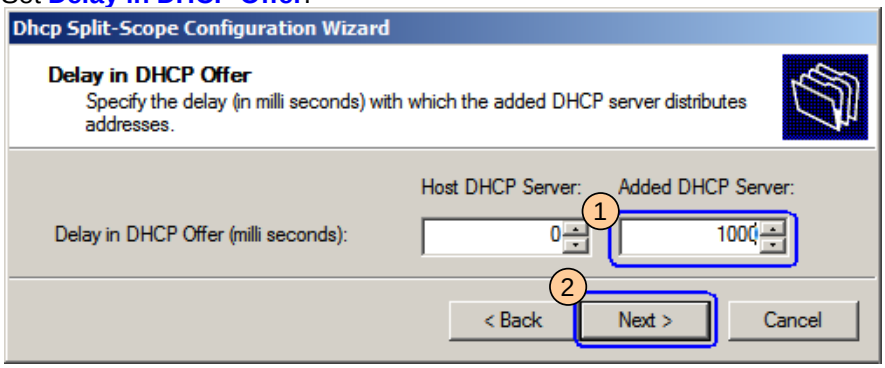
| | |
|---|---|
| 7. Click **Next**. | The operations on the standby server are the same. |
| 8. Add the DHCP scope.<br>  | On the standby server, perform (5) . |
| 9. Select **Disable DHCPv6 stateless mode for this server** and click **Next**.<br>  | The operations on the standby server are the same. |
| 10. Complete the DHCP installation as prompted. | |

## 6.4 Installing the DHCP Service

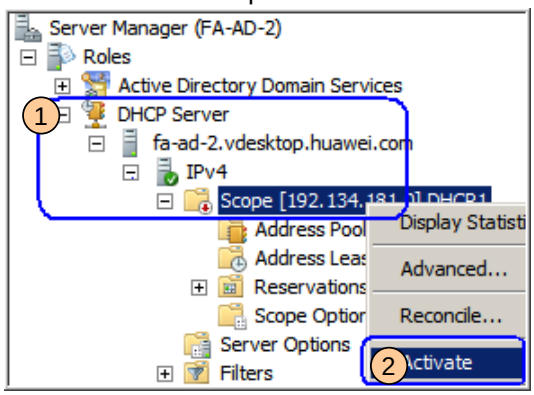
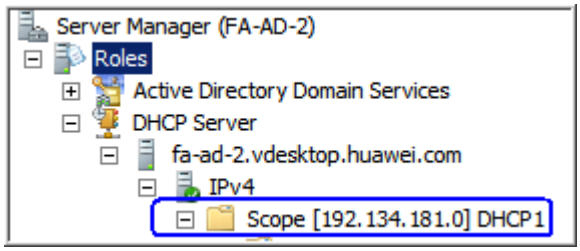
| Step 2 Configure functions of the standby DHCP server. | |
|---|---|
| 1. Log in to the standby AD/DNS/DHCP server using VNC. | - |
| 2. Configure the functions of the standby DHCP server.<br>For details, see step 1 in section ***6.4 Installing the DHCP Service***. Pay attention to the **Second column.** | - |

| Step 3 Synchronize the IP address pool from the active DHCP server to the standby DHCP server. | |
|---|---|
| 1. Log in to the active AD/DNS/DHCP VM using VNC. | - |
| 2. Open the **DHCP Split-Scope Configuration Wizard**.<br>  | - |
| 3. On the **Additional DHCP Server** dialog box, add a server.<br>  <br>  | (2) In the dialog box displayed, enter the IP address or computer name of the standby DHCP server. |

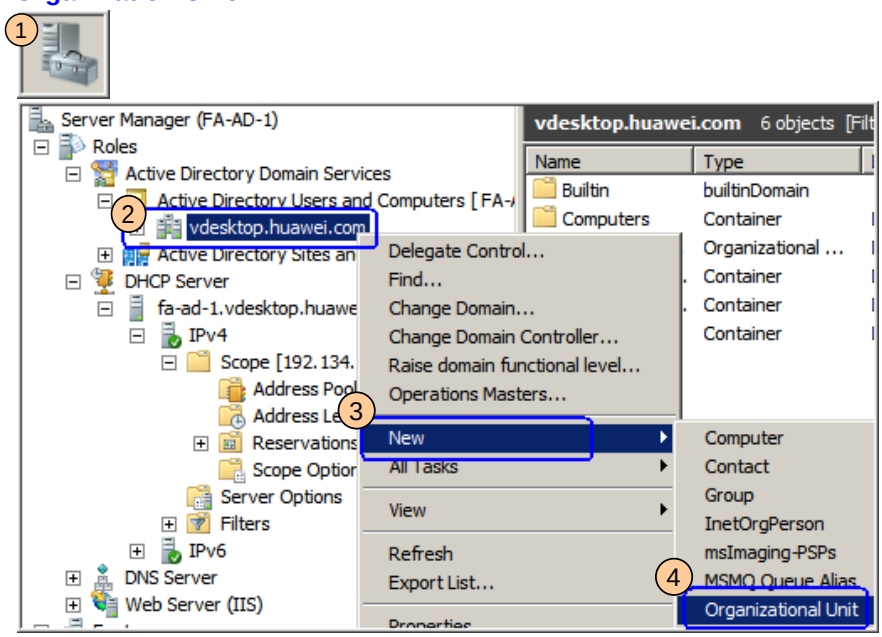
**Step 3 Synchronize the IP address pool from the active DHCP server to the standby DHCP server.**

| | |
|---|---|
| 4. Click **Next**. | - |
| 5. Set **Delay in DHCP Offer**.<br>  | (1) In this example, **1000** indicates that the standby DHCP server waits 1000 ms and starts to assign IP addresses if the active DHCP server does not assign IP addresses. |
| 6. Complete the synchronization operation as prompted. | - |

**Step 4 Activate the IP address pool of the standby DHCP server.**

| | |
|---|---|
| 1. Log in to the standby AD/DNS/DHCP VM using VNC. | - |
| 2. Activate the address pool.<br>  | |
| 3. The status after the activation is as follows:<br>  | - |

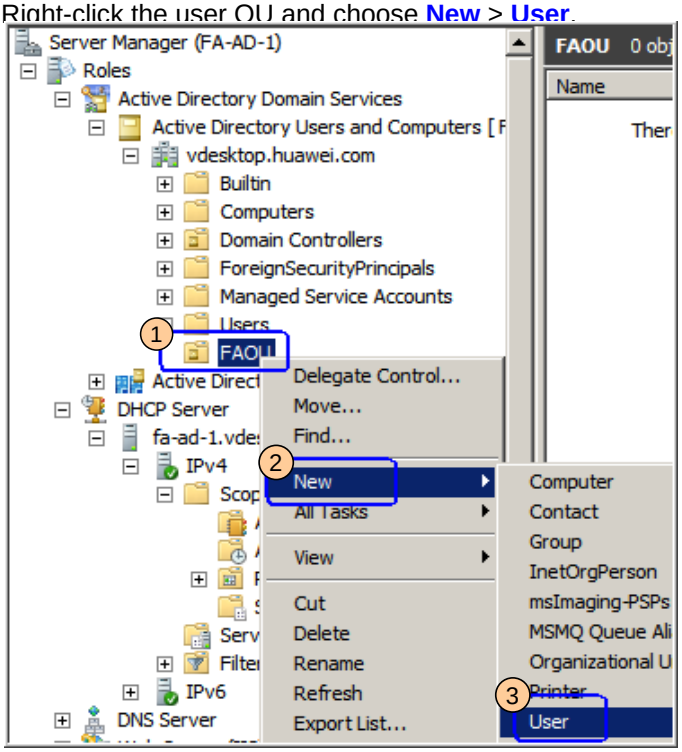
## 6.5 Creating Domain Accounts on only the Active Server

| Step 1 Create an organization unit (OU). | |
|---|---|
| 1. Log in to the active AD server using VNC. | - |
| 2. Right-click the infrastructure domain name and choose **New** > **Organization Unit**.<br>  | If an OU already exists, skip over this operation. |
| 3. Enter the user OU name (B1), for example, **UserOU**, and click **OK**. | Enter the planned user OU name. |

## 6.5 Creating Domain Accounts on only the Active Server

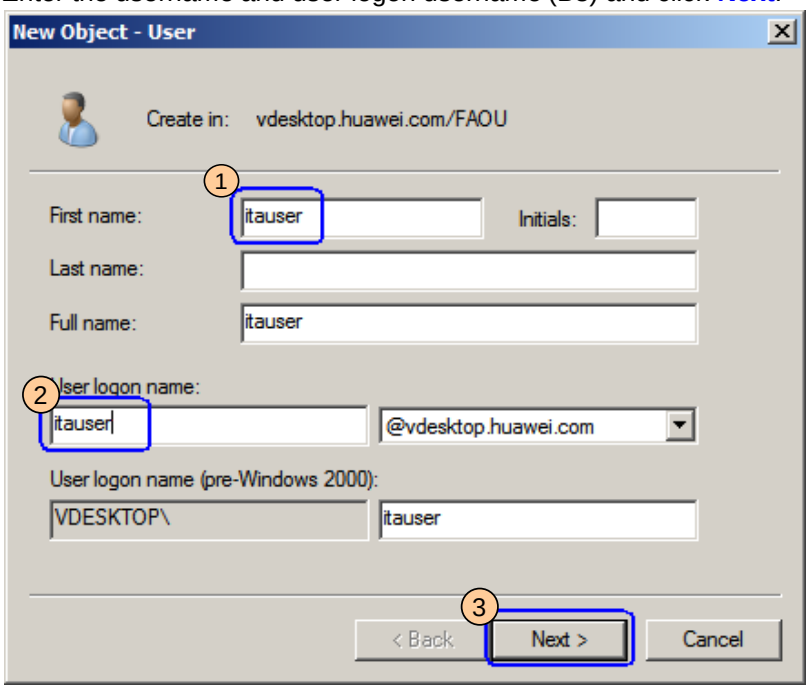
### Step 2 Create users.

1. Right-click the user OU and choose **New** > **User**.




1 Select the OU created in step 1.

2. Enter the username and user logon username (B3) and click **Next**.




Add the following domain accounts:

Account used for logging in to the ITA server, for example, itauser

Account used for logging in to the Loggetter server, for example, loguser

Domain management account, for example, vdsadmin

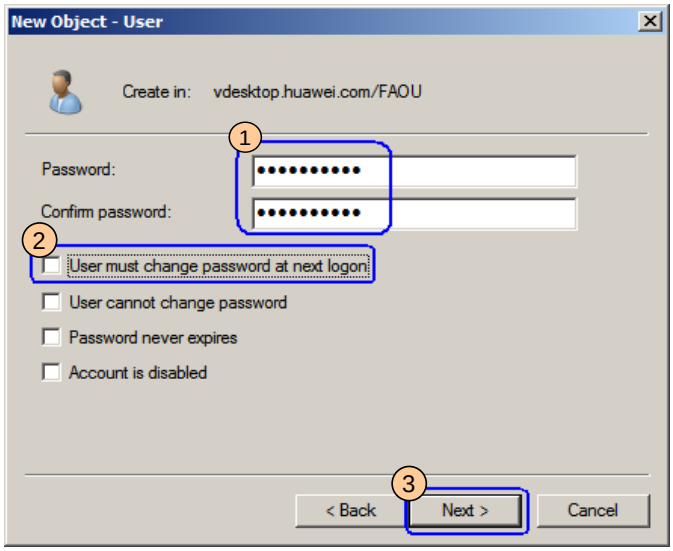
Tomcat domain account, for example, ITAServiceUser

Log service domain account, for example, LogServiceUser

## 6.5 Creating Domain Accounts on only the Active Server

### Step 2 Create users.

3. Enter the user password (B3).




(1) The passwords must meet the following conditions:
- Consists of at least 6 characters.
- Cannot be the same as the username or the username in reverse order.
- Contain at least three of the following combinations:
  - Lowercase letters
  - Uppercase letters
  - Digits
  - Space or special characters, including `~!@#$%^&*()-_=+\|[{}];:'",<.>/?

(2) Deselect this option.

4. Click **Finish**.

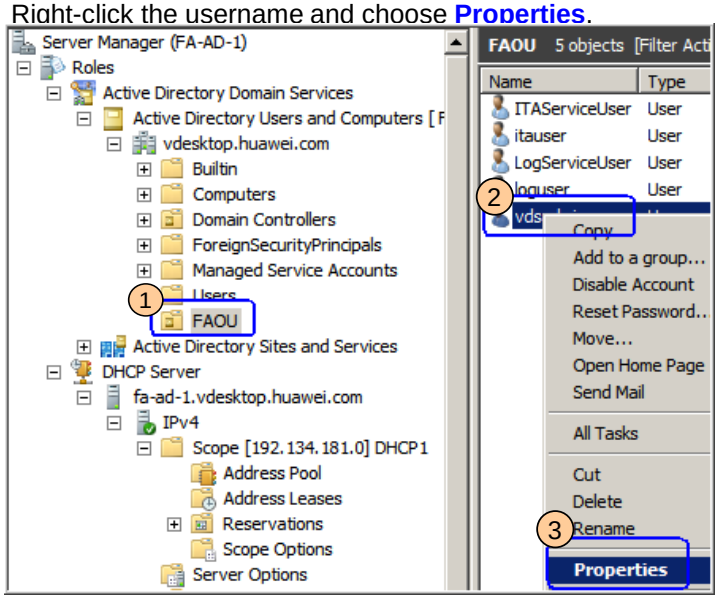
-

5. Add the following accounts in the same way:
   - Account used for logging in to the ITA server, for example, itauser
   - Account used for logging in to the Loggetter server, for example, loguser
   - Domain management account, for example, vdsadmin
   - Tomcat domain account, for example, ITAServiceUser
   - Log service domain account, for example, LogServiceUser

-

### Step 3 Set the domain administrator properties.

1. Right-click the username and choose **Properties**.

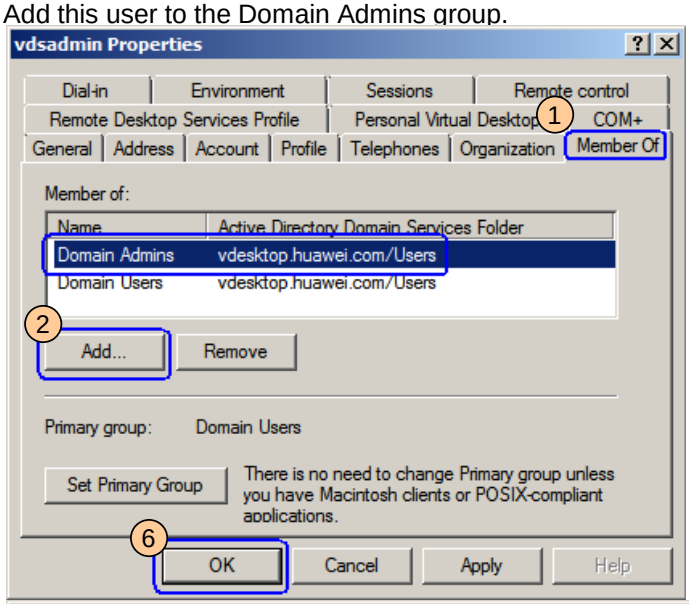


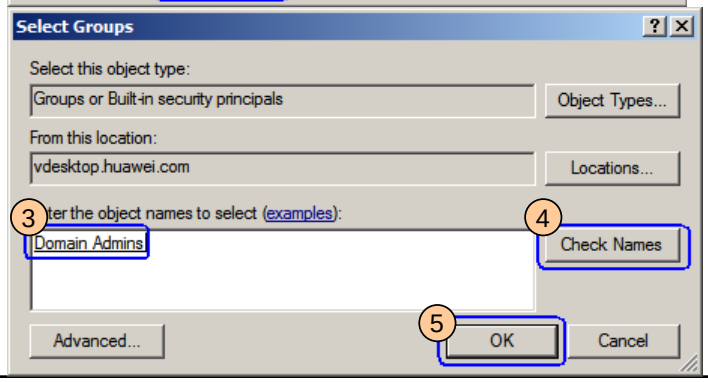

(1) This account (for example, vdsadmin) is used to add VMs to a domain.

## 6.5 Creating Domain Accounts on only the Active Server

### Step 3 Set the domain administrator properties.

2. Add this user to the Domain Admins group.



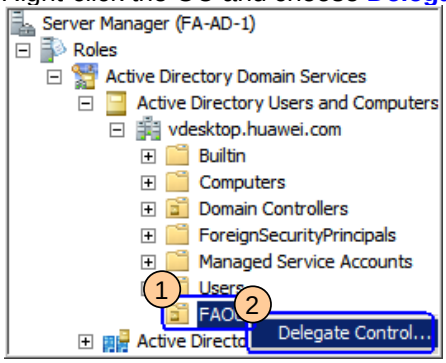

-

3. Add the Tomcat domain account, for example **ITAServiceUser**, to the **Domain Admins** and **DHCP Users** groups.

-

### Step 4 Set user rights.

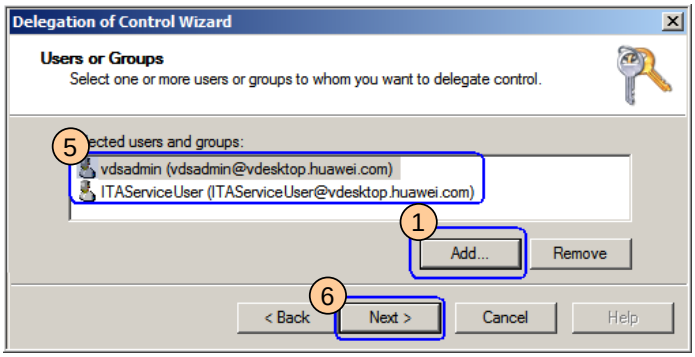
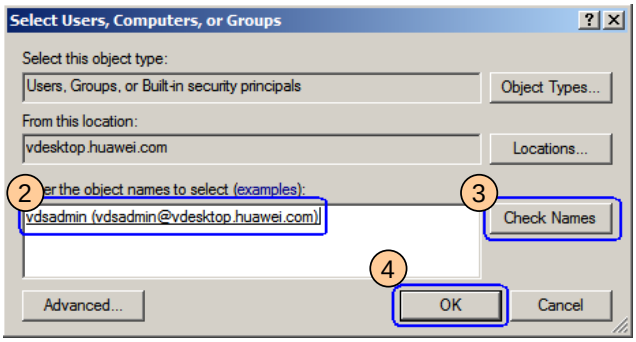
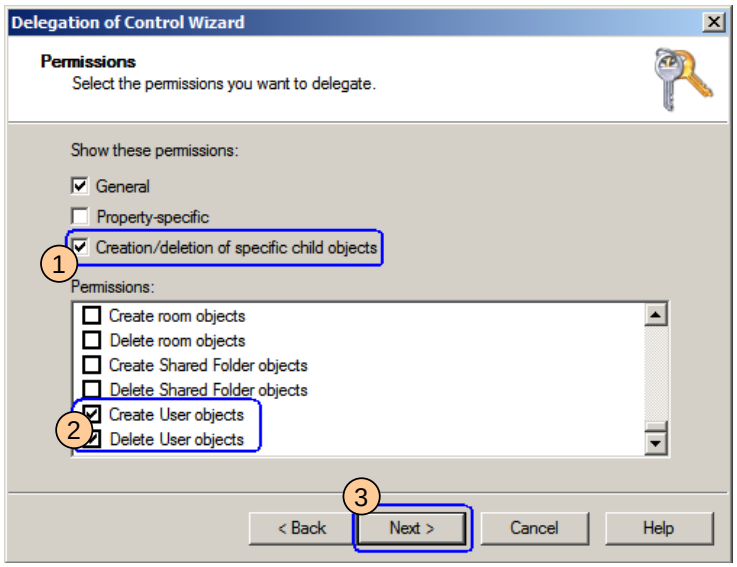
1. Right-click the OU and choose **Delegate Control**.




1 Select the newly created OU.

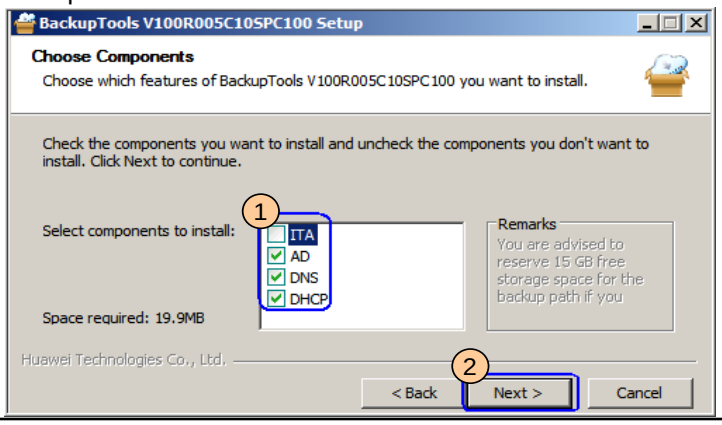
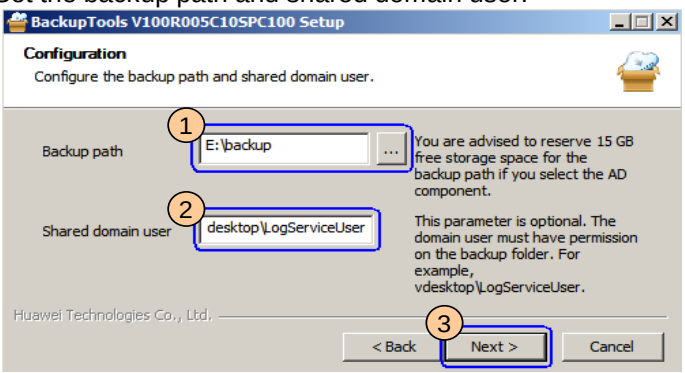
## 6.5 Creating Domain Accounts on only the Active Server

### Step 4 Set user rights.

| | |
|---|---|
| 2. Open the **Users or Groups** window as prompted. | - |
| 3. Add an account.<br>  <br><br>  <br> | 2 Enter a **domain management account**, such as **vdsadmin**. |
| 4. Repeat the previous step to add a **Tomcat service domain account**, such as **ITAServiceUser**, and click **Next**. | - |
| 5. Select **Create a custom task to delegate** and click **Next** twice. | |
| 6. Assign operation permissions to the user.<br>  <br> | - |
| 7. Complete the configuration as prompted. | - |

## 6.6 Configuring Backup and Performing Security Hardening

### Step 1 Install the backup tool. (The operations on the active and standby servers are the same except that the VMs you need to log in are different.)

| | |
|---|---|
| 1. Log in to the active AD/DNS/DHCP server using the **Administrator** account in VNC mode. | Log in to the standby server using the **SWMaster** account. |
| 2. On the active AD/DNS/DHCP server, mount **FusionAccess_Installer_Win_V100R005C10SPC100.iso**. | You do not need to select **Restart the VM now to install the OS**. |
| 3. Double-click the CD-ROM drive directory and click **BackupTools** in the **Installation Wizard** window. | - |
| 4. Retain the default values and select the components for which the backup tool is to be installed.<br>  | - |
| 5. Set the backup path and shared domain user.<br>  | 2 Enter the **log service domain account**, that is, the LogServer domain account created when the Loggetter is installed. For example, enter **vdesktop\LogServiceUser**. |
| 6. Complete the installation as prompted. | - |

### Step 2 Configure security hardening. (The operations on the active and standby servers are the same.)

| | |
|---|---|
| **CAUTION**<br>Before performing security hardening, ensure that no user has logged in to the standby AD/DNS/DHCP VM.<br>1. In the **Installation Wizard** window, click **Security**. | - |
| 2. Perform security hardening as prompted. Restart the VM and log in the VM as user **SWMaster**. | After the hardening, the **Administrator** account changes to **Swmaster**. |

## 6.6 Configuring Backup and Performing Security Hardening

**Step 3 Configure security information for the standby AD/DNS/DHCP server.**

1. See step 1 to step 2 in 6.6 Configuring Backup and Performing Security Hardening to install the backup tool on the standby server and perform security hardening.

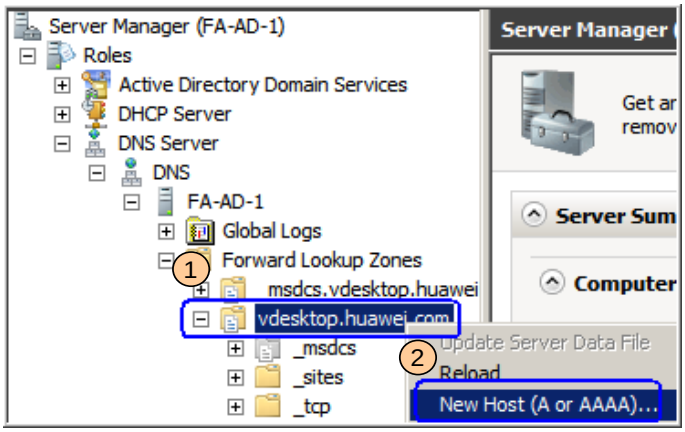
## 6.7 Configuring DNS Policies

**Step 1 Configure the forward and reverse DNS lookups.**
**(Perform this operation only on the active server.)**

1. Log in to the active AD/DNS/DHCP VM using VNC.

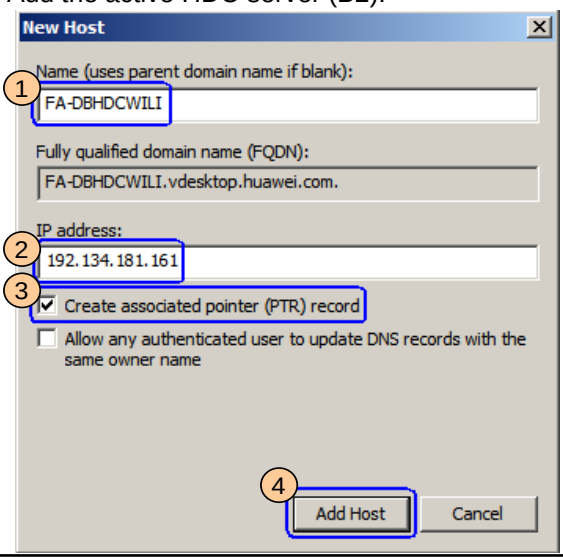
-

2. Open the **New Host** window.




-

3. Add the active HDC server (B2).




Repeat steps 1 2 4 to add the following information:

| 1 | 2 |
|---|---|
| Active HDC server name | Service IP address |
| Standby HDC server name | Service IP address |
| Prefix of the domain name used for accessing the WI (D4) | vLB floating IP address |

4. Close the **New Host** window. In the navigation tree, expand **Reverse Lookup Zones**, right-click **Reverse IP address segment**, and choose **Refresh** to check whether the reverse DNS lookup is automatically added.

