Huawei Cloud Certification Training

HCIA-Cloud Computing

Lab Guide (Basic Exercises)

ISSUE: 5.0

HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2022. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions

HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base Bantian, Longgang Shenzhen 518129 People's Republic of China

Website: https://e.huawei.com

Huawei Certification System

The Huawei certification system is a platform for shared growth, part of a thriving partner ecosystem. There are two types of certification: one for ICT architectures and applications, and one for cloud services and platforms. There are three levels of certification available:

Huawei Certified ICT Associate (HCIA)

Huawei Certified ICT Professional (HCIP)

Huawei Certified ICT Expert (HCIE)

Huawei certification courses cover the entire ICT domain, with a focus on how today's architecture generates cloud-pipe-device synergy. The courses present the latest developments of all essential ICT aspects to foster a thriving ICT talent ecosystem for the digital age.

HCIA-Cloud Computing V5.0 is intended for beginners. Focusing on the virtualization technologies and FusionAccess of Huawei, this course aims to help you learn the basics of cloud computing and resource pooling, and to cultivate cloud computing engineers that are capable of using FusionCompute for virtualization and managing FusionAccess.

The HCIA-Cloud Computing V5.0 certification includes the following courses: basics of cloud computing (server, storage, network, and OS), overview of FusionCompute, routine management and troubleshooting of virtualization resource pools, overview of FusionAccess and related components, as well as their installation, deployment, service management, and troubleshooting.

Passing the HCIA-Cloud Computing V5.0 certification means that you are capable of designing, managing, and maintaining FusionCompute and FusionAccess.

Huawei Certification
Cloud Service & Platform
HarmonyOS
IoT
GaussDB
openGauss
openEuler
Big Data
Kunpeng Application Developer
MDC
AI
Cloud
ICT Infrastructure
Storage
Intelligent Computing
Enterprise Communication
Intelligent Vision
Data Center
Datacom
WLAN
Security
SDN
Transmission
Access
LTE
5G
HCIE
Huawei Certified ICT Expert
HCIP
Huawei Certified ICT Professional
HCIA
Huawei Certified ICT Associate

About This Document

Overview

This course is specific to HCIA-Cloud Computing certification. It is intended for those who are preparing for HCIA-Cloud Computing certification or want to understand basic configurations of storage, networks, Linux, and KVM virtualization.

About the Exercises

This document consists of four exercises:

- Exercise 1: Basic storage configuration. Simulate a storage service scenario. Use the Huawei OceanStor eStor storage emulator to create volumes and map the volumes to service hosts to mount LUNs. This exercise helps trainees master the basic configuration logic of SAN storage.
- Exercise 2: Basic network configuration, including the switch view introduction, basic switch configuration, as well as VLAN and routing principle implementation. This exercise helps trainees master the basic usage of switches and basic principles of Layer 2 and Layer 3 network communication from multiple perspectives.
- Exercise 3: Linux basics, including the bash commands, file viewing commands, basic operations on the text editor, and Linux service management. This exercise helps trainees master the basic usage of the Linux operating system.
- Exercise 4: KVM virtualization, including creating VMs using KVM virtualization, managing networks, configuring bridging, and configuring NAT networks. This exercise helps trainees deepen their understanding of KVM virtualization principles and master the basic principles of communication between VMs and external networks.

Account List

Product documentation: FusionCompute OceanStor eStor Installation Guide.

Table 1-1 Account list

Item	Username	Password
OceanStor eStor	admin	For details, see "Deploying eStor" in *FusionCompute OceanStor eStor Installation Guide*.

Lab Environment Setup

Checking Devices

Make sure that all required software tools are ready before the exercises. The following table lists the devices.

Table 1-2 Software and tools

Software	Used For	Description
FusionCompute_OceanStor_eStor_V1R1C00T32_single_controller.zip	Storage configuration exercise	One for each group
FusionCompute 8.1.1	Storage configuration exercise	Shared by all groups
eNSP V100R003C00SPC100	Network configuration exercise	One for each person
VirtualBox 6.1.34	Linux/KVM virtualization exercise	One for each person
openEuler-22.03-LTS-x86_64-dvd	Linux/KVM virtualization exercise	/

Contents

About This Document 3
Overview 3
About the Exercises 3
Account List 3
Lab Environment Setup 4
1 Storage Exercise 7
1.1 Overview 7
1.1.1 About This Exercise 7
1.1.2 Objectives 7
1.1.3 IP Address Planning 7
1.1.4 Guideline 7
1.2 Configuration Procedure 8
1.2.1 Deploying OceanStor eStor 8
1.2.2 Initializing OceanStor eStor 11
1.2.3 Deploying a Service Host 14
1.2.4 Creating a Host and a Host Group 17
1.2.5 Creating a LUN, LUN Group, and Mapping View 21
1.2.6 Lab Verification 22
1.3 Quiz 23
2 Network Configuration Exercise 24
2.1 Introduction to the Switch View 24
2.1.1 Overview 24
2.1.2 Configuration Procedure 24
2.2 Basic Switch Configuration 27
2.2.1 Overview 27
2.2.2 Configuration Procedure 28
2.3 VLAN Implementation Exercise 32
2.3.1 Overview 32
2.3.2 Configuration Procedure 33
2.4 Routing Implementation Exercise 39
2.4.1 Overview 39
2.4.2 Configuration Procedure 40
2.5 Quiz 46
3 Linux Exercise 47

3.1 Overview 47
3.1.1 About This Exercise 47
3.1.2 Objectives 47
3.2 Preparations 47
3.2.1 Creating a VM 47
3.2.2 Installing an OS on the VM 50
3.3 Useful Commands 56
3.3.1 help 56
3.3.2 Other Common Commands 57
3.4 bash Commands 58
3.4.1 Power Supply Control and User Switching 58
3.4.2 Basic Directory and File Operations 58
3.5 File Viewing Commands 61
3.5.1 Viewing Files 61
3.5.2 (Optional) Searching for Files 64
3.6 Basic Operations on the Vim Text Editor 65
3.6.1 Normal Mode of Vim 65
3.6.2 Insert Mode of Vim 69
3.6.3 Command Line Mode of Vim 72
3.7 openEuler System and User Management 74
3.7.1 Network Management 74
3.7.2 Service Management 78
3.7.3 User Management 79
3.8 Quiz 81
4 KVM Installation and Resources Provisioning 82
4.1 Overview 82
4.1.1 About This Exercise 82
4.1.2 Objectives 82
4.1.3 Lab Networking 82
4.1.4 Exercise Planning 84
4.2 Exercise Configuration 84
4.2.1 Guideline 84
4.2.2 Procedure 85
4.3 Quiz 105

1 Storage Exercise

1.1 Overview

1.1.1 About This Exercise

This exercise describes how to create and map Huawei SAN storage resources to help trainees deepen their understanding of Huawei SAN storage concepts and service processes.

1.1.2 Objectives

- Understand the concepts of disk domains and storage pools of Huawei storage devices.
- Be familiar with the concepts and configurations of Huawei storage devices, such as hosts, host groups, LUNs, LUN groups, and mapping views.
- Understand the process and method of configuring Huawei SAN storage services.

1.1.3 IP Address Planning

Table 1-1 IP address planning for the exercise

NE	Interface	IP Address
Service host	Host interface	192.168.32.41/24
OceanStor eStor	Management interface	192.168.32.40/24
	Service interface	192.168.32.42/24

1.1.4 Guideline

1. Deploy and initialize OceanStor eStor.
2. Deploy service hosts.
3. Configure hosts and host groups.
4. Configure LUNs and LUN groups.
5. Create a mapping view and log in to the host to verify mounting.

1.2 Configuration Procedure

1.2.1 Deploying OceanStor eStor

Step 1 Log in to FusionCompute using the provided login information. Choose **Resource Pools** > **Create VM** > **Deploy VM Using Template**.

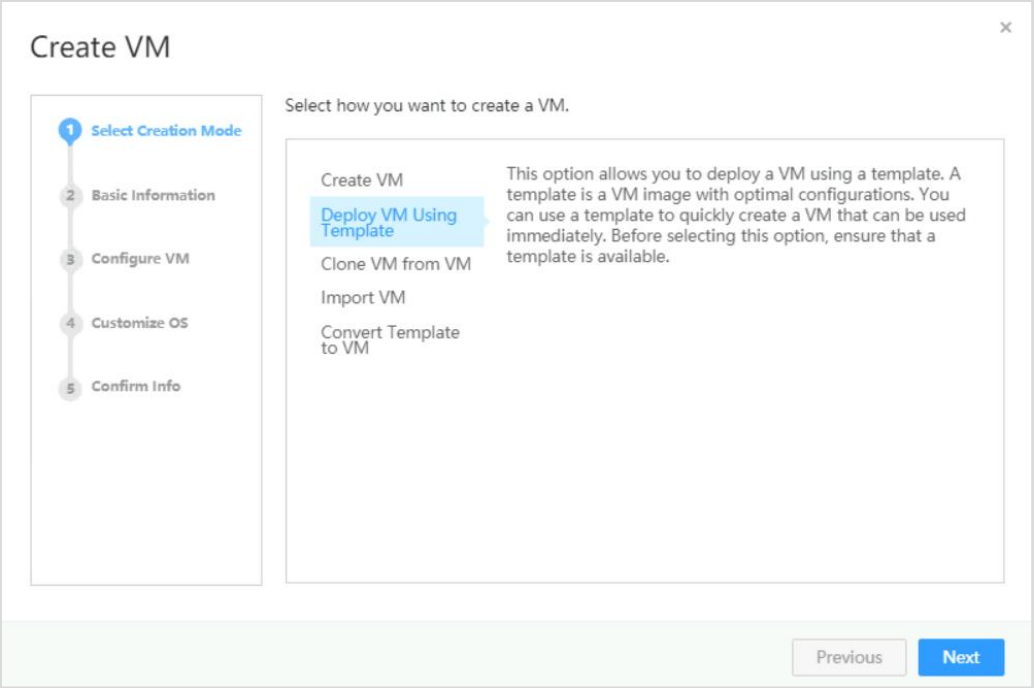


Figure 1-1 Selecting a creation mode

Step 2 Set the VM name, select the **estor** template created by the trainer, and click **Next**.

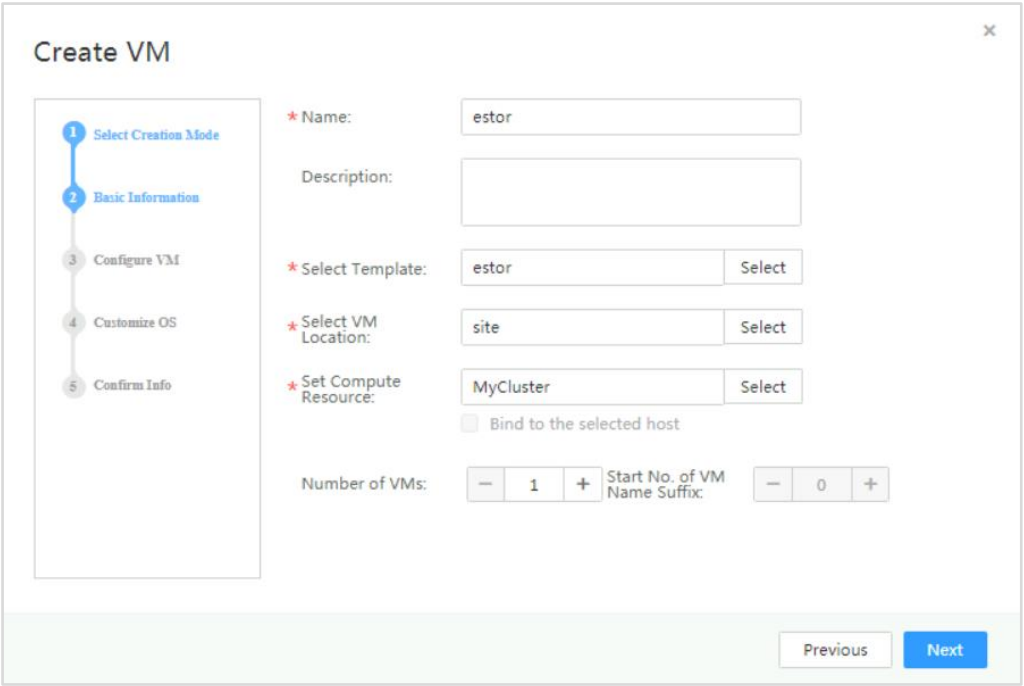


Figure 1-2 Basic settings

Step 3 Retain the default VM configuration and click **Next**.

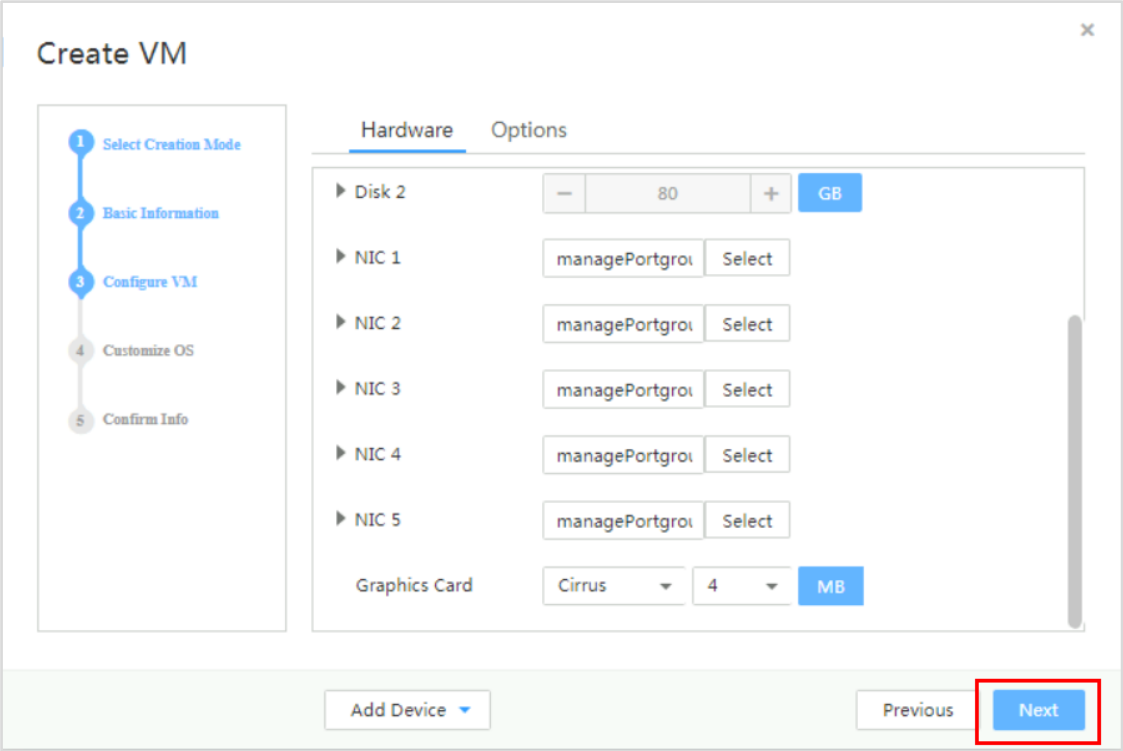


Figure 1-3 VM configuration

Step 4 Deselect **Generate Initial Password** and click **Next**.

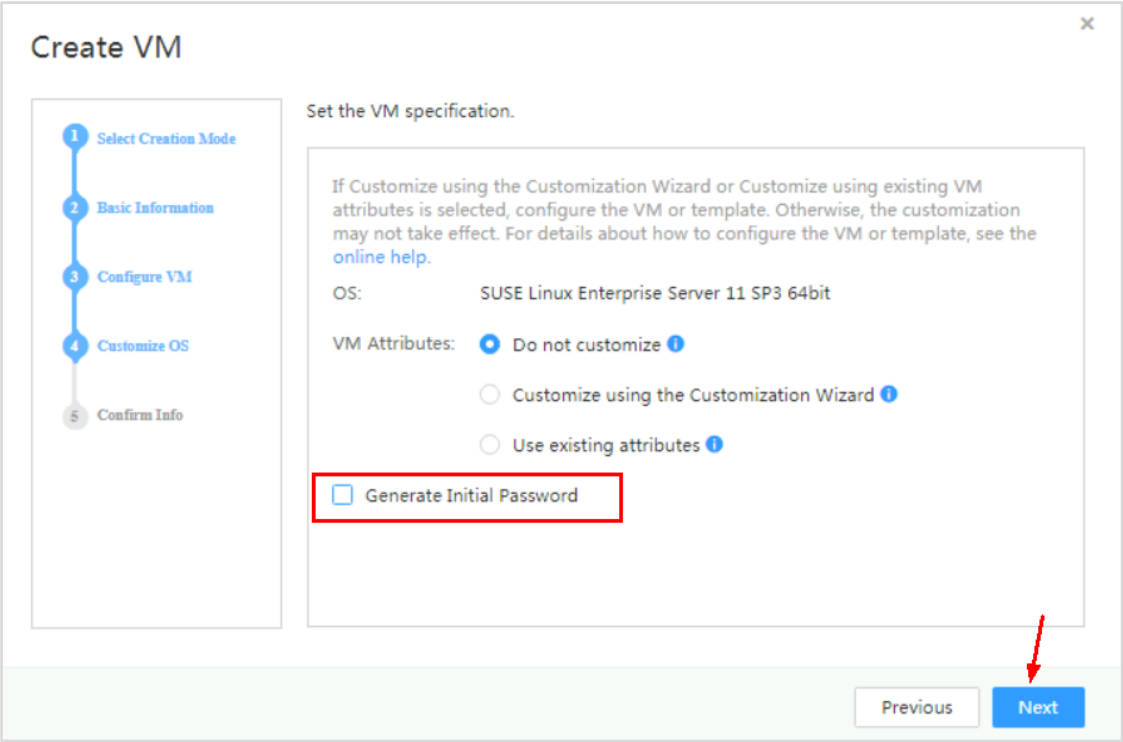


Figure 1-4 Selecting VM specifications

Step 5 Select **Start VM immediately after creation** and click **OK**.

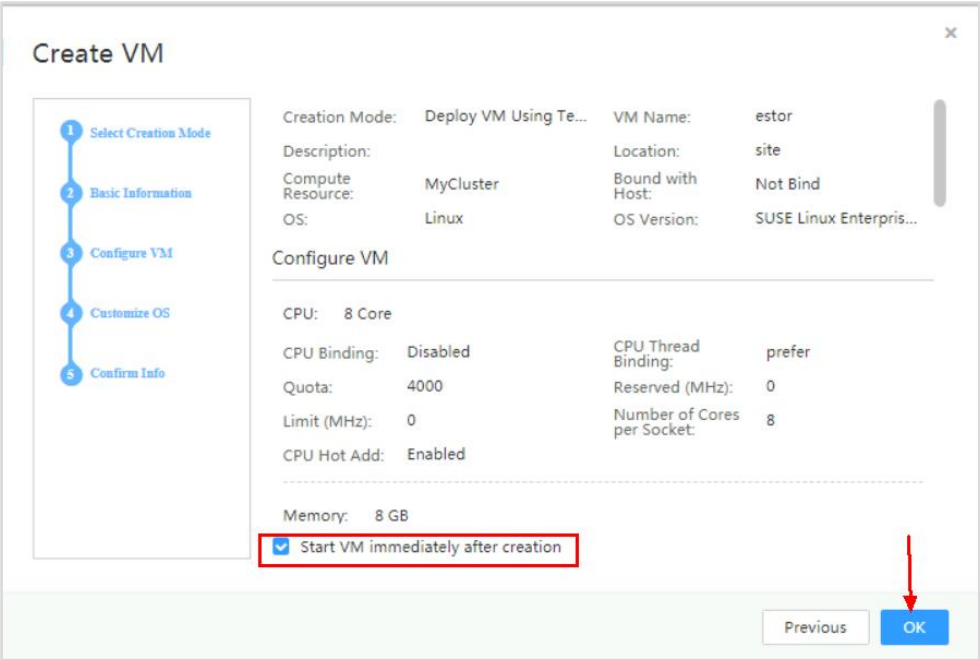


Figure 1-5 Confirming information and creating a VM

Step 6 Log in to the **estor** VM and configure basic information.

- Select the **estor** VM and click **Log In Using VNC** on the **Summary** page.

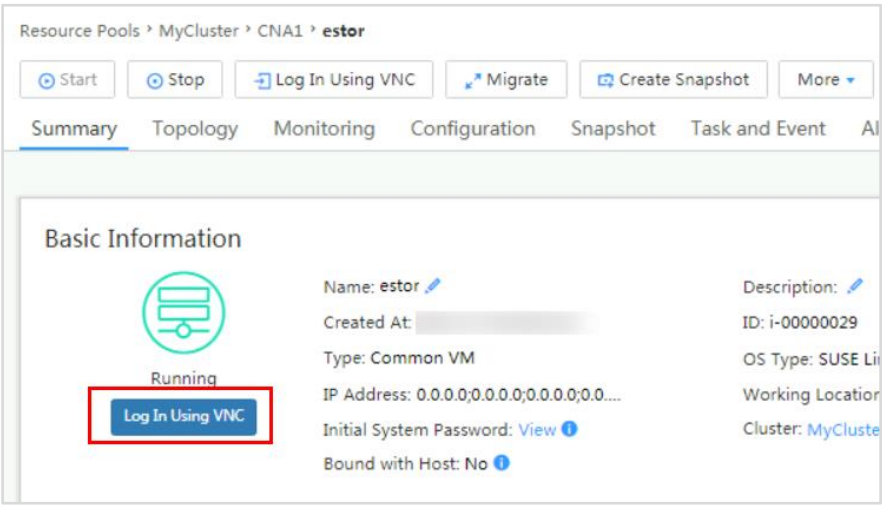


Figure 1-6 Summary page

- Enter the IP address, subnet mask, and gateway of the controller in sequence. Enter the last two digits of the product SN, for example, **01**, and enter **yes**.

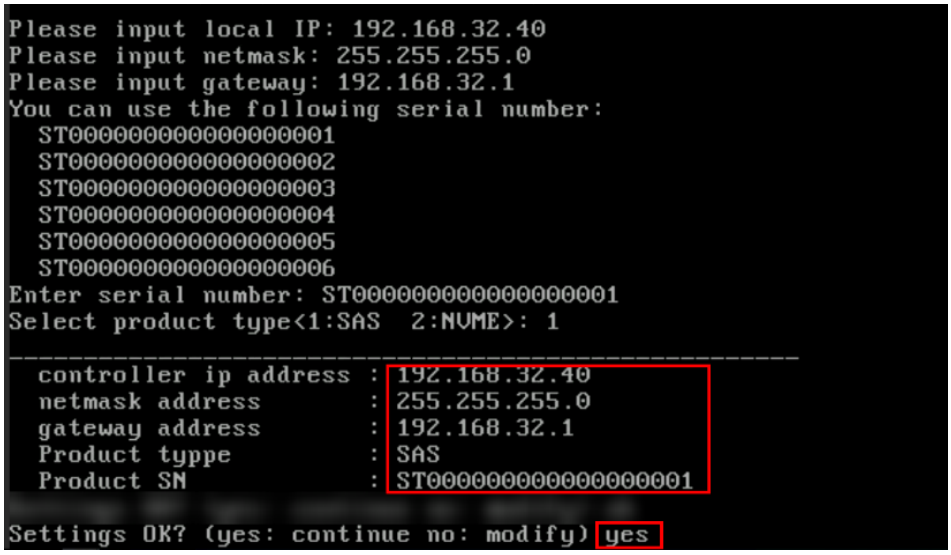


Figure 1-7 Initial configuration of OceanStor eStor

- After the configuration is complete, wait 5 to 8 minutes for OceanStor eStor to start.

1.2.2 Initializing OceanStor eStor

Step 1 Enter **https://*X.X.X.X*:8088** (replace *X.X.X.X* with the controller address) to open the OceanStor eStor login page. Enter the user name and password to log in.

#For details about the user name and password, see the Account List.

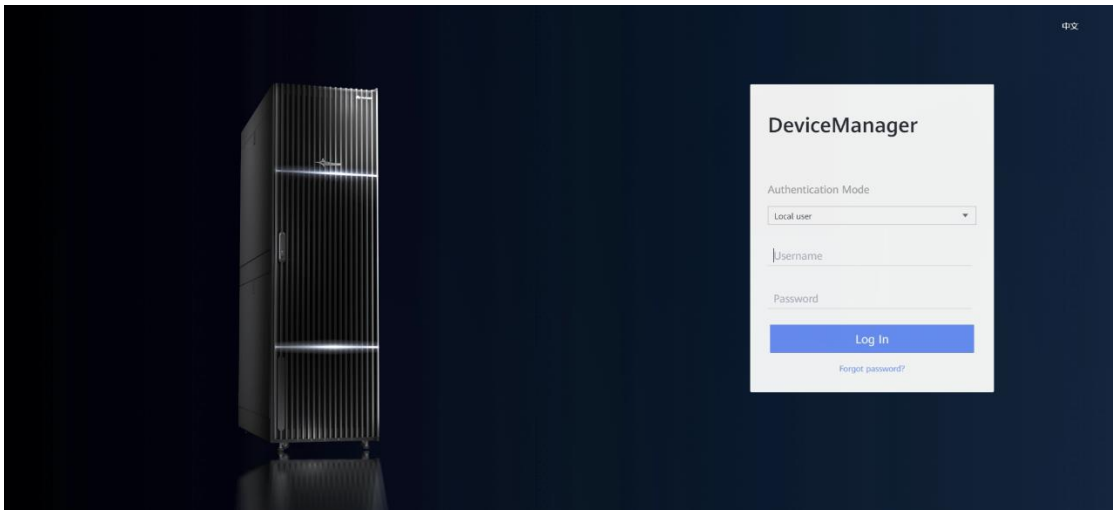


Figure 1-8 Logging in to OceanStor eStor

- Enter the user name and password, change the password as prompted, log in to the device, and perform initial configuration.

Step 2 Perform initial configuration of OceanStor eStor.

- Configure basic information.

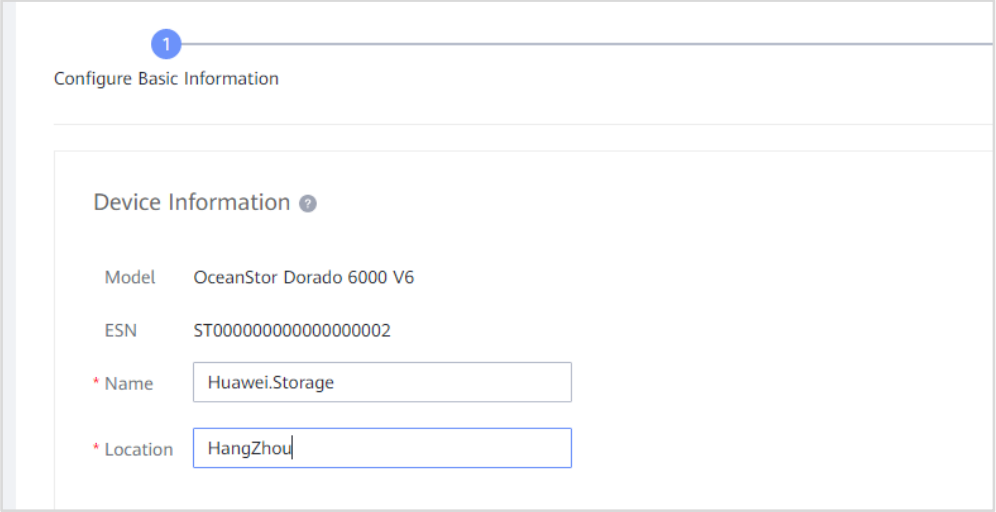


Figure 1-9 Initial configuration of OceanStor eStor

- On the **License Management** page, click **Import License** if you have not imported a license before. Otherwise, click **Update License**.

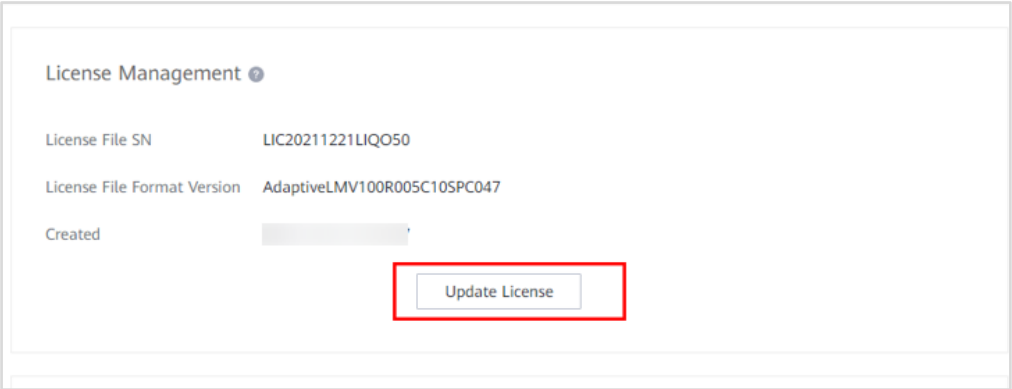


Figure 1-10 Updating a license

- On the page that is displayed, click **...** next to **License File**, select the local license file prepared by the trainer, and click **Upload**.

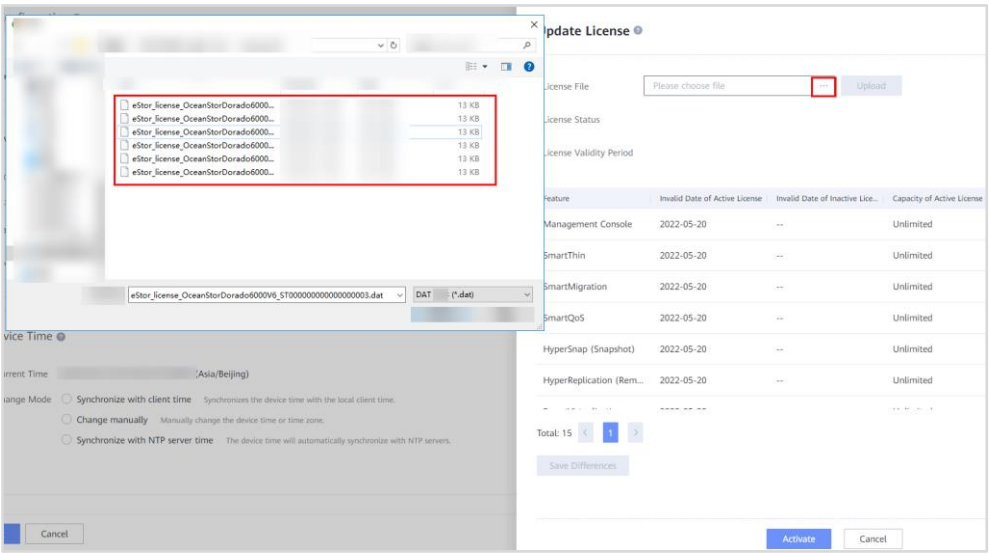


Figure 1-11 Updating a license

- Click **Next**.

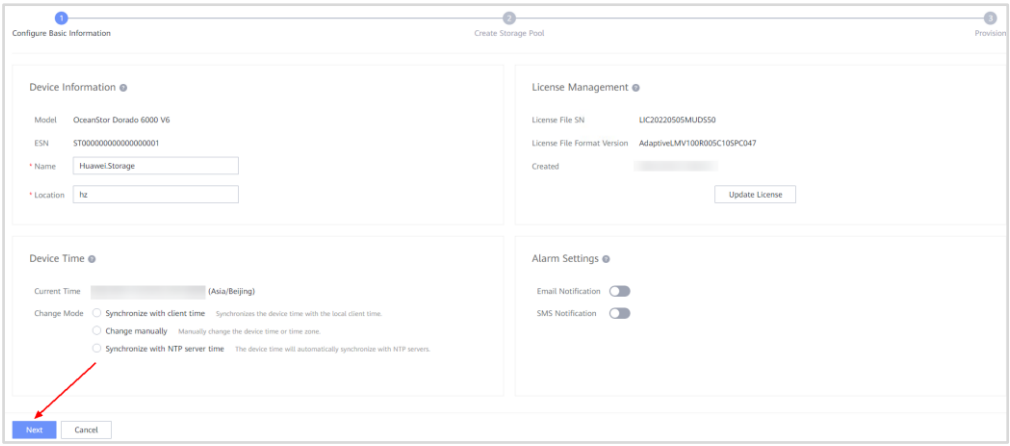


Figure 1-12 License management

- Create a storage pool and set the number of disks and RAID policy (retain the default settings in this example). Then click **Next**.

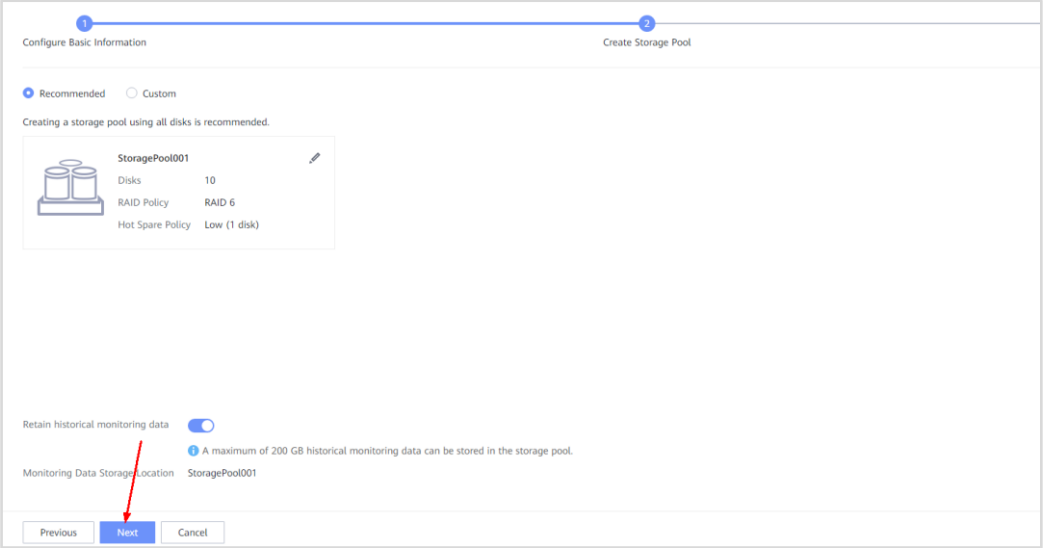


Figure 1-13 Storage pool configuration

- Retain the default settings on the **Provision** page and click **Finish**.

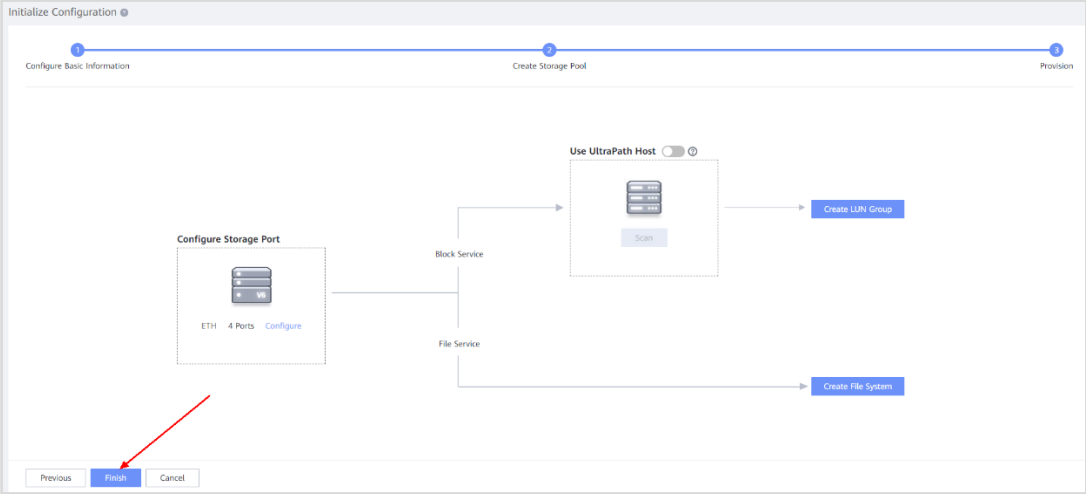


Figure 1-14 Resource provisioning

- Configure an IP address for the OceanStor eStor service interface.

On the **System** page, choose **Hardware** > **Ports**. Click the corresponding Ethernet port and configure the IP address according to the trainer's IP address plan. In this example, the IP address of the service interface is 192.168.32.42/24.

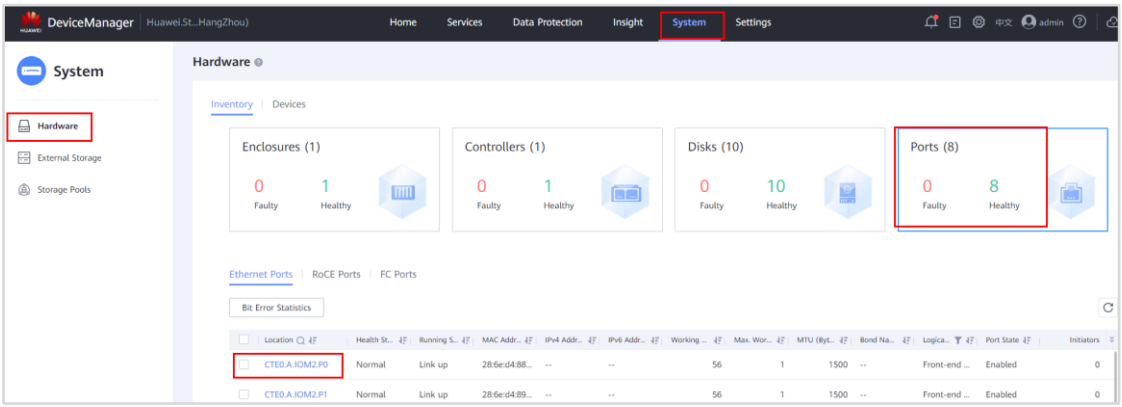


Figure 1-15 System hardware overview

1.2.3 Deploying a Service Host

Step 1 Create a service host.

- Log in to FusionCompute, click **Create VM**, and select **Import Template**. Select the CentOS 7.6 template file (prepared by the trainer) on the jump server and click **Next**.

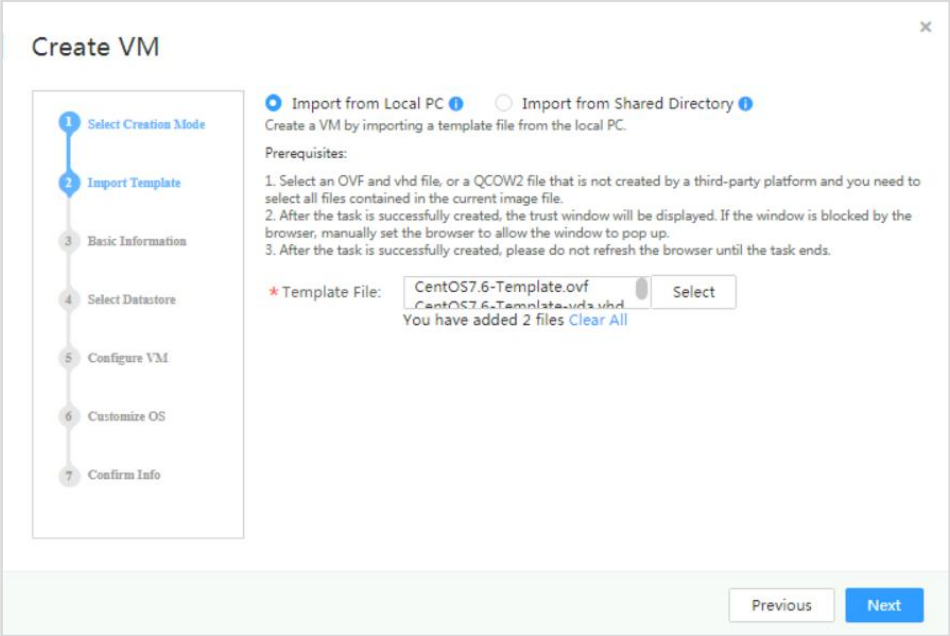


Figure 1-16 Creating a VM using a template

- On the **Basic Information** page, enter the name and select the compute resource.

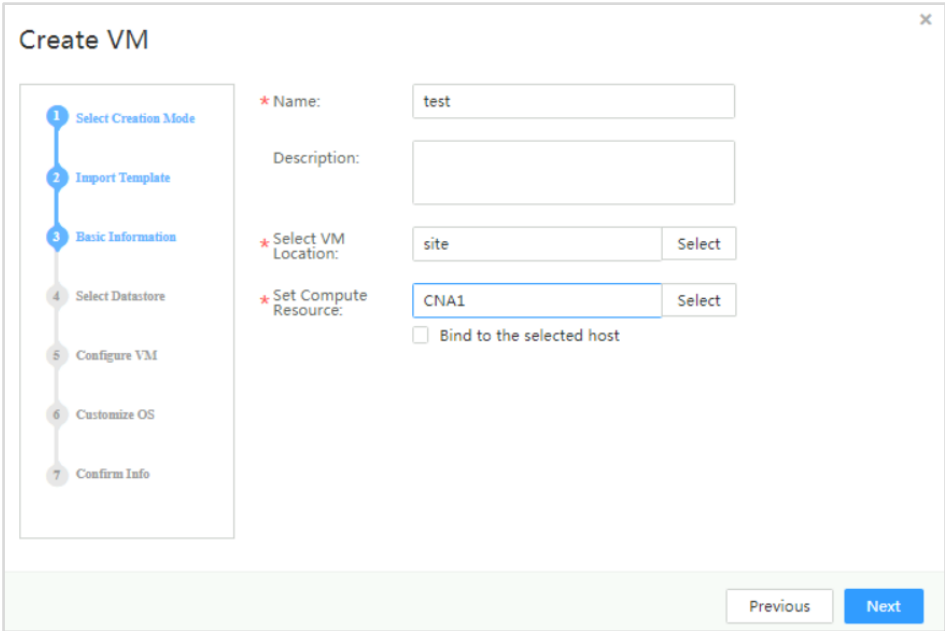


Figure 1-17 Basic information

- Ensure that the port group of the VM is the same as that of the eStor VM. For the configuration of other steps, see the eStor VM creation process. Click **OK**.

Step 2 Configure the IP address and iSCSI information of the service host.

- Log in to the VM using VNC and configure the IP address of the service host based on the IP address plan.

```
localhost login: root
Password:
Last login:
[root@localhost ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 28:6e:d4:88:c8:c7  txqueuelen 1000  (Ethernet)
        RX packets 62  bytes 4208 (4.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 72  bytes 6408 (6.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 72  bytes 6408 (6.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

virbr0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 192.168.122.1  netmask 255.255.255.0  broadcast 192.168.122.255
        ether 52:54:00:59:62:13  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@localhost ~]# vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

Figure 1-18 Configuration of the VM IP address

- After the configuration is complete, restart the network service and check the port IP address again.

```
[root@localhost ~]# systemctl  restart network
[root@localhost ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.32.41  netmask 255.255.255.0  broadcast 192.168.32.255
        inet6 fe80::fb69:7372:93f7:ce49  prefixlen 64  scopeid 0x20<link>
        ether 28:6e:d4:88:c8:c7  txqueuelen 1000  (Ethernet)
        RX packets 303  bytes 46258 (45.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 76  bytes 12245 (11.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure 1-19 Restarting the network service

- Test the connectivity with the OceanStor eStor management or service interface.

```
[root@localhost ~]# ping 192.168.32.40
PING 192.168.32.40 (192.168.32.40) 56(84) bytes of data.
64 bytes from 192.168.32.40: icmp_seq=1 ttl=64 time=0.601 ms
64 bytes from 192.168.32.40: icmp_seq=2 ttl=64 time=0.182 ms
64 bytes from 192.168.32.40: icmp_seq=3 ttl=64 time=0.201 ms
64 bytes from 192.168.32.40: icmp_seq=4 ttl=64 time=0.165 ms
^C
```

Figure 1-20 Testing connectivity with the management interface

- Change the iSCSI initiator name and connect to the storage device.

Run the following command to change the iSCSI initiator name:

```
[root@localhost ~]# vi /etc/iscsi/initiatorname.iscsi
```

```
[root@localhost ~]# vi /etc/iscsi/initiatorname.iscsi
```

Figure 1-21 Changing the iSCSI initiator name

Run the following commands to check the initiator name and restart the service:

```
[root@localhost iscsi]# cat initiatorname.iscsi
[root@localhost iscsi]# systemctl restart iscsi
```

```
[root@localhost iscsi]# cat initiatorname.iscsi
InitiatorName=iqn.20[redacted].hcia
[root@localhost ~]# systemctl  restart iscsi
[root@localhost ~]#
```

Figure 1-22 Modifying the iSCSI initiator and restarting the service

Run the following commands to connect to the storage device:

```
[root@localhost iscsi]# iscsiadm –m discovery –t st –p 192.168.32.42
[root@localhost iscsi]# iscsiadm –m node –l
```

```
[root@localhost ~]# iscsiadm  -m discovery -t st -p 192.168.32.42
192.168.32.42:3260,513 iqn.[redacted].com.example::2100020000040506::20200:192.168.32.42
[root@localhost ~]# iscsiadm -m node -l
Logging in to [iface: default, target: iqn.[redacted].com.example::2100020000040506::20200:192.168.32.42, portal: 192.168.32.42,326
0] (multiple)
Login to [iface: default, target: iqn.2014-08.com.example::2100020000040506::20200:192.168.32.42, portal: 192.168.32.42,3260] su
ccessful.
[root@localhost ~]# _
```

Figure 1-23 Connecting to the storage device

1.2.4 Creating a Host and a Host Group

Step 1 Enter **https://*X.X.X.X*:8088** (replace *X.X.X.X* with the controller address) to open the OceanStor eStor login page. Enter the user name and password to log in.

Step 2 In the service list, select **Host Groups**, click **Hosts** on the right, and choose **Create**.

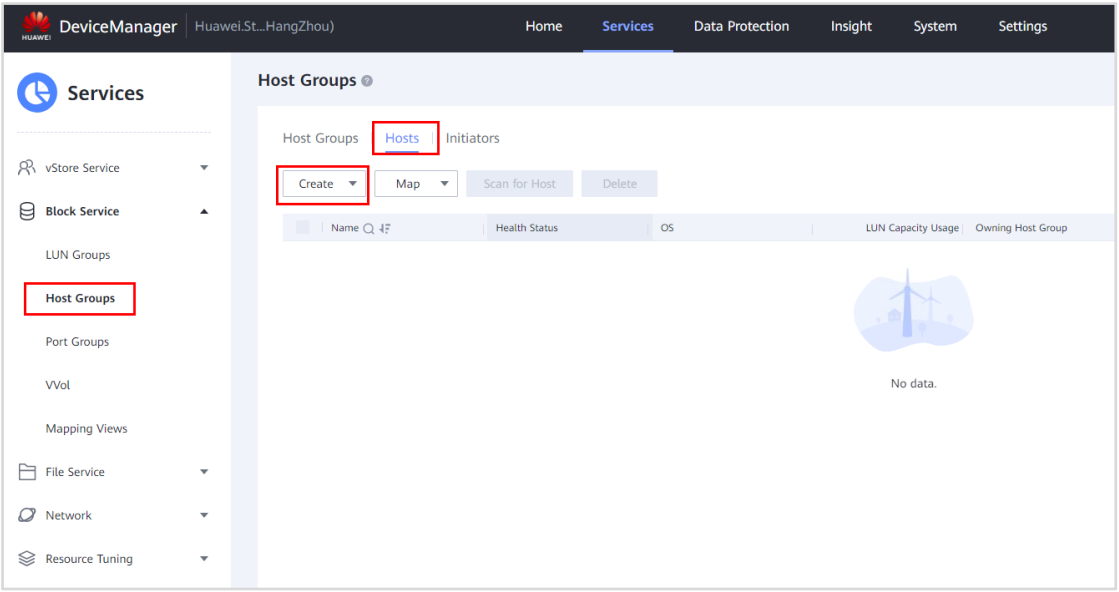


Figure 1-24 Creating a host

Step 3 Set the host name to **test**, set the initiator type to iSCSI, select the configured iSCSI initiator name, and click **OK**.

- If there is no initiator, ask the trainer to configure one.

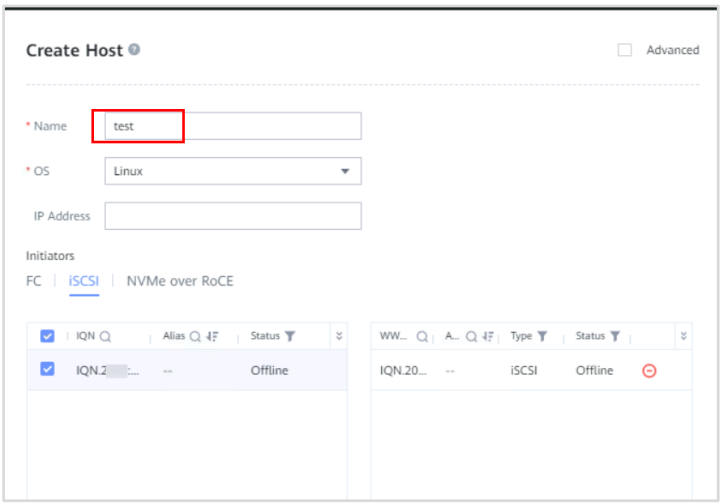


Figure 1-25 Add an iSCSI initiator.

Step 4 In the displayed dialog box, select **I have read and understand the consequences associated with performing this operation** and click **OK**.

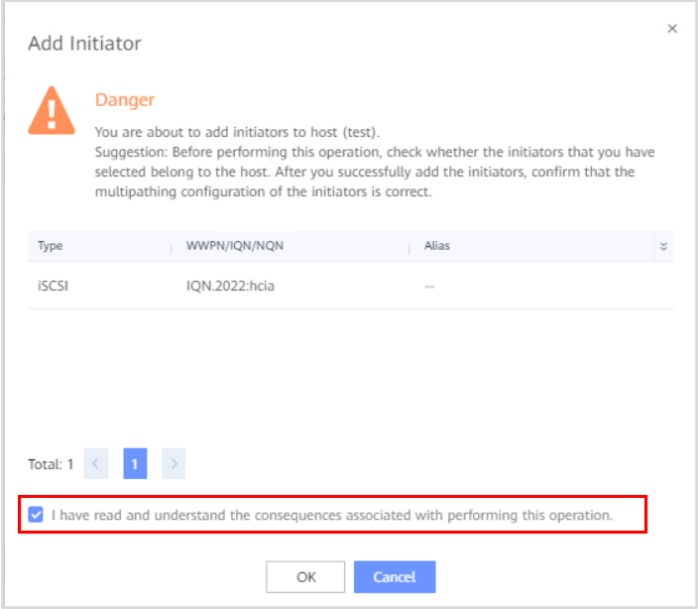


Figure 1-26 Confirming initiator adding and creating a host

Step 5 In the **Execution Result** dialog box that is displayed, click **Close**.

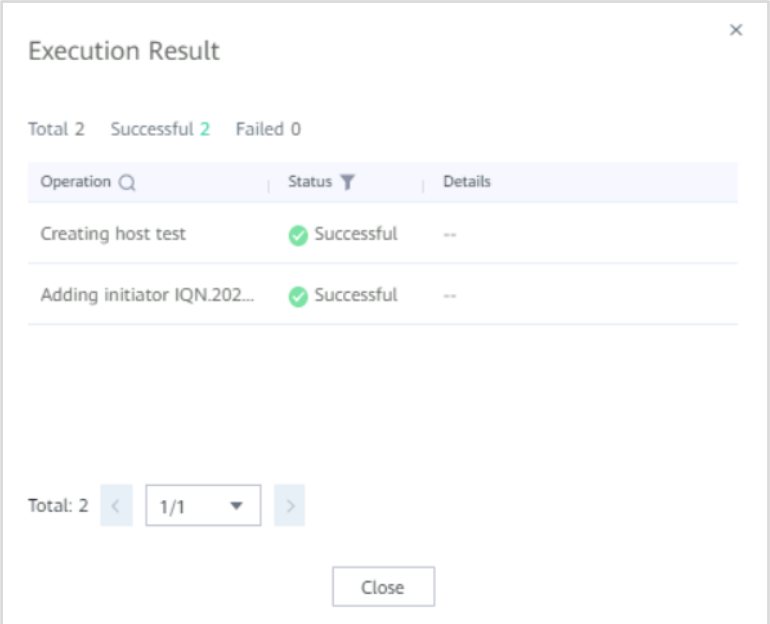


Figure 1-27

Step 6 In the service list, select **Host Groups**, click **Host Groups** on the right, and choose **Create**.

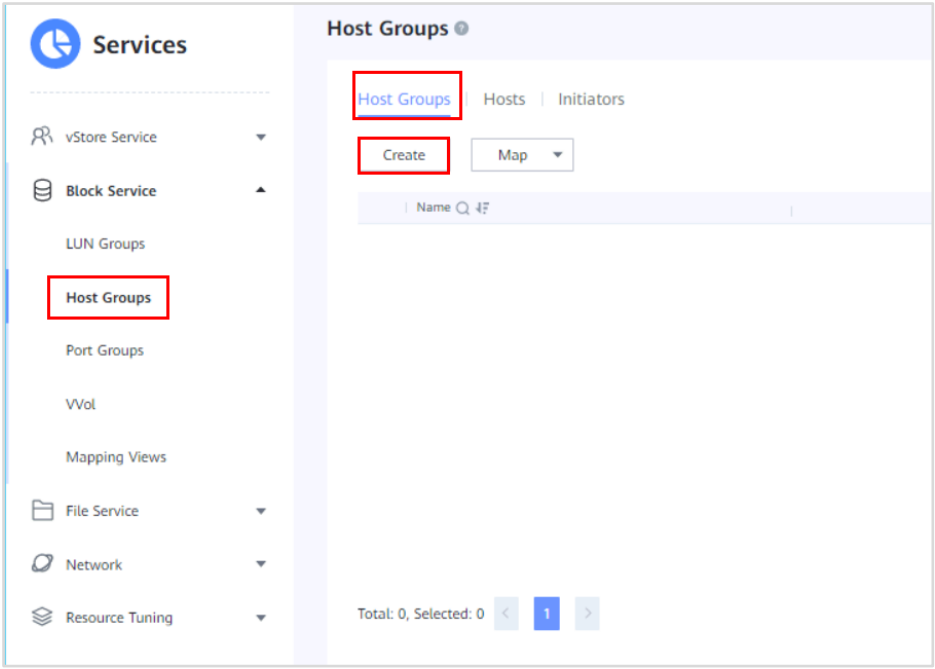


Figure 1-28 Creating a host group

Step 7 Set the host group name to **HostGroup001**, select the created host **test**, and click **OK**.

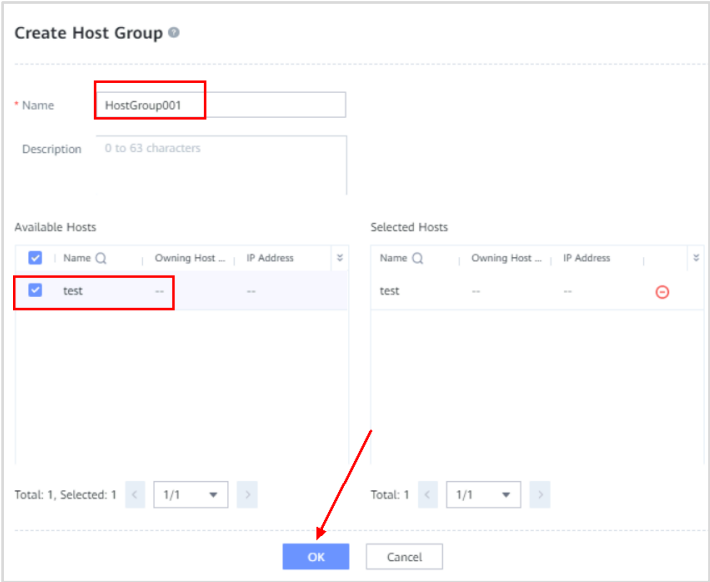


Figure 1-29 Adding a host

Step 8 In the **Execution Result** dialog box that is displayed, click **Close**.

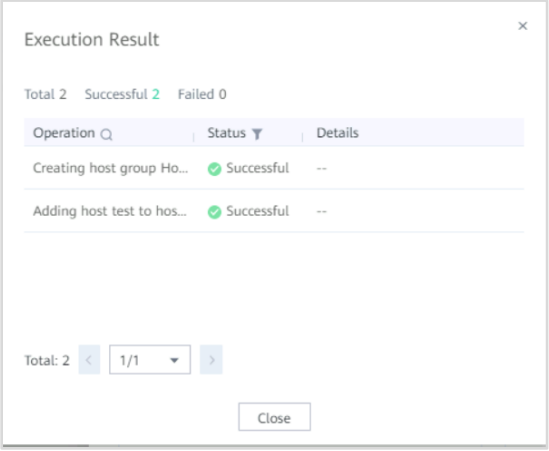


Figure 1-30 Execution result

1.2.5 Creating a LUN, LUN Group, and Mapping View

Step 1 In the service list, select **LUN Groups**, click **LUN Groups** on the right, and choose **Create**.

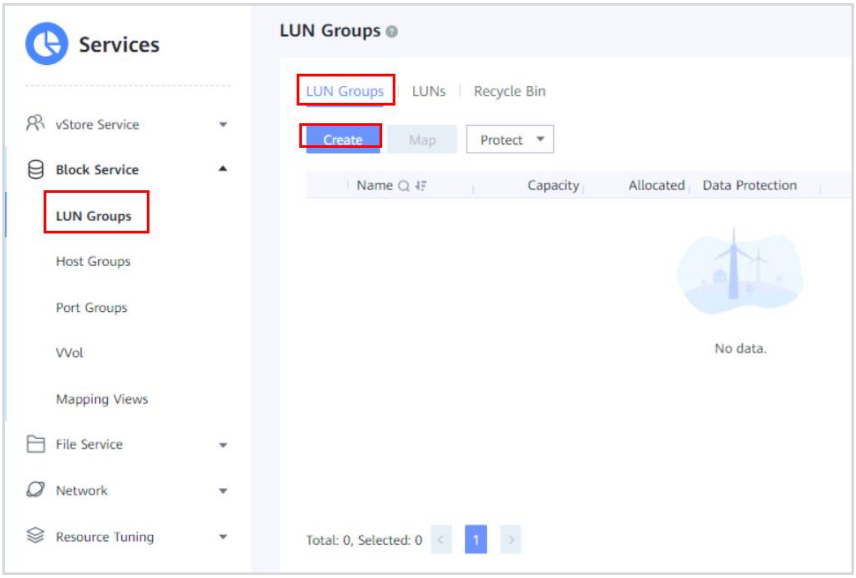


Figure 1-31 Creating a LUN group

Step 2 Set parameters according to the following figure and click **OK** to create a LUN, LUN group, and mapping.

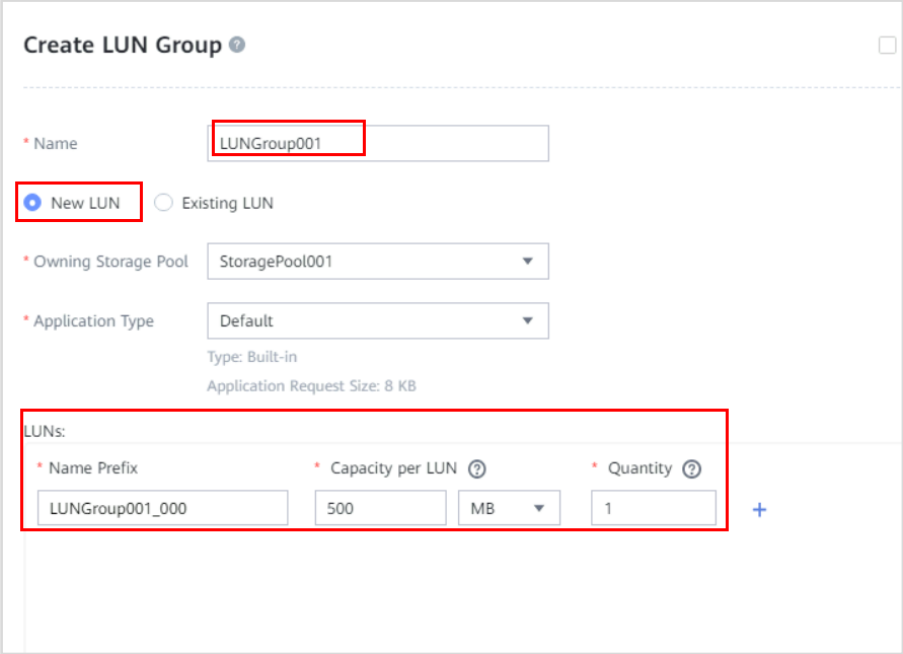


Figure 1-32 Creating a LUN and a LUN group and mapping the LUN to a host group

1.2.6 Lab Verification

Step 1 Log in to the service host using VNC and run the following commands to rescan for and view disks:

```
[root@localhost ~]# iscsiadm –m session –R
[root@localhost ~]# fdisk –l
```

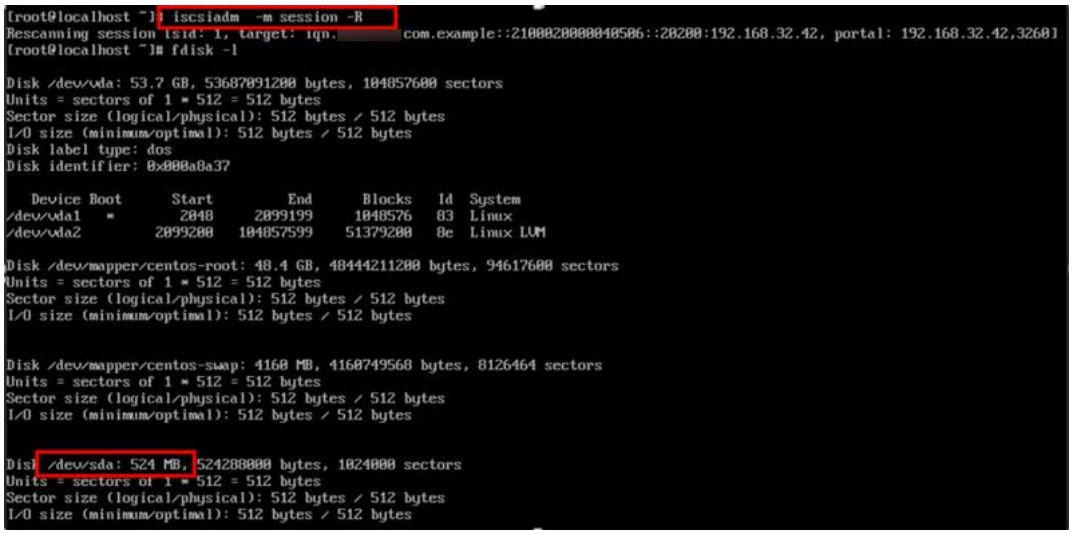


Figure 1-33 Viewing the mounted disk

1.3 Quiz

After a host uses an iSCSI initiator to connect to a storage device, if the iSCSI initiator name changes, will the initiator name be updated on the storage device? If the host initiator name will not be updated, what should I do?

Answer:

The initiator name will not be updated on the storage device. You need to remove the iSCSI connection from the host, restart the iSCSI service, and reconnect the host to the storage device.

2 Network Configuration Exercise

2.1 Introduction to the Switch View

2.1.1 Overview

2.1.1.1 About This Exercise

This exercise describes the basic switch operation views.

2.1.1.2 Objectives

- Understand the basic operations on the eNSP simulator.
- Understand the basic operation views of Huawei switches.

2.1.1.3 Guideline

1. Start a switch on eNSP.
2. Enter the user view.
3. Enter the system view.
4. Enter the interface view.
5. Exit the interface view and system view.

2.1.2 Configuration Procedure

2.1.2.1 Starting a Switch

Step 1 Run the eNSP software, click the switch icon, and drag it to the topology on the right.

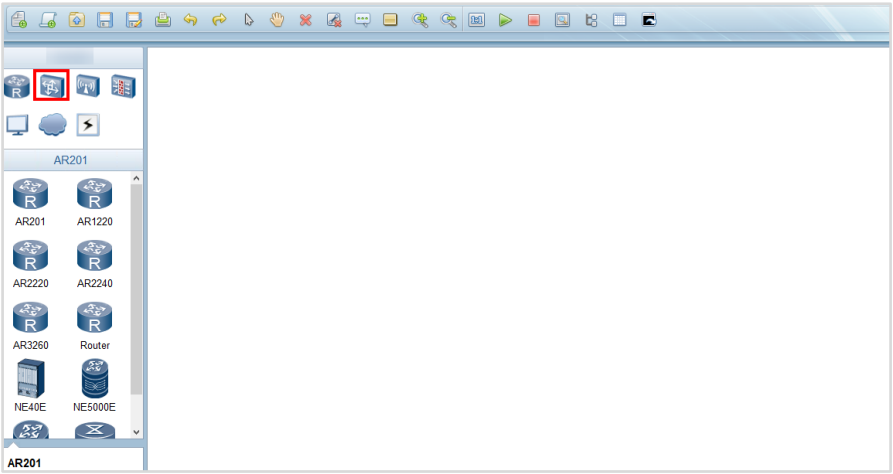


Figure 2-1 Clicking the switch icon

Step 2 Right-click the switch, choose **Start**, and wait for 2 to 5 minutes.

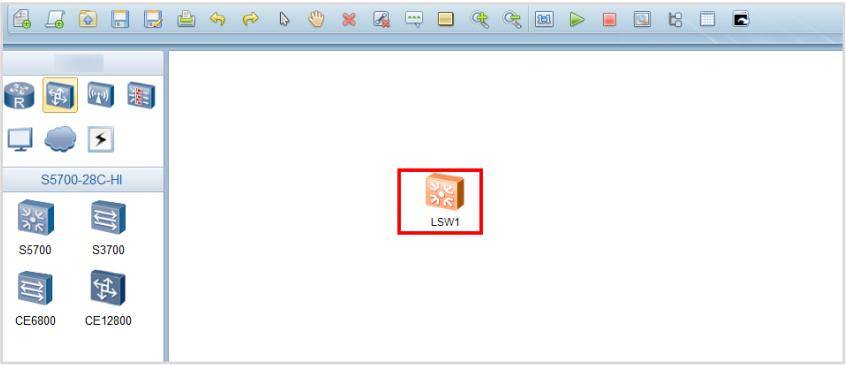


Figure 2-2 Starting a switch

2.1.2.2 Entering the User View

Step 1 Double-click the switch to enter the CLI. <> indicates the user view.

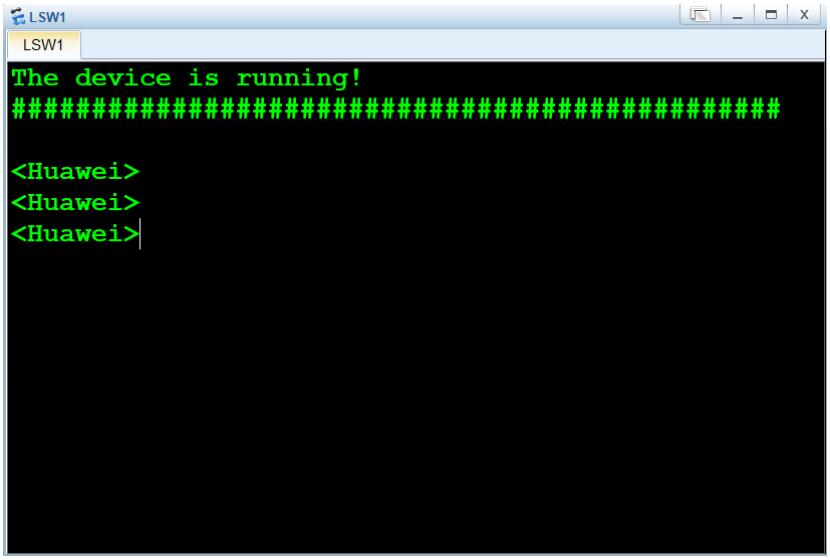


Figure 2-3 User view

Step 2 In the user view, you can run display commands to query information or configuration. Run the following commands:

```
<Huawei>display interface brief
<Huawei>display version
```

```
<Huawei>display  interface  brief
PHY: Physical
*down: administratively down
(l): loopback
(s): spoofing
(b): BFD down
(e): ETHOAM down
(dl): DLDP down
(d): Dampening Suppressed
InUti/OutUti: input utility/output utility
Interface                   PHY   Protocol InUti OutUti   inErrors  outErrors
GigabitEthernet0/0/1        down  down        0%     0%          0          0
GigabitEthernet0/0/2        down  down        0%     0%          0          0
GigabitEthernet0/0/3        down  down        0%     0%          0          0
GigabitEthernet0/0/4        down  down        0%     0%          0          0
GigabitEthernet0/0/5        down  down        0%     0%          0          0
GigabitEthernet0/0/6        down  down        0%     0%          0          0
GigabitEthernet0/0/7        down  down        0%     0%          0          0
```

```
<Huawei>display  version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.110 (S5700 V200R001C00)
Copyright (c) [redacted] HUAWEI TECH CO., LTD

Quidway S5700-28C-HI Routing Switch uptime is 0 week, 0 day, 0 hour, 5 minutes
```

Figure 2-4 Viewing the interface and version information

2.1.2.3 Entering the System View

Step 1 Run the following command to enter the system view of the switch:

```
<Huawei>system-view
```

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]
```

Figure 2-5 System view

Step 2 Run the following command in the system view to change the system name:

```
[Huawei]sysname SW1
```

```
[Huawei]sysname SW1
[SW1]
```

Figure 2-6 Changing the system name

2.1.2.4 Entering the Interface View

In the interface view, you can configure information such as the link type (Layer 2) and IP address (Layer 3) for the interface.

Step 1 Check brief information about interfaces in the system view.

```
[SW1]display interface brief
```

```
[SW1]display int brief
PHY: Physical
*down: administratively down
(l): loopback
(s): spoofing
(b): BFD down
(e): ETHOAM down
(dl): DLDP down
(d): Dampening Suppressed
InUti/OutUti: input utility/output utility
Interface                   PHY   Protocol InUti OutUti   inErrors  outErrors
GigabitEthernet0/0/1        down  down        0%     0%          0          0
GigabitEthernet0/0/2        down  down        0%     0%          0          0
```

Figure 2-7 Checking interface information

Step 2 Run the following command to enter the GigabitEthernet0/0/1 interface view:

```
[SW1]interface GigabitEthernet 0/0/1
[SW1-GigabitEthernet0/0/1]
```

```
[SW1]interface  GigabitEthernet 0/0/1
[SW1-GigabitEthernet0/0/1]
```

Figure 2-8 Interface view

2.1.2.5 Exiting the Interface View and System View

Step 1 Run the following command to exit the GigabitEthernet0/0/1 interface view:

```
[SW1-GigabitEthernet0/0/1]quit
[SW1]
```

Step 2 Run the following command to exit the SW1 system view and return to the user view:

```
[SW1]quit
<SW1>
```

2.2 Basic Switch Configuration

2.2.1 Overview

2.2.1.1 About This Exercise

This exercise describes how to perform basic configurations on Huawei switches.

2.2.1.2 Objectives

- Understand how to change the system name of a Huawei switch.
- Understand how to use the **?** key on Huawei switches.
- Understand how to use the **display** command on Huawei switches.
- Understand how to use the **undo** command on Huawei switches.

2.2.1.3 Guideline

1. Change the system name.
2. Use the **?** key.
3. Run the **display** command.
4. Run the **undo** command.

2.2.2 Configuration Procedure

2.2.2.1 Changing the System Name

Step 1 Log in to the switch and enter the system view.

```
<Huawei>system-view
```

Step 2 Change the system name to **SW1** and then change it back to **Huawei**.

```
[Huawei]sysname SW1
[SW1]sysname Huawei
[Huawei]
```

2.2.2.2 Using the ? Key

? is used to display available commands.

Step 1 Check the available parameters of the **interface** command.

```
[Huawei]interface  ?
```

```
[Huawei]interface  ?
  Eth-Trunk        Ethernet-Trunk interface
  GigabitEthernet  GigabitEthernet interface
  LoopBack         LoopBack interface
  MEth             MEth interface
  NULL             NULL interface
  Tunnel           Tunnel interface
  Vlanif           Vlan interface
```

Figure 2-9 Available parameters of the interface command

Step 2 Check the available parameters of the **port** command in the interface view.

```
[Huawei]interface  GigabitEthernet 0/0/1
[Huawei-GigabitEthernet0/0/1]port ?
```

```
[Huawei]interface  GigabitEthernet 0/0/1
[Huawei-GigabitEthernet0/0/1]port ?
  add-tag        Add outer tag based on acl
  default        Specify current port's PVID VLAN characteristics
  discard        Discard
  link-flap      Link flap
  link-type      Switch port link type
  mux-vlan       Multiplex vlan
  priority       Specify current port's priority
  type           Type
  vlan-mapping   VLAN Mapping
  vlan-stacking  VLAN Stacking
```

Figure 2-10 Available parameters of the port command

2.2.2.3 Running the display Command

Step 1 Run the following command in the system view to check interface information:

```
<Huawei>display interface brief
```

```
<Huawei>display  interface  brief
PHY: Physical
*down: administratively down
(l): loopback
(s): spoofing
(b): BFD down
(e): ETHOAM down
(dl): DLDP down
(d): Dampening Suppressed
InUti/OutUti: input utility/output utility
Interface                   PHY   Protocol InUti OutUti   inErrors  outErrors
GigabitEthernet0/0/1        down  down        0%     0%          0          0
GigabitEthernet0/0/2        down  down        0%     0%          0          0
GigabitEthernet0/0/3        down  down        0%     0%          0          0
GigabitEthernet0/0/4        down  down        0%     0%          0          0
GigabitEthernet0/0/5        down  down        0%     0%          0          0
GigabitEthernet0/0/6        down  down        0%     0%          0          0
GigabitEthernet0/0/7        down  down        0%     0%          0          0
```

Figure 2-11 Checking brief interface information

Step 2 Run the following command to check the current device version:

```
<Huawei>display version
```

```
<Huawei>display  version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.110 (S5700 V200R001C00)
Copyright (c) [redacted] HUAWEI TECH CO., LTD

Quidway S5700-28C-HI Routing Switch uptime is 0 week, 0 day, 0 hour, 5 minutes
```

Figure 2-12 Checking the current version

Step 3 Run the following command in the system view to check the routing table:

```
[Huawei]display ip routing-table
```

```
[Huawei]dis ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 2        Routes : 2

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

Figure 2-13 Checking the routing table

Step 4 Run the following command to check the current device configuration:

```
[Huawei]display current-configuration
```

```
[Huawei]display  current-configuration
#
sysname Huawei
#
cluster enable
ntdp enable
ndp enable
#
drop illegal-mac alarm
#
diffserv domain default
#
drop-profile default
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password simple admin
 local-user admin service-type http
#
```

Figure 2-14 Checking the current configuration

Step 5 Run the following commands to enter the interface view and check the configuration in the current view:

```
[Huawei]interface GigabitEthernet 0/0/1
[Huawei-GigabitEthernet0/0/1]display this
```

```
[Huawei]interface GigabitEthernet 0/0/1
[Huawei-GigabitEthernet0/0/1]dis this
#
interface GigabitEthernet0/0/1
 port link-type access
#
return
```

Figure 2-15 Checking the configuration in the current view

2.2.2.4 Running the undo Command

Step 1 Enter the interface view and set interface parameters.

```
[Huawei]interface GigabitEthernet 0/0/1
[Huawei-GigabitEthernet0/0/1]port link-type access
```

Step 2 Check the configuration of the current interface.

```
[Huawei-GigabitEthernet0/0/1]display this
```

```
[Huawei-GigabitEthernet0/0/1]dis this
#
interface GigabitEthernet0/0/1
 port link-type access
#
return
[Huawei-GigabitEthernet0/0/1]
```

Figure 2-16 Configuration of the current interface

Step 3 Delete the configuration of the current interface.

```
[Huawei-GigabitEthernet0/0/1]undo port link-type
```

```
[Huawei-GigabitEthernet0/0/1]undo port link-type
```

Figure 2-17 Deleting the configuration

Step 4 Check the configuration of the current interface again.

```
[Huawei-GigabitEthernet0/0/1]display this
```

```
[Huawei-GigabitEthernet0/0/1]dis this
#
interface GigabitEthernet0/0/1
#
return
```

Figure 2-18 Configuration of the current interface

2.3 VLAN Implementation Exercise

2.3.1 Overview

2.3.1.1 About This Exercise

This exercise configures virtual local area networks (VLANs) on switches, so that users in the same VLAN can communicate only with each other.