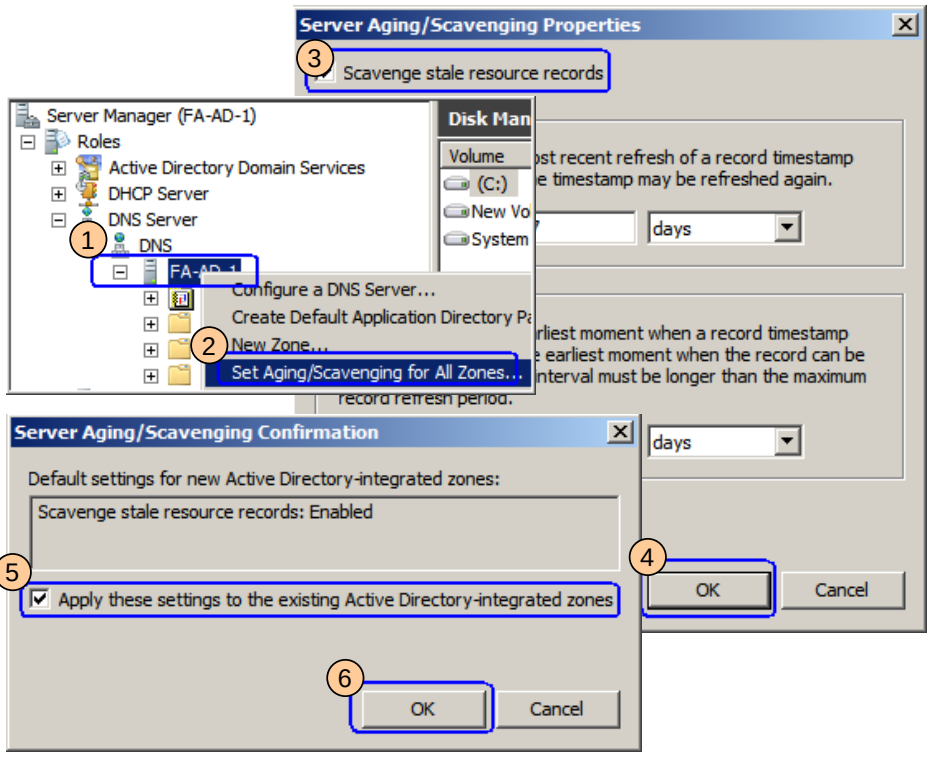
-

## 6.7 Configuring DNS Policies

### Step 2 Enable the DNS aging and scavenging functions. (Perform this operation only on the active server.)

1. Enable the DNS aging and scavenging functions.

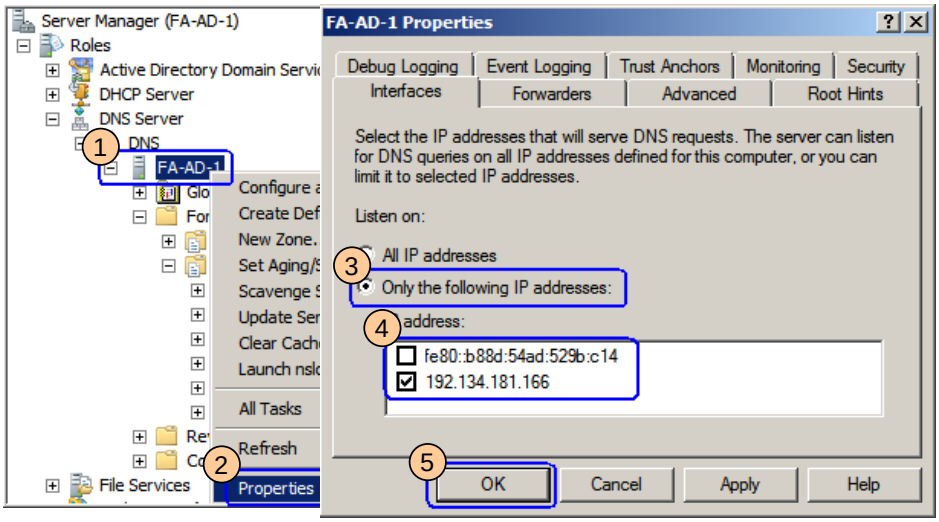
-




### Step 3 Set the address on which the DNS server listens. (The operations on the active and standby servers are the same.)

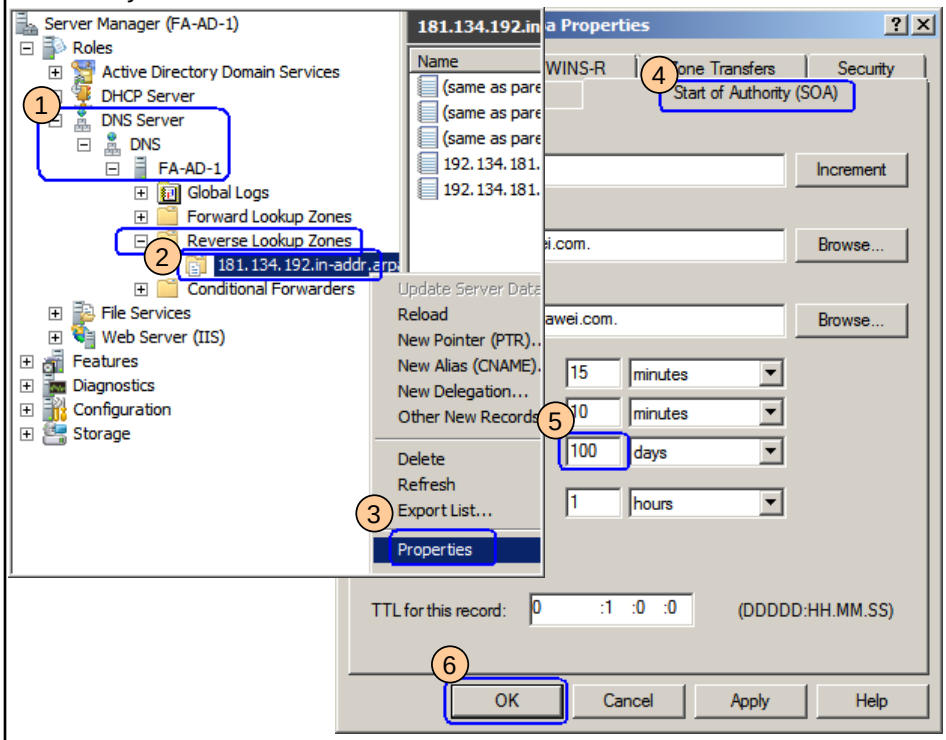
1. Set the address on which the DNS server listens.

-



## 6.7 Configuring DNS Policies

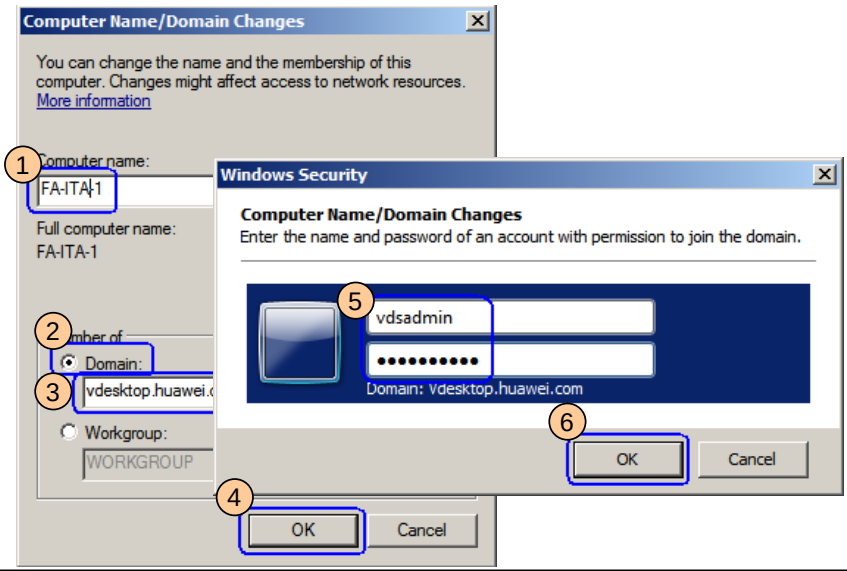
### Step 4 Modify the Start of Authority (SOA) record. (Perform this operation only on the active server.)

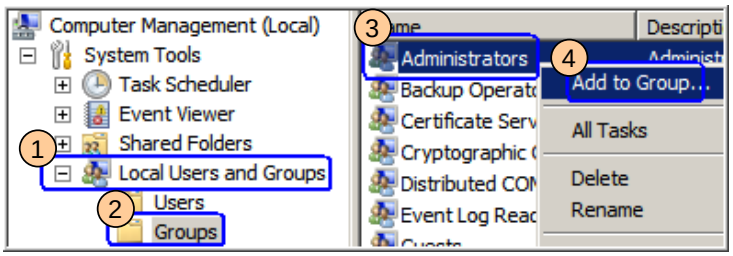
| | |
|---|---|
| 1. Modify the SOA record.<br>  | - |

### Step 5 Configure the DNS policies for the standby AD/DNS/DHCP server.

| | |
|---|---|
| 1. Log in to the standby AD/DNS/DHCP server as user Swmaster. | - |
| 2. See **Step 3 Set the address on which the DNS server listens** to complete the configuration on the standby server. You need to perform only this step on the standby server. | - |

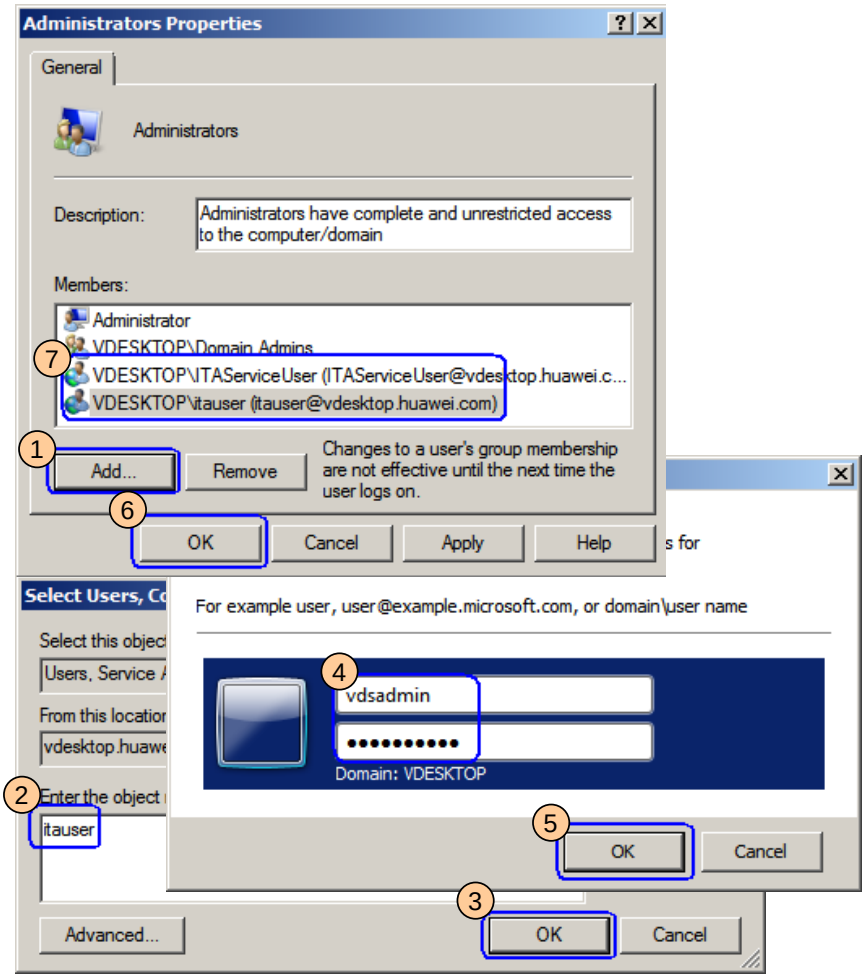
## 6.8 Installing the ITA

| **Step 1 Add the VM to the domain.**<br>**(The operations on the active and standby servers are the same, but the servers to be logged in are different.)** | |
|---|---|
| 1. Log in to the infrastructure VM hosting the active ITA service as user Administrator. | To install the standby ITA server, log in to the infrastructure VM hosting the standby ITA service. |
| 2. Click **Start**, enter **sysdm.cpl** in **Search programs and files**, and press **Enter**. Then, click **Change** in the **System Properties** dialog box. | - |
| 3. Add the infrastructure VM to the domain.<br>  | 1 Enter the VM name.<br>3 Enter the infrastructure domain name.<br>5 Enter the domain administrator username and password. |
| 4. Restart the VM and then log in to the VM as user **Administrator**. | - |

| **Step 2 Add the domain account to the administrator group.**<br>**(The operations on the active and standby servers are the same.)** | |
|---|---|
| 1. Click **Start**, enter **compmgmt.msc** in **Search programs and files**, and press **Enter**. | - |
| 2. Open the **Add to Group** window.<br>  | - |

**Step 2 Add the domain account to the administrator group.**
**(The operations on the active and standby servers are the same.)**

3. Add the domain account to the administrator group.




2 Add the following accounts:
- **Tomcat domain account,** for example, ITAServiceUser
- Domain account used for logging in to the ITA server, for example, itauser

Repeat 1 2 3 4 5 to add the domain accounts.

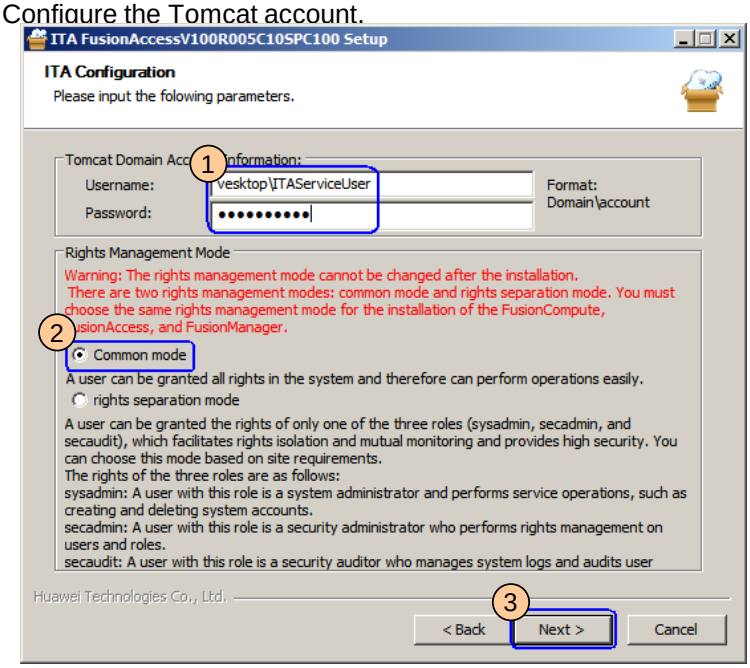
**Step 3 Install the ITA.**
**(The operations are different on the active and standby servers.)**

| | |
|---|---|
| 1. Log out of the VM and then log in to the infrastructure VM hosting the active ITA service using an **ITA server login account,** such as **itauser**. | To install the standby ITA server, log in to the infrastructure VM hosting the standby ITA service. |
| 2. On the active ITA server, mount **FusionAccess_Installer_Win_V100R005C10SPC100.iso**. | You do not need to select **Restart the VM now to install the OS**. |
| 3. Double-click the CD-ROM drive directory and click **IT Adaptor** in the **Installation Wizard** window. | - |
| 4. Open the **ITA Configuration** window as prompted. | - |

## 6.8 Installing the ITA

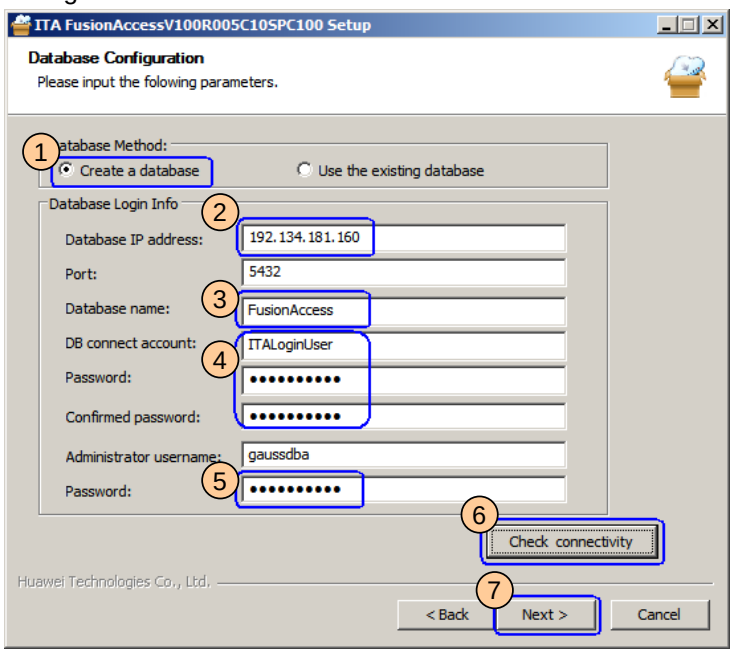
### Step 3 Install the ITA. (The operations are different on the active and standby servers.)

5. Configure the Tomcat account.




1. Enter the Tomcat domain account, for example, ITAServiceUser.
2. The rights management mode must be the same as the mode set when FusionCompute is installed.

6. Configure the database.

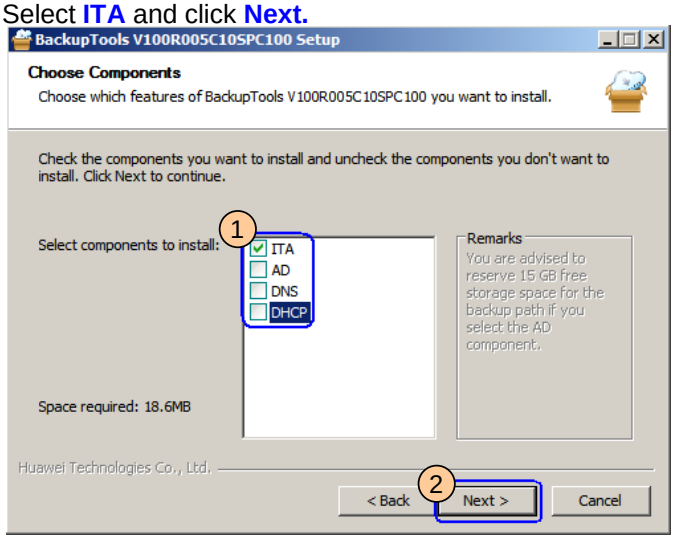
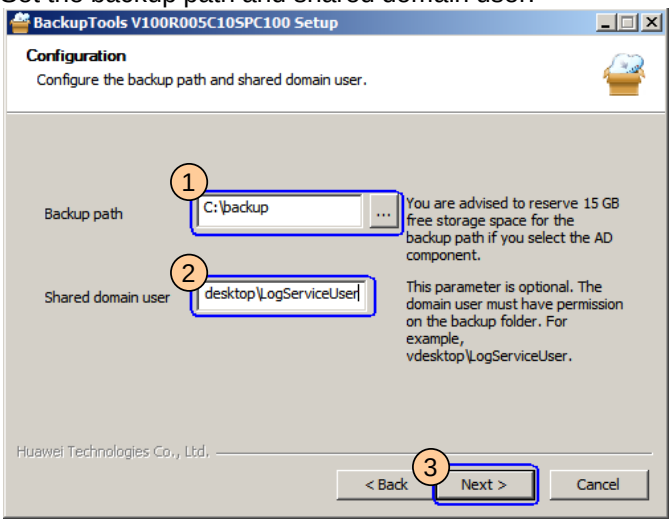



1. Select **Create a database** for the active ITA and **Use the existing database** for the standby ITA.
2. Enter the floating IP address of the GaussDB
3. Enter the ITA database name (G2).
4. Set the password for accessing the ITA database (G3).
5. Enter the default password, which is Huawei@123.

7. Complete the ITA software installation as prompted.

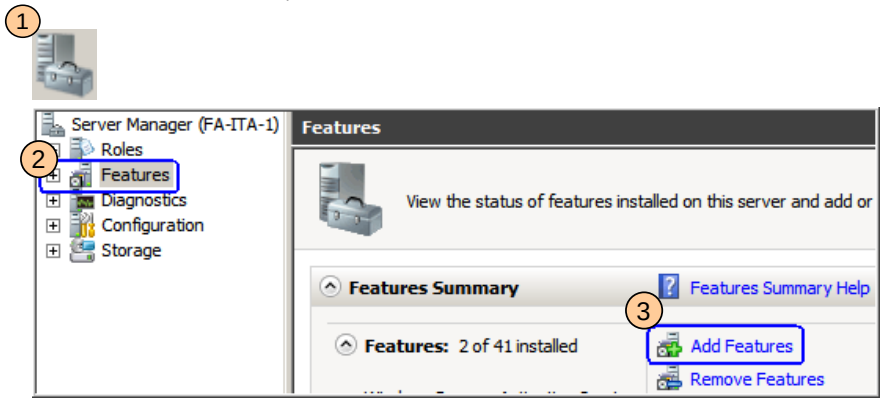
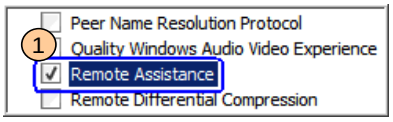
-

## 6.8 Installing the ITA

| **Step 4 Install the backup tool. (The operations on the active and standby servers are the same.)** | |
|---|---|
| 1. In the **Installation Wizard** window, click **BackupTools**. | - |
| 2. Select **ITA** and click **Next.**<br>  | - |
| 3. Set the backup path and shared domain user.<br>  | (2) Enter the **log service domain account**, that is, the LogServer domain account created when the Loggetter is installed. For example, enter **vdesktop\LogServiceUser**. |
| 4. Complete the installation as prompted. | - |

| **Step 5 Perform security hardening. (The operations on the active and standby servers are the same.)** | |
|---|---|
| 1. In the **Installation Wizard** window, click **Security**. | - |
| 2. Complete the security hardening as prompted. | - |
| 3. Restart the VM and then log in to the VM using the domain account **SWMaster**. | **Vdesktop\SWMaster** |

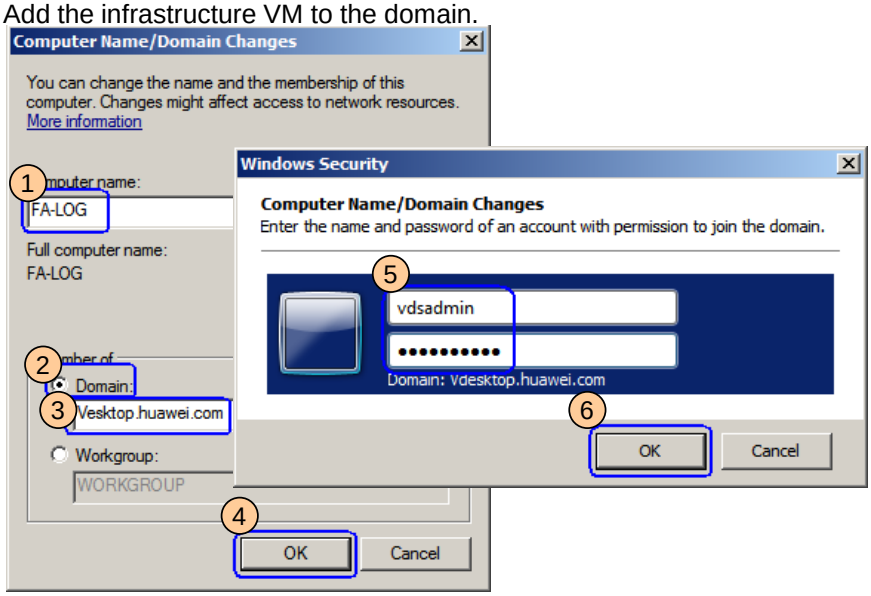
## 6.8 Installing the ITA

| **Step 6 Configure the remote assistant service. (The operations on the active and standby servers are the same.)** | |
|---|---|
| 1. On the active ITA server, choose **Features** > **Add Features**.<br>  | - |
| 2. Select **Remote Assistance**.<br>  | - |
| 3. Click **Next** and complete the configuration as prompted. | - |

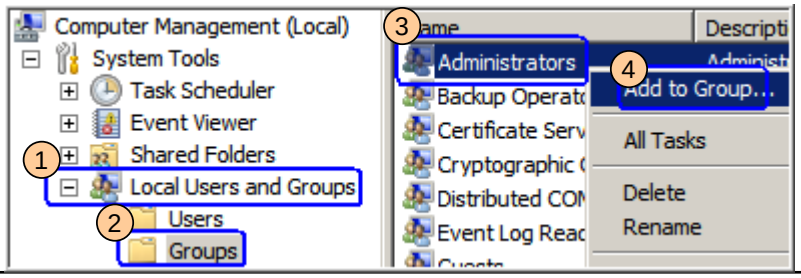
| **Step 7 Install the standby ITA server.** | |
|---|---|
| 1. Log in to the standby ITA server. | - |
| 2. Install the ITA on the standby server by following the operations in section ***6.8 Installing the ITA***. | - |

## 6.9 Installing the Loggetter

### Step 1 Add the VM to the domain.

| | |
|---|---|
| 1. Log in to the infrastructure VM hosting the Loggetter service as user Administrator. | |
| 2. Click **Start**, enter **sysdm.cpl** in **Search programs and files**, and press **Enter**. Then, click **Change** in the **System Properties** dialog box. | - |
| 3. Add the infrastructure VM to the domain.<br>  | 1 Enter the VM name (B2).<br>3 Enter the infrastructure domain name (D1).<br>5 Enter the domain administrator username and password (F2). |
| 4. Restart the VM and then log in to the VM as user **Administrator**. | - |

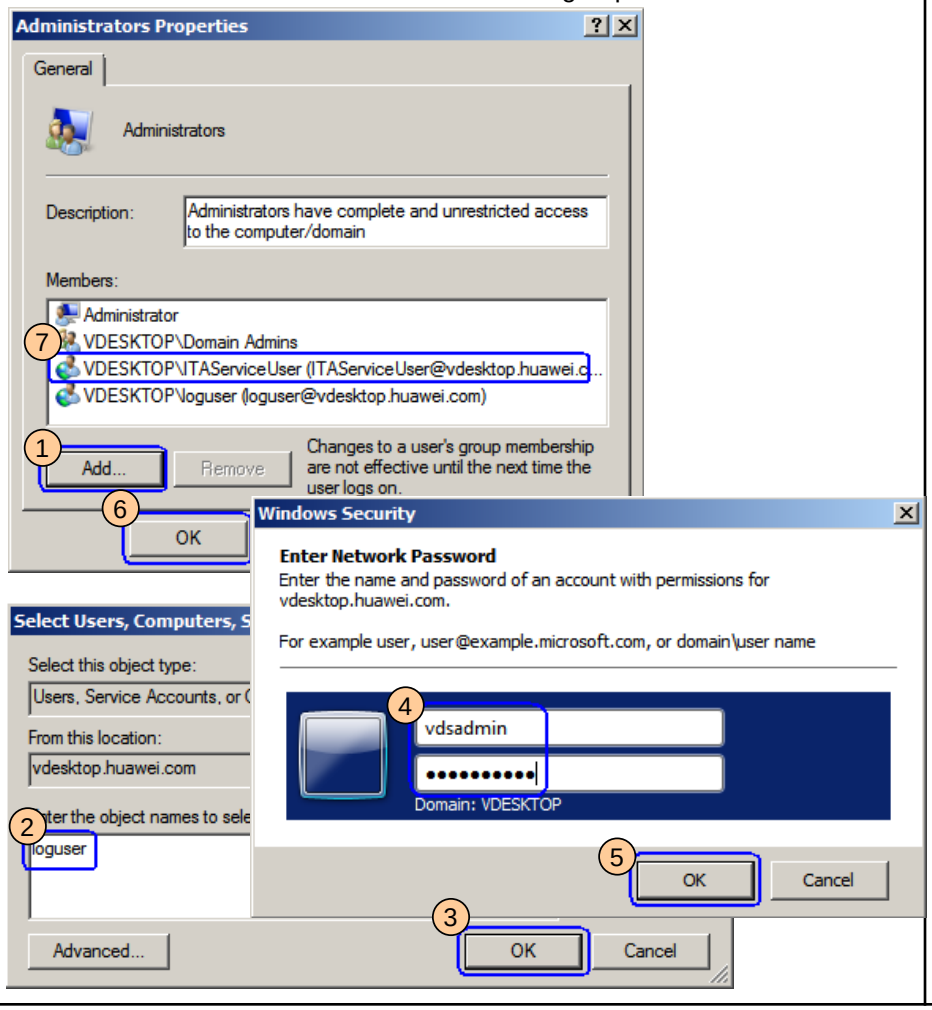
### Step 2 Add the domain account to the administrator group.

| | |
|---|---|
| 1. Click **Start**, enter **compmgmt.msc** in **Search programs and files**, and press **Enter**. | - |
| 2. Open the **Add to Group** window.<br>  | - |

## 6.9 Installing the Loggetter

### Step 2 Add the domain account to the administrator group.

3. Add the domain account to the administrator group.




2 Add the following accounts:
- **Tomcat domain account,** for example, ITAServiceUser (F3)
- Domain account used for logging in to the Loggetter server, for example, loguser (F1)
- Log service domain account, for example, LogServiceUser (F4)

4 Enter the domain management account (F2).

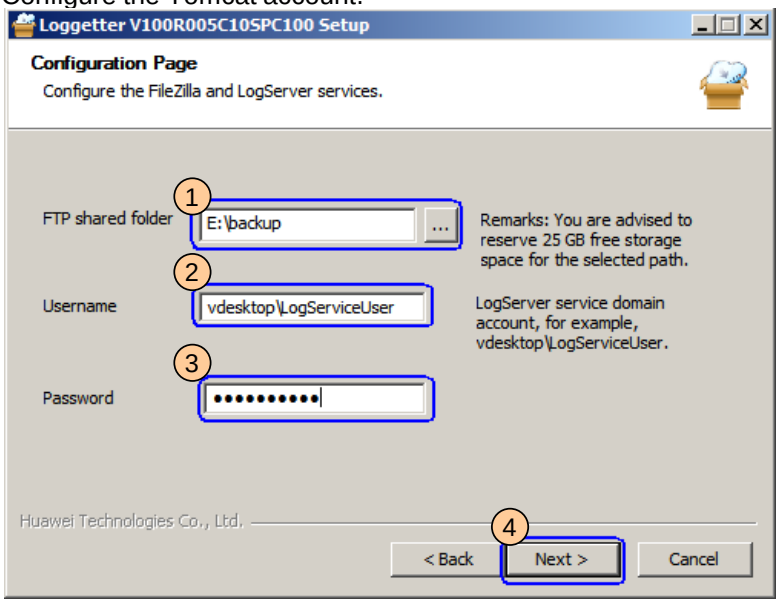
Repeat 1 2 3 4 5 to add the domain accounts.

### Step 3 Install the Loggetter.

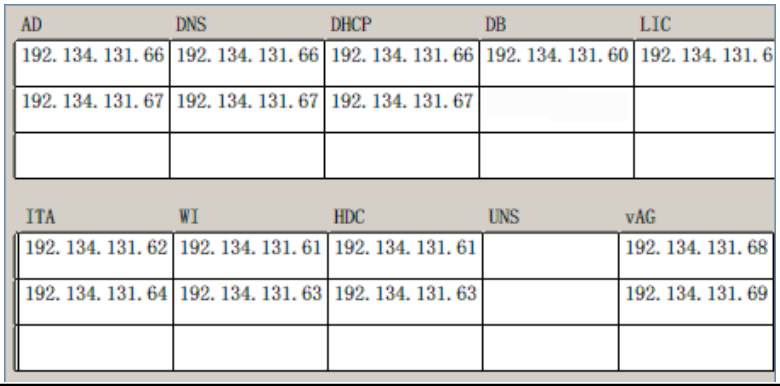
| | |
|---|---|
| 1. Log out of the VM and use the **Loggetter login domain account**, such as **loguse**r, to log in to the infrastructure VM on which the Logggetter service is deployed. | - |
| 2. On the Loggetter server, mount **FusionAccess_Installer_Win_V100R005C10SPC100.iso**. | **You do not need to select** Restart the VM now to install the OS. |
| 3. Double-click the CD-ROM drive directory and click **Loggetter** in the **Installation Wizard** window. | - |
| 4. Open the **Configure the FileZila and LogServer services** window as prompted. | - |

## 6.9 Installing the Loggetter

### Step 3 Install the Loggetter.

| | |
|---|---|
| 5. Configure the Tomcat account.<br>  <br> | (2) Enter the log service domain account, for example, LogServiceUser (F4). |
| 6. Complete the installation as prompted. | - |

### Step 4 Configure the Loggetter backup task.

| | |
|---|---|
| 1. Choose **Start > All Programs > Loggetter > Loggetter**. | - |
| 2. Configure component IP addresses (B2).<br>  | ● Enter the service plane IP addresses of the components.<br>● Enter the floating IP address of the DB.<br>● Enter the IP address of the active node in the first row for the nodes working in active/standby mode.<br>● **FTP Data Configuration**:retain the default value. |
| 3. Click **finish**. | - |

| AD | DNS | DHCP | DB | LIC |
|---|---|---|---|---|
| 192. 134. 131. 66 | 192. 134. 131. 66 | 192. 134. 131. 66 | 192. 134. 131. 60 | 192. 134. 131. 6 |
| 192. 134. 131. 67 | 192. 134. 131. 67 | 192. 134. 131. 67 | | |
| | | | | |

| ITA | WI | HDC | UNS | vAG |
|---|---|---|---|---|
| 192. 134. 131. 62 | 192. 134. 131. 61 | 192. 134. 131. 61 | | 192. 134. 131. 68 |
| 192. 134. 131. 64 | 192. 134. 131. 63 | 192. 134. 131. 63 | | 192. 134. 131. 69 |
| | | | | |

### Step 5 Perform security hardening.

| | |
|---|---|
| 1. In the **Installation Wizard** window, click **Security**. | - |
| 2. Complete the security hardening as prompted. | - |
| 3. Restart the VM and then log in to the VM using a domain account. | - |

# 7 Initial Configuration

## 7.1 Configuring the Virtualization Environment

### Step 1 Configure the virtualization environment.

1. Enter **http://Service plane IP address of the active ITA:8081** in the address box of your browser and press **Enter**.

   http://192.168.181.62:8081

2. Enter the **username** and **password.** The **username** and **password** vary with the **Rights Management Mode** set when the ITA is installed.

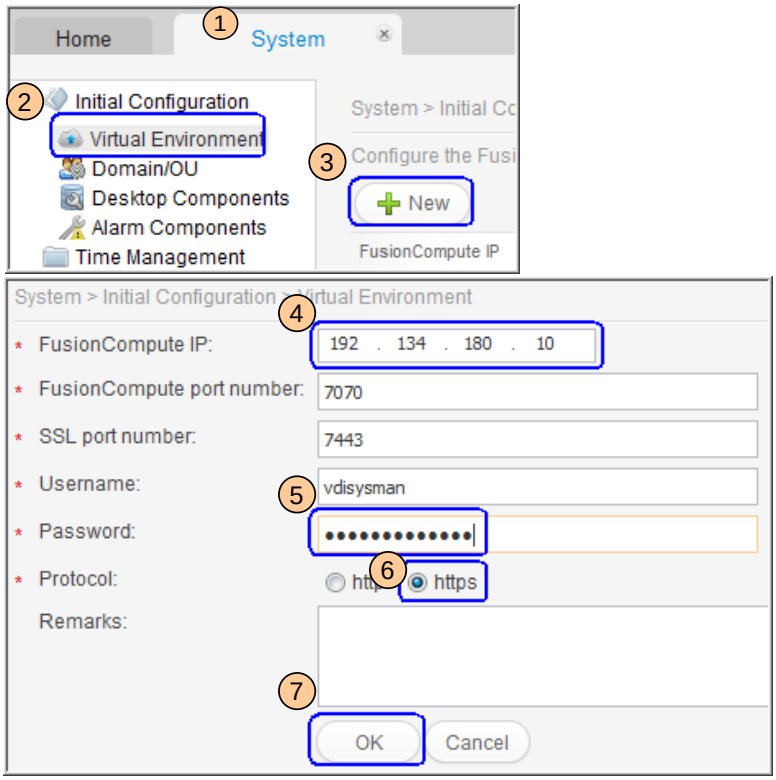
   | Rights Management Mode | Username | Password |
   |---|---|---|
   | **Common mode** | **admin** | **Huawei123#** |
   | **Rights separation mode** | **sysadmin** | **Sysadmin#** |

   Change the password after you log in to FusionAccess for the first time.

3. Click **System**.

   -

4. Configure the virtualization environment.



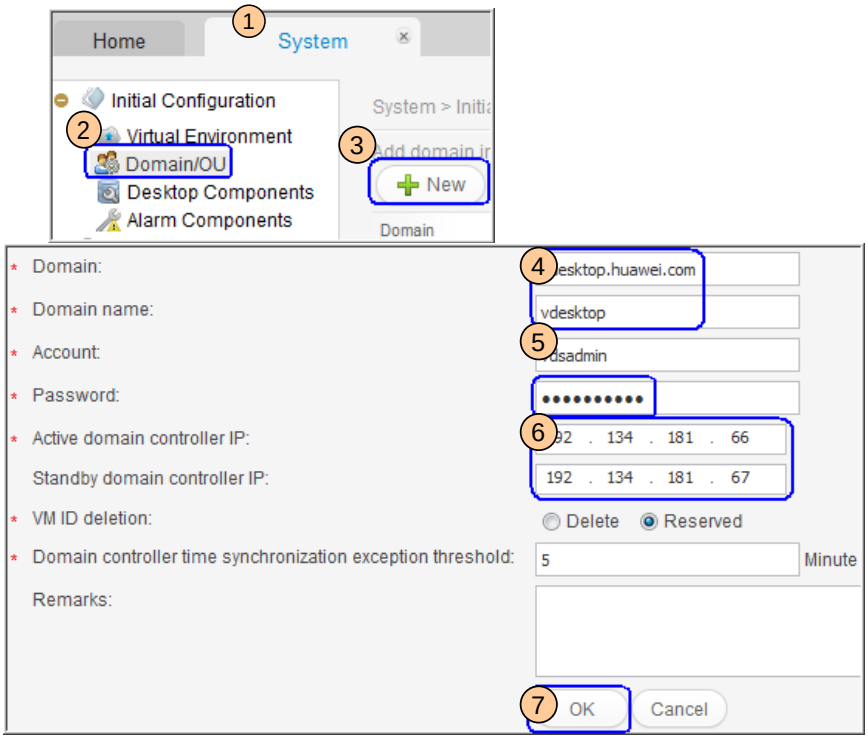

4 Enter the floating IP address of the VRM node.

5 The default password is **VdiEnginE@234**.

## 7.2 Configuring the Domain

### Step 1 Configure the domain.

1. Add the domain information.




4 Enter the domain information (D1).

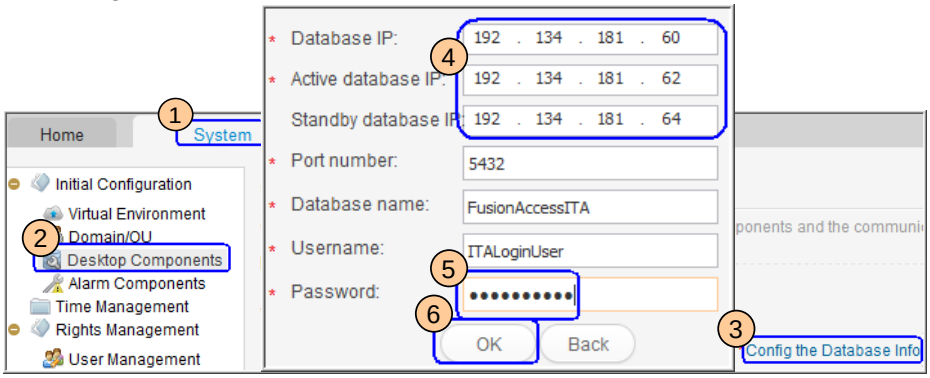
5 Enter the domain administrator username and password (F2). The domain administrator is used to add VMs to a domain.

6 Enter the service plane IP addresses of the AD server (B2).

## 7.3 Configuring Desktop Components

### Step 1 Configure the ITA.

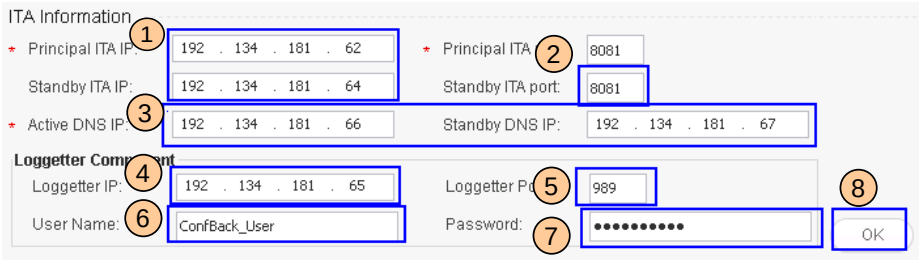
1. Configure the database.




4 Enter the service plane IP addresses of the active and standby GuassDBs.

5 Enter the password used for accessing the ITA database. This password is set when the ITA is installed.

2. Configure the ITA.




1 Enter the service plane IP addresses of the active and standby ITAs (B2).

2 The default value is **8081**.

3 Enter the service plane IP addresses of the active and standby DNSs (B2).

4 Enter the service plane IP address of Loggerter (B2).

5 The default value is **989**.

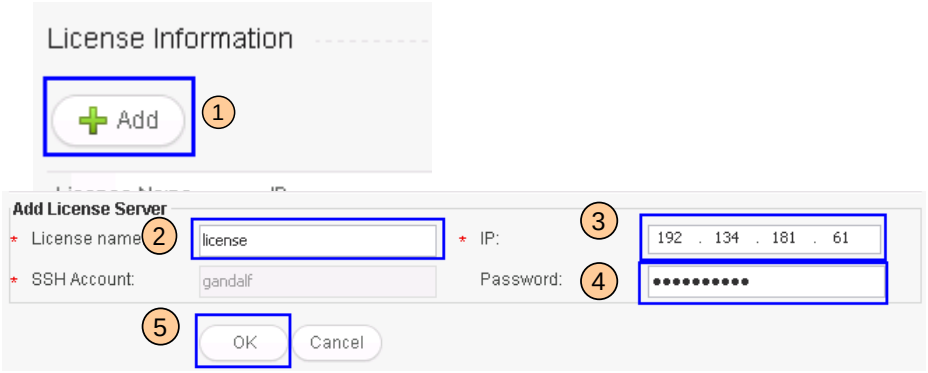
6 Enter the username of the FTP service account of the log server. The default value is **ConfBack_User**.

7 Enter the password of the FTP service account of the log server. The default value is **Huawei123#**.

## 7.3 Configuring Desktop Components

### Step 2 Configure the license.

1. Add the license server.




3 Enter the service plane IP address of the License server (B2).

4 The password of SSH and the default value is **Huawei@123**

2. Click **Return**.

-

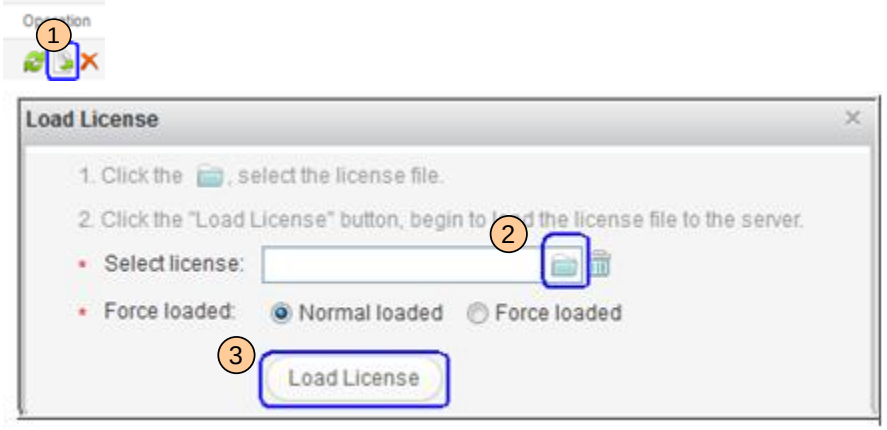
3. Obtain the ESN.


-

4. Apply for a license based on the ESN. For details, see the *FusionCloud Desktop Solution V100R005C20SPCXXX License User Guide*, which is available in the following path at http://support.huawei.com/enterprise: Product Support > Cloud Computing & Data Centers > Cloud Computing > FusionAccess > FusionCloud Desktop Solution.

-

5. Load the license.

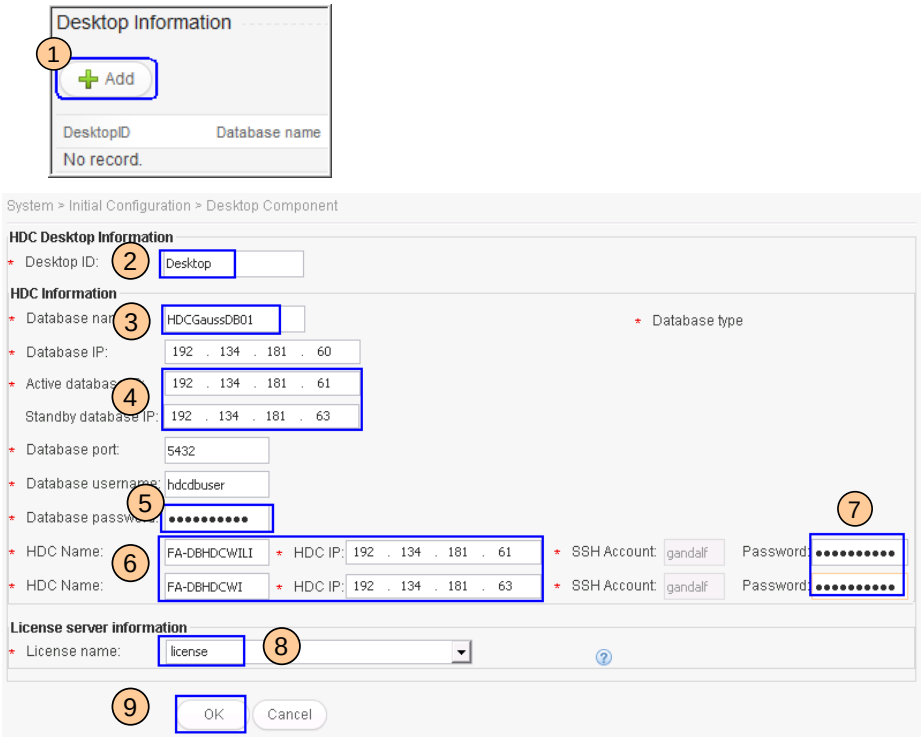



-

## 7.3 Configuring Desktop Components

### Step 3 Configure the Desktop.

1. Add the Desktop information.




2. Click **Return to Desktop Configuration List**.

2 Enter the Desktop ID.

3 Enter the HDC database instance name (G1).

4 **Database IP**: floating IP address (B2)
**Active database IP and Standby database IP**: service IP addresses of the active and standby GaussDB server (B2)

5 Enter the HDC database instance user password, which is Huawei@123 by default.

6 Enter the computer name and IP address (B2) of the service plane VM of the HDC server. The value is the same as that of Name in Configure the forward and reverse DNS lookups.

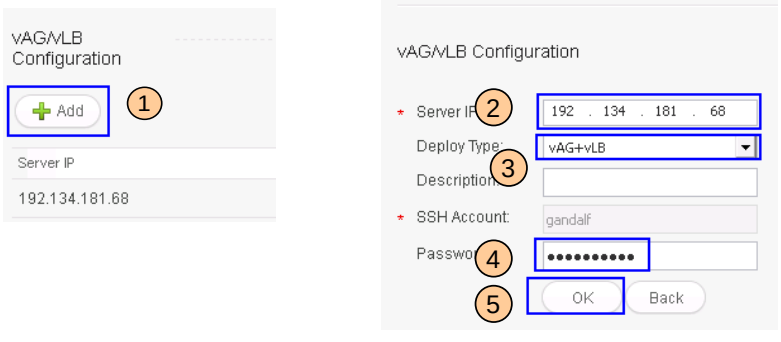
7 The default password of SSH is **Huawei@123**.

8 Enter the name of the license added in Step 3.

-

### Step 4 Configure the vAG/vLB.

1. Add the vAGvLB.




2. Click **Back.**

2 Enter the service plane IP address of the vAG server (B2).

3 Select **vAGvLB, vAG,** or **vLB** based on deployment mode.

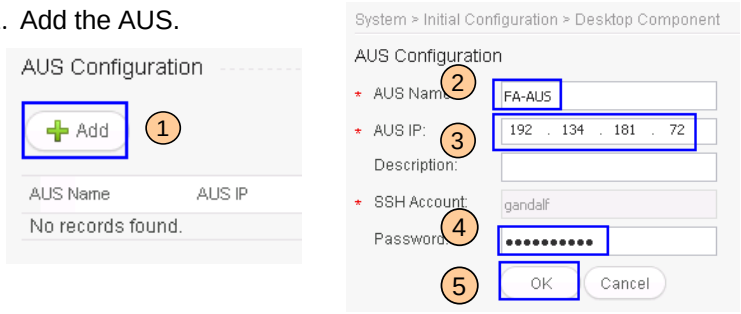
4 The default password of SSH is **Huawei@123**.

-

## 7.3 Configuring Desktop Components

### Step 5 Configure the AUS.

1. Add the AUS.




2 Enter the service plane IP address of the AUS (B2).

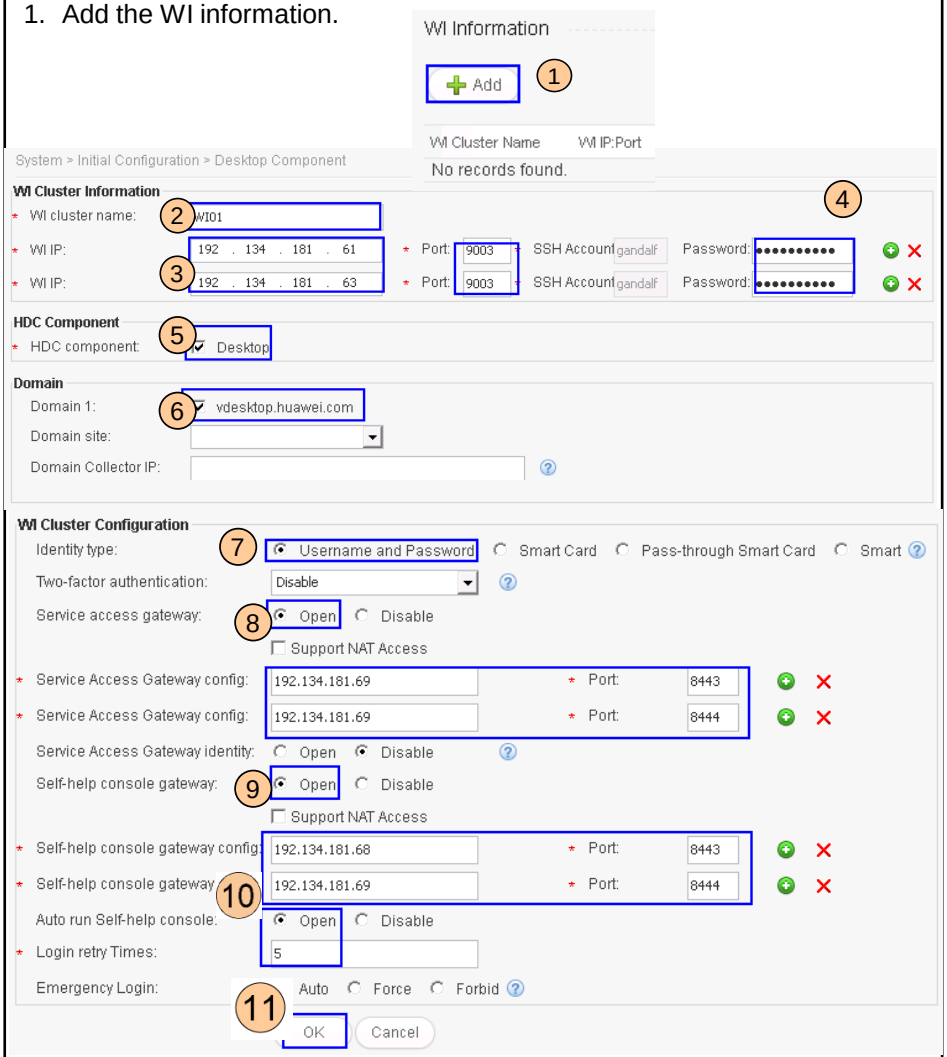
4 The default password of SSH is **Huawei@123**.