2.3.1.2 Objectives

- Understand the implementation of VLAN.
- Understand the link types of VLAN.
- Understand how to configure different types of VLAN interfaces.
- Understand how to assign VLANs based on interfaces.
- Understand the functions of different interface types.

2.3.1.3 Networking Topology

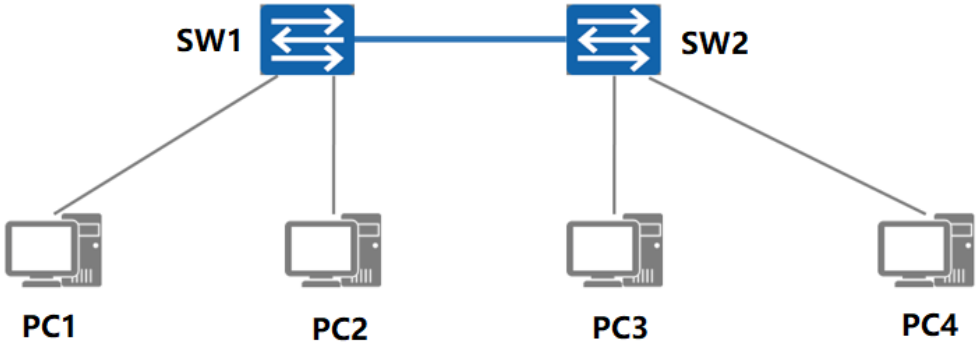


Figure 2-19 Networking diagram

2.3.1.4 Exercise Planning

- PC1, PC2, PC3, and PC4 are connected to a campus network through access switches SW1 and SW2. Create VLAN 10 and VLAN 20, assign PC1 and PC2 to VLAN 10, and assign PC3 and PC4 to VLAN 20.
- Configure the type of interfaces interconnecting the access switches to trunk and configure the trunk interfaces to allow packets from corresponding VLANs to pass

through. Configure the type of interfaces connecting the access switches to the PCs to access and change the PVIDs of the access interfaces to the VLAN IDs to be assigned to the PCs.

- After the configuration, users in the same VLAN can communicate only with each other, while users in different VLANs are isolated at Layer 2.

Table 2-1 VLAN interface type and parameter plan

Device	Interface	Interface Type	VLAN Parameter
SW1 (LSW1)	GE0/0/1	Trunk	PVID: 1 Allowed VLANs: VLAN 10 and VLAN 20
	GE0/0/2	Access	PVID: 10
	GE0/0/3	Access	PVID: 20
SW2 (LSW2)	GE0/0/1	Trunk	PVID: 1 Allowed VLANs: VLAN 10 and VLAN 20
	GE0/0/2	Access	PVID: 10
	GE0/0/3	Access	PVID: 20

2.3.1.5 Guideline

1. Set up a topology.
2. Configure IP addresses for the hosts.
3. Create VLANs on the switches.
4. Configure access and trunk interfaces on the switches.
5. Verify the configuration.

2.3.2 Configuration Procedure

2.3.2.1 Setting Up a Topology

Step 1 Run eNSP and set up a topology according to the following figure using switch and PC icons.

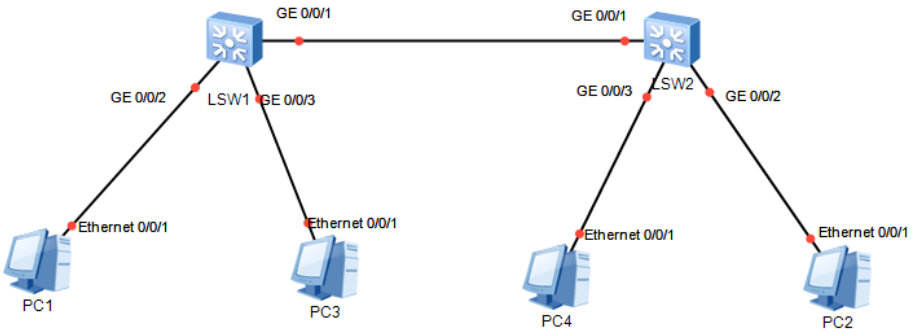


Figure 2-20 Setting up a topology

Step 2 Select all devices and click the button in the red box in the following figure to start the devices.

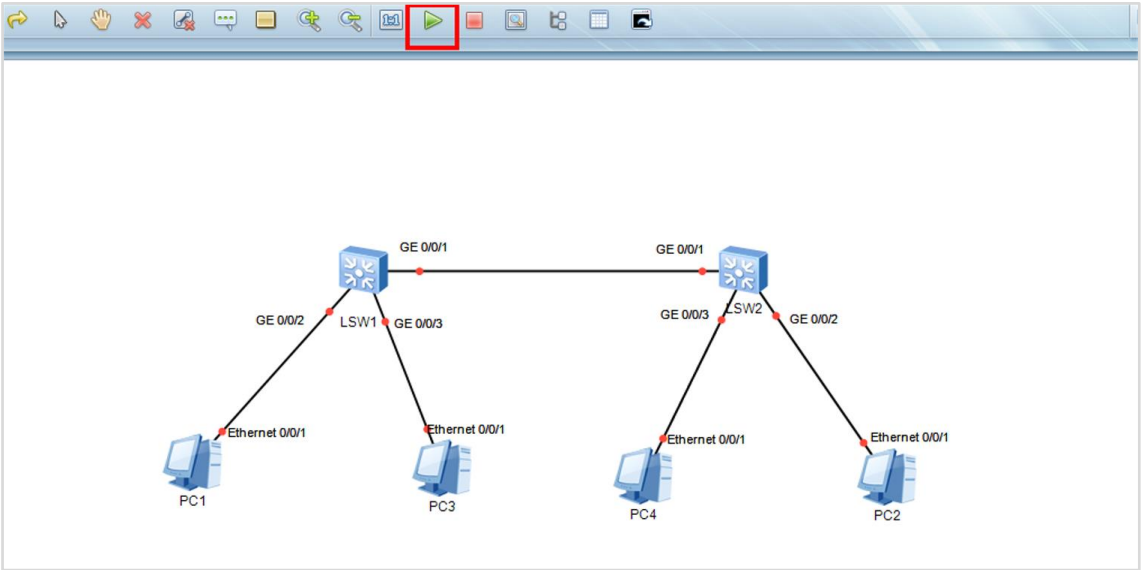


Figure 2-21 Starting devices

Step 3 Check that link indicator turns green after the devices are started.

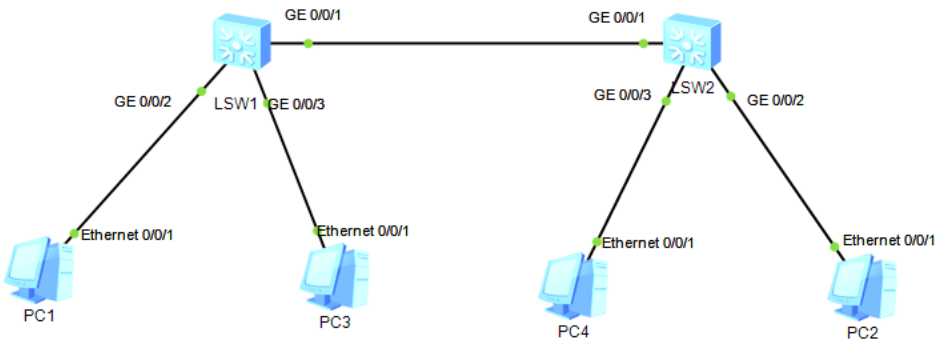


Figure 2-22 Started devices

2.3.2.2 Configuring Hosts

Step 1 Double-click PC1 and PC2, set the IP addresses of PC1 and PC2 respectively according to the following figure, and click **Apply**.

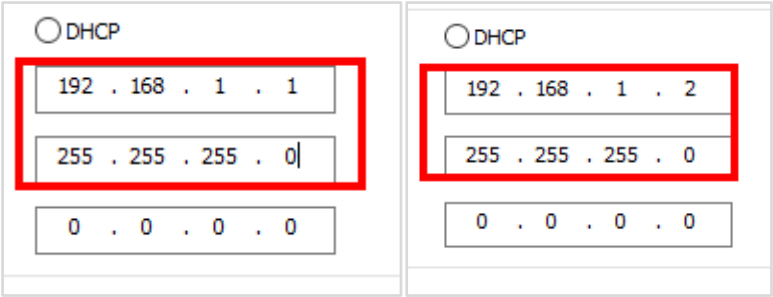


Figure 2-23 Configuring IP addresses

Step 2 Double-click PC3 and PC4, set the IP addresses of PC3 and PC4 respectively according to the following figure, and click **Apply**.

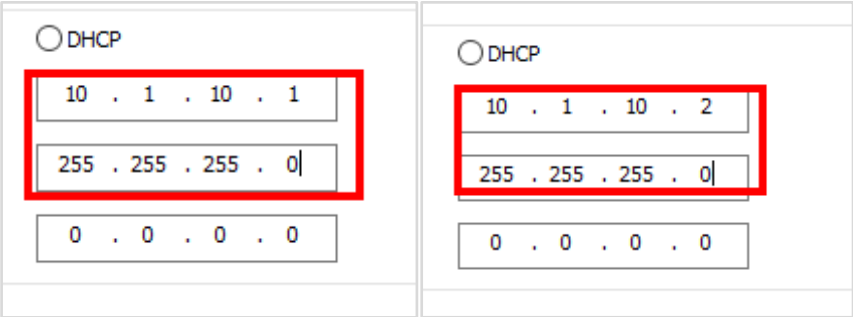


Figure 2-24 Configuring IP addresses

2.3.2.3 Configuring Switches

Step 1 Configure LSW1.

Double-click LSW1 to enter the CLI. Run the following commands to enter the system view and change the system name:

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname SW1
```

```
<Huawei>sys
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sys
[Huawei]sysname SW1
[SW1]
```

Figure 2-25 Changing the system name

Step 2 Create VLAN 10 and VLAN 20.

```
[Huawei]vlan batch 10 20
```

```
[Huawei]vlan batch  10 20
Info: This operation may take a few seconds. Please wait for a moment...done.
```

Figure 2-26 Creating VLANs

Step 3 Set the interface type of GE0/0/2 and GE0/0/3 to access and set their default VLAN IDs to 10 and 20, respectively.

```
[SW1]interface GigabitEthernet 0/0/2
[SW1-GigabitEthernet0/0/2]port link-type access
[SW1-GigabitEthernet0/0/2]port default vlan 10
[SW1]interface GigabitEthernet 0/0/3
[SW1-GigabitEthernet0/0/2]port link-type access
[SW1-GigabitEthernet0/0/2]port default vlan 20
```

Run the **dis this** command on the two interfaces and verify the configurations.

```
[SW1-GigabitEthernet0/0/2]dis this
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 10
```

```
[SW1-GigabitEthernet0/0/3]dis this
#
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 20
```

Figure 2-27 Checking the interface configuration

Step 4 Configure GE0/0/1 as a trunk interface and configure it to allow packets from VLAN 10 and VLAN 20 to pass through.

```
[SW1]int GigabitEthernet 0/0/1
[SW1-GigabitEthernet0/0/1]port link-type trunk
[SW1-GigabitEthernet0/0/1]port trunk  allow-pass vlan 10 20
```

Run the **dis this** command and verify the configuration.

```
[SW1-GigabitEthernet0/0/1]dis this
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10 20
#
return
```

Figure 2-28 Checking the interface configuration

Step 5 Configure LSW2. You can configure LSW2 by referring to the configuration on LSW1.

- Change the system name to **SW2** and create VLAN 10 and VLAN 20.
- Set the interface type of GE0/0/2 and GE0/0/3 to access and set their default VLAN IDs to 10 and 20, respectively.
- Configure GE0/0/1 as a trunk interface and configure it to allow packets from VLAN 10 and VLAN 20 to pass through.

After the configuration is complete, run the following command to check the configuration.

```
[SW2]dis current-configuration interface
```

```
[SW2]dis current-configuration  interface
#
interface Vlanif1
#
interface MEth0/0/1
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10 20
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 10
#
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 20
#
```

Figure 2-29 Checking the interface configuration

2.3.2.4 Exercise Verification

- Testing the Connectivity in VLAN 10

Step 1 Double-click PC1 and click the **CLI** tab to enter the CLI. Ping the IP address of PC2 in the same VLAN.

```
PC>ping 192.168.1.2

Ping 192.168.1.2: 32 data bytes, Press Ctrl_C to break
From 192.168.1.2: bytes=32 seq=1 ttl=128 time=63 ms
From 192.168.1.2: bytes=32 seq=2 ttl=128 time=63 ms
From 192.168.1.2: bytes=32 seq=3 ttl=128 time=63 ms
From 192.168.1.2: bytes=32 seq=4 ttl=128 time=62 ms
From 192.168.1.2: bytes=32 seq=5 ttl=128 time=63 ms

--- 192.168.1.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 62/62/63 ms
```

Figure 2-30 Verifying connectivity

- Testing the Connectivity in VLAN 20

Step 2 Double-click PC3 and click the **CLI** tab to enter the CLI. Ping the IP address of PC4 in the same VLAN.

```
PC>ping 10.1.10.2

Ping 10.1.10.2: 32 data bytes, Press Ctrl_C to break
From 10.1.10.2: bytes=32 seq=1 ttl=128 time=63 ms
From 10.1.10.2: bytes=32 seq=2 ttl=128 time=78 ms
From 10.1.10.2: bytes=32 seq=3 ttl=128 time=62 ms
From 10.1.10.2: bytes=32 seq=4 ttl=128 time=63 ms
From 10.1.10.2: bytes=32 seq=5 ttl=128 time=63 ms

--- 10.1.10.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 62/65/78 ms
```

Figure 2-31 Verifying connectivity

- Verifying that Users in VLAN 10 Cannot Communicate with Users in VLAN 20

Step 3 Change the default VLAN of the interface connecting LSW2 to PC2 to VLAN 20.

```
[SW2]interface GigabitEthernet 0/0/2
[SW2-GigabitEthernet0/0/2]port link-type access
[SW2-GigabitEthernet0/0/2]port default vlan 20
```

Step 4 Double-click PC1 and click the **CLI** tab to enter the CLI. Ping the IP address of PC2 again.

```
PC>ping 192.168.1.2

Ping 192.168.1.2: 32 data bytes, Press Ctrl_C to break
Request timeout!
Request timeout!
Request timeout!
Request timeout!
Request timeout!
```

Figure 2-32 Verifying connectivity

2.4 Routing Implementation Exercise

2.4.1 Overview

2.4.1.1 About This Exercise

This exercise configures static routes to allow users on different network segments to communicate with each other.

2.4.1.2 Objectives

- Understand basic operations on Huawei Layer 3 switches.
- Understand basic information in routing tables of Huawei Layer 3 switches.
- Understand how to configure VLANIF interfaces on Huawei Layer 3 switches.
- Understand how to configure static routes on Huawei Layer 3 switches.

2.4.1.3 Networking Topology

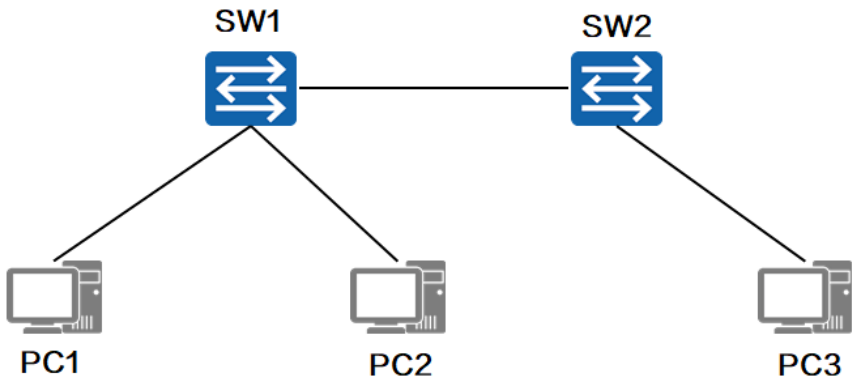


Figure 2-33 Networking diagram

2.4.1.4 Exercise Planning

- PC1, PC2, and PC3 belong to different departments and are connected to a campus network through access switches SW1 and SW2.
- The interconnection network segment of SW1 and SW2 is 10.1.40.0/24. PC1 resides on 10.1.10.0/24, PC2 resides on 10.1.20.0/24, and PC3 resides on 10.1.30.0/24.

- Configure static routes on SW1 and SW2 so that users in different departments can communicate with each other.

Table 2-2 Interface and address plan

Device	Interface	Interface Type	VLAN	VLANIF Interface
SW1 (LSW1)	GE0/0/1	Access	PVID: 10	VLANIF 10: 10.1.10.254/24 VLANIF 20: 10.1.20.254/24 VLANIF 40: 10.1.40.1/24
	GE0/0/2	Access	PVID: 20	
	GE0/0/3	Access	PVID: 40	
SW2 (LSW2)	GE0/0/1	Access	PVID: 30	VLANIF 30: 10.1.30.254/24 VLANIF 40: 10.1.40.2/24
	GE0/0/3	Access	PVID: 40	

Table 2-3 Static route plan

Device	Static Route
SW1 (LSW1)	ip route-static 10.1.30.0 24 10.1.40.2
SW2 (LSW2)	ip route-static 10.1.10.0 24 10.1.40.1 ip route-static 10.1.20.0 24 10.1.40.1

2.4.1.5 Guideline

1. Set up a topology.
2. Configure IP addresses for the hosts.
3. Configure interfaces on the switches and configure IP addresses for the interfaces.
4. Configure static routes on the switches.
5. Verify the configuration on the hosts.

2.4.2 Configuration Procedure

2.4.2.1 Setting Up a Topology

Step 1 Run eNSP and set up a topology according to the following figure using switch and PC icons. Start the devices and mark the planned IP addresses.

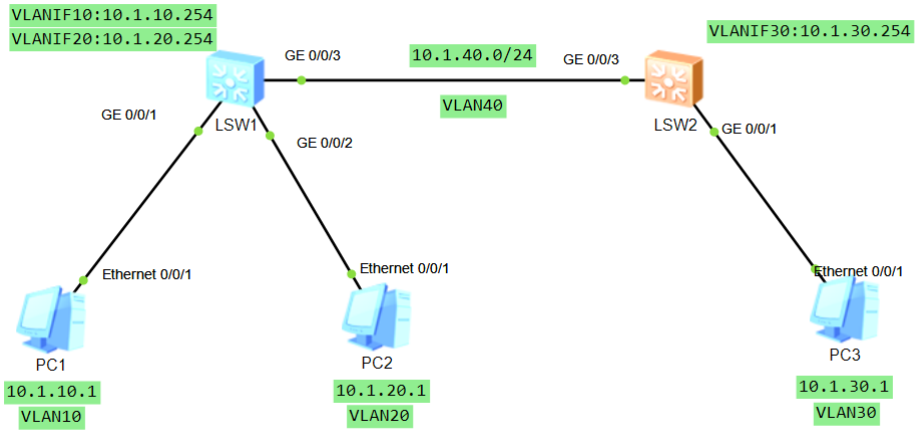


Figure 2-34 Setting up a topology and planning IP addresses

2.4.2.2 Configuring Hosts

Step 1 Double-click PC1, PC2, and PC3 and set the IP addresses of PC1, PC2, and PC3 respectively according to the following figure.

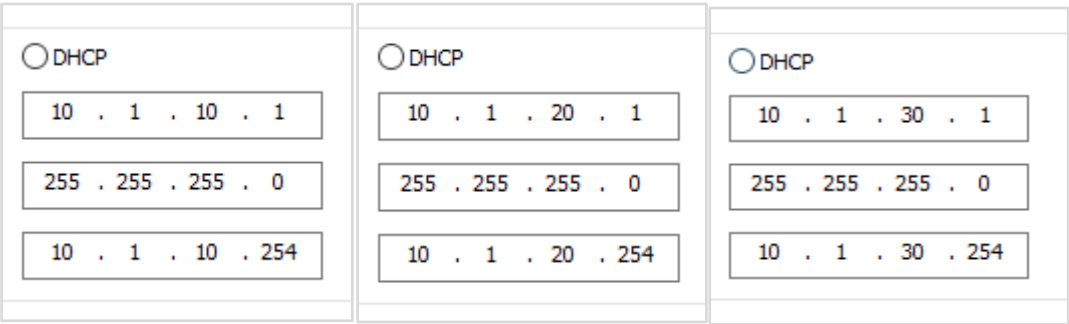


Figure 2-35 Configuring IP addresses

2.4.2.3 Configuring Switches

Step 1 Configure LSW1.

- Double-click LSW1 to enter the CLI. Run the following command to change the system name to **SW1**.

```
[Huawei]sysname SW1
[SW1]
```

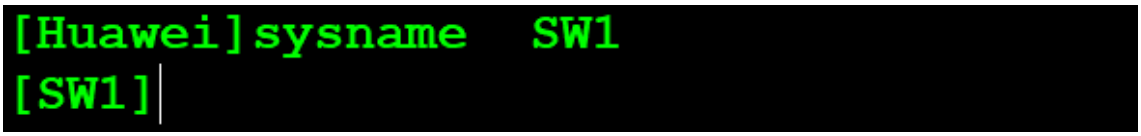


Figure 2-36 Changing the system name

- Create VLANs.

```
[SW1]vlan batch 10 20 40
```

```
Info: This operation may take a few seconds. Please wait for a moment...done.
```

```
[SW1]vlan batch  10 20 40
Info: This operation may take a few seconds. Please wait for a moment...done.
[SW1]
```

Figure 2-37 Creating VLANs

- Configure interfaces as planned.

```
[SW1]interface GigabitEthernet 0/0/1
[SW1-GigabitEthernet0/0/1]port link-type access
[SW1-GigabitEthernet0/0/1]port default vlan 10
[SW1-GigabitEthernet0/0/1] interface GigabitEthernet 0/0/2
[SW1-GigabitEthernet0/0/2]port link-type access
[SW1-GigabitEthernet0/0/2]port default vlan 20
[SW1-GigabitEthernet0/0/2] interface GigabitEthernet 0/0/3
[SW1-GigabitEthernet0/0/3] port link-type access
[SW1-GigabitEthernet0/0/3]port default vlan 40
[SW1-GigabitEthernet0/0/3]quit
[SW1]interface   Vlanif 10
[SW1-Vlanif10]ip address 10.1.10.254 24
[SW1-Vlanif10]quit
[SW1]interface   Vlanif 20
[SW1-Vlanif20]ip address 10.1.20.254 24
[SW1]interface   Vlanif 40
[SW1-Vlanif40]ip address 10.1.40.1 24
```

```
[SW1]display  current-configuration  interface
#
interface Vlanif1
#
interface Vlanif10
 ip address 10.1.10.254 255.255.255.0
#
interface Vlanif20
 ip address 10.1.20.254 255.255.255.0
#
interface Vlanif40
 ip address 10.1.40.1 255.255.255.0
#
interface MEth0/0/1
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 10
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 20
#
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 40
```

Figure 2-38 Configuring interfaces

- Configure a static route as planned.

```
[SW1]ip route-static 10.1.30.0 24 10.1.40.2
```

```
[SW1]ip route-static 10.1.30.0 24 10.1.40.2
```

Figure 2-39 Configuring a static route

- Check the routing table.

```
[SW1]display ip routing-table
```

```
[SW1]dis ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 9        Routes : 9

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      10.1.10.0/24  Direct  0    0           D   10.1.10.254     Vlanif10
    10.1.10.254/32  Direct  0    0           D   127.0.0.1       Vlanif10
      10.1.20.0/24  Direct  0    0           D   10.1.20.254     Vlanif20
    10.1.20.254/32  Direct  0    0           D   127.0.0.1       Vlanif20
      10.1.30.0/24  Static  60   0          RD   10.1.40.2       Vlanif40
      10.1.40.0/24  Direct  0    0           D   10.1.40.1       Vlanif40
      10.1.40.1/32  Direct  0    0           D   127.0.0.1       Vlanif40
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

Figure 2-40 Routing table on SW1

Step 2 Configure LSW2.

- Double-click LSW2 to enter the CLI and change the system name to **SW2**.

```
[Huawei]sysname  SW2
[SW2]
```

- Create VLANs.

```
[SW2]vlan batch 30 40
Info: This operation may take a few seconds. Please wait for a moment...done.
```

- Configure interfaces as planned.

```
[SW2]interface GigabitEthernet 0/0/1
[SW2-GigabitEthernet0/0/1]port link-type access
[SW2-GigabitEthernet0/0/1]port default vlan 30
[SW2-GigabitEthernet0/0/1]interface GigabitEthernet 0/0/3
[SW2-GigabitEthernet0/0/3]port link-type access
[SW2-GigabitEthernet0/0/3]port default vlan 40
[SW2-GigabitEthernet0/0/3]quit
[SW2]interface Vlanif 30
[SW2-Vlanif20]ip address 10.1.30.254 24
[SW2]interface Vlanif 40
```

```
[SW2-Vlanif40]ip address 10.1.40.2 24
```

```
[SW2]dis current-configuration  interface
#
interface Vlanif1
#
interface Vlanif30
 ip address 10.1.30.254 255.255.255.0
#
interface Vlanif40
 ip address 10.1.40.2 255.255.255.0
#
interface MEth0/0/1
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 30
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 40
```

Figure 2-41 Configuring interfaces

- Configure static routes as planned.

```
[SW2]ip route-static 10.1.10.0 24 10.1.40.1
[SW2]ip route-static 10.1.20.0 24 10.1.40.1
```

```
[SW2]ip route-static 10.1.10.0 24 10.1.40.1
[SW2]ip route-static 10.1.20.0 24 10.1.40.1
```

Figure 2-42 Configuring static routes

- Check the routing table.

```
[SW2]display ip routing-table
```

```
[SW2]dis ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 8        Routes : 8

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      10.1.10.0/24  Static  60   0           RD   10.1.40.1       Vlanif40
      10.1.20.0/24  Static  60   0           RD   10.1.40.1       Vlanif40
      10.1.30.0/24  Direct  0    0            D   10.1.30.254     Vlanif30
    10.1.30.254/32  Direct  0    0            D   127.0.0.1       Vlanif30
      10.1.40.0/24  Direct  0    0            D   10.1.40.2       Vlanif40
      10.1.40.2/32  Direct  0    0            D   127.0.0.1       Vlanif40
      127.0.0.0/8   Direct  0    0            D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0            D   127.0.0.1       InLoopBack0
```

Figure 2-43 Routing table on SW2

2.4.2.4 Testing Connectivity

- Ping the IP address of PC2 (10.1.20.1) from PC1.

```
PC>ping 10.1.20.1

Ping 10.1.20.1: 32 data bytes, Press Ctrl_C to break
Request timeout!
From 10.1.20.1: bytes=32 seq=2 ttl=127 time=31 ms
From 10.1.20.1: bytes=32 seq=3 ttl=127 time=31 ms
From 10.1.20.1: bytes=32 seq=4 ttl=127 time=31 ms
From 10.1.20.1: bytes=32 seq=5 ttl=127 time=47 ms

--- 10.1.20.1 ping statistics ---
  5 packet(s) transmitted
  4 packet(s) received
  20.00% packet loss
  round-trip min/avg/max = 0/35/47 ms
```

Figure 2-44 Testing connectivity

- Ping the IP address of PC3 (10.1.30.1) from PC1.

```
PC>ping 10.1.30.1

Ping 10.1.30.1: 32 data bytes, Press Ctrl_C to break
From 10.1.30.1: bytes=32 seq=1 ttl=126 time=78 ms
From 10.1.30.1: bytes=32 seq=2 ttl=126 time=62 ms
From 10.1.30.1: bytes=32 seq=3 ttl=126 time=63 ms
From 10.1.30.1: bytes=32 seq=4 ttl=126 time=47 ms
From 10.1.30.1: bytes=32 seq=5 ttl=126 time=63 ms

--- 10.1.30.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 47/62/78 ms
```

Figure 2-45 Testing connectivity

- Ping the IP address of PC2 (10.1.20.1) from PC3.

```
PC>ping 10.1.20.1

Ping 10.1.20.1: 32 data bytes, Press Ctrl_C to break
Request timeout!
From 10.1.20.1: bytes=32 seq=2 ttl=126 time=63 ms
From 10.1.20.1: bytes=32 seq=3 ttl=126 time=47 ms
From 10.1.20.1: bytes=32 seq=4 ttl=126 time=62 ms
From 10.1.20.1: bytes=32 seq=5 ttl=126 time=94 ms

--- 10.1.20.1 ping statistics ---
  5 packet(s) transmitted
  4 packet(s) received
  20.00% packet loss
  round-trip min/avg/max = 0/66/94 ms
```

Figure 2-46 Testing connectivity

2.5 Quiz

After you run the **display ip interface brief** on an existing VLANIF interface on a switch, the command output shows that the physical status and protocol status of the VLANIF interface are both Down. Why does this occur?

Reference answer:

No physical interface assigned to the VLAN corresponding to the VLANIF interface is in Up state.

3 Linux Exercise

3.1 Overview

3.1.1 About This Exercise

This section introduces the bash commands, file management commands, and network configuration commands on the openEuler OS.

3.1.2 Objectives

- Master bash commands.
- Master file management commands.
- Master the basic operations on the text editor.
- Master the basic operations of openEuler system and network configurations.

3.2 Preparations

3.2.1 Creating a VM

Step 1 Open VirtualBox 6.1.34 and click **New** to create a VM.

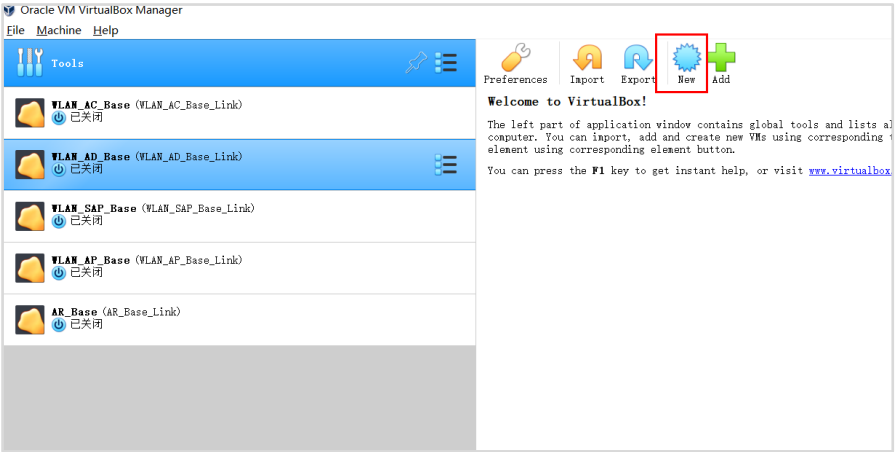


Figure 3-1 Creating a VM

Step 2 Enter the VM name, select the OS type and version, and click **Next**.

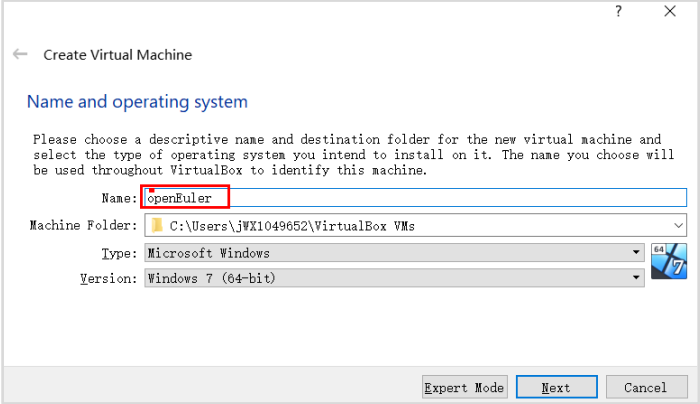


Figure 3-2 VM name and OS type

Step 3 Select the memory size and click **Next**. (You are advised to select 4096 MB.)

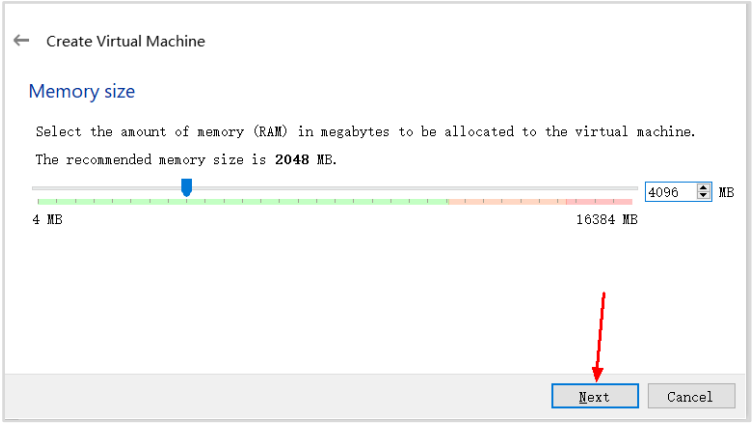


Figure 3-3 Setting the memory

Step 4 Select **Create a virtual hard disk now** and click **Create**.

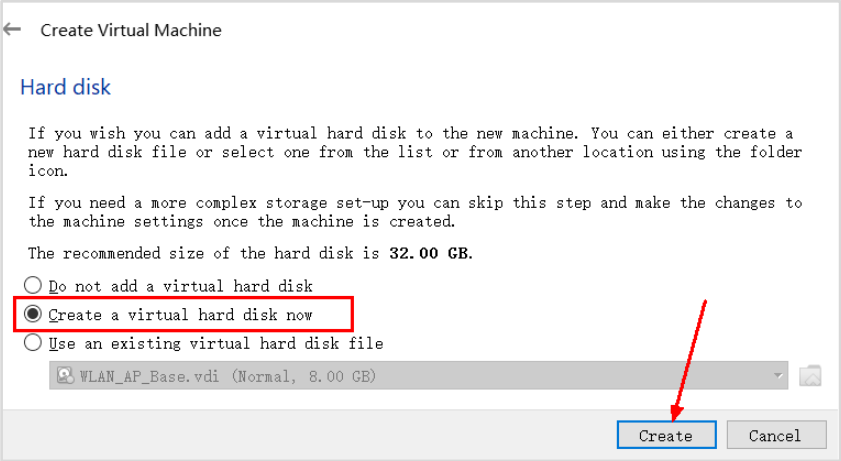


Figure 3-4 Setting the virtual hard disk

Step 5 Select **VHD (Virtual Hard Disk)** and click Next.

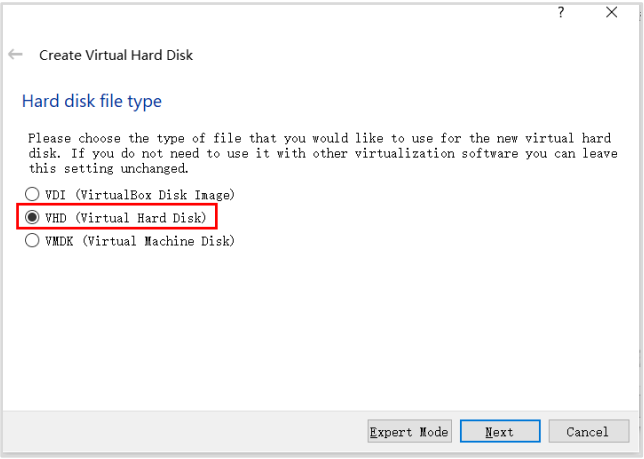


Figure 3-5 Setting the virtual hard disk

Step 6 Select the size of the disk and click **Create**. (You are advised to select 30 GB.)

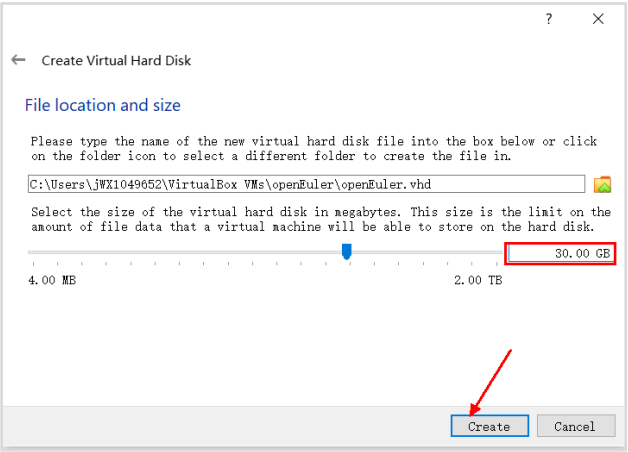


Figure 3-6 Setting the file location and size

Step 7 Click **Settings** on the main page.

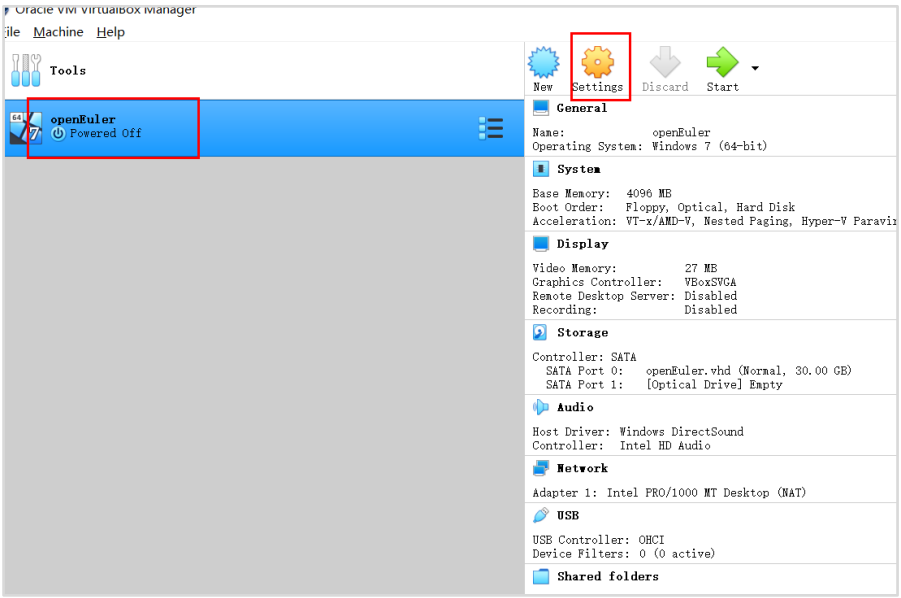


Figure 3-7 Main page

Step 8 On the **System** > **Motherboard** tab page, change the boot order to boot from the hard disk first.

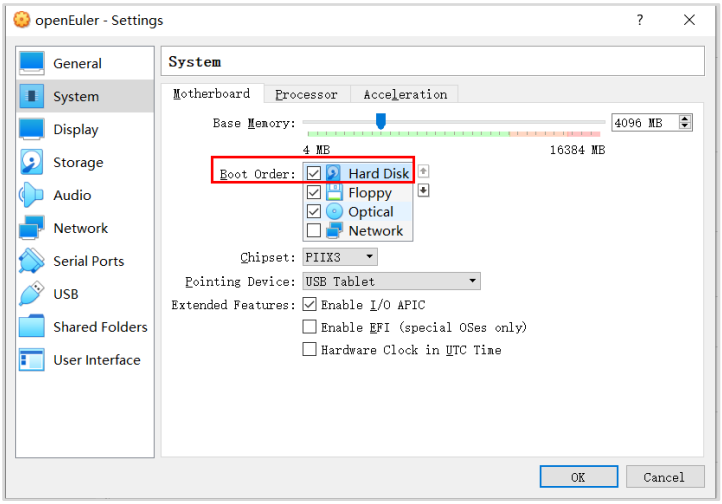


Figure 3-8 Setting the boot order

3.2.2 Installing an OS on the VM

Step 1 Start the VM.

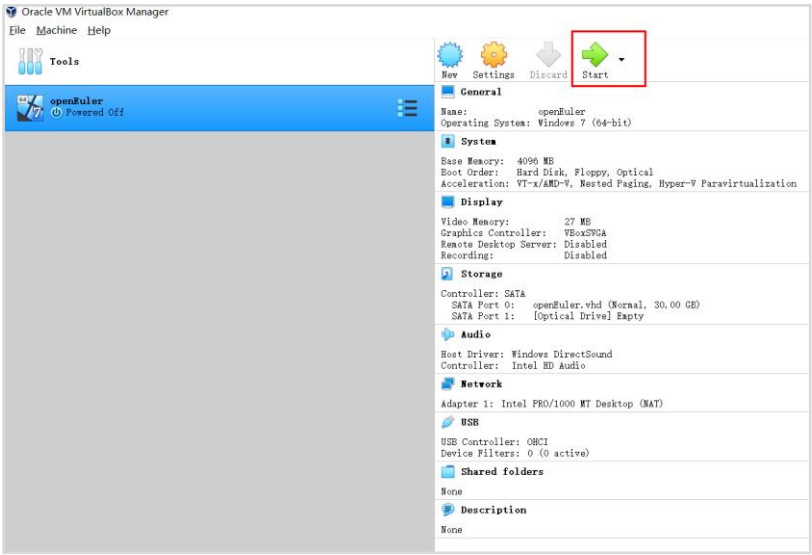


Figure 3-9 Starting the VM

Step 2 Select a local openEuler image file and click **Start**.

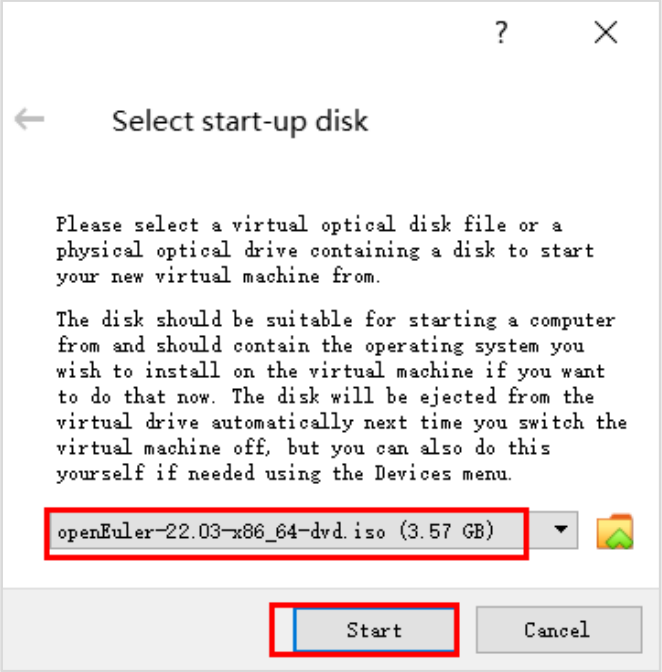


Figure 3-10 Starting the VM

Step 3 Select **Install openEuler**.

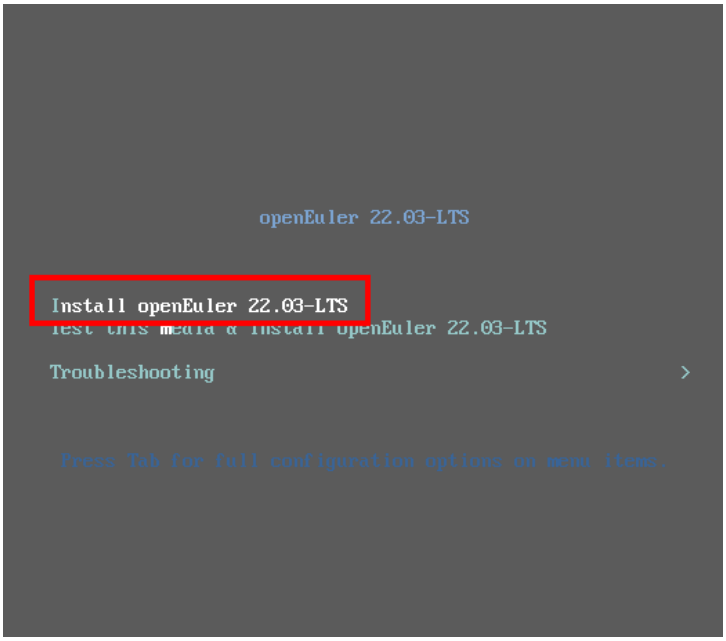


Figure 3-11 Installing the OS

Step 4 Select **English** and click **Continue**.

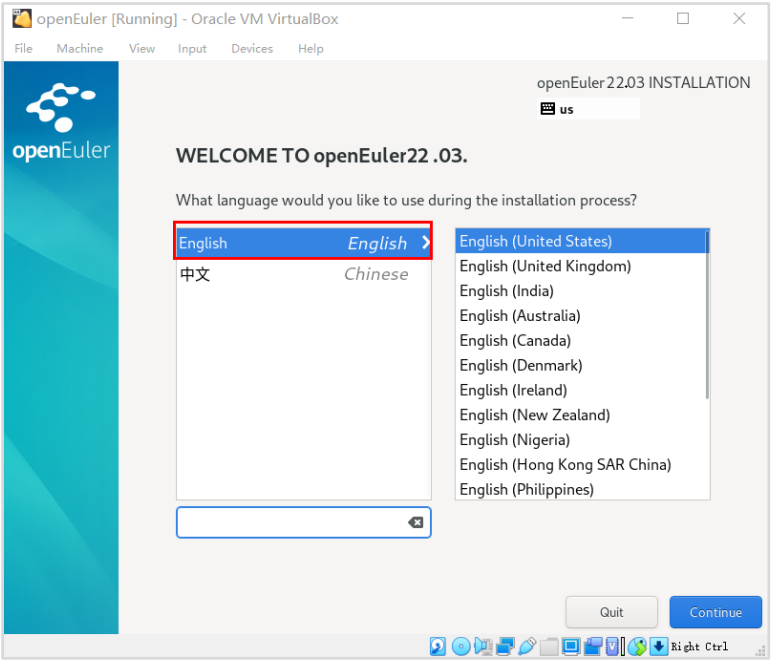


Figure 3-12 Selecting the OS language

Step 5 Click **Installation Destination** and select a disk for installation.

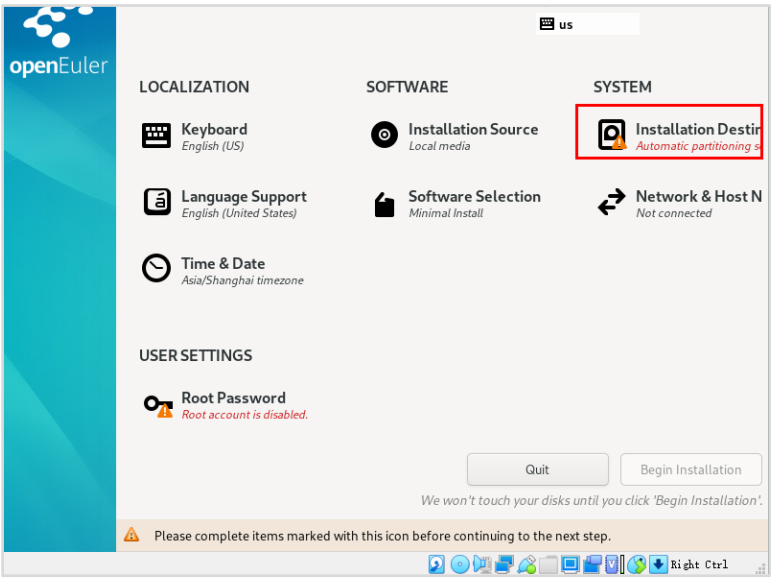


Figure 3-13 Selecting the disk for installation

Step 6 Use the default settings and click **Done**. The main page is displayed.

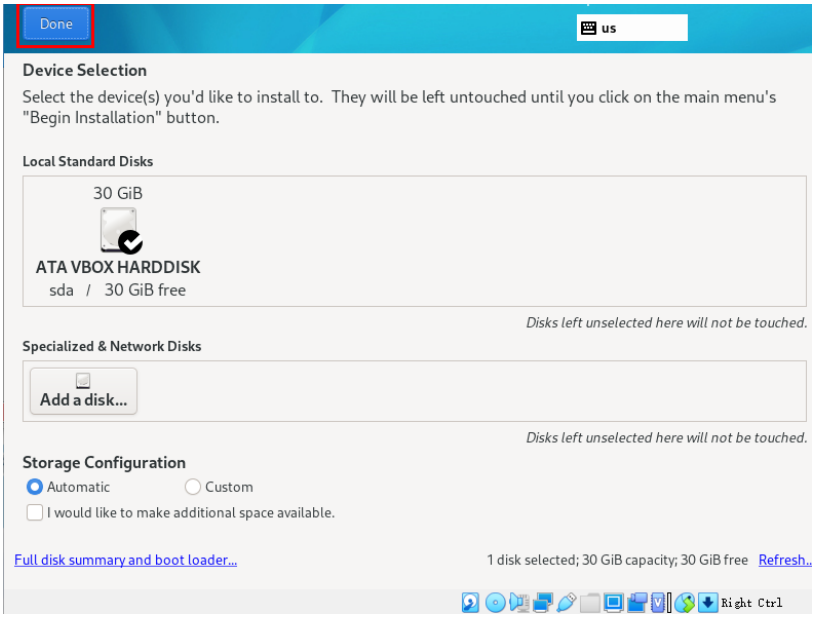


Figure 3-14 Selecting the installation destination

Step 7 Select **Network & Hostname** to configure the network.

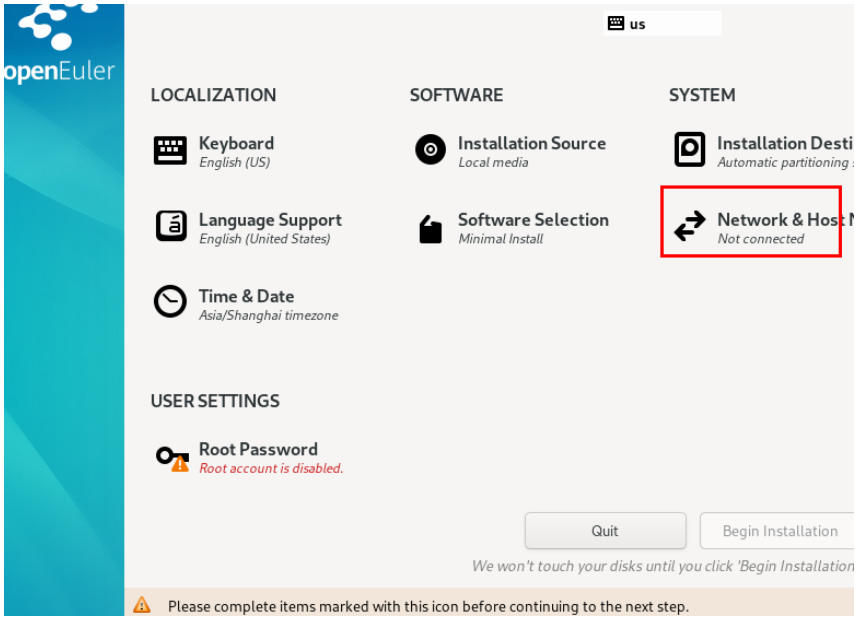


Figure 3-15 Configuring the network

Step 8 Enable the **enp0s3** network adapter and click **Done**. The main page is displayed.

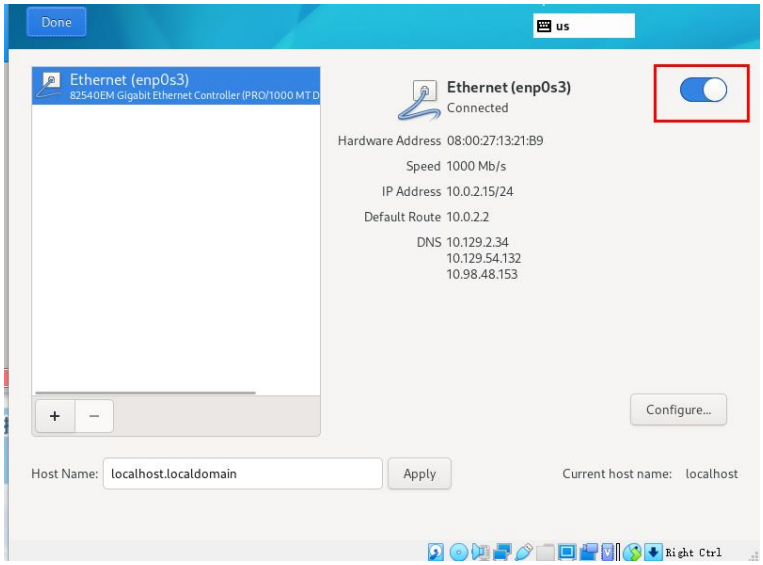


Figure 3-16 Configuring the network

Step 9 Select **Root Password** to configure the root password.

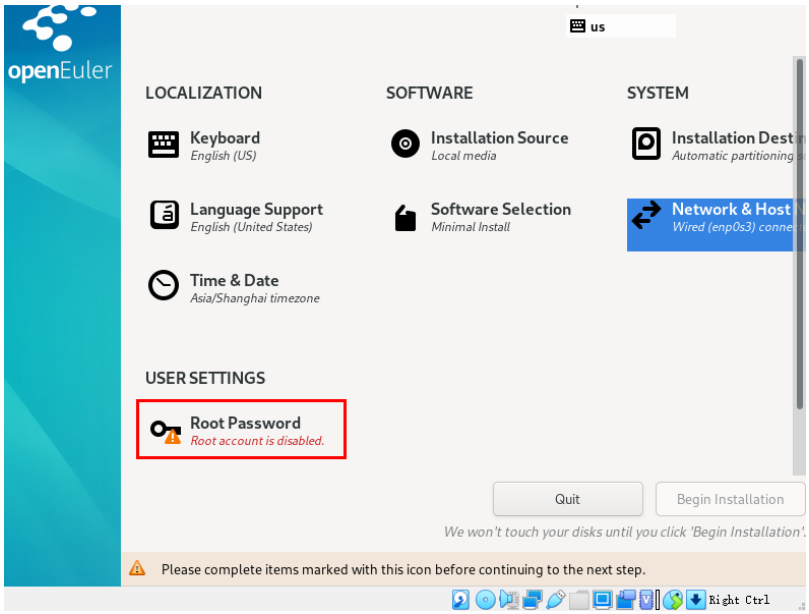


Figure 3-17 Configuring the root password

Step 10 Enter the root password, confirm the password, and click **Done**. The main page is displayed.

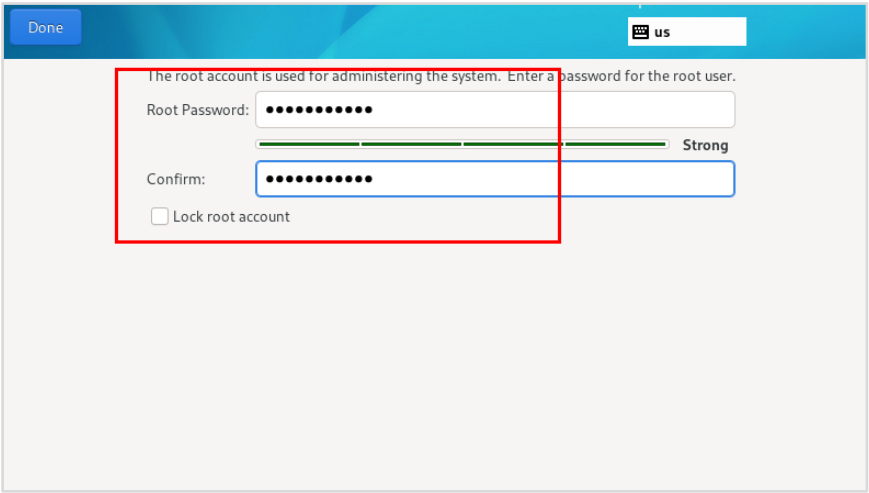


Figure 3-18 Configuring the root password

Step 11 Click **Begin Installation**.

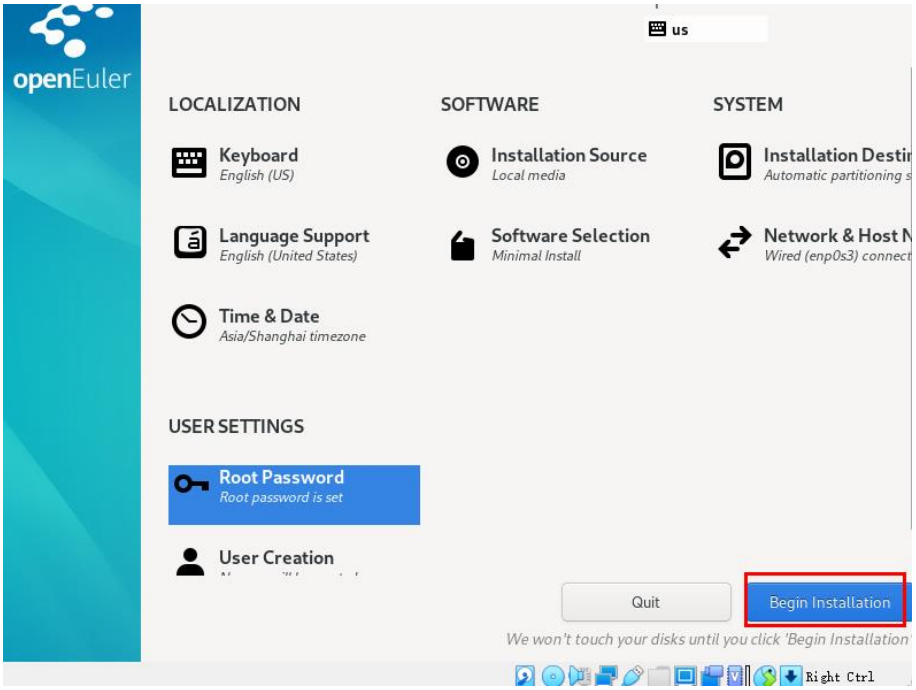


Figure 3-19 Beginning installation

Step 12 Click **Reboot System**.

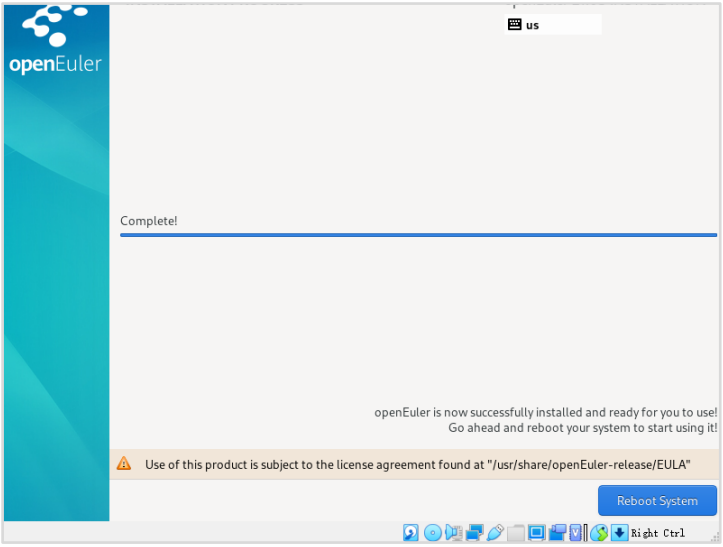


Figure 3-20 Completing installation

Step 13 Log in to the VM as user **root**.

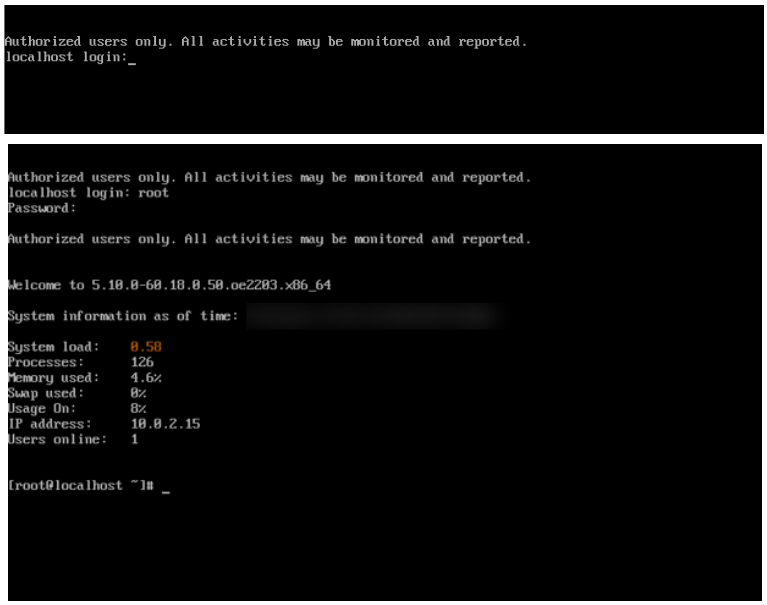


Figure 3-21 Logging in to the VM

3.3 Useful Commands

3.3.1 help

Step 1 Run the **help** command.

```
[root@localhost ~]# help pwd
pwd: pwd [-LP]
    Print the name of the current working directory.
```

```
      Options:
        -L          print the value of $PWD if it names the current working
                    directory
        -P          print the physical directory, without any symbolic links

      By default, `pwd' behaves as if `-L' were specified.

      Exit Status:
      Returns 0 unless an invalid option is given or the current directory
      cannot be read.
[root@localhost ~]# help -d pwd
pwd - Print the name of the current working directory.
[root@localhost ~]# help -s pwd
pwd: pwd [-LP]
```

3.3.2 Other Common Commands

Step 1 Run the **last** command to display the latest login information about the users.

```
[root@localhost ~]# last
root     pts/1        192.168.3.127    Thu May  5 10:41   still logged in
root     pts/0        192.168.3.113    Thu May  5 08:20   still logged in
root     tty1                          Thu May  5 08:19   still logged in
reboot   system boot  5.10.0-60.18.0.5 Thu May  5 08:13   still running
```

Step 2 Run the **history** command to view historical commands.

```
[root@localhost ~]# history
    1  ls -l
```

Step 3 Press **Tab** to complete the command.

When entering a command, you can press **Tab** to automatically complete the command or file path. For example, after you enter **wh** and press **Tab**, the following information is displayed:

```
[root@localhost ~]# wh
whatis    whereis   which     while     whiptail  who       whoami
```

Step 4 Run the **wget** command to download a file from a specified URL.

Note that the host on which you run the **wget** command must be able to access the Internet.

```
[root@localhost ~]# wget https://wordpress.org/latest.zip
```

3.4 bash Commands

3.4.1 Power Supply Control and User Switching

Step 1 Start the openEuler VM and log in to the VM as user **root**.

Step 2 Practice using the basic bash commands.

Run the **reboot** command to reboot openEuler.

```
[root@localhost ~]# reboot
```

After the reboot, log in to openEuler as user **root**.

Run the **logout** or **exit** command to log out.

```
[root@localhost ~]# logout
```

3.4.2 Basic Directory and File Operations

Step 1 Run the **pwd** command to view the current directory.

```
[root@localhost ~]# pwd
/root
[root@localhost ~]#
# The command output indicates that the current directory is the /root directory.
```

Step 2 Run the **ls** commands.

- View the files and directories in the current directory.

```
[root@localhost ~]# ls
anaconda-ks.cfg
[root@localhost ~]# ls .
anaconda-ks.cfg
# The command output indicates that the anaconda-ks.cfg file exists in the current directory.
```

- View the files and directories in the upper-level directory.

```
[root@localhost ~]# ls ..
afs   boot   etc    lib      lost+found   mnt   proc   run     srv   tmp   var
bin   dev    home   lib64    media        opt   root   sbin    sys   usr
```

- View the files and directories in the **/tmp** directory.

```
[root@localhost ~]# ls /tmp
systemd-private-6b5ec1dcc15141d0bf3edecae5a0c8ca-chronyd.service-ae8LHA
systemd-private-6b5ec1dcc15141d0bf3edecae5a0c8ca-systemd-logind.service-K97Nbh
```

- View all files and directories in the current directory.

```
[root@localhost ~]# ls -a
```

```
.    anaconda-ks.cfg   .bash_logout    .bashrc   .tcshrc
......
# The command output indicates that the current directory contains hidden files and directories.
```

- View detailed information about non-hidden files and directories in the current directory.

```
[root@localhost ~]#ls -l
total 4
-rw-------. 1 root root 1139 Jul   8 11:07 anaconda-ks.cfg
```

- View detailed information about all files and directories in the current directory.

```
[root@localhost ~]#ls -al
total 36
dr-xr-x---.   2 root root 4096 Jul   8 11:38 .
dr-xr-xr-x. 18 root root 4096 Jul   8 11:00 ..
-rw-------.   1 root root 1139 Jul   8 11:07 anaconda-ks.cfg
-rw-------.   1 root root   236 Jul   8 11:45 .bash_history
```

Step 3 Run the **cd** commands to switch to directories.

- Switch to the root directory of the system.

```
[root@localhost ~]# cd /
[root@localhost /]#
# Note that ~ changes to /.
```

- Switch to the **/etc/** directory.

```
[root@localhost /]# cd /etc
[root@localhost etc]#
```

- Use the relative path to switch to the **/etc/sysconfig/** directory.

```
[root@localhost etc]# cd sysconfig
[root@localhost sysconfig]#
```

- Use the absolute path to switch to the **/etc/sysconfig/** directory.

```
[root@localhost etc]# cd /etc/sysconfig
[root@localhost sysconfig]#
```

- Switch to the upper-level directory.

```
[root@localhost sysconfig]# cd ..
[root@localhost etc]#
```

- Switch to the home directory of the current user.

```
[root@localhost sysconfig]#cd
[root@localhost ~]#
```

- Switch to the previous directory.

```
[root@localhost sysconfig]# cd -
/etc
[root@localhost etc]#
```

- Switch to the home directory of the current user.

```
[root@localhost etc]#cd /etc/sysconfig
[root@localhost sysconfig]#cd ~
[root@localhost ~]#
```

Step 4 Run the **mkdir** commands to create directories.

- Create the **test1** directory in the current directory.

```
[root@localhost ~]# mkdir test1
[root@localhost ~]# ls
anaconda-ks.cfg   test1
```

- Create the **test2** directory using a relative path.

```
[root@localhost ~]# mkdir ./test2
[root@localhost ~]# ls
anaconda-ks.cfg   test1 test2
```

- Create the **test3** directory using an absolute path.

```
[root@localhost ~]# mkdir /root/test3
[root@localhost ~]# ls
anaconda-ks.cfg   test1 test2 test3
```

Step 5 Run the **touch** commands to create files.

Create the **huawei.txt** and **huawei1.txt** files.

```
[root@localhost ~]# cd test1
[root@localhost test1]# touch /root/test1/huawei.txt
[root@localhost test1]# touch huawei1.txt
[root@localhost test1]# ls
huawei.txt     huawei1.txt
```

Step 6 Run the **cp** commands to copy files.

- Copy **huawei.txt** to the **/root/test2** directory and name it **huawei.txt.bak**.

```
[root@localhost test1]# cp huawei.txt /root/test2/huawei.txt.bak
[root@localhost test1]# ls /root/test2
huawei.txt.bak
```

- Copy the **test1** directory to the **/root/test2** directory.

```
[root@localhost test1]# cp -r /root/test1 /root/test2/
```

```
[root@localhost test1]# ls /root/test2/
huawei.txt.bak test1
```

Step 7 Run the **rm** commands to delete files.

- Delete the **huawei.txt** file from the **/root/test1** directory.

```
[root@localhost test1]# rm huawei.txt
rm: Are you sure you want to delete the common empty file huawei.txt? y      # Enter y to confirm the deletion.
[root@localhost test1]# rm -f huawei1.txt                # -f forcibly deletes the file and does not display any message.
[root@localhost test1]# ls
[root@localhost test1]#
```

- Delete the **test1** directory from the **/root** directory.

```
[root@localhost test1]# cd
[root@localhost ~]# ls
anaconda-ks.cfg   test1   test2   test3
[root@localhost ~]# rmdir /root/test1      # Deletes an empty directory.
[root@localhost ~]# ls
anaconda-ks.cfg   test2   test3
[root@localhost ~]# mkdir /root/test1
[root@localhost ~]# touch /root/test1/huawei3.txt
[root@localhost ~]# rm -r /root/test1      # -r recursively deletes the directory and all files in the directory.
```

```
[root@localhost ~]# rm -r /root/test1
rm: descend into directory '/root/test1'? y
rm: remove regular empty file '/root/test1/huawei3.txt'? y
rm: remove directory '/root/test1'? y
```

Figure 3-22 Deleting files

Step 8 Run the **mv** command to move and rename a file.

Move the **huawei.txt.bak** file from the **/root/test2** directory to the **/root** directory and rename the file as **huawei.txt**.

```
[root@localhost ~]# mv /root/test2/huawei.txt.bak   ~/huawei.txt
[root@localhost ~]# ls
anaconda-ks.cfg   huawei.txt   test2   test3
```

3.5 File Viewing Commands

3.5.1 Viewing Files

Step 1 Copy the **/etc/passwd** file to the **/root** directory.

```
[root@localhost test3]# cd
[root@localhost ~]# cp /etc/passwd ~
```

Step 2 Run the **cat** command to view the content of a small text file.

View the content of the **passwd** file.

```
[root@localhost ~]# cat passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin
systemd-coredump:x:999:997:systemd Core Dumper:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
systemd-resolve:x:193:193:systemd Resolver:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
systemd-timesync:x:998:995:systemd Time Synchronization:/:/sbin/nologin
unbound:x:997:994:Unbound DNS resolver:/etc/unbound:/sbin/nologin
......
```

Step 3 Run the **head** commands to view the first several lines of a file.

- View the first 10 lines of the file by default.

```
[root@localhost ~]# head passwd                    # If no option is added to the head command, the
first 10 lines of the file are displayed by default.
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
```

- View the first five lines of the file.

```
[root@localhost ~]# head -n 5 passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
```

- View all content except the last 20 lines of the file.

```
[root@localhost etc]# head -n -20 passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
```

- View the first 10 bytes of the file.

```
[root@localhost ~]# head -c 10 passwd
root:x:0:0[root@localhost ~]#
```

Step 4 Run the **tail** commands to view the last several lines of a file.

- View the last 10 lines of the file by default.

```
[root@localhost etc]# tail passwd        # Similar to head, if no option is added to the head command,
the last 10 lines of the file are displayed by default.
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
chrony:x:995:992::/var/lib/chrony:/sbin/nologin
systemd-network:x:990:990:systemd Network Management:/:/usr/sbin/nologin
systemd-resolve:x:989:989:systemd Resolver:/:/usr/sbin/nologin
systemd-timesync:x:988:988:systemd Time Synchronization:/:/usr/sbin/nologin
gluster:x:987:987:GlusterFS daemons:/run/gluster:/sbin/nologin
radvd:x:75:75:radvd user:/:/sbin/nologin
qemu:x:107:107:qemu user:/:/sbin/nologin
dnsmasq:x:985:985:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin h
```

- View the last five lines of the file.

```
[root@localhost ~]# tail -n 5 passwd
```

- View the updated data in of a log file dynamically.

```
[root@localhost ~]# tail -f /var/log/messages
```

Step 5 Run the **less** command to view (and search) the file content of a large file.

View the file. Press the up and down arrow keys to navigate the lines; press the space bar to scroll one page forward; enter a slash (/) and a keyword to search for the keyword; and press **q** to exit.

```
[root@localhost ~]# less passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
```

```
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
...
```

Step 6 Run the **more** command to view (and search) the file content of a large file.

View the file. Press the space bar to scroll one page forward or exit when you reach the end of the file; enter a slash (/) and a keyword to search for the keyword; and press **q** to exit.

```
[root@localhost ~]# more passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
...
```

3.5.2 (Optional) Searching for Files

Step 1 Run the **find** commands.

- Search for the file named **passwd** in the **/etc** directory.

```
[root@localhost etc]# find /etc -name passwd
/etc/pam.d/passwd
/etc/passwd
```

- Search for files that belong to user **root** in the **/root** directory.

```
[root@localhost etc]# find /root -user root
/root
/root/bzip2-1.0.6.tar.gz
/root/bzip2-1.0.6
/root/bzip2-1.0.6/compress.o
/root/bzip2-1.0.6/libbz2.a
......
```

- Search for files larger than 512 KB in the **/etc** directory.

```
[root@localhost etc]# find /etc -size +512k
/etc/ima/digest_lists/0-metadata_list-rpm-python3-perf-5.10.0-60.18.0.50.oe2203.x86_64
/etc/ima/digest_lists/0-metadata_list-rpm-kernel-5.10.0-60.18.0.50.oe2203.x86_64
/etc/ima/digest_lists/0-metadata_list-rpm-kernel-tools-5.10.0-60.18.0.50.oe2203.x86_64
```

Step 2 Run the **whereis** command.

This command can only be used to find binary files, source code files, and man pages.

View the location of the **bash** command.

```
[root@localhost ~]# whereis bash
bash: /usr/bin/bash
```

3.6 Basic Operations on the Vim Text Editor

3.6.1 Normal Mode of Vim

3.6.1.1 Cursor Control

Step 1 Run the following command to verify that the VM can access the Internet. (Prepare the VM by referring to section 3.2 and ensure that the VM can access the Internet.)

```
[root@openEuler ~]# ping www.huawei.com
```

Step 2 Download the tutorial file.

```
[root@openEuler ~]# wget -c http://www.silecs.info/formations/Linux-TP-export/vimtutor-en.txt -O
vimtutor
```

Step 3 Run the following **vim** command to open the **vimtutor** file.

```
[root@openEuler ~]# vim vimtutor # Open the vimtutor file with vim. The tutorial home page is
displayed.
===============================================================================
=    W e l c o m e    t o    t h e    V I M    T u t o r    -    Version 1.7      =
===============================================================================
      Vim is a very powerful editor that has many commands, too many to
      explain in a tutor such as this.   This tutor is designed to describe
      enough of the commands that you will be able to easily use Vim as
      an all-purpose editor.
      The approximate time required to complete the tutor is 25-30 minutes,
      depending upon how much time is spent with experimentation.
      ATTENTION:
      The commands in the lessons will modify the text.   Make a copy of this
      file to practise on (if you started "vimtutor" this is already a copy).

      It is important to remember that this tutor is set up to teach by
      use.   That means that you need to execute the commands to learn them
      properly.   If you only read the text, you will forget the commands!
      Now, make sure that your Shift-Lock key is NOT depressed and press
      the    j    key enough times to move the cursor so that Lesson 1.1
      completely fills the screen.
~~~
```

```
                    Lesson 1.1:  MOVING THE CURSOR


  ** To move the cursor, press the h,j,k,l keys as indicated. **
           ^
           k                Hint:  The h key is at the left and moves left.
     < h       l >                 The l key is at the right and moves right.
           j                       The j key looks like a down arrow.
           v
  1. Move the cursor around the screen until you are comfortable.

  2. Hold down the down key (j) until it repeats.
     Now you know how to move to the next lesson.

  3. Using the down key, move to lesson 1.2.

NOTE: If you are ever unsure about something you typed, press <ESC> to place
      you in Normal mode.  Then retype the command you wanted.

NOTE: The cursor keys should also work.  But using hjkl you will be able to
      move around much faster, once you get used to it.  Really!

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Figure 3-23 Moving the cursor to view the document

Step 5 Press **Ctrl+D** to scroll one page forward; press **Ctrl+U** to scroll one page backward; press **k**, **j**, **h**, and **l** keys to move the cursor up, down, left, and right, respectively.

Step 6 Enter **gg** to move the cursor to the first line of the document; enter **G** to move the cursor to the last line of the document.

```
===============================================================================
=   W e l c o m e   t o   t h e   V I M   T u t o r   -   Version 1.7       =
===============================================================================

     Vim is a very powerful editor that has many commands, too many to
     explain in a tutor such as this.  This tutor is designed to describe
     enough of the commands that you will be able to easily use Vim as
     an all-purpose editor.

     The approximate time required to complete the tutor is 25-30 minutes,
     depending upon how much time is spent with experimentation.

     ATTENTION:
     The commands in the lessons will modify the text.  Make a copy of this
     file to practise on (if you started "vimtutor" this is already a copy).

     It is important to remember that this tutor is set up to teach by
```

Figure 3-24 Moving the cursor to view the document

```
This tutorial was written by Michael C. Pierce and Robert K. Ware,
Colorado School of Mines using ideas supplied by Charles Smith,
Colorado State University.  E-mail: bware@mines.colorado.edu.

Modified for Vim by Bram Moolenaar.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
                                                                 970,1         Bot
```

Figure 3-25 Moving the cursor to view the document

Step 7 Enter *n***gg** to move the cursor to line *n* of the document, for example, **10gg**.

```
===============================================================================
=   W e l c o m e   t o   t h e   V I M   T u t o r   -   Version 1.7      =
===============================================================================

    Vim is a very powerful editor that has many commands, too many to
    explain in a tutor such as this.  This tutor is designed to describe
    enough of the commands that you will be able to easily use Vim as
    an all-purpose editor.

    The approximate time required to complete the tutor is 25-30 minutes,
    depending upon how much time is spent with experimentation.

    ATTENTION:
    The commands in the lessons will modify the text.  Make a copy of this
    file to practise on (if you started "vimtutor" this is already a copy).

    It is important to remember that this tutor is set up to teach by
    use.  That means that you need to execute the commands to learn them
    properly.  If you only read the text, you will forget the commands!

    Now, make sure that your Shift-Lock key is NOT depressed and press
    the   j   key enough times to move the cursor so that Lesson 1.1
    completely fills the screen.
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
                        Lesson 1.1:  MOVING THE CURSOR
```

Figure 3-26 Moving the cursor to view the document

Step 8 Scroll down until you can see the full content of section 2.6, and then move the cursor to the second line starting with **--->**.

```
                        Lesson 2.6: OPERATING ON LINES


                    ** Type  dd   to delete a whole line. **

  Due to the frequency of whole line deletion, the designers of Vi decided
  it would be easier to simply type two d's to delete a line.

  1. Move the cursor to the second line in the phrase below.
  2. Type  dd  to delete the line.
  3. Now move to the fourth line.
  4. Type   2dd   to delete two lines.

--->  1)  Roses are red,
--->  2)  Mud is fun,
--->  3)  Violets are blue,
--->  4)  I have a car,
--->  5)  Clocks tell time,
--->  6)  Sugar is sweet
--->  7)  And so are you.
```

Figure 3-27 Moving the cursor to view the document

3.6.1.2 Quick Deletion

Step 1 Enter **dd** to delete the line.

```
--->  1)  Roses are red,
--->  3)  Violets are blue,
--->  4)  I have a car,
--->  5)  Clocks tell time,
--->  6)  Sugar is sweet
--->  7)  And so are you.
```

Figure 3-28 Deleting a line

Step 2 Move the cursor to line 4 and enter **2dd** to delete lines 4 and 5.

3.6.1.3 Copying and Pasting

Step 1 Move the cursor down to the third line of section 2.7, and then enter **yy** to copy the line.

```
                    Lesson 2.7: THE UNDO COMMAND


 ** Press  u  to undo the last commands,   U  to fix a whole line. **

1. Move the cursor to the line below marked ---> and place it on the
   first error.
2. Type  x  to delete the first unwanted character.
3. Now type  u  to undo the last command executed.
4. This time fix all the errors on the line using the  x  command.
5. Now type a capital  U  to return the line to its original state.
6. Now type  u  a few times to undo the  U  and preceding commands.
7. Now type CTRL-R (keeping CTRL key pressed while hitting R) a few times
   to redo the commands (undo the undo's).
```

Figure 3-29 Copying a line

Step 2 Enter **p** to paste the copied content to the current line.

```
                    Lesson 2.7: THE UNDO COMMAND


 ** Press  u  to undo the last commands,   U  to fix a whole line. **

1. Move the cursor to the line below marked ---> and place it on the
   first error.
2. Type  x  to delete the first unwanted character.
3. Now type  u  to undo the last command executed.
3. Now type  u  to undo the last command executed.
4. This time fix all the errors on the line using the  x  command.
5. Now type a capital  U  to return the line to its original state.
6. Now type  u  a few times to undo the  U  and preceding commands.
7. Now type CTRL-R (keeping CTRL key pressed while hitting R) a few times
   to redo the commands (undo the undo's).
```

Figure 3-30 Pasting the copied content

Step 3 Move the cursor to **5**, and then enter **P** to paste the copied content above the current line.

```
                    Lesson 2.7: THE UNDO COMMAND


 ** Press  u  to undo the last commands,   U  to fix a whole line. **

1. Move the cursor to the line below marked ---> and place it on the
   first error.
2. Type  x  to delete the first unwanted character.
3. Now type  u  to undo the last command executed.
3. Now type  u  to undo the last command executed.
4. This time fix all the errors on the line using the  x  command.
3. Now type  u  to undo the last command executed.
5. Now type a capital  U  to return the line to its original state.
6. Now type  u  a few times to undo the  U  and preceding commands.
7. Now type CTRL-R (keeping CTRL key pressed while hitting R) a few times
   to redo the commands (undo the undo's).
```

Figure 3-31 Pasting the copied content

3.6.1.4 Undoing

Step 1 Enter **u** twice to undo the paste operations.

```
                    Lesson 2.7: THE UNDO COMMAND


 ** Press  u  to undo the last commands,   U  to fix a whole line. **

1. Move the cursor to the line below marked ---> and place it on the
   first error.
2. Type  x  to delete the first unwanted character.
3. Now type  u  to undo the last command executed.
4. This time fix all the errors on the line using the  x  command.
5. Now type a capital  U  to return the line to its original state.
6. Now type  u  a few times to undo the  U  and preceding commands.
7. Now type CTRL-R (keeping CTRL key pressed while hitting R) a few times
   to redo the commands (undo the undo's).

--> Fiix the errors oon thhis line and reeplace them witth undo.
```

Figure 3-32 Undoing

3.6.2 Insert Mode of Vim

3.6.2.1 Deleting Text

Step 1 Run the following command to open **vimtutor** again.

```
[root@openEuler ~]# vimtutor
```

Step 2 Move the cursor down until you can see the full content of section 1.3.

```
                    Lesson 1.3: TEXT EDITING - DELETION


          ** Press  x  to delete the character under the cursor. **

  1. Move the cursor to the line below marked --->.

  2. To fix the errors, move the cursor until it is on top of the
     character to be deleted.

  3. Press the  x  key to delete the unwanted character.

  4. Repeat steps 2 through 4 until the sentence is correct.

---> The ccow jumpedd ovverr thhe mooon.

  5. Now that the line is correct, go on to lesson 1.4.

NOTE: As you go through this tutor, do not try to memorize, learn by usage.


~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Figure 3-33 Moving the cursor to view the content

Step 3 Move the cursor to the unwanted **c** in the line starting with **--->**, and then press **x** to delete the character.

```
                    Lesson 1.3: TEXT EDITING - DELETION


          ** Press  x  to delete the character under the cursor. **

  1. Move the cursor to the line below marked --->.

  2. To fix the errors, move the cursor until it is on top of the
     character to be deleted.

  3. Press the  x  key to delete the unwanted character.

  4. Repeat steps 2 through 4 until the sentence is correct.

---> The ccow jumpedd ovverr thhe mooon.

  5. Now that the line is correct, go on to lesson 1.4.

NOTE: As you go through this tutor, do not try to memorize, learn by usage.



~~~
```

Figure 3-36 Moving the cursor to view the content

Step 2 Move the cursor to **text** in the first line starting with **--->**, and then press **i** to enter the insert mode.

```
                    Lesson 1.4: TEXT EDITING - INSERTION


                      ** Press  i  to insert text. **

  1. Move the cursor to the first line below marked --->.

  2. To make the first line the same as the second, move the cursor on top
     of the first character AFTER where the text is to be inserted.

  3. Press  i  and type in the necessary additions.

  4. As each error is fixed press <ESC> to return to Normal mode.
     Repeat steps 2 through 4 to correct the sentence.

---> There is text misng this .
---> There is some text missing from this line.

  5. When you are comfortable inserting text move to lesson 1.5.



~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
-- INSERT --
```

Figure 3-37 Insert mode

Step 3 Enter the missing word **some** by referring to the line below.

```
---> There is some text misng this .
---> There is some text missing from this line.
```

Figure 3-38 Inserting content

Step 4 Move the cursor and enter other missing characters to make the first line the same as the second. Press **Esc** to exit the insert mode and return to the normal mode.

```
---> There is some text missing from this line.
---> There is some text missing from this line.
```

Figure 3-39 Returning to the normal mode

Step 5 Move the cursor to the end of the first line starting with **--->**, enter **o** to insert a line below the current line, and enter **Add the first line here.**.

```
---> There is some text missing from this line.
Add the first line here.
---> There is some text missing from this line.
```

Figure 3-40 Inserting a line

Step 6 Move the cursor to the end of the second line starting with **--->**, enter **O** to insert a line above the current line, and enter **Add the second line here.**.

```
---> There is some text missing from this line.
Add the first line here.
Add the second line here.
---> There is some text missing from this line.
```

Figure 3-41 Inserting a line

3.6.3 Command Line Mode of Vim

Step 1 Move the cursor down until you can see the full content of section 1.2.

```
                    Lesson 1.2: EXITING VIM


  !! NOTE: Before executing any of the steps below, read this entire lesson!!

  1. Press the <ESC> key (to make sure you are in Normal mode).

  2. Type:      :q! <ENTER>.
     This exits the editor, DISCARDING any changes you have made.

  3. Get back here by executing the command that got you into this tutor. That
     might be:  vimtutor <ENTER>

  4. If you have these steps memorized and are confident, execute steps
     1 through 3 to exit and re-enter the editor.

NOTE:  :q! <ENTER>  discards any changes you made.  In a few lessons you
       will learn how to save the changes to a file.

  5. Move the cursor down to lesson 1.3.


~~~
```

Figure 3-43 Forcible exit

Step 3 Enter **:wq** and press **Enter** to save and exit the tutorial.

```
:wq
```

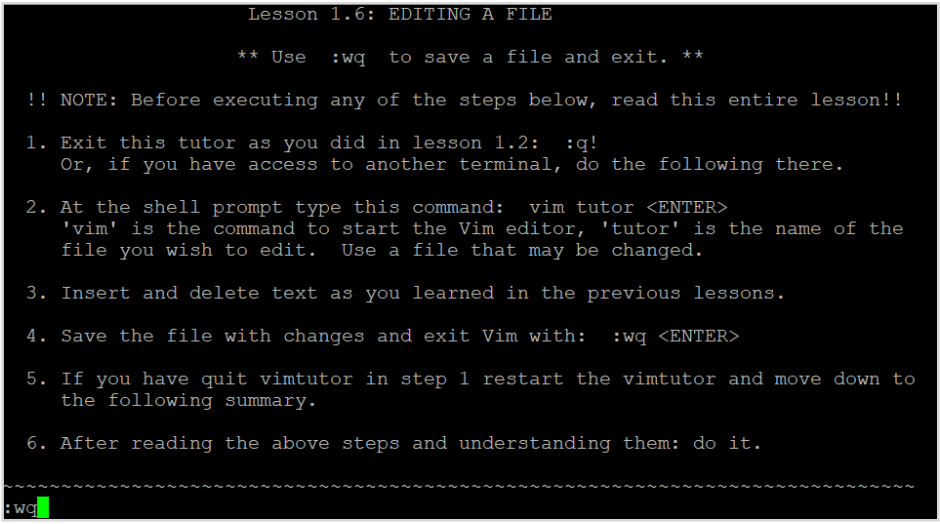


Figure 3-44 Save and exit

Step 4 Run the **%s/Lesson/Class/g** command to replace all occurrences of **Lesson** in the file with **Class**.

```
:%s/Lesson/Class/g
```

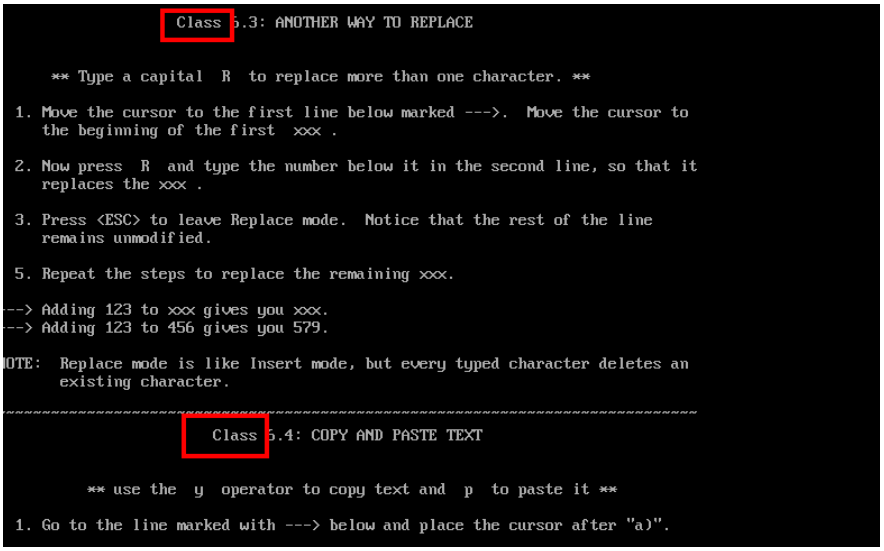


Figure 3-45 Replacing characters

3.7 openEuler System and User Management

3.7.1 Network Management

3.7.1.1 Host Name Management

Step 1 View the host name.

```
[root@localhost ~]# hostname
localhost.localdomain
[root@localhost ~]# cat /etc/hostname   # View the host name configuration file.
localhost.localdomain
```

Step 2 Change the host name temporarily.

```
[root@localhost ~]# hostname huawei   # Change the host name temporarily. The change becomes
invalid after a restart.
[root@localhost ~]# hostname
huawei
[root@localhost ~]# bash   # Start a new session.
Welcome to 5.10.0-60.18.0.50.oe2203.x86_64
System information as of time: system_time
System load:      0.16
Processes:        129
Memory used:      3.7%
Swap used:        0%
Usage On:         23%
IP address:       10.0.2.15
Users online:     3
[root@huawei ~]#                          # In the command prompt, the host name is changed to
huawei.
[root@huawei ~]# exit
exit
[root@localhost ~]#
```

Step 3 Change the host name permanently.

```
Method 1:
[root@localhost ~]# hostnamectl set-hostname openEuler       # This method requires a re-login
instead of a restart.
Method 2:
[root@localhost ~]# vim /etc/hostname
#Change the host name in the file, save the change, and exit. The host name is changed after the
system is restarted.
[root@localhost ~]# reboot
```

3.7.1.2 Network Management

Step 1 Run the **ip** command to add a temporary IP address to the network adapter.

```
[root@openEuler ~]# ip addr show
```

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen
1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
qlen 1000
    link/ether 08:00:27:a5:05:8a brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
        valid_lft 83814sec preferred_lft 83814sec
    inet6 fe80::e2e1:a18b:f73a:d89e/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[root@openEuler ~]# ip addr add 192.168.110.100/24 dev enp0s3
[root@openEuler ~]# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen
1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
qlen 1000
    link/ether 08:00:27:a5:05:8a brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
        valid_lft 83599sec preferred_lft 83599sec
    inet 192.168.110.100/24 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::e2e1:a18b:f73a:d89e/64 scope link noprefixroute
```

Step 2 Run the **ip** command to delete the temporary IP address of the network adapter.

```
[root@openEuler ~]# ip addr del 192.168.110.100/24 dev enp0s3
[root@openEuler ~]# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen
1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
qlen 1000
    link/ether 08:00:27:a5:05:8a brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
        valid_lft 83814sec preferred_lft 83814sec
    inet6 fe80::e2e1:a18b:f73a:d89e/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Step 3 Configure a static route.

Set a static route to network range 192.168.2.0/24, with the next hop being the gateway.

```
[root@openEuler ~]# ip route
default via 10.0.2.2 dev enp0s3 proto dhcp metric 100
default via 192.168.3.1 dev enp0s8 proto dhcp metric 101
10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.15 metric 100
[root@openEuler ~]# ip route add 192.168.2.0/24 via 10.0.2.254 dev enp0s3
[root@openEuler ~]# ip route
default via 10.0.2.2 dev enp0s3 proto dhcp metric 100
default via 192.168.3.1 dev enp0s8 proto dhcp metric 101
10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.15 metric 100
192.168.2.0/24 via 10.0.2.15 dev enp0s3
```

Step 4 Use the **nmcli** command to create a network connection and apply it to an interface of the host:

- View the current NetworkManager status.

```
[root@openEuler ~]# nmcli general status
STATE        CONNECTIVITY   WIFI-HW   WIFI      WWAN-HW   WWAN
connected    full           enabled   enabled   enabled   enabled
```

```
[root@openEuler ~]# nmcli general status
STATE        CONNECTIVITY   WIFI-HW   WIFI      WWAN-HW   WWAN
connected    full           enabled   enabled   enabled   enabled
```

Figure 3-46 Viewing network connections

- View the current connections.

```
[root@openEuler ~]# nmcli connection show
NAME          UUID                                   TYPE       DEVICE
enp0s3        2c2c3fe1-67e0-417d-be50-c7f2ef1d890b   ethernet   enp0s3
enp0s8        233d807e-9a81-4f5d-bce4-837fd69ea526   ethernet   enp0s8
virbr0        37fb512e-e88d-4f19-a6a1-fdb02c633ea2   bridge     virbr0
net-static    e4c1c576-7a43-4838-96da-321fc76e91b2   ethernet   --
```

```
[root@openEuler ~]# nmcli connection show
NAME          UUID                                   TYPE       DEVICE
enp0s3        2c2c3fe1-67e0-417d-be50-c7f2ef1d890b   ethernet   enp0s3
enp0s8        233d807e-9a81-4f5d-bce4-837fd69ea526   ethernet   enp0s8
virbr0        37fb512e-e88d-4f19-a6a1-fdb02c633ea2   bridge     virbr0
net-static    e4c1c576-7a43-4838-96da-321fc76e91b2   ethernet   --
```

Figure 3-47 Viewing connections

- View the status of the network devices.

```
[root@openEuler ~]# nmcli device status
DEVICE       TYPE       STATE        CONNECTION
enp0s3       ethernet   connected    enp0s3
......
```

```
[root@openEuler ~]# nmcli device status
DEVICE      TYPE      STATE                   CONNECTION
enp0s3      ethernet  connected               enp0s3
enp0s8      ethernet  connected               enp0s8
virbr0      bridge    connected (externally)  virbr0
lo          loopback  unmanaged               --
virbr0-nic  tun       unmanaged               --
```

Figure 3-48 Viewing network devices

- Create a new network connection **net-static** and apply it to an interface of the host.

```
[root@openEuler ~]# nmcli con add type ethernet con-name net-static ifname enp0s3 ip4
192.168.110.10/24 gw4 192.168.110.254
#  conn indicates that the operation is performed on a connection.
#  add adds (a connection).
#  type indicates the type of the connection.
#  con-name indicates the connection name.
#  ifname indicates the name of the network adapter.
[root@openEuler ~]# nmcli connection show
```

```
[root@openEuler ~]# nmcli connection show
NAME        UUID                                  TYPE      DEVICE
enp0s8      233d807e-9a81-4f5d-bce4-837fd69ea526  ethernet  enp0s8
enp0s3      2c2c3fe1-67e0-417d-be50-c7f2ef1d890b  ethernet  enp0s3
virbr0      37fb512e-e88d-4f19-a6a1-fdb02c633ea2  bridge    virbr0
net-static  e4c1c576-7a43-4838-96da-321fc76e91b2  ethernet  --
```

Figure 3-49 Viewing network connections

- Enable the created network connection **net-static**.

```
[root@openEuler ~]# nmcli con up net-static ifname enp0s3
[root@openEuler ~]# nmcli connection show
```

```
[root@openEuler ~]# nmcli connection show
NAME        UUID                                  TYPE      DEVICE
enp0s8      233d807e-9a81-4f5d-bce4-837fd69ea526  ethernet  enp0s8
net-static  e4c1c576-7a43-4838-96da-321fc76e91b2  ethernet  enp0s3
virbr0      37fb512e-e88d-4f19-a6a1-fdb02c633ea2  bridge    virbr0
```

Figure 3-50 Viewing network connections

```
[root@openEuler ~]# nmcli con down net-static              # Disable the connection.
```

Step 5 Use the **nmcli** command to configure a static route.

```
[root@openEuler ~]# nmcli connection modify enp0s3 +ipv4.routes "192.168.100.0/24 10.0.15.254"
```

Step 6 Change the host IP address using the configuration file of the ifcfg-enp0s3 network adapter.

```
[root@openEuler ~]# cat /etc/sysconfig/network-scripts/ifcfg-enp0s3
TYPE=Ethernet            # Interface type
PROXY_METHOD=none        # Method for proxy configuration
BROWSER_ONLY=no          # Whether the proxy configuration is for browser only
BOOTPROTO=dhcp           # Boot-time protocol
```

```
DEFROUTE=yes            # Whether to assign the default route to this interface
IPV4_FAILURE_FATAL=no         # Whether to disable this interface if the IPv4 configuration fails
IPV6INIT=yes            # Whether to initialize IPv6
IPV6_AUTOCONF=yes           # Whether to configure IPv6 automatically
IPV6_DEFROUTE=yes           # Whether to assign the default IPv6 route to this interface
IPV6_FAILURE_FATAL=no         # Whether to disable this interface if the IPv6 configuration fails
IPV6_ADDR_GEN_MODE=stable-privacy     # IPv6 address generation mode
NAME=enp0s3             # Name of the network connection
UUID=2c2c3fe1-67e0-417d-be50-c7f2ef1d890b # UUID of the devcie
ONBOOT=yes              # Whether to start this interface with the system
DEVICE=enp0s3           # Name of the physical device
```

- When configuring the network, change **dhcp** to **static** or **none** and add the following information:

```
IPADDR=192.168.110.11
NETMASK=255.255.255.0
GATEWAY=192.168.110.254
```

- Run the following commands for the configuration to take effect.

```
[root@openEuler ~]# ifdown enp0s3
[root@openEuler ~]# ifup enp0s3
```

Step 7 Edit **/etc/hosts**.

```
[root@openEuler ~]# vim /etc/hosts      # The hosts file records the mapping between host names
and IP addresses for quick domain name resolution. Add the following information to the end of the
file:
192.168.110.11   server         # After adding this line, save the file and exit.
[root@openEuler ~]# ping server -c 3
PING server (192.168.110.11) 56(84) bytes of data.
64 bytes from server (192.168.110.11): icmp_seq=1 ttl=40 time=53.3 ms
64 bytes from server (192.168.110.11): icmp_seq=2 ttl=40 time=51.3 ms

--- server ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 51.288/52.351/53.338/0.838 ms
```

3.7.2 Service Management

Step 1 View the current services.

```
[root@openEuler ~]#   systemctl list-units --type service
UNIT                    LOAD      ACTIVE   SUB        DESCRIPTION
atd.service               loaded active   running   Deferred execution scheduler
auditd.service            loaded   active   running   Security Auditing Service
chronyd.service         loaded   active   running   NTP client/server
crond.service           loaded   active   running   Command Scheduler
dbus.service            loaded   active   running   D-Bus System Message Bus
dkms.service         loaded   active   exited    Builds and install new kernel modules throug
dracut-shutdown.service      loaded   active   exited    ROceanstor eStore /run/initramfs on shutdown
firewalld.service           loaded   active   running   firewalld - dynamic firewall daemon
```

```
getty@tty1.service        loaded   active   running   Getty on tty1
gssproxy.service          loaded   active   running   GSSAPI Proxy Daemon
hwclock-save.service      loaded   active   exited    Update RTC With System Clock
```

Step 2 View the status of a service, for example, the firewall service.

```
[root@openEuler ~]# systemctl status firewalld.service      # View the service status.
○ firewalld.service - firewalld - dynamic firewall daemon
     Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled; vendor preset: enabled)
     Active: inactive (dead)
       Docs: man:firewalld(1)
[root@openEuler ~]# systemctl is-active firewalld.service            # Check whether the service is
running.
active
[root@openEuler ~]# systemctl is-enabled firewalld.service   # Check whether the service is enabled.
enabled
```

Step 3 Terminate a service, such as the firewall service.

```
[root@openEuler ~]# systemctl stop firewalld.service
[root@openEuler ~]# systemctl is-active firewalld.service
inactive
```

Step 4 Restart a service, for example, the firewall service.

```
[root@openEuler ~]# systemctl restart firewalld.service
[root@openEuler ~]# systemctl is-active firewalld.service
active
```

Step 5 Disable a service, for example, the firewall service.

```
[root@openEuler ~]# systemctl disable firewalld.service
Removed /etc/systemd/system/multi-user.target.wants/firewalld.service.
Removed /etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service.
[root@openEuler ~]# systemctl is-enabled firewalld.service
disabled
```

Step 6 Enable a service, for example, the firewall service.

```
[root@openEuler ~]# systemctl enable firewalld.service
Created symlink /etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service →
/usr/lib/systemd/system/firewalld.service.
Created symlink /etc/systemd/system/multi-user.target.wants/firewalld.service →
/usr/lib/systemd/system/firewalld.service.
[root@openEuler ~]# systemctl is-enabled firewalld.service
enabled
```

3.7.3 User Management

Step 1 Use the **id** command to view the ID of a user and the ID of the group to which the user belongs.

```
[root@localhost ~]# id
uid=0(root) gid=0(root) groups=0(root)
```

Step 2 Log in to the system as user **root**, create users **tom**, **bob**, and **jack**, and set the UID of **jack** to 1024.

```
[root@localhost ~]# useradd tom
[root@localhost ~]# useradd bob
[root@localhost ~]# useradd -u 1024 jack
[root@localhost ~]# tail -3 /etc/passwd
tom:x:1001:1001::/home/tom:/bin/bash
bob:x:1002:1002::/home/bob:/bin/bash
jack:x:1024:1024::/home/jack:/bin/bash
[root@localhost ~]# useradd -d /home/myd bob1        # Use the -d parameter to specify the home
directory for the new user.
```

Step 3 Change the home directory of **tom** to **/home/tony**.

```
[root@localhost ~]# usermod -md /home/tony/ tom
# m and d are often used together to specify the home directory of a user.
[root@openEuler ~]# tail -4 /etc/passwd
tom:x:1000:1000::/home/tony/:/bin/bash
bob:x:1001:1001::/home/bob:/bin/bash
jack:x:1024:1024::/home/jack:/bin/bash
bob1:x:1025:1025::/home/myd:/bin/bash
```

Step 4 Delete user **bob** and its home directory.

```
[root@localhost ~]# userdel -r bob                    # Use the -r parameter to delete the user's
home directory.
[root@openEuler ~]# tail -3 /etc/passwd
tom:x:1000:1000::/home/tony/:/bin/bash
jack:x:1024:1024::/home/jack:/bin/bash
bob1:x:1025:1025::/home/myd:/bin/bash
```

Note: The command output shows the last three lines of the user configuration file. You can see that user **bob** does not exist.

The **bob** directory does not exist in the **/home** directory.

```
[root@openEuler ~]# ls /home/
jack   myd   tony
```

Step 5 Use the **su** command to switch users.

Switch from the current user (**root**) to **jack** on the terminal.

```
[root@openEuler ~]# su jack
[root@openEuler root]$ pwd
/root
[root@openEuler root]$ exit
exit
[root@openEuler ~]# su - jack
```

```
[root@openEuler ~]$ pwd
/home/jack
[root@openEuler ~]$ exit
```

3.8 Quiz

On Linux, how do we view the updated contents of a log file in real time?

Answer:

Run the **tail -f /var/log/XX/file.log** command to view the updated data of the log file.

4 KVM Installation and Resources Provisioning

4.1 Overview

4.1.1 About This Exercise

In this lab, bridged networks and NAT networks are configured to enable the communication between VMs and external networks. This lab introduces two network modes (NAT and bridge) in KVM virtualization to help trainees understand the basic principles of communication between VMs and external networks. A computer with at least 4 cores and 8 GB memory is recommended.

4.1.2 Objectives

- Understand the basic principles of KVM virtualization.
- Grasp the creation and process of KVM.
- Grasp the features and configuration method of bridged networks and NAT networks.

4.1.3 Lab Networking

4.1.3.1 Lab Environment Overview

- In this lab, the host VM is created using Oracle VM VirtualBox Manager (VirtualBox), and the lab VM is created using KVM virtualization on the host VM.
- In this lab, two physical interfaces are planned for the host VM: management interface (enp0s8) and service interface (enp0s3). The service interface is configured to NAT networks and the management interface is configured to bridged network and is used for remote access using virtual network console (VNC) or Secure Shell (SSH).
- In this lab, the type of the **default** network and the **test** network are NAT.
- In this lab, **virbr0** is the default bridge, and **virbr1** and **virbr2** are new bridges.
- In this lab, VMs access the Internet through NAT and bridged networks.

4.1.3.2 NAT Networks

- VM 01 is the lab VM.
- You need to create VM 01 and modify its network in this lab.

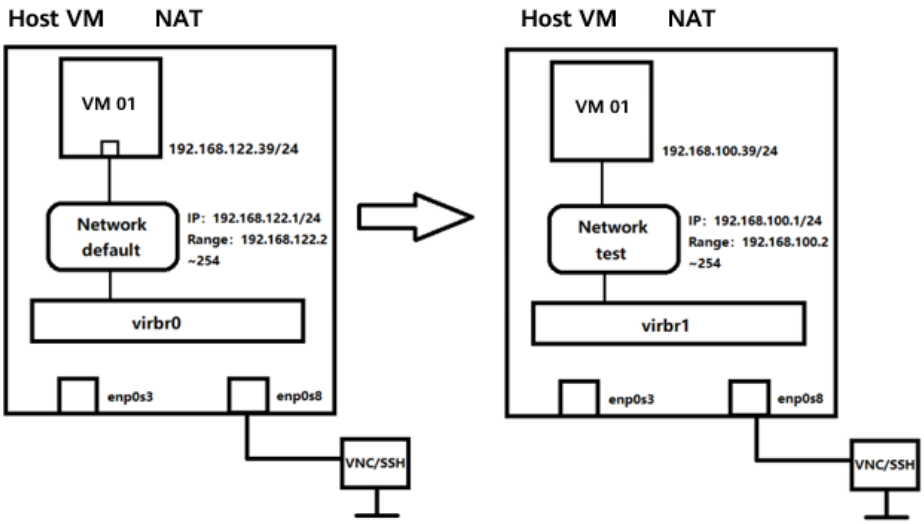


Figure 4-1 Lab Networking of NAT networks

4.1.3.3 Bridged Networks

- VM 02 is the lab VM.
- You need to create VM 02 using bridges in this lab.

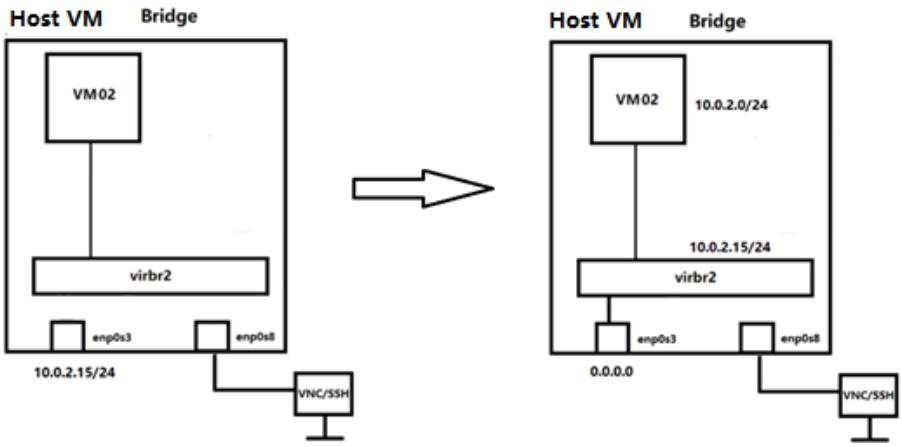


Figure 4-2 Lab networking of bridged networks

4.1.4 Exercise Planning

Table 4-1 Host VM port and parameter design

Device	Port	Connection Method	IP Address
Host VM	NIC 1 (enp0s3)	NAT	10.0.2.0/24 (service)
	NIC 2 (enp0s8)	Bridge	192.168.3.0/24 (management)

Table 4-2 Host VM bridge and parameter design

Device	Network Bridge	IP Address	Physical Interface
Host VM	virbr0	192.168.122.1/24	None
	virbr1	192.168.100.1/24	None
	virbr2	10.0.2.15/24	enp0s3

4.2 Exercise Configuration

4.2.1 Guideline

- Creating a host VM
  1. Select the connection methods of ports, compute and storage resources, and enable the corresponding virtualization features as planned.
  2. Import the image file and install the operating system (OS).
- Preparing the lab
  1. Use a terminal tool to log in to the host VM and disable services such as the firewall service.
  2. Install virtualization components and check their statuses.
  3. Download the OS image file to the local host VM for backup.
- Creating a VM using NAT
  1. Specify **default** to create VM 01 and install the OS on VM 01.
  2. Log in to VM 01, view its IP address, test its connectivity with external networks, and verify the NAT network.
- Changing the network information of VM 01.
  1. Create **test** using NAT, change the network of VM 01 to **test**, and reboot VM 01.

2. Log in to VM 01, view the new IP address allocated by **test**, and verify its connectivity with external networks.

- Create a VM using bridges
  1. Create **virbr2**, bind the planned physical service port **enp0s3**, and assign the IP address of the original physical port to **virbr2**.
  2. Specify **virbr2** to create VM 02 and install the operating system on VM 02. Log in to VM 02, view its IP address, test the connectivity between VM 02 and the host VM or external networks, and verify the bridged network.

4.2.2 Procedure

4.2.2.1 Creating a Host VM

Step 1 Run Oracle VM VirtualBox Manager and click **New** to create a VM.

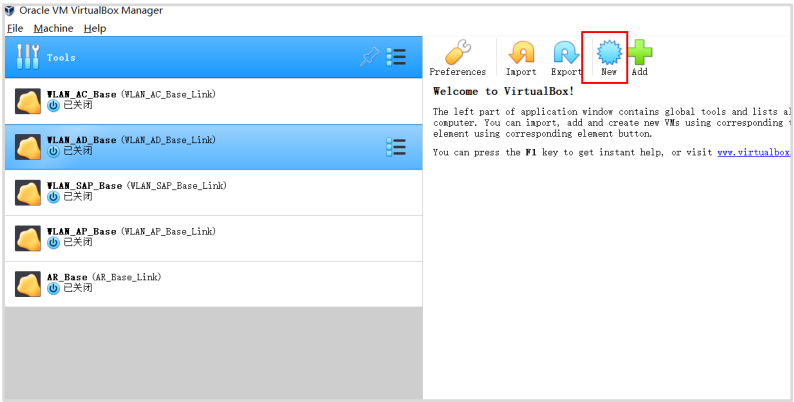


Figure 4-3 Creating a VM

Step 2 Enter the VM name, select the OS type and version, and click **Next**.

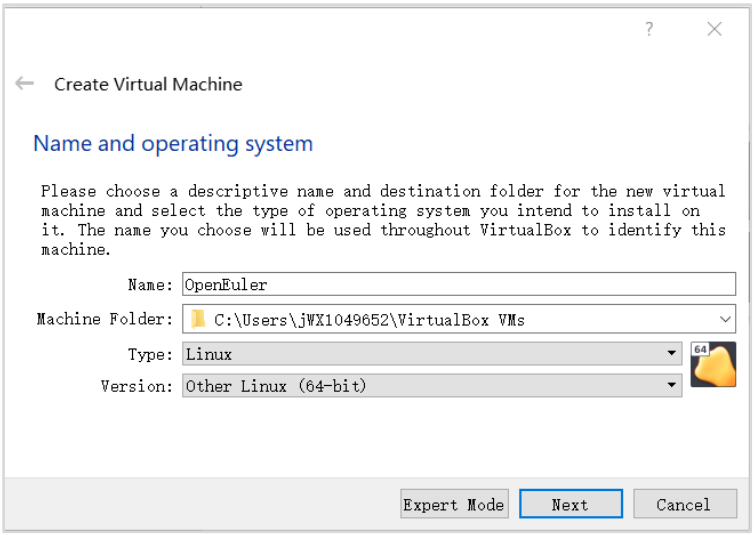


Figure 4-4 Configuring the VM name and OS type

Step 3 Select the memory size and click **Next**. (You are advised to select 4,096 MB.)

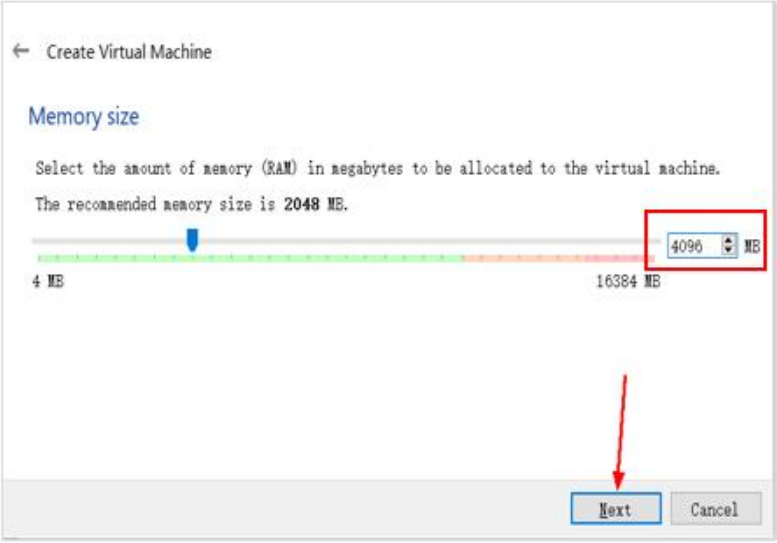


Figure 4-5 Configuring memory

Step 4 Select **Create a virtual hard disk now** and click **Create**.

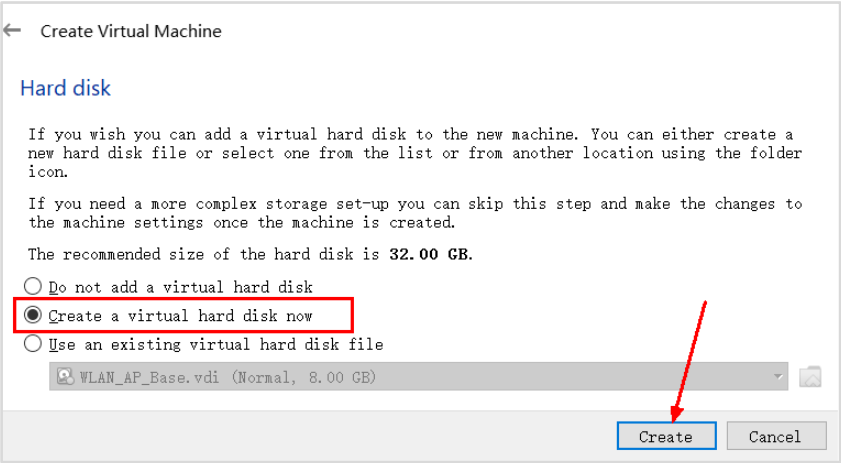


Figure 4-6 Creating a virtual hard disk

Step 5 Select **VHD (Virtual Hard Disk)** and click **Next**.

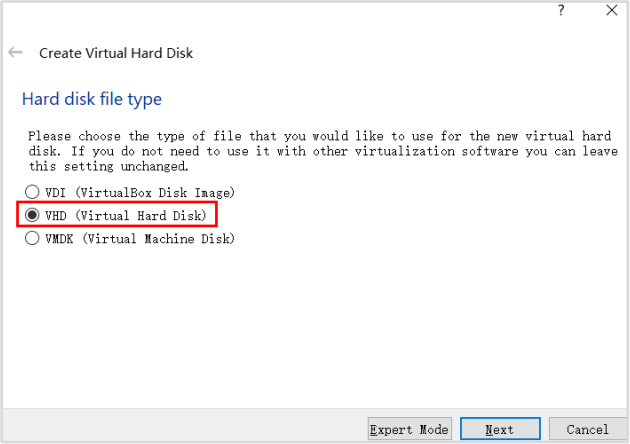


Figure 4-7 Configuring the virtual hard disk

Step 6 Select the size of the disk and click **Next**. (You are advised to select 30 GB.)

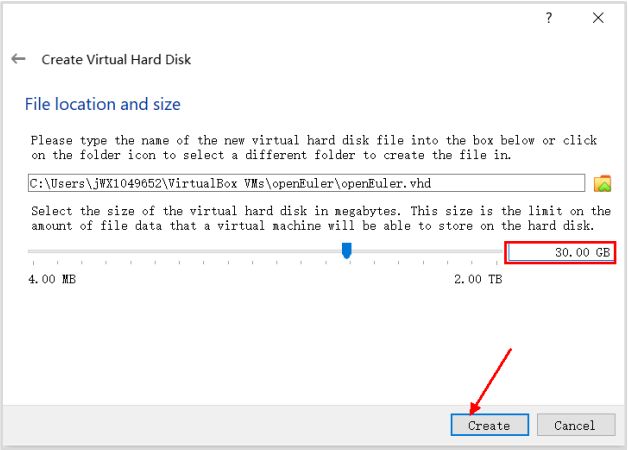


Figure 4-8 Selecting the location and size of the virtual hard disk

Step 7 On the main page of the software, click the created VM (**openEuler**) and **Settings**.

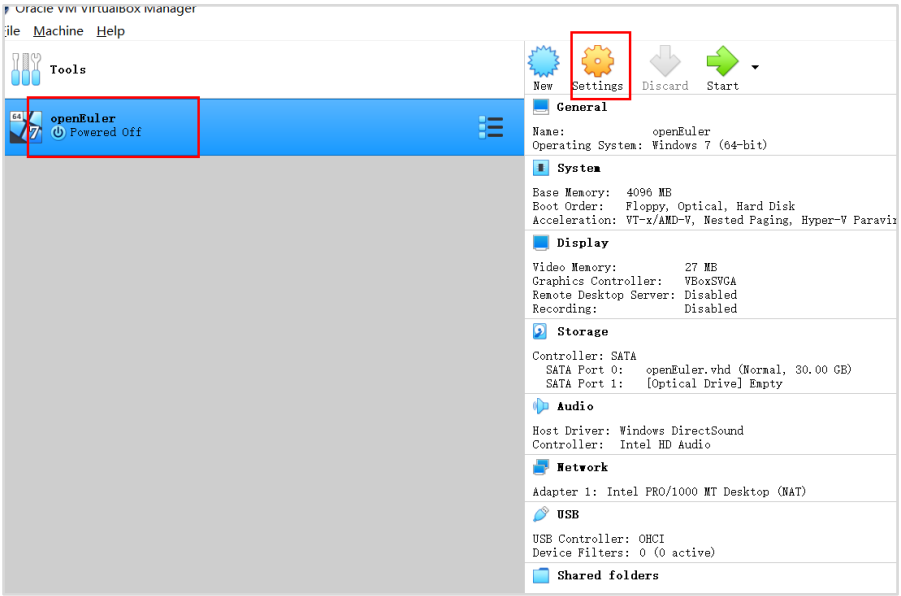


Figure 4-9 Configuring the VM

Step 8 On the **openEuler – Settings** page, choose **System**, click **Motherboard**, and adjust the boot order to boot from the hard disk first.

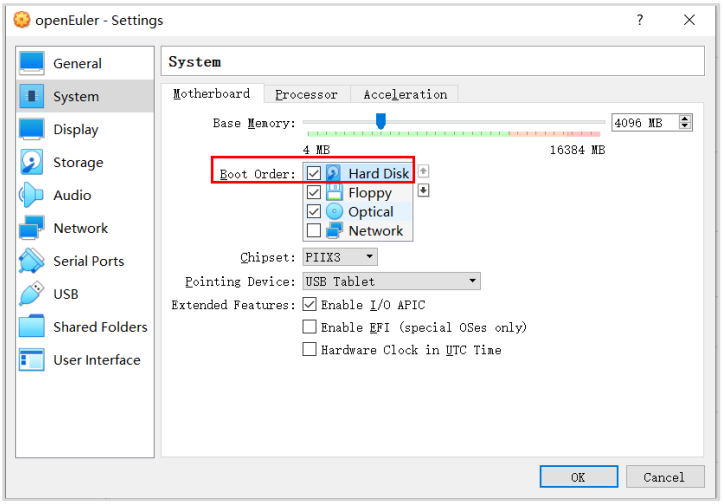


Figure 4-10 Changing the boot order

Step 9 Choose **System**, click **Acceleration**, and select **KVM** for **Paravirtualization Interface**.

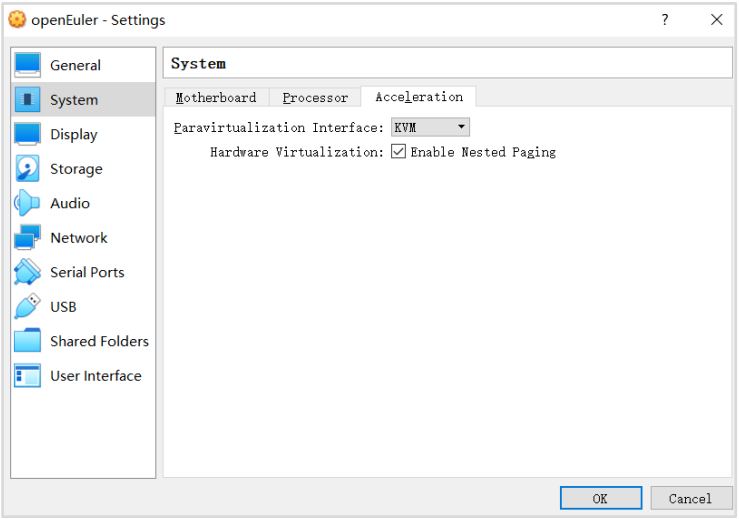


Figure 4-11 Selecting the paravirtualization interface

Step 10 Choose **Network**, click **Adapter 2**, and select **Enable Network Adapter**. Select **Bridged Adapter** for **Attached to**.

Step 11 This adapter is used as the planned management adapter.

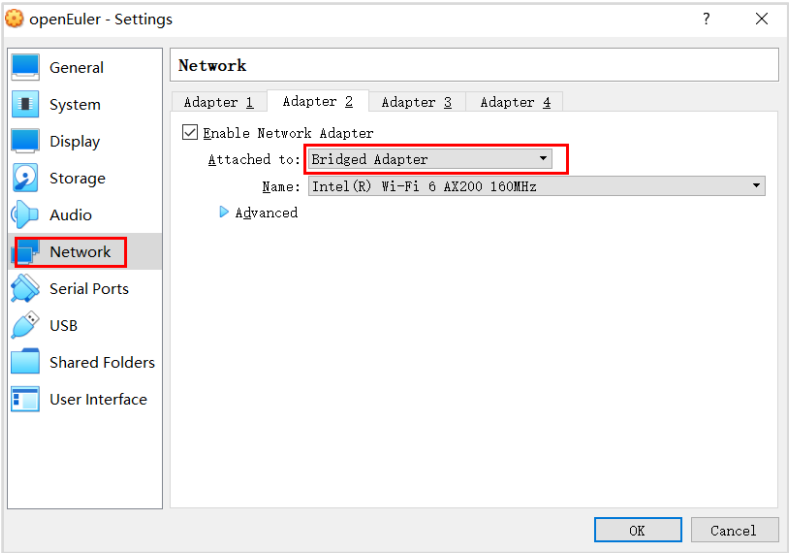


Figure 4-12 Changing the connection method of NIC 2

Step 12 Choose **System**, click **Processor**, set **Processor(s)** to **4**, and select **Enbale Nested VT-x/AMD-V** for **Extended Features**.

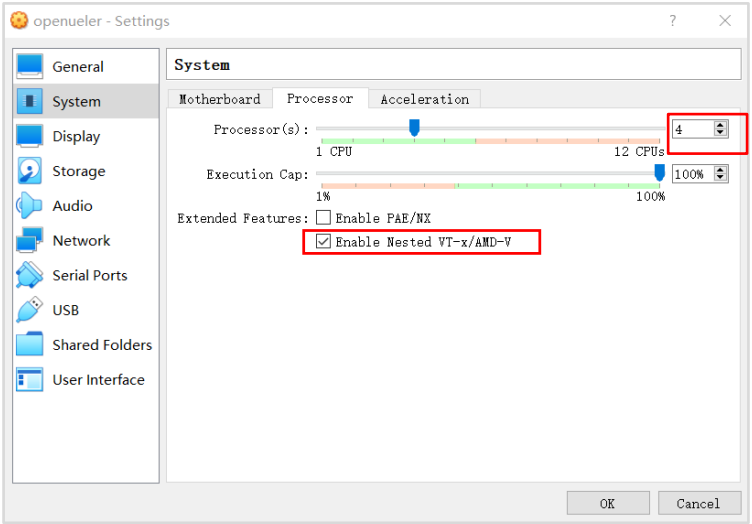


Figure 4-13 Configuring Processors

If **Nested VT-x/AMD-V** cannot be enabled, you can perform the following steps:

1. Click **OK** to save the configuration.
2. Press **Win+X** to go to the Windows PowerShell (administrator) page.
3. Run the following command to enable nested VT-x/AMD-V.

```
PS C:\WINDOWS\system32> cd "d:\Download\virtualbox"          # VirtualBox installation path
In PS D:\Download> .\VBoxManage.exe modifyvm "openEuler" --nested-hw-virt on     # the text with double quotation marks is the VM name.
```

```
PS C:\WINDOWS\system32> cd "d:\Download\virtualbox"

PS D:\Download> .\VBoxManage.exe modifyvm "openEuler" --nested-hw-virt on
PS D:\Download>
```

Figure 4-14 Run the command

Note: After running commands, you need to recheck whether these two options are selected. If yes, click **OK**.

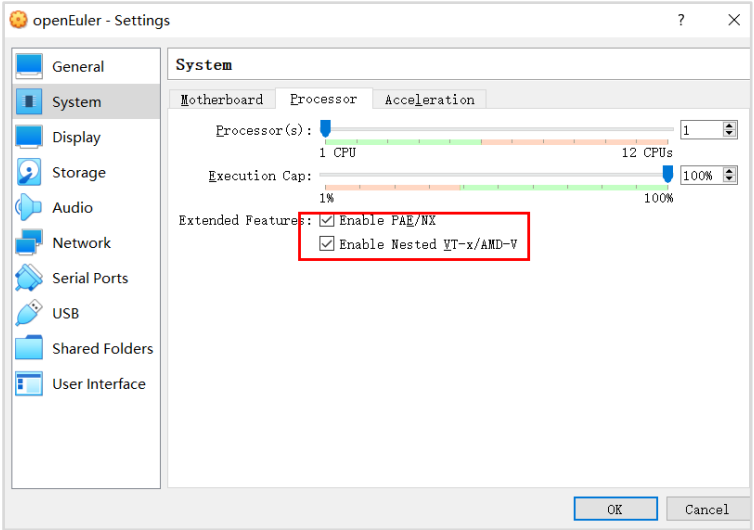


Figure 4-15 Enabling nested VT-x/AMD-V

4.2.2.2 Installing an OS on the VM

Step 1 Choose **openEuler** and click **Start** to start the VM.

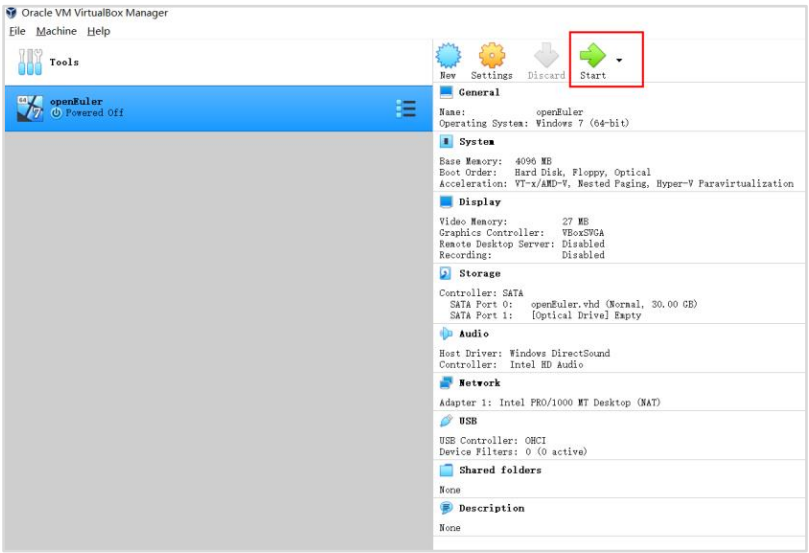


Figure 4-16 Starting the VM

Step 2 Select a local openEuler image file and click **Start**.

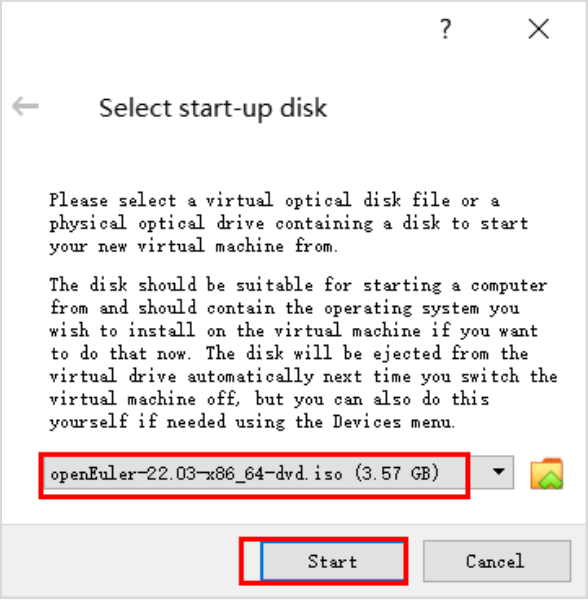


Figure 4-17 Selecting start-up disk and starting the VM

Step 3 Select **Install openEuler 22.03-LTS**.

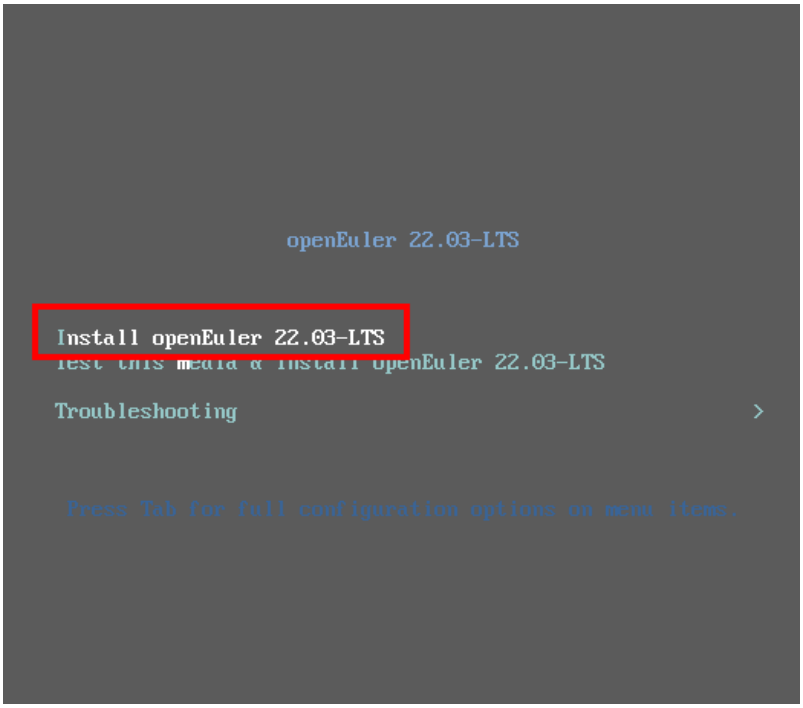


Figure 4-18 Installing the OS

Step 4 Select **English** and click **Continue**.

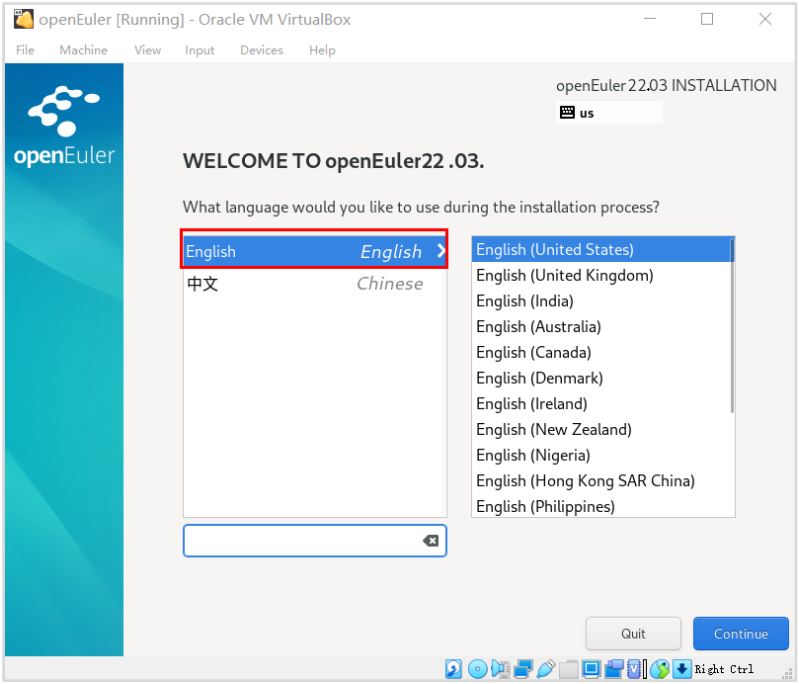


Figure 4-19 Selecting the OS language

Step 5 Click **Installation Destination** to select a disk where to install the OS.

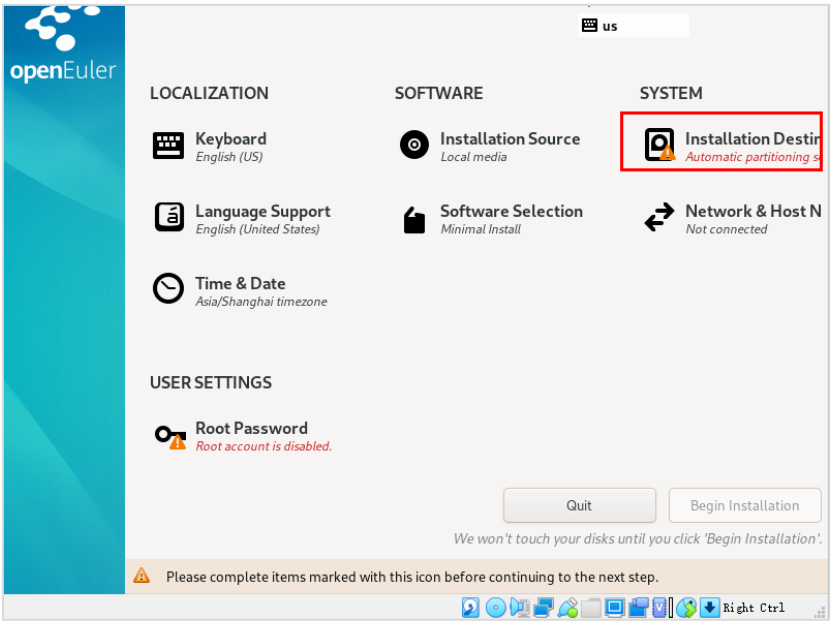


Figure 4-20 Selecting the installation destination

Step 6 Use the default settings and click **Done**.

Step 7 The main page is displayed.

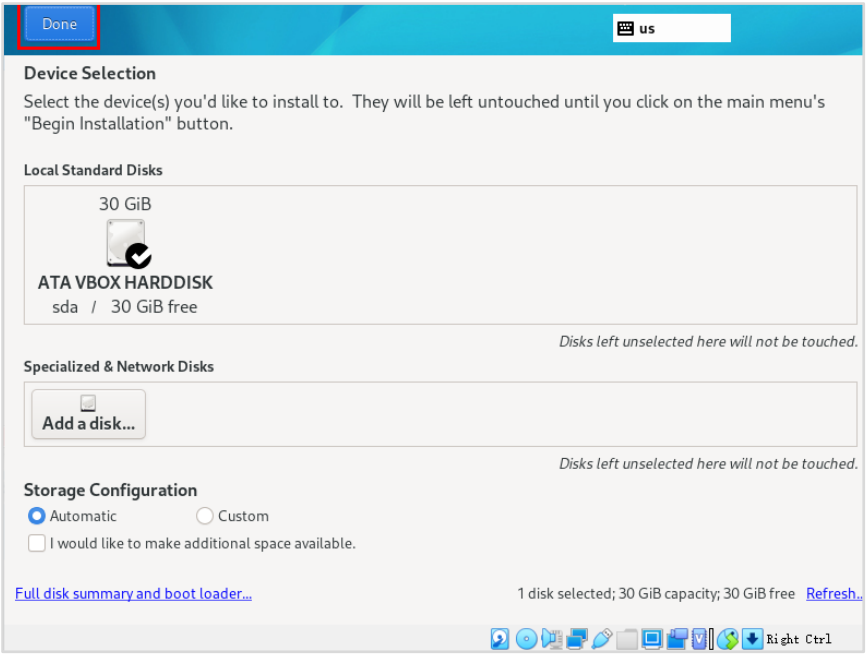


Figure 4-21 Selecting the installation destination

Step 8 Click **Network & Host Name** to configure the network.

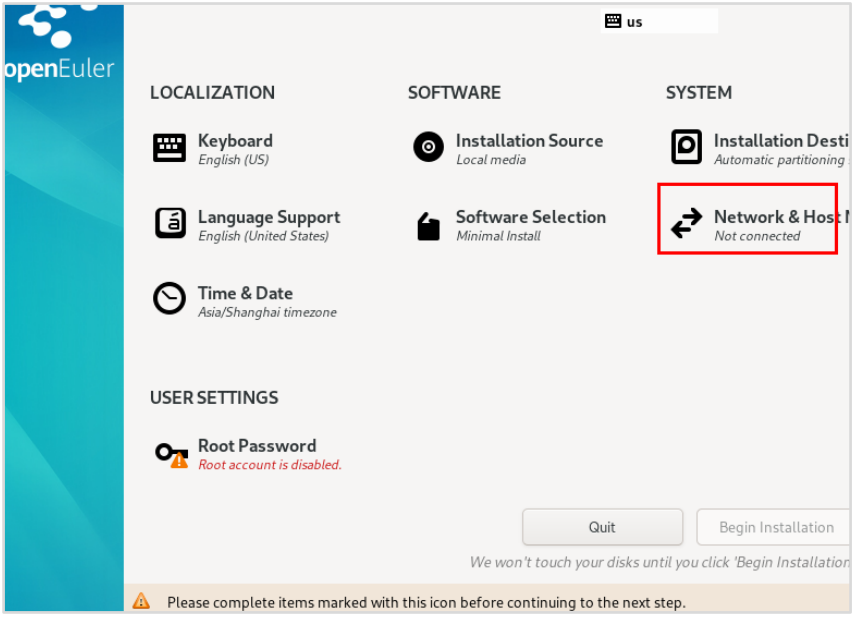


Figure 4-22 Configuring the network and host name

Step 9 Enable the NIC 1 (enp0s3) and the NIC 2 (enp0s8). Click **Done**.

Step 10 The main page is displayed.

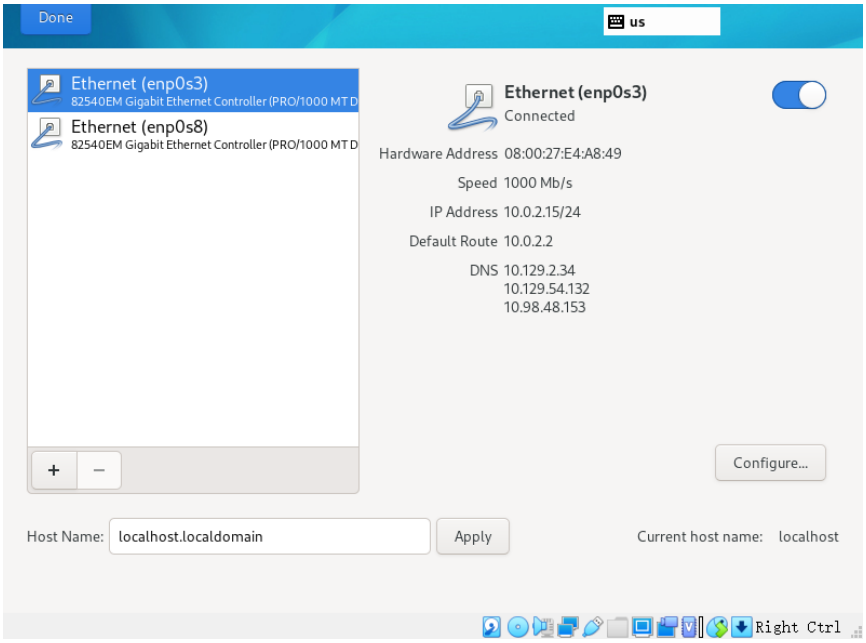


Figure 4-23 Enabling the NIC 1 (enp0s3)

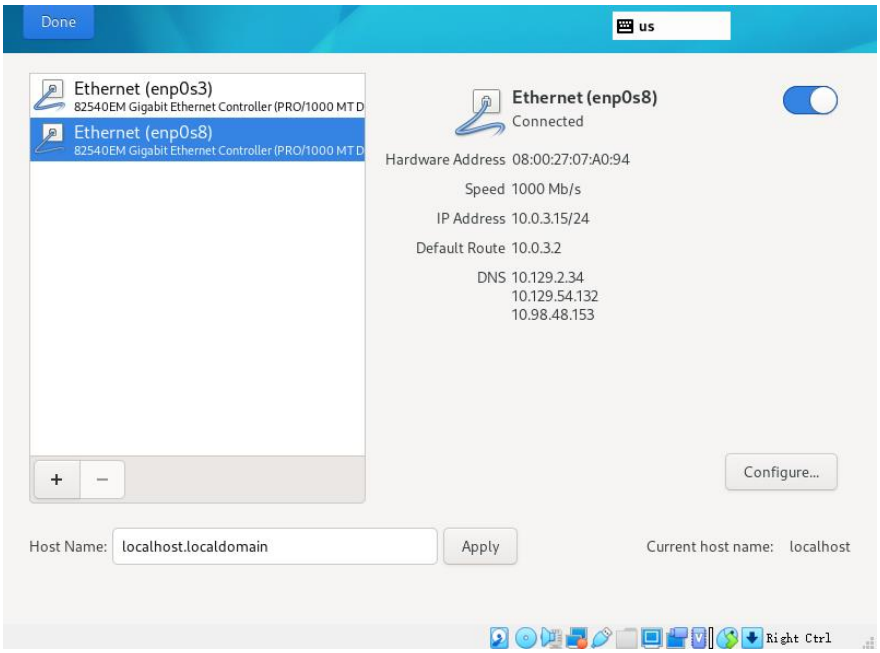


Figure 4-24 Enabling the NIC 2 (enp0s8)

Step 11 Select **Root Password** to configure it.

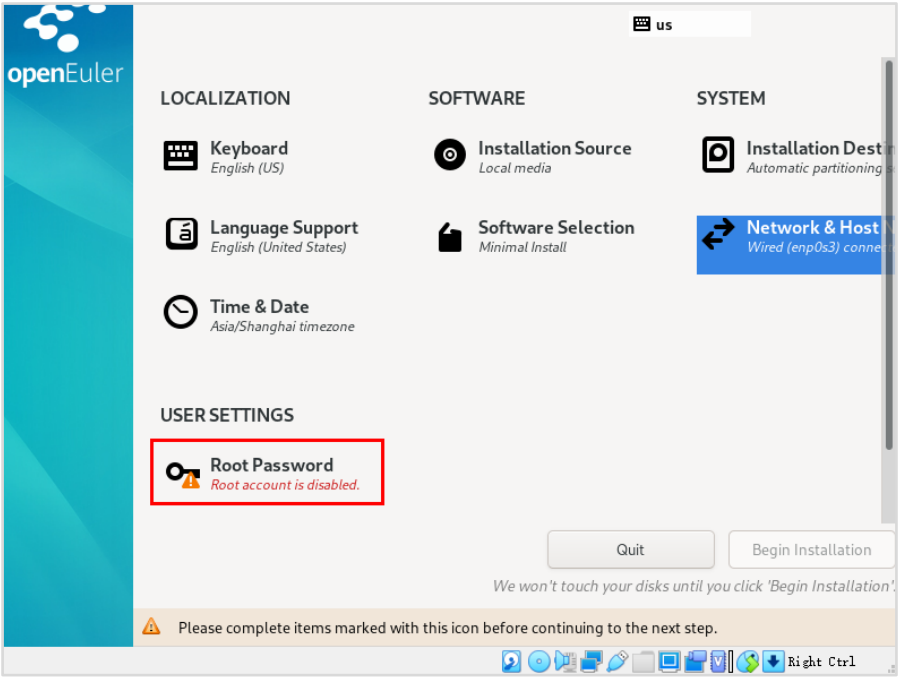


Figure 4-25 Configuring the root password

Step 12 Enter the root password, confirm it, and click **Done**. Click **Done**.

Step 13 The main page is displayed.

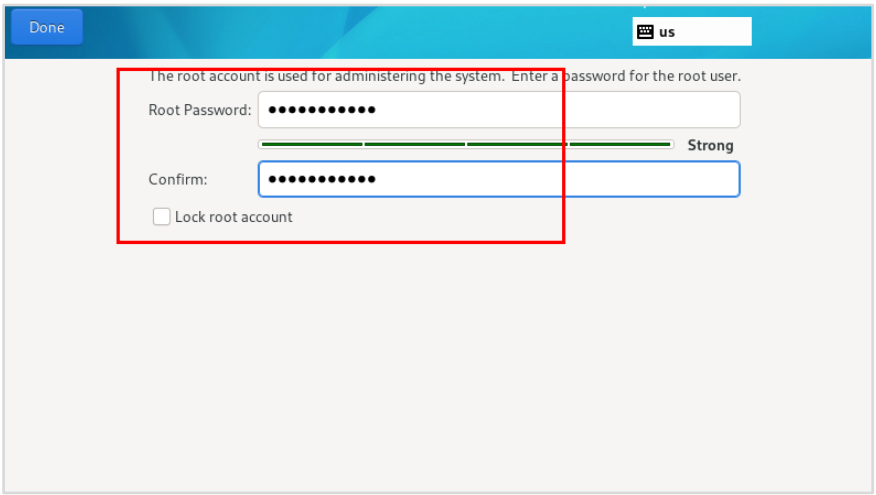


Figure 4-26 Configuring the root password

Step 14 Click **Begin Installation**.

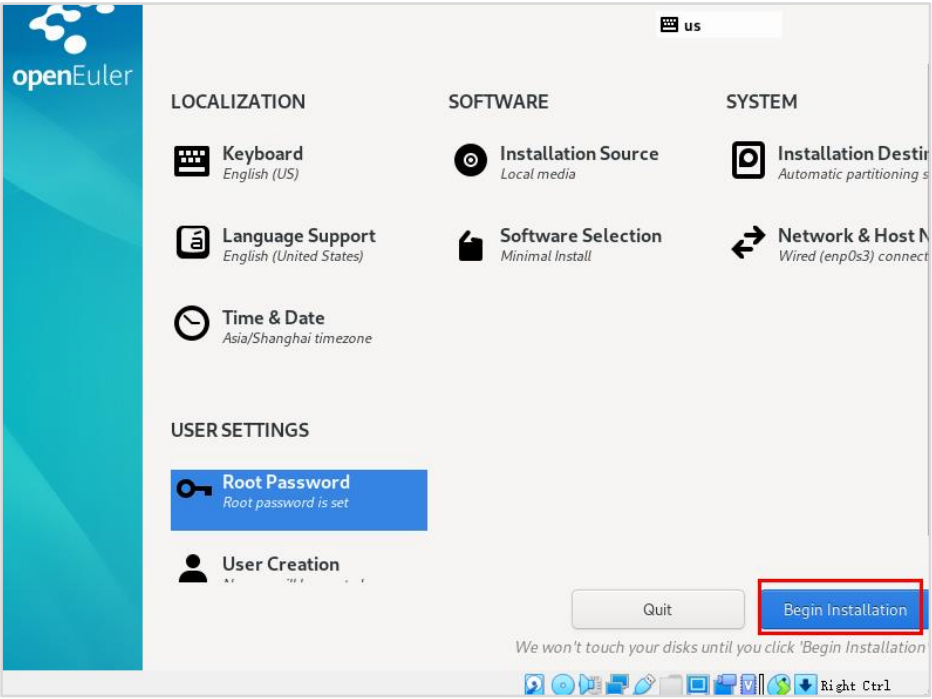


Figure 4-27 Installing the OS on the VM

Step 15 Click **Reboot System**.

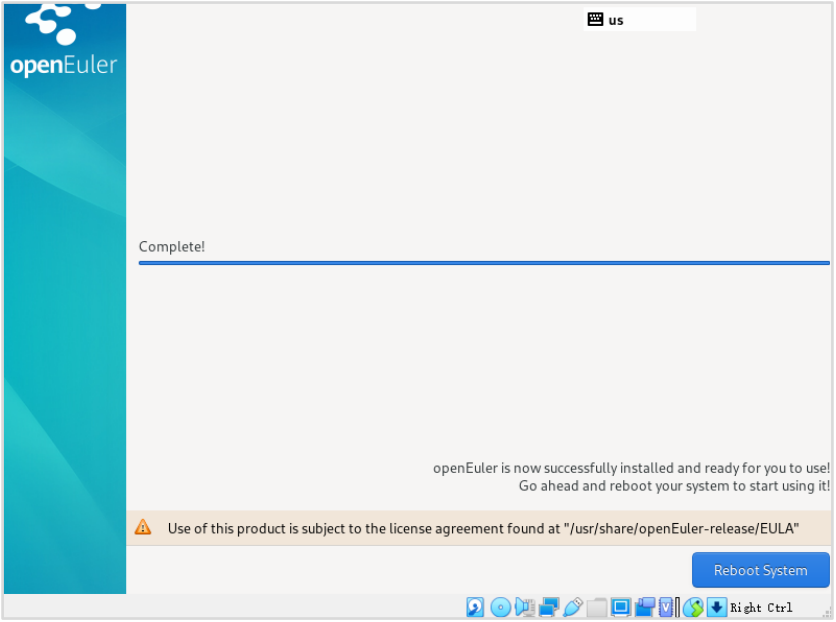


Figure 4-28 Rebooting the OS

Step 16 Enter **root** and the password to log in to the VM.

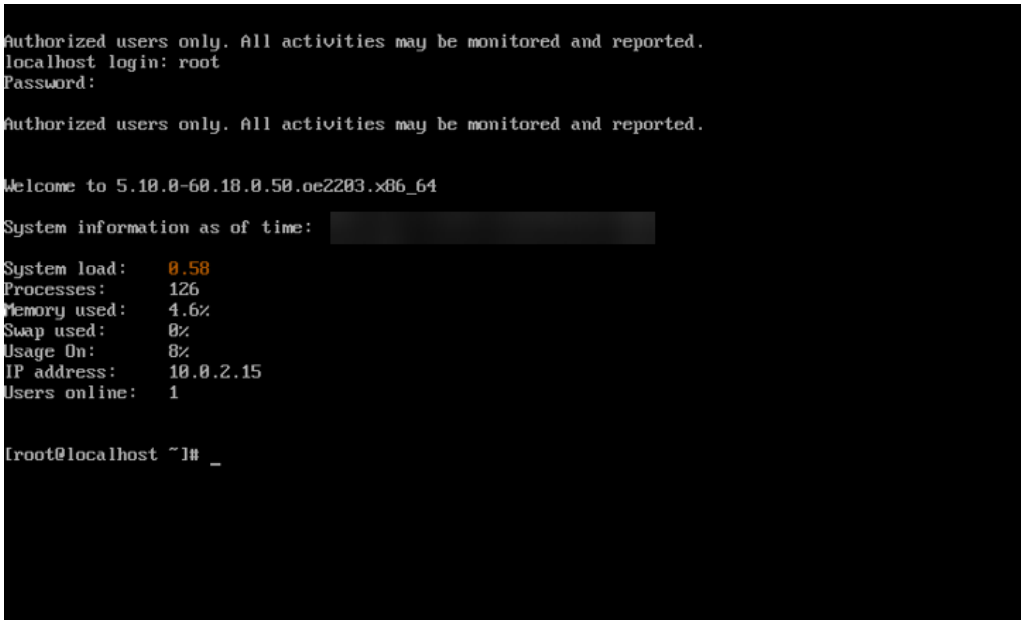


Figure 4-29 Logging in to the VM

Step 17 Run the following command to view the current IP address.

10.0.2.15/24 is the service address, and **192.168.3.117/24** is the management address.