2. Click **Back.**

-

### Step 6 Configure the WI.

1. Add the WI information.




3 Enter the service plane IP addresses of the WI (B2).

6 Select **Enable** and enter the service plane IP addresses of the vAG (B2).

7 If **Support NAT Access** is selected after you select **Open**, enter the public IP address of the firewall in **Service Access Gateway config**.
If **Support NAT Access** is not selected, enter the service IP address of the vAG in **Service Access Gateway config**.
Select **Enable** and enter the service plane IP addresses of the vAG (B2).

8 If **Support NAT Access** is selected after you select **Open**, enter the public IP address of the firewall in **Self-help console gateway config**.
If **Support NAT Access** is not selected, enter the service IP address of the vAG in **Self-help console gateway config** (B2).

Select **Enable** and enter the login attempts based on site requirements.

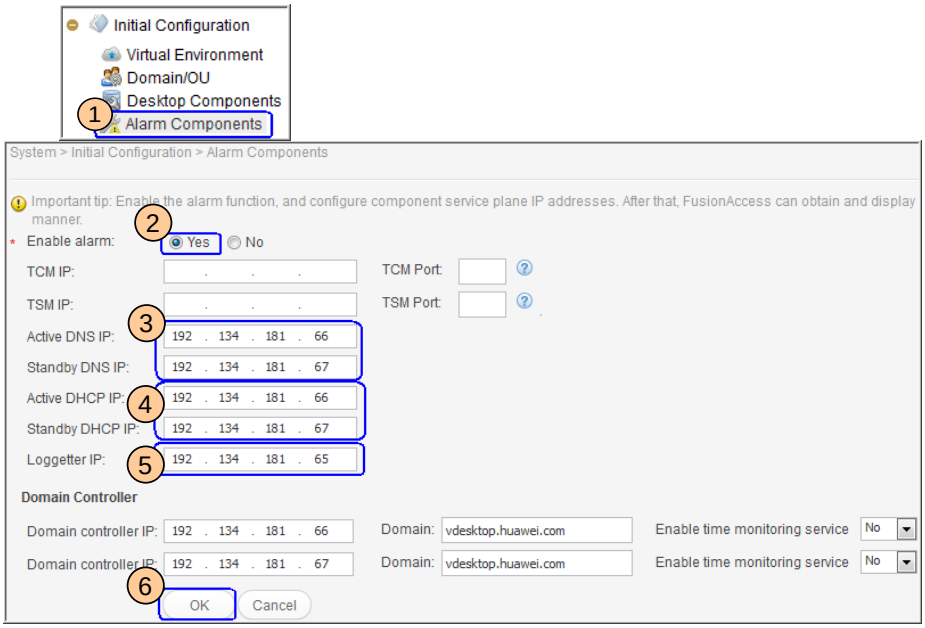
2. Click **Return**.

-

## 7.4 Configuring Alarm Components

### Step 1 Configure the alarm components.

1. Add the alarm components.



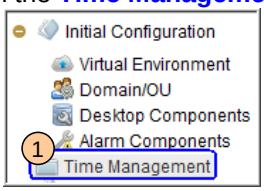

2. Complete the configuration as prompted.

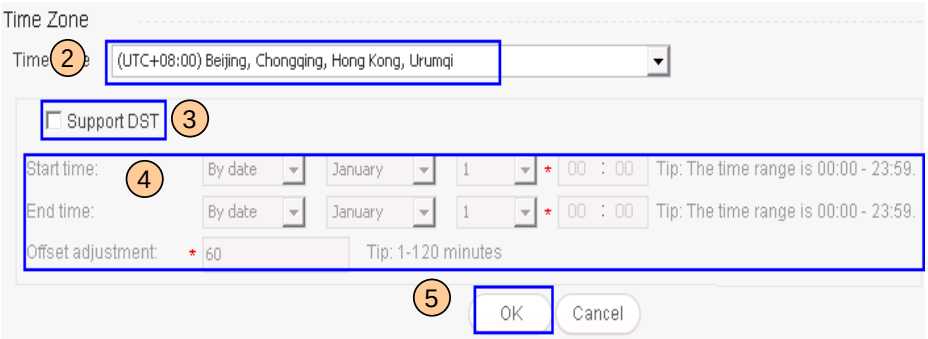
| | |
|---|---|
| | 3 Enter the service plane IP addresses of the DNS servers (B2).<br>4 Enter the service plane IP addresses of the DHCP servers (B2).<br>5 Enter the service plane IP address of the Loggetter server (B2). |
| - | |

## 7.5 Configuring Time Synchronization

### Step 1 Configure the DST rules.

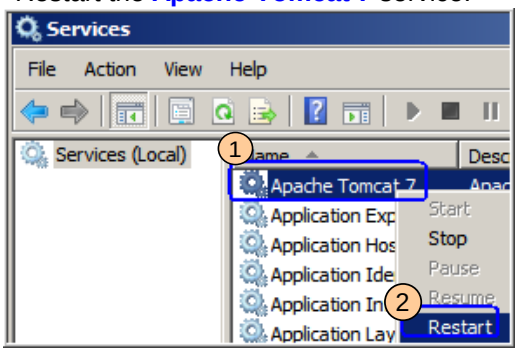
1. In the **Time Management** dialog box, set the time zone.

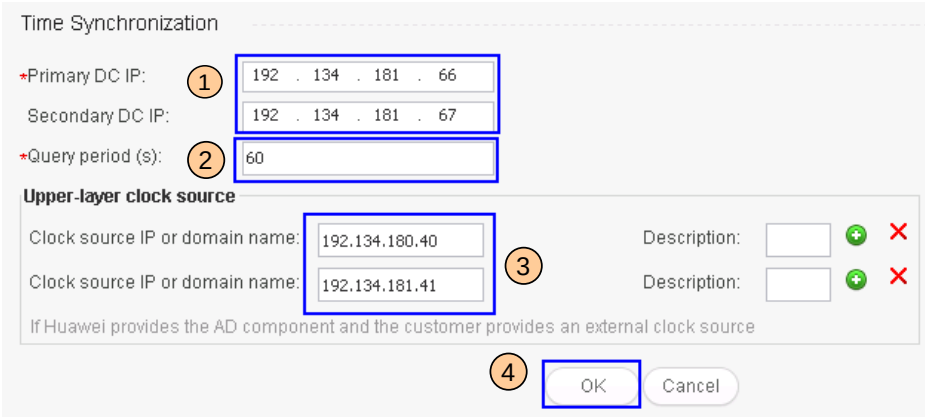



| | |
|---|---|
| | 2 Set the time zone based on actual conditions.<br>3 Select this option if the DST is observed in the time zone.<br>4 Set the data based on actual conditions. |

## 7.5 Configuring Time Synchronization

| Step 1 Configure the DST rules. | |
|---|---|
| 2. Log in to the active ITA server over VNC using the domain account. | - |
| 3. Choose **Start > Administrator Tools > Services**. | - |
| 4. Restart the **Apache Tomcat 7** service.<br>  | - |
| 5. Log in to FusionAccess using the service plane IP address of the standby ITA server. | - |
| 6. Repeat **Steps 1 to 4** to configure the DST rules. | - |

| Step 2 Configure time synchronization. | |
|---|---|
| 1. Set time synchronization information.<br>  | ① Enter the service plane IP addresses of the AD servers (B2).<br><br>③ If the customer provides a stable clock source, enter the address or domain name of the clock source.<br>If the customer does not provide the clock source, enter the management IP addresses or domain name of the CNA nodes hosting the VRMs. |

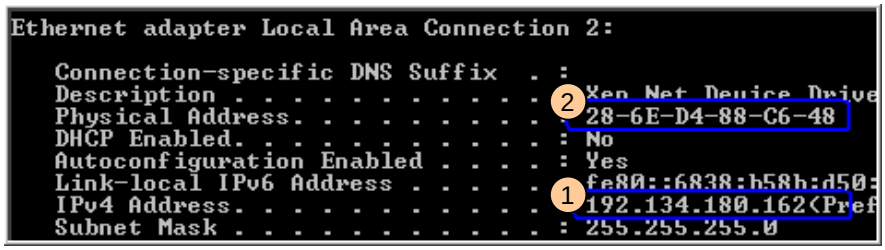
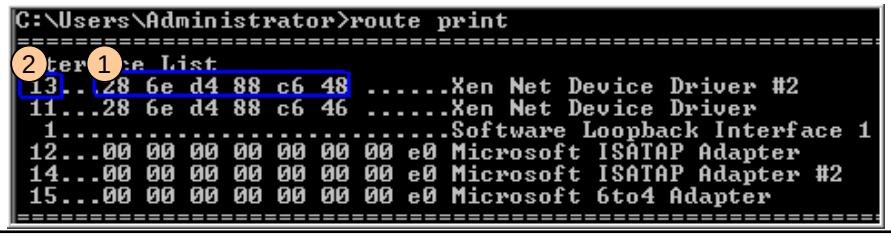
## 7.6 Checking Component Status

| Step 1 Check the components. | |
|---|---|
| 1. Choose **Alarm> Status Check**. | - |
| 2. If the status is normal for all components, the components are successfully installed. | - |

# Appendix 1 Configuring the Desktop Cloud Address

**(After configuration, you can access FusionAccess from FusionManager.)**

## Step 3 (Optional) Configure the maintenance network.

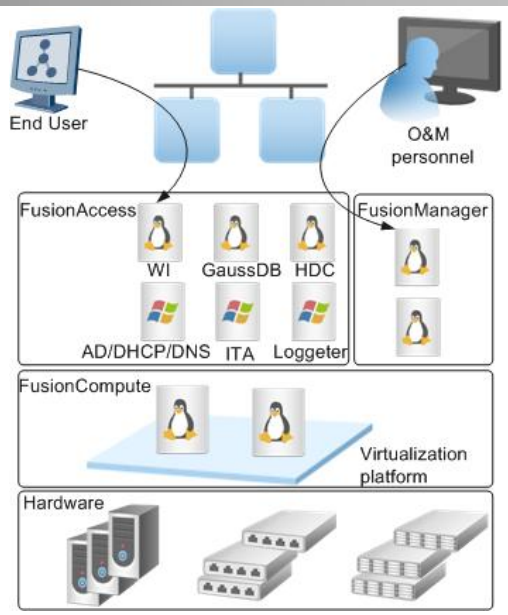
| | |
|---|---|
| 2. Log in to the active AD server as user SWMaster. | - |
| 3. On the DOS window, run the **ipconfig /all** command to query the MAC address of the management NIC of the infrastructure VM based on the **management plane IP network segment**.<br>  | In this example, the system management plane IP network segment is **192.136.1.*XXX*** and the MAC address of the management NIC is **28-6E-D4-88-C6-5C**. |
| 4. Run the **route print** command to query the management NIC interface ID based on the MAC address.<br>  | In this example, the management NIC interface ID is **13**. |
| 5. Add route to the active AD server.<br>**route -p add** *System administrator PC network segment* **mask** *Subnet mask Desktop cloud management plane gateway* **if** *Management NIC interface ID*<br><br>For example, if the system administrator accesses FusionManager through the 192.154.0.0/23 network segment, management plane gateway IP address is 192.136.1.1, and the management NIC interface ID is 13, run the following command:<br>**route -p add *192.154.0.0* mask *255.255.254.0* *192.136.1.1* if *13*** | - |
| 6. If the system administrator needs to access FusionManager through multiple network segments, add routes for all the network segments. For details, see **Step 5**. | - |
| 7. Log in to the infrastructure VM hosting the standby AD, active ITA, standby ITA, and Loggetter, respectively and repeat steps **1** to **6** to add the route data. | - |

# FusionAccess Lab Guide

Issue 01
Date: 2015-07

## Introduction to FusionAccess

Huawei FusionAccess is virtual machine (VM) management software deployed on a virtualization platform. It enables users to access virtual desktops by using networked client devices, such as thin clients (TCs), desktop computers, laptops, and smartphones. FusionAccess transforms the traditional PC-dominated office model with features such as security, investment, and office efficiency. It is an optimal choice for large- and medium-sized enterprises, government agencies, and mobile offices.



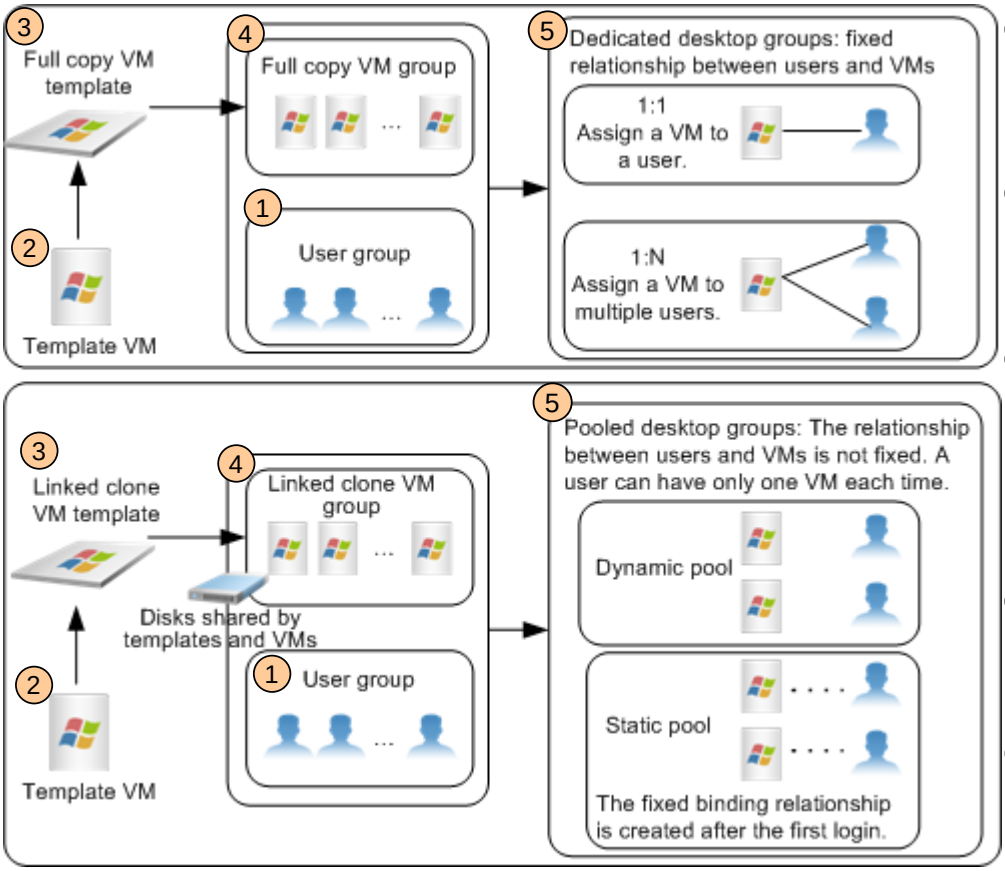

## Objectives

This guide help you quickly complete configuration and service provisioning tasks in FusionAccess.
This guide focuses on provisioning and managing services. There are some tasks label as optional, which means trainees can skip this task. However, the instructor must prepare those tasks earlier.

# 1 Service Provisioning Rules and Application Scenarios

## 1.1 Service Provisioning Rules

The following figure shows the relationships among the template, VM, VM group, user group, and linked clone.




1 User or user group: One or a group of domain users who can log in to VMs using domain accounts.

2 Template VM: An empty VM on FusionCompute for creating various types of VM templates.

3 VM template: A template used to create VMs for users. You can convert a template VM into a template by configuring or optimizing the template VM or installing software on the template VM.

4 VM group: A group of user VMs created by using the same VM template.

5 Desktop group: a group of VMs assigned to users or user groups.

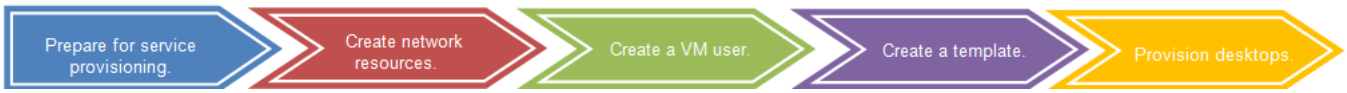
## 1.2 Application Scenarios

This document describes how to create and provision VMs by using a full copy template or a linked clone template. The following table describes the functions of VMs created using the two types of templates.

| Template Type | Relationships Between End Users and VMs | Application Scenario |
|---|---|---|
| **Full copy** | After a full copy VM is assigned to a user, **the user can only log in to the assigned VM.** After the VM shuts down, the user data and customized configurations are **stored**. Only a user who has **Administrator** rights can log in to a full copy VM. | Office automation (OA) |
| **Linked clone** | If a VM is assigned to a user who is **in the static pool, the user can log in to the same VM each time. However, if the VM is assigned to a user who is in the dynamic pool, the user can log in to a different VM each time.** By default, the user data and customized configuration are **not stored** after a VM shuts down. Only a user who has **Users** rights can log in to a linked clone VM. | Call center |

# 2 Preparations

## 2.1 Process




**Templates** include full copy templates and linked clone templates.
**Desktop service provisioning** is quick provisioning.

## 2.2 Prerequisites

FusionAccess has been installed and configured.

## 2.3 Obtaining Files

The data planning template created during software installation. This template contains service provisioning information.

**Note:**
This template is referred to as the **Data Planning Template** in this document.

## 2.4 Obtaining Software

The VM described in this document runs Windows 7 operating system (OS).

| Item | Name | Where to Obtain | Description |
|---|---|---|---|
| OS ISO file | - | - | Prepared by the lab administrator. |
| Image-making tool | FusionAccess_Mirror_V100R005C20SPCxxx.iso | http://support.huawei.com/enterprise > Downloads > IT > FusionCloud > FusionAccess > FusionAccess > V100R005C20SPCxxx | This tool supports Chinese, English, and Arabic OS image files. |
| OS patches (Windows 7 32-bit) | •976932<br>•2958122<br>•Other path | •**976932**: http://www.microsoft.com/zh-cn/download/details.aspx?id=5842<br>•**2958122**: http://support.microsoft.com/kb/2958122 | •For versions earlier than Windows 7 SP1, install **976932**. For Windows 7 SP1 and later versions, this patch is not required.<br>•For Windows 7 SP1 version, install **2958122**.<br>•Select OS patches by the type and language of OSs. |
| OS patches (Windows 7 64-bit) | | | |
| Application software | - | - | Prepared by the lab administrator. |

# 2 Preparations (cont.)

## 2.5 Data

Before provisioning services, plan the following data with lab administrator:

| Type | Parameter | Example Value and Planned Value |
|---|---|---|
| **A. Network information** | **(A1) port group name**<br>Name of the port group for the service plane. | *portgrounp*<br>**Planned value:** _____ |
| | **(A2) port group**<br>Number of the port group for the service plane.<br>The VMs with ports in the same port group belong to the same virtual network even if the VMs are deployed on different physical servers. | *133*<br>**Planned value:** _____ |
| | **(A3) Scope Name**<br>Name of the IP address pool, from which IP addresses are assigned to user VMs. | *UserVM_DHCP*<br>**Planned value:** _____ |
| | **(A4) Scope**<br>The IP address segment that can be assigned to user VMs. | IP address pool: *192.134.133.10 to 192.134.133.100*<br>Gateway: *192.134.133.1*<br>**Planned value:**<br>IP address pool: _____<br>Gateway: _____ |
| **B. User information** | **(B1) OU Name**<br>Name of the organization unit (OU) to which a user VM belongs. | *UserOU*<br>**Planned value:** _____ |
| | **(B2) Group name**<br>Name of a user group. | *vds*<br>**Planned value:** _____ |
| | **(B3) Domain user name and Password**<br>Username and password for logging in to the user VM. | Username: *vdsuser*<br>Password: *Huawei123*<br>**Planned value:**<br>IP address pool: _____<br>Gateway: _____ |
| **C. Template VM information** | **(C1) VM name**<br>Name of a template VM. | *full_copy*<br>*link2*<br>**Planned value:** _____ |
| | **(C2) Serial number for the ISO VM that runs Windows XP.** | *XXXXX-XXXXX-XXXXX-XXXXX-XXXXX*<br>**Planned value:** _____ |
| **D. VM provisioning information** | **(D1) VM Group name**<br>Name of a VM group. | *vds_full*<br>**Planned value:** _____ |
| | **(D2) VM naming rule**<br>Naming rule for VMs. | *vm_namerule##*<br>**Planned value:** _____ |
| | **(D3) VM Group name**<br>Name of a desktop group. | *Desktop*<br>**Planned value:** _____ |

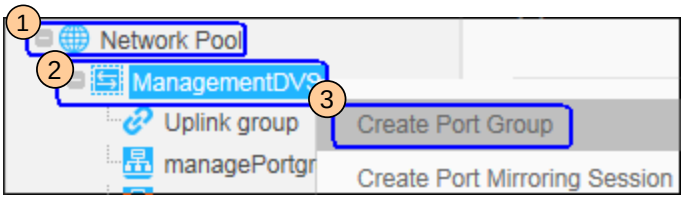
# 3 Creating Network Resources(Optional Task)

**Note:**

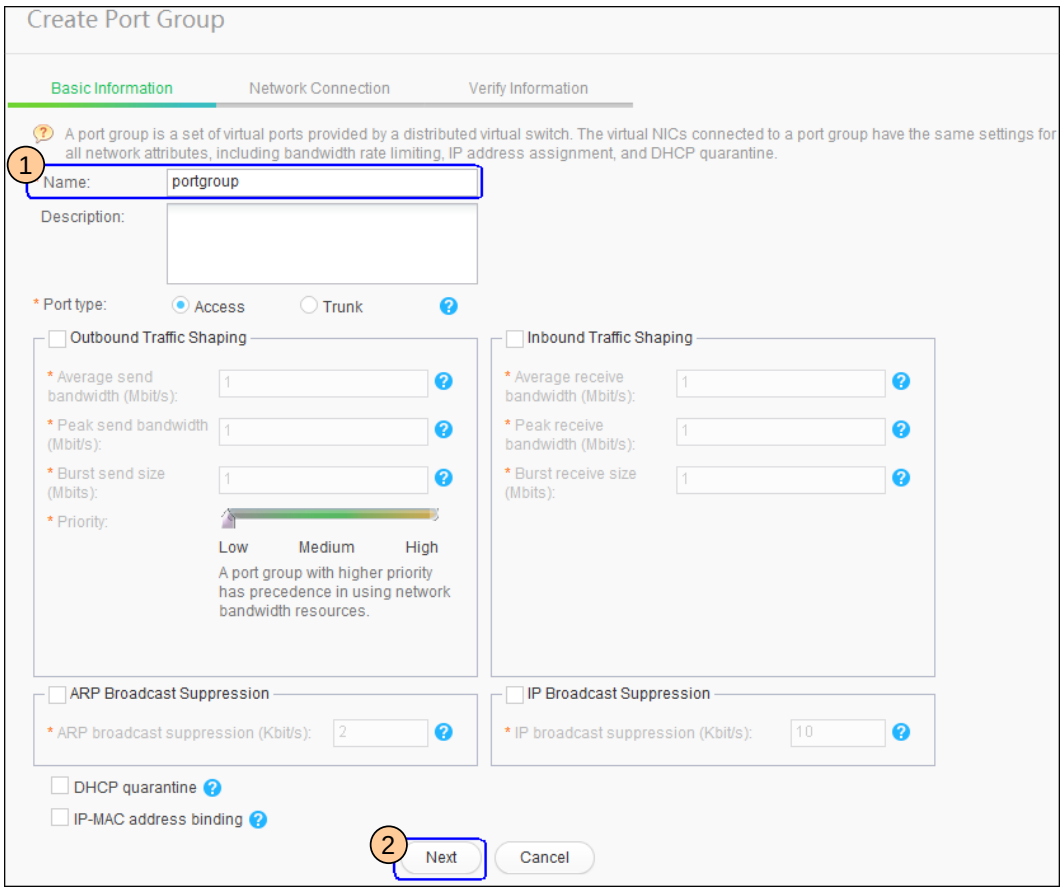
If the user VM uses the network resources created for the service plane during the FusionAccess installation, you can skip over this section.