```
[root@localhost ~]# ip addr
```

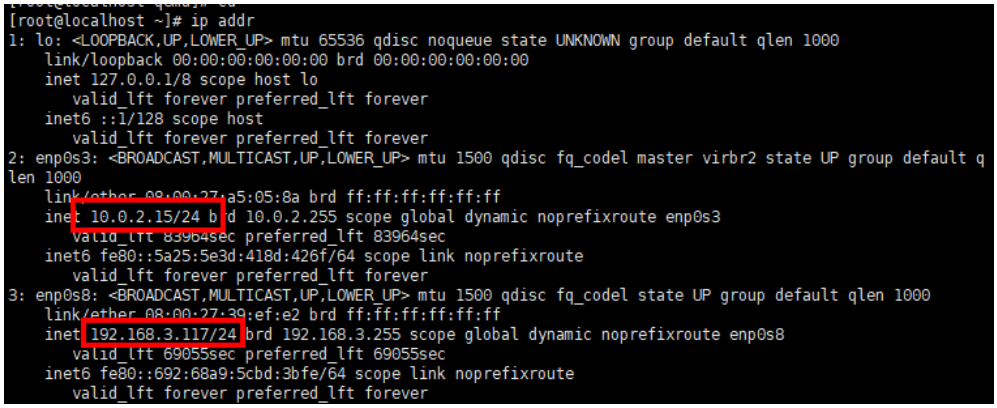


Figure 4-30 Viewing the current IP address

4.2.2.3 Preparing the Lab

Step 1 Start a terminal tool and enter the management IP address to log in to the VM.

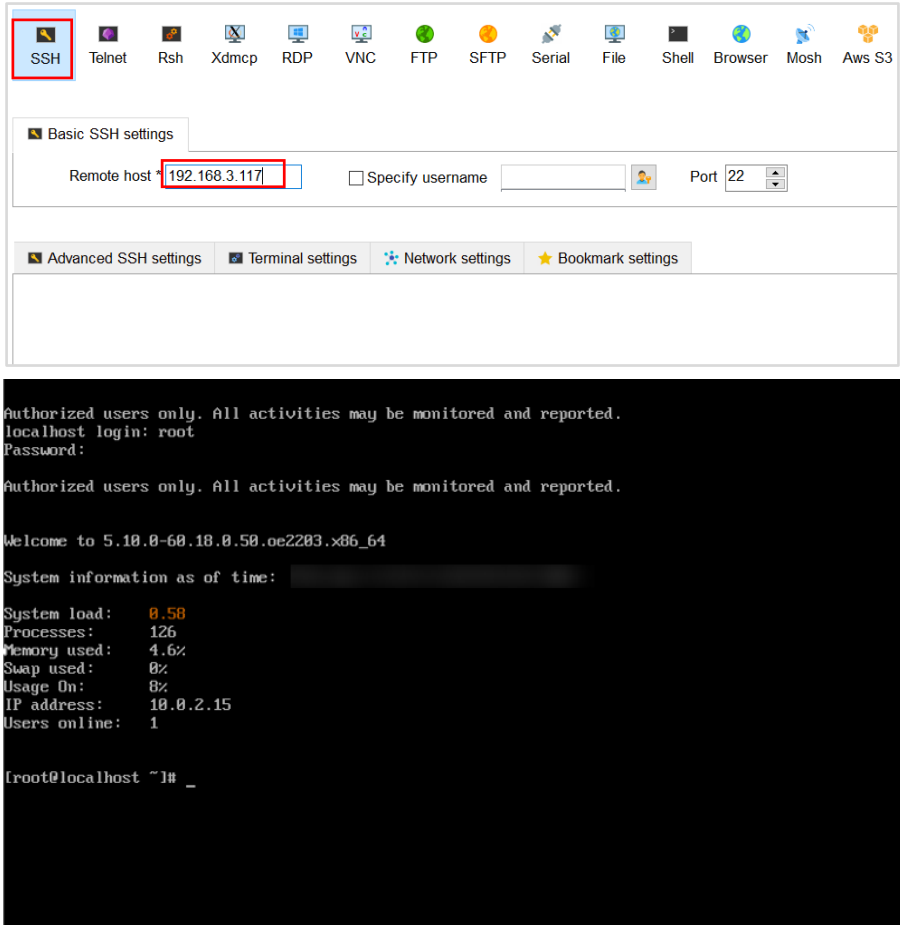


Figure 4-31 Logging in to the VM

Step 2 Run the following commands to disable the corresponding service.

```
[root@localhost ~]# systemctl disable firewalld.service          # Disabling the firewall service
 for [root@localhost ~]# vi /etc/selinux/config                   # Changing SELINUX=disabled
[root@localhost ~]# reboot                                        # Rebooting the VM
```

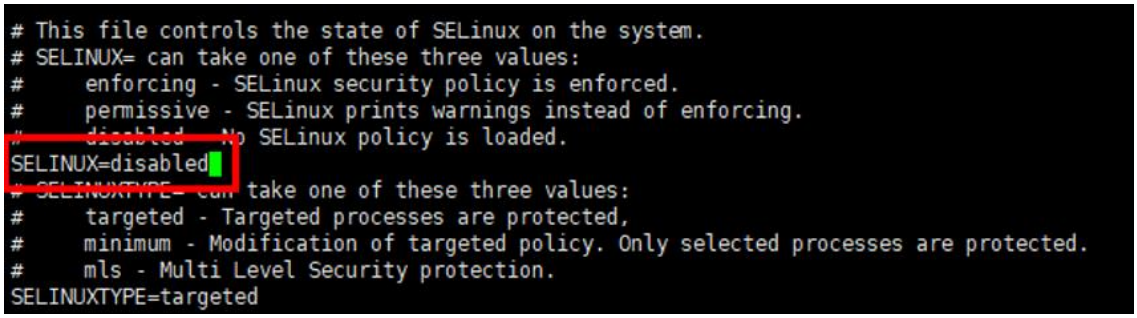


Figure 4-32 Disabling the firewall service

```
[root@localhost ~]# systemctl status firewalld                    # Checking the status of the firewall service
○ firewalld.service - firewalld - dynamic firewall daemon
     Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled; vendor preset: enabled)
     Active: inactive (dead)
```

```
          Docs: man:firewalld(1)
[root@localhost ~]# cat /etc/selinux/config

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of these three values:
#       targeted - Targeted processes are protected,
#       minimum - Modification of targeted policy. Only selected processes are protected.
#       mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Step 3 Install virtualization components and start **libvirtd**.

```
[root@localhost ~]# yum -y install libvirt qemu virt-install wget net-tools bridge-utils
[root@localhost ~]# systemctl start libvirtd
[root@localhost ~]# systemctl enable libvirtd
```

- **libvirt** is an open-source API, daemon and management tool for managing virtualization platforms.
- **QEMU** is open-source (emulation) software. It can emulate all resources required by VMs, including the CPU, memory, I/O device, USB, and NICs.
- **virt-install** is a command line tool for creating VMs and installing OSs for KVM, Xen, or other hypervisors supporting **libvirt**.
- **wget** is a free tool for automatically downloading files from Internet.
- **net-tools** is a network configuration tool.
- **bridge-utils** is used to configure Linux bridges.

Step 4 Check the status of components and **libvirtd**.

- The status of the **QEMU** component

```
[root@localhost ~]# rpm -qi qemu
Name            : qemu
Epoch           : 2
Version         : 6.2.0
Release         : 29.oe2203
Architecture: x86_64
...
```

- The status of the **libvirt** component

```
[root@localhost ~]# rpm -qi libvirt
Name            : libvirt
Version         : 6.2.0
Release         : 36.oe2203
Architecture: x86_64
...
```

- The service status of **libvirtd**

```
[root@localhost ~]# systemctl status libvirtd
○ libvirtd.service - Virtualization daemon
     Loaded: loaded (/usr/lib/systemd/system/libvirtd.service; enabled; vendor preset: enabled)
......
```

Step 5 Download the image to the **/opt** directory.

```
[root@localhost ~]# cd /opt
[root@localhost opt]# wget https://mirrors.tuna.tsinghua.edu.cn/openeuler/openEuler-22.03-LTS/ISO/x86_64/openEuler-22.03-LTS-x86_64-dvd.iso
```

4.2.2.4 Creating a VM Using **default** and Communicating with External Networks Using NAT

Step 1 Create VM 01 using **default**.

```
[root@localhost opt]# virt-install --name vm01 --virt-type kvm --video vga --memory 1024 --vcpu 1 --disk size=8 --cdrom /opt/openEuler-22.03-LTS-x86_64-dvd.iso --network network=default --graphics vnc,listen=0.0.0.0,port=5900,password=123456 --noautoconsole
```

Parameters

```
--virt-type          Specifies the name of the management program.
--cdrom CDROM        Specifies the optical disc drive installation media.
--memory MEMORY      Specifies the memory.
--vcpus VCPUS        Specifies the number of virtual CPUs.
--noautoconsole      Do not automatically try to connect to the guest console.
--disk DISK          Specifies storage with various options. For example, the disk size is 10 GB.
--network NETWORK    Specifies network interfaces. For example:
                       --network bridge=mybr0
                       --network network=my_libvirt_virtual_net
--graphics GRAPHICS  Configures the display settings of guest machines.
```

1. View the ID of virtual network console (VNC).

```
[root@localhost opt]# virsh vncdisplay vm01
:0
```

2. Run a VNC login tool, enter the management IP address (192.168.3.117), and the port number (5900), and click **OK**.

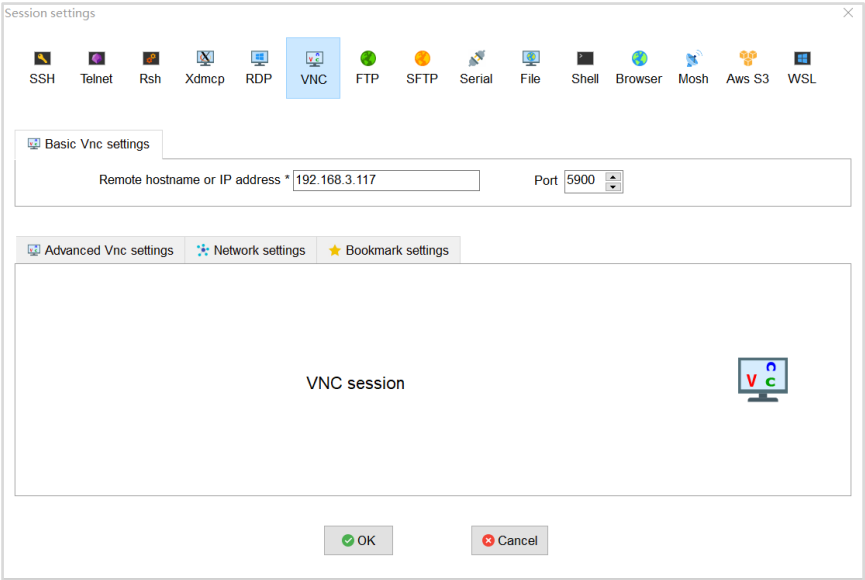


Figure 4-33 Logging in to VNC

3. Install the operating system as described in section 4.2.2.2.

Note: If VM 01 is shut off after being rebooted, run the **virsh start vm01** command to manually start it.

Step 2 Verify the connectivity of VM 01.

1. Log in to VM 01 using VNC, view the current IP address, and test the connectivity with external networks.

Alternatively, run the following commands to view the IP address of VM 01 on the host VM and log in to VM 01 using SSH.

```
[root@server ~]# virsh domifaddr vm01
 name       MAC address          Protocol     Address
-------------------------------------------------------------------------------
 vnet0      52:54:00:a2:f0:37    ipv4         192.168.122.39/24
[root@server ~]# ssh 192.168.122.39
```

2. After logging in to the VM using VNC, run the **ip addr** command to view the current IP address.

```
[root@localhost ~]# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 52:54:00:a2:f0:37 brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    inet 192.168.122.39/24 brd 192.168.122.255 scope global dynamic noprefixroute ens3
       valid_lft 3555sec preferred_lft 3555sec
    inet6 fe80::2565:2379:ac61:ded0/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
[root@localhost ~]# _
```

Figure 4-34 Viewing the current IP address

Note: The **default** network is in NAT mode, the specified bridge is **virbr0**, and the IP address obtained by the VM is the one configured in the address pool for **default**.

3. Test the connectivity with external networks.

```
[root@localhost ~]# ping www.huawei.com
PING www.huawei.com.lxdns.com (122.225.83.146) 56(84) bytes of data.
64 bytes from 122.225.83.146 (122.225.83.146): icmp_seq=1 ttl=54 time=17.0 ms
64 bytes from 122.225.83.146 (122.225.83.146): icmp_seq=2 ttl=54 time=12.7 ms
64 bytes from 122.225.83.146 (122.225.83.146): icmp_seq=3 ttl=54 time=11.6 ms
64 bytes from 122.225.83.146 (122.225.83.146): icmp_seq=4 ttl=54 time=12.8 ms
64 bytes from 122.225.83.146 (122.225.83.146): icmp_seq=5 ttl=54 time=11.4 ms
^C
--- www.huawei.com.lxdns.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4009ms
rtt min/avg/max/mdev = 11.418/13.101/17.002/2.030 ms
[root@localhost ~]#
```

Figure 4-35 Testing the connectivity with external networks

4.2.2.5 Changing **default** to **test** and Enabling the VM to Communicate with External Networks Using NAT

Step 1 Create **test** and specify the new bridge **virbr1**.

1. Change **default** and generate an XML file for **test**.

Before change

```
[root@localhost opt]# virsh net-edit default
<network>
<name>default</name>                                          #Changing the value to test
<uuid>504fd670-7a5c-45e9-8034-2a78959734ef</uuid>             #Changing two digits
  <forward mode='nat'/>
<bridge name='virbr0' stp='on' delay='0'/>                    #Changing virbr0 to virbr1
  <mac address='52:54:00:1b:53:3b'/>
<ip address='192.168.122.1' netmask='255.255.255.0'>   #Changing it to the new IP address
    <dhcp>
<range start='192.168.122.2' end='192.168.122.254'/> #Changing it to the new address pool
    </dhcp>
  </ip>
</network>
```

After change

```
<network>
<name>test</name> #The name has been changed to test.
<uuid>504fd670-7a5e-75e9-805e-2a78959734ef</uuid>     #The UUID has been changed.
  <forward mode='nat'/>
<bridge name='virbr1' stp='on' delay='0'/>          #The designated bridge has been changed to virbr1.
  <mac address='52:54:00:1b:53:3b'/>
The <ip address='192.168.100.1' netmask='255.255.255.0'>          #IP address has been changed.
    <dhcp>
<range start='192.168.100.2' end='192.168.100.254'/>          #The address pool has been modified.
    </dhcp>
  </ip>
</network>
```

After change, the **test.xml** file is generated in **/etc/libvirt/qemu/networks/**. You can run the following command to define and start **test**.

```
The [root@localhost ~]# virsh net-define /etc/libvirt/qemu/networks/test.xml     # Defining the network from the test.xml file
The [root@localhost ~]# virsh net-start test     # starting test
[root@localhost ~]# virsh net-list                # Viewing the network list
```

2. Start the network to check whether virbr1 is automatically generated.

The configuration file is stored in **/run/NetworkManager/system-connections**.

In this case, you can run the **ifconfig** command to view the API address of the generated **virbr1** and run the **brctl show** command to view the generated bridge **virbr1**.

```
[root@localhost ~]# brctl show
[root@localhost ~]# ifconfig
```

Step 2 Change the network of VM 01 to **test**.

```
[root@localhost ~]# virsh edit vm01
    <interface type='network'>
      <mac address='52:54:00:a2:f0:37'/>
<source network='test'/>                                  #Changing default to test
      <model type='e1000'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x03' function='0x0'/>
    </interface>
    <serial type='pty'>
```

- Reboot VM 01.

```
[root@localhost ~]# virsh destroy vm01
[root@localhost ~]# virsh start vm01
```

- On the VM 01, run the **ip addr** command to view the current IP address.

Check whether the IP address is the IP address range of **test**.

```
[root@localhost ~]# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 52:54:00:a2:f0:37 brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    inet 192.168.100.39/24 brd 192.168.100.255 scope global dynamic noprefixroute ens3
       valid_lft 3590sec preferred_lft 3590sec
    inet6 fe80::2565:2379:ac61:ded0/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
[root@localhost ~]#
```

Figure 4-36 Viewing the current IP address

- Test the communication with external networks.

```
[root@localhost ~]# ping www.huawei.com
PING www.huawei.com.lxdns.com (183.134.11.40) 56(84) bytes of data.
64 bytes from 183.134.11.40 (183.134.11.40): icmp_seq=1 ttl=54 time=14.6 ms
64 bytes from 183.134.11.40 (183.134.11.40): icmp_seq=2 ttl=54 time=16.4 ms
64 bytes from 183.134.11.40 (183.134.11.40): icmp_seq=3 ttl=54 time=13.8 ms
64 bytes from 183.134.11.40 (183.134.11.40): icmp_seq=4 ttl=54 time=14.4 ms
64 bytes from 183.134.11.40 (183.134.11.40): icmp_seq=5 ttl=54 time=19.5 ms
64 bytes from 183.134.11.40 (183.134.11.40): icmp_seq=6 ttl=54 time=19.7 ms
```

Figure 4-37 Testing the connectivity with external networks

4.2.2.6 Specifying a Bridge to create a VM and Communicate with External Networks Using Bridges

Step 1 Create **virbr2** and specify it to create VM 02 using bridges.

1. Create **virbr2**, assign the IP address of the original physical interface to it, and bind it to the physical service interface.

```
[root@localhost ~]# brctl addbr virbr2
[root@localhost ~]# brctl addif virbr2 enp0s3
[root@localhost ~]# ifconfig enp0s3 0.0.0.0
#After the enp0s3 interface is bound to the bridge, no IP address is required. Set the IP address of enp0s3 to 0.0.0.0.
[root@localhost ~]# ifconfig virbr2 10.0.2.15 netmask 255.255.255.0
# Assigning the IP address of the original physical interface to virbr2.
```

2. Specify **virbr2** to create VM 02.

```
[root@localhost ~]# virt-install --name vm02 --virt-type kvm --video vga --memory 1024 --vcpu 1 --disk size=10 --cdrom /opt/openEuler-22.03-LTS-x86_64-dvd.iso --network bridge=virbr2 --graphics vnc,listen=0.0.0.0,port=5901,password=123456 --noautoconsole
[root@localhost ~]# virsh vncdisplay vm02
1
```

3. Log in to the VM using VNC referring to step 1 in Section 4.2.2.4, change the port number to **5901**, and install the OS.

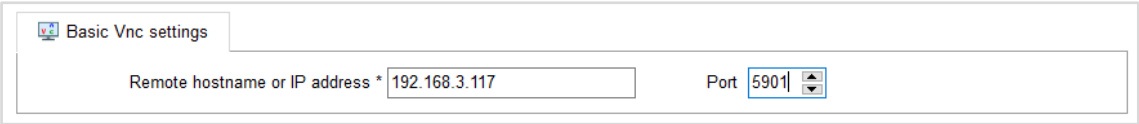


Figure 4-38 Logging in to the VM using VNC

4. View the IP address of VM 02.

```
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.17  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::e2e1:a18b:f73a:d89e  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:a5:05:8a  txqueuelen 1000  (Ethernet)
        RX packets 72  bytes 10322 (10.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 160  bytes 13730 (13.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure 4-39 Viewing the IP address of VM 02

5. Test the connectivity between VM 02 and external networks.

```
[root@localhost ~]# ping www.huawei.com
PING www.huawei.com.lxdns.com (122.225.83.146) 56(84) bytes of data.
64 bytes from 122.225.83.146 (122.225.83.146): icmp_seq=1 ttl=55 time=17.0 ms
64 bytes from 122.225.83.146 (122.225.83.146): icmp_seq=2 ttl=55 time=12.9 ms
64 bytes from 122.225.83.146 (122.225.83.146): icmp_seq=3 ttl=55 time=12.8 ms
64 bytes from 122.225.83.146 (122.225.83.146): icmp_seq=4 ttl=55 time=13.1 ms
^C
```

Figure 4-40 Testing the connectivity with external networks

- Test the connectivity between VM 02 and the host VM.

```
[root@localhost ~]# ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.083 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.056 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.044 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.053 ms
^C
```

Figure 4-41 Testing the connectivity with the host VM

4.3 Quiz

In KVM virtualization, what are the differences between NAT networks and bridged networks in assigning IP addresses to VMs?

Answer:

NAT networks use the address pool configured on the corresponding network to assign IP addresses to VMs. Bridged networks use the address segment of the physical interface or bridge interface to allocate addresses to VMs.

Huawei Cloud Certification Training

HCIA-Cloud Computing

Lab Guide (FusionCompute)

ISSUE: 5.0

HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2022. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions

HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base Bantian, Longgang Shenzhen 518129 People's Republic of China

Website: https://e.huawei.com

Huawei Certification System

The Huawei certification system is a platform for shared growth, part of a thriving partner ecosystem. There are two types of certification: one for ICT architectures and applications, and one for cloud services and platforms. There are three levels of certification available:

Huawei Certified ICT Associate (HCIA)

Huawei Certified ICT Professional (HCIP)

Huawei Certified ICT Expert (HCIE)

Huawei certification courses cover the entire ICT domain, with a focus on how today's architecture generates cloud-pipe-device synergy. The courses present the latest developments of all essential ICT aspects to foster a thriving ICT talent ecosystem for the digital age.

HCIA-Cloud Computing V5.0 is intended for beginners. Focusing on the virtualization technologies and FusionAccess of Huawei, this course aims to help you learn the basics of cloud computing and resource pooling, and to cultivate cloud computing engineers that are capable of using FusionCompute for virtualization and managing FusionAccess.

The HCIA-Cloud Computing V5.0 certification includes the following courses: basics of cloud computing (server, storage, network, and OS), overview of FusionCompute, routine management and troubleshooting of virtualization resource pools, overview of FusionAccess and related components, as well as their installation, deployment, service management, and troubleshooting.

Passing the HCIA-Cloud Computing V5.0 certification means that you are capable of designing, managing, and maintaining FusionCompute and FusionAccess.

Huawei Certification
Cloud Service & Platform
HarmonyOS
IoT
GaussDB
openGauss
MDC
Big Data
AI
openEuler
Kunpeng Application Developer
Cloud
ICT Infrastructure
Storage
Intelligent Computing
Datacom
WLAN
Transmission
Access
Enterprise Communication
Security
LTE
Intelligent Vision
SDN
5G
Data Center
HCIE
Huawei Certified ICT Expert
HCIP
Huawei Certified ICT Professional
HCIA
Huawei Certified ICT Associate

About This Document

Overview

This document is intended for HCIA-Cloud Computing certification training courses. It is intended for trainees who preparing for the HCIA-Cloud Computing exam or those that want to understand, use, and manage FusionCompute, Huawei's server virtualization product.

About the Exercises

This lab guide consists of four exercises:

- Exercise 1: FusionCompute environment setup. This exercise illustrates how to set up FusionCompute using servers and storage devices based on live network services. It covers the installation of CNA and VRM, helping you understand the FusionCompute architecture from the underlying layer.
- Exercise 2: FusionCompute resource management, including management of compute, storage, and network resources. On completion of this exercise, you will be able to understand the three major functions of FusionCompute server virtualization: compute virtualization, storage virtualization, and network virtualization, and understand the advantages of FusionCompute in resource management.
- Exercise 3: FusionCompute VM provisioning and management. This exercise covers VM creation, VM flavor adjustment, HA, live migration, as well as security group and rule group management. On completion of this exercise, you will be able to perform basic service O&M.
- Exercise 4: common FusionCompute O&M, including alarm, system, and permission management. On completion of this exercise, you will understand the basic O&M capabilities of FusionCompute.

Lab Environment Overview

Scenarios

In the equipment room of a company, two servers have been installed and BMC management addresses have been configured for them. The company plans to use Huawei FusionCompute virtualization suite to set up a service test platform for service tests and employee skill training. This platform needs to provide functions such as virtual machine (VM) resource management, VM live migration, VM snapshot, and high availability (HA). To fulfill subsequent service requirements of the company, VRM will be deployed on two VM nodes, and logical unit numbers (LUNs) will be created on the

company's existing storage devices for the platform. The following describes how to set up FusionCompute and perform service O&M on FusionCompute.

Design

Based on the service application scenarios of the company, the administrator designs the environment as follows:

- Connect two servers to a management jump server and a storage device, respectively, through a switch. On the network, eth2 is a management port while eth0 is a storage port.
- Deploy VRM on two VM nodes.
- Create LUNs on the company's existing storage devices for the platform.
- Considering that operations such as live migration and HA need to be performed on VMs, create LUNs on backend storage to ensure high availability.

Networking Topology

- As shown in Figure 1-1, use management ports (eth2) to connect CNA01 and CNA02 to the jump server through a switch. For details about IP address planning, see the network configuration description.
- As shown in Figure 1-1, use storage ports (eth0) to connect CNA01 and CNA02 to the storage device through a switch. For details about IP address planning, see the network configuration description.
- Deploy VRM on two VM nodes. After the deployment, CNA01 and CNA02 belong to the same FusionCompute resource pool.
- The physical networking in the experiment is subject to the actual environment.

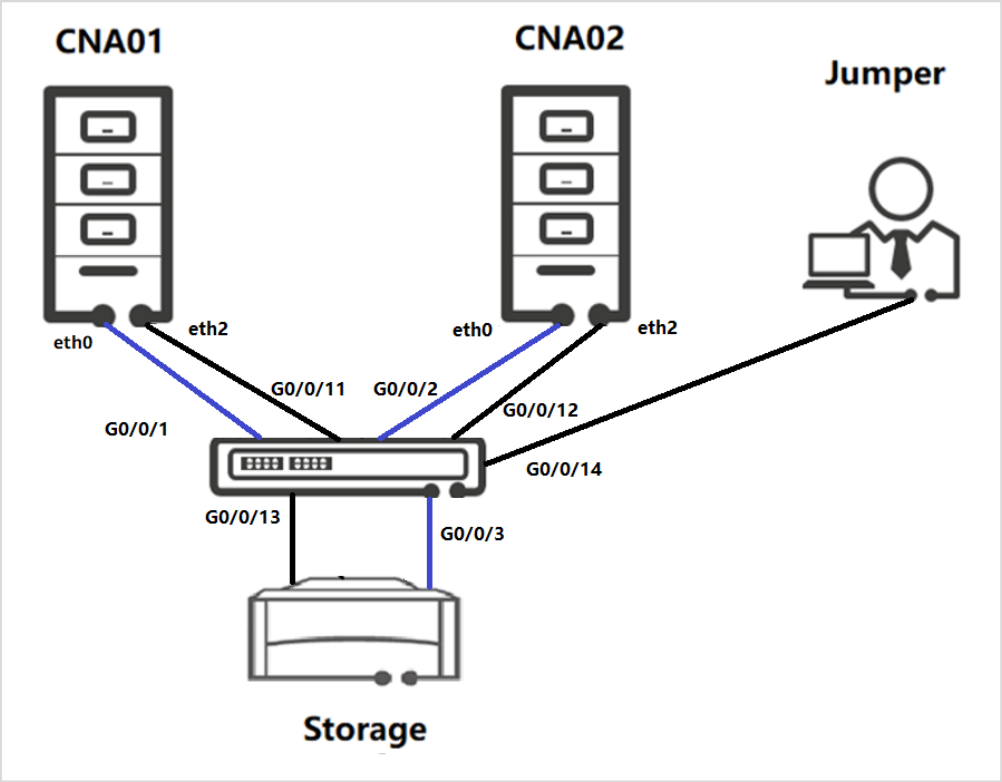


Figure 1-1 HCIA-Cloud Computing V5.0 networking topology

Devices and Software Description

Table 1-1 Devices

Device	Quantity	Remarks
Server	2	2 for each group
Switch	1	Shared by all groups
Huawei OceanStor V3/V5 series storage devices	1	Shared by all groups
Jump server	1	1 for each group

- Software and tools (which need to be uploaded by the trainer to the jump server in advance)

Table 1-2 Software and tools

Software	Description	How to Obtain
FusionCompute-LinuxInstaller-8.1.1-X86_64.zip	Server virtualization installation tool	https://support.huawei.com/enterprise/en/distributed-storage/fusioncompute-pid-8576912/software
FusionCompute_VRM-8.1.1-X86_64.zip	VRM software package	
FusionCompute_CNA-8.1.1-X86_64.iso	CNA image	
CentOS-7-x86_64-DVD-2009.iso	CentOS image	http://ftp.sjtu.edu.cn/centos/7.9.2009/isos/x86_64/CentOS-7-x86_64-DVD-2009.iso
PuTTY	Terminal login tool	https://the.earth.li/~sgtatham/putty/0.76/w64/putty-64bit-0.76-installer.msi
WinSCP	Terminal login tool	https://winscp.net/download/WinSCP-5.19.6-Setup.exe

Device Network Configurations

- The actual network configuration in the experiment is subject to the actual environment.

Table 1-3 Network configurations

NE	Port	Description	VLAN	IP Address
CNA01	eth2	Management/ Service channel	102	192.168.32.24/24
	eth0	Storage channel	96	Logical port address: 192.168.96.131/24
CNA02	eth2	Management/ Service channel	102	192.168.32.34/24
	eth0	Storage channel	96	Logical port address: 192.168.96.132/24
VRM01 (active)	/	Management address	102	192.168.32.35/24 (floating IP address) 192.168.32.36/24
VRM02 (standby)	/	Management address	102	192.168.32.37/24
Storage	Management port	Device login and configuration	101	10.154.88.117/24
	Service port	Provides the storage service.	96	192.168.96.2/24
Jump server	Management port	Connects to the management network.	102	192.168.32.2/24

Switch Configurations

- The switch configuration in the experiment is subject to the actual environment.

Table 1-4 Switch configurations

Switch	VLAN	Port	Description	Port Type	Port Configuration	VLANIF Configuration
SW1	VLAN 96 VLAN 102 VLAN 101 VLAN 100 (used for VM services)	G0/0/1	Connects to port eth0 of CNA01.	Trunk	PVID: 96 Allow pass VLAN: all	/
		G0/0/2	Connects to port eth0 of CNA02.	Trunk	PVID: 96 Allow pass VLAN: all	
		G0/0/3	Connects to the storage service port.	Access	Default VLAN: 96	
		G0/0/11	Connects to port eth2 of CNA01.	Trunk	PVID: 102 Allow pass VLAN: all	VLANIF102: 192.168.32.1/24
		G0/0/12	Connects to port eth2 of CNA02.	Trunk	PVID: 102 Allow pass VLAN: all	
		G0/0/14	Connects to the jump server.	Access	Default VLAN: 102	
		G0/0/13	Connects to the storage management port.	Access	Default VLAN: 101	VLANIF101: 10.154.88.1/24

FusionCompute Accounts

(Link to the product documentation: FusionCompute 8.1.1 Product Documentation)

Table 1-5 FusionCompute accounts

NE	Username	Password
FusionCompute-LinuxInstaller	admin	For details, see **Installation and Configuration** > **Installation Guide** > **FusionCompute Web Tool-based Installation** > **FusionCompute 8.1.1 Custom Installation** in *FusionCompute 8.1.1 Product Documentation*.
CNA node	root	Custom
CNA node	grub	Custom
CNA node	gandalf	Custom
VRM	admin	Custom

Contents

About This Document 3
Overview 3
About the Exercises 3
Lab Environment Overview 3
1 FusionCompute Environment Setup 11
1.1 Introduction 11
1.1.1 About This Exercise 11
1.1.2 Objectives 11
1.1.3 Procedure 11
1.2 CNA Installation 11
1.3 VRM Installation 22
1.4 Quiz 31
2 FusionCompute Resource Management 32
2.1 Compute Resource Management 32
2.1.1 Introduction 32
2.1.2 Creating a Cluster 32
2.1.3 Moving a Host 34
2.1.4 Deleting a Cluster 36
2.1.5 Configuring Cluster Policies 37
2.2 Storage Resource Management 39
2.2.1 Introduction 39
2.2.2 Configuring Storage Ports 39
2.2.3 Adding IP SAN Storage 42
2.2.4 Creating a Disk 51
2.3 Network Resource Management 52
2.3.1 Introduction 52
2.3.2 DVS Management 52
2.4 Quiz 57
3 FusionCompute VM Provisioning and Management 58
3.1 VM Provisioning 58
3.1.1 Introduction 58
3.1.2 VM Provisioning 58
3.2 VM Management 80
3.2.1 Introduction 80

3.2.2 VM Parameter Modification 81
3.2.3 VM Storage Adjustment 92
3.2.4 VM Snapshot Management 94
3.2.5 VM Live Migration 98
3.2.6 VM Rule Group 100
3.2.7 Security Group Creation 108
3.2.8 VM HA 113
3.3 Quiz 116
4 Common O&M Management 117
4.1 Introduction 117
4.1.1 About This Exercise 117
4.1.2 Objectives 117
4.1.3 Procedure 117
4.2 Viewing the System ESN 117
4.3 Managing Alarms 118
4.4 Configuring the System Clock 120
4.5 Permission Management 121
4.5.1 Role Management 121
4.5.2 User Management 122
4.5.3 Password Policy Management 123
4.6 Quiz 124

1 FusionCompute Environment Setup

1.1 Introduction

1.1.1 About This Exercise

In this exercise, you need to install CNA on two prepared servers and use installation tools to deploy VRM to set up a dual-node FusionCompute cluster.

1.1.2 Objectives

- Install and configure CNA.
- Install VRM using tools.
- Log in to FusionCompute.

1.1.3 Procedure

This exercise describes how to manually install FusionCompute. For details about how to install it using a web tool, see FusionCompute 8.1.1 Product Documentation.

Figure 1-1 Procedure

1.2 CNA Installation

Step 1 Log in to the management page of the CNA01 server, mount the CNA image package, and install the image.

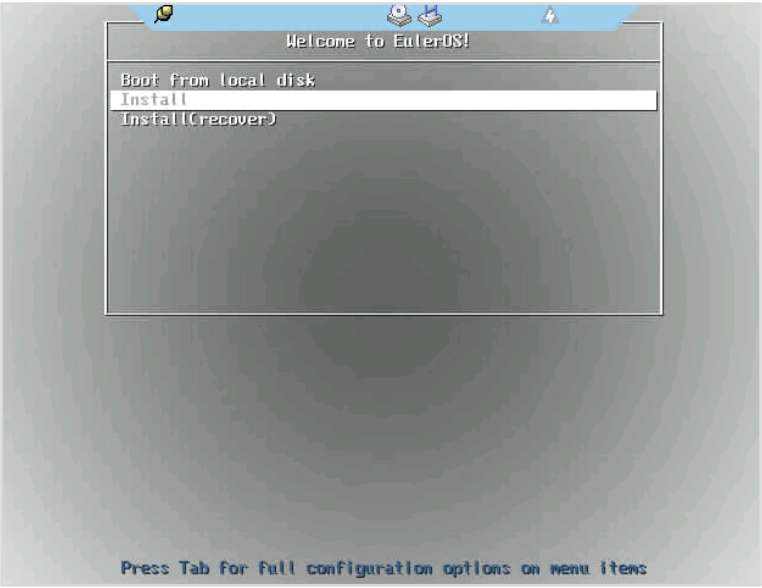


Figure 1-2 Installation page

Step 2 Move the cursor to **Install** and press **Enter** to go to the CNA installation and configuration page.

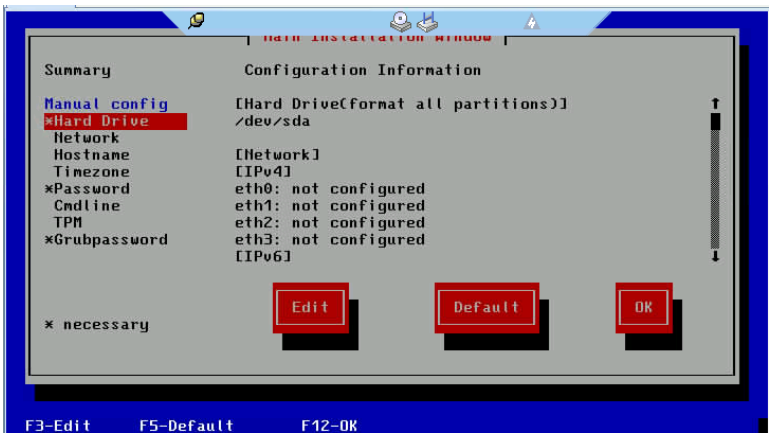


Figure 1-3 Selecting a disk

Step 3 Move the cursor to ***Hard Drive** and press **Enter** to go to the disk configuration page. Confirm that the disk information is correct, move the cursor to **OK**, press **Enter**, and then click **Yes**.

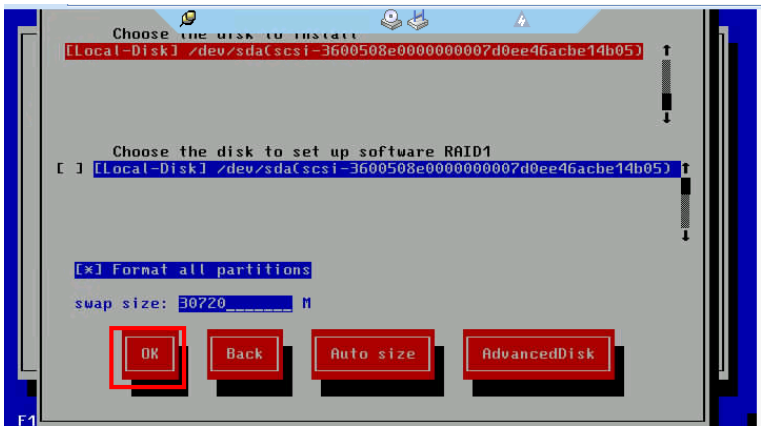


Figure 1-4 Selecting a disk

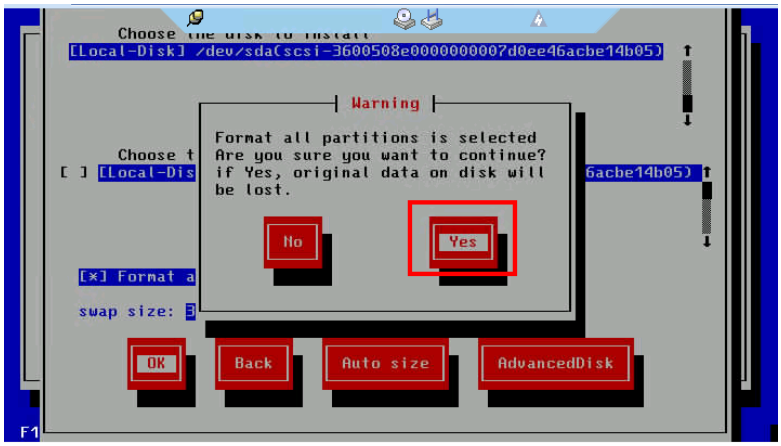


Figure 1-5 Formatting a disk

Step 4 Configure the CNA network. Move the cursor to **Network** and press **Enter**.

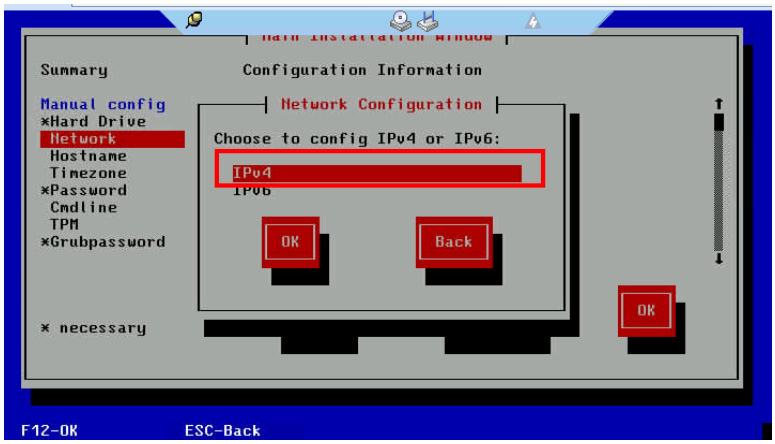


Figure 1-6 Configuring an IPv4 network

Step 5 Select **IPv4** and press **Enter**.

Step 6 Select the eth2 NIC and press **Enter**. On the NIC IP configuration page, configure the CNA01 IP address (to **192.168.32.24**) as planned. Move the cursor to **OK** and press **Enter**. (Set the CNA02 IP address to **192.168.32.34**.)

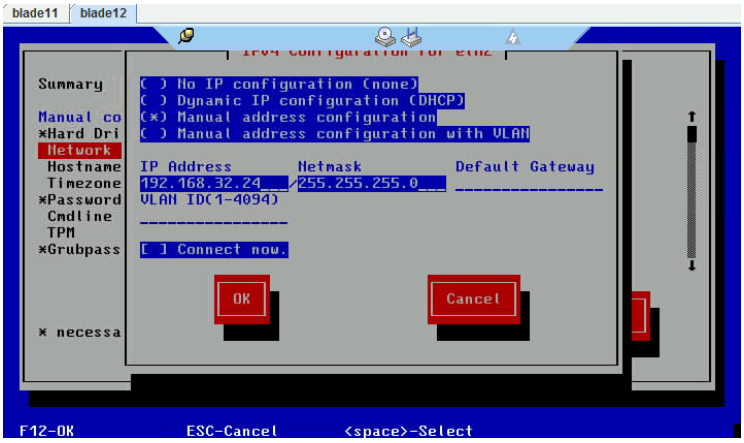


Figure 1-7 Configuring the network

Step 7 Set the default gateway address 192.168.32.1, move the cursor to **OK**, and press **Enter**.

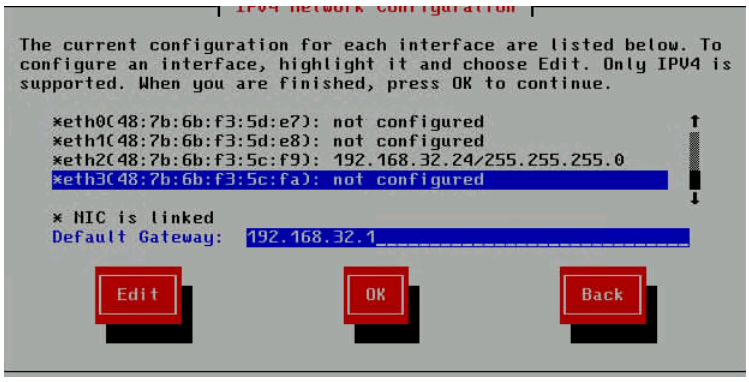
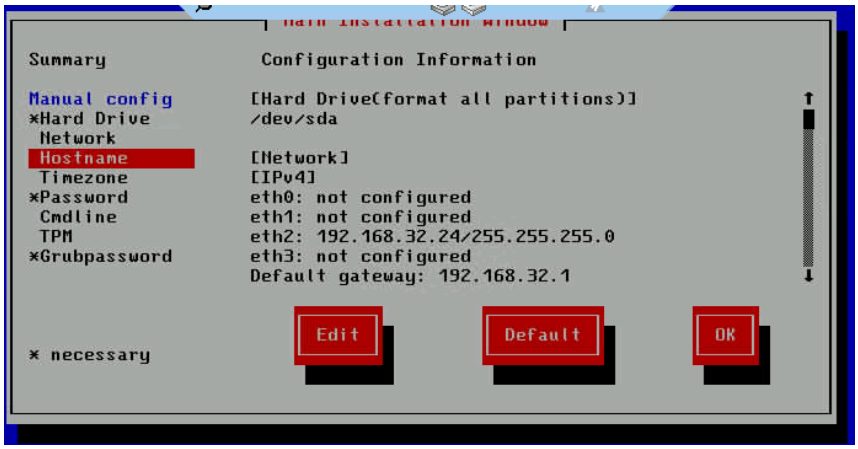


Figure 1-8 Configuring the gateway

Step 8 Move the cursor to **OK** and press **Enter** to complete the network configuration.

Step 9 Move the cursor to **Hostname**, press **Enter**, enter the host name **CNA01**, move the cursor to **OK**, and then press **Enter**. (Set the CNA02 host name to **CNA02**.)



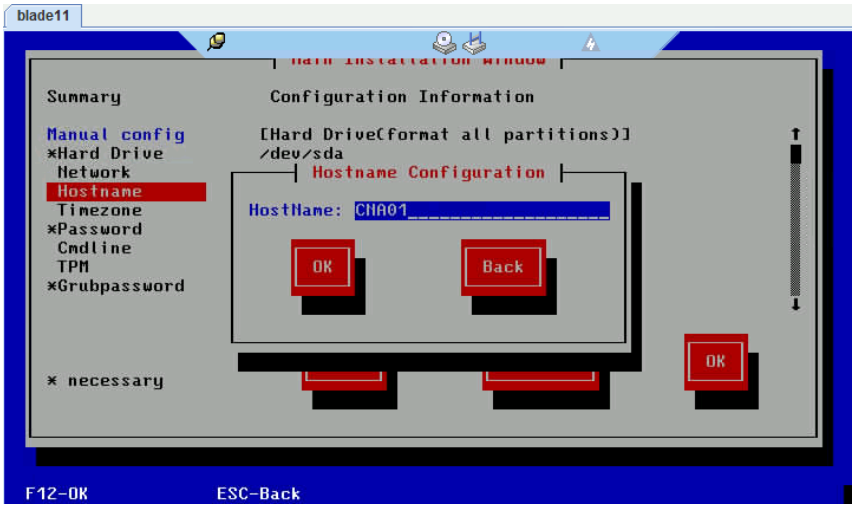


Figure 1-9 Setting the host name

Step 10 Move the cursor to **Timezone**, press **Enter**, and configure the clock based on the current time.

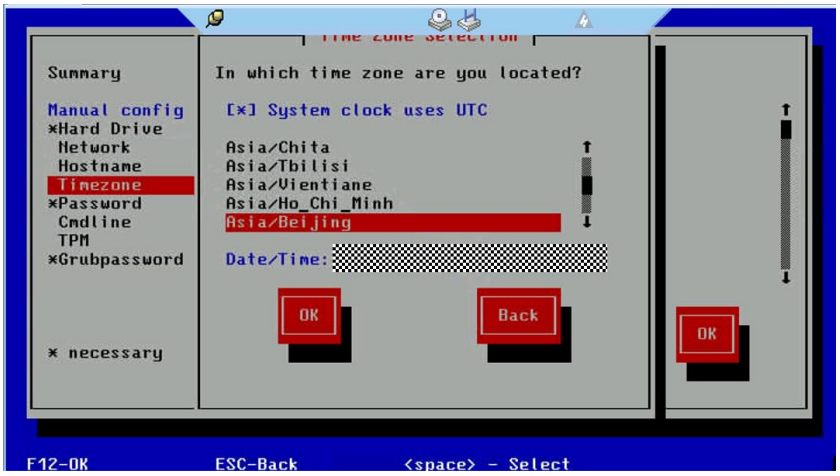
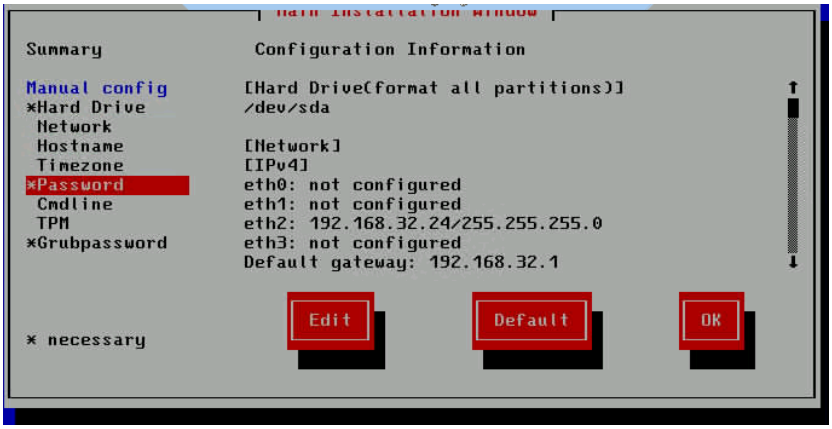


Figure 1-10 Setting the time zone

Step 11 Move the cursor to **Password** and press **Enter**. Enter the planned password for the **root** user to log in to CNA. Move the cursor to **OK** and press **Enter**.



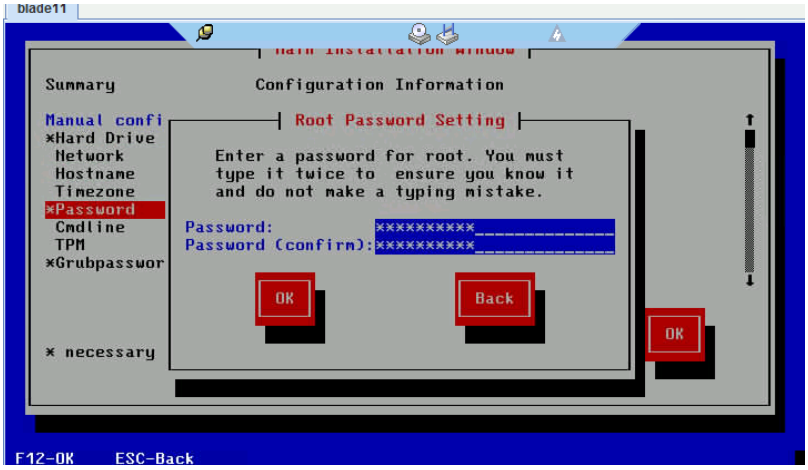


Figure 1-11 Setting the password for the root user to log in to the host

Step 12 Move the cursor to **Grubpassword**, press **Enter**, and enter **Grubpassword** as planned. Move the cursor to **OK** and press **Enter**.

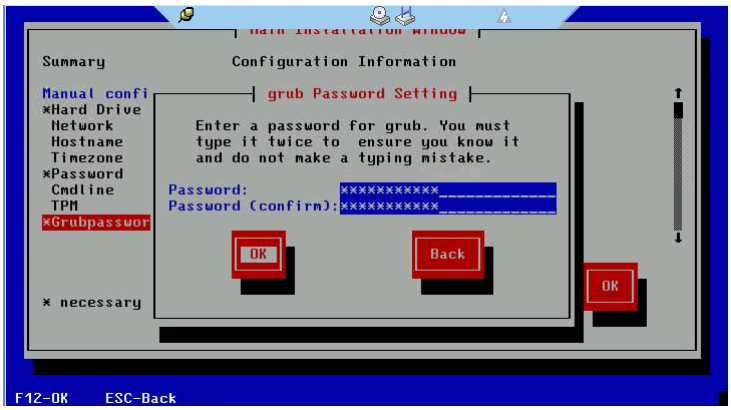
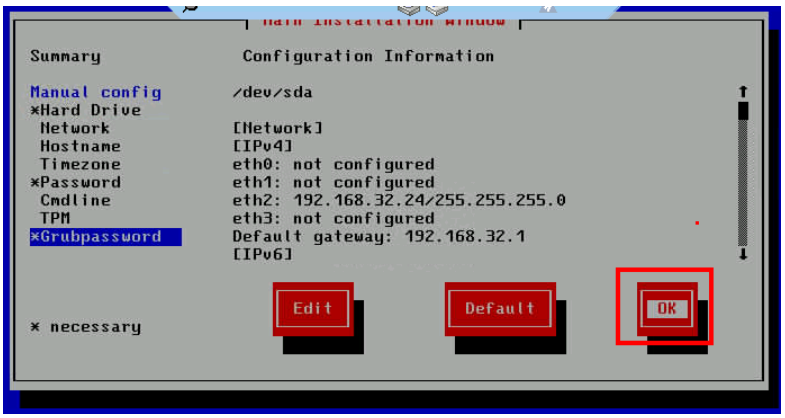


Figure 1-12 Setting a GRUB password

Step 13 Move the cursor to **OK** and press **Enter**. Select **yes** twice to go to the CNA installation page.



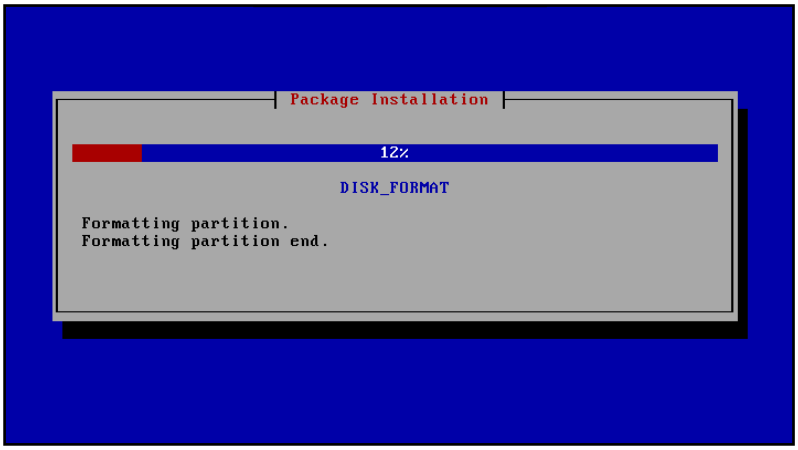


Figure 1-13 Installing the system

Step 14 Wait for about 3 to 6 minutes until the installation is complete. You can also install CNA02 in this period. After the installation progress reaches 100%, the CNA node restarts.

Step 15 Perform Step 1 to Step 14 again to install CNA02.

Step 16 Log in to the CLI of CNA01 as the **root** user.

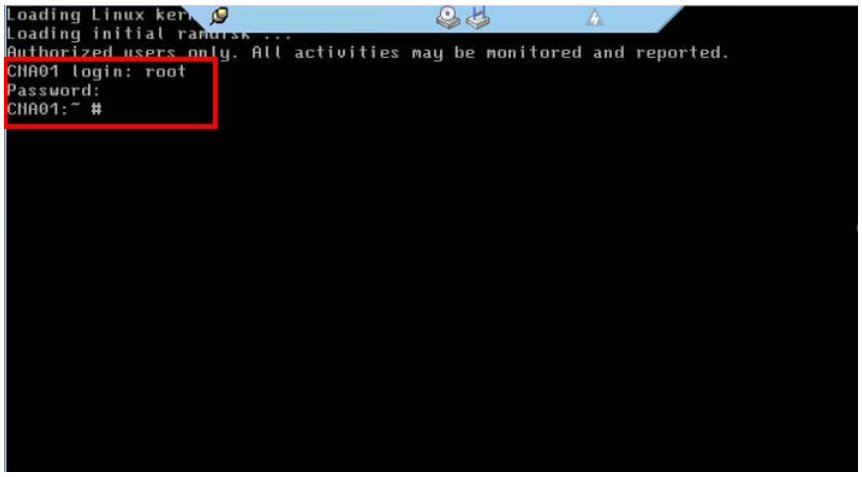


Figure 1-14 Logging in to CNA01 as the root user

Step 17 Set the password for the **gandalf** user to log in to CNA01.

```
CNA01:~#cnaInit
```

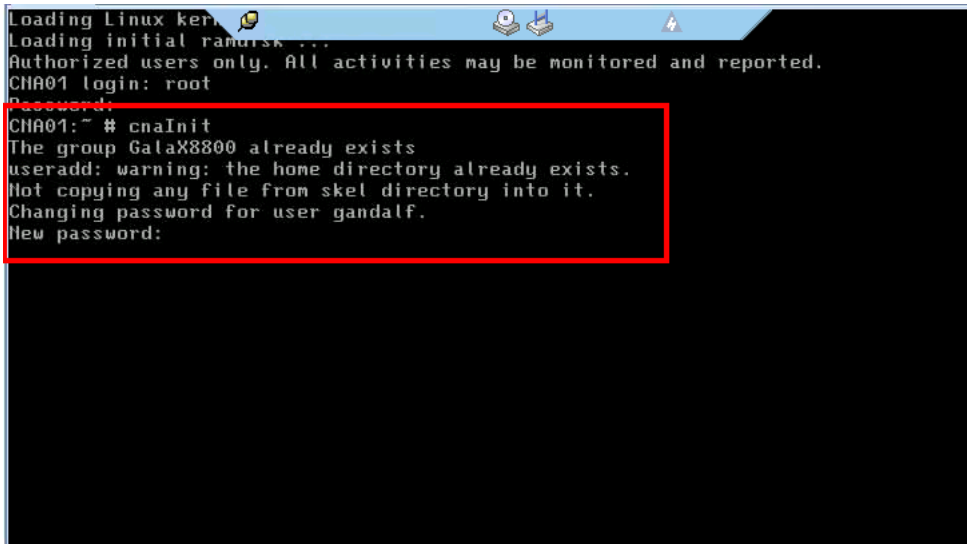


Figure 1-15 Setting the password for the gandalf user

Step 18 Enter a password for the **gandalf** user and confirm the password.

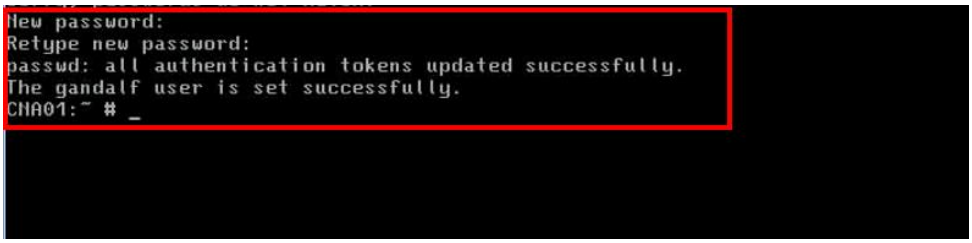


Figure 1-16 Setting the password for the gandalf user

Step 19 Use a terminal tool to log in to CNA01 as the **gandalf** user.

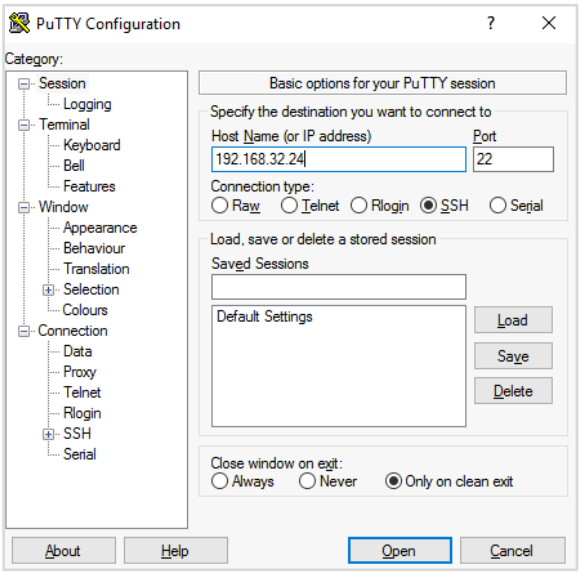


Figure 1-17 Remotely logging in to CNA01 as the gandalf user

Step 20 Switch to the **root** user and enter the password of the **root** user to log in.

```
[gandalf@CNA01 ~]$ su - root
```

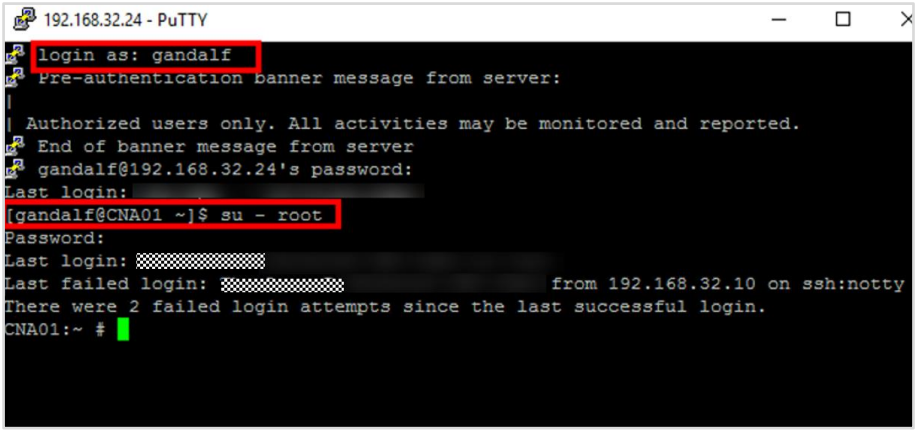


Figure 1-18 Switching to the root user

Step 21 Enable SFTP for CNA01.

```
CNA01:~ # sh /opt/galax/gms/common/util/configSshSftp.sh open
```

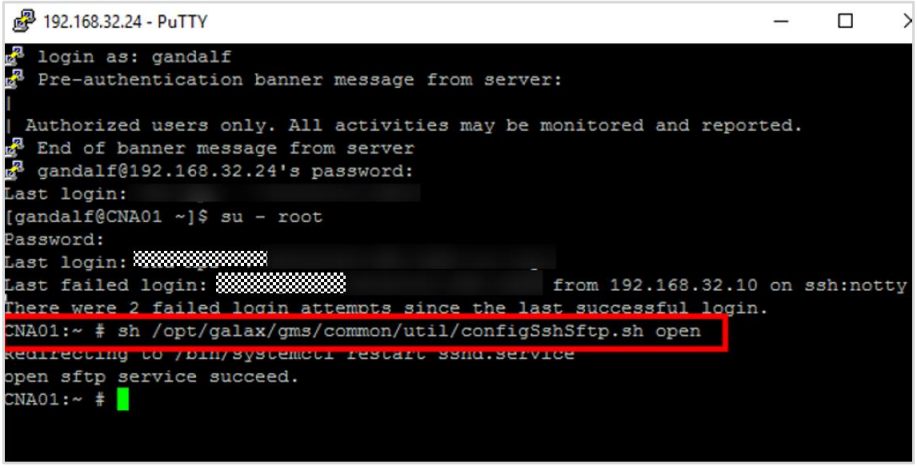


Figure 1-19 Enabling SFTP

Step 22 Use WinSCP (or another terminal tool such as MobaXterm) to log in to CNA01 as the **gandalf** user through SFTP.

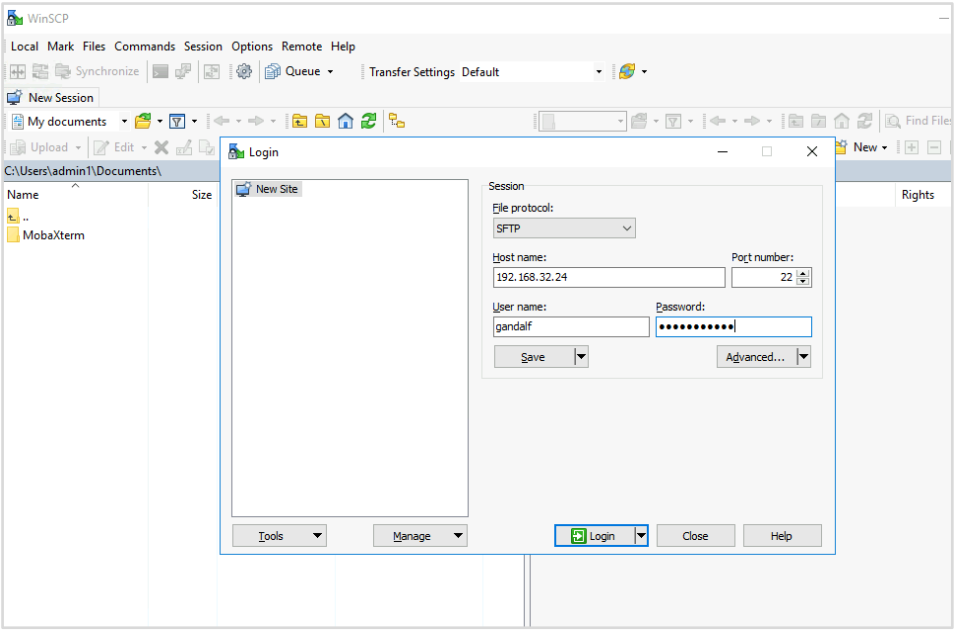
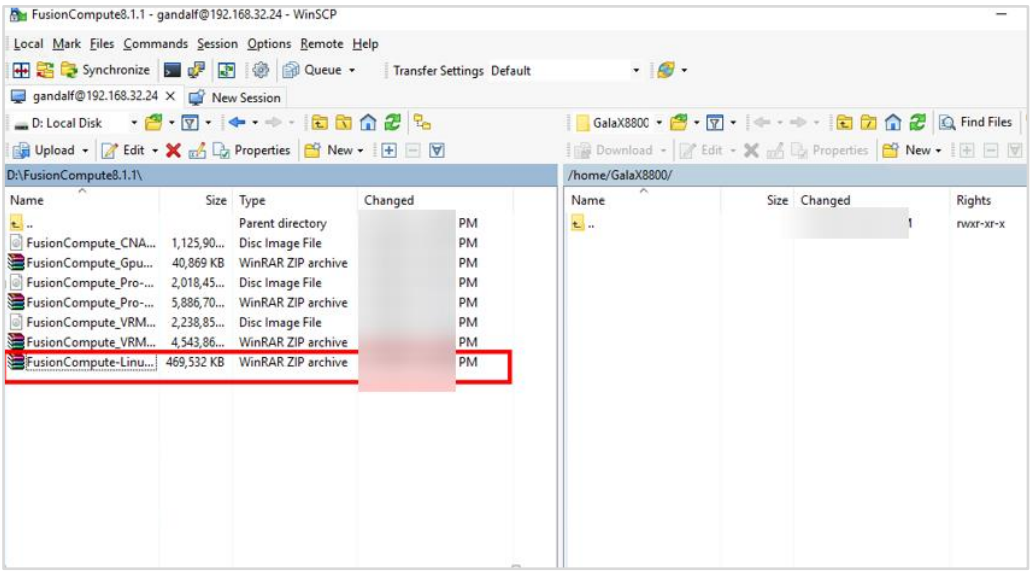


Figure 1-20 Remotely logging in to CNA01

Step 23 After login, find the **FusionCompute-LinuxInstaller-8.1.1-X86_64.zip** installation package on the left and drag it to the **/home/GalaX8800** directory on the right. In the dialog box that is displayed, click **OK**.



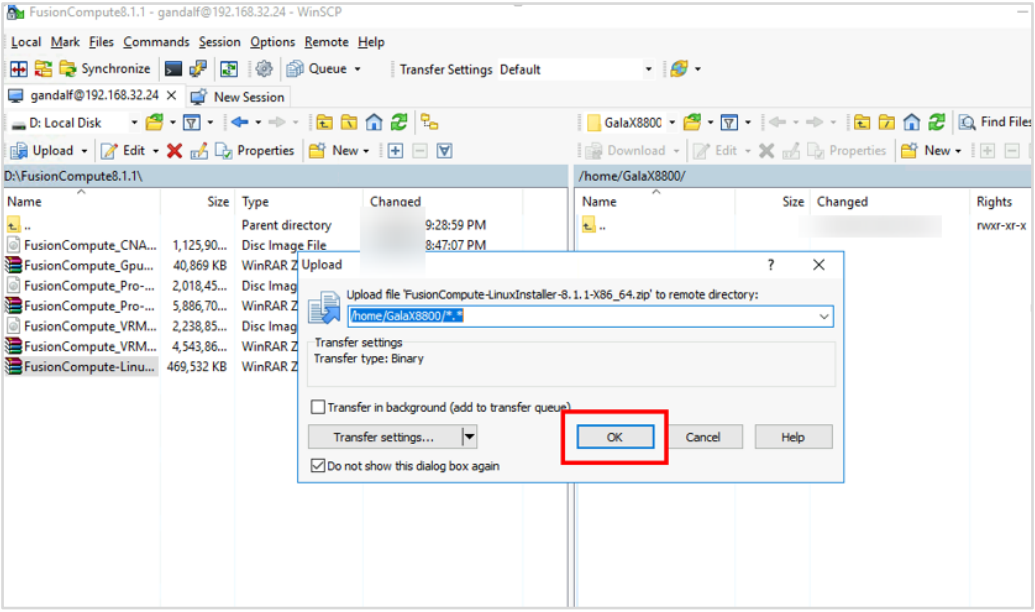


Figure 1-21 Uploading the installation package

Step 24 Open the CNA01 CLI you have logged in on PuTTY, go to the **/home/GalaX8800** directory and decompress the **FusionCompute-LinuxInstaller-8.1.1-X86_64.zip** package.

```
CNA01:~ # cd /home/GalaX8800/
CNA01: /home/GalaX8800 # unzip FusionCompute-LinuxInstaller-8.1.1-X86_64.zip
```

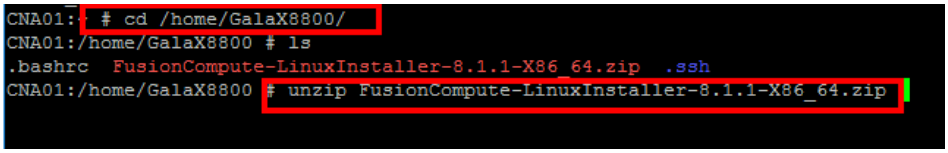


Figure 1-22 Decompress the installation package.

Step 25 Go to the **FusionCompute-LinuxInstaller-8.1.1-X86_64** folder and install the webInstaller tool.

```
CNA01: /home/GalaX8800 # cd FusionCompute-LinuxInstaller-8.1.1-X86_64
CNA01: /home/GalaX8800/ FusionCompute-LinuxInstaller-8.1.1-X86_64 # bash bin/webInstaller.sh
install
```

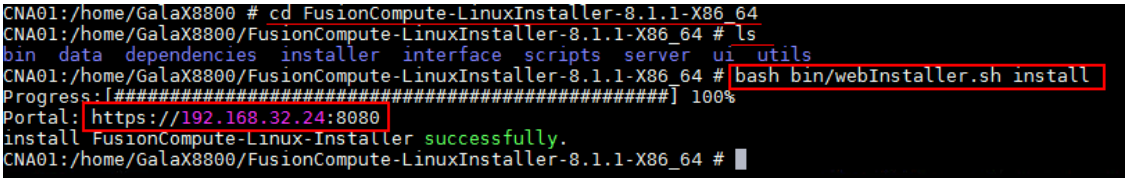


Figure 1-23 Running installation commands

Step 26 Open the browser on the jump server and enter **https://192.168.32.24:8080** (192.168.32.24 is the management IP address of CNA01) in the address box to open the login page of FusionCompute.

- Obtain the initial account and password in Table 1-5.
- Change the initial password, record the new password, and log in again.

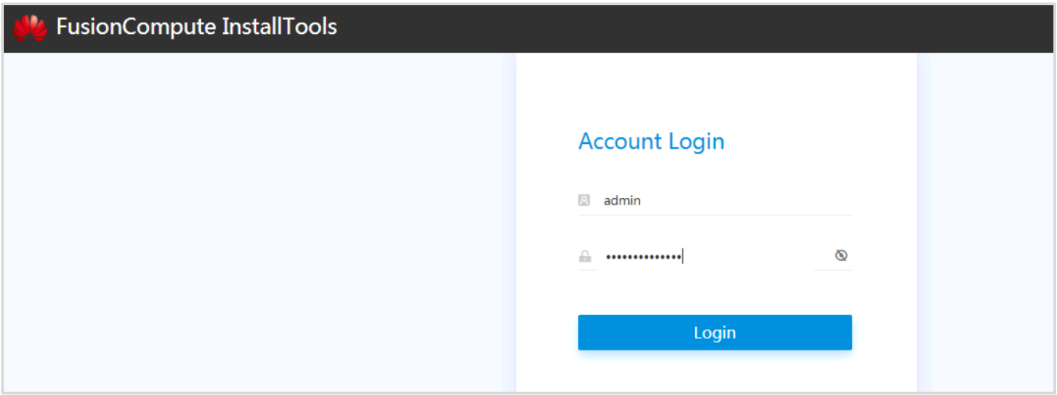


Figure 1-24 WebUI login page

(Note: If you click on the operation page after successfully logging in using the Firefox browser, you may be automatically logged out and a message is displayed, indicating that you have not logged in or the login times out.)

Possible cause: The time of the server where the FusionCompute web installation tool is deployed is not synchronized with the local time. As a result, the Firefox browser considers that the registered session has expired.

Solution: Change the local time or run the **data -s** *xx:xx:xx* command (*xx:xx:xx:xx* indicates hours:minutes:seconds respectively) on the server to ensure that the local time is the same as the time of the server where the web installation tool is deployed, refresh the browser, and log in again.)

1.3 VRM Installation

Step 1 Log in to FusionCompute InstallTools, set the installation language to **English**, choose **Custom Installation**, select **VRM** for **Components**, and click **Next**.

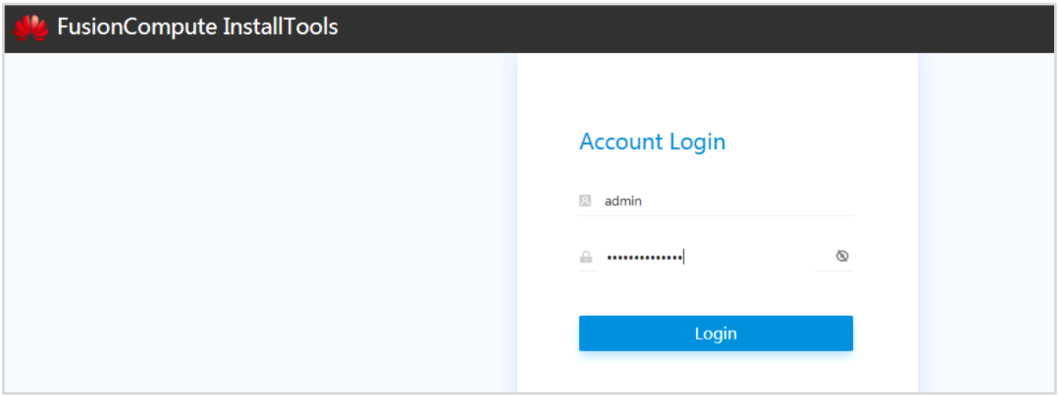


Figure 1-25 Logging in to FusionCompute

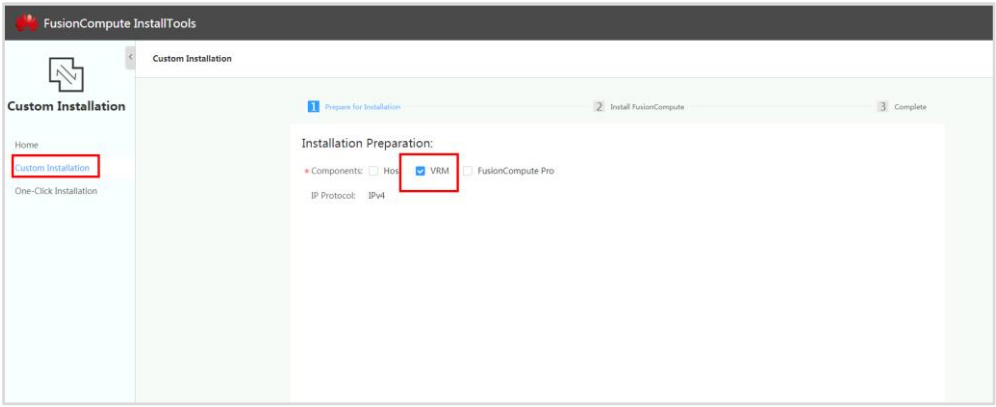


Figure 1-26 Selecting VRM

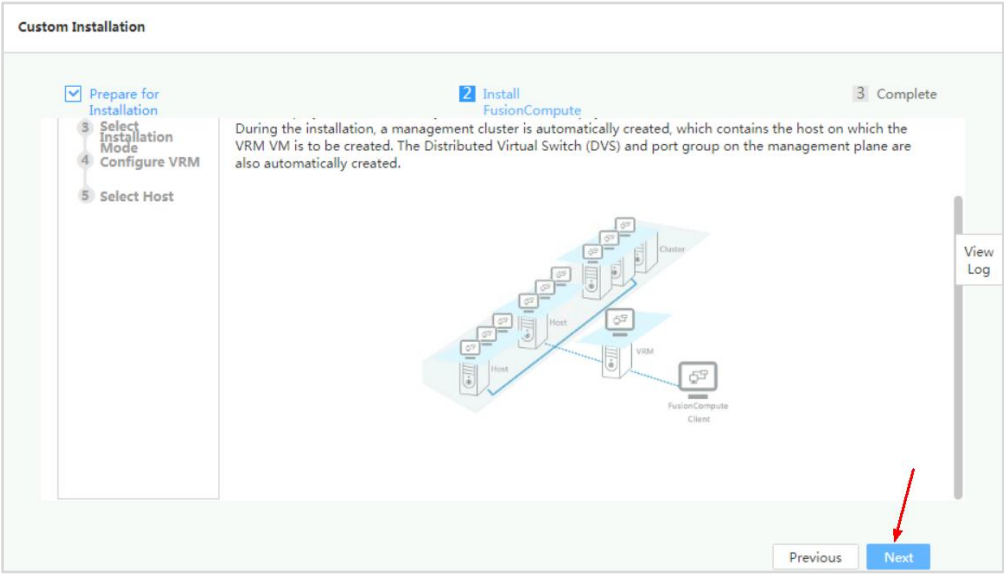


Figure 1-27 Clicking Next

Step 2 Click the position in the red box in the following figure and upload the installation package.

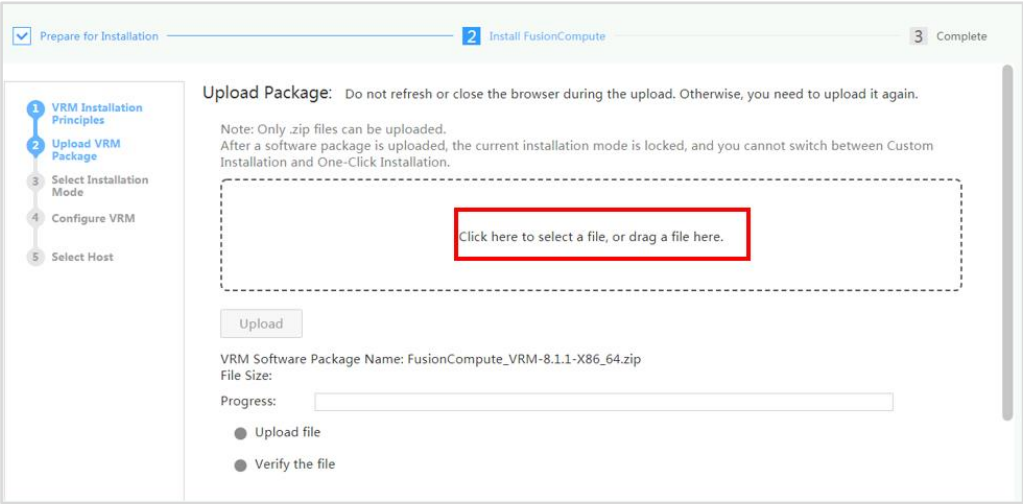


Figure 1-28 Uploading the installation package

Step 3 In the displayed dialog box, select the **FusionCompute_VRM-8.1.1-X86_64.zip** package and click **Open**.

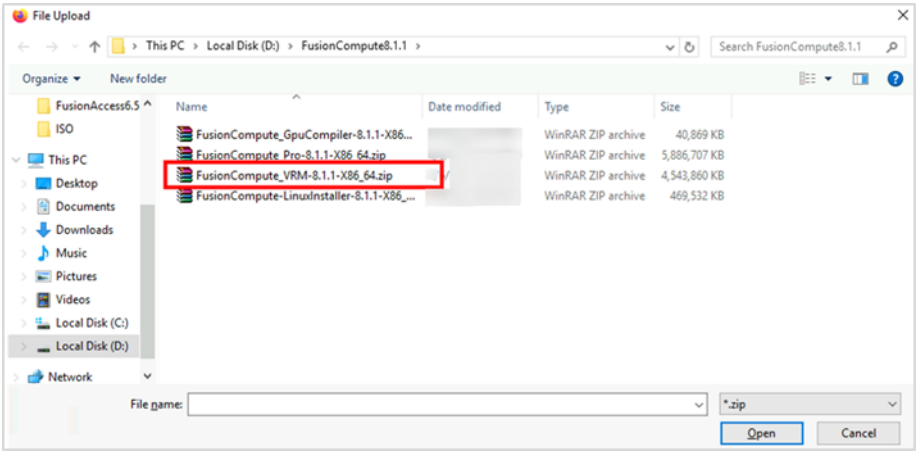


Figure 1-29 Selecting the VRM software package

Step 4 Click **Upload** to upload the software package. Click **Next** after the configuration is complete.

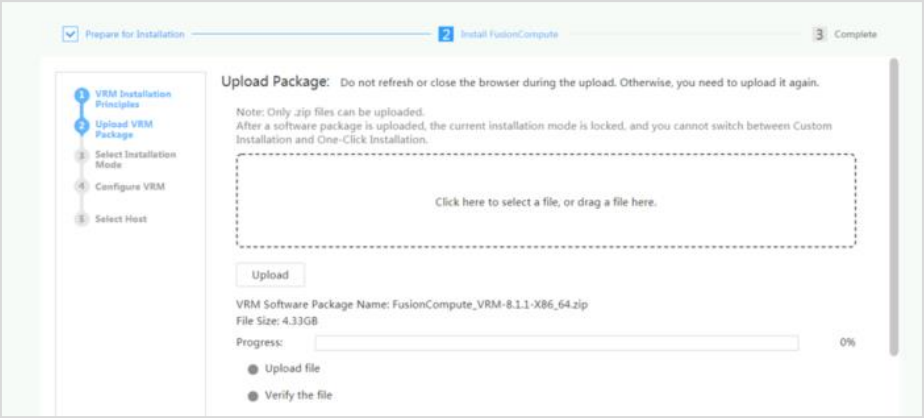


Figure 1-30 Uploading the software package

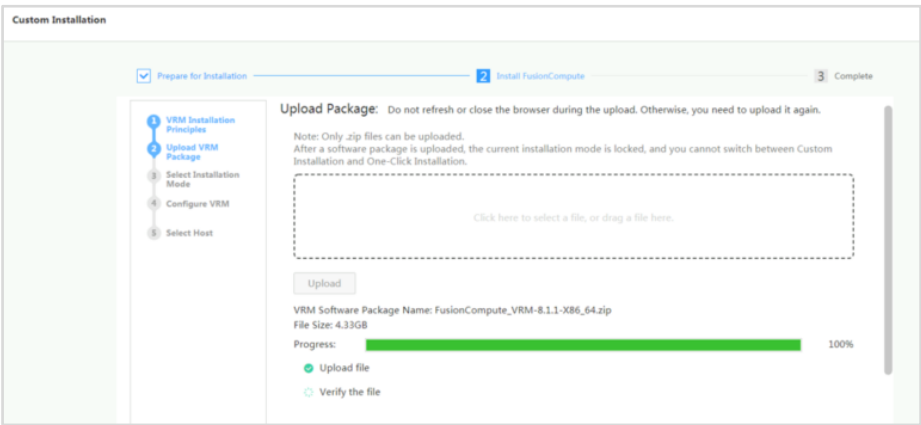


Figure 1-31 Software package uploaded successfully

Step 5 Click **Custom installation** and click **Next**.

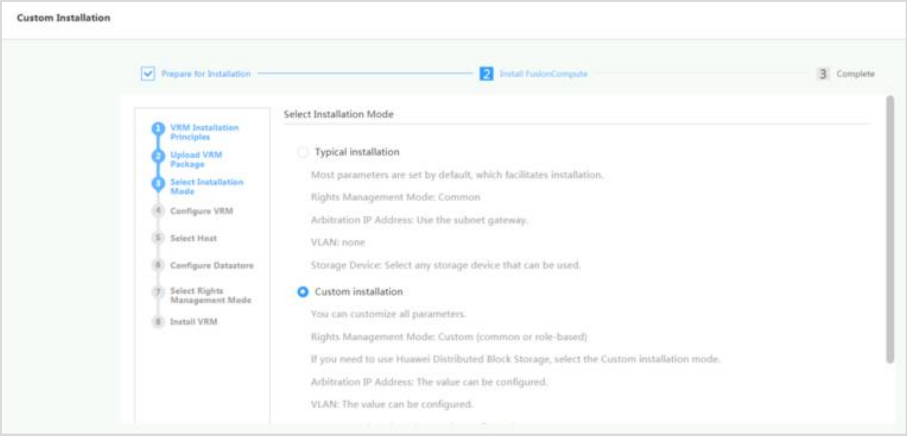


Figure 1-32 Clicking Custom installation

Step 6 The VRM setting page is displayed. Set VRM parameters as follows and click **Next**.

- **Installation Mode**: **Active/standby**
- **Configuration Mode**: **By scale**
- **Floating IP Address**: **192.168.32.35**
- **Active VRM Node Name** and **Active VRM Node IP Address**: **VRM01** and **192.168.32.36**, respectively
- **Standby VRM Node Name** and **Standby VRM Node IP Address**: **VRM02** and **192.168.32.37**, respectively
- **Subnet Mask**: **255.255.255.0**
- **Subnet Gateway**: **192.168.32.1**
- **Quorum IP Address 01**: **192.168.32.1**
- Set other parameters as planned.

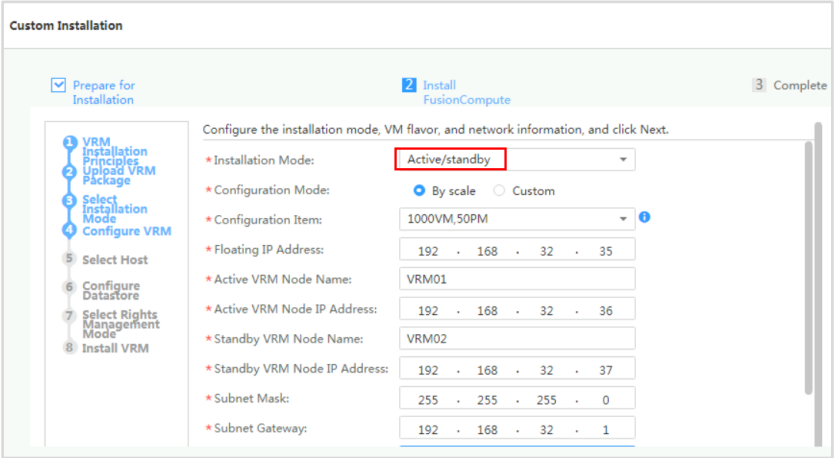


Figure 1-33 Setting VRM parameters

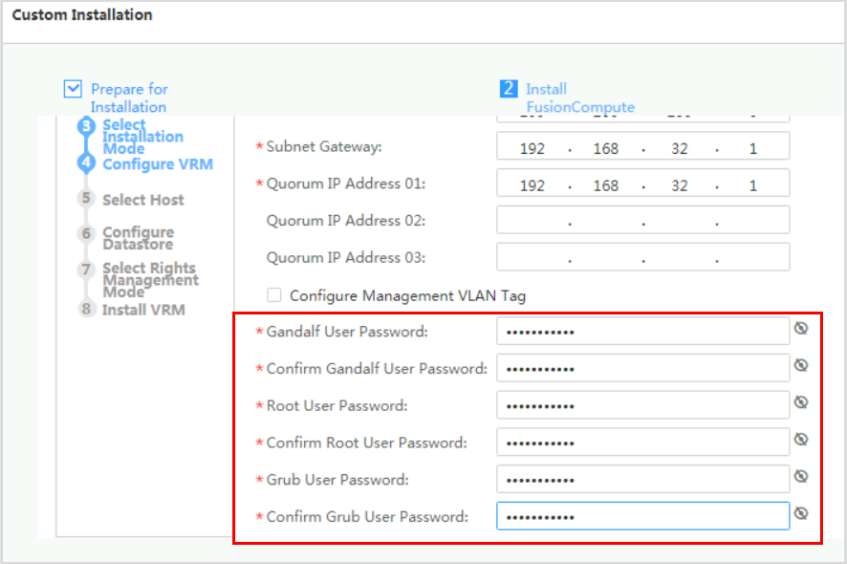


Figure 1-34 Setting VRM parameters

Step 7 Enter information about the CNA01 and CNA02 hosts, and click **Configure Host**.

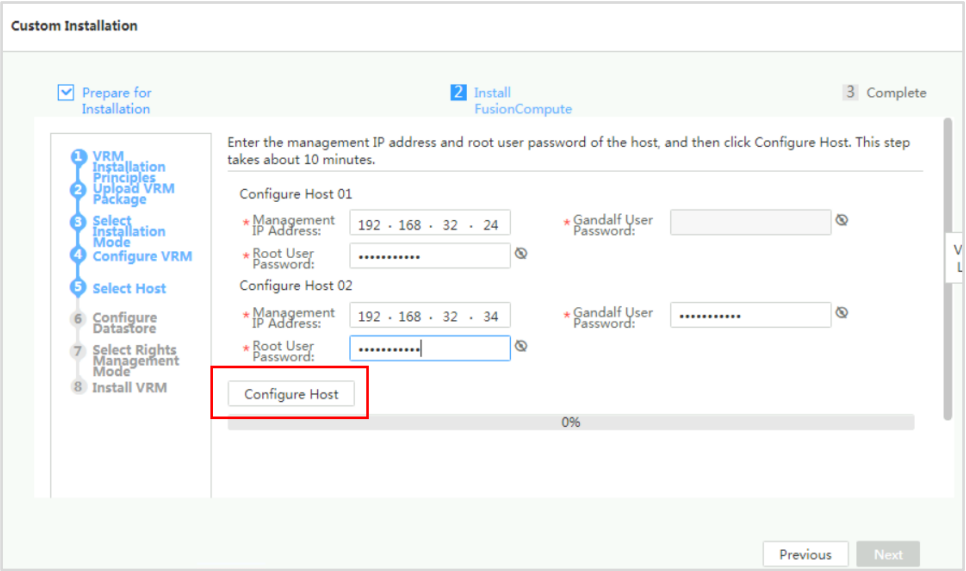


Figure 1-35 Configuring hosts

(This step takes about 5 to 10 minutes.)

Step 8 Wait until the configuration is complete and click **Next**.

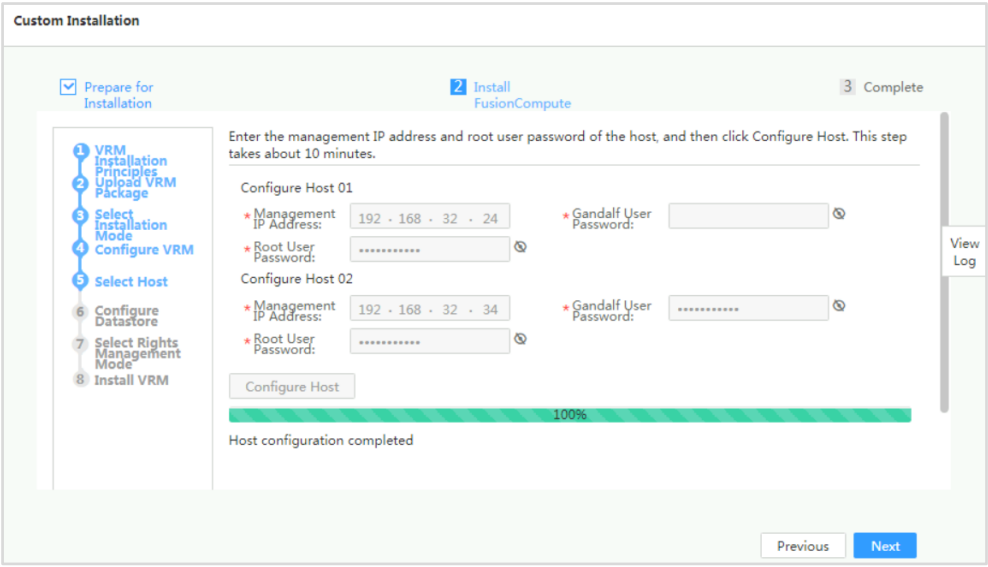


Figure 1-36 Host configuration completed

(The size of CNA host disk space cannot be less than 140 GB. Otherwise, the datastores cannot be discovered.)

Step 9 Select a local storage for each node and click **Next**.

(Select disks based on the site requirements.)

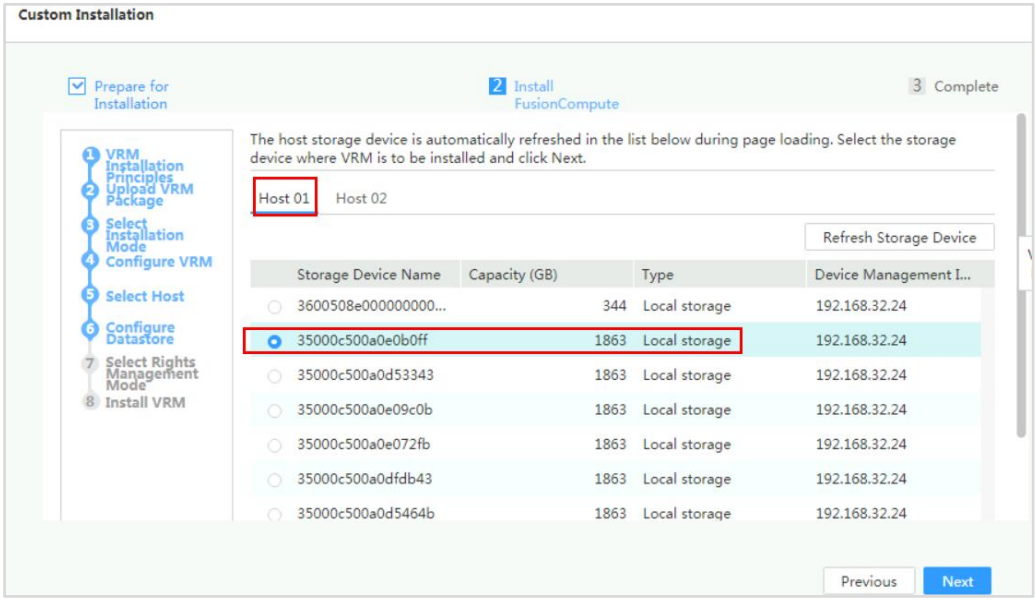


Figure 1-37 Host 01

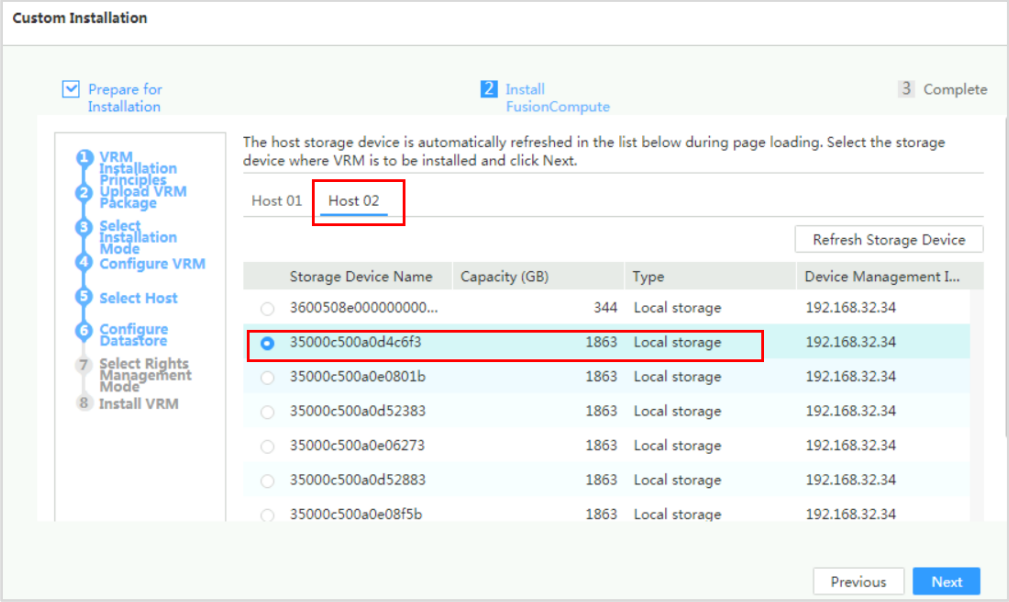


Figure 1-38 Host 02

Step 10 Set the password of the VRM **admin** user as planned and click **Next**.

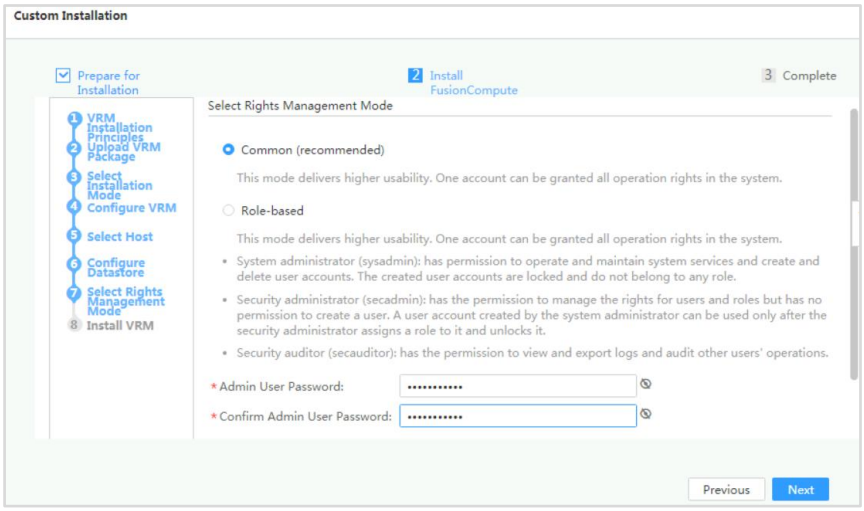


Figure 1-39 Configuring the login password

Step 11 After installation is complete, click **Next** to view the FusionCompute login information.

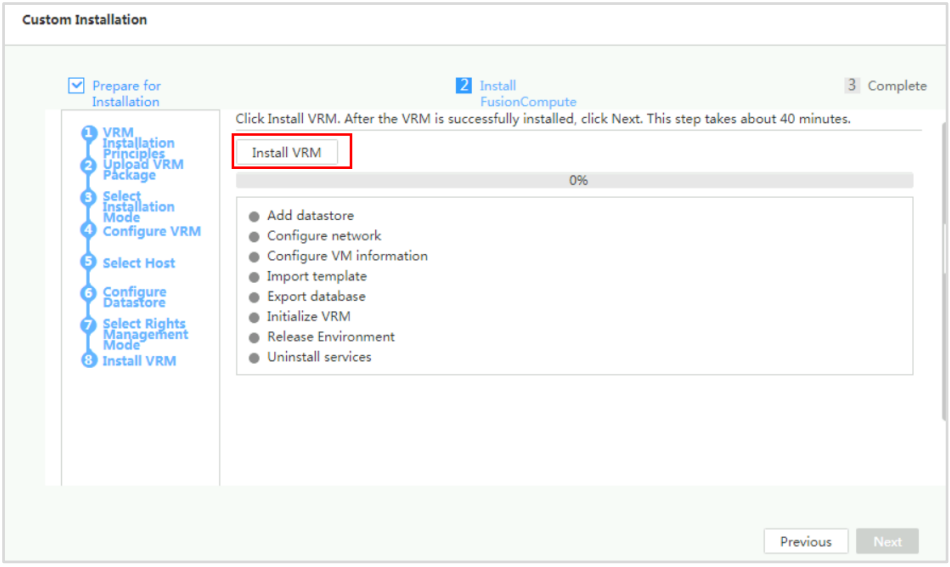


Figure 1-40 Installing VRM

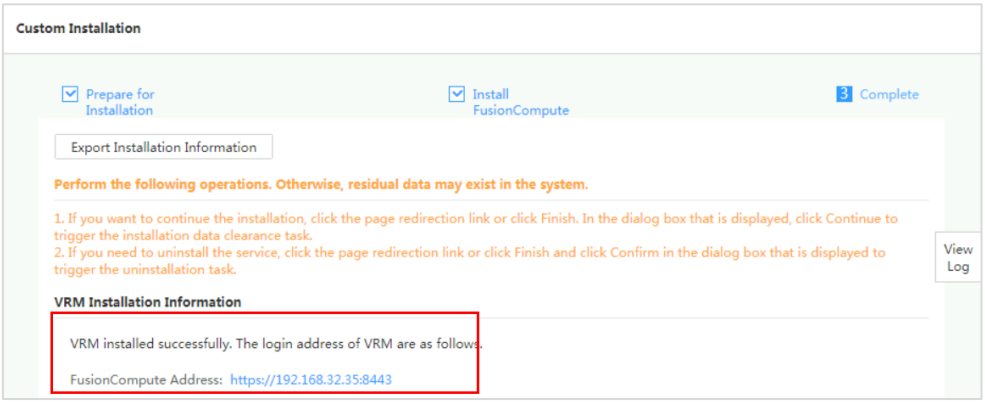


Figure 1-41 VRM installed

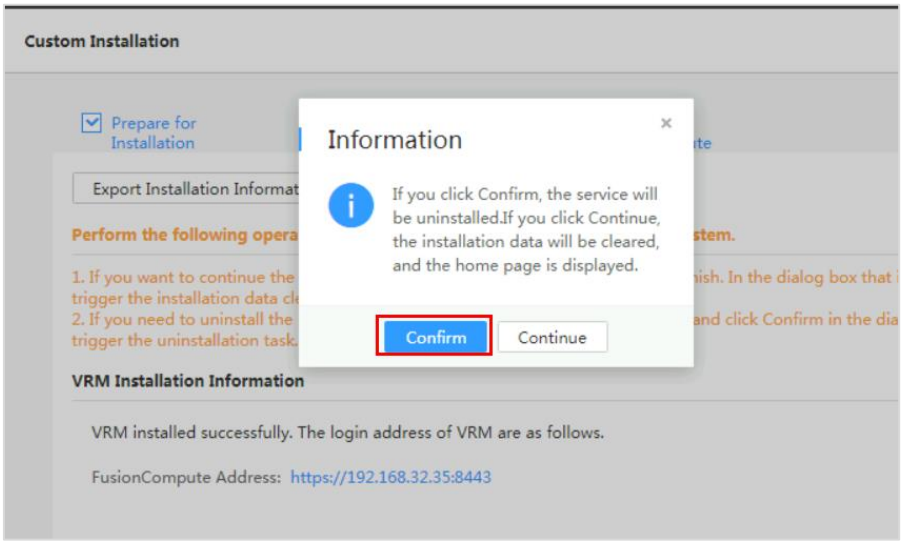


Figure 1-42 Clicking Confirm

Step 12 Open your browser, enter the FusionCompute login address (VRM floating IP address, which is 192.168.32.35 in this exercise) in the address box, and press **Enter**. In the dialog box that is displayed, click **OK** to accept the license agreement. Enter the user name **admin** and the configured password, and click **Login**.

(If no commercial license is loaded to the system, free trial will expire in 90 days.)

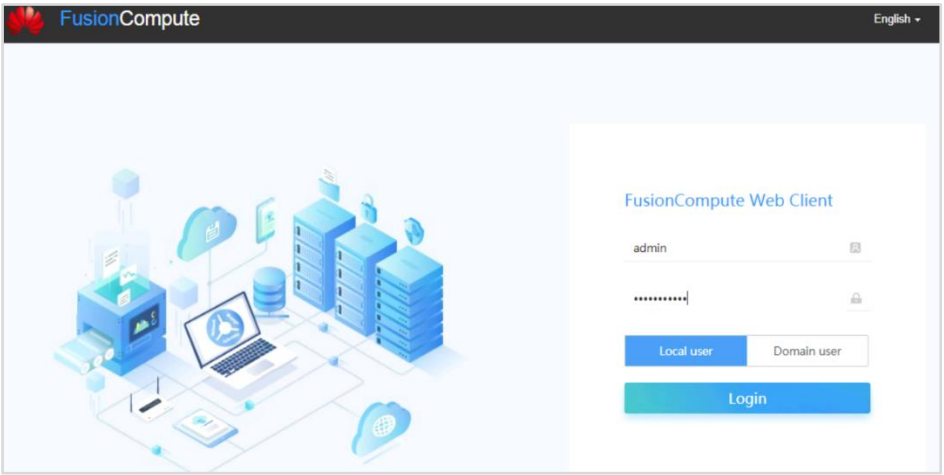


Figure 1-43 Logging in to FusionCompute

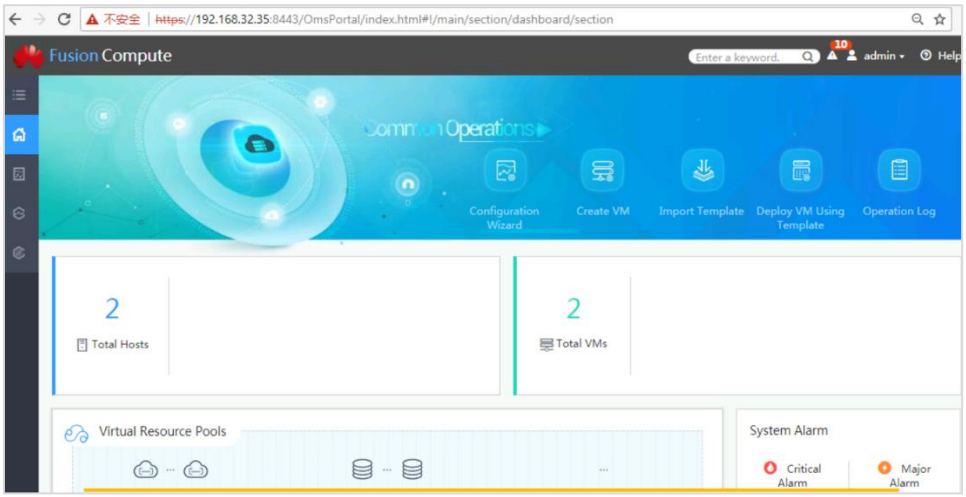


Figure 1-44 Logged in successfully (ignoring system alarms)

Step 13 Choose **Help** > **About** in the upper right corner to check the version.

Figure 1-45 Checking the version

1.4 Quiz

What are the principles for deploying FusionCompute hosts?

Answers:

Deployment principles: Multiple hosts can be deployed based on customer requirements for compute resources. The hosts also provide storage resources if local hard disks are used to provide storage resources. If a small number of hosts, for example, fewer than 10 hosts, are deployed, you can add all the hosts to the management cluster, which therefore also provides user services. If a large number of hosts are deployed, you can add the hosts to one or more service clusters by service to facilitate service management.

2 FusionCompute Resource Management

2.1 Compute Resource Management

2.1.1 Introduction

2.1.1.1 About This Exercise

This exercise illustrates how to configure compute resources on the installed FusionCompute as an administrator, to facilitate cluster capacity expansion and host moving during employee training.

2.1.1.2 Objectives

- Understand clusters, hosts, and the relationship between hosts and clusters.
- Describe the cluster operation process and configure a cluster policy.
- Understand host operations and related parameters.

2.1.1.3 Procedure

Figure 2-1 Procedure

2.1.2 Creating a Cluster

Step 1 Log in to FusionCompute. Choose **Resource Pools**.

Step 2 Click **Create Cluster**.

Step 3 Set basic cluster parameters to those shown in the following figure and click **Next**.

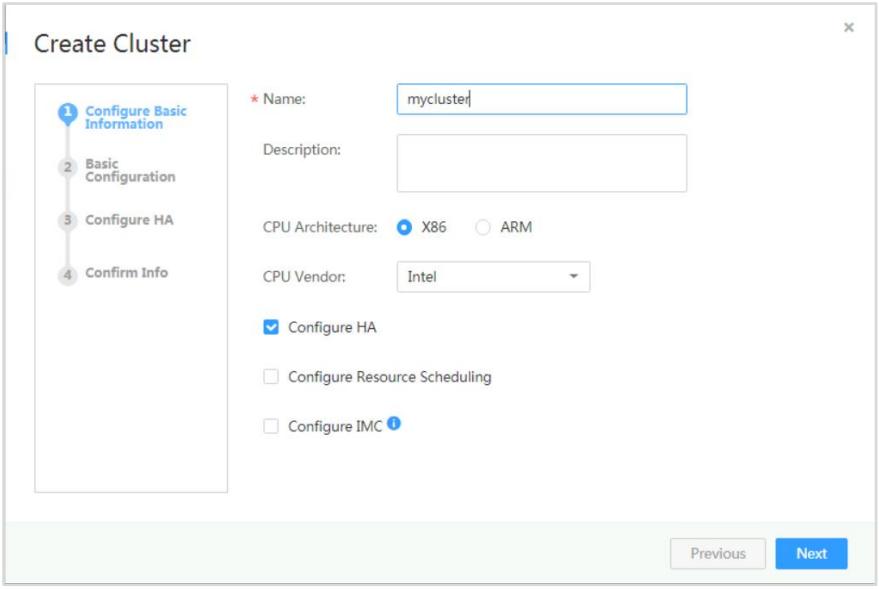


Figure 2-2 Create Cluster

Step 4 In the **Basic Configuration** pane, use the default settings and click **Next**.

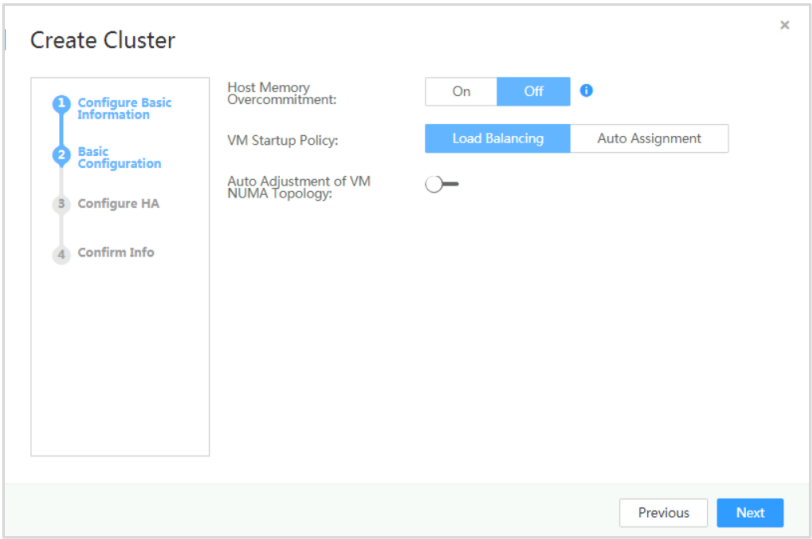


Figure 2-3 Base Configuration

Step 5 In the **Configure HA** pane, use the default settings and click **Next**.

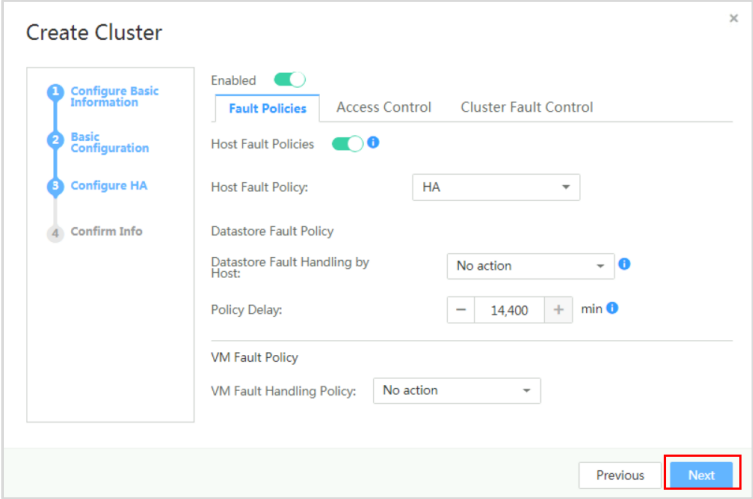


Figure 2-4 Configuring HA

Step 6 Click **OK** to complete cluster creation.

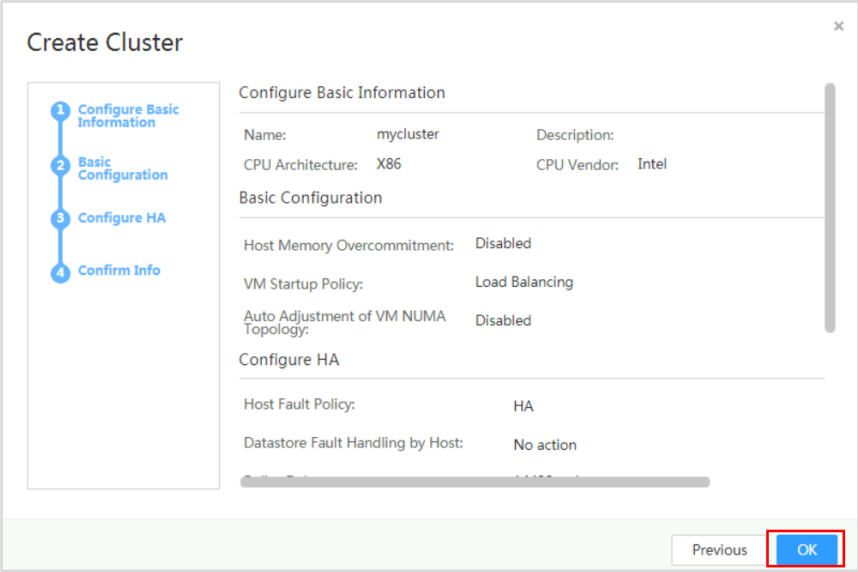


Figure 2-5 Clicking OK

2.1.3 Moving a Host

Step 1 Choose **Resource Pools** > **ManagementCluster** > **CNA01**.

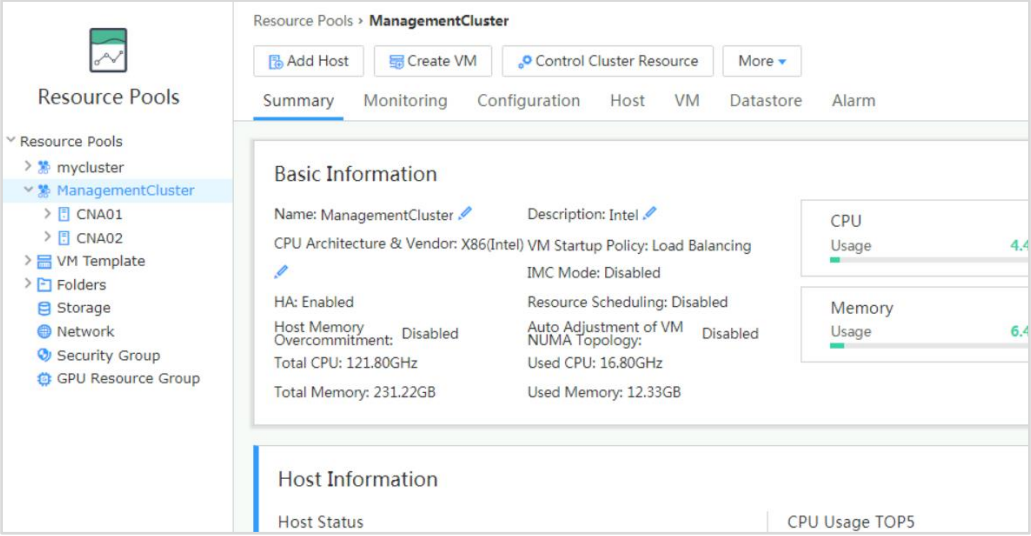


Figure 2-6 Accessing the CNA01 management page

Step 2 Click **More** and choose **Move**.

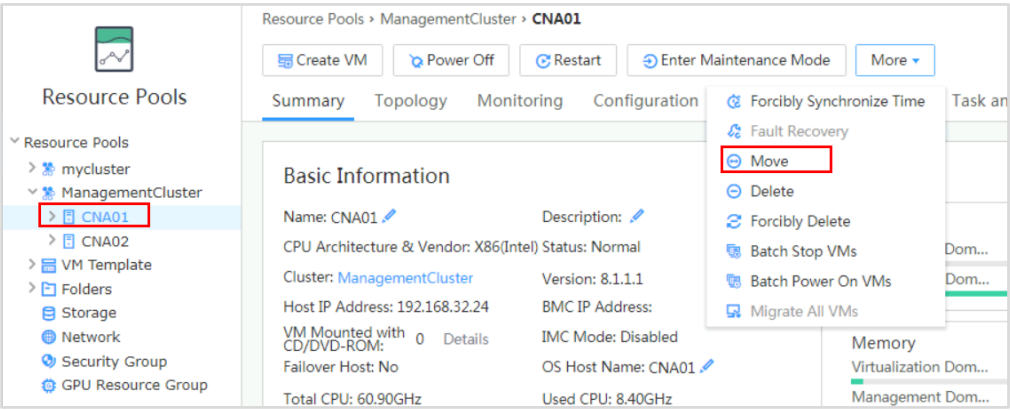


Figure 2-7 Choosing Move

Step 3 Select **mycluster** and click **OK** to move the CNA01 host to the mycluster cluster.

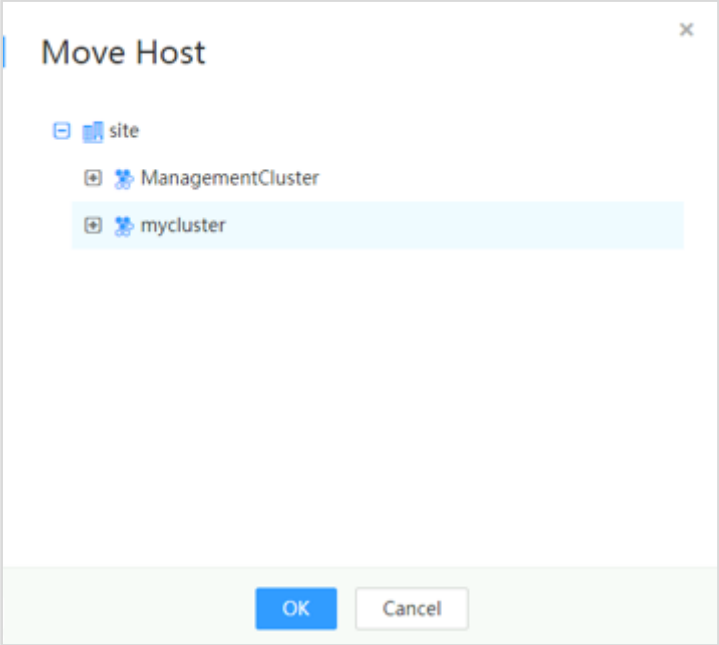


Figure 2-8 Moving a host to the mycluster cluster

Step 4 Repeat Step 2 and Step 3 to move the CNA02 host to the mycluster cluster.

Step 5 Choose **Resource Pools** > **mycluster** > **CNA01** and **Resource Pools** > **mycluster** > **CNA02**. Information about the two hosts is displayed in the pane on the right.

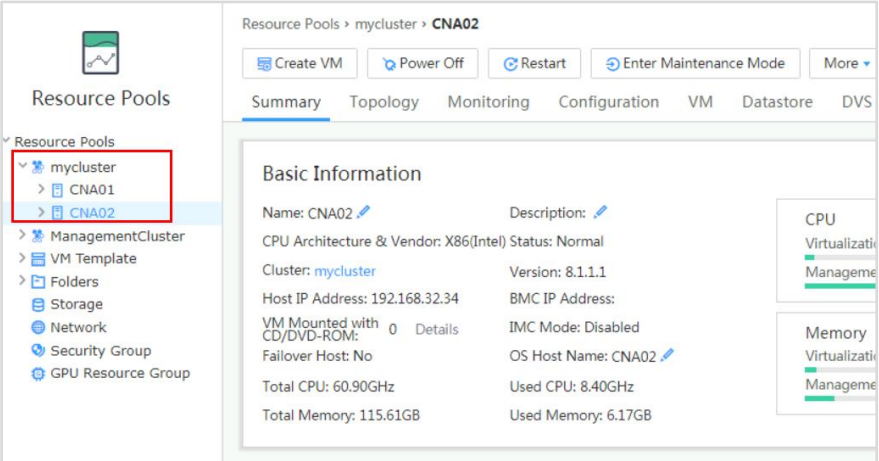


Figure 2-9 Both hosts moved to the mycluster cluster

2.1.4 Deleting a Cluster

Step 1 Choose **Resource Pools** > **ManagementCluster**. Click **More** and choose **Delete**.

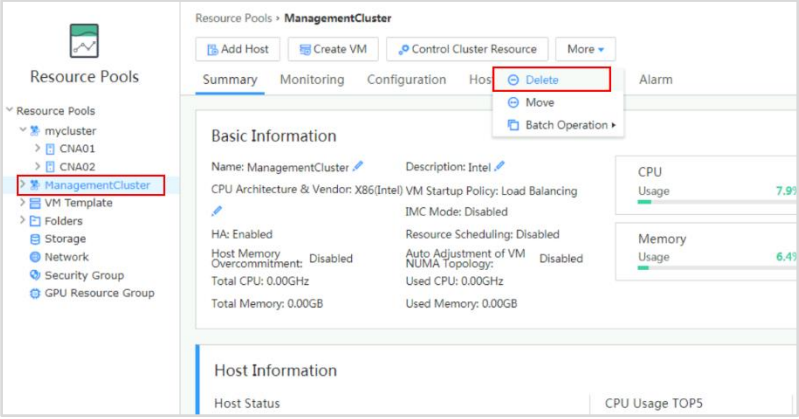


Figure 2-10 Deleting empty cluster ManagementCluster

Step 2 In the displayed dialog box, click **OK** to delete ManagementCluster.

2.1.5 Configuring Cluster Policies

Step 1 Choose **Resource Pools** > **mycluster**. Click the **Configuration** tab to view the cluster configuration.

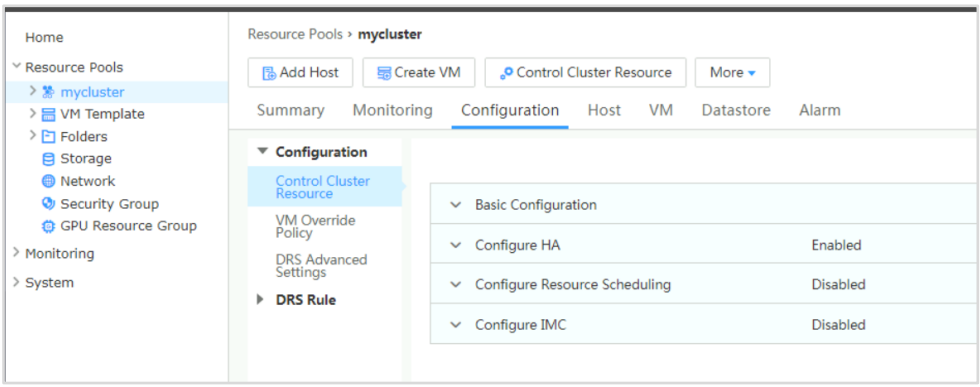
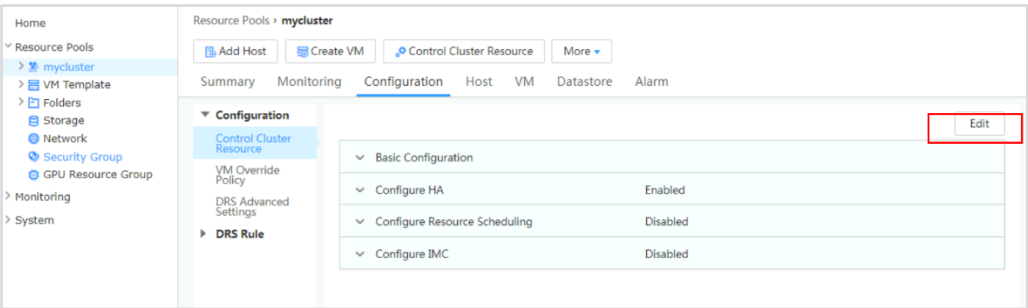


Figure 2-11 Configuration tab page

Step 2 Click **Edit** in the upper right corner of the **Configuration** tab page. In the **Control Cluster Resource** pane, toggle on **Auto Adjustment of VM NUMA Topology**. Click **OK** to close the **Control Cluster Resource** pane.



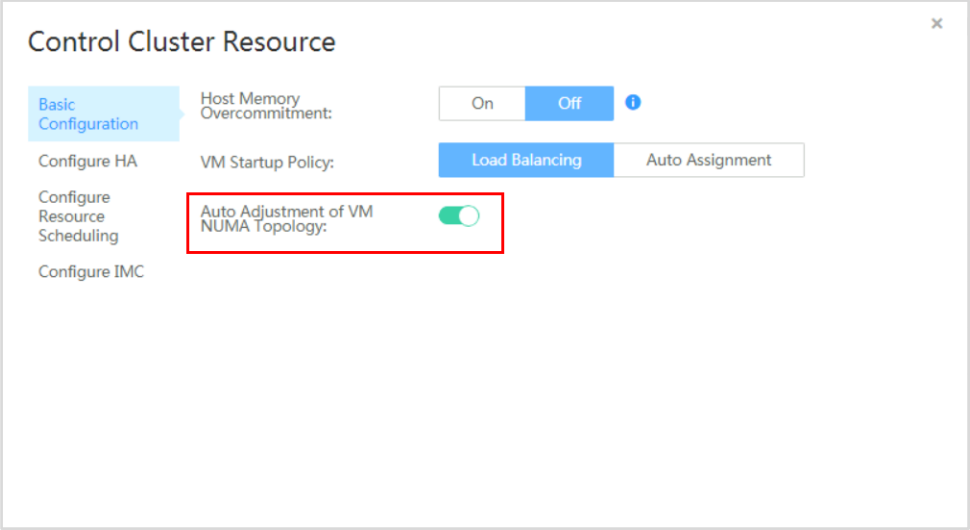


Figure 2-12 Toggling on Auto Adjustment of VM NUMA Topology

Step 3 On the **Configuration** tab page, verify that the function has been enabled.

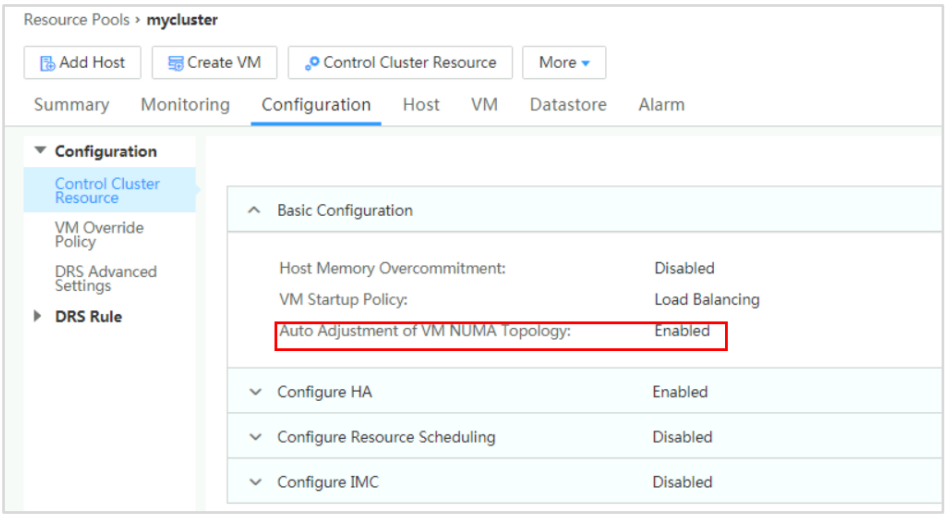


Figure 2-13 Verifying that the function has been enabled

Step 4 Repeat Step 1 and Step 2 to toggle off **Auto Adjustment of VM NUMA Topology**.

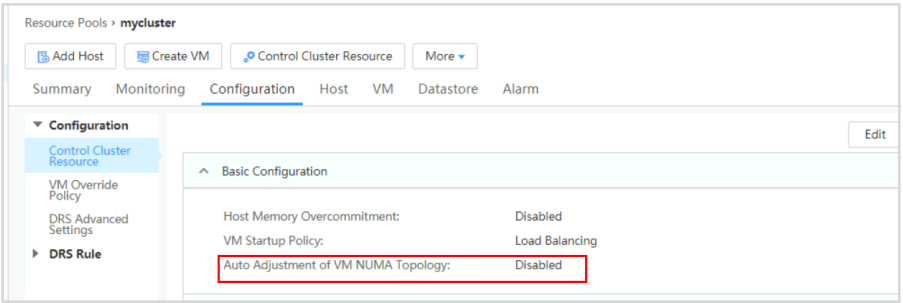


Figure 2-14 Verifying that the function has been disabled

2.2 Storage Resource Management

2.2.1 Introduction

2.2.1.1 About This Exercise

This exercise illustrates how to configure storage resources on the installed FusionCompute. You need to connect backend SAN storage devices to FusionCompute and manage disks on FusionCompute, to facilitate subsequent services such as high availability (HA) and live migration.

2.2.1.2 Objectives

- Understand the FusionCompute storage model.
- Create storage network ports and understand related parameters.
- Add universal IP-SAN storage.
- Configure storage resources.
- Create a disk and understand related parameters.

2.2.1.3 Procedure

Figure 2-15 Procedure

2.2.2 Configuring Storage Ports

2.2.2.1 Changing the iSCSI Initiator WWN of a Host

Step 1 Choose **Resource Pools** > **mycluster** > **CNA01**. Click the **Configuration** tab.

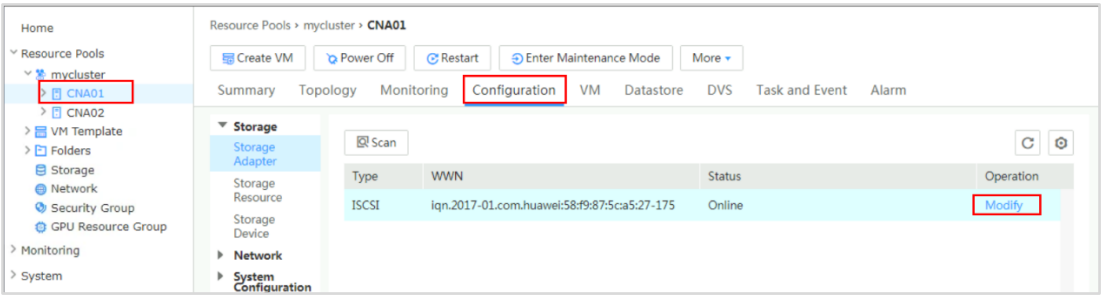


Figure 2-16 Configuration tab page

Step 2 Click **Modify** in the **Storage Adapter** pane and change the WWN of CNA01 to **iqn.20*XX*.huawei.hcia:cna01**.

Figure 2-17 Changing the WWN of CNA01

Step 3 Repeat the preceding two steps to change the iSCSI initiator WWN of CNA02 to **iqn.20*XX*.huawei.hcia:cna02**.

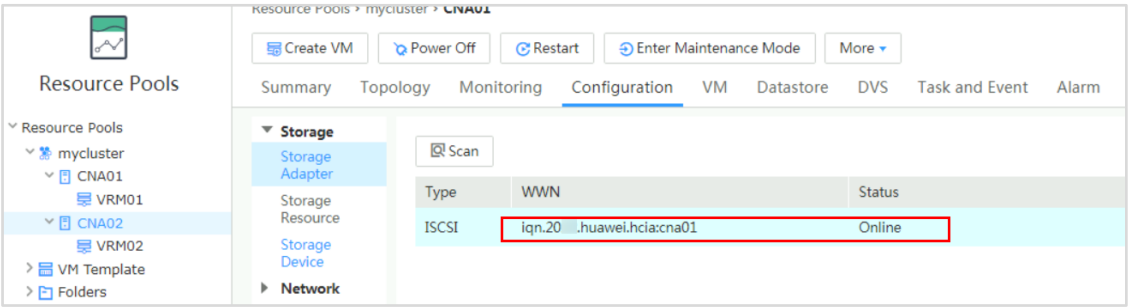


Figure 2-18 Changing the WWN of CNA02

2.2.2.2 Adding Storage Ports

Step 1 Choose **Resource Pools** > **mycluster** > **CNA01**. Click the **Configuration** tab.

Step 2 Choose **Network** > **Logical Interface** on the **Configuration** tab page.

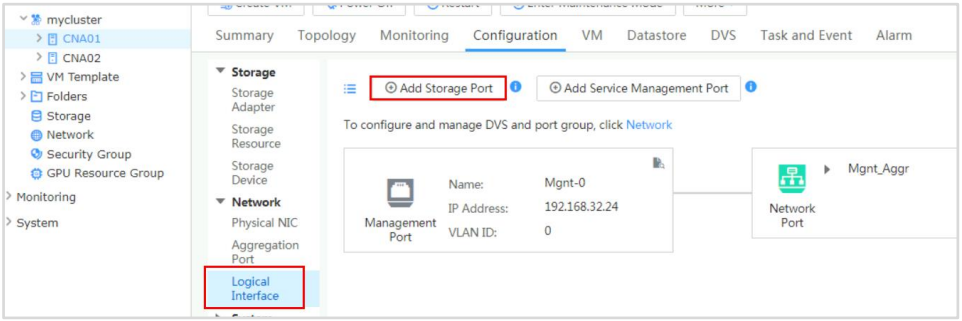


Figure 2-19 Configuring a logical interface

Step 3 Click **Add Storage Port**. Select **eth0** and click **Next**.

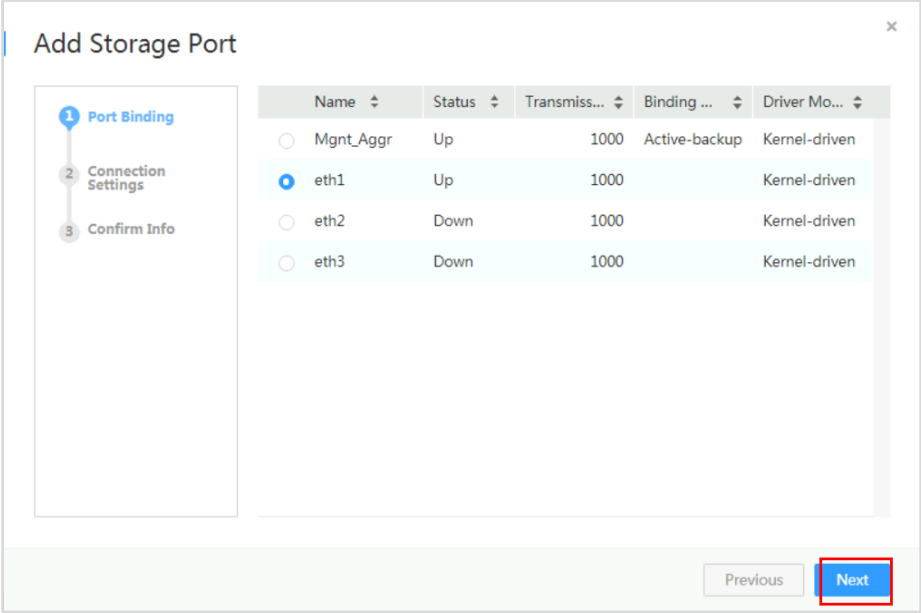


Figure 2-20 Selecting a storage port

Step 4 Enter the storage port information (set **VLAN ID** to **96** and **IPv4 Address** to **192.168.96.131**) of the CNA01 host, as shown in the following figure. (Set **IPv4 Address** to **192.168.96.132** for CNA02.)

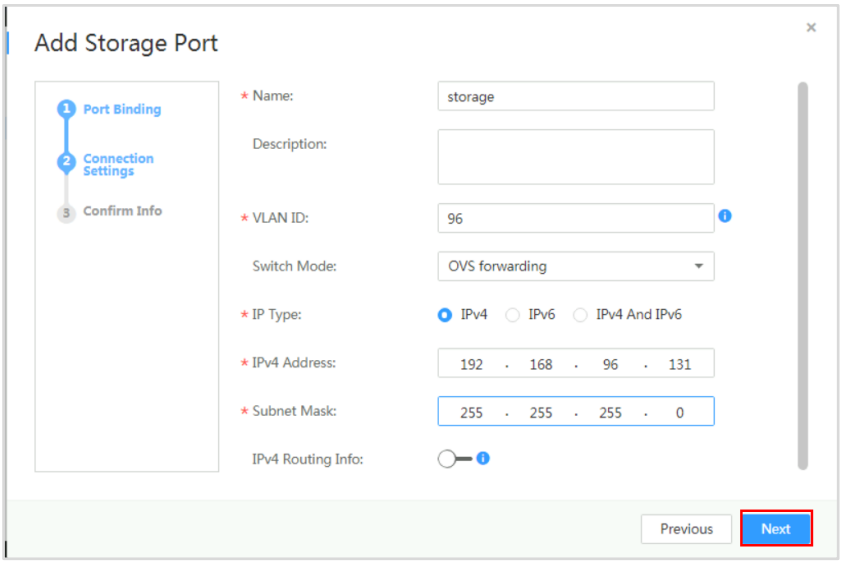


Figure 2-21 Configuring storage information

Step 5 Click **Next**. Confirm the information and click **OK**.

Step 6 Repeat the preceding steps to add a storage port to the CNA02 host.

2.2.3 Adding IP SAN Storage

2.2.3.1 Adding Storage Resources

- The trainer must ensure that the corresponding service port IP addresses have been configured on the storage device before this experiment.

Step 1 Choose **Resource Pools** > **Storage**. Click the **Storage Resources** tab.

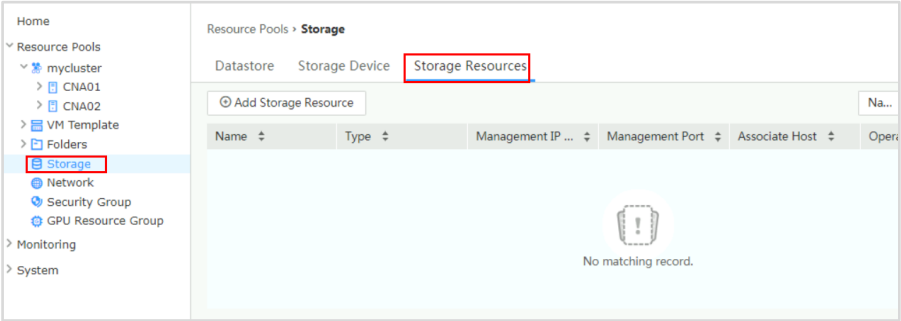


Figure 2-22 Storage Resources tab page

Step 2 Click **Add Storage Resource**. Set basic information, as shown in the following figure.

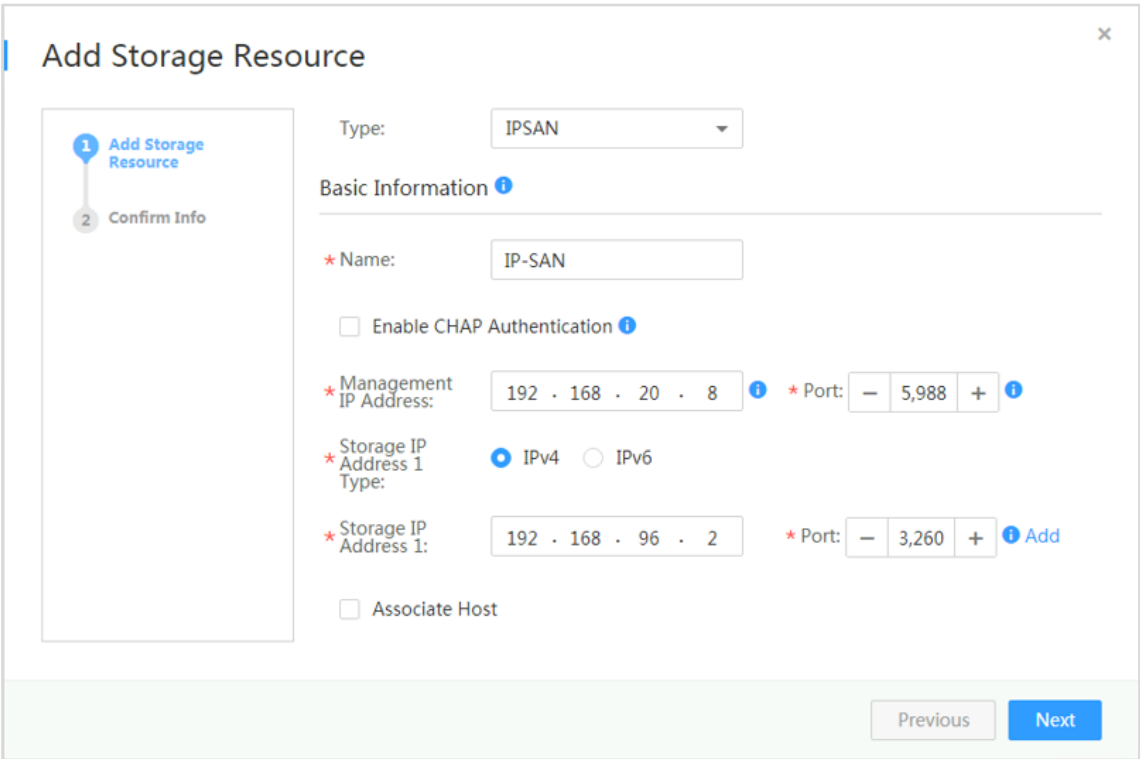


Figure 2-23 Configuring storage

Step 3 Click **Next**. Confirm the information and click **OK**.

Step 4 View the storage resource created on the **Storage Resources** tab page.

Step 5 Click **More** in the row that contains the IP-SAN storage resource and choose **Associate Host**.

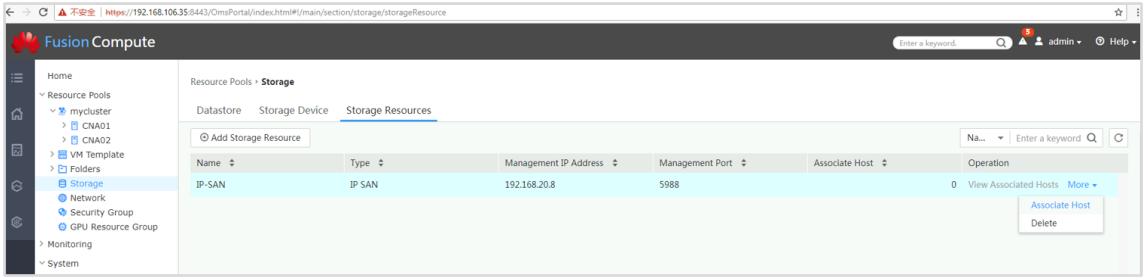


Figure 2-24 Associating a host

Step 6 In the **Associate Host** dialog box, select **site** and click **OK**.

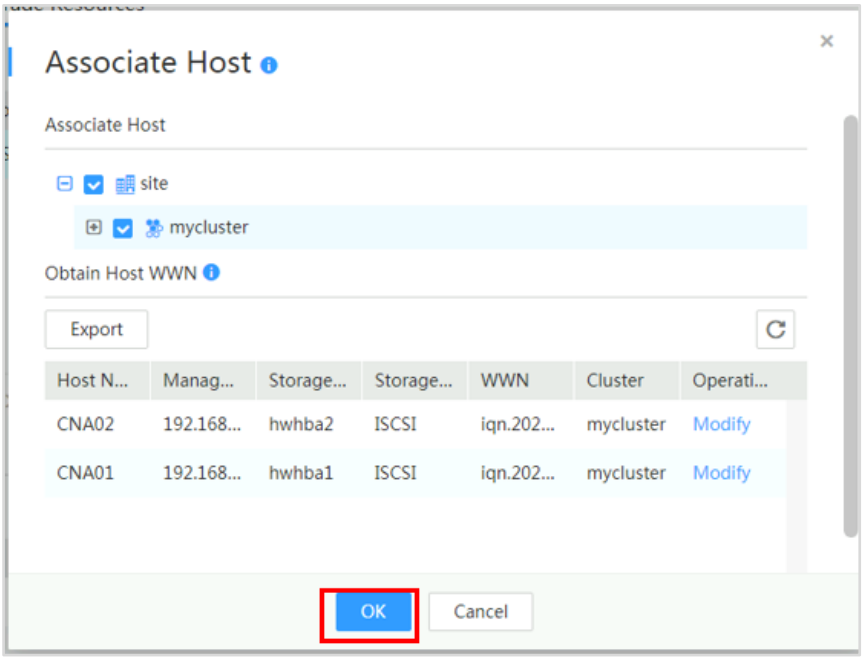


Figure 2-25 Selecting a cluster

Step 7 On the **Storage Resources** tab page, verify that two hosts have been associated with the storage resource.

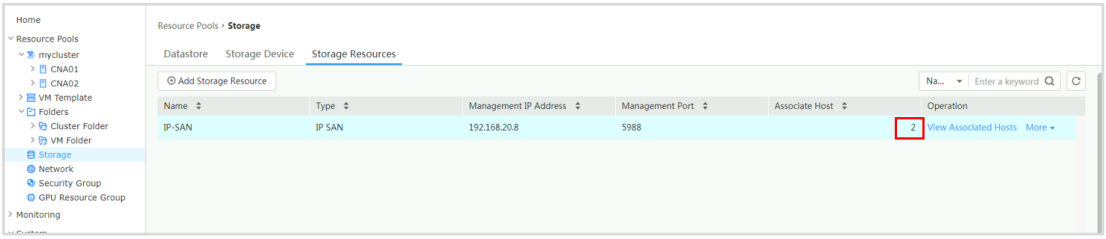


Figure 2-26 Verify successful association

Step 8 Log in to the storage device (using the provided login information), and create mappings between LUNs and the host group (CNA01 and CNA02) by referring to the basic storage exercise.

- Create LUNs.

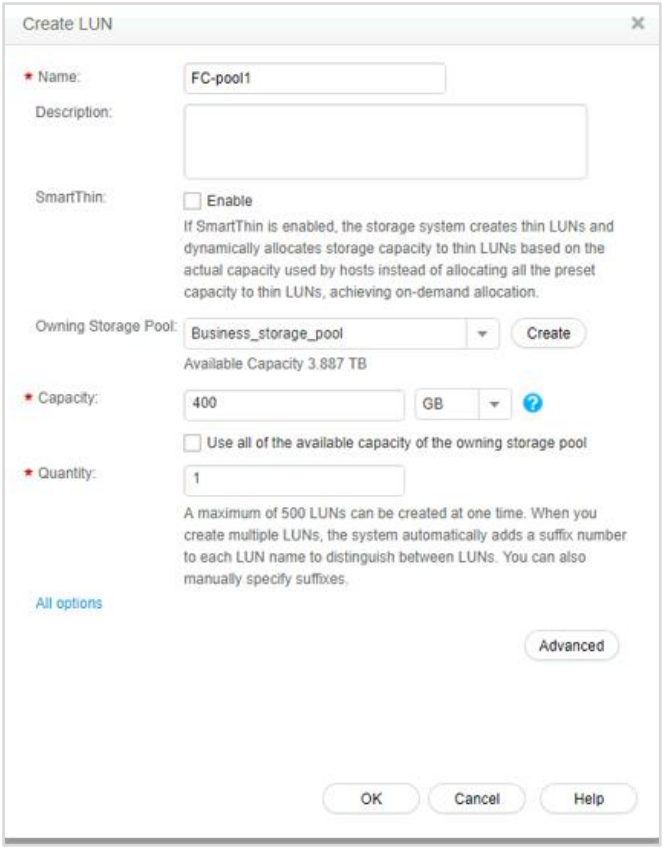


Figure 2-27 Creating LUNs

- Create a LUN group.

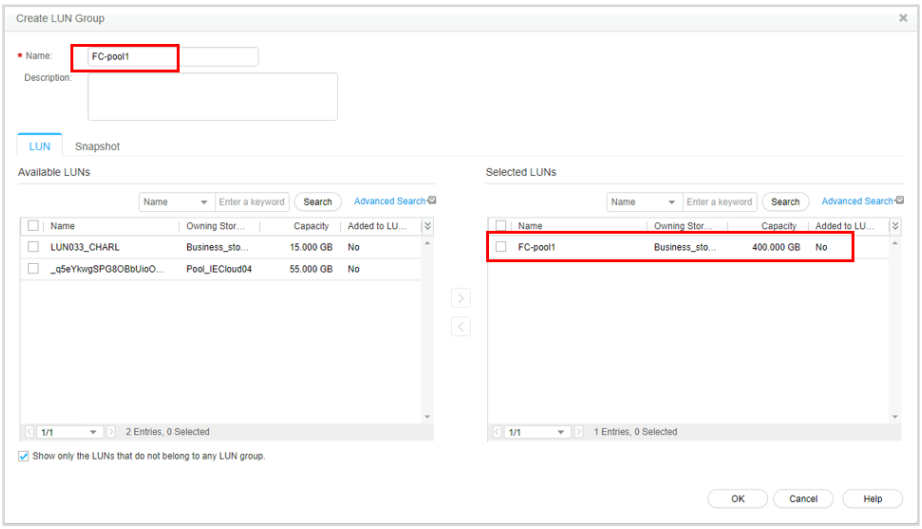


Figure 2-28 Creating a LUN group

- Create a host for CNA01.

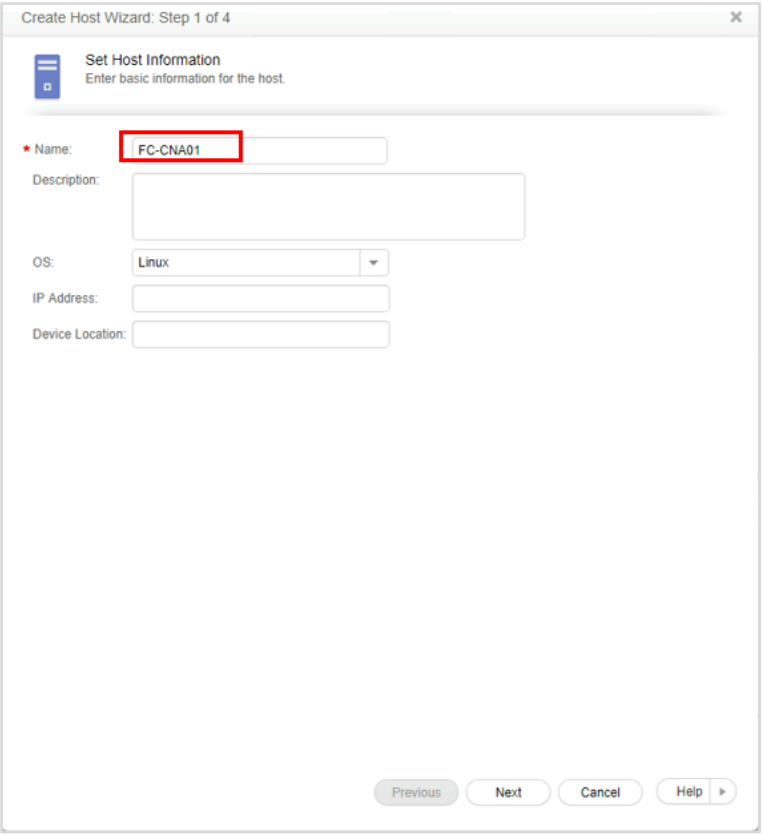


Figure 2-29 Creating a host

- In the **Available Initiators** area, select an iSCSI initiator and click the downward arrow button to add the initiator for the CNA01 host.

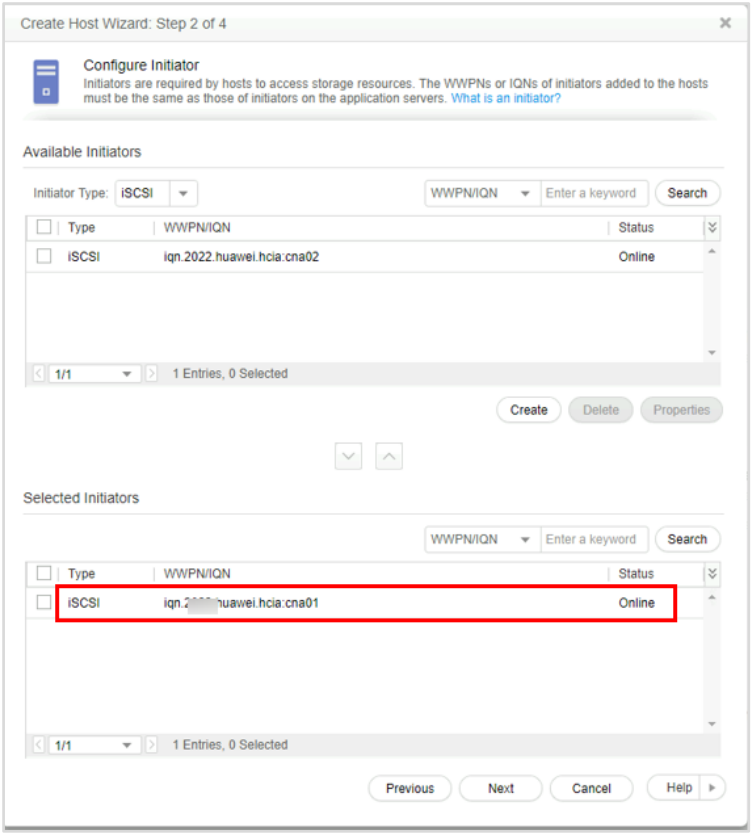


Figure 2-30 Adding an initiator for the CNA01 host

- Create a host for CNA02 and add an initiator for the CNA02 host by referring to the steps in Figure 2-29 and Figure 2-30.

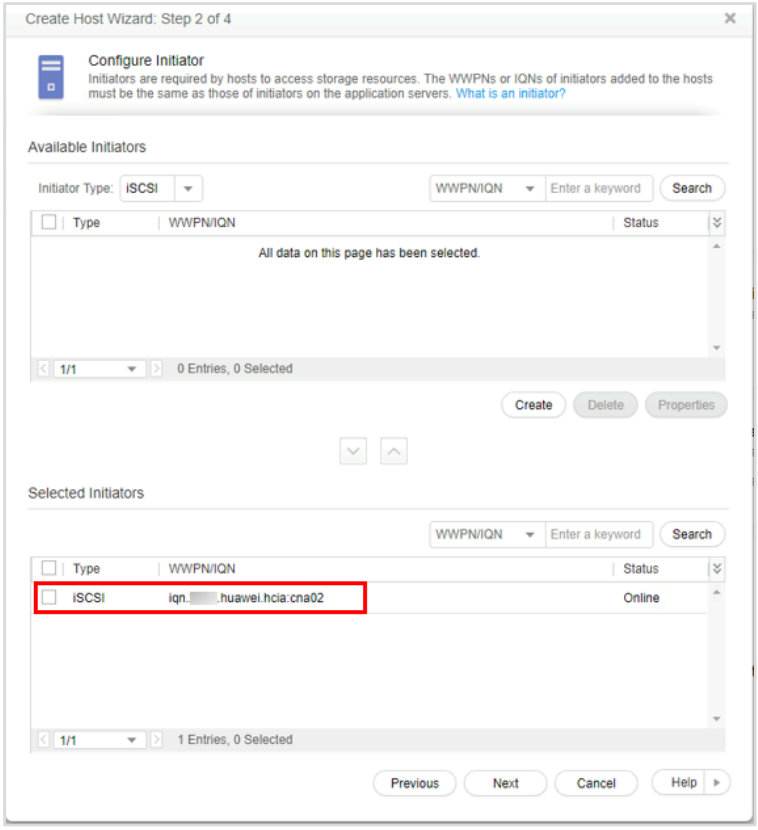


Figure 2-31 Adding an initiator for the CNA02 host

- Create a host group.

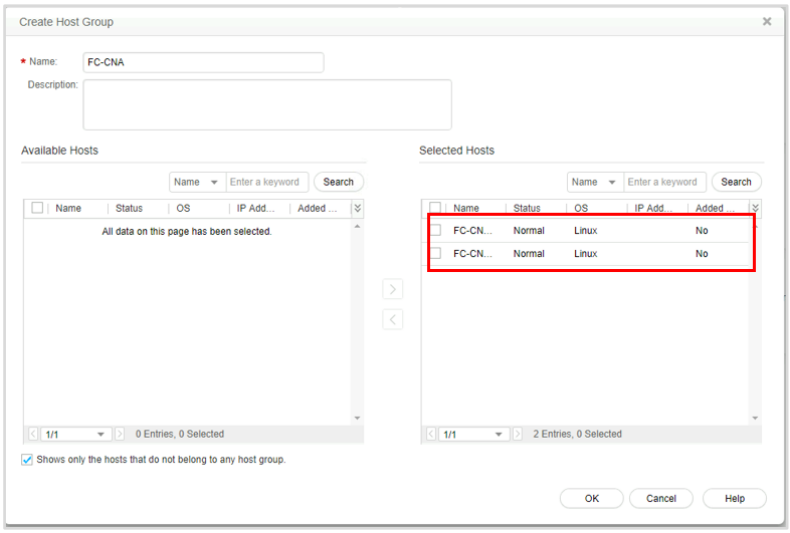


Figure 2-32 Creating a host group

- Create mappings between LUNs and the CNA cluster.

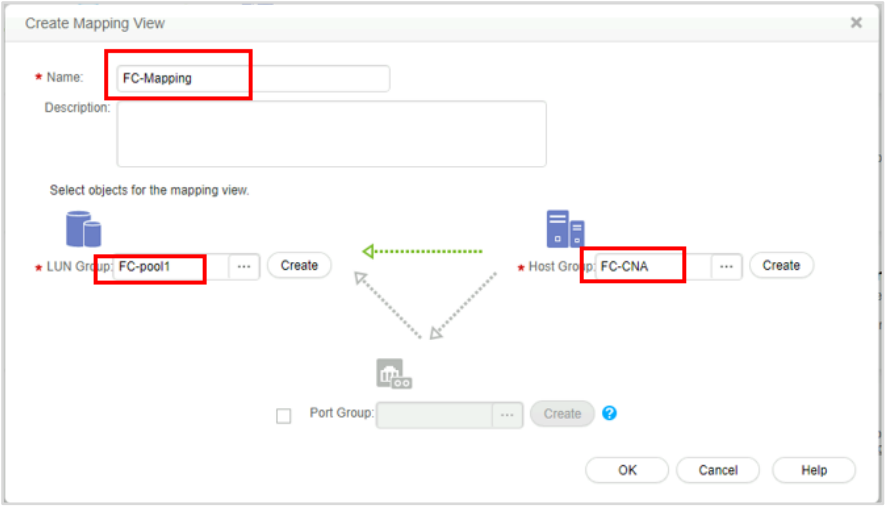


Figure 2-33 Creating mappings

2.2.3.2 Scanning for Storage Devices

Step 1 Choose **Resource Pools** > **Storage**. Click the **Storage Device** tab.

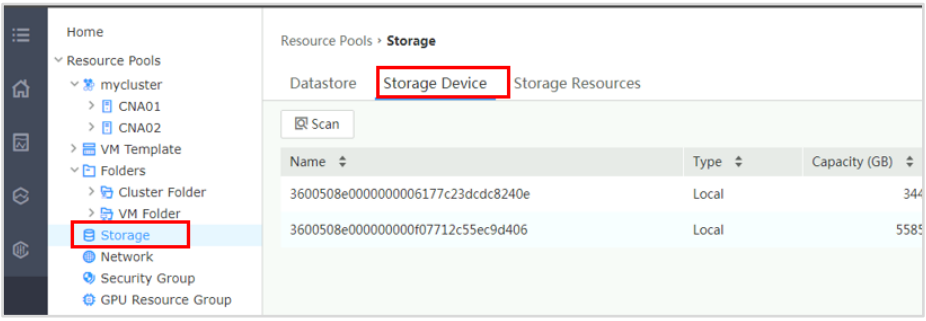


Figure 2-34 Scan storage devices.

Step 2 Click **Scan**. In the displayed dialog box, select **site** and click **OK** to scan for storage devices.

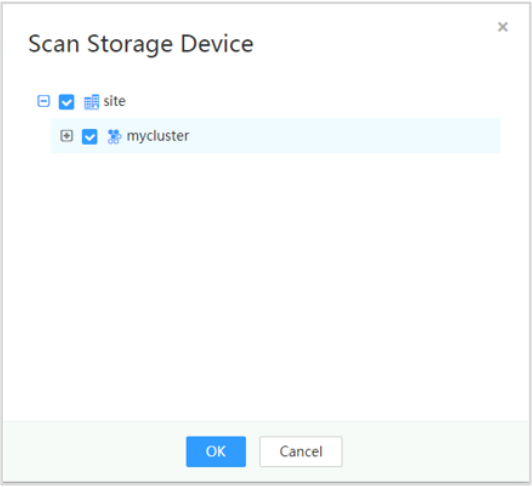


Figure 2-35 Clicking OK to scan for storage devices

Step 3 Choose **System** > **Tasks and Logs** > **Task Center** to view the scan progress.

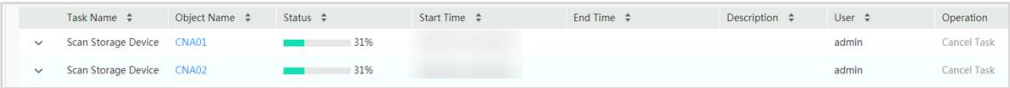


Figure 2-36 Viewing the progress

Step 4 Click the refresh icon in the upper right corner of the **Task Center** page to refresh the progress. After successful scanning, choose **Resource Pools** > **Storage** and click the **Storage Device** tab page to view the detected storage devices.

Figure 2-37 Scanned successfully

2.2.3.3 Adding a Datastore

Step 1 Choose **Resource Pools** > **Storage**. Click the **Datastore** tab.

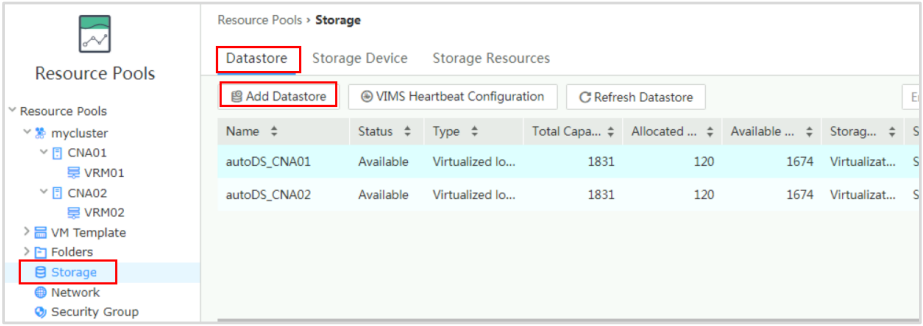


Figure 2-38 Datastore tab page

Step 2 Click **Add Datastore**. In the displayed dialog box, select IP SAN storage and click **Next**.

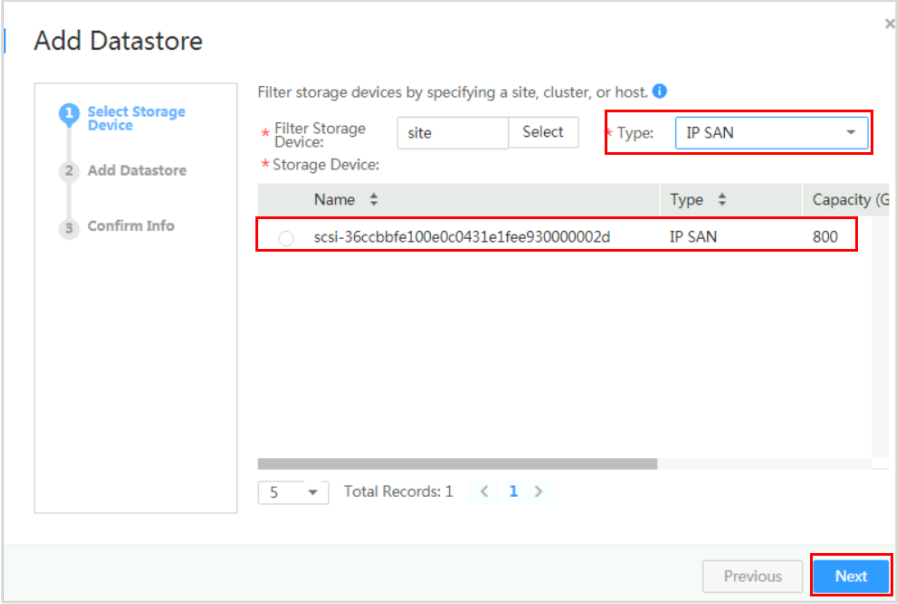


Figure 2-39 Adding IP SAN storage

Step 3 Set datastore parameters and click **Next**.

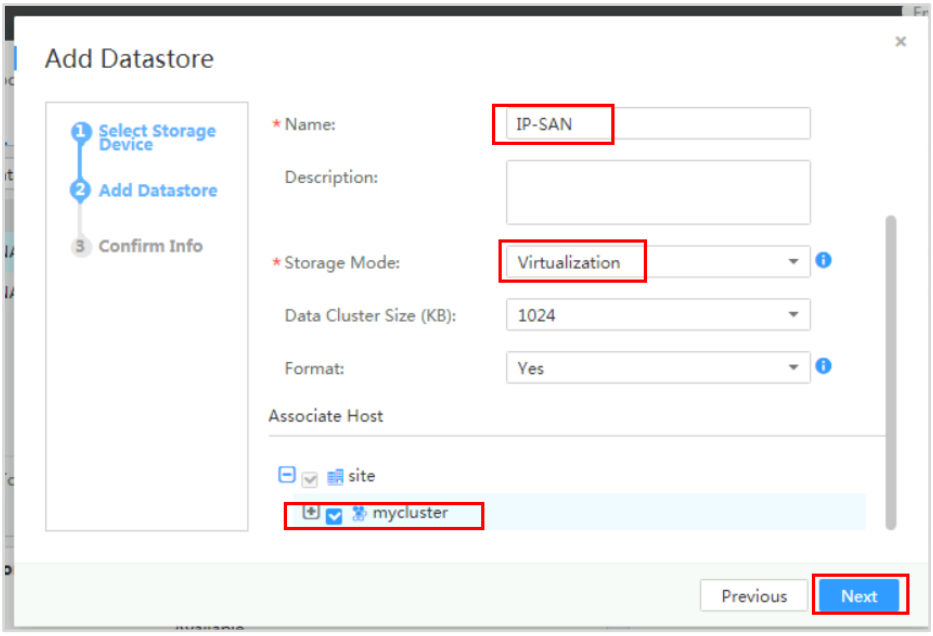


Figure 2-40 Configuring storage

Step 4 In the displayed dialog box, click **OK**. Confirm the information and click **OK**.

(The datastore adding takes 3 to 5 minutes. You can view the progress in the task center.)

Step 5 View the new datastore on the **Datastore** tab page.

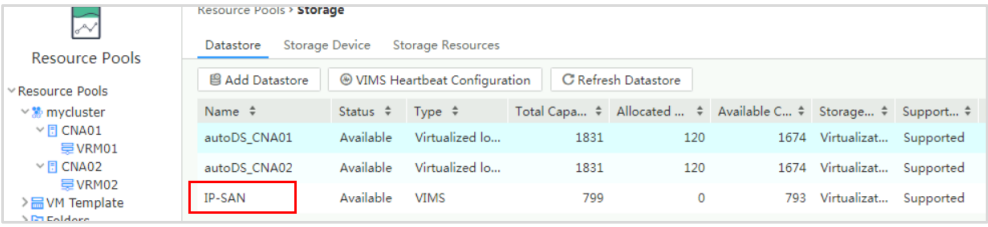


Figure 2-41 Datastore added successfully

2.2.4 Creating a Disk

2.2.4.1 Creating a Thin Provisioning Disk

Step 1 Choose **Resource Pools** > **Storage**. Click the **Datastore** tab.

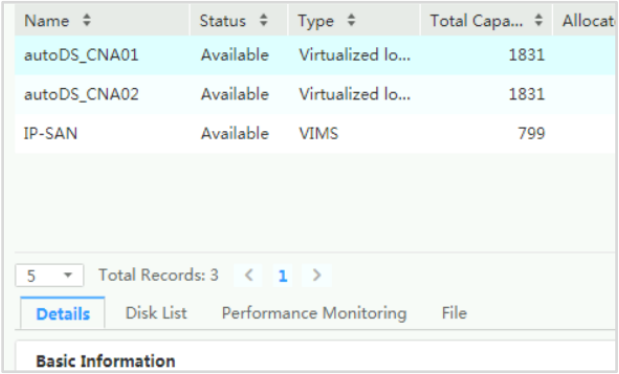


Figure 2-42 Datastore tab page

Step 2 On the **Datastore** tab page, select **IP-SAN**. Click the **Disk List** tab and click **Create Disk**.

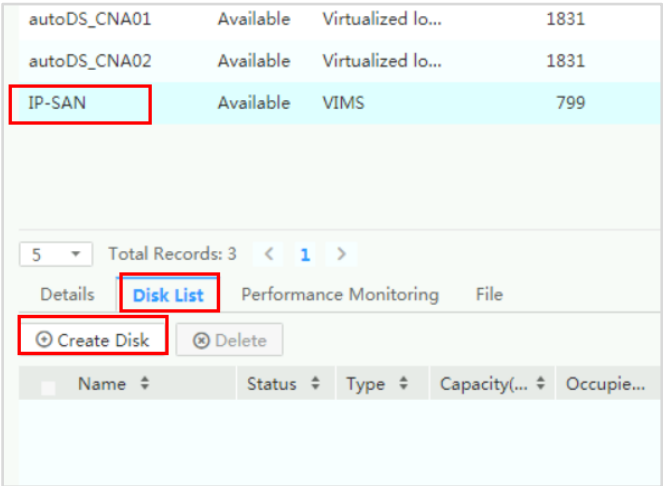


Figure 2-43 Creating a disk

Step 3 In the **Create Disk** dialog box, set disk parameters. Set **Name** to **DISK01**, **Capacity(GB)** to **10**, **Type** to **Non-shared**, **Configuration Mode** to **Thin provisioning**, and **Disk Mode** to **Dependent**. Confirm the settings and click **OK**.

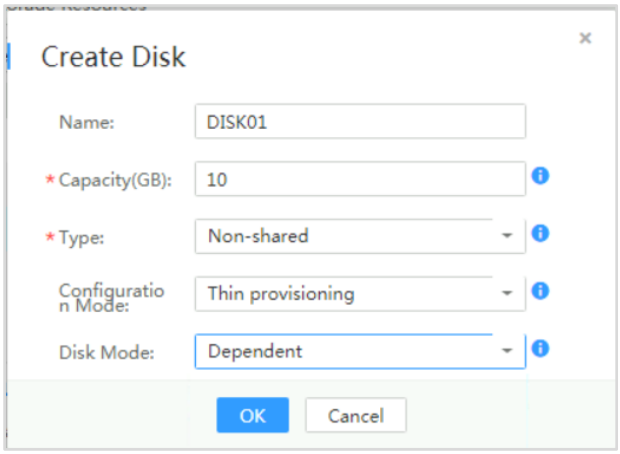


Figure 2-44 Setting parameters to create a disk

2.3 Network Resource Management

2.3.1 Introduction

2.3.1.1 About This Exercise

This exercise illustrates how to configure network resources on the installed FusionCompute. You need to plan distributed virtual switches (DVSs) and design virtual networks on FusionCompute to fulfill service requirements such as access between service VMs, high availability (HA), and live migration.

2.3.1.2 Objectives

- Understand concepts related to distributed virtual switches (DVSs).
- Create a DVS.
- Understand the concept and creation method of port groups.

2.3.1.3 Procedure

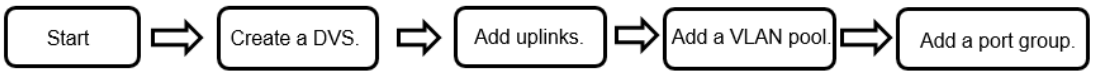


Figure 2-45 Procedure

2.3.2 DVS Management

2.3.2.1 Creating a DVS

Step 1 Choose **Resource Pools** > **Network**.

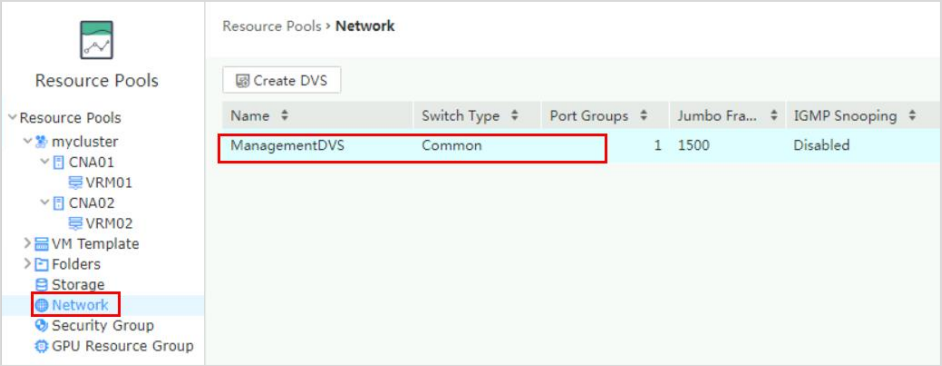


Figure 2-46 Network page

Step 2 Click **Create DVS**. In the **Create DVS** dialog box, set **Name** to **physnet** and **Switch Type** to **Common**, and use the default values for other parameters.

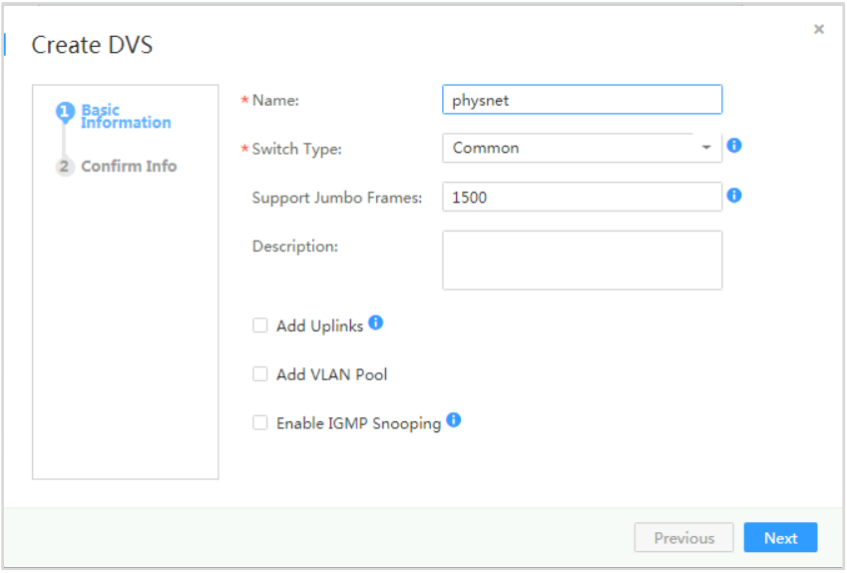


Figure 2-47 Setting parameters

Step 3 Click **Next**. Confirm the information and click **OK**.

Step 4 Choose **Resource Pools** > **Network** to view the DVS.

Figure 2-48 Viewing a DVS

2.3.2.2 Deleting a DVS

Step 1 Choose **Resource Pools** > **Network**.

Step 2 Click **More** in the **Operation** column of the **physnet** DVS and choose **Delete**. In the displayed dialog box, click **OK** to delete the DVS.

Figure 2-49 Deleting a DVS

2.3.2.3 Adding Uplinks

Step 1 Choose **Resource Pools** > **Network**.

Step 2 Select **ManagementDVS** and click **Add** on the **Uplink Group** tab page.

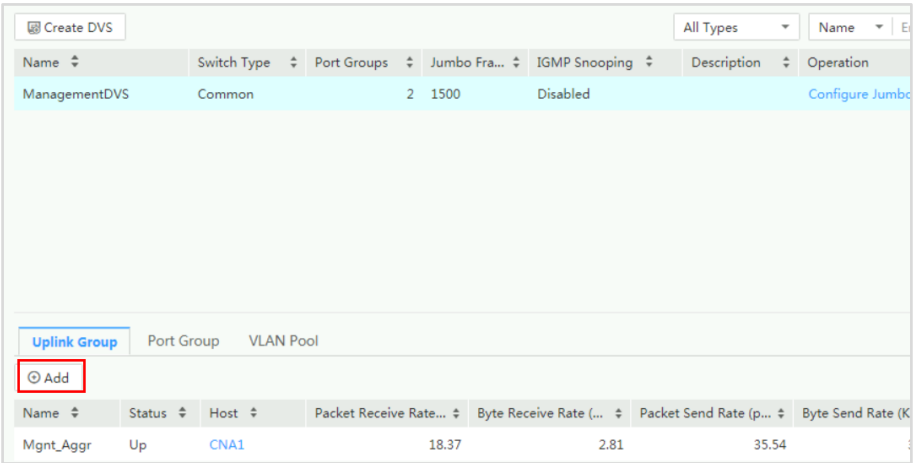


Figure 2-50 Adding uplinks

Step 3 In the displayed dialog box, expand **CNA02**, select **Mgnt_Aggr**, and click **OK**.

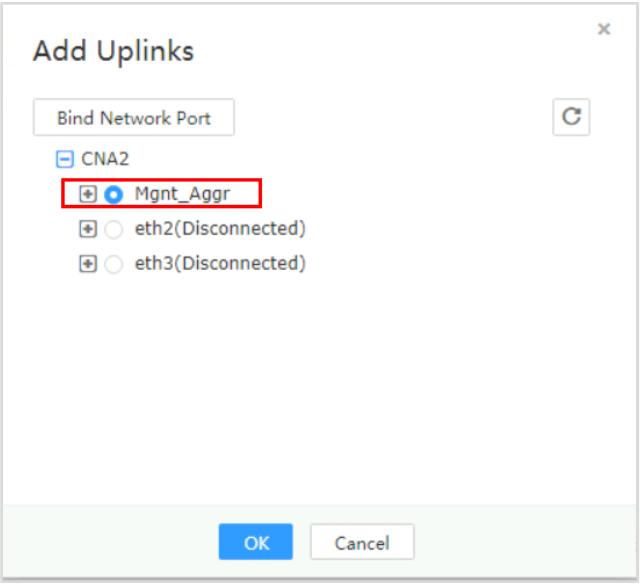


Figure 2-51 Selecting Mgnt_Aggr

Step 4 On the **Uplink Group** tab page, view the new uplinks.

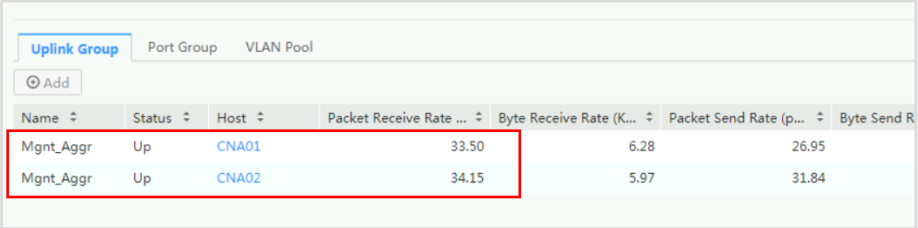


Figure 2-52 Viewing uplinks

2.3.2.4 Adding a VLAN Pool

Step 1 Choose **Resource Pools** > **Network**.

Step 2 Select **ManagementDVS** and click **Add** on the **VLAN Pool** tab page.

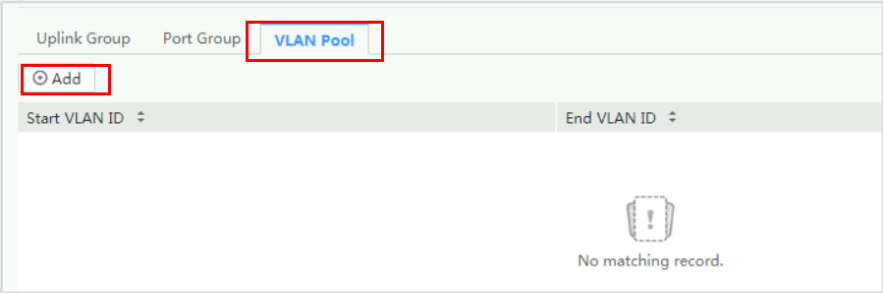


Figure 2-53 Adding a VLAN pool

Step 3 Set **Start VLAN ID** to **2** and **End VLAN ID** to **4094**, and click **OK**.

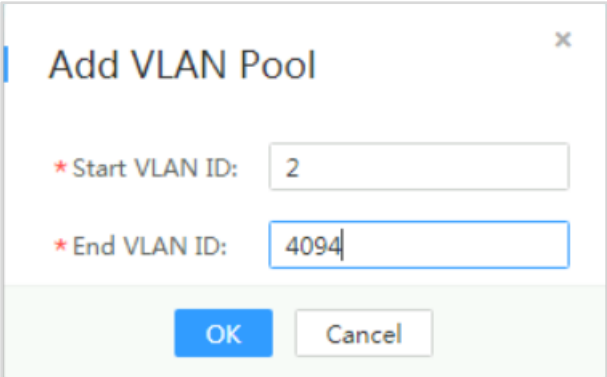


Figure 2-54 Configuring VLANs

Step 4 On the **VLAN Pool** tab page, view the new VLAN information.

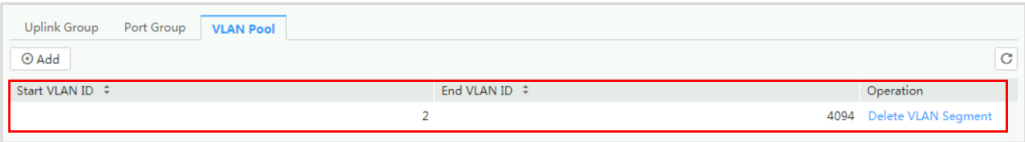


Figure 2-55 Viewing VLAN information

2.3.2.5 Adding a Port Group

Step 1 Choose **Resource Pools** > **Network**.

Step 2 Select **ManagementDVS** and click **Add** on the **Port Group** tab page.

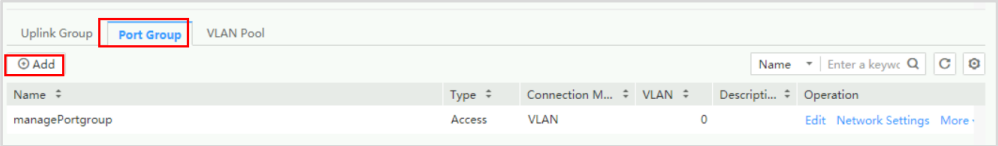


Figure 2-56 Adding a port group

Step 3 Set the port group name to **test**, use the default values for other parameters, and click **Next**.

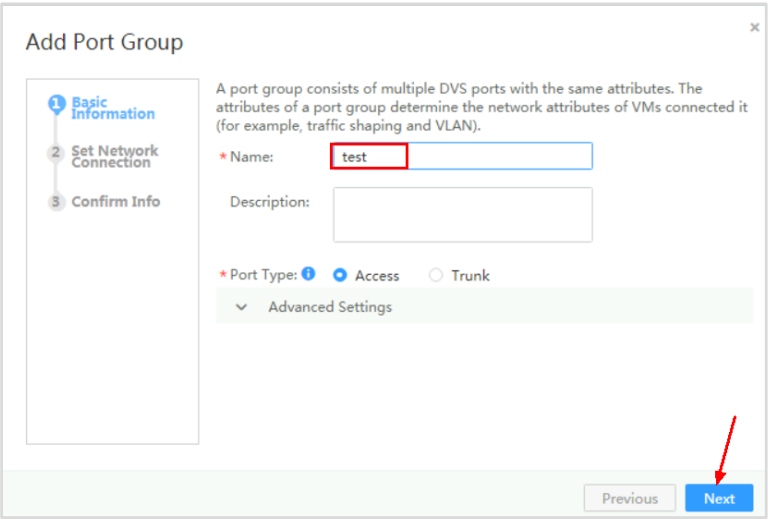


Figure 2-57 Configuring a port group

Step 4 Set **VLAN** to **100** and click **Next**.

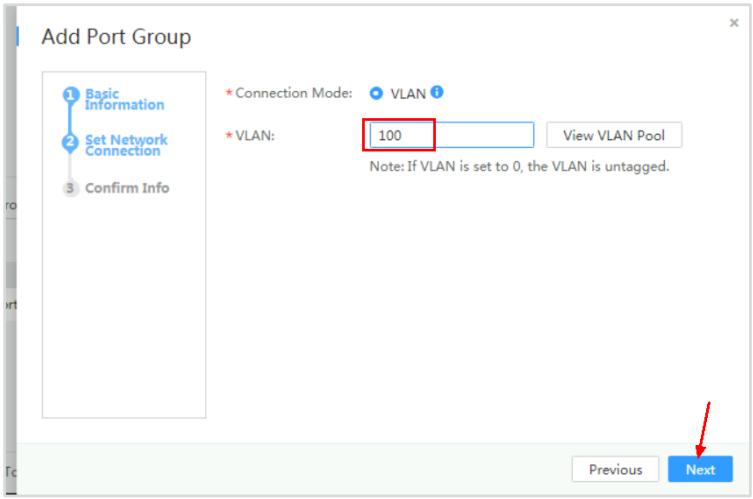


Figure 2-58 Setting the VLAN

Step 5 Confirm the information and click **OK**.

Step 6 On the **Port Group** tab page, view the port group information.

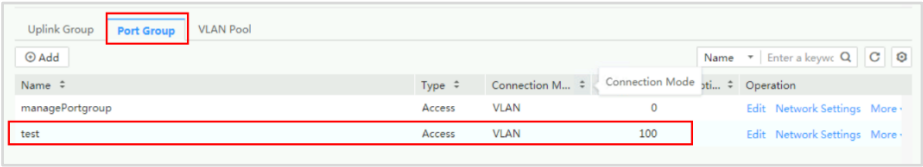


Figure 2-59 Viewing port group information

2.4 Quiz

FusionCompute supports three disk configuration modes: **Common**, **Thick provisioning lazy zeroed**, and **Thin provisioning**. What are the characteristics of disks in **Common** and **Thin provisioning** modes, and what are the differences between disks in these two modes?

Answers:

Common: The system allocates disk space based on the disk capacity. During disk creation in this mode, data remaining on the physical device will be zeroed out. The performance of the disks in this mode is better than that in the other two modes, but the creation duration may be longer than that required in the other modes.

Thin provisioning: In this mode, the system allocates part of the configured disk capacity for the first time, and allocates the rest disk capacity based on the storage usage of the disk until the configured disk capacity is allocated.

3 FusionCompute VM Provisioning and Management

3.1 VM Provisioning

3.1.1 Introduction

3.1.1.1 About This Exercise

This exercise illustrates how to create VMs, install OSs, and import templates on FusionCompute.

3.1.1.2 Objectives

- Create a VM.
- Import a template and create a VM using the template.
- Create a template.

3.1.1.3 Procedure

Figure 3-1 Procedure

3.1.2 VM Provisioning

3.1.2.1 Creating a VM

Step 1 Choose **Resource Pools** > **mycluster**.

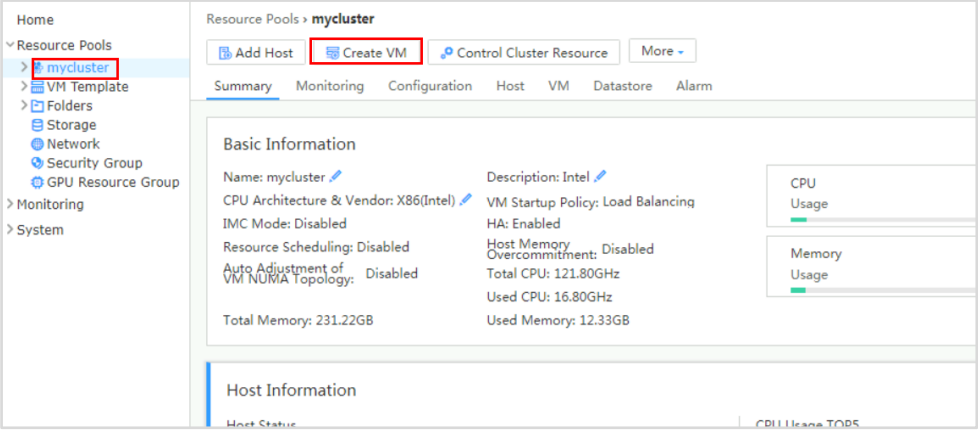


Figure 3-2 Cluster management page

Step 2 Click **Create VM**. The VM creation window is displayed. On the **Select Creation Mode** page, select **Create VM** and click **Next**.

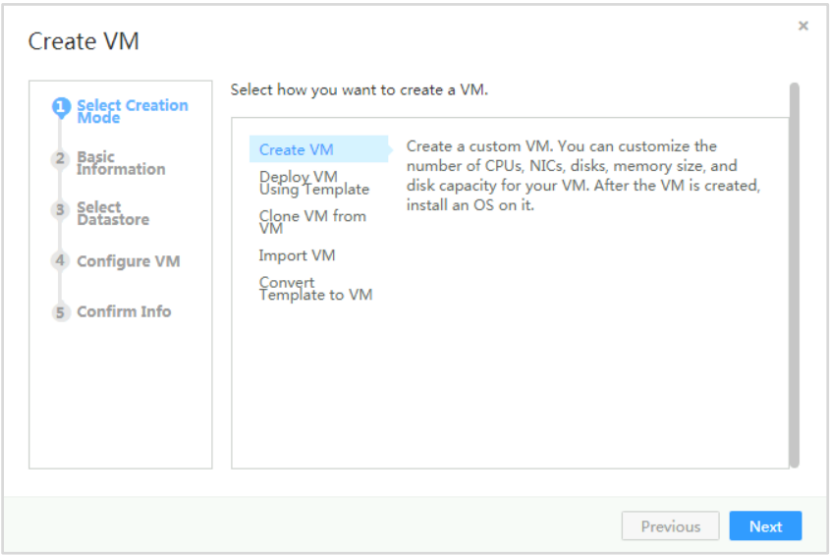


Figure 3-3 Creating a VM

Step 3 Set **Name** to **test01**, **Select VM Location** to **site**, **Set Compute Resource** to **mycluster**, and **OS** to **Linux**.

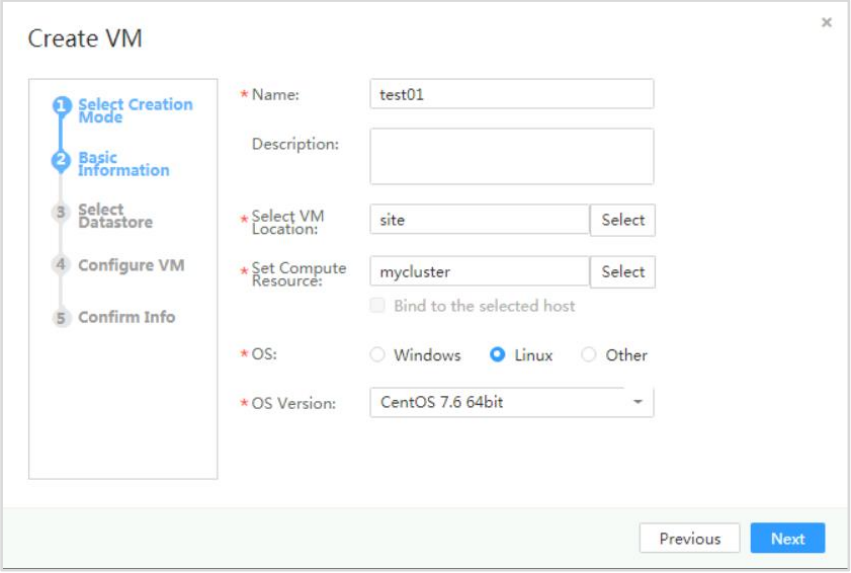


Figure 3-4 Configuring a VM

Step 4 Click **Next**. On the **Select Datastore** page, select **IP-SAN** and click **Next**.

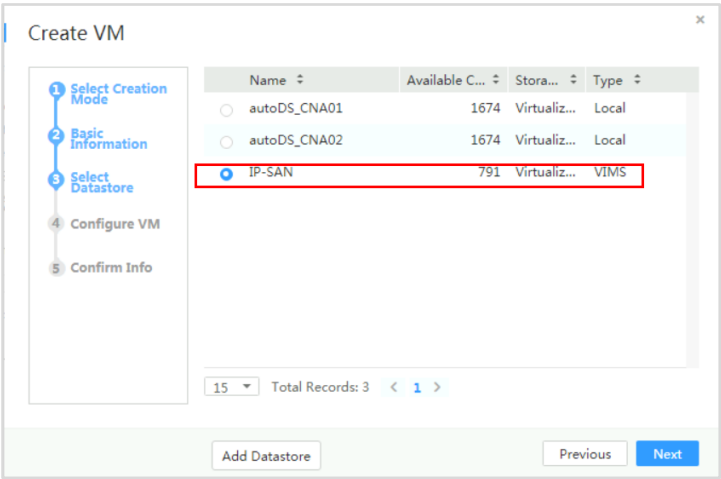


Figure 3-5 Selecting a datastore

Step 5 Set VM parameters. Set **CPU** to **2** (vCPU), **Memory** to **4 GB**, and **Disk 1** to **40 GB**. Use the default values for other parameters and click **Next**.

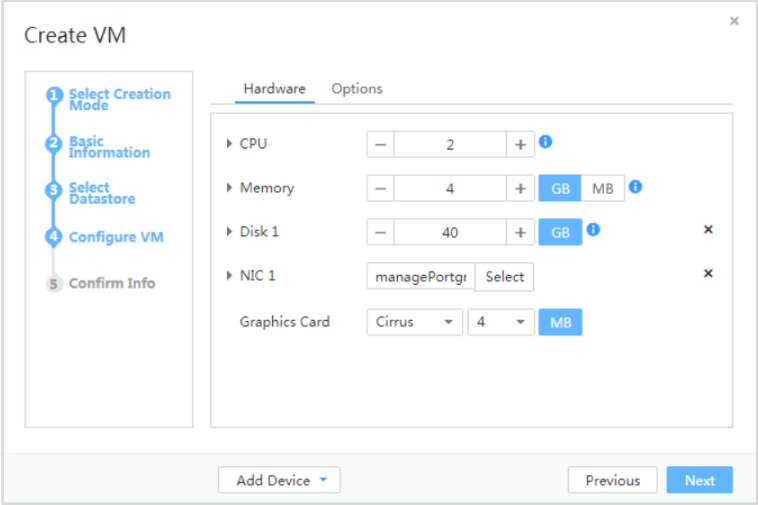


Figure 3-6 Configuring the VM

Step 6 Confirm the information and click **OK**.

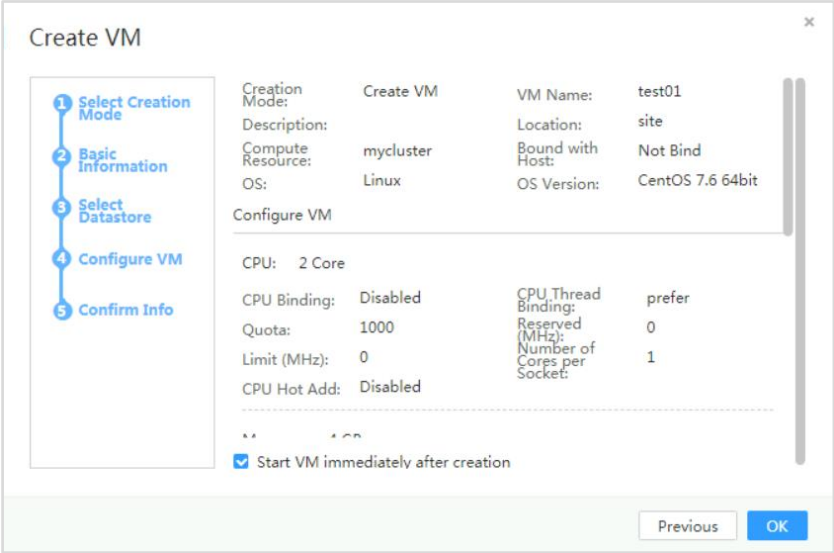


Figure 3-7 VM created successfully

Step 7 Choose **Resource Pools** > **mycluster**. On the **VM** tab page, view the VM status.

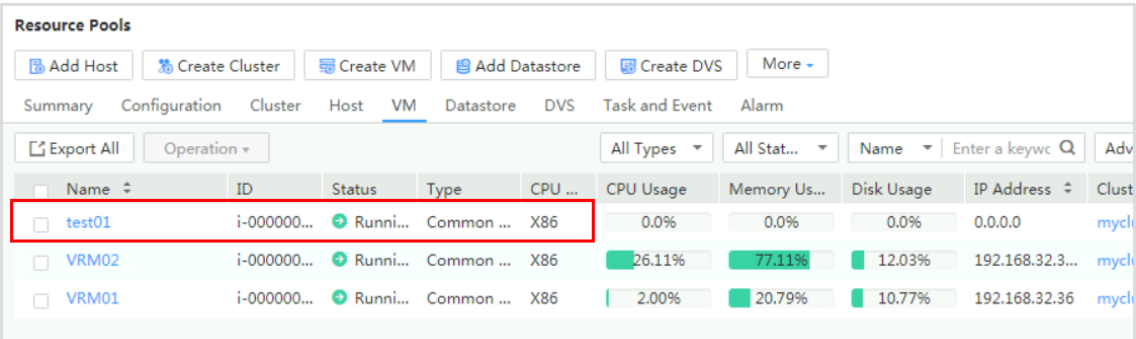


Figure 3-8 Viewing VM information

Step 8 Click **test01** in the **Name** column to go to the VM management page.

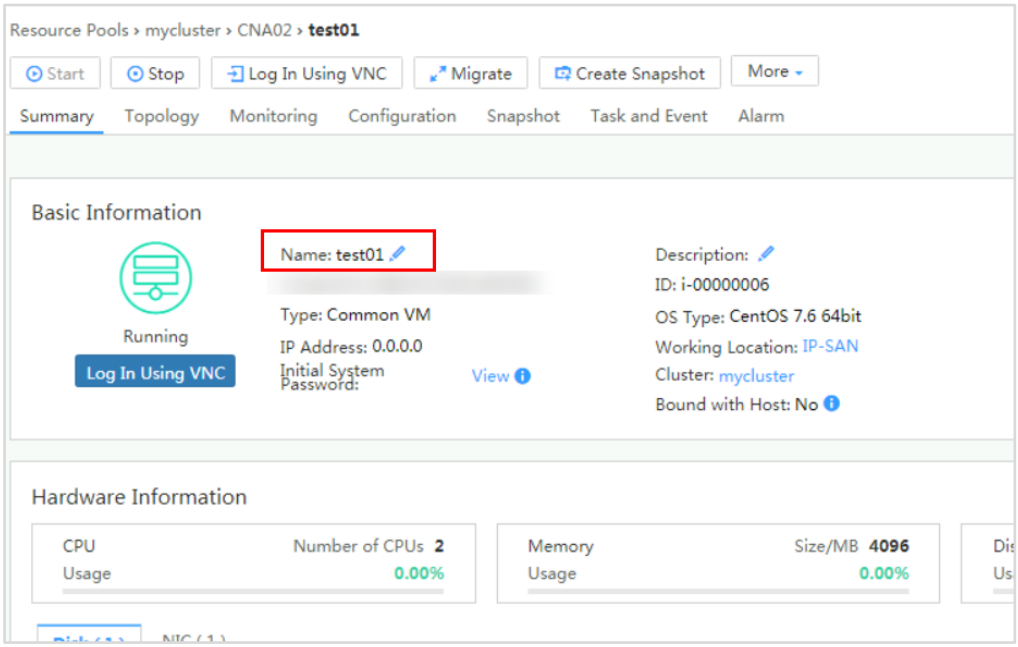


Figure 3-9 VM management page

3.1.2.2 Installing the OS

Step 1 Choose **Resource Pools** > **mycluster** > **VM** > **test01**. The VM management page is displayed.

Step 2 Click the **Configuration** tab. In the navigation pane on the left, click **CD/DVD-ROM Drive Unmounted**.

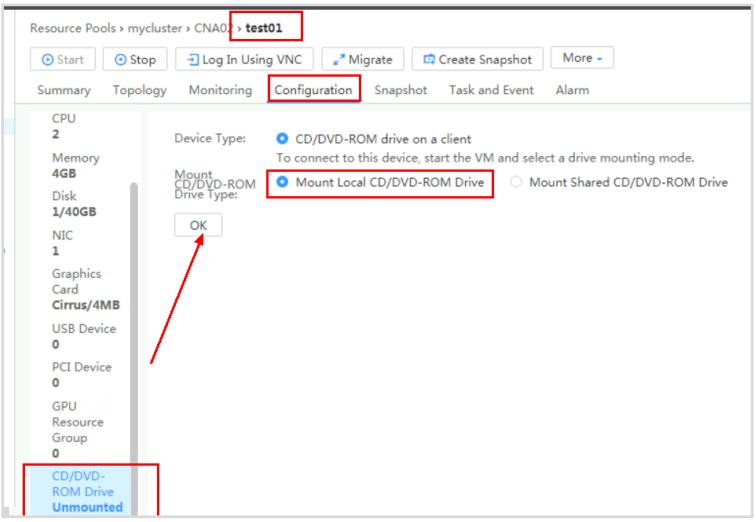


Figure 3-10 Mounting a CD/DVD-ROM drive

Step 3 Set **Mount CD/DVD-ROM Drive Type** to **Mount Local CD/DVD-ROM Drive** and click **OK**. In the **Launch Application** dialog box that is displayed, select **FCPortalClientPlugin** and click **Open link**.

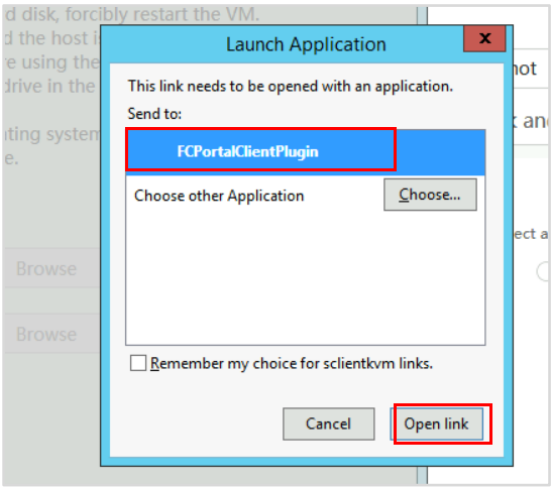


Figure 3-11 Starting the plug-in

(Note: If you use the plug-in for the first time, the system may prompt you to install the plug-in, as shown in the following figure. Click **OK** and click the link in the red box to download and install the plug-in. After the installation is complete, perform Step 2 again.)

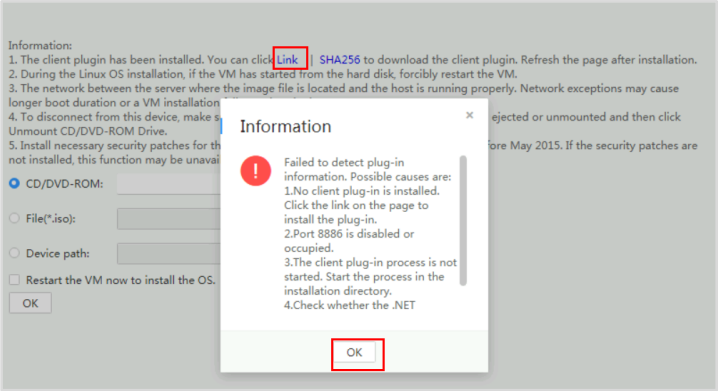


Figure 3-12 (Optional) Downloading and installing the plug-in

Step 4 On the drive management page, select **File(*.iso)** and click **Browse**. In the displayed dialog box, select the local CentOS image file and click **Open**. Select **Restart the VM now to install the OS** and click **OK**. (You can also use the **openEuler-22.03-LTS-x86_64-dvd** image file.)

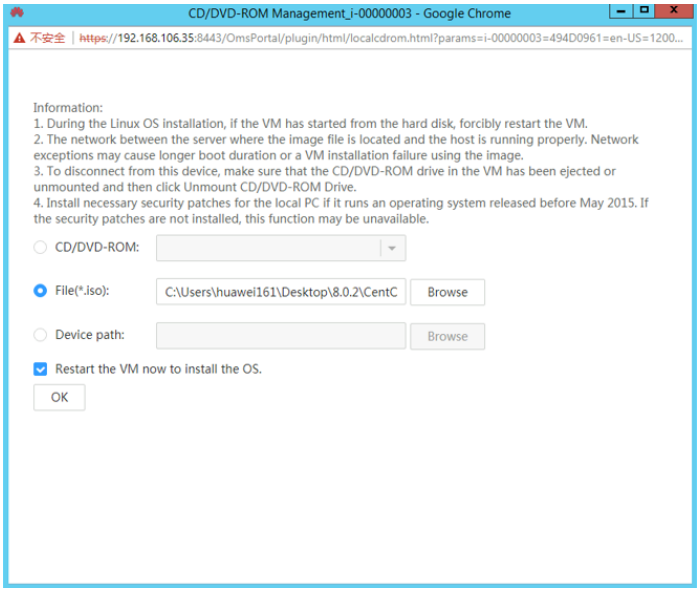


Figure 3-13 Selecting an image file

Step 5 After the CD/DVD-ROM drive is successfully mounted, open the VM VNC console and go to the OS installation page to complete the OS installation.

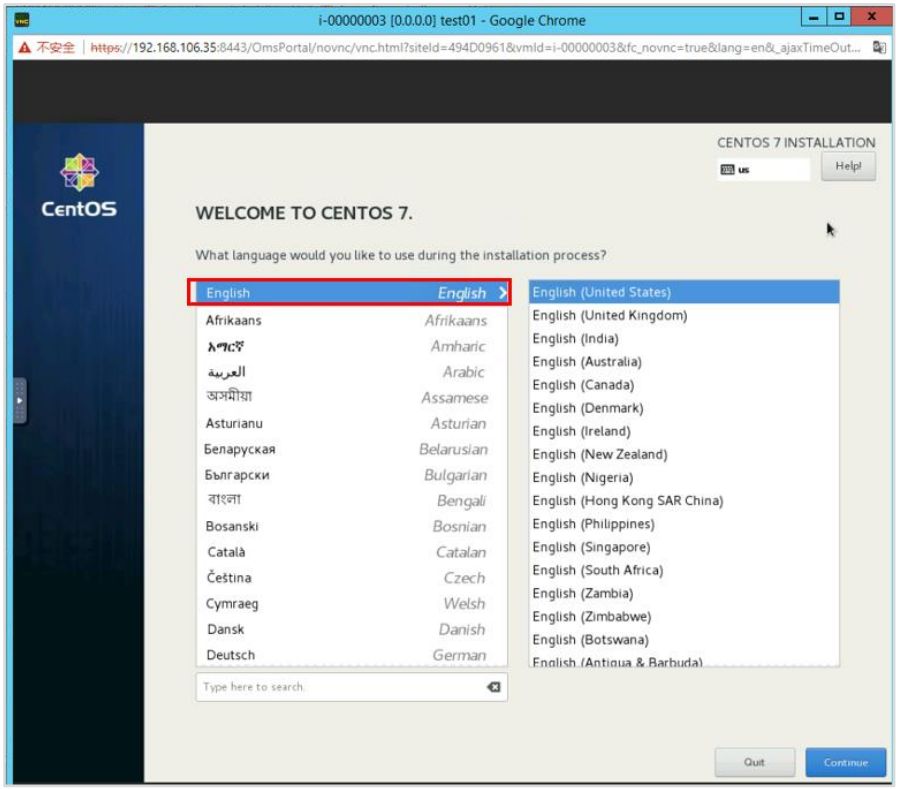


Figure 3-14 System installation

Step 6 After selecting the installation destination, click **Begin Installation**.

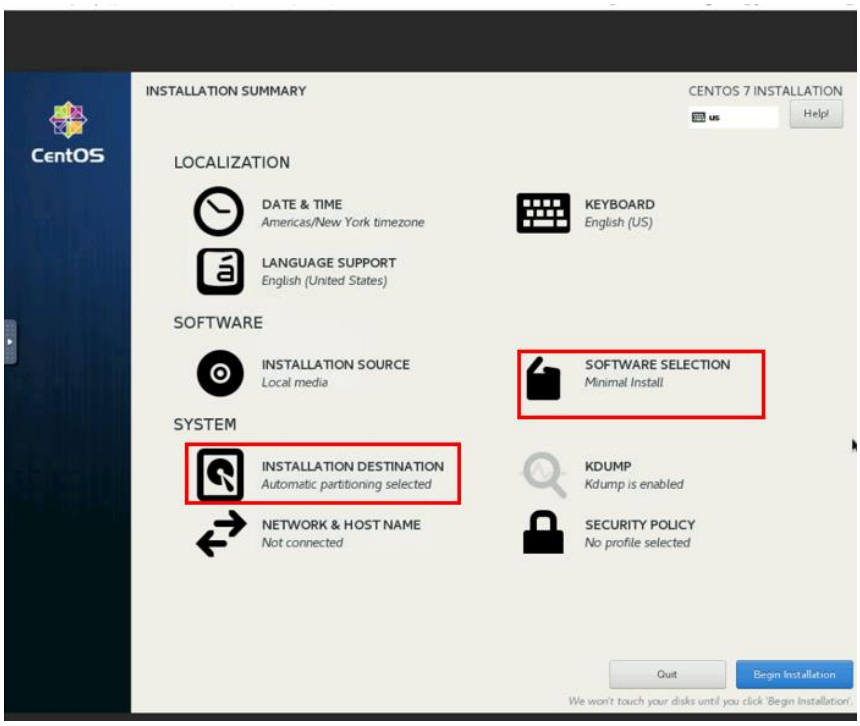


Figure 3-15 Configuring installation information

Step 7 Configure the **root** password.

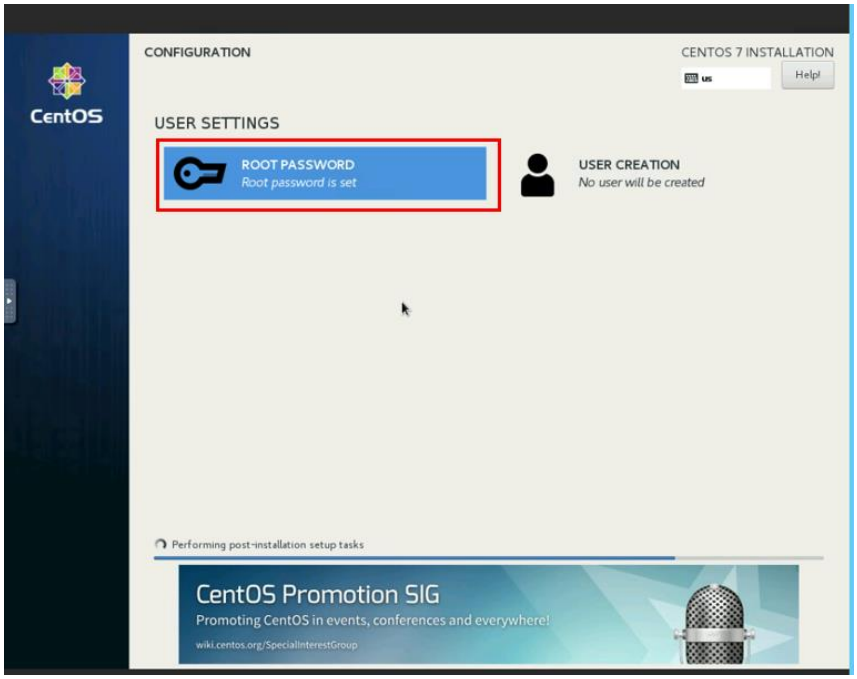


Figure 3-16 Configuring the root password

Step 8 After the installation is complete, click **Reboot**.

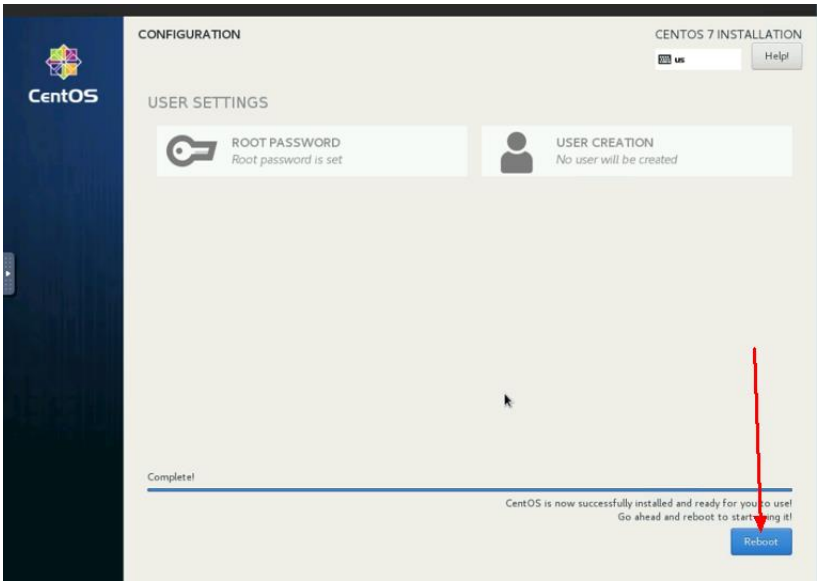
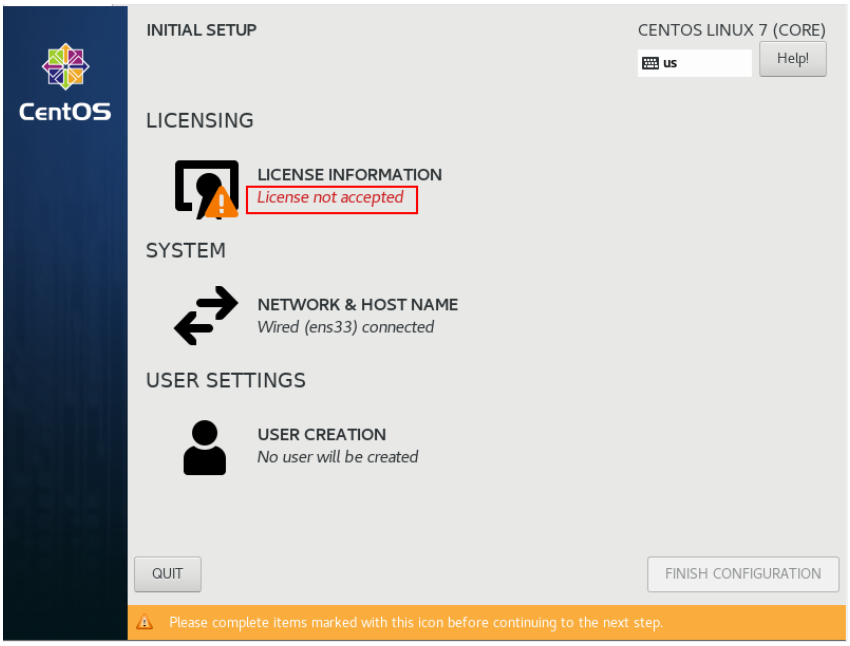


Figure 3-17 Rebooting

Step 9 Accept the license.



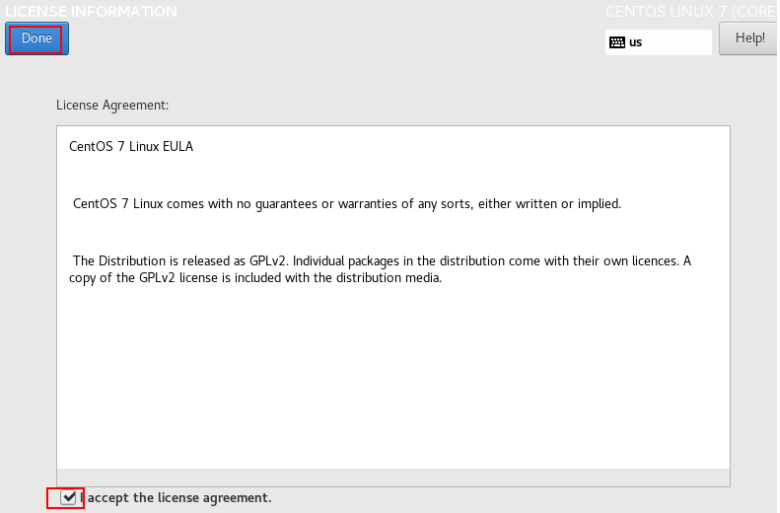


Figure 3-18 Accept the license

Step 10 Create a user account and configure the password.

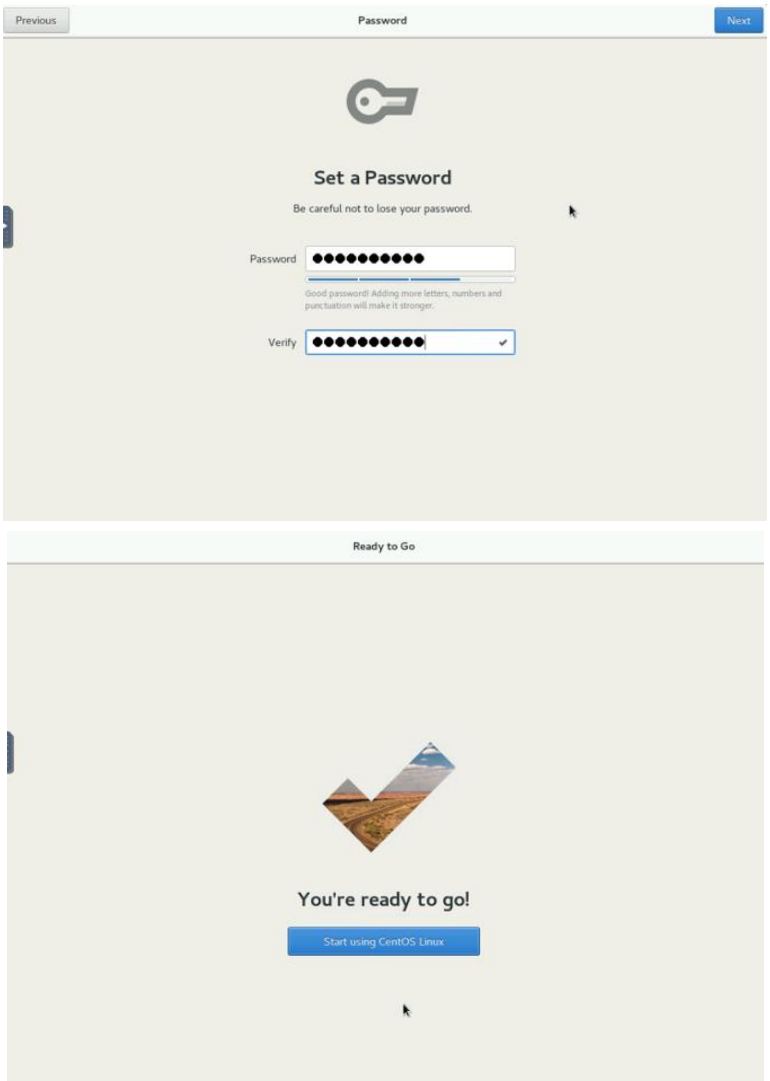


Figure 3-19 Creating a user account and configuring the password

3.1.2.3 (Optional) Installing VMTools

Step 1 Choose **Resource Pools** > **mycluster** > **CNA01** > **test01**. Click **More** and choose **Tools** > **Mount Tools**.

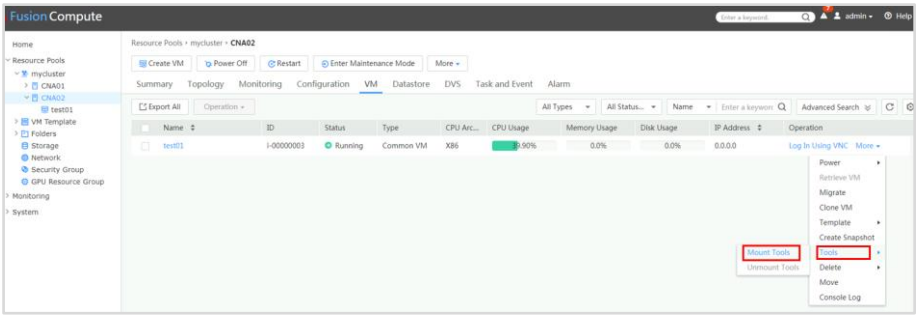


Figure 3-20 Mounting VMTools

Step 2 Log in to VM test01 as the **root** user using VNC.

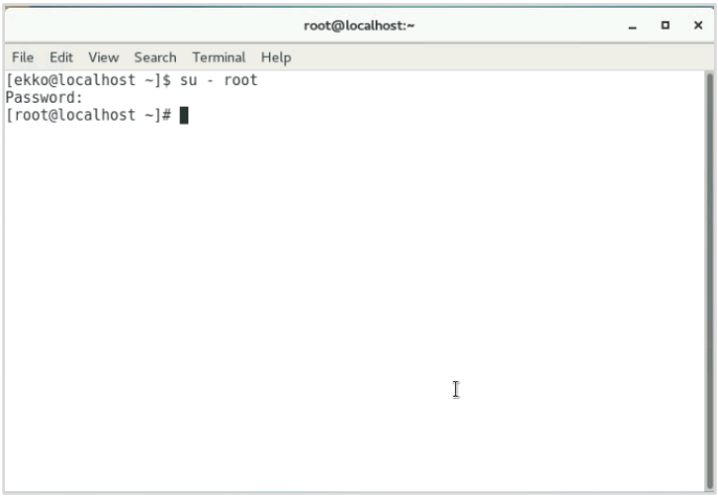


Figure 3-21 Logging in to the VM

Step 3 Check for the qemu-guest-agent service.