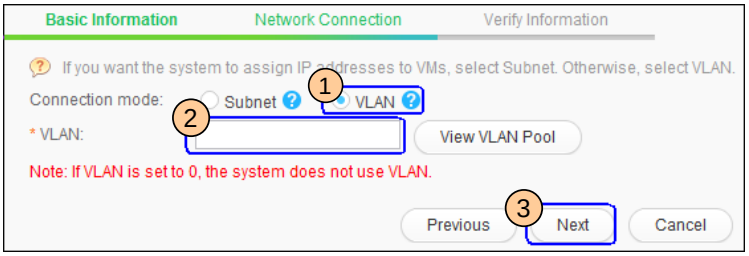
## 3.1 Creating a Port Group

### Step 1: Create a port group.

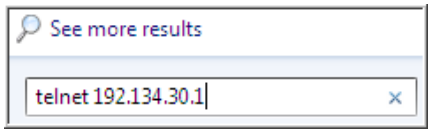
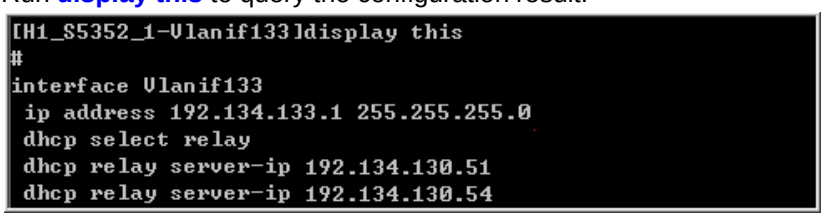
| | |
|---|---|
| 1. Visit *http://VRM floating IP address* to log in to FusionCompute. | Obtain the VRM floating IP address from the **Data Planning Template**. |
| 2. Choose **Network Pool**. | - |
| 3. Go to the **Create Port Group** page.<br>  | 1 Select the distributed virtual switch (DVS) connecting to the service plane.<br>**Note:**<br>In this example, the management plane and service plane belong to the same network segment.<br>After you choose **XXXDVS** in the navigation tree, the VLAN pool range is displayed on the **Summary** tab page. |

4. Set the port group name (A1).

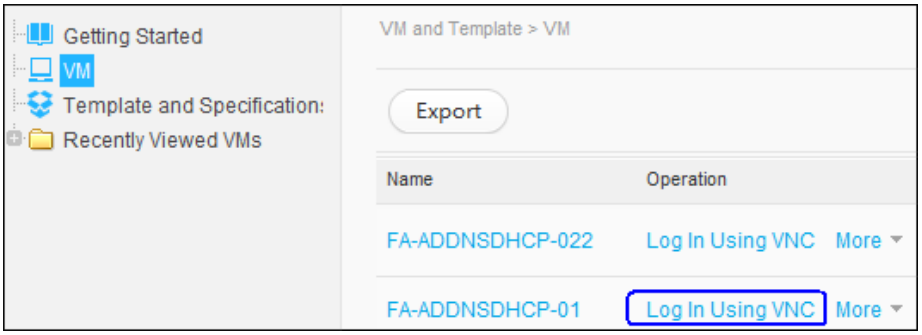
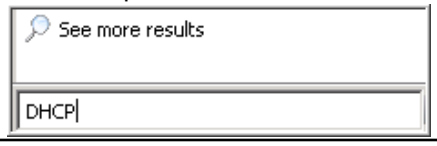
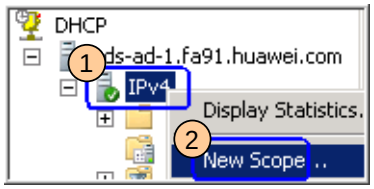
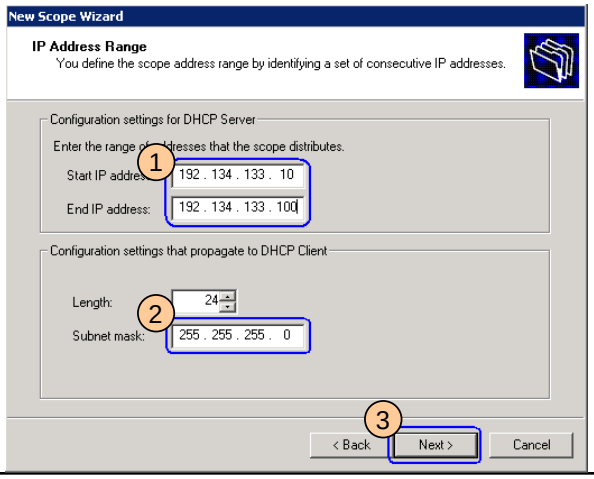


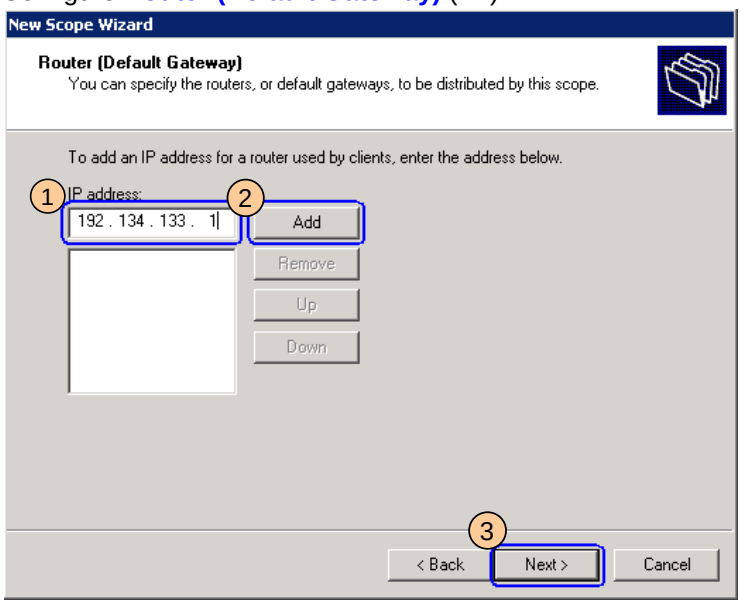
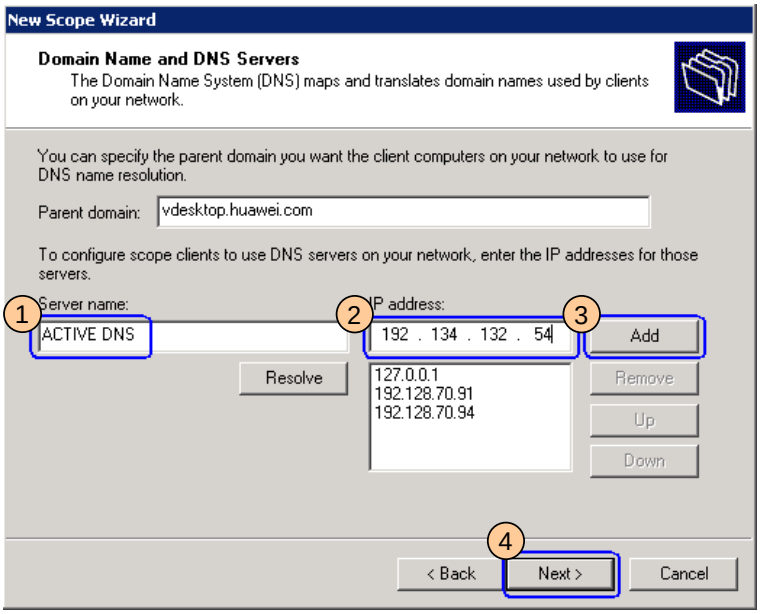
| Step 1: Create a port group. | |
|---|---|
| 5. Set the VLAN ID (A2).<br>  <br> | To view the VLAN ID range of the VLAN pool, click **View VLAN Pool**.<br><br>The **VLAN ID** is used in subsequent operations described in **Configure an aggregation switch**, **Creating a Template**, **and Provisioning VMs**. |
| 6. Confirm the settings and click **Create**. | - |
| 7. In the displayed dialog box, click **OK**. | - |

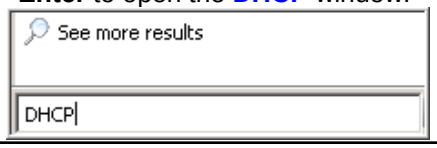
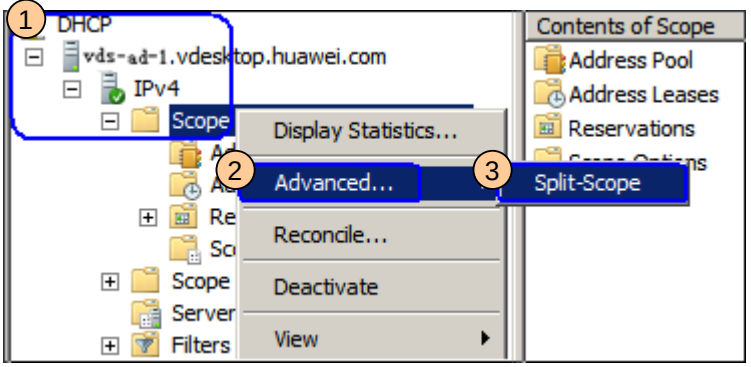
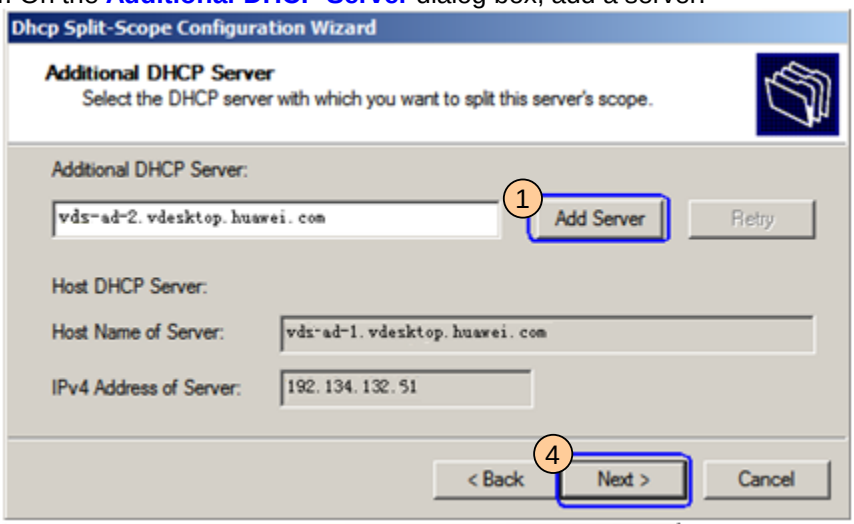
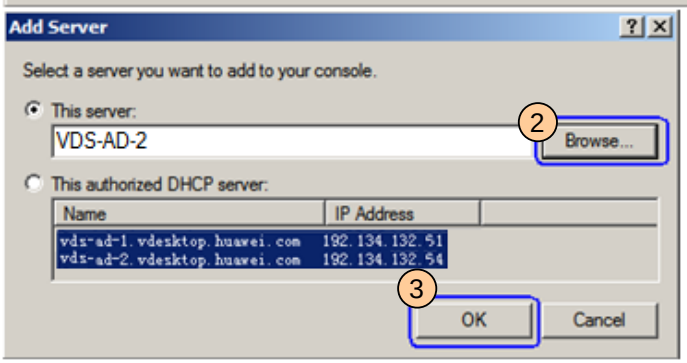
## 3.2 Configuring the Network Environment

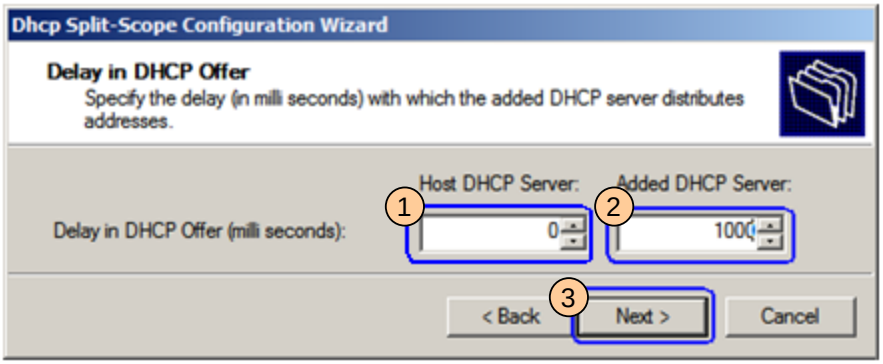
| Step 1: Configure an aggregation switch. | |
|---|---|
| 1. On the local PC, choose **Start**, enter **telnet** *switch IP address* in the **Search** text box, and press **Enter** to log in to the aggregation switch.<br>  <br> | |
| 2. On the DVS, configure IP addresses and gateway IP (A4) for the DHCP server that allocates IP addresses for user VMs.<br>**<Quidway>system-view**<br>**[Quidway] interface vlanif** *Service plane vlanid*<br>**[Quidway-Vlanif***vlanid***] ip address** *Gateway and subnet mask of the DHCP address pool*<br>**[Quidway-Vlanif***vlanid***] dhcp select relay**<br>**[Quidway-Vlanif***vlanid***] dhcp relay server-ip** *Service IP address of the active DHCP server*<br>**[Quidway-Vlanif***vlanid***] dhcp relay server-ip** *Service IP address of the standby DHCP server*<br>**[Quidway-Vlanif***vlanid***] quit**<br>**[Quidway] quit**<br>**<Quidway>save** | VLAN ID is the one created in **3.1 "Creating a Port Group."**<br><br>Enter the planned DHCP address pool data (A4). |
| 3. Run **display this** to query the configuration result.<br>  <br> | Before running this command, run **system-view** to go to **[Quidway]**. |

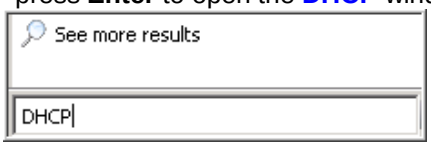
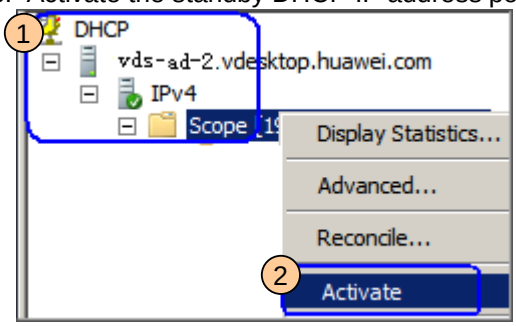
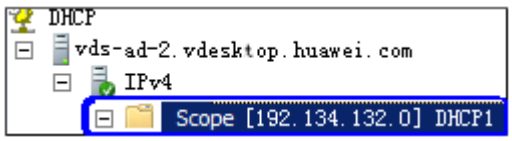
## 3.3 Adding a DHCP Address Pool(Optional Task)

| Step 1 Create a DHCP address pool. | |
|---|---|
| 1. On FusionCompute, choose **VM and Template** > **VM**. | - |
| 2. Log in to the active DHCP server using virtual network computing (VNC).<br>  | Login account:<br>•If server security hardening is performed, the account is **Swmaster**.<br>•If server security hardening is not performed, the account is **Administrator**.<br><br>Account password: obtained from the **Data Planning Template**.<br><br>In this document, the DHCP server and AD server are deployed on the same VM. |
| 3. On the active DHCP server, enter **DHCP** in the **Search** text box and press **Enter** to open the **DHCP** window.<br>  | - |
| 4. On the active DHCP server, open the **New Scope** window.<br>  | - |
| 5. Click **Next**.<br>In the displayed dialog box, set **Scope Name** (A3) and click **Next**. | - |
| 6. Enter the start IP address, end IP address, and subnet mask (A4).<br>  | 1 2<br><br>Enter the planned DHCP address pool data. |

| Step 1 Create a DHCP address pool. (cont.) | |
|---|---|
| 7. Specify **Excluded address range** and click **Next**.<br>Set **Lease Duration** and click **Next**.<br>Select **Yes, I want to configure these options now** and click **Next**. | Retain the default values of the parameters. |
| 8. Configure **Router (Default Gateway)** (A4).<br>  | 1 Enter the planned **gateway IP** address of the DHCP address pool. |
| 9. Configure the DNS server for the VMs in the DHCP address pool.<br>  | 2 Enter the service IP address of the DNS server.<br><br>To configure both the active and standby DNS servers, repeat 1 2 3.<br><br>If the service IP address of the DNS server exists by default, you do not need to add the IP address. |
| 10. Create the DHCP address pool as instructed. Retain the default values of the parameters. | - |

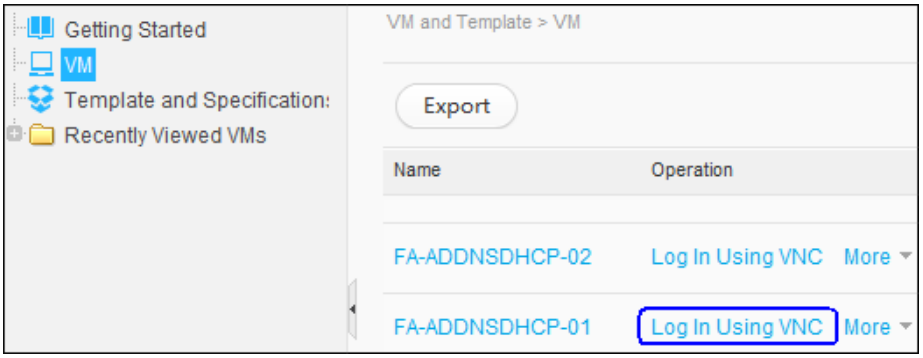
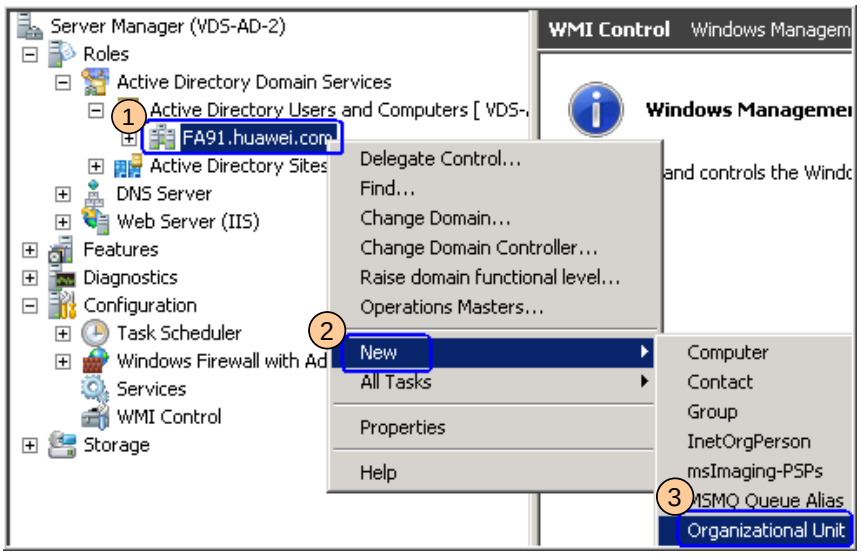
| Step 2 Synchronize the IP address pool on the active DHCP server to the standby DHCP server | |
|---|---|
| 1. Log in to the active DHCP server using virtual network computing (VNC). | - |
| 2. On the active DHCP server, enter **DHCP** in the **Search** text box and press **Enter** to open the **DHCP** window.<br>  | |
| 3. DHCP Split-Scope.<br>  | - |
| 4. On the **Additional DHCP Server** dialog box, add a server.<br>  <br>  | 2 In the dialog box displayed, enter the IP address or computer name of the standby DHCP server. |
| 5. Click **Next**. | - |

| Step 2 Synchronize the IP address pool on the active DHCP server to the standby DHCP server | |
|---|---|
| 6. On the **Additional DHCP Server** dialog box, set the **Delay in DHCP Offer**.<br>  | (2) In this example, **1000** indicates that the standby DHCP server starts to assign IP addresses 1000 ms later. |
| 7. Complete the synchronization operation as prompted. | - |

| Step 3 Activate the standby DHCP IP address pool | |
|---|---|
| 1. Log in to the standby DHCP server using virtual network computing (VNC). | - |
| 2. On the standby DHCP server, enter **DHCP** in the **Search** text box and press **Enter** to open the **DHCP** window.<br>  | - |
| 3. Activate the standby DHCP IP address pool.<br>  | - |
| 4. Check that the IP address pool status is the same as follows.<br>  | - |

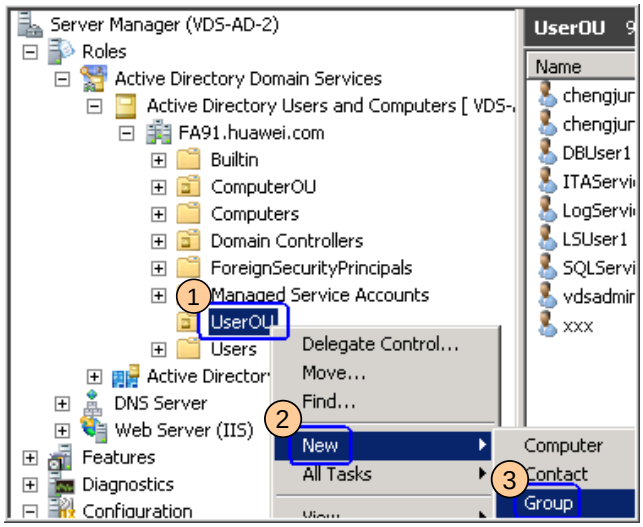
# 4 Creating a VM User

The relationship between the user OU, user group, and domain users in this document is only an example. In actual service provisioning, create VM users based on the planned data.

| Step 1: Create a user OU. | |
|---|---|
| 1. On the FusionCompute portal, choose **VM and Template** > **VM**. | - |
| 2. Log in to the active AD server using VNC.<br>  | Login account: **Swmaster**<br><br>Account password: obtained from the **Data Planning Template**. |
| 3. Click  in the lower left corner of the active AD server desktop. | - |
| 4. Create a user OU.<br>  | If the user OU already exists, skip over this step. |
| 5. Enter the OU name (B1), for example **UserOU**, and click **OK**. | Enter the planned name of the user OU. |

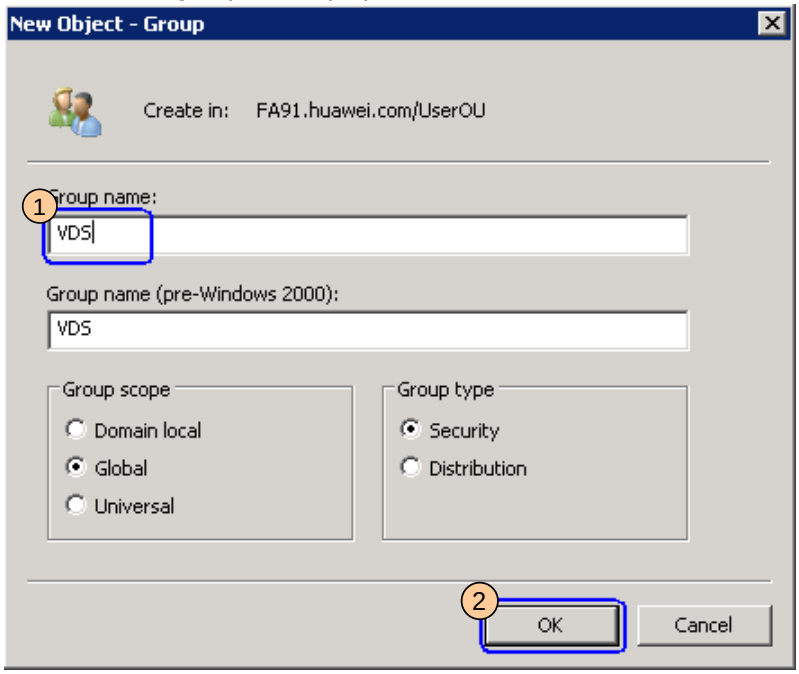
## Step 2: Create a user group.

1. Right-click the created user OU, and choose **New** > **Group**.




1 Select the newly created user OU.

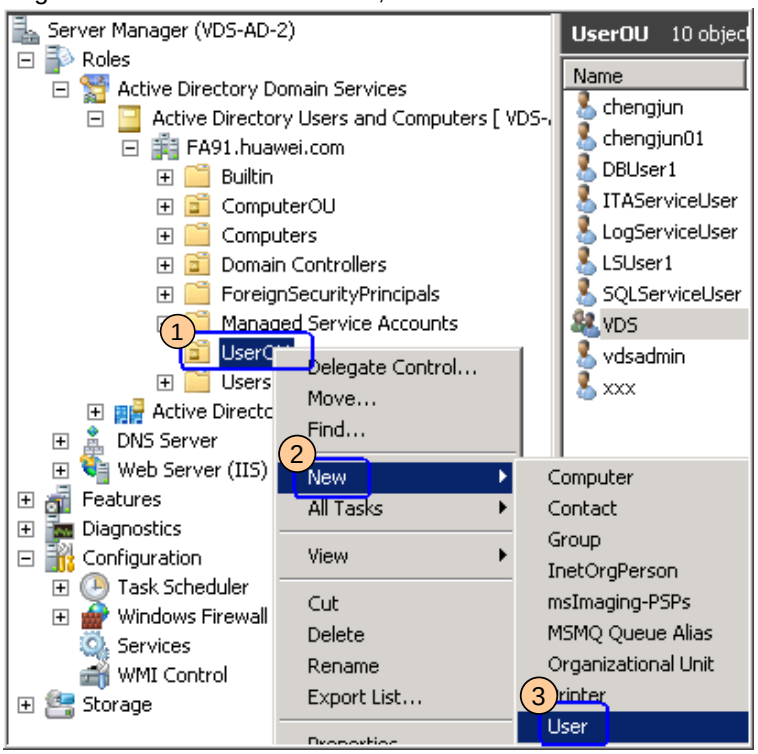
2. Enter the user group name (B2).




-

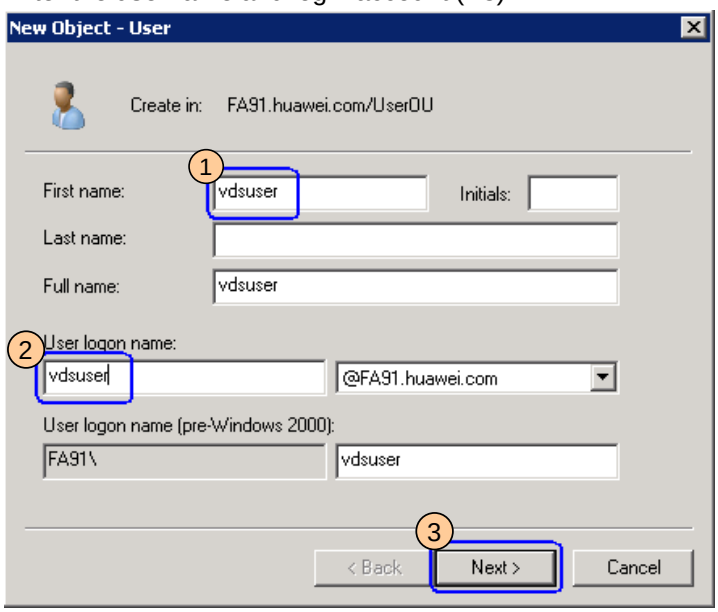
## Step 3: Create a user.

1. Right-click the created user OU, and choose **New** > **User**.




1 Select the newly created user OU.

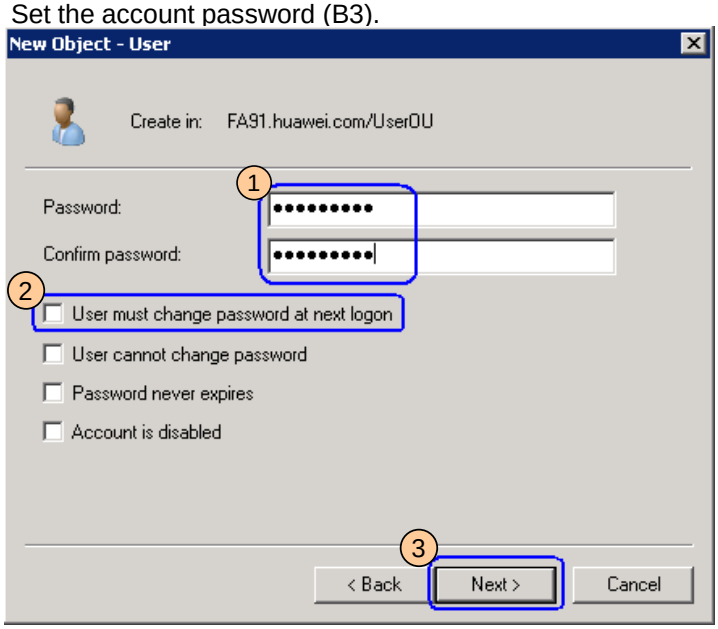
2. Enter the username and login account (B3).