```
[root@localhost ~]# ps -eaf | grep qemu-ga
```

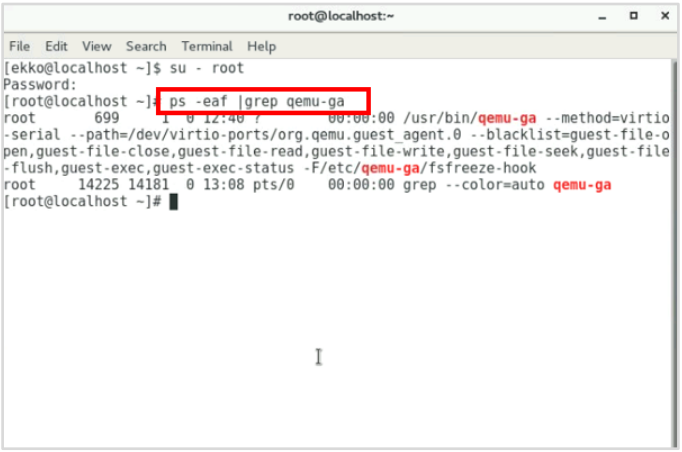


Figure 3-22 Checking for the qemu-guest-agent service

If the command output contains "qemu-guest-agent", the qemu-guest-agent service exists in the system. (If the command output does not contain "qemu-guest-agent", go to Step 5.)

Step 4 Uninstall the open source qemu-guest-agent service.

```
[root@localhost ~]# rpm -e qemu-guest-agent
[root@localhost ~]# reboot
```

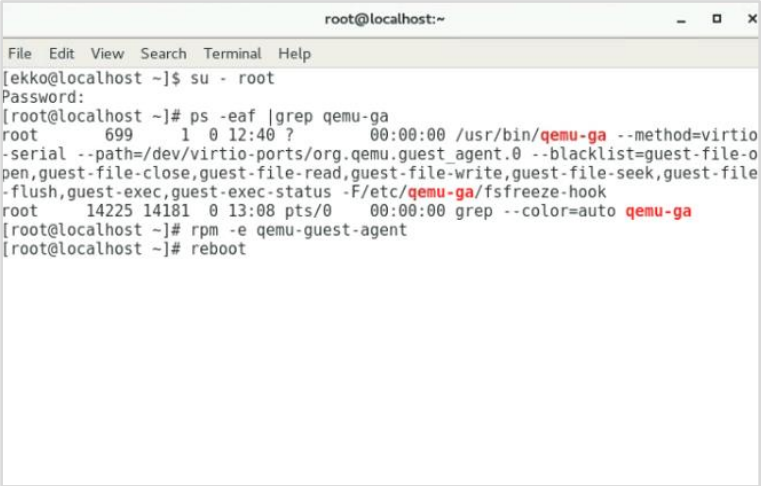


Figure 3-23 Uninstalling the qemu-guest-agent service

Step 5 Restart the VM, log in to the VM as the **root** user, and mount a CD/DVD-ROM drive to the VM.