-

## Step 3: Create a user.

3. Set the account password (B3).




4. Click **Finish**.

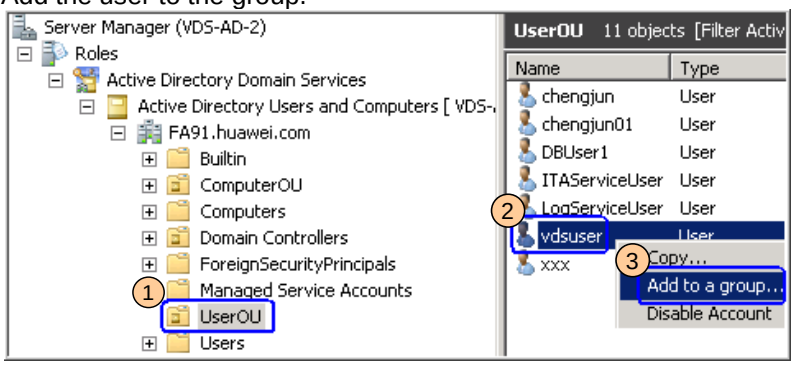
(1) The password must:

- Contain at least one uppercase letter (A-Z), one lowercase letter (a-z), one digit (0-9), and one space character or special character (~!@#$%^&*()-_=+\|{};:'",<.>/?).
- Contain 8 to 32 characters.
- Cannot be same as the recent three passwords.
- Cannot contain the username or the username in reversed order.

(2) Select user password policies based on the actual requirements.

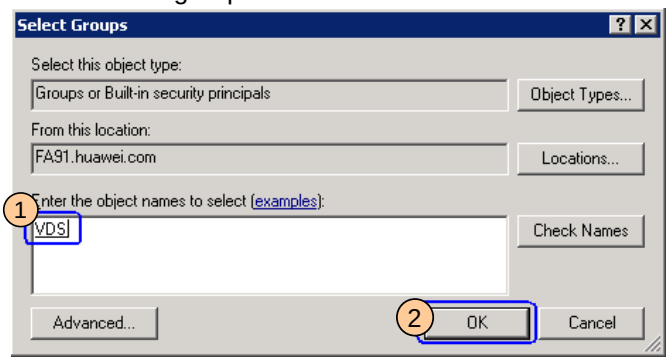
## Step 4: Add the user to the user group.

1. Add the user to the group.




(2) Select the user to be added.

2. Select a user group.




(1) Enter the name of the user group created on the AD server.

3. Click **OK**.

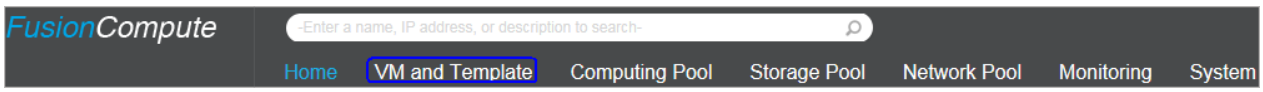
-

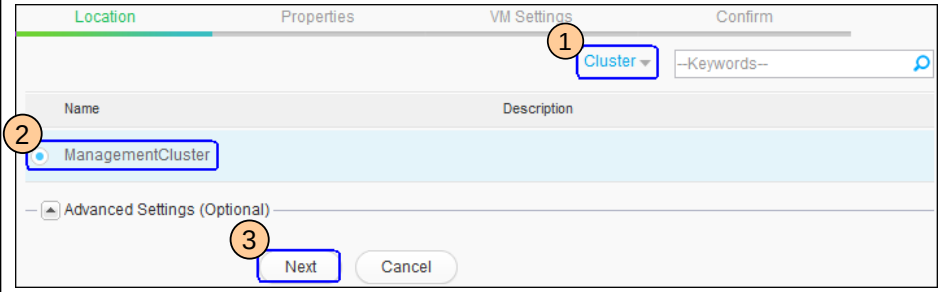
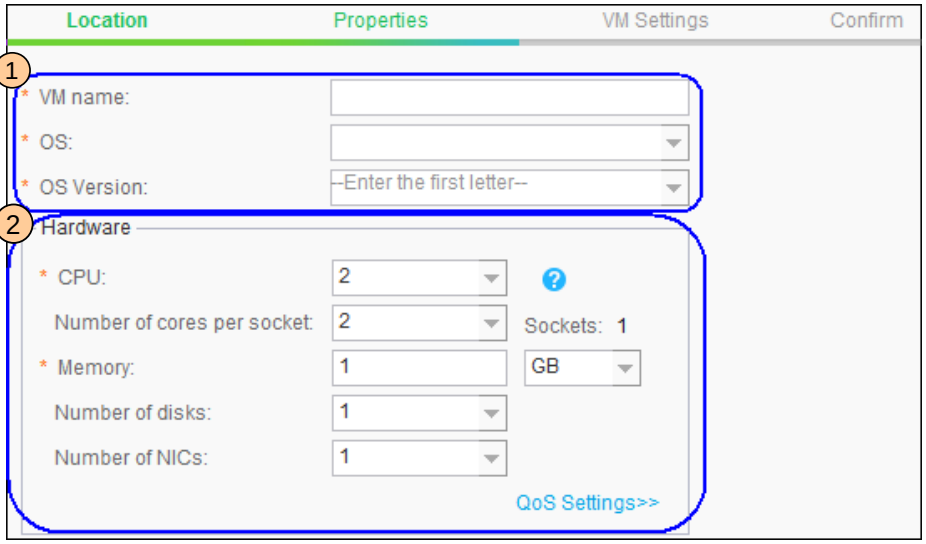
# 5 Creating a Template

## 5.1 Creating a Template VM

### Step 1: Create a template VM.

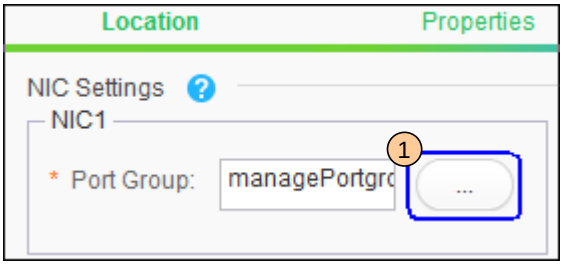
1. On the FusionCompute portal, choose **VM and Template**.

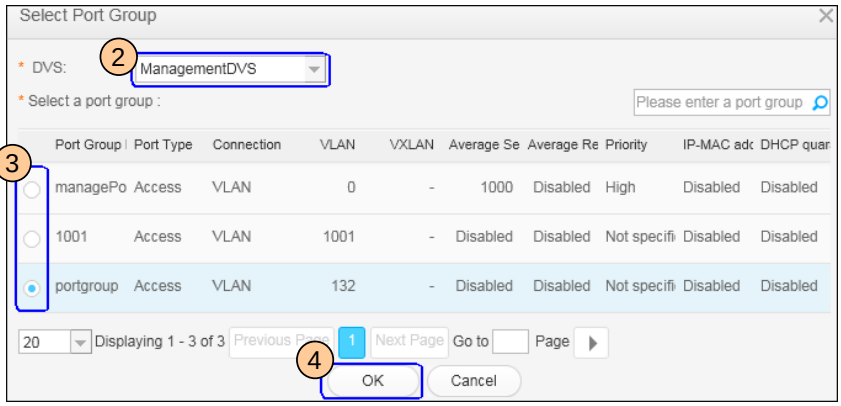



| | |
|---|---|
| 2. On **Getting Started**, choose **Create VM** go to the **Create VM** page. | - |
| 3. Select the location for creating the VM.<br>  | Select a location for creating a VM:<br>1<br>• **Cluster**: The VM is created on any host that is under the cluster.<br>• **Host**: The VM is created on a specified host. |
| 4. Set the following parameters:<br>  | 1<br>• **VM name**: (C1)<br>• **OS type and version**: Set the parameters based on the OS of the VM template to be created. Note that the value must be the same as the OS to be loaded later.<br>2<br>**Hardware specifications**: Set the parameters based on the hardware configuration requirements. |
| 5. On the **Properties** tab page, click **Next**. | - |

## Step 1: Create a template VM. (cont.)

6. Set the port group.

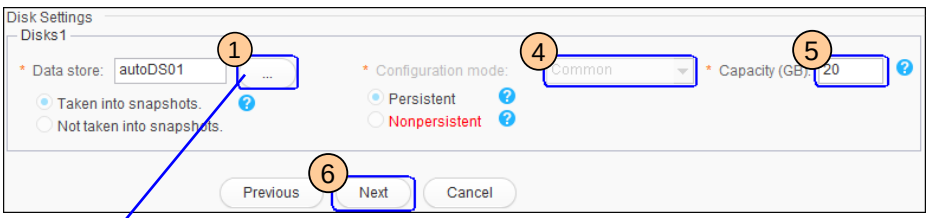


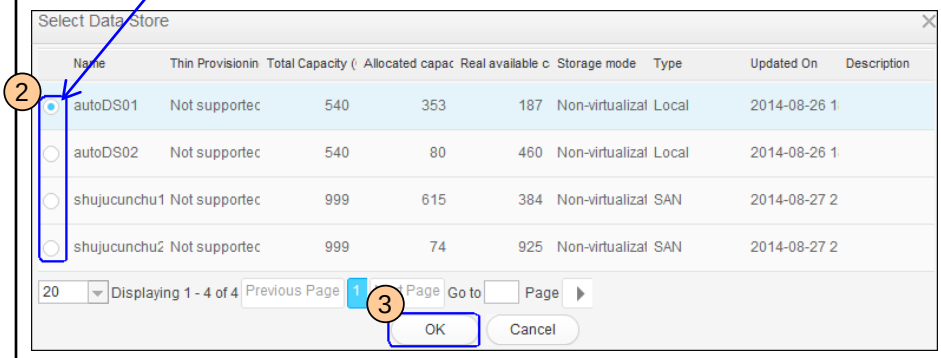




3

Select the port group created in **3.1 "Creating a Port Group."**

7. Set **Data store**, **Configuration mode**, and **Capacity** in sequence, and click **Next**.




4

- Set **Configuration mode** to **Common** for system disks.
- When creating a full copy template, set **Configuration mode** to **Thick provisioning lazy zeroed** for user disks if this option is available.

8. Check the VM information and click **Finish**.

The creation progress is displayed in the **Task Center** page.

9. In the displayed dialog box, click **OK**.

-

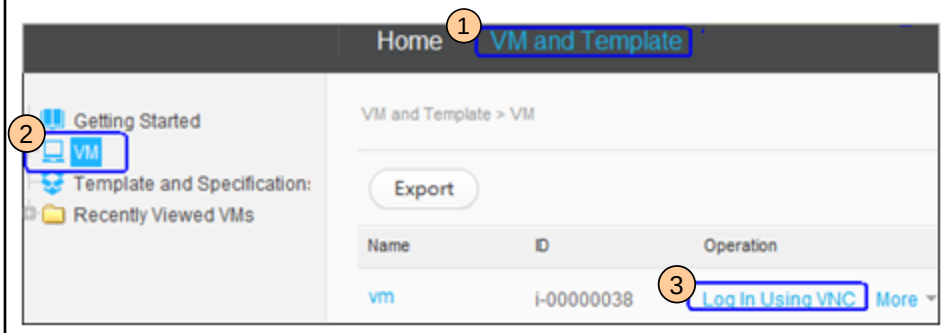
10. Go to the **VM** tab page.

If the VM status is **Running**, you can perform subsequent operations.

## 5.2 Installing a VM

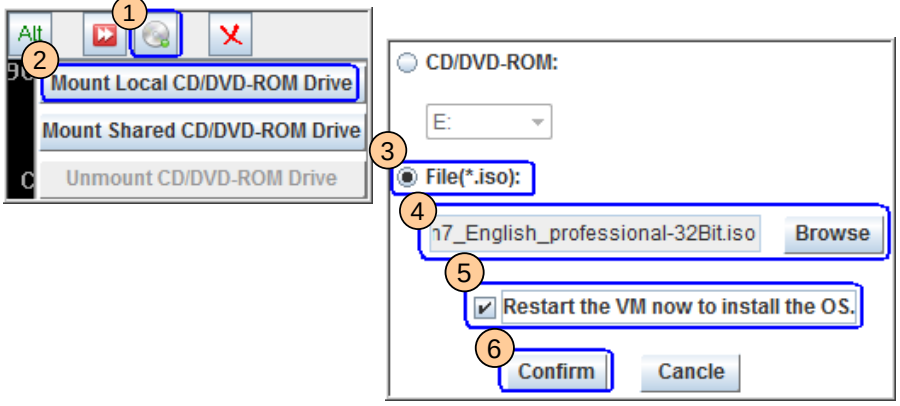
### Step 1: Install the OS.

1. Log in to **template VM** using VNC.




In the row that contains the newly created template VM, click **Log In Using VNC**.

2. Attach the ISO file.




4 The type of the IOS file must be the same as that of the OS selected in **5.1 "Creating a Template VM."**

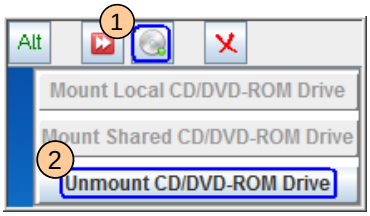
**Note:**
A host can be mounted to only one CD-ROM drive. Before mounting the CD-ROM drive, ensure that the CD-ROM drive is not mounted to any other VM on this host.

3. Install the VM OS. During the installation, set the parameters as follows:

| UI Information | Value |
|---|---|
| Which type of installation do you want? | **Custom (advanced)** |
| Type a user name | **LocalAccount (or customized)** |
| Help protect your computer and improve Windows automatically | **Use recommended settings** |
| Select your computer's current location | **Work network** |

The VM automatically restarts multiple times during installation.

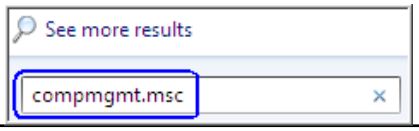
4. Unmount the CD-ROM drive.




-

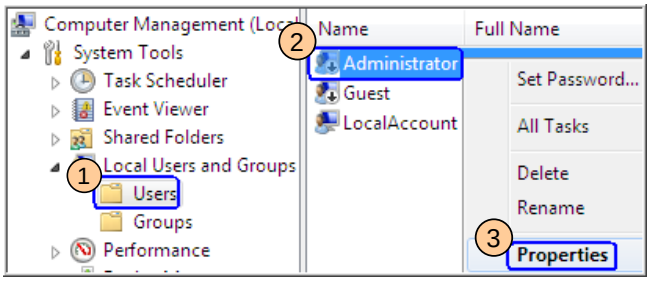
## Step 2: Activate the administrator account and set the password for this account.

1. On the template VM, go to the **Computer Management** window.



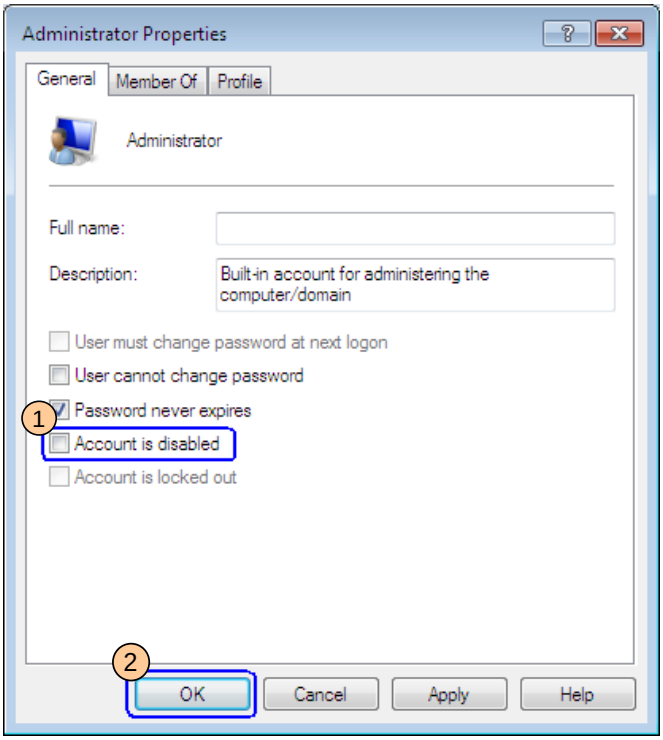

**compmgmt.msc**

2. Go to the **Administrator Properties** window.



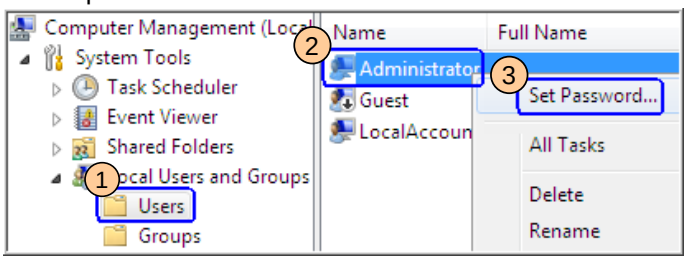

-

3. Activate the **Administrator** account.




1 Deselect this option.

4. Set the password for the **Administrator** account.




-

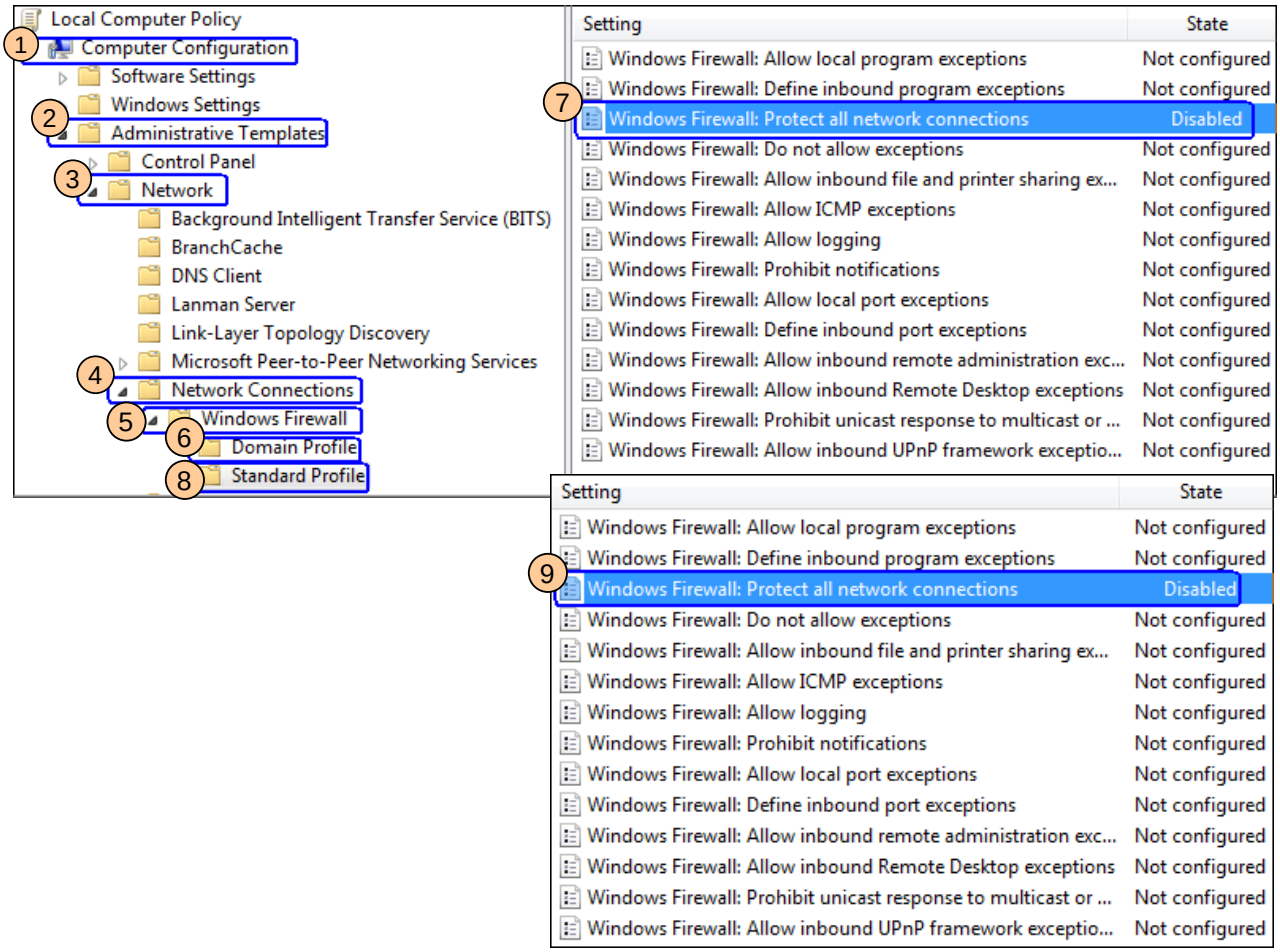
5. Click **Proceed**, set the password, and click **OK** twice as prompted. After the setting is complete, log off the VM and log in to the VM as **Administrator**.

-

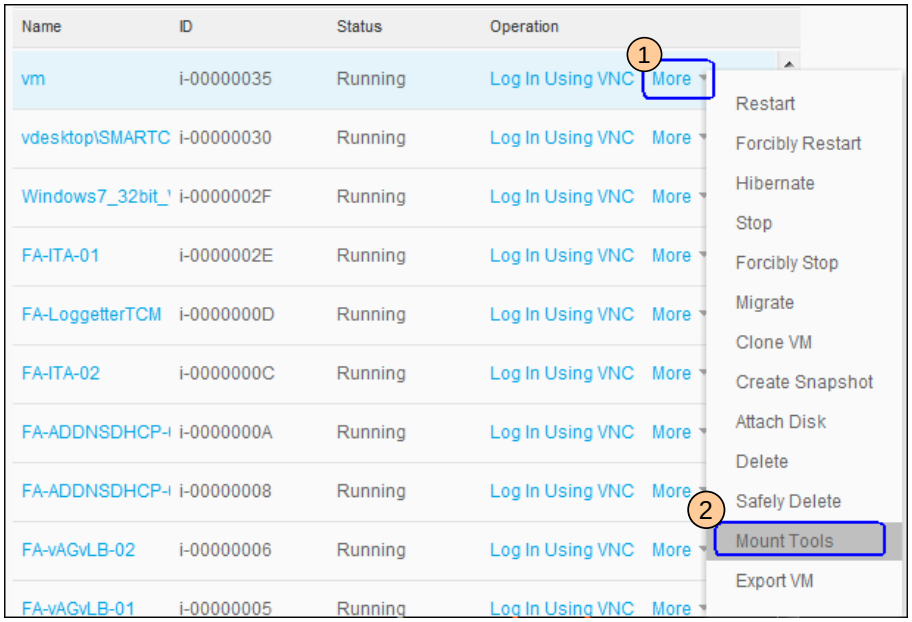
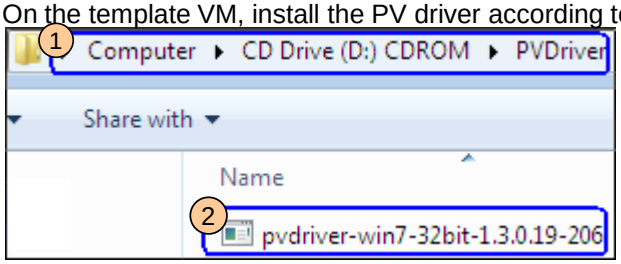
## Step 3: Disable the firewall on the VM.

| | |
|---|---|
| 1. Click **Start**, enter **gpedit.msc** in **Search programs and files**, and press **Enter**. | - |

2. Disable Windows Firewall.




| | |
|---|---|
| 3. Close the **Local Group Policy Editor** window. | - |

| Step 4: Install the paravirtualized (PV) driver. | |
|---|---|
| 1. On the FusionCompute portal, install tools for the template VM.<br>  <br> | Template VM |
| 2. On the template VM, install the PV driver according to the OS type.<br>  <br> | - |
| 3. After installation, restart the VM twice according to the displayed messages and log in to the VM as **Administrator**. | - |

| Step 5: Copy software and install the OS patches. | |
|---|---|
| 1. Copy the Windows 7 OS patches and application software (non-iso file) to disk **C:**. | - |
| 2. On the template VM, install the OS patches.<br>• iso file: Find the Windows 7 OS patches on the mounted CD-ROM drive.<br>• Non-iso file: Find the Windows 7 OS patches in **C:** on the VM. | - |

## 5.3 Configuring VMs

### Step 1: Use Desktop Cloud Image Optimization Tool to configure the OS for the VM.

1. In the VNC window of the template VM, attach the **FusionAccess_Mirror_V100R005C20SPCxxx.iso** file of **Desktop Cloud Image Optimization Tool.**

**Note:**

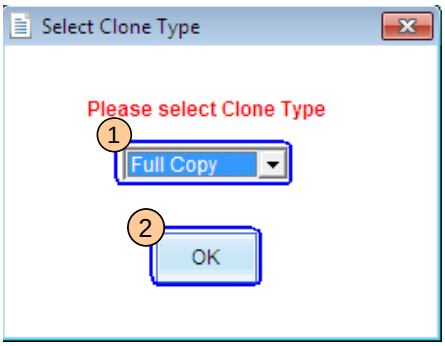
Do not select **Restart the VM now to install the OS** when attaching the tool or mounting the CD-ROM drive.

-

2. On the VM, open the CD-ROM, double-click **run.bat**.

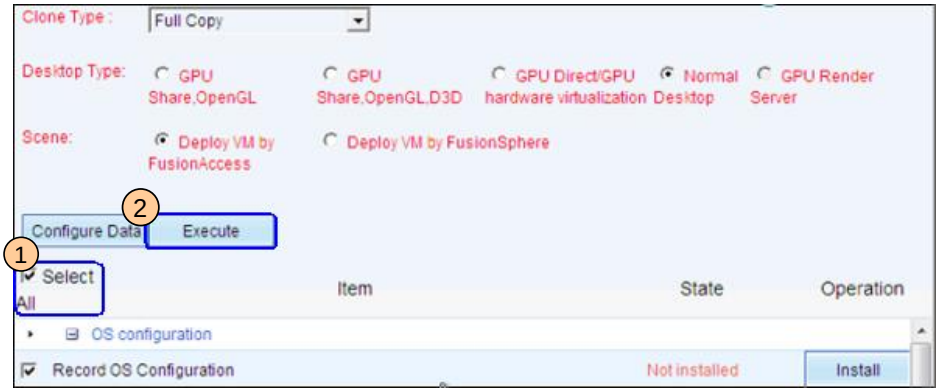
-

3. Select the clone type.



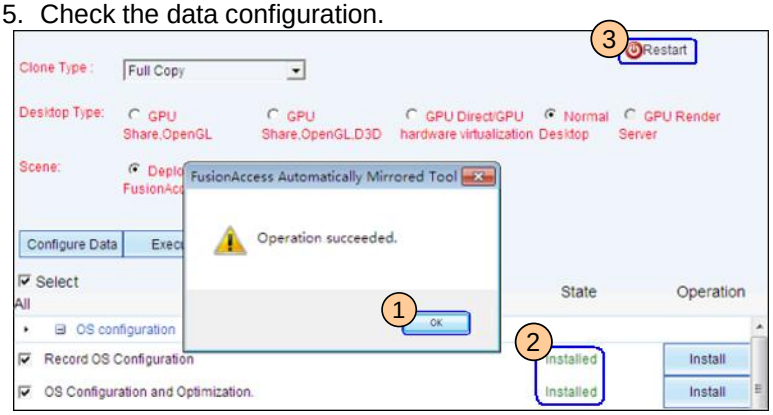

- To create a full copy template, select **Full copy**.
- To create a linked clone template, select **Linked clone**.

4. Configure the OS.




-

5. Check the data configuration.

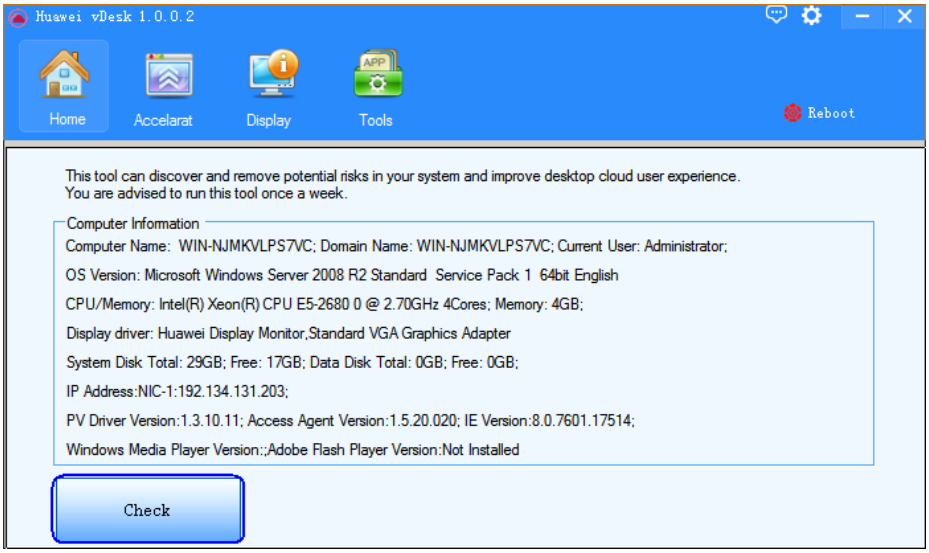
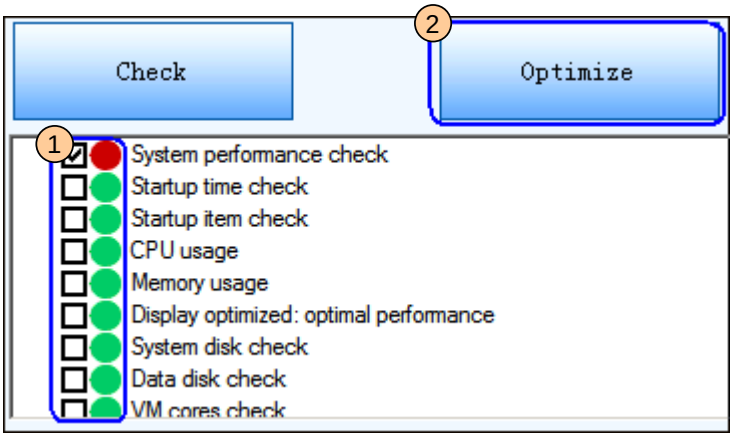
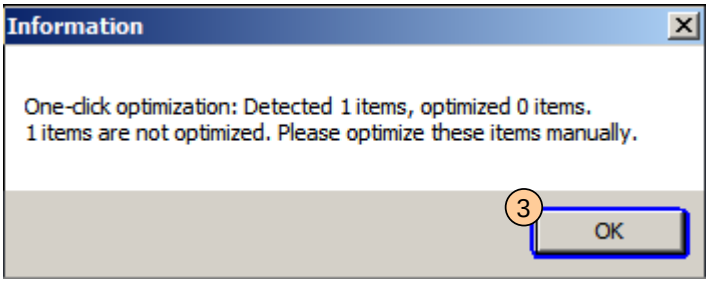



-

6. Restart the VM and log in to the VM as **Administrator**.

-

## Step 2: Optimize the ISO VM.

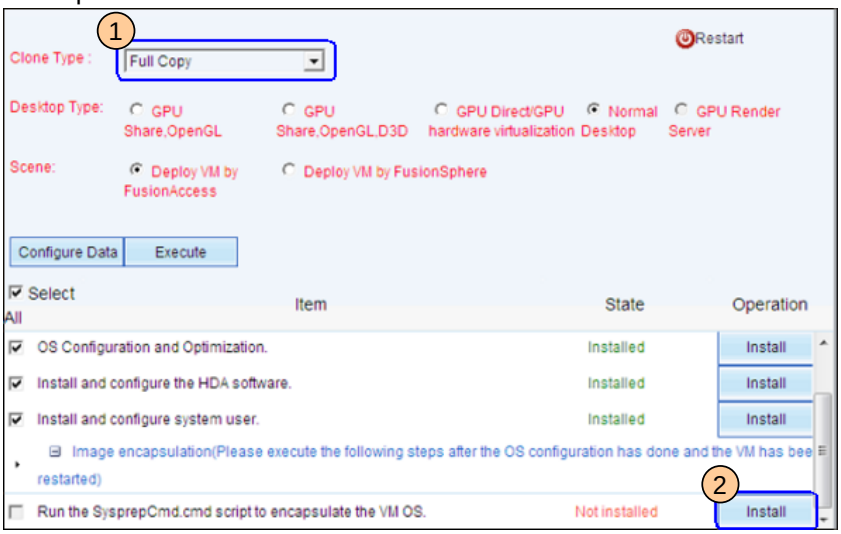
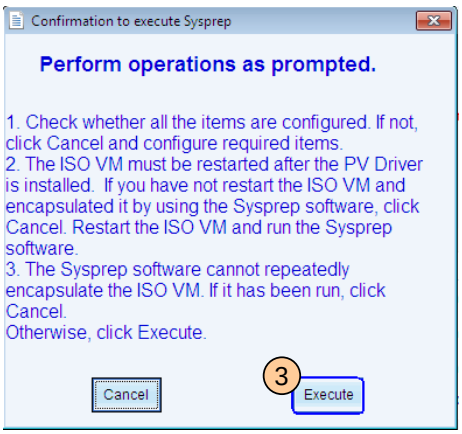
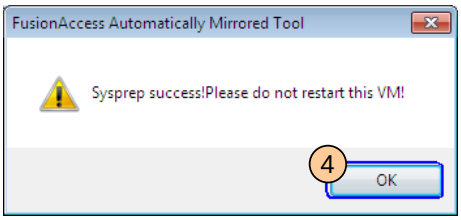
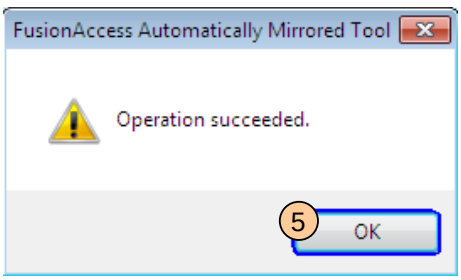
| | |
|---|---|
| 1. On the template VM, choose **Start > All Programes > Huawei FusionAccess**, and click **Huawei vDesk** to run the optimization tool. | - |
| 2. Click **Check**.<br>  | - |
| 3. Click **Optimize**.<br>  <br>  | (1) Items marked by red circles are recommended optimization items identified by the system. Select optimization items based on the actual situation.<br><br>(3) Manually optimize the items that cannot be optimized automatically by the system. |

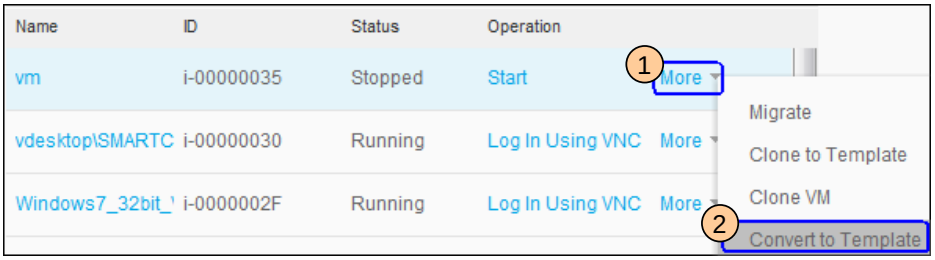
## Step 3: Install the application software.

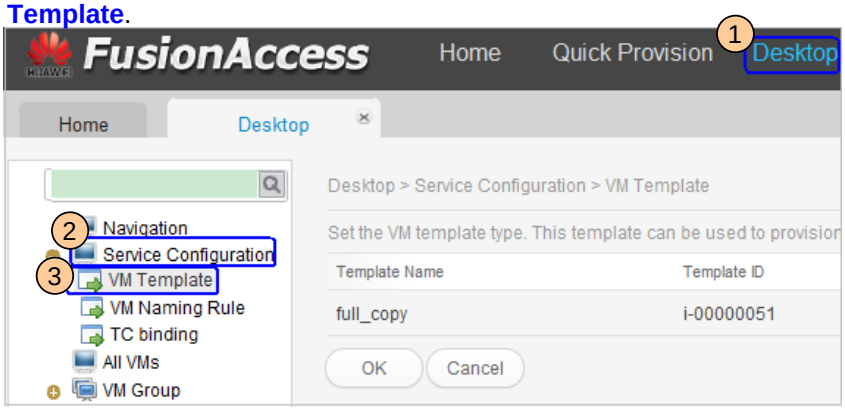
| | |
|---|---|
| 1. Install the application software in **C:** on the template VM. | - |

- **To create a full copy VM, see section 5.4 Creating a Full Copy VM Template.**
- **To create a linked clone VM, see section 5.5 Creating a Linked Clone VM Template.**

## 5.4 Creating a Full Copy VM Template

| **Step 1: Encapsulate the VM OS.** | |
|---|---|
| 1. In the VNC window of the template VM, attach **FusionAccess_Mirror_V100R005C20SPCxxx.iso**. | If the iso file has been mounted, skip this step. |
| 2. In the CD-ROM window on the VM, double-click **run.bat**. | - |
| 3. Encapsulate the OS.<br>  <br><br>  <br><br>  <br><br>  <br> | 1 Select the clone type based on the template type.<br>4<br>**CAUTION**<br>After the encapsulation is successful, do not restart the VM.<br>For details about the application scenarios for the full copy template, see section 1 "Service Provisioning Rules and Application Scenarios." |
| 4. Close the **Desktop Cloud Image Optimization Tool** window. | - |
| 5. Unmount the DVR-ROM drive and shut down the VM. | - |

| Step 2: Convert the VM into a template. | |
|---|---|
| 1. On the FusionCompute portal, choose **VM and Template > VM**. | - |
| 2. Convert the VM into a template.<br>  | You can view the conversion progress on the **Task Center** page. The templates that are converted successfully will be displayed in **Template and Specifications > VM Template**. |

| Step 3: Configure the template on FusionAccess. | |
|---|---|
| 1. Log in to FusionAccess.<br>The address format is *https://service IP address of the ITA server:8448.* | - |
| 2. On FusionAccess, choose **Desktop** > **Service Configuration** > **VM Template**.<br>  | - |
| 3. Configure a full copy VM template.<br>  | 1 Set the type to **Full Copy Template**. |

## 5.5 Creating a Linked Clone VM Template(Optional Task)

### Step 1: Set the login policies for the Users user group.

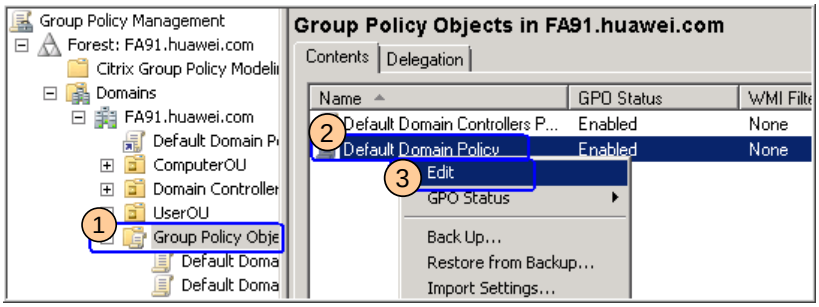
1. On the FusionCompute portal, log in to the active AD server using the VNC.

-

2. In **Search programs and files**, enter **gpmc.msc** and press **Enter** to open the **Group Policy Management** window.

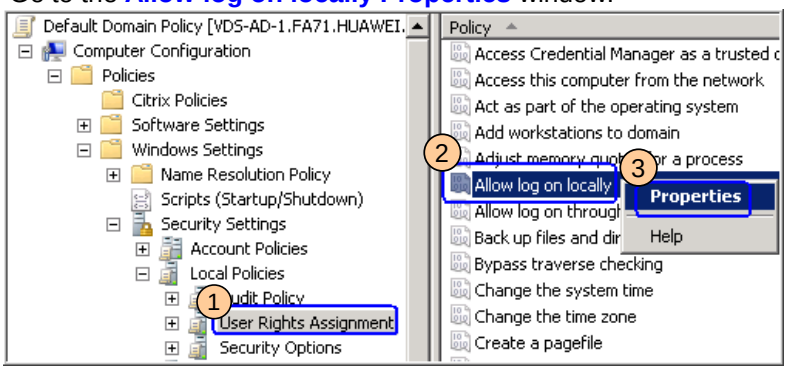
-

3. Go to the **Group Policy Management Editor** window.



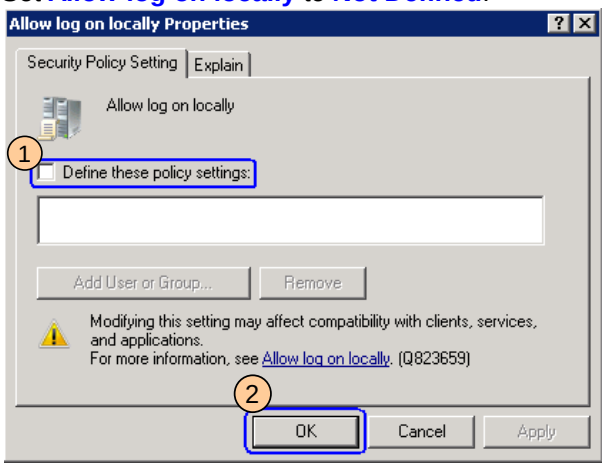

(2) Select the group policy that has taken effect for the user VM. If there is no group policy available, select **Default Domain Policy**.

4. Go to the **Allow log on locally Properties** window.



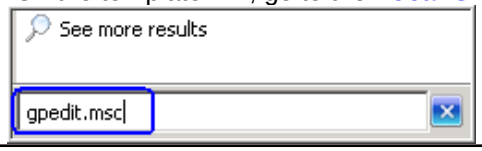

-

5. Set **Allow log on locally** to **Not Defined**.

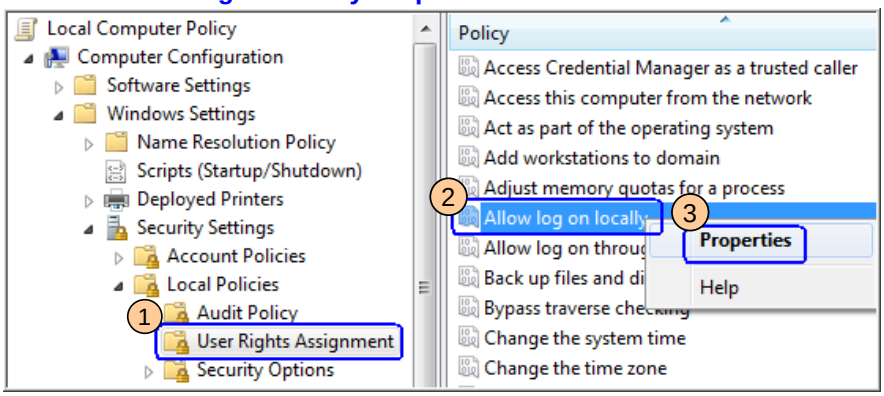
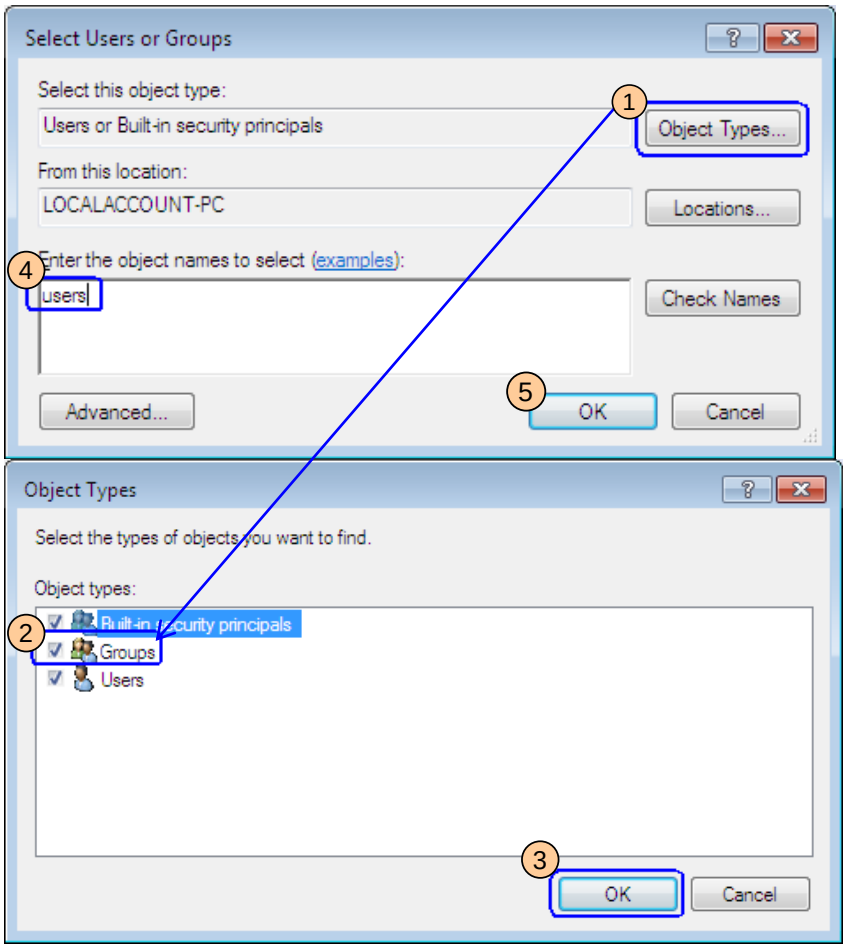


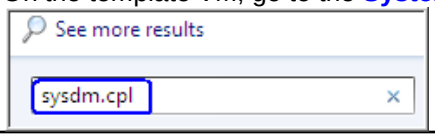
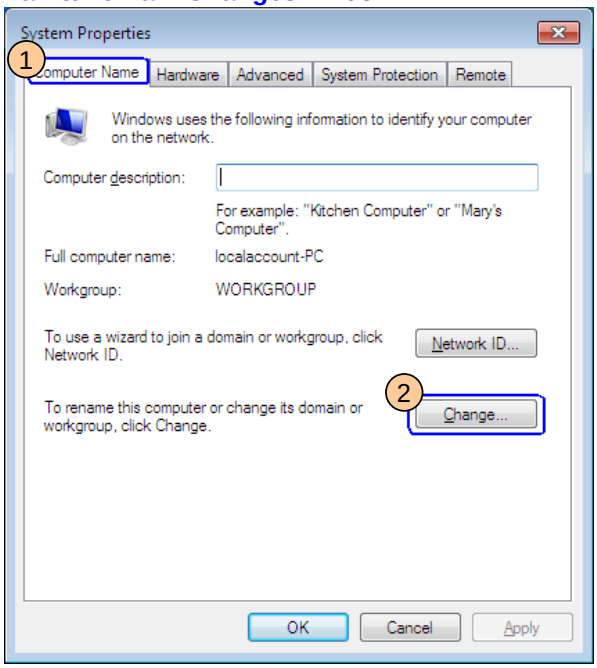
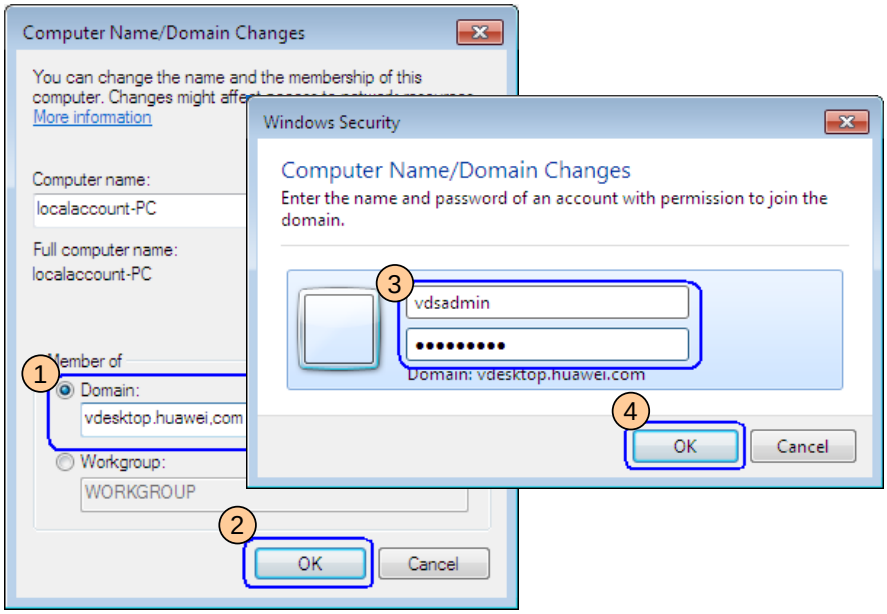

-

6. On the template VM, go to the **Local Group Policy Editor** window.

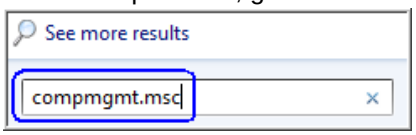
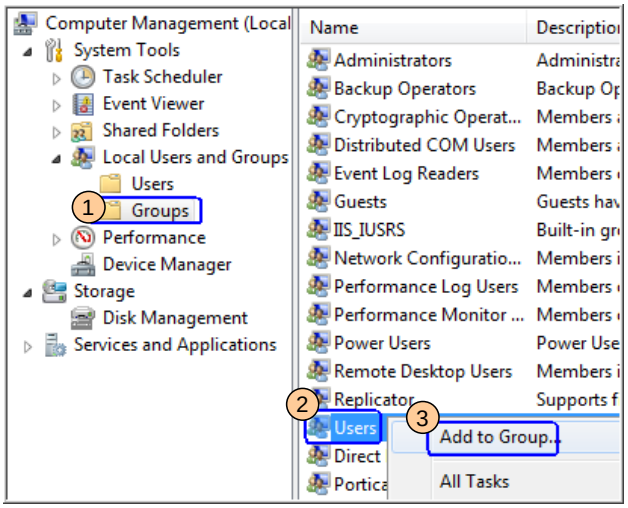
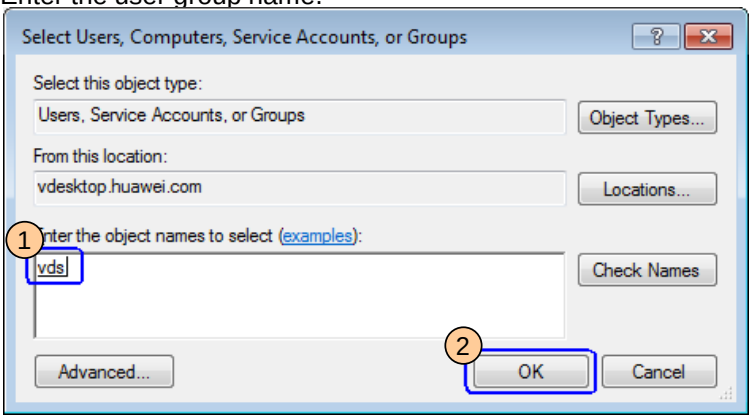
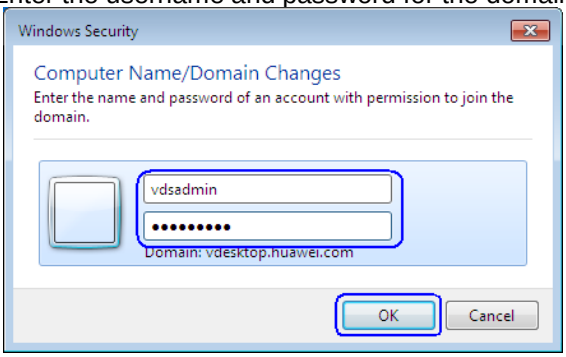