```
[root@localhost ~]# mkdir xvdd
[root@localhost ~]# mount /dev/sr0 xvdd
```

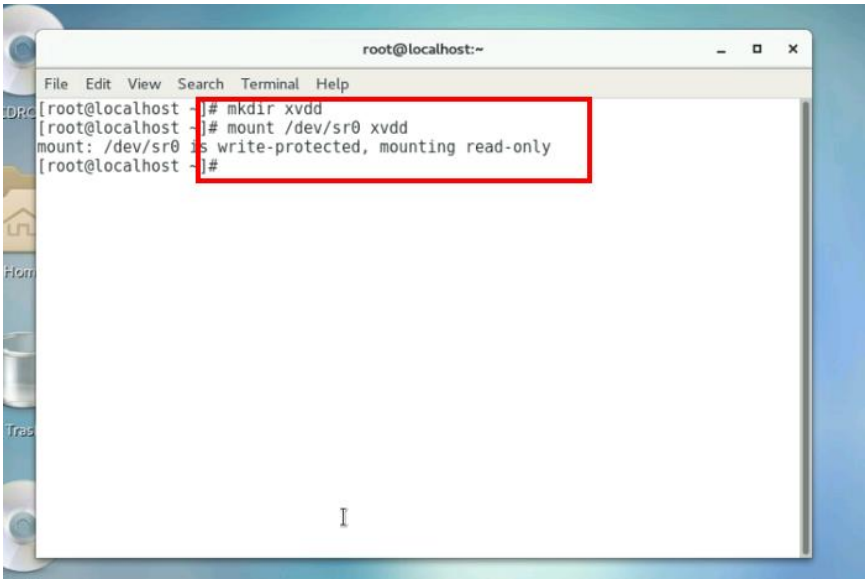


Figure 3-24 Mounting a CD/DVD-ROM drive to a VM

Step 6 Check the VMTools installation package.

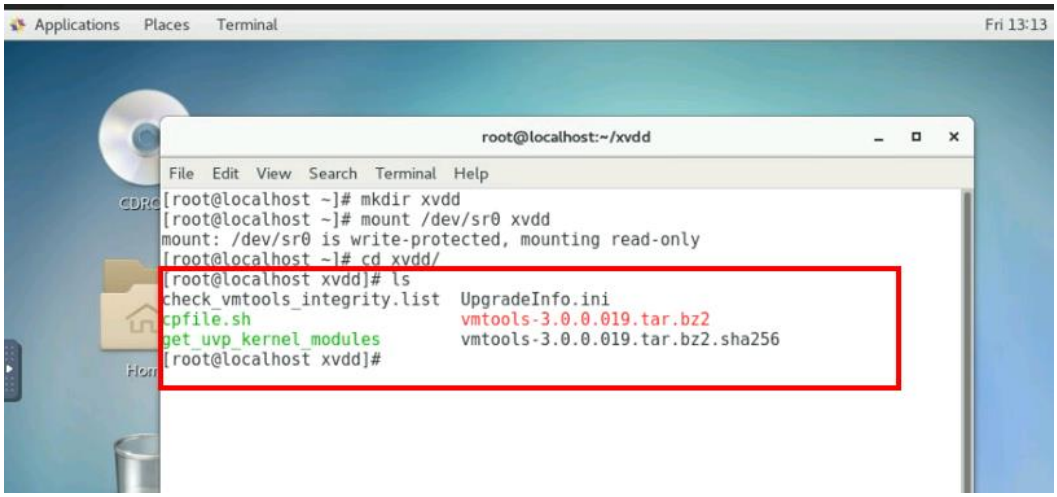


Figure 3-25 Checking the VMTools installation package

Step 7 Copy the VMTools installation package to the **/root** directory and decompress the package.

```
[root@localhost xvdd]# cp vmtools-3.0.0.019.tar.bz2 /root
[root@localhost xvdd]# cd /root
[root@localhost ~]# tar –xjvf vmtools-3.0.0.019.tar.bz2
```

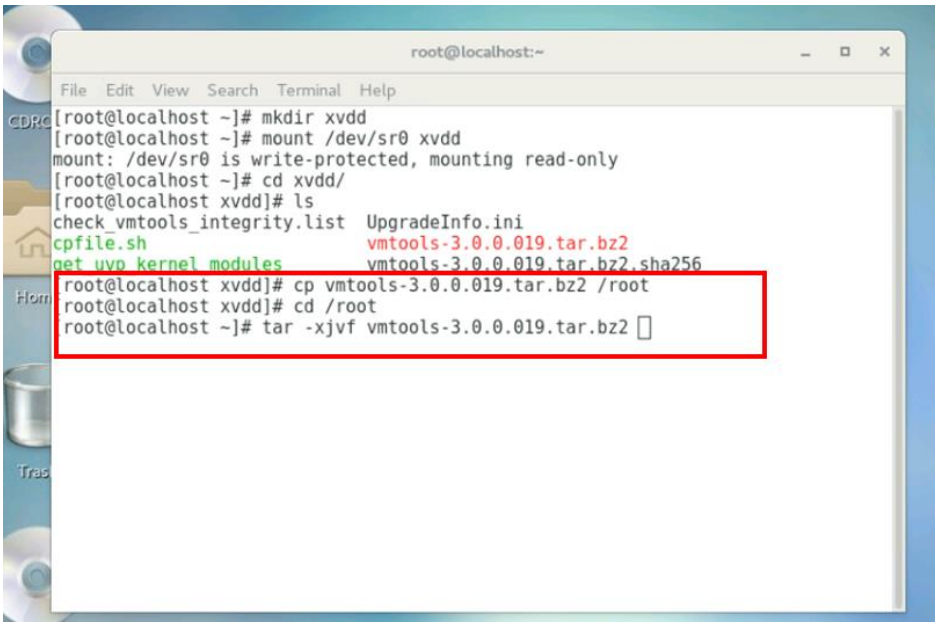


Figure 3-26 Decompressing the VMTools installation package

Step 8 Install VMTools and restart the system.

```
[root@localhost ~]# cd vmtools
[root@localhost ~]# ./install
...
The UVP VMTools is installed successfully.
```

```
Reboot the system for the installation to take effect.
[root@localhost ~]# reboot
```

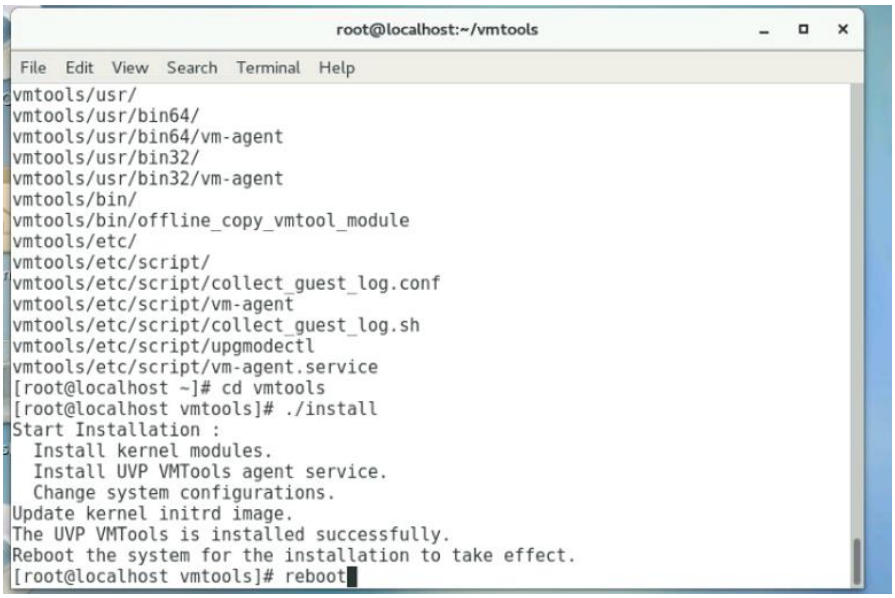


Figure 3-27 Restarting the system after VMTools is installed

3.1.2.4 Creating a VM Template

Step 1 Choose **Resource Pools** > **mycluster** > **CNA01** > **test01**. Click **More** and choose **Tools** > **Export as Template**.

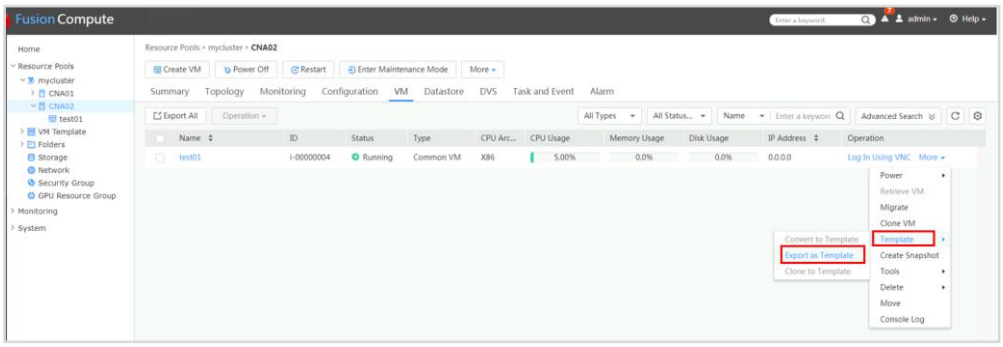


Figure 3-28 Operation page of test01

Step 2 Set **Export Destination** to **Local PC** and click **Next**.

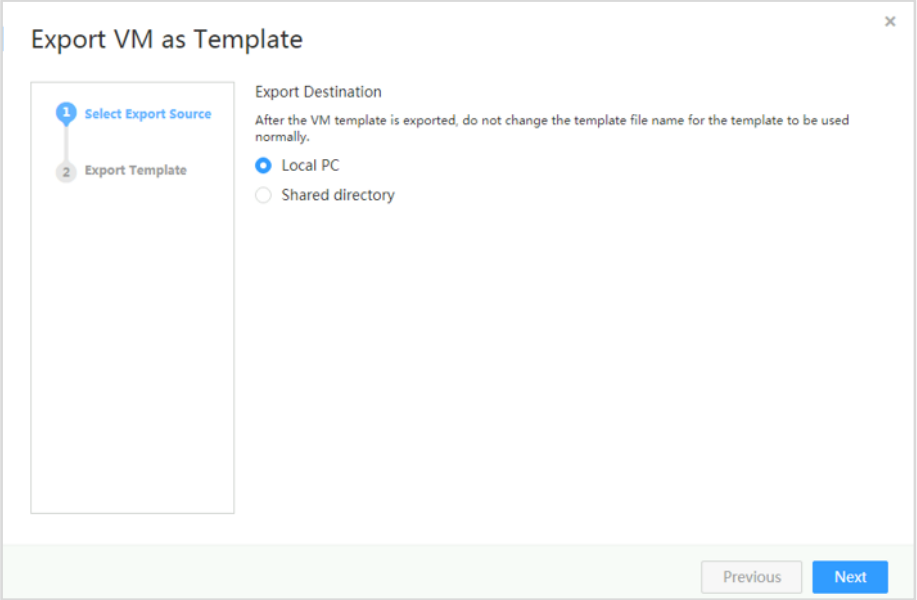


Figure 3-29 Exporting a template

Step 3 Enter the template name and click **OK**.

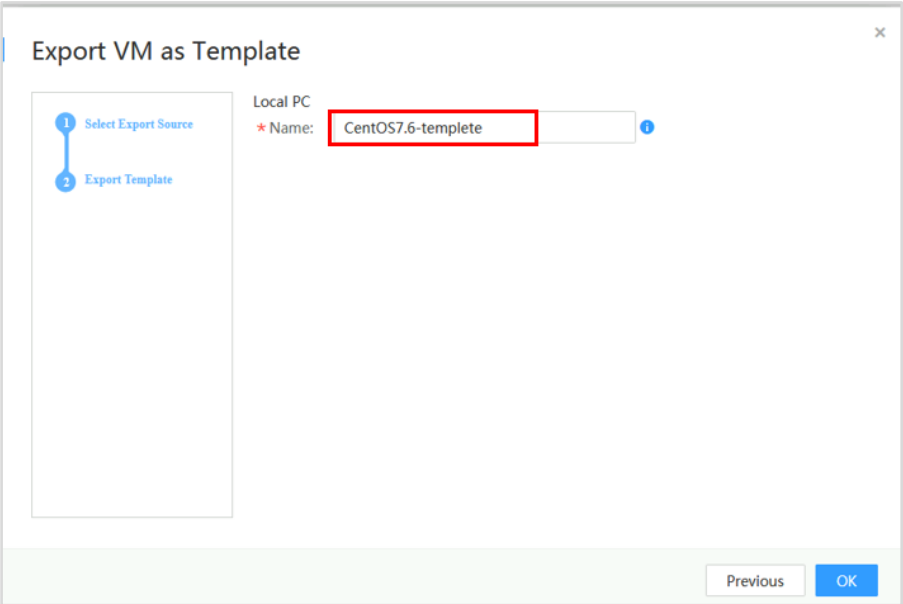


Figure 3-30 Configuring the template name

Step 4 Click **OK** in the two dialog boxes that are displayed.

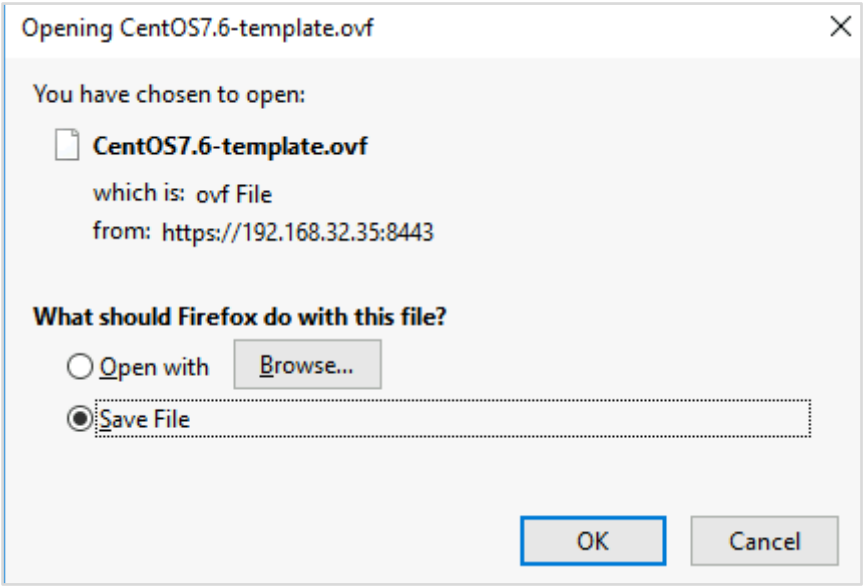


Figure 3-31 Saving the template

Step 5 View the export progress on the **Task Center** page.

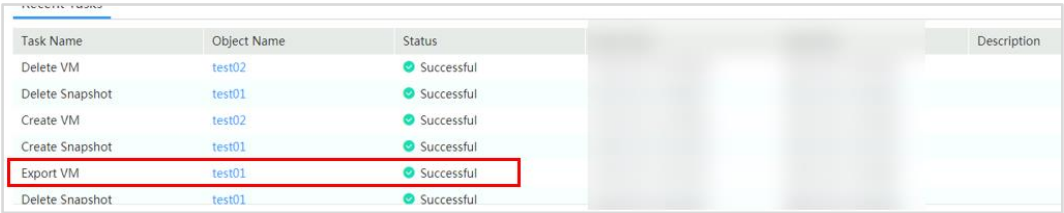


Figure 3-32 Confirming that the export is successful

Step 6 In the download directory of the browser, find the exported VM template file.

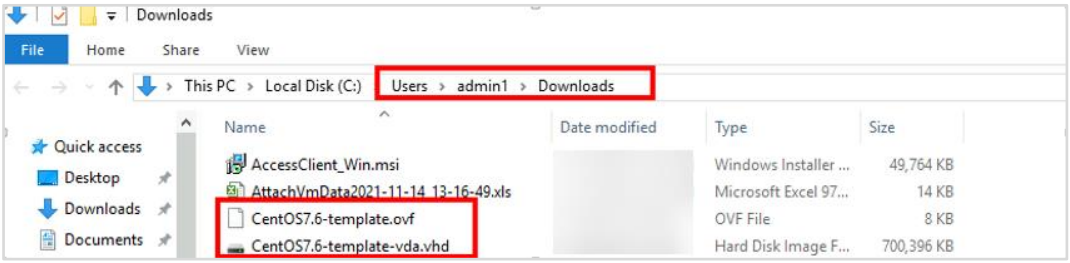


Figure 3-33 Determining the template location

3.1.2.5 Deleting a VM

Step 1 Choose **Resource Pools** > **mycluster** > **VM** > **test01**. The VM management page is displayed.

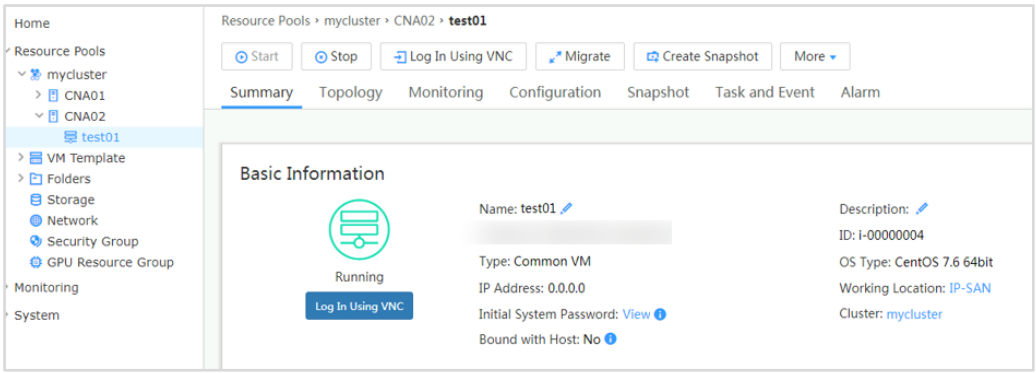


Figure 3-34 VM management page

Step 2 Click **Operation** and choose **Safely Delete** from the drop-down list.

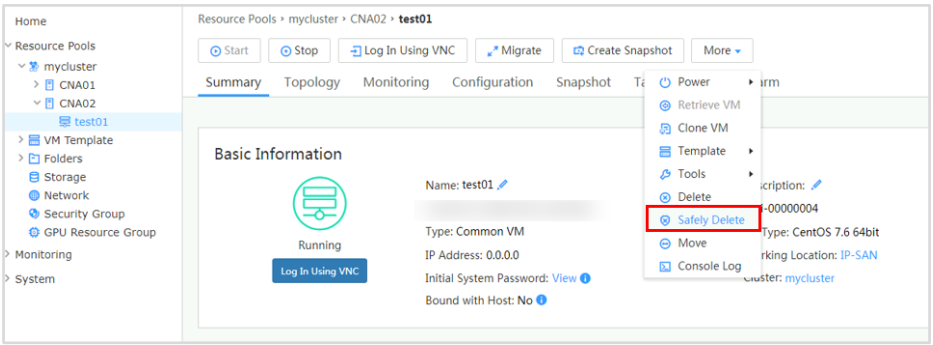


Figure 3-35 Choosing Safely Delete

Step 3 In the **Information** dialog box that is displayed, click **Delete now** and click **OK** to delete VM test01.

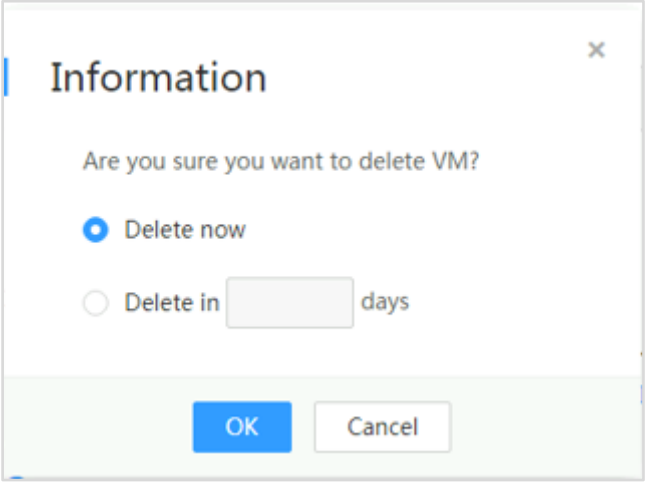


Figure 3-36 Delete now

Step 4 Enter **YES** as prompted to confirm the deletion.

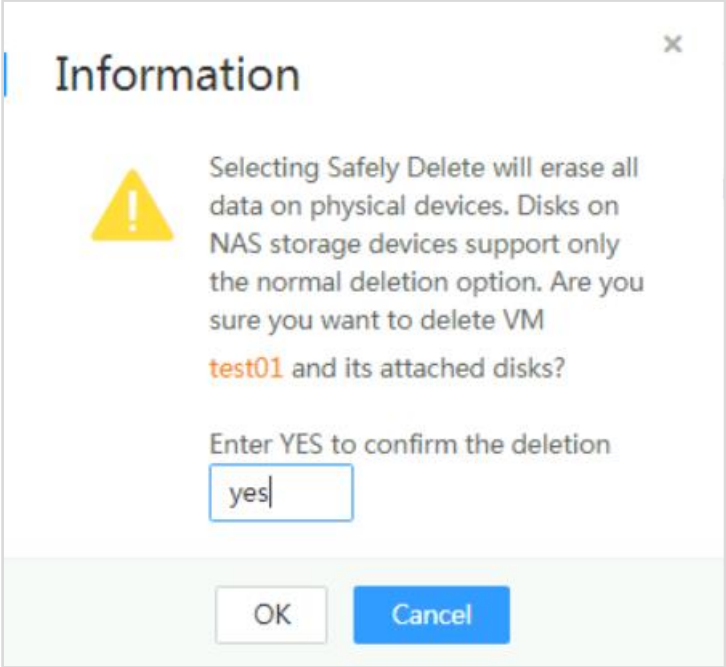


Figure 3-37 Entering YES

3.1.2.6 Importing a Template

Step 1 Choose **Resource Pools** > **VM Template**.

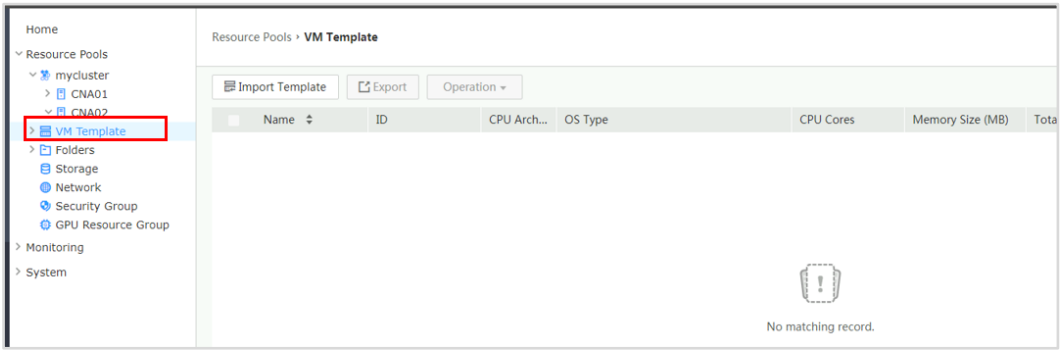


Figure 3-38

Step 2 Click **Import Template**.

Step 3 Click **Import from Local PC** and click **Select** next to the **Template File** text box. In the dialog box that is displayed, select the image template you have exported to the local path in section 3.1.2.4 "Creating a VM Template" and click **Open**. Confirm the information and click **Next**.

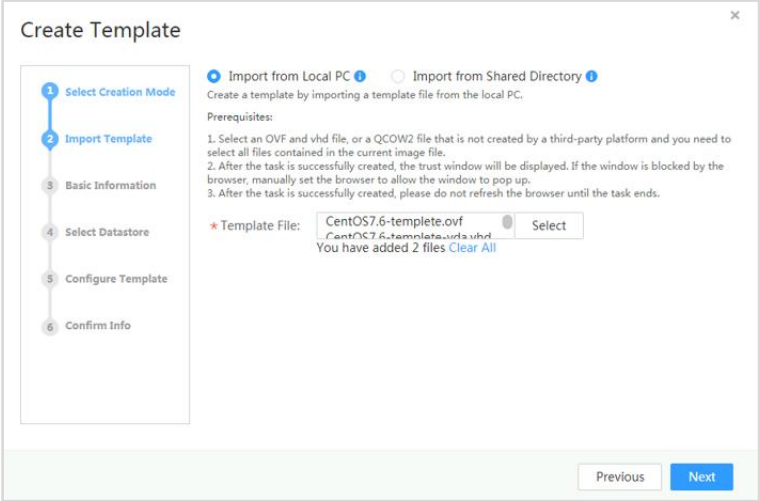


Figure 3-39 Importing a template

Step 4 Set **Name** to **CentOS**, **Select Template Location** to **site**, and **Set Compute Resource** to **mycluster**, and click **Next**.

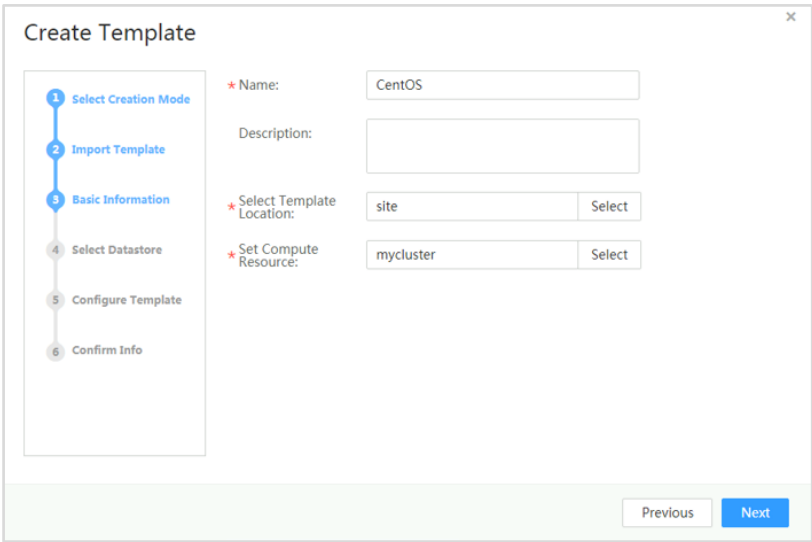


Figure 3-40 Configuring a template

Step 5 On the **Select Datastore** page, select **IP-SAN** and click **Next**.

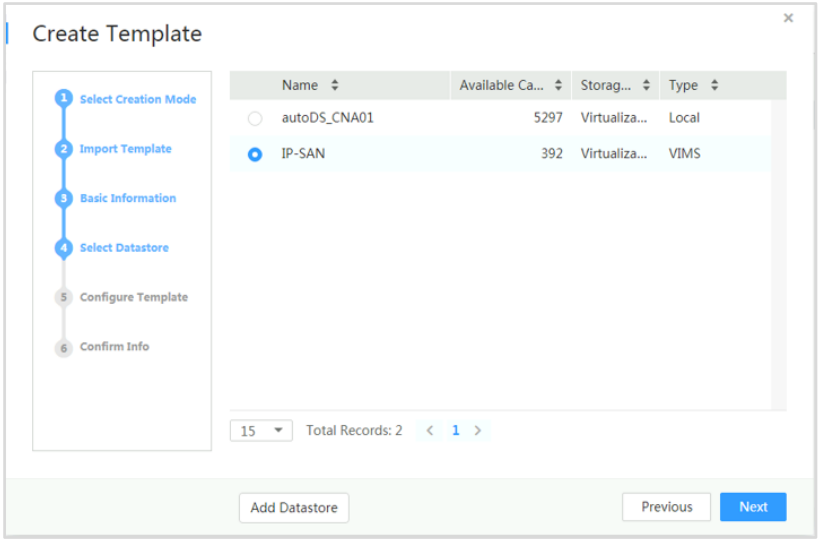


Figure 3-41 Select a datastore

Step 6 Use the default values for hardware configuration parameters and click **Next**.

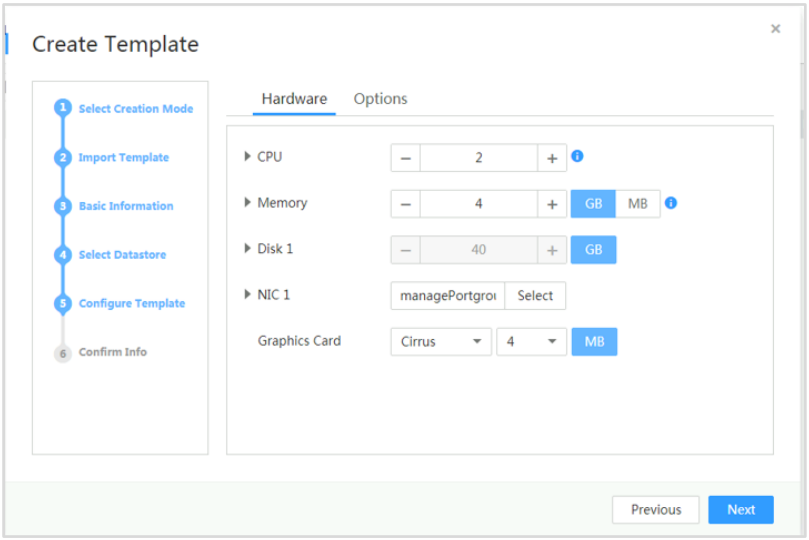


Figure 3-42 Setting template parameters

Step 7 Confirm the information and click **OK**. Wait until the template is created. (This step takes some time. Please wait.)

Note: Deselect **Generate Initial Password**.

Step 8 After the template is uploaded, verify that the template is displayed on the **VM Template** page.

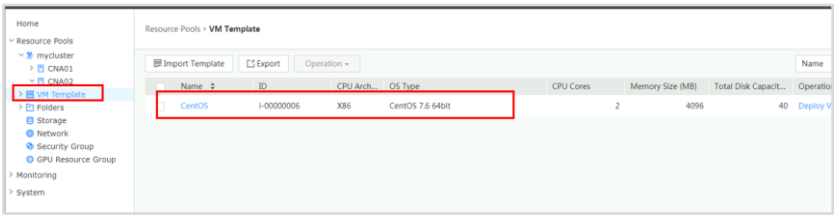


Figure 3-43 Viewing the template

3.1.2.7 Deploying a VM Using a Template

Step 1 Choose **Resource Pools** > **VM Template**. The VM template management page is displayed.

Step 2 Select the **CentOS** template, click **Operation**, and choose **Deploy VM Using Template**.

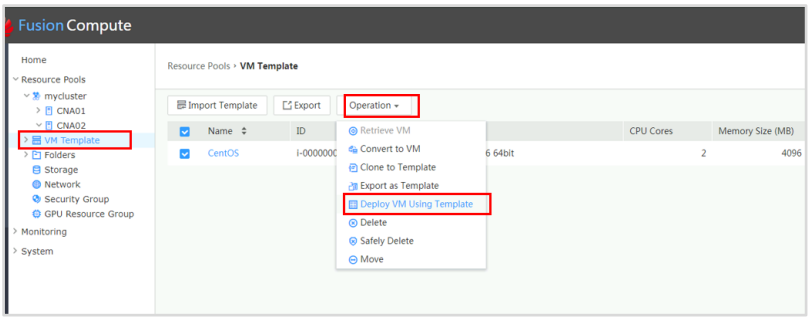


Figure 3-44 Deploying a VM using a template

Step 3 Set **Name** to **CentOS01**, use the default values for other parameters, and click **Next**.

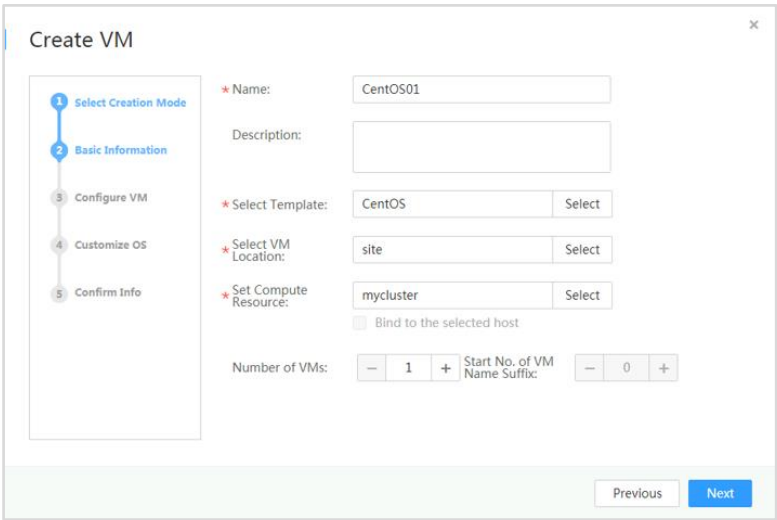


Figure 3-45 Configuring a VM

Step 4 Use the default values and click **Next**.

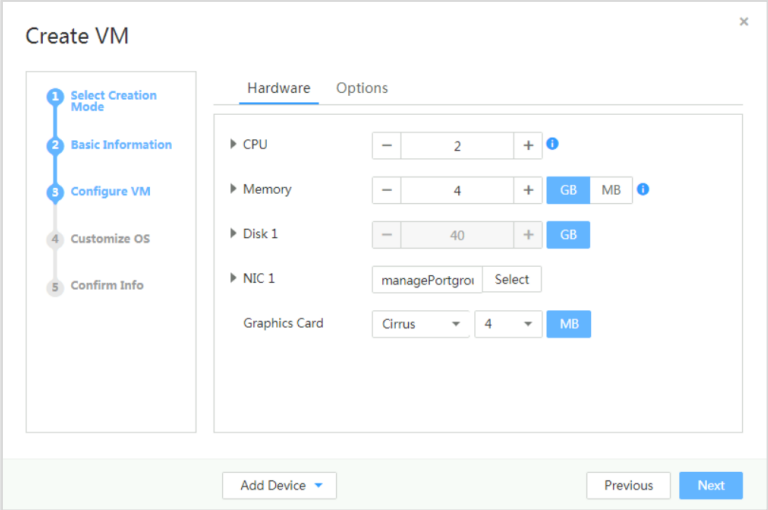


Figure 3-46 Setting VM parameters

Step 5 Deselect **Generate Initial Password** and click **Next**.

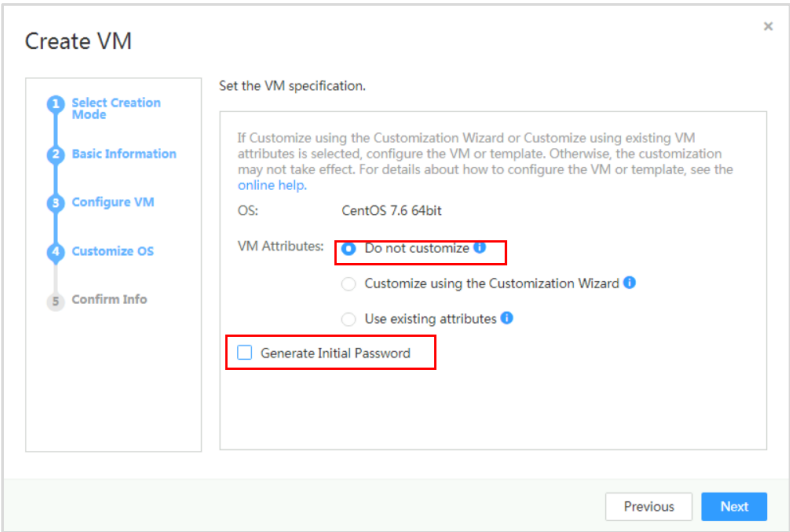


Figure 3-47 Deselecting Generate Initial Password

Step 6 Confirm the information, select **Start VM immediately after creation**, and click **OK**.

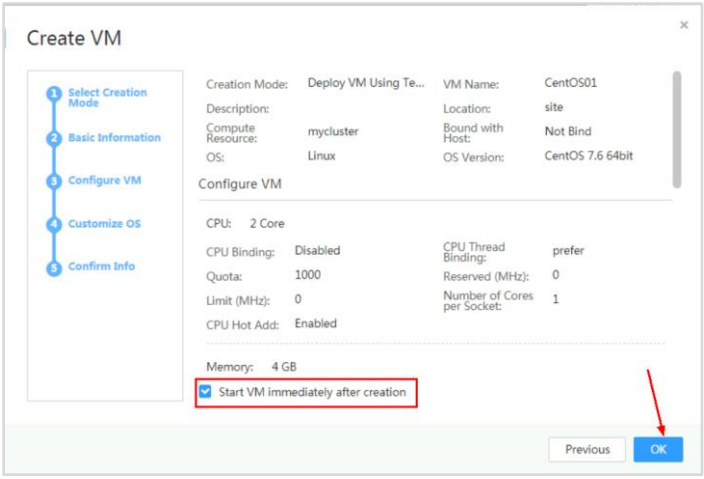


Figure 3-48 VM created

Step 7 Choose **Resource Pools** > **mycluster**. On the **VM** tab page, view the new VM.

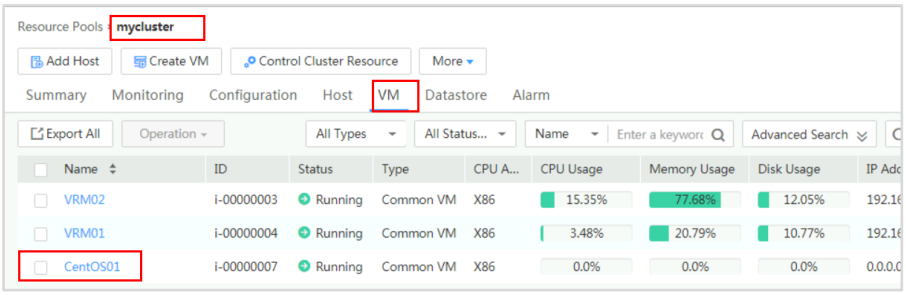


Figure 3-49 Viewing the new VM

3.1.2.8 Deleting a VM

For details, see section 3.1.2.5 "Deleting a VM."

Step 1 Choose **Resource Pools** > **VM**. The VM list page is displayed.

Step 2 Locate VM CentOS01, click **More**, and choose **Safely Delete** from the drop-down list.

Step 3 In the **Information** dialog box that displayed, select **Delete now** and click **OK** to delete the template.

Step 4 Enter **YES** as prompted to confirm the deletion.

3.2 VM Management

3.2.1 Introduction

3.2.1.1 About This Exercise

This exercise illustrates how to manage VMs on FusionCompute, including adjusting flavors, creating snapshots, live migrating VMs, configuring security groups, and configuring HA.

3.2.1.2 Objectives

- Adjust VM flavors and understand precautions on these operations.
- Migrate VMs.
- Configure rule groups.
- Configure security groups.
- Understand how and why to configure HA.

3.2.1.3 Procedure

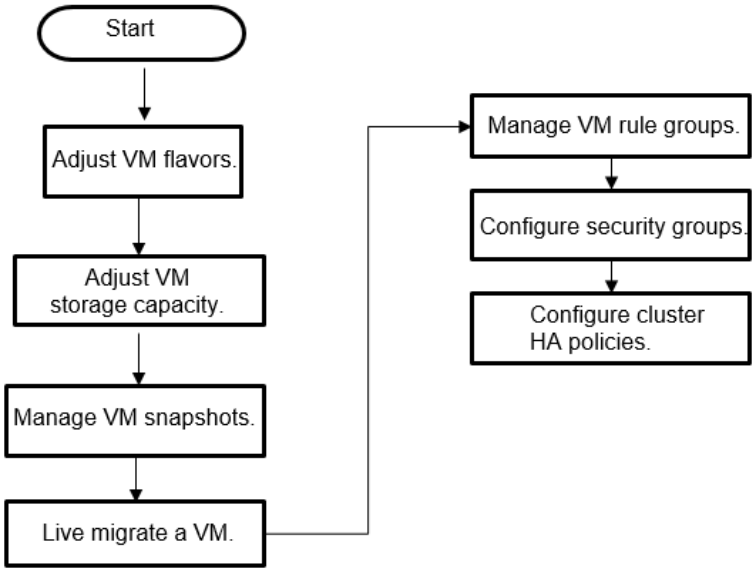


Figure 3-50 Procedure

3.2.2 VM Parameter Modification

3.2.2.1 Deploying a VM Using a Template

Step 1 Deploy a CentOS VM using the CentOS template created in section 3.1.2.7 "Deploying a VM Using a Template." Set **Name** to **CentOS02** on the **Basic Information** page and to **IP-SAN** on the **Select Datastore** page. Deselect **Generate Initial Password** on the **Customize OS** page, select **Start VM immediately after creation** on the **Confirm Info** page, and use the default values for other parameters to create VM CentOS02.

3.2.2.2 Configuring the VM Network

Step 1 On the CentOS VM management page of FusionCompute, click the **Configuration** tab. Choose **NIC** in the navigation tree on the left. The network adapter configuration page is displayed.

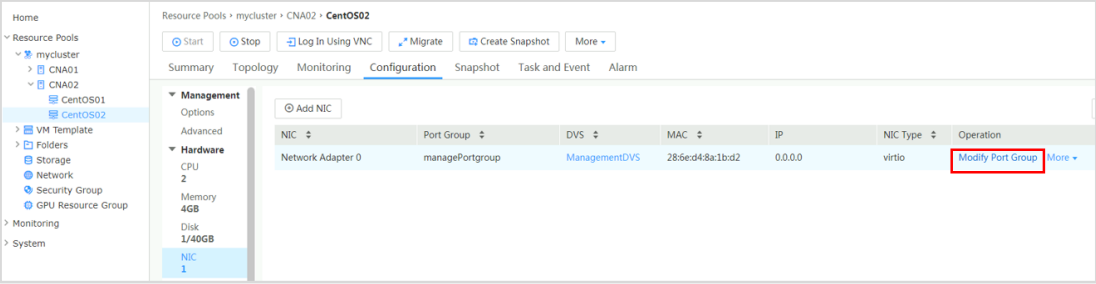


Figure 3-51 Network adapter configuration page

Step 2 Click **Modify Port Group** in the **Operation** column. In the dialog box that is displayed, click **OK**. Change the port group name to **test** and click **OK**.

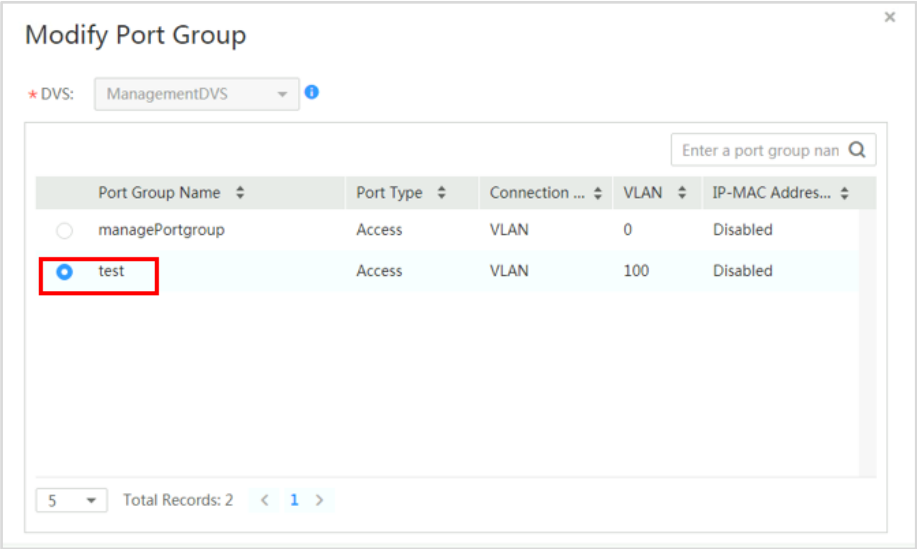


Figure 3-52 Modifying a port group

3.2.2.3 Adding a VM Network Adapter

Step 1 In the navigation tree on the left of FusionCompute, select the VM to be operated (for example, CentOS02), click the **Configuration** tab, choose **Hardware** > **NIC**, and click **Add NIC**.

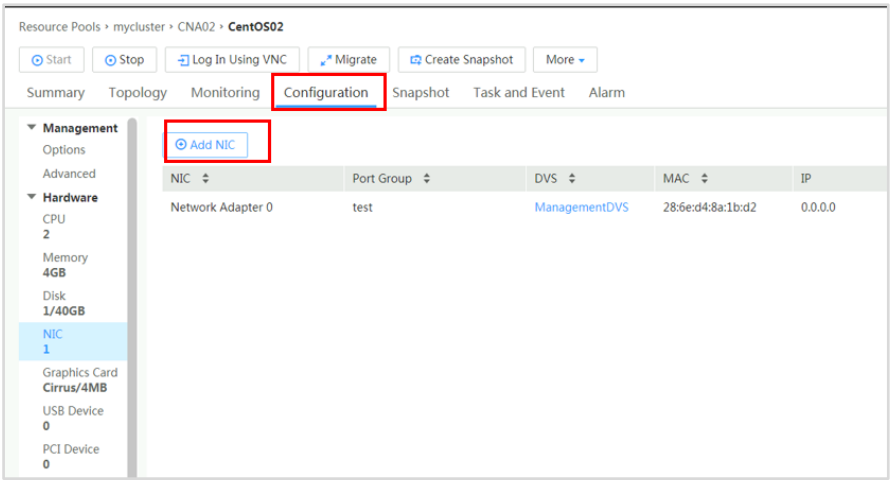


Figure 3-53 Adding a network adapter

Step 2 Set **Port Group** to **managePortgroup**, use the default values for other parameters, and click **OK**.

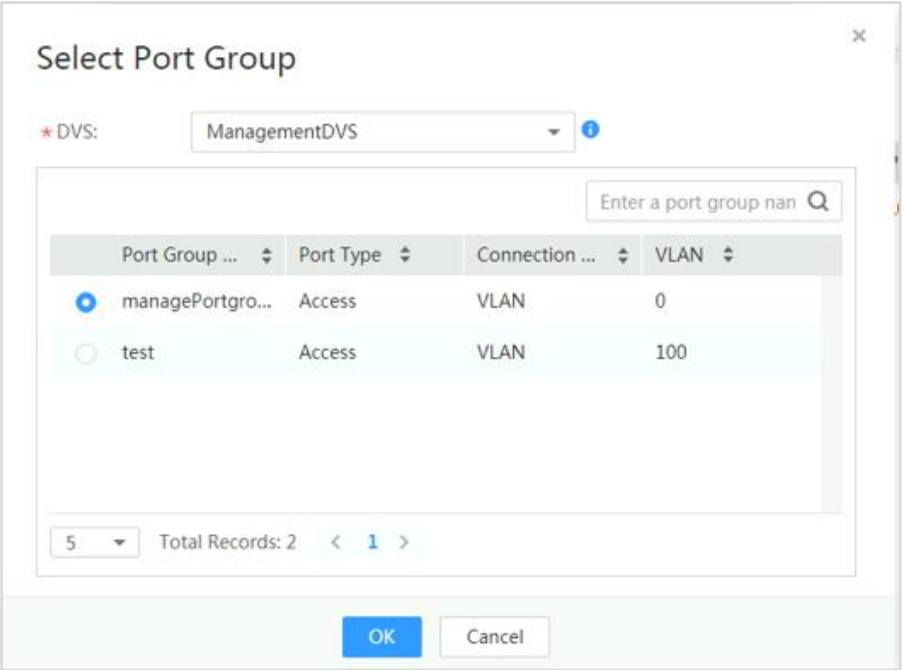


Figure 3-54 Selecting a port group

Step 3 View network adapter information of the VM on the network adapter management page.

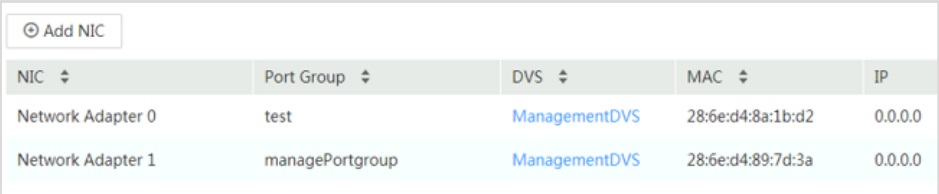


Figure 3-55 Viewing network adapter information

3.2.2.4 Adding CPUs to a VM

Step 1 Choose **Resource Pools** > **mycluster**. Select the CentOS02 VM. On the CentOS02 VM management page, click the **Summary** tab and view the current CPU quantity of the VM. (You can also log in to the VM and run the **cat /proc/cpuinfo|grep "cpu cores" |wc -l** command to view and record the current CPU information.)

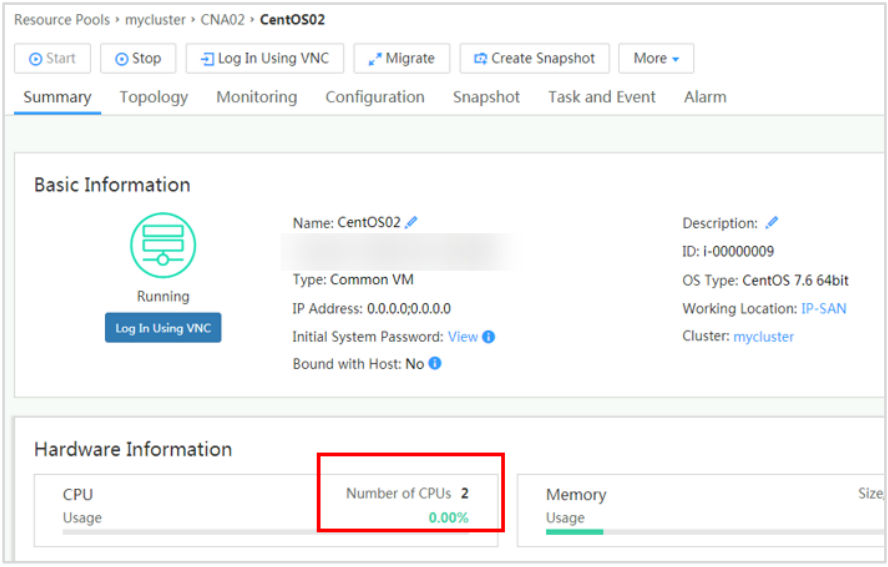


Figure 3-56 Viewing the current CPU quantity of the VM

Step 2 Click the **Configuration** tab, choose **CPU**, set **Number of Cores** to **4**, and click **OK**.

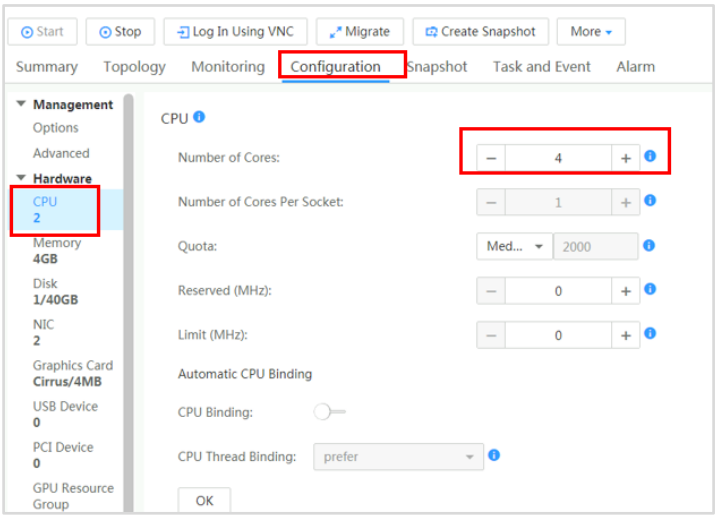


Figure 3-57 Changing the number of CPU cores

Step 3 Restart the CentOS02 VM.

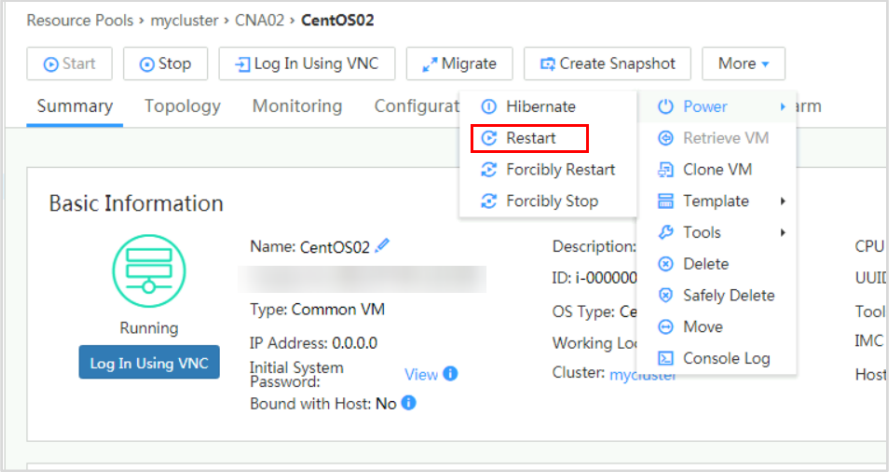


Figure 3-58 Restarting the system

Step 4 Click the **Summary** tab to view the modified CPU information. (You can also log in to the VM and run the **cat /proc/cpuinfo|grep "cpu cores" |wc -l** command to view the modified CPU information.)

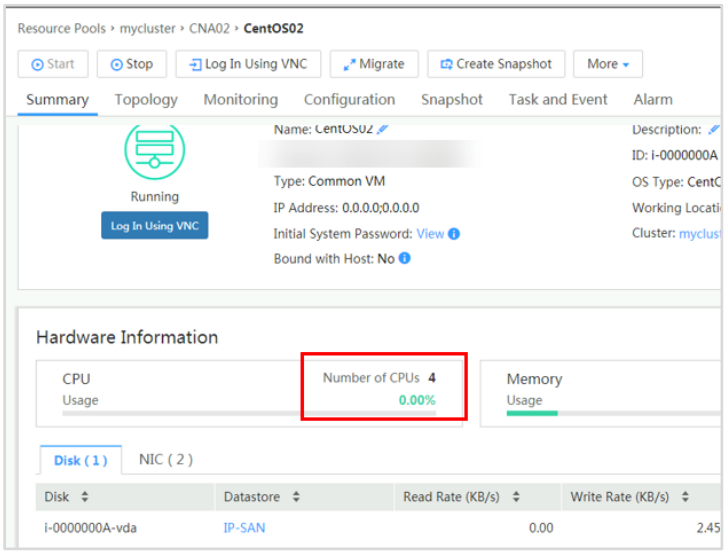


Figure 3-59 Checking the number of CPU cores after modification

3.2.2.5 Hot-Adding Memory to a VM

Step 1 Choose **Resource Pools** > **mycluster**. Select the CentOS02 VM. On the CentOS02 VM management page, click the **Summary** tab and view the current memory capacity of the VM. (You can also log in to the VM and run the **free -g** command to view the current memory information.)

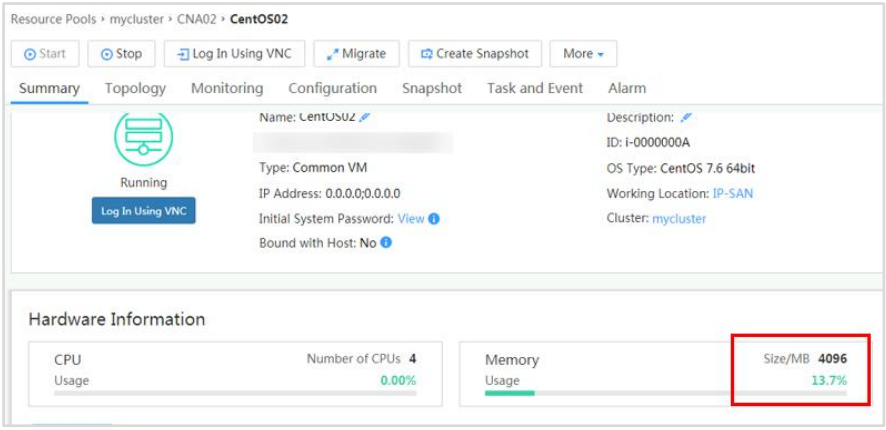


Figure 3-60 Viewing the memory capacity

Step 2 Go back to the CentOS02 VM management page, choose **Configuration** > **Memory**, set **Memory** to **8 GB**, and click **OK**.

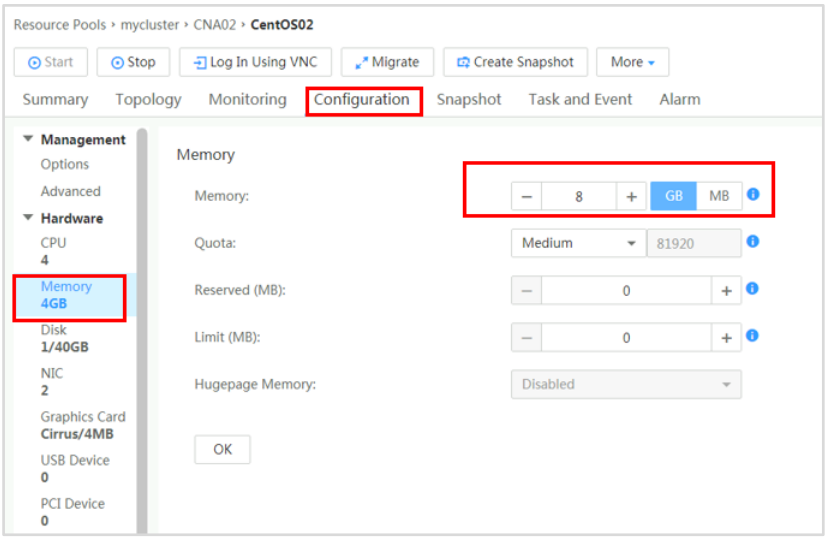


Figure 3-61 Changing the memory size

Step 3 Click the **Summary** tab. Verify that the VM memory size has changed to 8192 MB. (You can also log in to the VM and run the **free -g** command to view the memory capacity after modification.)

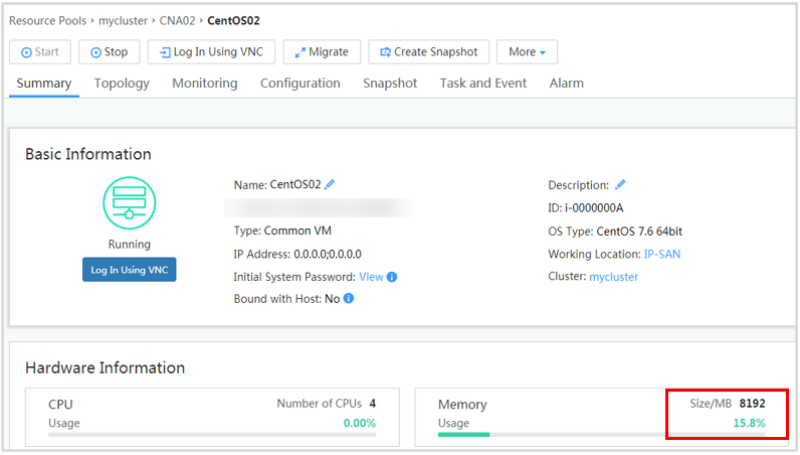


Figure 3-62 Viewing the memory capacity after modification

3.2.2.6 Expanding the VM Disk Capacity

Step 1 Choose **Resource Pools** > **mycluster**. Select the CentOS02 VM. On the CentOS02 VM management page, click the **Summary** tab and view the current disk capacity of the VM.

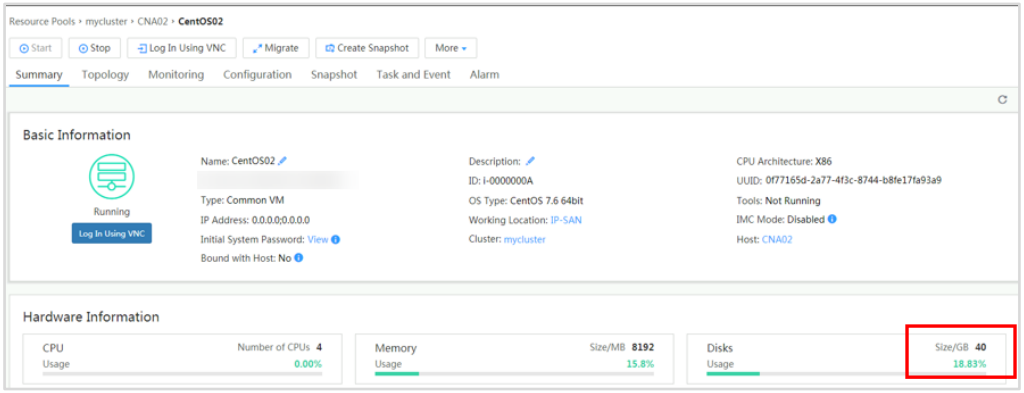


Figure 3-63 View the disk capacity

Step 2 On the **Configuration** tab page, choose **Hardware** > **Disk**. The disk management page is displayed.

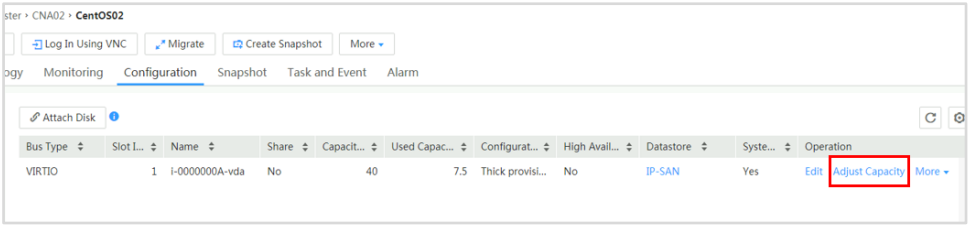


Figure 3-64 Disk management page

Step 3 Click **Adjust Capacity** in the **Operation** column of the disk. In the dialog box that is displayed, set **Capacity (GB)** to **60** and click **Save**.

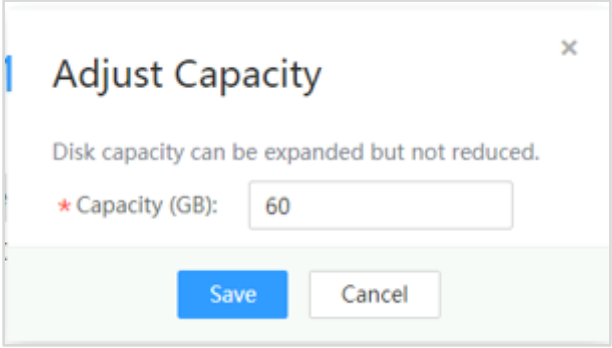


Figure 3-65 Adjusting the disk capacity

Step 4 After the task is complete, verify that the disk capacity has changed to 60 GB on the disk management page.

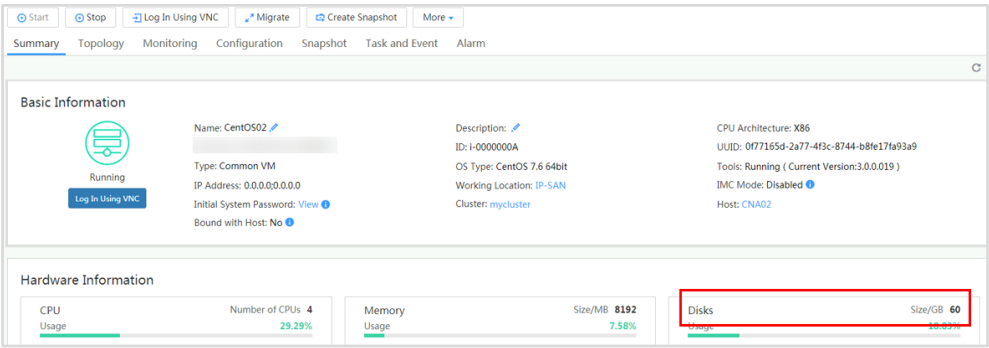
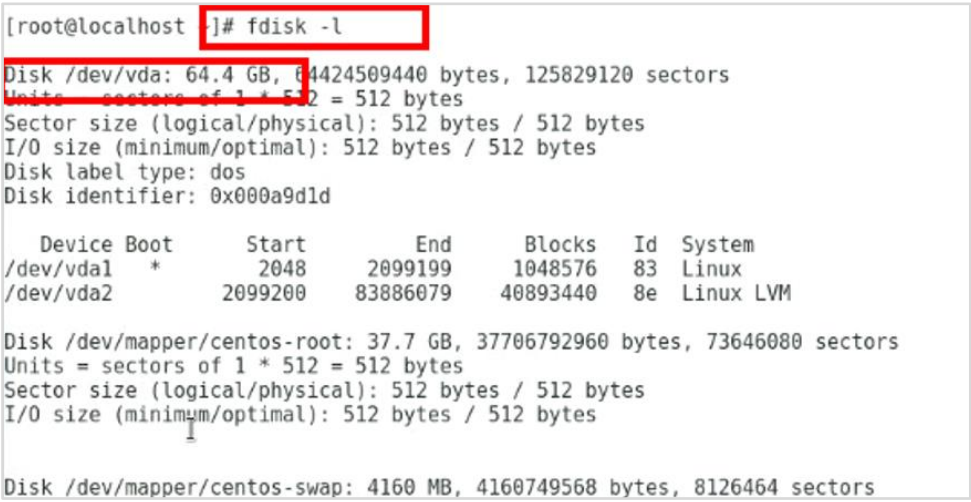


Figure 3-66 Viewing the disk capacity after adjustment

Step 5 (Optional) Log in to the CentOS02 VM using VNC and view the current disk capacity. The command output shows that the disk capacity has been changed to 60 GB.

```
[root@localhost ~]# fdisk –l
```



```
[root@localhost ~]# fdisk -l

Disk /dev/vda: 64.4 GB, 64424509440 bytes, 125829120 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x000a9d1d

   Device Boot      Start         End      Blocks   Id  System
/dev/vda1   *        2048     2099199     1048576   83  Linux
/dev/vda2         2099200    83886079    40893440   8e  Linux LVM

Disk /dev/mapper/centos-root: 37.7 GB, 37706792960 bytes, 73646080 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/mapper/centos-swap: 4160 MB, 4160749568 bytes, 8126464 sectors
```

Figure 3-67 Check disk partitions.

Step 6 Check the current file system capacity. The command output shows that the total file system capacity remains unchanged (which is still 40 GB).

```
[root@localhost ~]# df –h
```

```
[root@localhost ~]# df -h
Filesystem              Size  Used Avail Use% Mounted on
/dev/mapper/centos-root  36G  3.5G   32G  10% /
devtmpfs                1.9G     0  1.9G   0% /dev
tmpfs                   1.9G     0  1.9G   0% /dev/shm
tmpfs                   1.9G  8.8M  1.9G   1% /run
tmpfs                   1.9G     0  1.9G   0% /sys/fs/cgroup
/dev/vda1              1014M  208M  807M  21% /boot
tmpfs                   376M   28K  376M   1% /run/user/0
[root@localhost ~]#
```

Figure 3-68 Checking the system mounting status

Step 7 Create a disk partition.

```
[root@localhost ~]# fdisk /dev/vda
```

```
[root@localhost ~]# fdisk /dev/vda
Welcome to fdisk (util-linux 2.23.2).
```

```
Command (m for help): n
Partition type:
   p   primary (2 primary, 0 extended, 2 free)
   e   extended
Select (default p): p
Partition number (3,4, default 3):
First sector (83886080-125829119, default 83886080):
Using default value 83886080
Last sector, +sectors or +size{K,M,G} (83886080-125829119, default 125829119):
Using default value 125829119
Partition 3 of type Linux and of size 20 GiB is set

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.

WARNING: Re-reading the partition table failed with error 16: Device or resource busy.
The kernel still uses the old table. The new table will be used at
the next reboot or after you run partprobe(8) or kpartx(8)
Syncing disks.
[root@localhost ~]#
```

Figure 3-69 Creating a disk partition

Step 8 Restart the Linux system.

```
[root@localhost ~]# reboot
```

Step 9 Create a physical volume (PV).

```
[root@localhost ~]# pvcreate /dev/vda3
```

```
File  Edit  View  Search  Terminal  Help
[root@localhost ~]# pvcreate /dev/vda3
  Physical volume "/dev/vda3" successfully created.
[root@localhost ~]#
```

Figure 3-70 Creating a PV

Step 10 View information about the current PV.

```
[root@localhost ~]# pvdisplay
```

```
[root@localhost ~]# pvdisplay
  --- Physical volume ---
  PV Name               /dev/vda2
  VG Name               centos
  PV Size               <39.00 GiB / not usable 3.00 MiB
  Allocatable           yes
  PE Size               4.00 MiB
  Total PE              9983
  Free PE               1
  Allocated PE          9982
  PV UUID               cK9xiT-Apo0-wmhZ-3hkT-XaIB-DytK-hdRmUr

  "/dev/vda3" is a new physical volume of "20.00 GiB"
  --- NEW Physical volume ---
  PV Name               /dev/vda3
  VG Name
  PV Size               20.00 GiB
  Allocatable           NO
  PE Size               0
  Total PE              0
  Free PE               0
  Allocated PE          0
  PV UUID               JV721r-breH-p0j0-28Os-ww2L-Halt-RBBJef
```

Figure 3-71 Viewing information about the current PV

Step 11 Add the new partition /dev/vda3 to the current volume group centos.

```
[root@localhost ~]# vgextend centos /dev/vda3
```

```
[root@localhost ~]# vgextend centos /dev/vda3
  Volume group "centos" successfully extended
[root@localhost ~]#
```

Figure 3-72 Expanding the capacity of a volume group

Step 12 View information about the centos volume group.

```
[root@localhost ~]# vgdisplay
```

```
[root@localhost ~]# vgdisplay
  --- Volume group ---
  VG Name               centos
  System ID
  Format                lvm2
  Metadata Areas        2
  Metadata Sequence No  4
  VG Access             read/write
  VG Status             resizable
  MAX LV                0
  Cur LV                2
  Open LV               2
  Max PV                0
  Cur PV                2
  Act PV                2
  VG Size               58.99 GiB
  PE Size               4.00 MiB
  Total PE              15102
  Alloc PE / Size       9982 / 38.99 GiB
  Free  PE / Size       5120 / 20.00 GiB
  VG UUID               Kr0HBu-VIwY-IEc6-uPPU-1WY4-soVo-bKyyMX
```

Figure 3-73 View information about the centos volume group

Step 13 Increase the capacity of a logical volume by 10 GB.

```
[root@localhost ~]# lvresize -L +10G /dev/mapper/centos-root
```

```
[root@localhost ~]# lvresize -L +10G /dev/mapper/centos-root
  Size of logical volume centos/root changed from <35.12 GiB (8990 extents) to <
45.12 GiB (11550 extents).
  Logical volume centos/root successfully resized.
[root@localhost ~]#
```

Figure 3-74 Expanding the capacity of a logical volume

Step 14 Check the file system capacity again.

```
[root@localhost ~]# xfs_growfs /dev/mapper/centos-root
```

```
[root@localhost ~]# lvresize -L +10G /dev/mapper/centos-root
  Size of logical volume centos/root changed from <35.12 GiB (8990 extents) to <
45.12 GiB (11550 extents).
  Logical volume centos/root successfully resized.
[root@localhost ~]# xfs_growfs /dev/mapper/centos-root
meta-data=/dev/mapper/centos-root isize=512    agcount=4, agsize=2301440 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=1        finobt=0 spinodes=0
data     =                       bsize=4096   blocks=9205760, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0 ftype=1
log      =internal               bsize=4096   blocks=4495, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
data blocks changed from 9205760 to 11827200
[root@localhost ~]#
```

Figure 3-75 Scanning the file system

Step 15 Check the file system capacity after capacity expansion. The capacity has been increased by 10 GB.

```
[root@localhost ~]# df –h
```

```
[root@localhost ~]# df -h
Filesystem                Size  Used Avail Use% Mounted on
/dev/mapper/centos-root    46G  3.5G   42G   8% /
devtmpfs                  1.9G     0  1.9G   0% /dev
tmpfs                     1.9G     0  1.9G   0% /dev/shm
tmpfs                     1.9G  8.9M  1.9G   1% /run
tmpfs                     1.9G     0  1.9G   0% /sys/fs/cgroup
/dev/vda1                1014M  208M  807M  21% /boot
tmpfs                     376M  8.0K  376M   1% /run/user/42
tmpfs                     376M   24K  376M   1% /run/user/0
[root@localhost ~]#
```

Figure 3-76 Checking the capacity

3.2.3 VM Storage Adjustment

3.2.3.1 Adding a Common Disk

Step 1 In the navigation tree on the left of FusionCompute, select **CentOS**, click the **Configuration** tab, choose **Hardware** > **Disk**, and click **Attach Disk**.

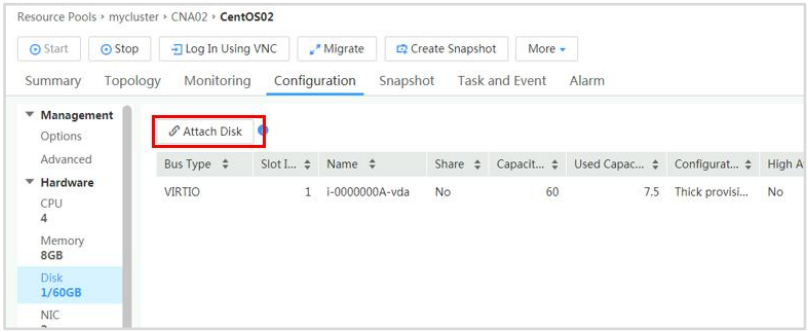


Figure 3-77 Attaching a disk to a VM

Step 2 Select the disk01 disk created in section 2.2.4 "Creating a Disk" and click **OK**.

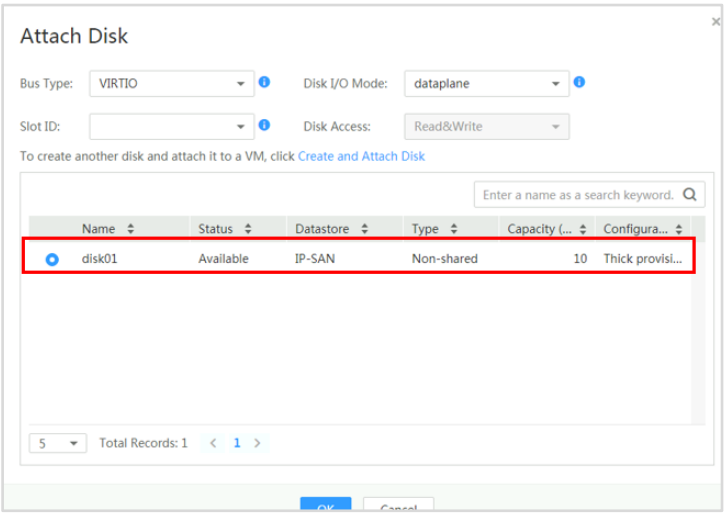


Figure 3-78 Selecting a disk

Step 3 On the VM disk management page, verify that the disk has been attached to the VM.

Figure 3-79 Viewing the attached disk

3.2.3.2 Adjusting the Disk Type

Step 1 On the CentOS02 VM management page, click **Stop**. In the dialog box that is displayed, click **OK** to stop the VM.

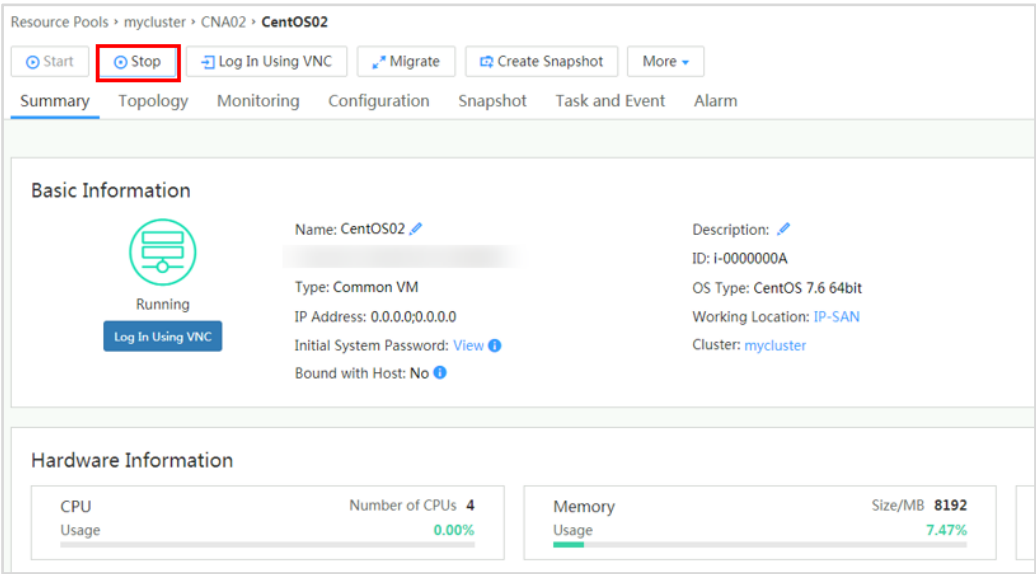


Figure 3-80 Stopping a VM

Step 2 On the CentOS02 VM disk management page, click **Edit** in the **Operation** column of disk01.

Figure 3-81 Editing disk information

Step 3 In the **Modify Disk** dialog box that is displayed, set **Disk Mode** to **Independent & persistent** and click **OK**.

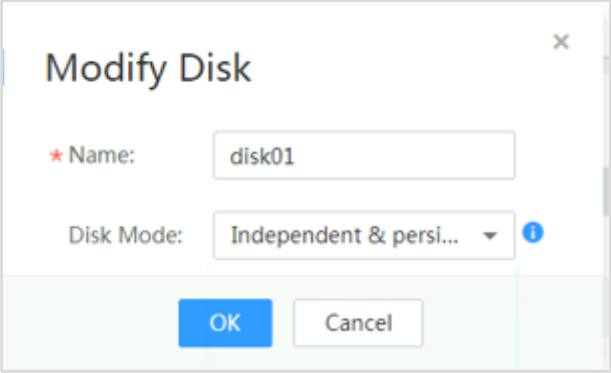


Figure 3-82 Changing the disk mode

3.2.3.3 Deleting a Disk

Step 1 On the CentOS02 VM disk management page, click **Detach** in the **Operation** column of disk01.

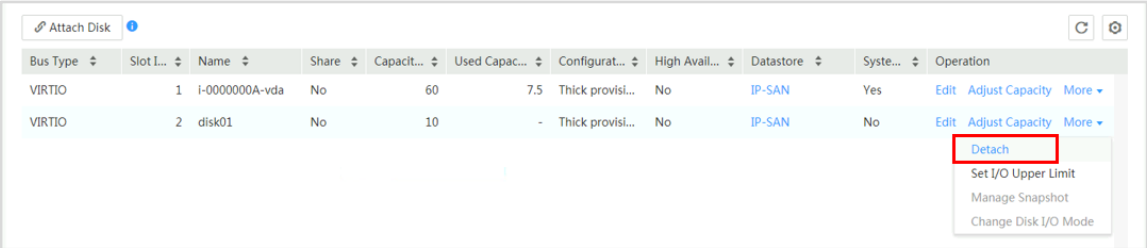


Figure 3-83 Detaching a disk from a VM

Step 2 Choose **Resource Pools** > **Storage** > **IP-SAN** > **Disk List**. Locate the row that contains **disk01**, click **More**, and choose **Safely Delete** to delete disk files.

Figure 3-84 Deleting a disk

3.2.4 VM Snapshot Management

3.2.4.1 Creating a Snapshot

Step 1 Log in to the CentOS02 VM using VNC, create the **/root/hcia** directory on the VM, and create the **huawei.txt** file in this directory.