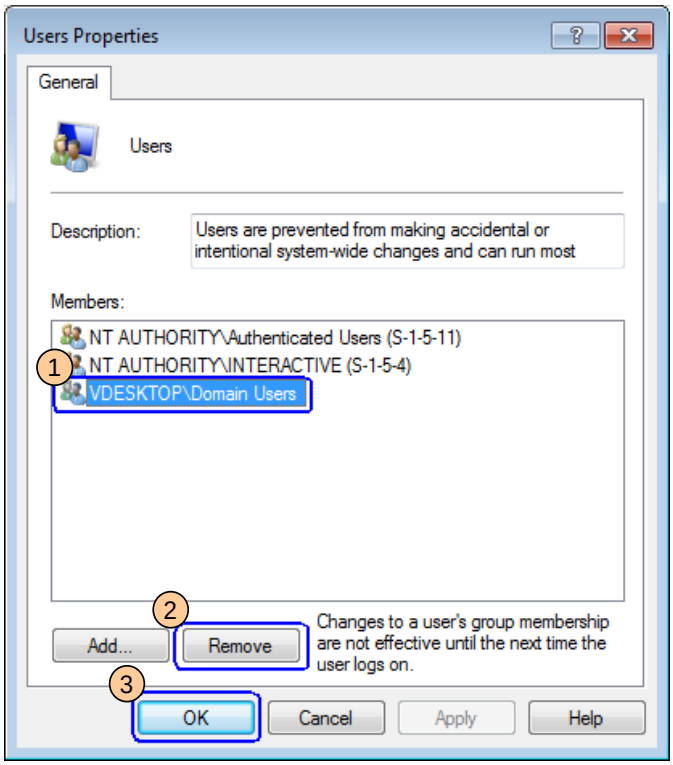

-

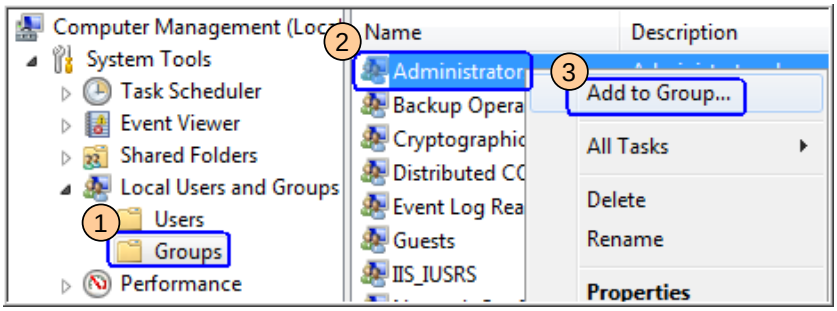
| Step 1: Set the login policies for the Users user group. (cont.) | |
|---|---|
| 7. Go to the **Allow log on locally Properties** window.<br>  | - |
| 8. Click **Add User or Group**. | - |
| 9. Add a group.<br>  | 2 Select **Groups**.<br>4 Enter **Users**. |
| 10. Click **OK**. The **Allow log on locally Properties** window is closed. | - |
| 11. Close the **Local Group Policy Editor** window. | - |

| Step 2: Add the VM to a domain. | |
|---|---|
| 1. On the template VM, go to the **System Properties** window.<br>  | **sysdm.cpl** |
| 2. On the **Computer Name** tab, click **Change**, go to the **Computer Name/Domain Changes** window.<br>  | - |
| 3. Enter the domain information.<br>  | 1 Enter the **Infrastructure domain information** obtained from the **Data Planning Template**. If the **user domain** is planned, enter the **user domain name**.<br><br>3 Enter the username and password for the domain administrator. You can obtain this information from the **Data Planning Template**. |
| 4. Click **OK** twice. The **System Properties** window is closed. | - |
| 5. Click **Restart Now** to restart the VM, and log in to the VM as **Administrator**. | - |

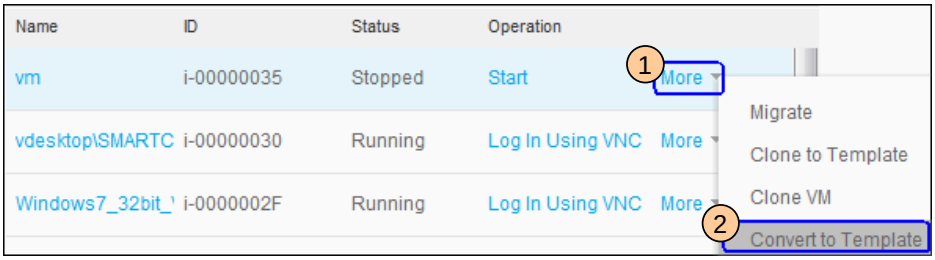
## Step 3: Configure a user group.

| | |
|---|---|
| 1. On the template VM, go to the **Computer Management** window.<br>  | **compmgmt.msc** |
| 2. Select a group.<br>  | 2 When selecting a user group, note the following:<br>•Do not add the user group to the **Guests** group.<br>•You can add the user group to the **Users** group only after the login policy of the **Users** group is configured.<br>•The users in the **Users** group do not have VM administrator rights. |
| 3. Click **Add**. | - |
| 4. Enter the user group name.<br>  | 1 The user group name must be consistent with the user group name added to the user domain on the AD server.<br>After a domain user is created on the AD server later, add the domain user to the user group created in this step. If linked clone VMs are assigned to this user group, the domain users in this group can log in to the linked clone VMs. |
| 5. Enter the username and password for the domain administrator.<br>  | 1 Enter the username and password for the domain administrator. You can obtain this information from the **Data Planning Template**. |

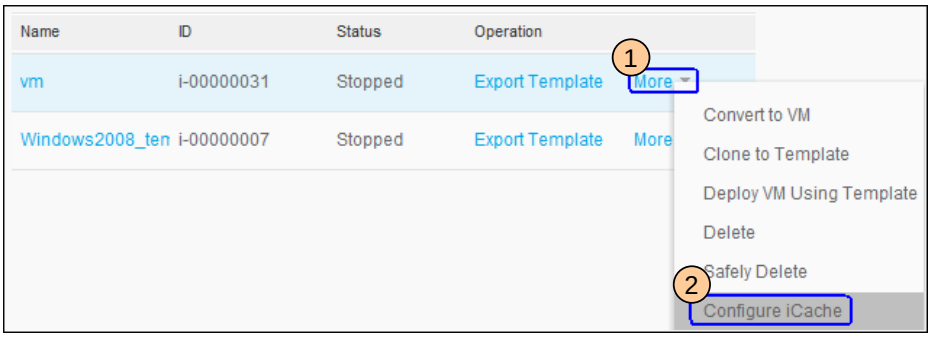
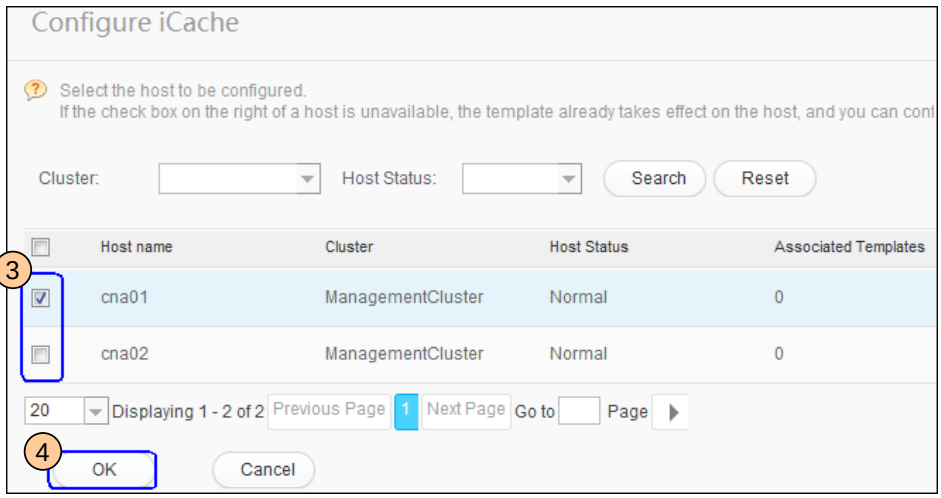
| Step 3: Configure a user group. (cont.) | |
|---|---|
| 6. Delete the **Domain Users** group.<br>  <br> | - |

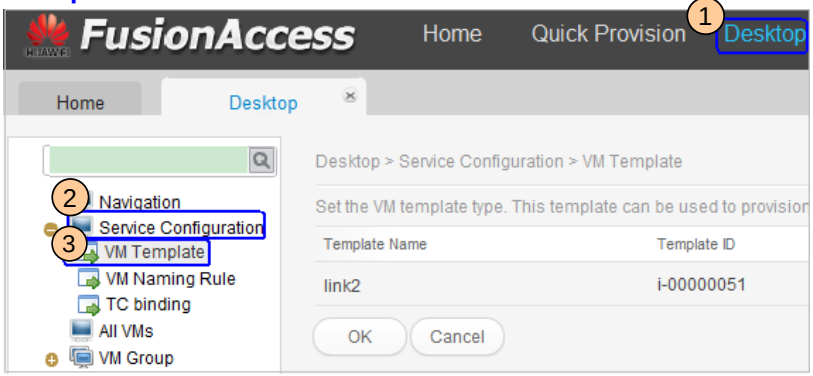
| Step 4: Configure the Administrator group. | |
|---|---|
| 1. Select the **Administrator** group.<br>  <br> | - |
| 2. Add the Tomcat account of the ITA service to the **Administrator** group. | Example: ITAServiceUser |
| 3. Delete the **Domain Admins** group. | See the substep 6 in **Step 3 "Configure a user group."** |
| 4. Shut down the VM. | - |

## Step 5: Convert the VM into a template.

| | |
|---|---|
| 1. On the FusionCompute portal, choose **VM and Template > VM**. | - |
| 2. Convert the VM into a template.<br>  <br> | You can view the conversion progress on the **Task Center** page. The templates that are converted successfully will be displayed in **Template and Specifications > VM Template**. |

## Step 6: On FusionCompute, configure an iCache for the template to improve data access efficiency.

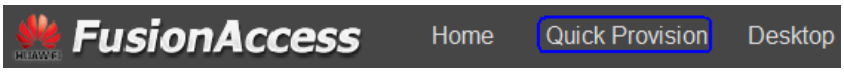
| | |
|---|---|
| 1. On the FusionCompute portal, choose **VM and Template > Template and Specifications**.<br>The **VM Template** page is displayed. | - |
| 2. Configure iCache for the template.<br>  <br><br>  <br> | The template is the one created in substep 2 of **Step 5 "Convert the VM into a template."**<br>3 Select the host to be configured with the iCache. The system automatically selects the host where the template is located.<br>**Note:**<br>• A VM created from a template can use an iCache only after the template is configured with an iCache and the VM runs on a host with an iCache.<br>• The iCache can be configured only when the storage type is NAS, virtual local disks, or LUN Pome.<br>• A template with an iCache can be used to create a maximum of 512 linked clones. |

| Step 7: Configure the template on FusionAccess. | |
|---|---|
| 1. Log in to FusionAccess.<br>The address format is *https://service IP address of the ITA server:8448*. | - |
| 2. On FusionAccess, choose **Desktop** > **Service Configuration** > **VM Template**.<br>  | - |
| 3. Configure a linked clone VM template.<br>  | 1 Set the type to **Link Clone Template**. |

# 6 Provisioning VMs

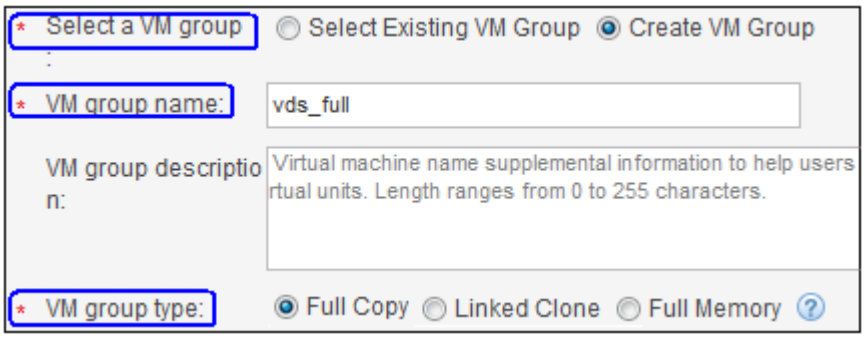
## Step 1: Create a VM.

1. On the FusionAccess portal, choose **Quick Provision**, go to the **Create VM** page.



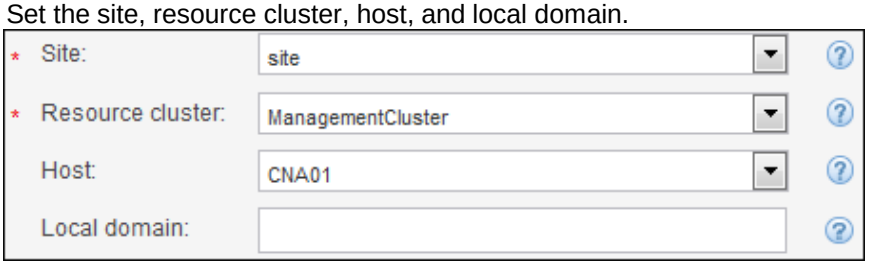

This section describes how to perform quick provisioning of **full copy** VMs.

2. Set VM group information.



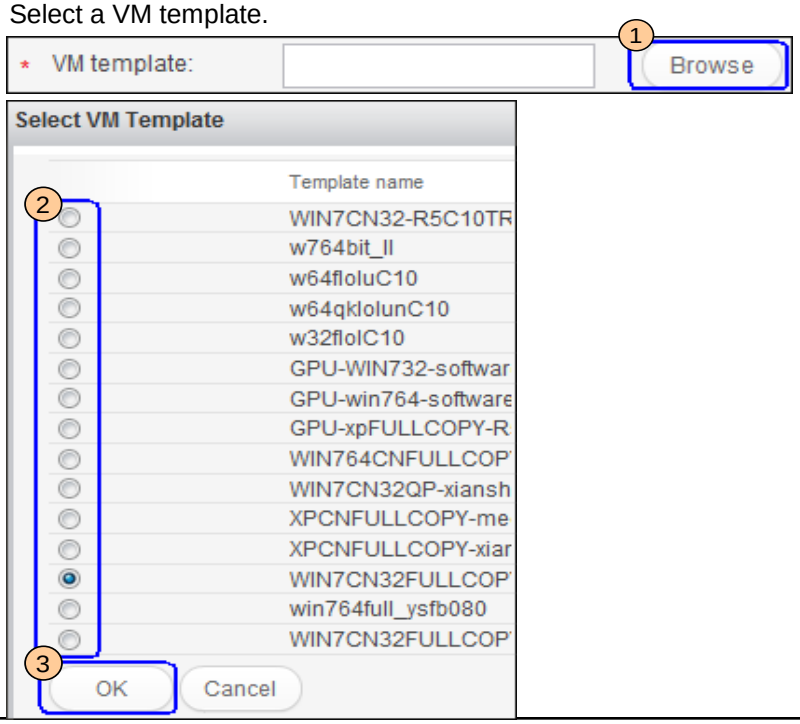

- Select Existing VM Group: Indicates that the VM group is defined previously in **Desktop > VM Group > Create VM Group**.
- Create VM Group: Indicates that you need to specify **VM group name** (D1), **VM group description**, and **VM group type** as planned.

3. Set the site, resource cluster, host, and local domain.



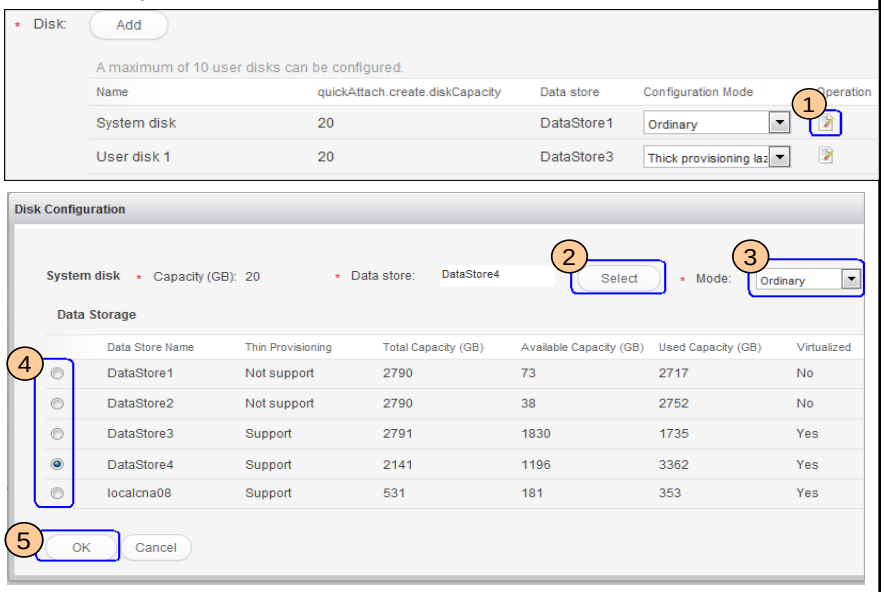
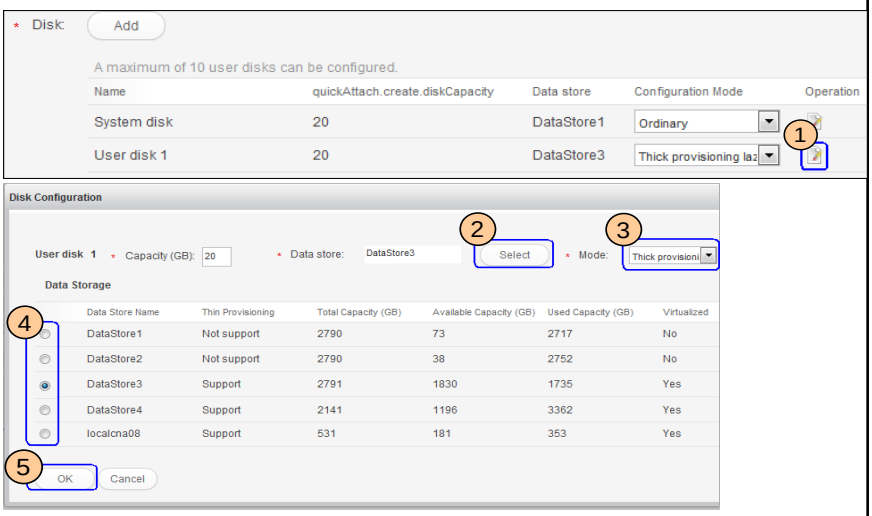

**Local domain** is the domain to which the VM belongs and is configured previously in **System > Rights Management > Role Management**.

4. Select a VM template.



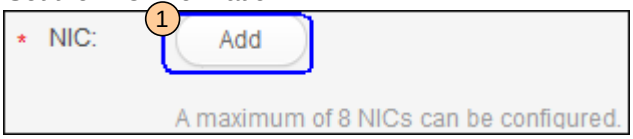

- If you need to provision full copy VMs, select a template of the **fullcopy** type.
- If you need to provision linked clone VMs, select a template of the **clonelink** type.

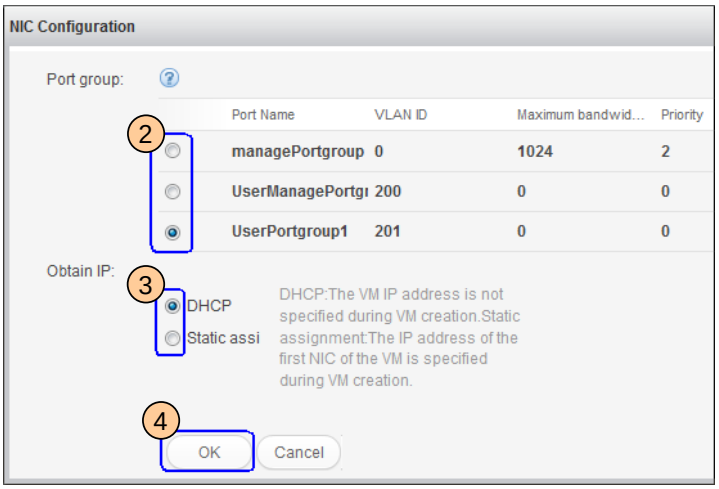
## Step 1: Create a VM.

| | |
|---|---|
| 5. Specify the number of VM CPUs and memory size. | • Number of CPUs: 1 to 32<br>• Memory size: 1024 MB to 524,288 MB |
| 6. Set the system disk information.<br>  <br> | (3) If the disk is created based on the default settings, the values in (2) and (3) are consistent with that on the template. If the user changes the settings in (2), the system automatically sets the value in (3) to the recommended value. Retain the recommended value.<br>• If the VM template is full copy template, and the mode supports the common mode, you are advised to set **Mode** to **Common**.<br>• If the VM template is full copy template, set **Mode** to **Thin provisioning**.<br>• If the data storage type is FusionStorage, set **Mode** to **Thin provisioning**. |
| 7. Set the user disk information.<br>  <br> | (3) If the disk is created based on the default settings, the values in (2) and (3) are consistent with that on the template. If the user changes the settings in (2), the system automatically sets the value in (3) to the recommended value. Retain the recommended value.<br>• If the VM template is full copy template, and the mode supports the Thick provisioning lazy zeroed mode, you are advised to set **Mode** to **Thick provisioning lazy zeroed**.<br>• If the VM template is full copy template, you are advised to set **Mode** to **Thin provisioning**.<br>• If the data storage type is FusionStorage, you are advised to set **Mode** to **Thin provisioning**. |
| 8. Add user disks.<br>  <br> | Perform this step when you need to add multiple user disks. Set the user disk information in the displayed dialog box by referring to step 7. |

## Step 1: Create a VM.

9. Set the NIC information.



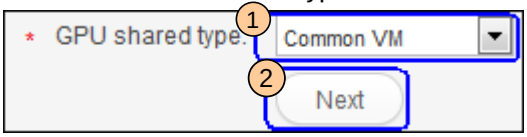




2 Select the port group of the service plane. Port groups for the NICs on the same VM must be different.

10. Specify the number of VMs to be created.

-

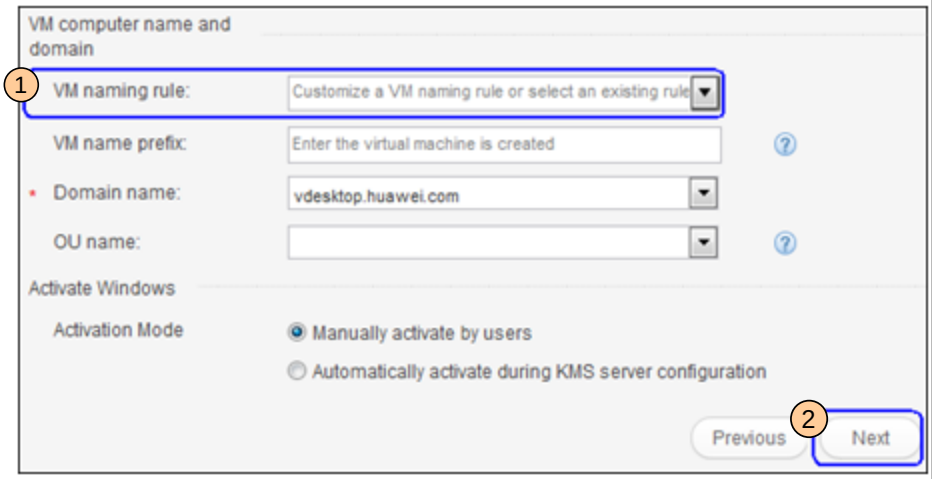
11. Select the GPU shared type.




Select the **GPU shared type** only when you need to provision full copy VMs.

## Step 2: Specify VM parameters.

1. Set the VM computer name and domain.



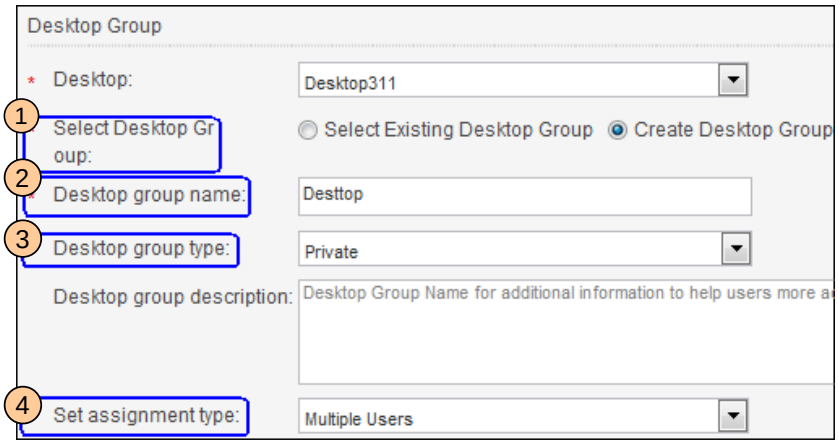

1 You can define or select **VM naming rule (D2)** from the drop-down list. VM naming rule=**Prefix** + **Number of digits**

- **The prefix** contains **a-z, A-Z, 0-9, and hyphen (-)**.
- **Number of digits** contains one or multiple number signs (#).

The naming rule is defined previously in **Desktop > Service Configuration > VM Naming Rule**.

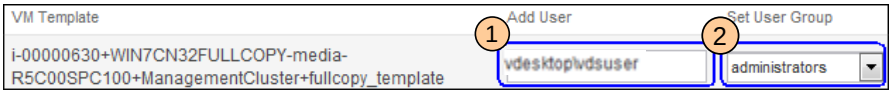
## Step 3: Assign desktops.

1. Configure the desktop group information.




- Select Existing Desktop Group: Indicates that the desktop group is defined previously in **Desktop > Desktop Group > Create Desktop Group**.
- Create Desktop Group: Indicates that you need to specify **Desktop group type** (D3), **Desktop group description**, and **Desktop group type** as planned.
- Specify **Set assignment type** when you need to provision full copy VMs.

2. Provision VMs.




Provision **a full copy VM:**

1 The user created in 4 Creating a VM User. You can find the user name on the AD server.

2 is set to **administrators**.

Provision a **linked clone** VM:

1 The user group created in 4 Creating a VM User. You can find the user group name on the AD server.

2 is set to **users**.

3. Click **Next**. After checking the VM information, click **Submit**.

-

# 7 Other Service Provisioning Methods

For details about service provisioning, see the *FusionCloud Desktop (Standard) V100R005C20 Virtual Desktop Management Guide.* The following tasks are described:

- Provisioning VMs running Windows XP, Windows 8.1, Windows Server 2012 R2 or Windows Server 2008 R2 to users who have **Administrator** rights.
- Provisioning VMs running Windows XP, Windows 7, Windows 8.1, Windows Server 2012 R2 or Windows Server 2008 R2 to users who have **Users** rights.
- Creating VMs from other types of templates and provision the created VMs.