```
[root@localhost ~]# mkdir /root/hcia
[root@localhost ~]# cd /root/hcia
[root@localhost hcia]# touch huawei.txt
[root@localhost hcia]# ls
huawei.txt
[root@localhost hcia]#
```

Figure 3-85 Creating the huawei.txt file on the VM

Step 2 On the **Snapshot** tab page of the VM, click **Create Snapshot**.

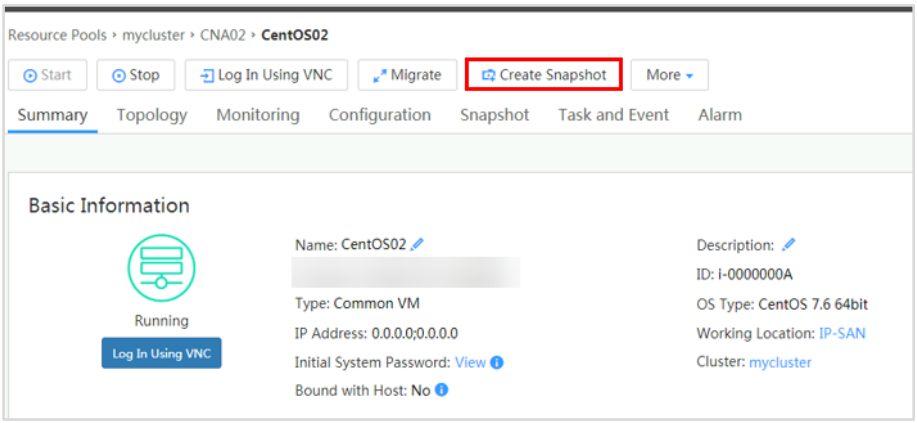


Figure 3-86 Creating a snapshot for a VM

Step 3 Enter **01** in the **Snapshot Name** text box and click **OK** in the displayed dialog box.

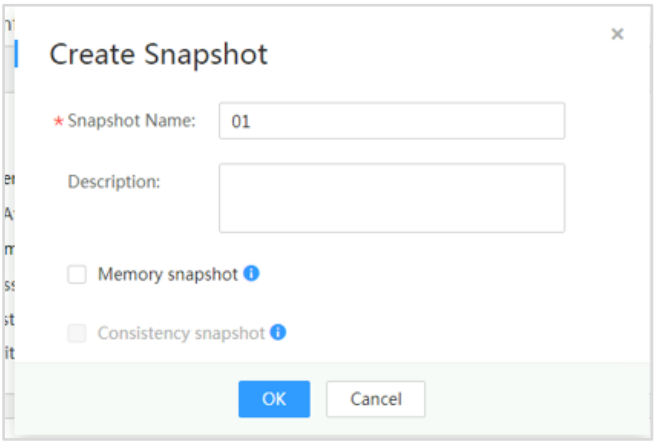


Figure 3-87 Setting the snapshot name

Step 4 Wait for about 1 minute and verify that snapshot 01 is displayed on the **Snapshot** tab page.

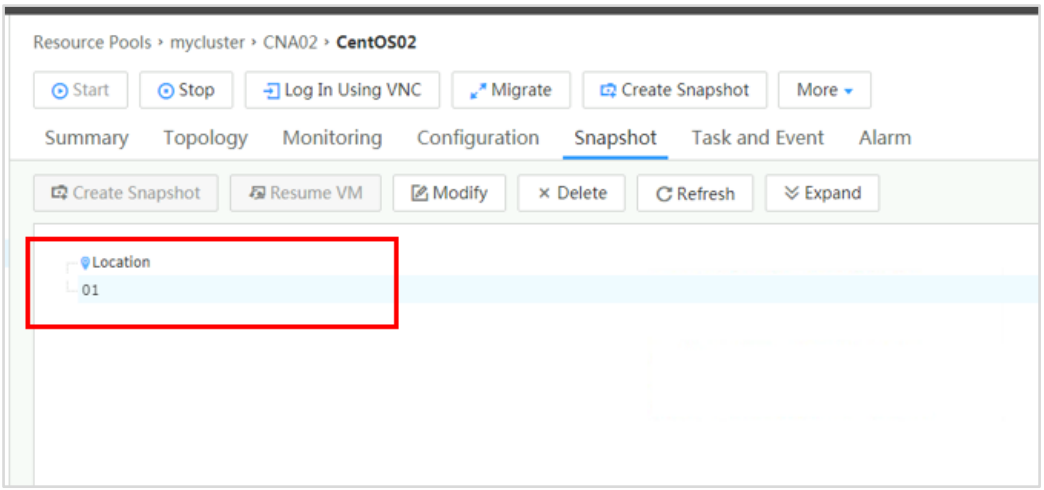


Figure 3-88 Viewing a snapshot

3.2.4.2 Rolling Back a Snapshot

Step 1 Log in to the VM using VNC and create the **huawei123.txt** file in the **/root/hcia** directory of the VM.

```
[root@localhost hcia]# touch huawei123.txt
[root@localhost hcia]# ls
huawei123.txt  huawei.txt
[root@localhost hcia]#
```

Figure 3-89 Creating the huawei123.txt file

Step 2 On the **Snapshot** tab page of the VM, click **Resume VM**.

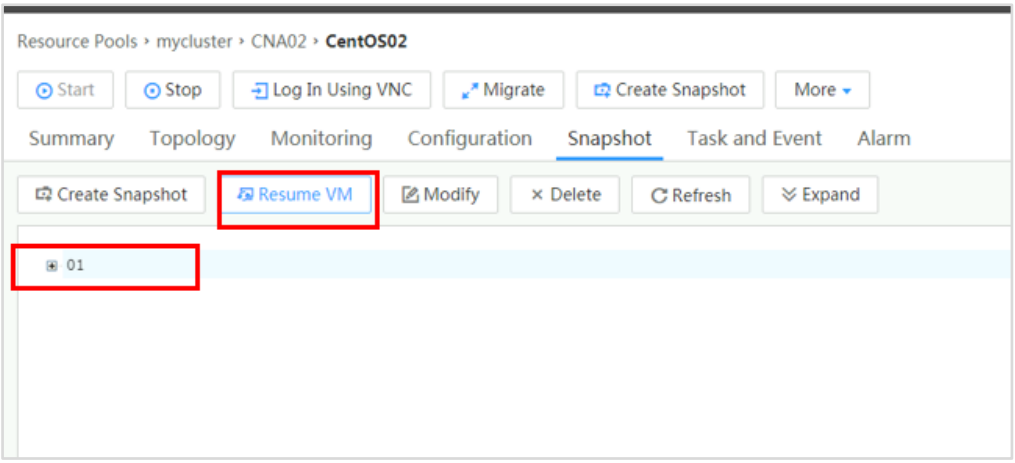


Figure 3-90 Restoring a VM

Step 3 In the **Warning** dialog box that is displayed, click **OK**.

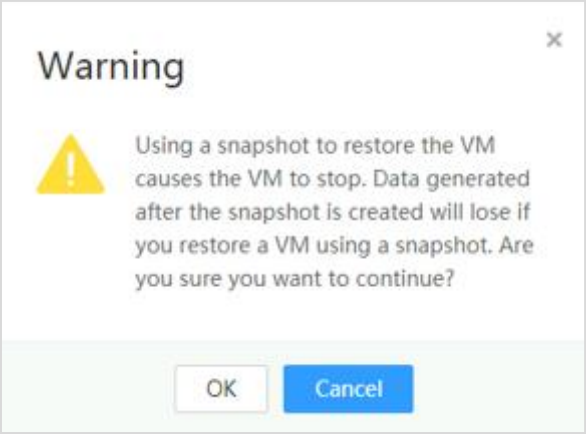


Figure 3-91 Confirming to restore a VM

Step 4 Choose **System** > **Tasks and Logs** > **Task Center** and view the snapshot rollback progress.

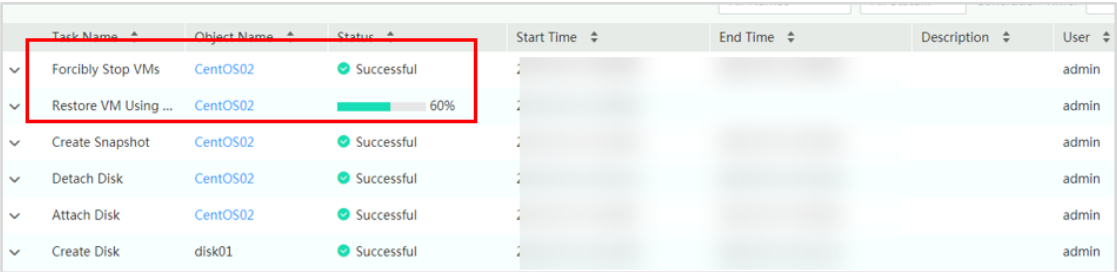


Figure 3-92 VM restoration progress

Step 5 Refresh the page. After the snapshot is rolled back, log in to the VM using VNC. Go to the **/root/hcia** directory of the VM and check the current files. If only the **huawei.txt** file exists, the snapshot restoration is successful.

```
[root@localhost ~]# cd /root/hcia
[root@localhost hcia]# ls
huawei.txt
[root@localhost hcia]#
```

Figure 3-93 Confirming the restoration success

3.2.4.3 Deleting a Snapshot

Step 1 On the snapshot management page of the CentOS02 VM, select the **01** snapshot and click **Delete**.

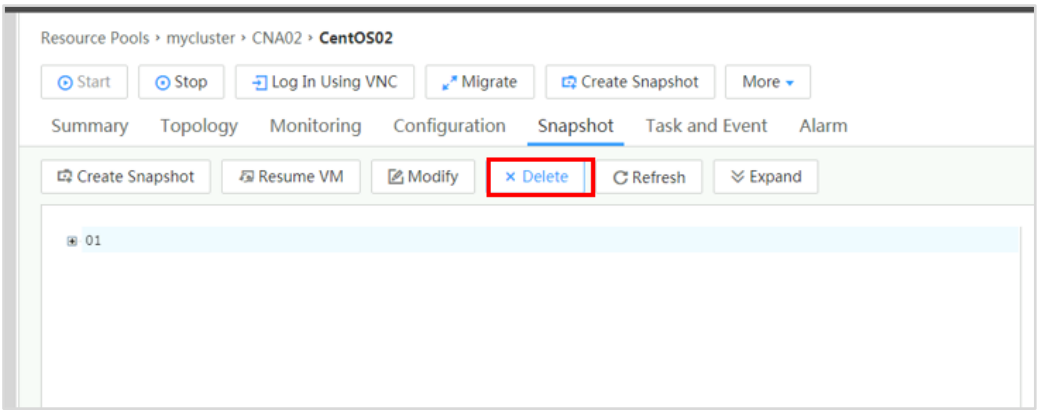


Figure 3-94 Deleting a snapshot

Step 2 In the **Warning** dialog box that is displayed, click **OK**.

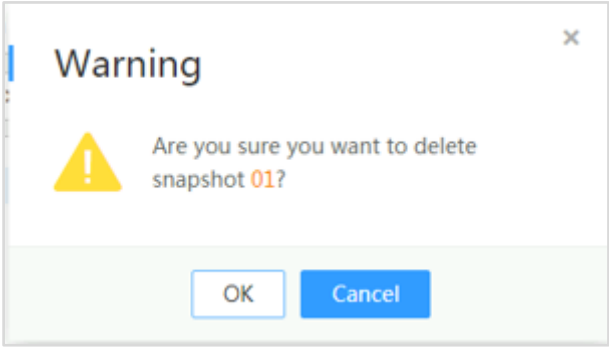


Figure 3-95 Confirming the deletion

Step 3 After the snapshot is deleted, verify that the deleted snapshot is not displayed on the snapshot management page.

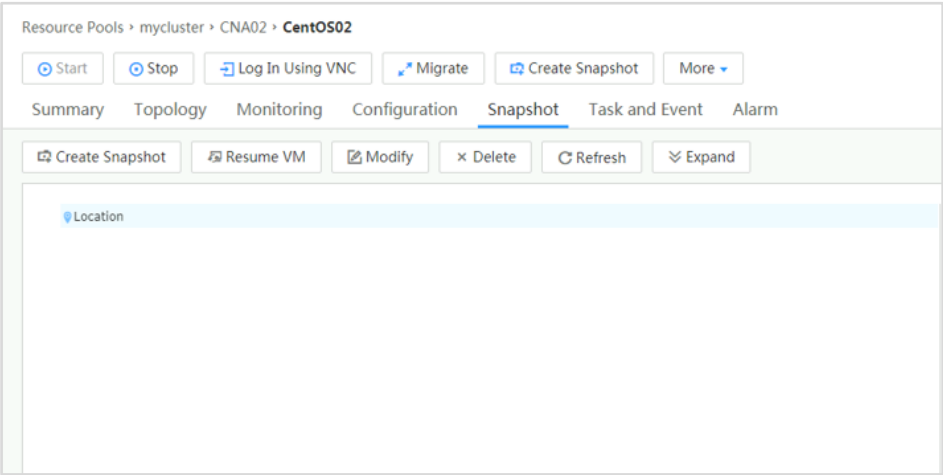


Figure 3-96 Verifying the snapshot deletion result

3.2.5 VM Live Migration

Step 1 On the CentOS02 VM management page, view the host (CNA02 in this example) where the VM is located and click **Migrate**.

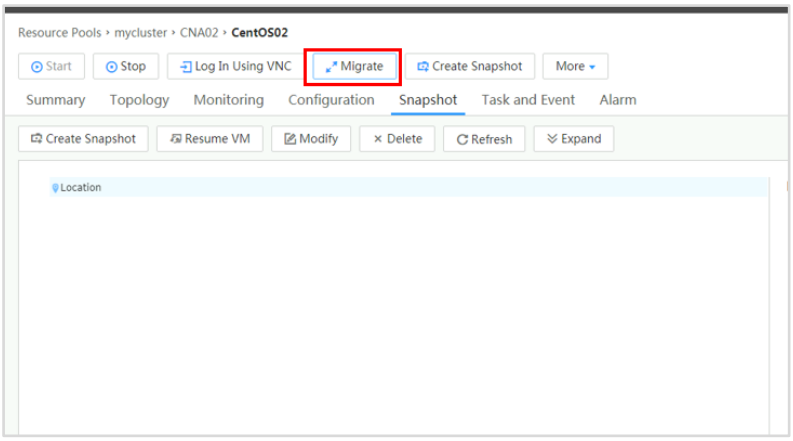


Figure 3-97 VM management page

Step 2 In the displayed dialog box, set **Select Migration Mode** to **Change Host** and **Migration Policy** to **Migration Priority**, and click **Next**.

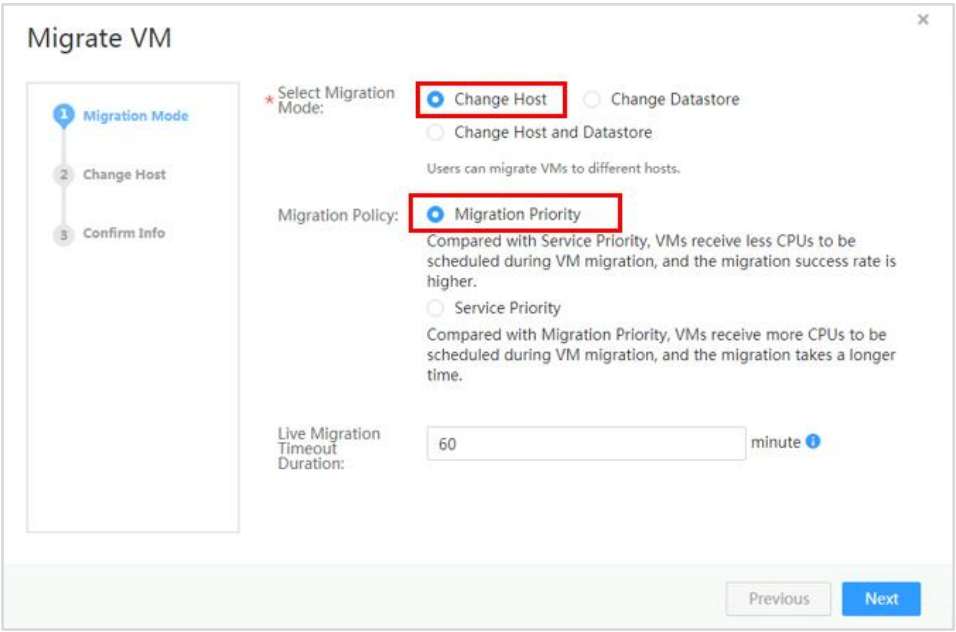


Figure 3-98 Selecting a migration policy

Step 3 Expand the mycluster cluster, click the remaining CNA host, and click **Next**. (The CNA host may vary according to the lab environment. The following uses CNA01 as an example.)

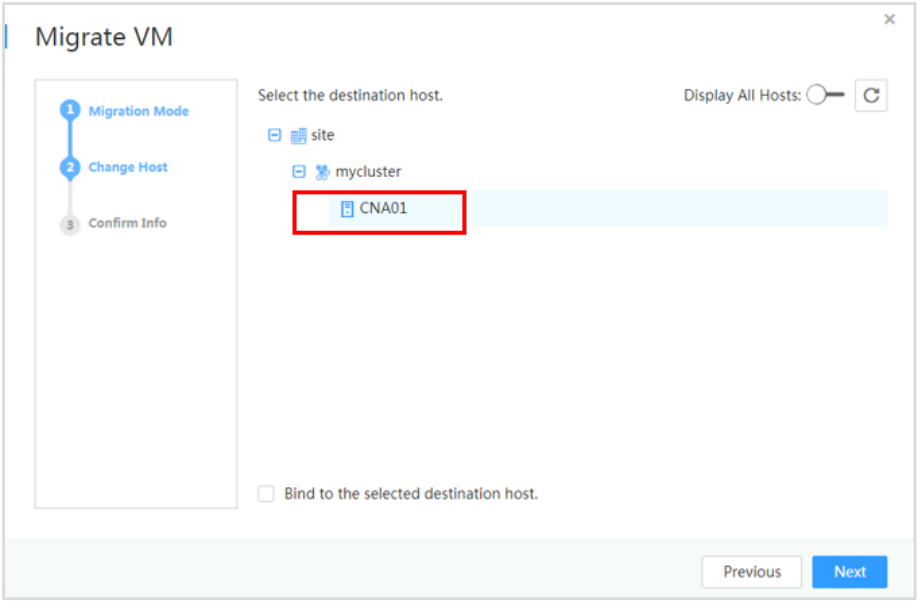


Figure 3-99 Selecting the host to be migrated

Step 4 Confirm the information and click **OK**.

Step 5 Choose **System** > **Tasks and Logs** > **Task Center** to view the task progress. Click to refresh the progress.

Figure 3-100 Migrated

Step 6 After the migration is complete, go to the CentOS02 VM management page, and verify that the VM has been migrated to CNA01.

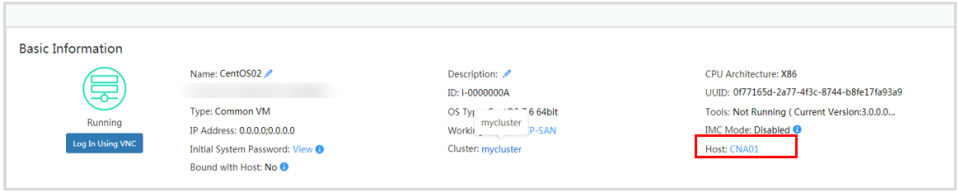


Figure 3-101 Verifying that the VM has been migrated to CNA01

3.2.6 VM Rule Group

3.2.6.1 Deploying a Second VM

Step 1 Deploy a new VM using the CentOS template created in section 3.1.2.7 "Deploying a VM Using a Template." Set the VM name to **CentOS03**, the compute resource to **CNA01**, and the storage resource to **IP-SAN**, use the default values for other parameters, deselect **Generate Initial Password**, select **Start VM immediately after creation**, and click **OK** to create VM CentOS03.

3.2.6.2 Verifying the "Mutually Exclusive VM" Rule Group

Step 1 Choose **Resource Pools** > **mycluster** > **CNA01**. On the **VM** tab page, view the VMs running on CNA01.

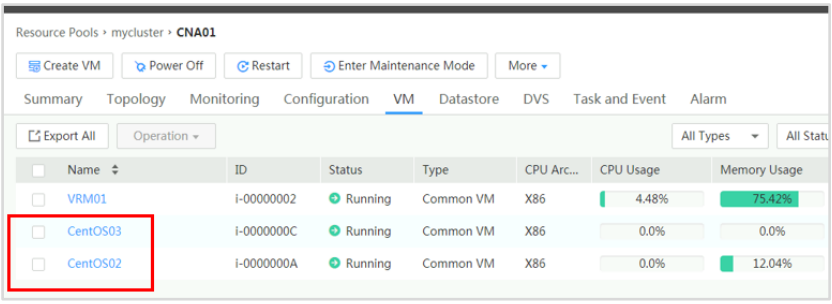


Figure 3-102 Viewing the VMs running on CNA01

Step 2 Choose **Resource Pools** > **mycluster**. Click the **Configuration** tab. Choose **Configuration** > **Control Cluster Resource**. Click **Edit**.

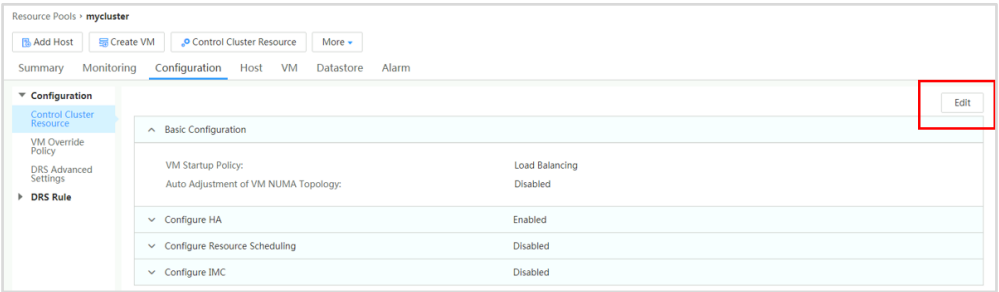


Figure 3-103 Editing cluster resources

Step 3 In the navigation pane, choose **Configure Resource Scheduling**. In the right pane, toggle on **Enable Compute Resource Scheduling**.

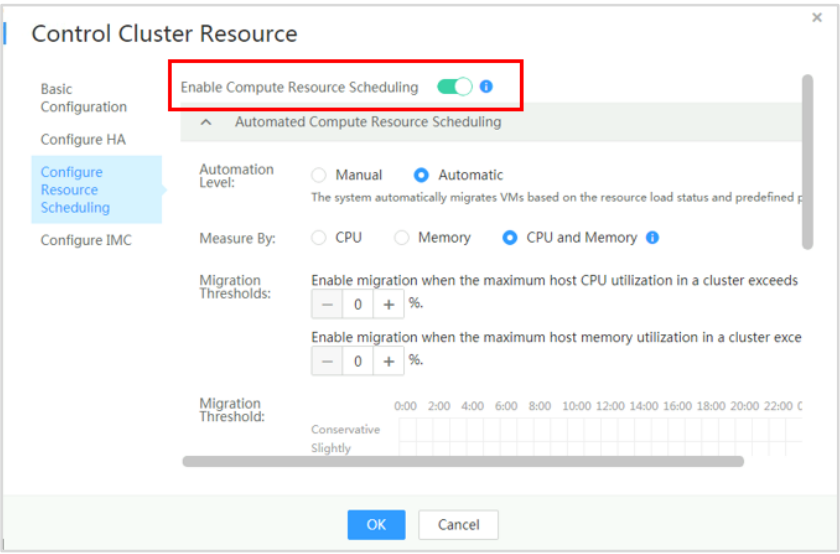


Figure 3-104 Toggling on Enable Compute Resource Scheduling

Step 4 Choose **Resource Pools** > **mycluster**. Click the **Configuration** tab. Choose **DRS Rule** > **Rule Group**. Click **Add**.

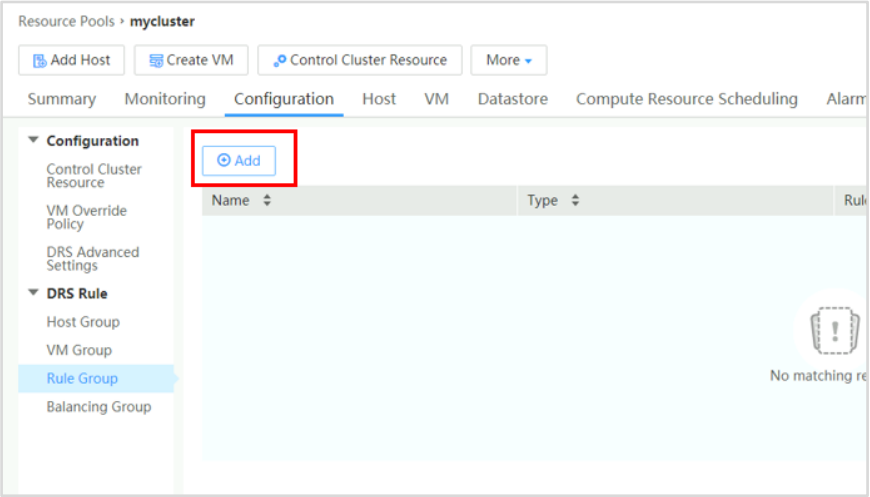


Figure 3-105 Adding a rule group

Step 5 Set **Name** to **Mutually exclusive** and **Type** to **Keep VMs mutually exclusive**. Select **CentOS02** and **CentOS03**, and click **OK**.

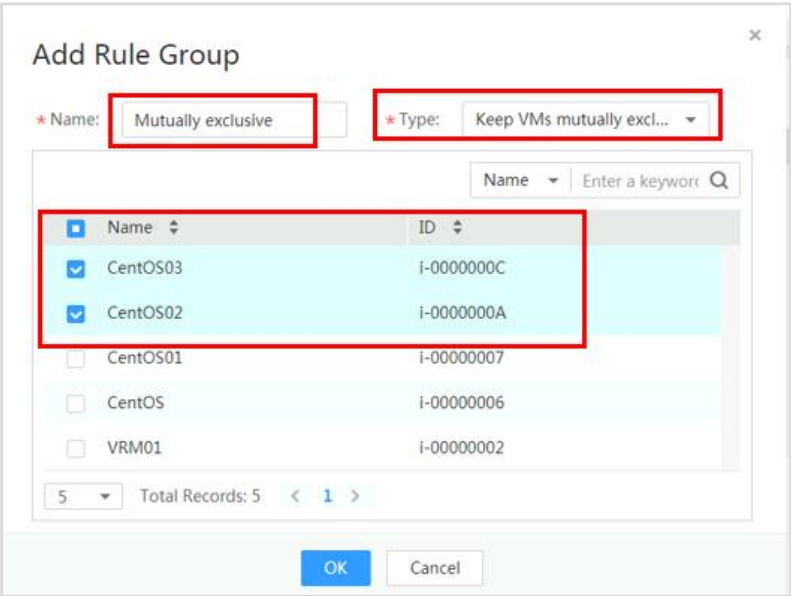


Figure 3-106 Configuring a "Mutually Exclusive VM" rule group

Step 6 Choose **System** > **Tasks and Logs** > **Task Center** and verify that a VM migration task is running. Click **Refresh** to refresh the progress.

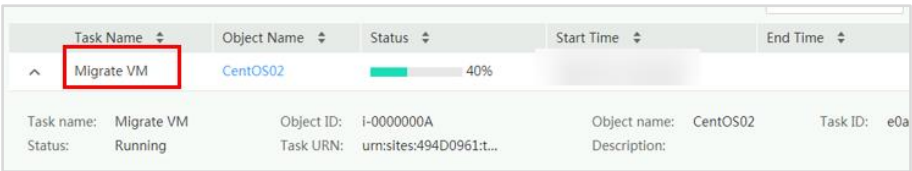


Figure 3-107 Viewing the migration progress

Step 7 After the migration is complete, choose **Resource Pools** > **mycluster** > **CNA01**. On the **VM** tab page, verify that only the CentOS VM is running on CNA01.

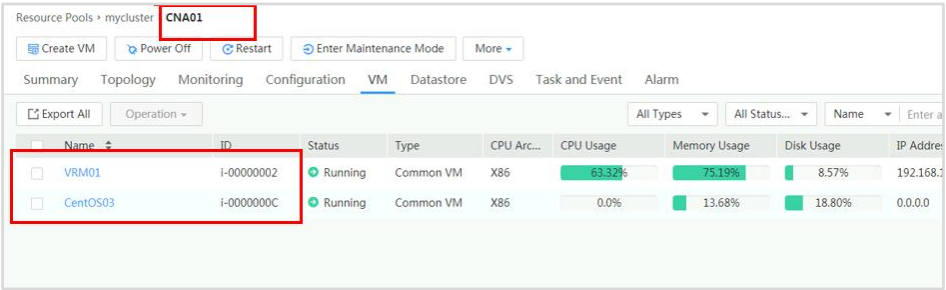


Figure 3-108 Viewing the VM running on CNA01

Step 8 Verify that the migrated VM is running on CNA02.

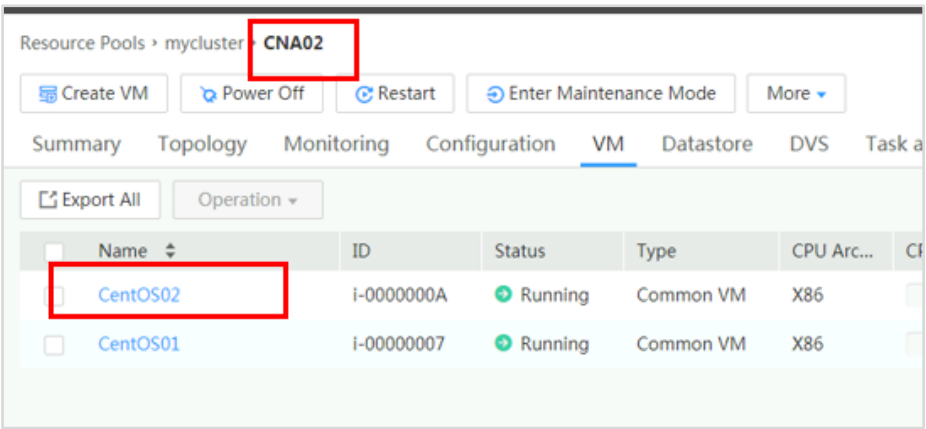


Figure 3-109 Viewing the VM running on CNA02

Step 9 Choose **Resource Pools** > **mycluster**. Click the **Configuration** tab. Choose **DRS Rule** > **Rule Group**. Click **Delete** in the **Operation** column of the row that contains **Mutually exclusive**. In the displayed dialog box, click **OK** to delete the **Mutually exclusive** rule group.

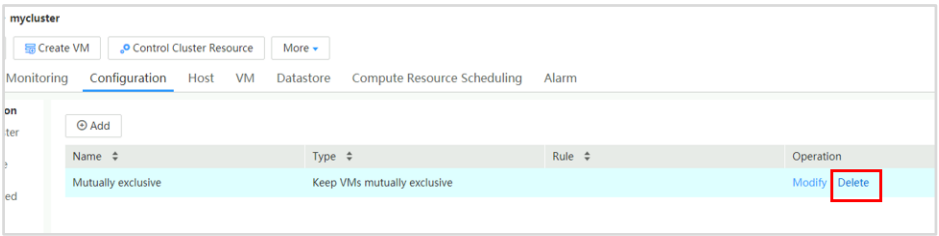


Figure 3-110 Deleting a rule group

3.2.6.3 Verifying the "Keep VMs together" Rule Group

Step 1 Choose **Resource Pools** > **mycluster**. Click the **Configuration** tab. Choose **DRS Rule** > **Rule Group**. Click **Add**.

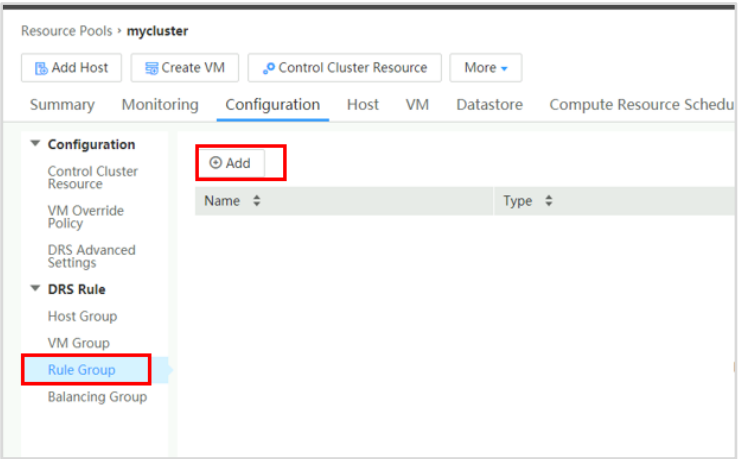


Figure 3-111 Adding a rule group

Step 2 Set **Name** to **together** and **Type** to **Keep VMs together**. Select **CentOS02** and **CentOS03**, and click **OK**.

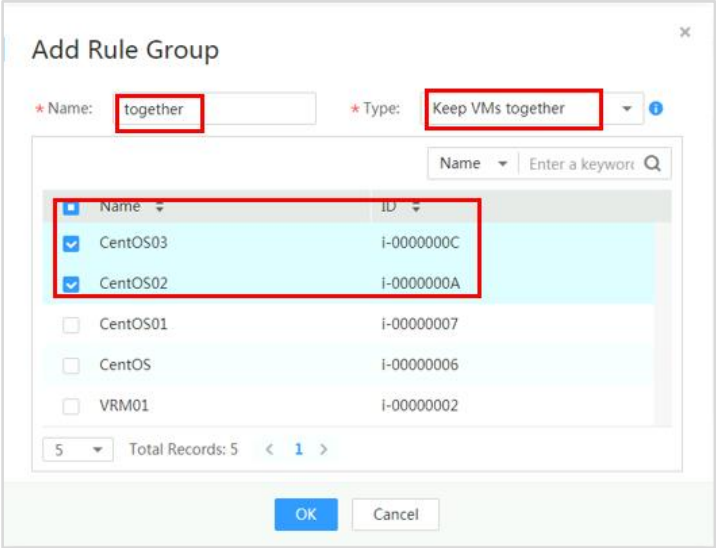


Figure 3-112 Configuring the "Keep VMs together" rule group

Step 3 Choose **System** > **Tasks and Logs** > **Task Center** and verify that a VM migration task is running. Click **Refresh** to refresh the progress.

Figure 3-113 Viewing the migration progress

Step 4 Wait until the migration is complete. Then you can view two CentOS VMs on the **VM** tab page of CNA01 or CNA02, indicating that the two VMs are running on the same host.

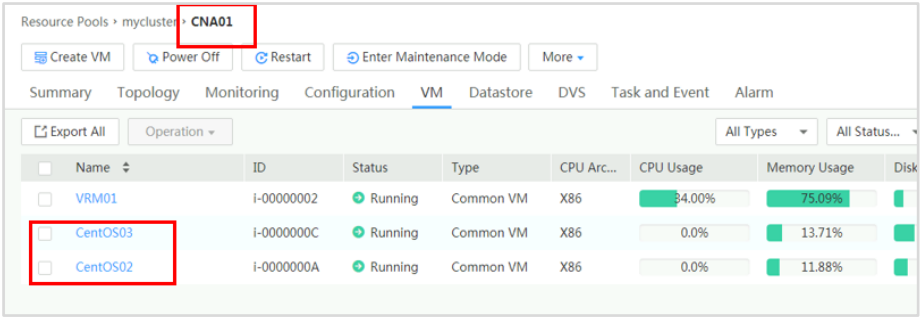


Figure 3-114 Verifying VMs running on CNA01

Step 5 Choose **Resource Pools** > **mycluster**. Click the **Configuration** tab. Choose **DRS Rule** > **Rule Group**. Click **Delete** in the **Operation** column of the row that contains **together**. In the displayed dialog box, click **OK** to delete the **together** rule group.

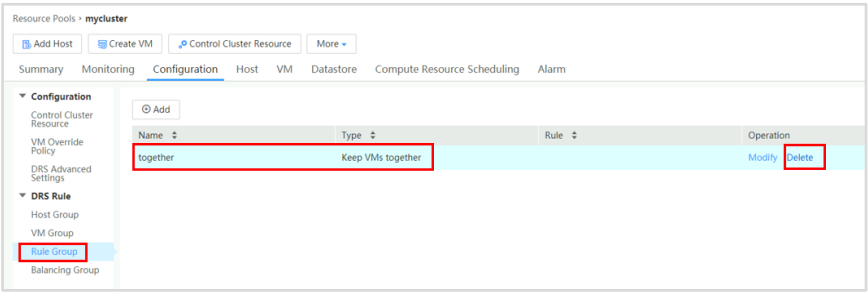


Figure 3-115 Deleting a rule group

3.2.6.4 Verifying the "VMs to hosts" Rule Group

Step 1 Choose **Resource Pools** > **mycluster**. Click the **Configuration** tab. Choose **DRS Rule** > **Host Group**. Click **Add**.

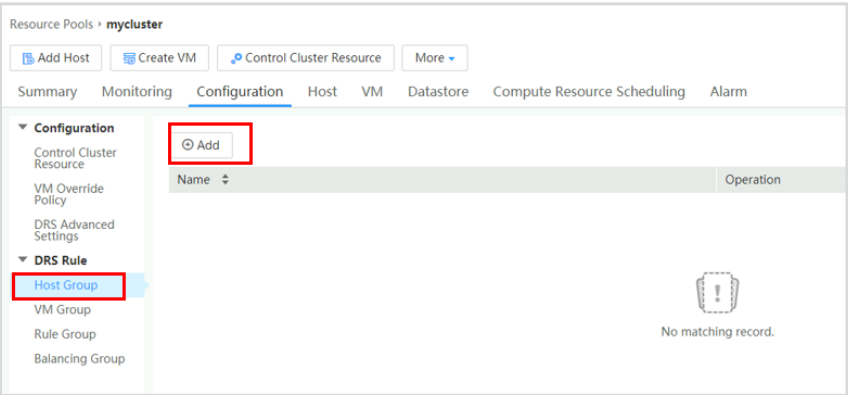


Figure 3-116 Add a host group

Step 2 Enter **hostgroup01** in the **Name** text box, select **CNA01**, and click **OK**.

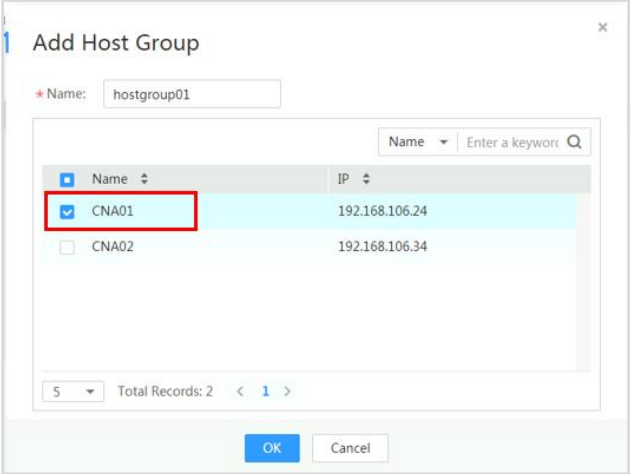


Figure 3-117 Selecting CNA01

Step 3 Choose **Resource Pools** > **mycluster**. Click the **Configuration** tab. Choose **DRS Rule** > **VM Group**. Click **Add**.

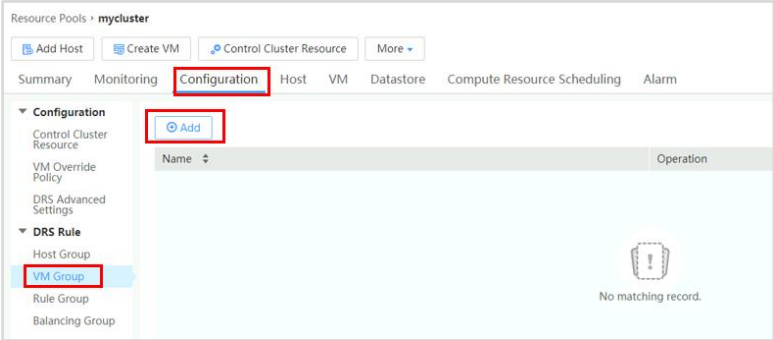


Figure 3-118 Adding a rule group

Step 4 Enter **vmgroup01** in the **Name** text box, select **CentOS02**, and click **OK**.

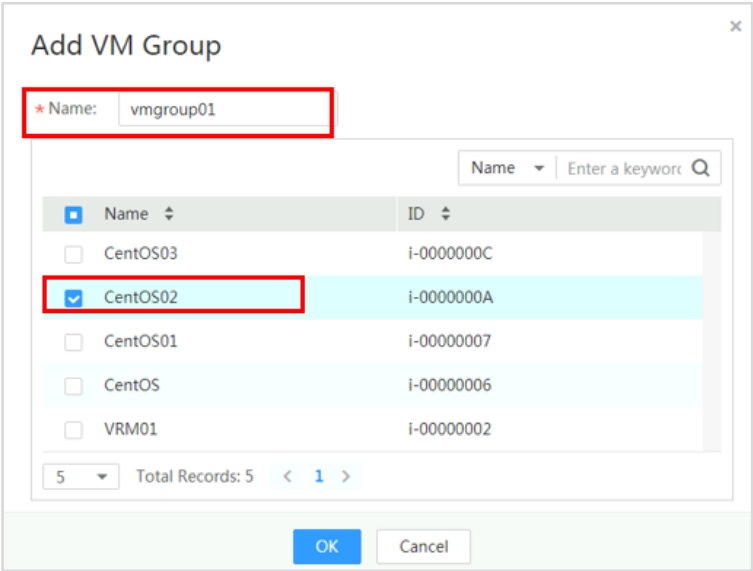


Figure 3-119 Adding a VM group

Step 5 Choose **Resource Pools** > **mycluster**. Click the **Configuration** tab. Choose **DRS Rule** > **Rule Group**. Click **Add**.

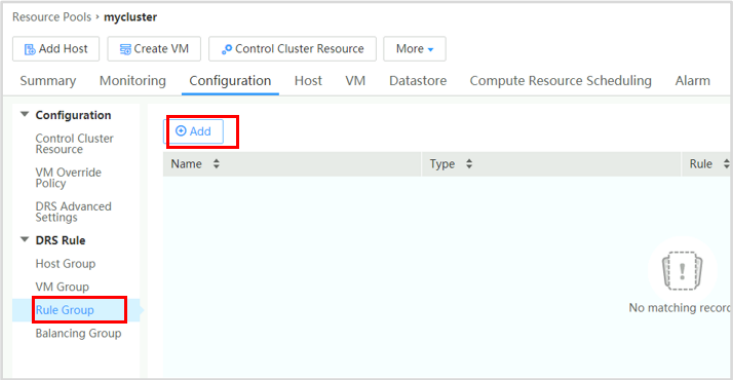


Figure 3-120 Adding a rule group

Step 6 Set **Name** to **v2h**, **Type** to **VMs to hosts**, and **Rule** to **Must not run on host group**. Select **vmgroup01** and **hostgroup01**, and click **OK**.

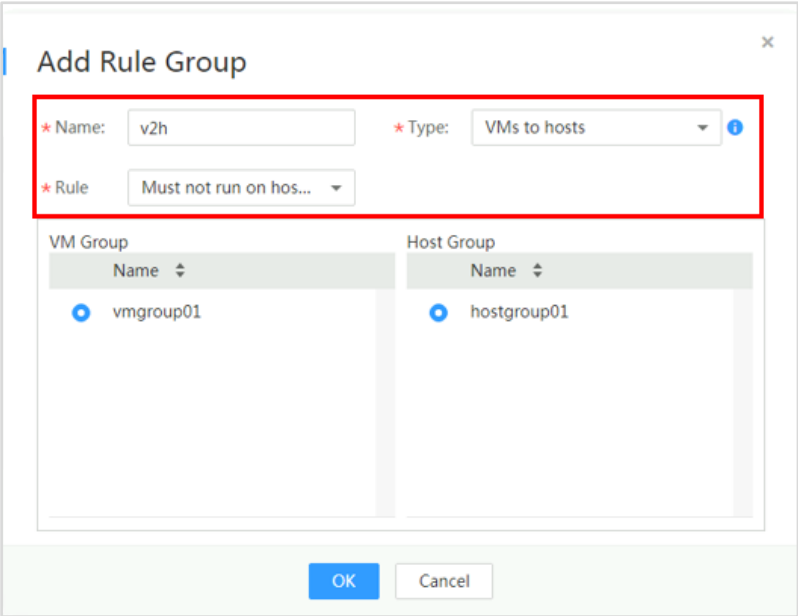


Figure 3-121 Configuring a "VMs to hosts" rule group

Step 7 Choose **System** > **Tasks and Logs** > **Task Center** and verify that a VM migration task is running. Click **Refresh** to refresh the progress.

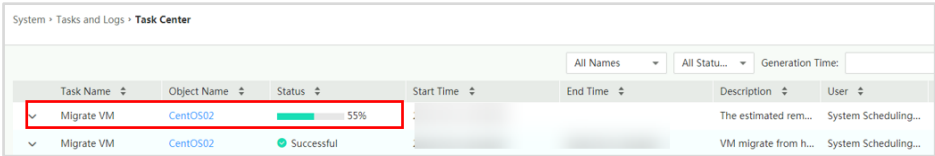


Figure 3-122 Viewing the migration progress

Step 8 Verify that the migrated VM is running on CNA02.

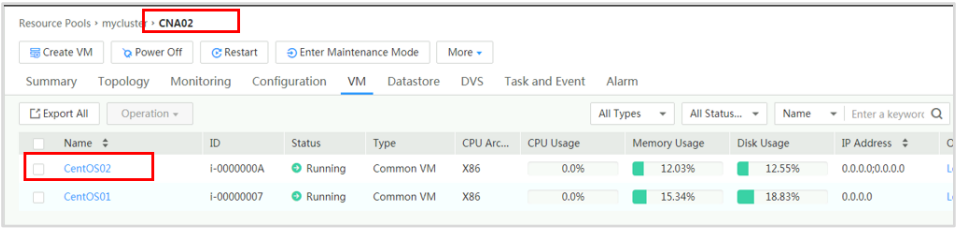


Figure 3-123 Verification

Step 9 Choose **Resource Pools** > **mycluster**. Click the **Configuration** tab. Choose **DRS Rule** > **Rule Group**. Click **Delete** in the **Operation** column of the row that contains **v2h**. In the displayed dialog box, click **OK** to delete the **v2h** rule group.

Step 10 Choose **Resource Pools** > **mycluster**. Click the **Configuration** tab. Choose **DRS Rule** > **VM Group**. Click **Delete** in the **Operation** column of the row that contains **vmgroup01**. In the displayed dialog box, click **OK** to delete the **vmgroup01** VM group.

Step 11 Choose **Resource Pools** > **mycluster**. Click the **Configuration** tab. Choose **DRS Rule** > **Host Group**. Click **Delete** in the **Operation** column of the row that contains **hostgroup01**. In the displayed dialog box, click **OK** to delete the **hostgroup01** host group.

3.2.7 Security Group Creation

Step 1 Log in to the CentOS02 and CentOS03 VMs using VNC, and set the eth0 IP addresses of the two VMs to **192.168.100.2/24** and **192.168.100.3/24**, respectively. (For details about the configuration method, see the Linux basics exercises.)

Step 2 Change the port group name of the CentOS03 VM to **test** by referring to section 3.2.2.2 "Configuring the VM Network." (The port group of the CentOS02 VM is also named **test**).

Step 3 Configure the physical service switch to allow packets from VLAN 100 to pass through. (For details, see the environment setup guide.)

Step 4 Log in to the CentOS03 VM using VNC and test the connectivity between CentOS03 and CentOS02.

```
[root@localhost ~]# ping 192.168.100.2
PING 192.168.100.2 (192.168.100.2) 56(84) bytes of data.
64 bytes from 192.168.100.2: icmp_seq=1 ttl=64 time=0.871 ms
64 bytes from 192.168.100.2: icmp_seq=2 ttl=64 time=0.260 ms
^C
```

Step 5 Choose **Resource Pools** > **Security Group**. Click **Add Security Group**.

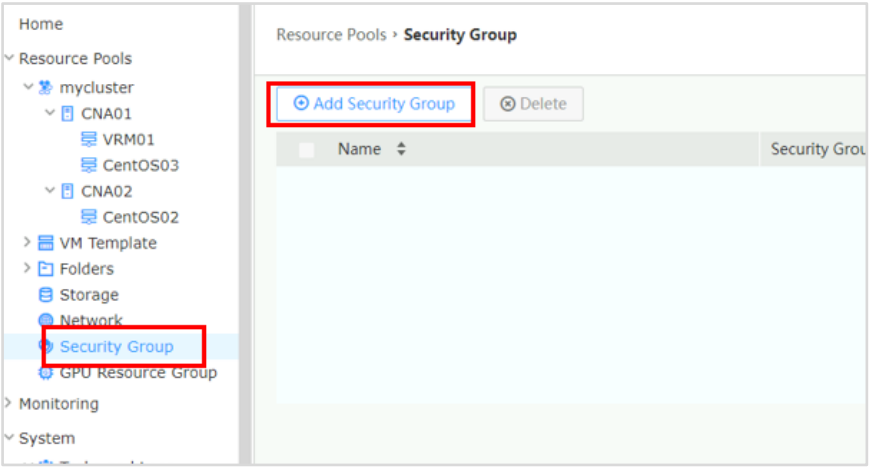


Figure 3-124 Adding a security group

Step 6 Set **Name** to **sec01** and **Security Group Type** to **Whitelist**, and click **OK**.

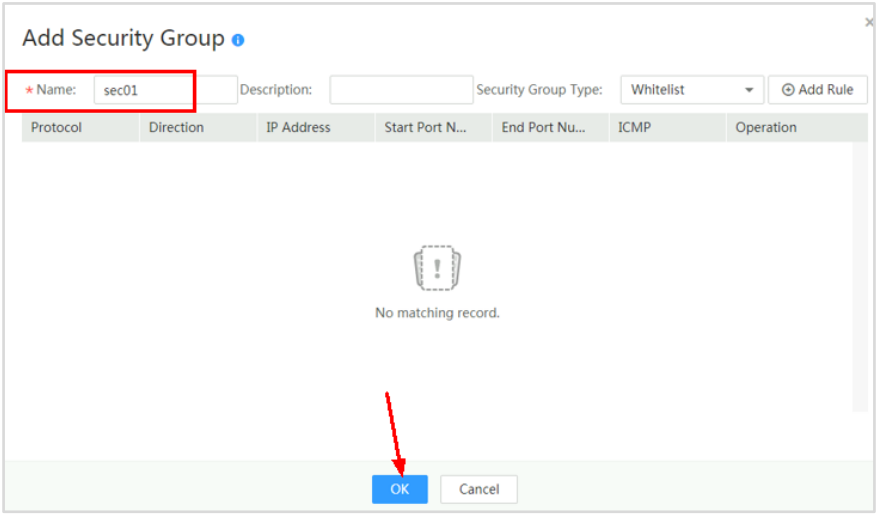


Figure 3-125 Configuring security group information

Step 7 After the security group is created, click **Add Rule** in the lower left corner of the security group management page.

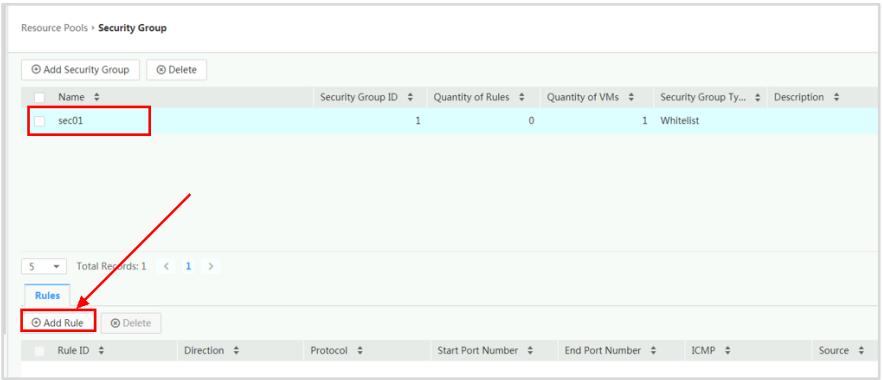


Figure 3-126 Adding rules

Step 8 Add the following rule and click **OK**. (Add this rule to enable the sec01 security group. If no rule is specified, the whitelist security group will allow all traffic.)

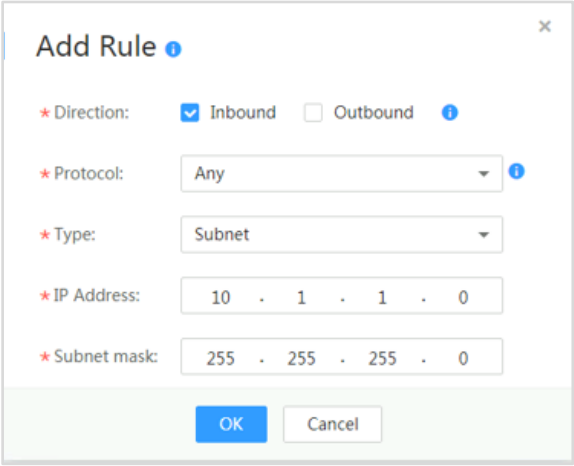


Figure 3-127 Configuring rule information

Step 9 Return to the CentOS02 VM management page and click **Stop** to stop the VM.

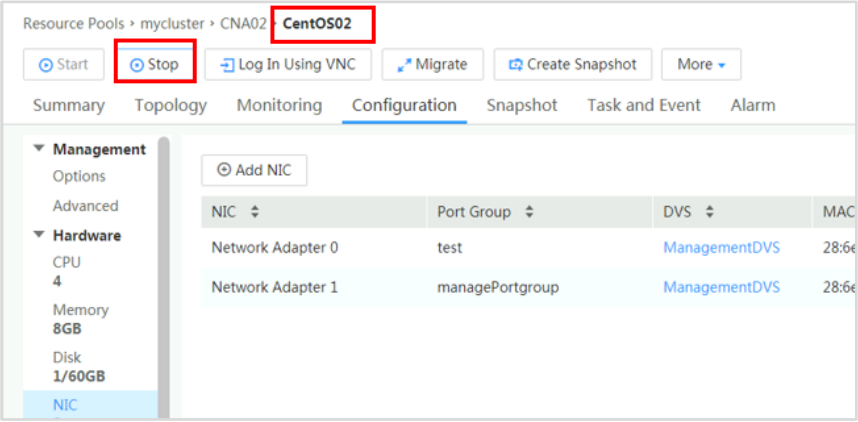


Figure 3-128 Stopping the CentOS02 VM

Step 10 After the VM is stopped, click the **Configuration** tab, and choose **Hardware** > **NIC**. Locate the row that contains **test**, click **More**, and choose **Configure Security Group**.

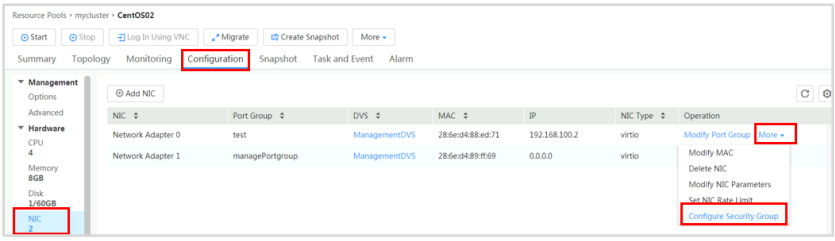


Figure 3-129 Configuring a security group

Step 11 Toggle on **Enable Security Group**, click **Select**, select the **sec01** security group, and click **OK**. In the **Configure Security Group** dialog box, click **OK**.

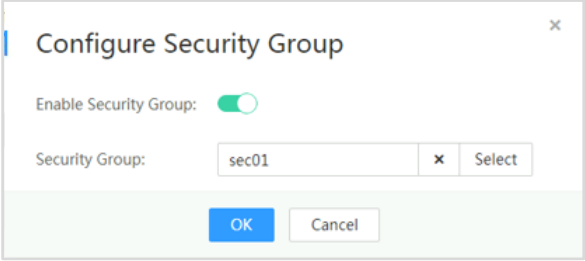


Figure 3-130 Selecting the sec01 security group

Step 12 Click **Start** to start the CentOS02 VM.

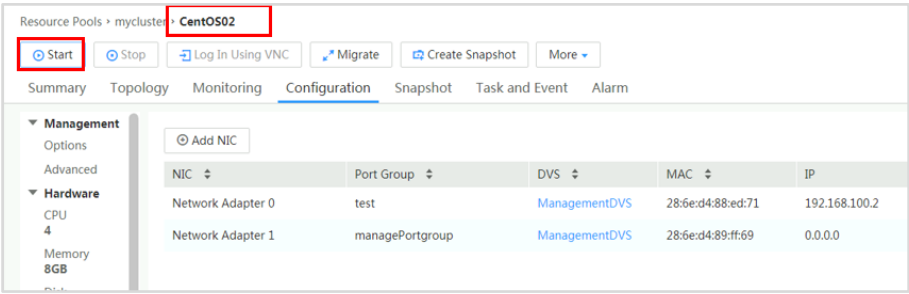


Figure 3-131 Starting a VM

Step 13 Log in to the CentOS03 VM using VNC and test the connectivity between CentOS03 and CentOS02 again.

```
[root@localhost ~]# ping 192.168.100.2
PING 192.168.100.2 (192.168.100.2) 56(84) bytes of data.
^C
--- 192.168.100.2 ping statistics ---
33 packets transmitted, 0 received, 100% packet loss, time 31999ms

[root@localhost ~]#
```

Figure 3-132 Testing connectivity

Step 14 Click **Add Rule** on the page of the sec01 security group.

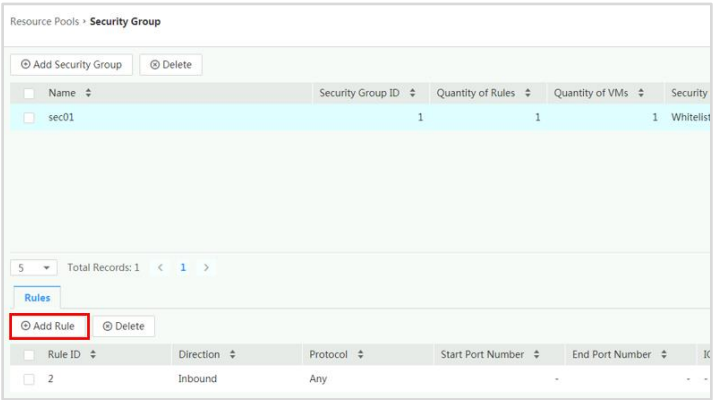


Figure 3-133 Adding another rule

Step 15 Set **Direction** to **Inbound**, **Protocol** to **ICMP**, **Type** to **Subnet**, **IP Address** to **192.168.100.0**, **Subnet mask** to **255.255.255.0**, **ICMP Type** to **Any**, and click **OK**. (You can change the values as required.)

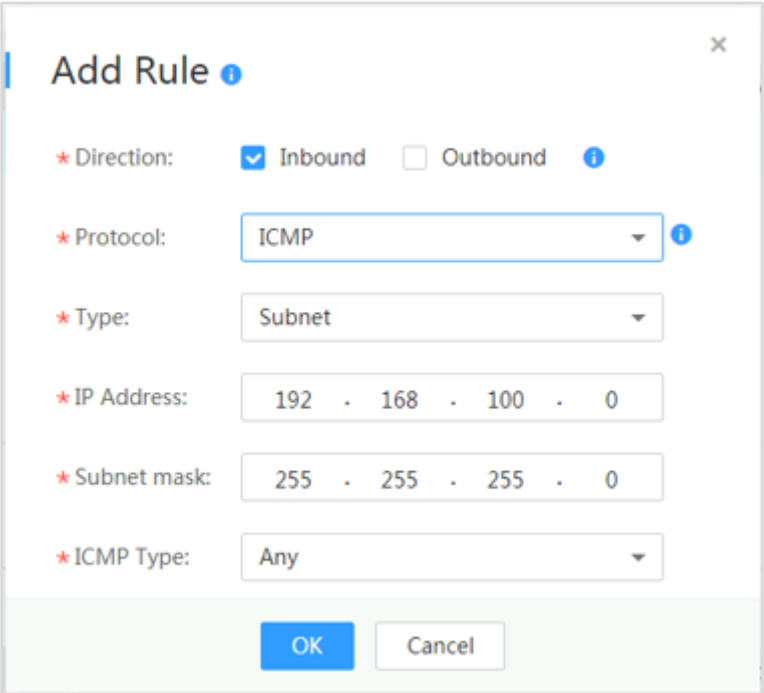


Figure 3-134 Configuring rule information

Step 16 After the security group is created, view information about the security group on the **Security Group** page.

Step 17 Log in to the CentOS03 VM using VNC and test the connectivity between CentOS03 and CentOS02 again.

```
[root@localhost ~]# ping 192.168.100.2
PING 192.168.100.2 (192.168.100.2) 56(84) bytes of data.
^C
--- 192.168.100.2 ping statistics ---
33 packets transmitted, 0 received, 100% packet loss, time 31999ms

[root@localhost ~]# ping 192.168.100.2
PING 192.168.100.2 (192.168.100.2) 56(84) bytes of data.
64 bytes from 192.168.100.2: icmp_seq=1 ttl=64 time=0.910 ms
64 bytes from 192.168.100.2: icmp_seq=2 ttl=64 time=0.246 ms
64 bytes from 192.168.100.2: icmp_seq=3 ttl=64 time=0.284 ms
64 bytes from 192.168.100.2: icmp_seq=4 ttl=64 time=0.241 ms
64 bytes from 192.168.100.2: icmp_seq=5 ttl=64 time=0.243 ms
^C
--- 192.168.100.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.241/0.384/0.910/0.264 ms
[root@localhost ~]#
```

Figure 3-135 Testing connectivity

3.2.8 VM HA

Step 1 Check the VMs on CNA02. As shown in the following figure, the CentOS02 VM exists on CNA02.

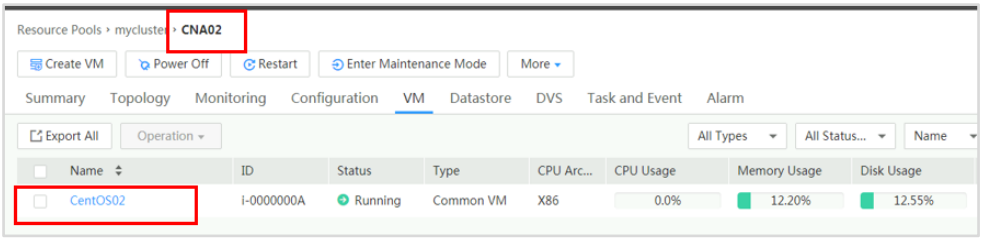


Figure 3-136 Checking the node where CentOS02 resides

Step 2 Choose **Resource Pools** > **mycluster**. Click the **Configuration** tab. Choose **Configuration** > **Control Cluster Resource**. Click **Edit**.

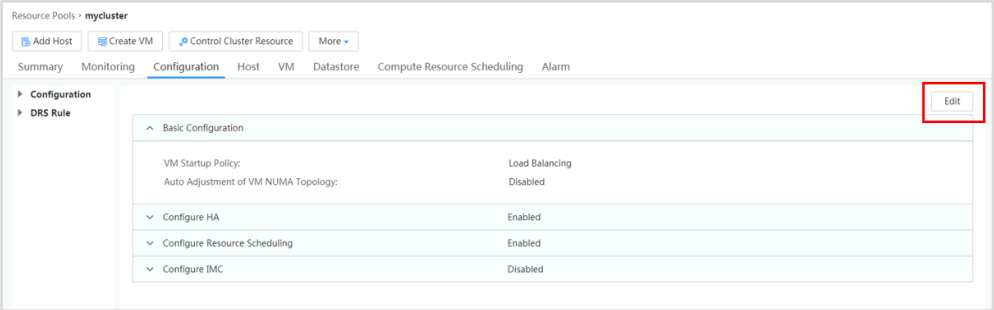


Figure 3-137 Editing cluster resource control

Step 3 In the **Control Cluster Resource** dialog box, choose **Configure HA** in the navigation pane. Toggle on **Enabled** to enable HA, toggle on **Host Fault Policies**, and set **Host Fault Policy** to **HA**.

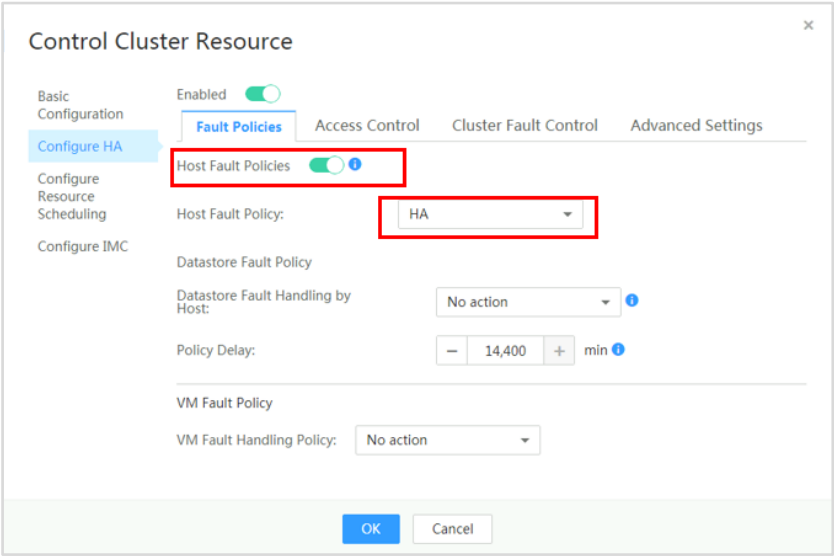


Figure 3-138 Configuring HA

Step 4 Click the **Cluster Fault Control** tab, toggle on **Enabled** to enable cluster fault control, and click **OK**.

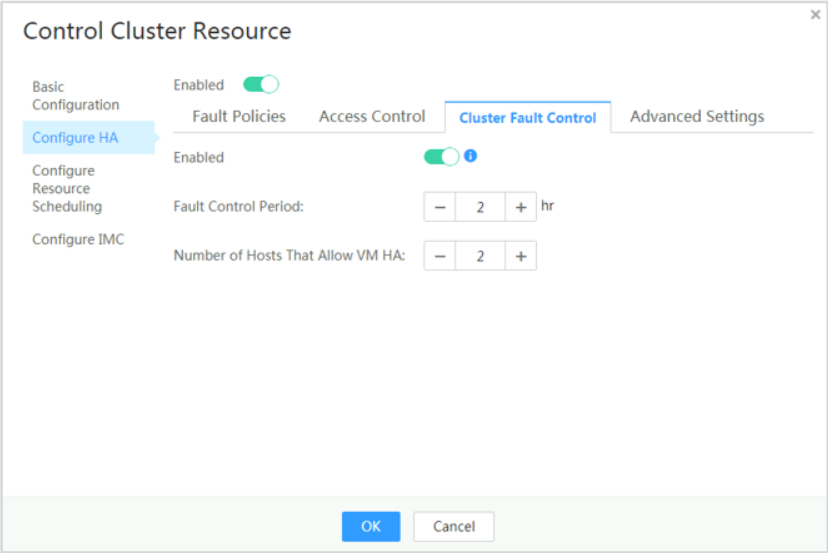


Figure 3-139 Enabling cluster fault control

Step 5 Power off the CNA02 host on the CNA02 management page to simulate a fault.

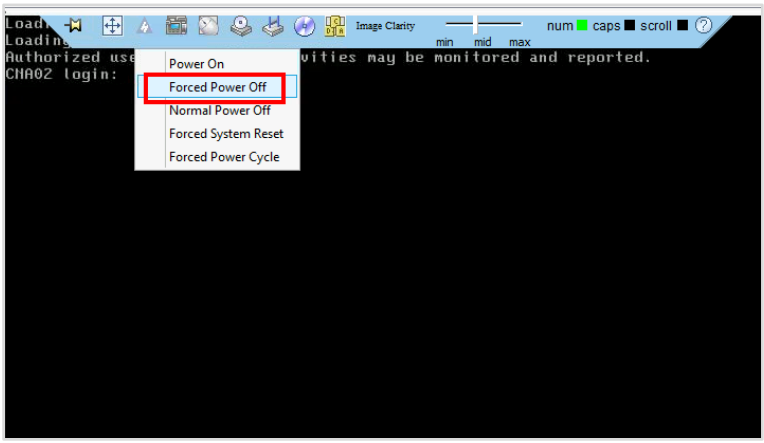


Figure 3-140 Forcibly powering off CNA02

Step 6 Choose **Resource Pools** > **mycluster**. On the **Host** tab page, verify that the CNA02 host is in **Faulty** state.

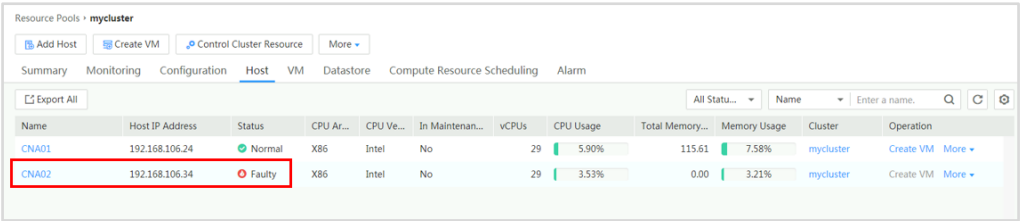


Figure 3-141 Viewing the status of CNA02

Step 7 Go to **Task Center** to view VM HA tasks.

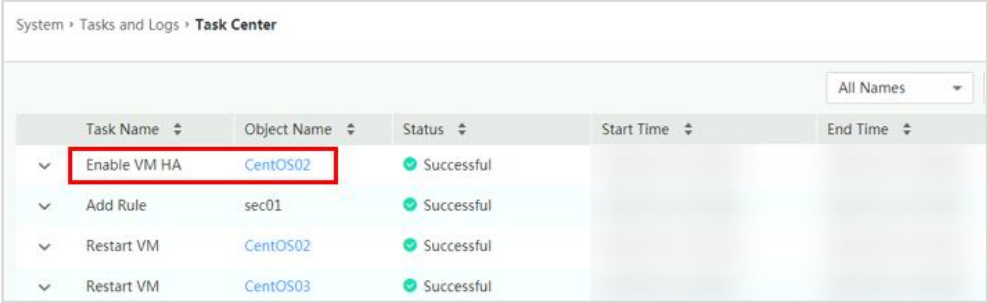


Figure 3-142 Viewing VM HA tasks

Step 8 Choose **Resource Pools** > **mycluster** > **CNA01**. Click the **VM** tab. On the **VM** tab page, verify that the CentOS02 VM is on the CNA01 host.

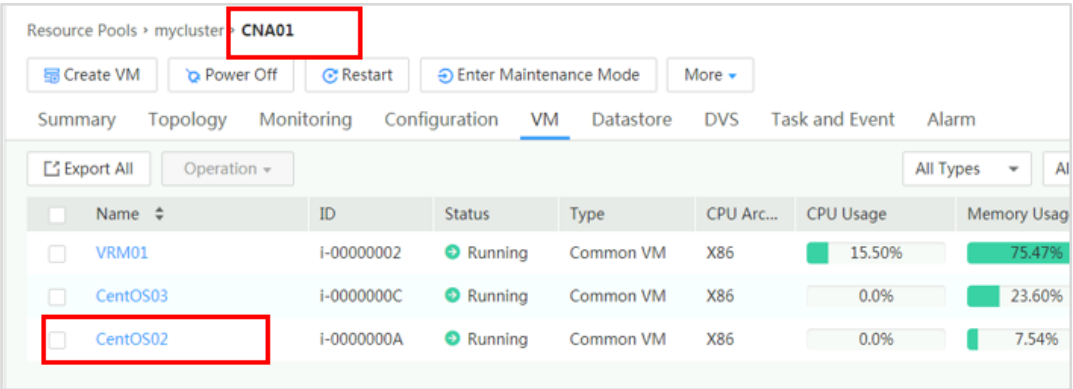


Figure 3-143 Checking the node where CentOS02 resides

Step 9 Power on the CNA02 host on the CNA02 management page.

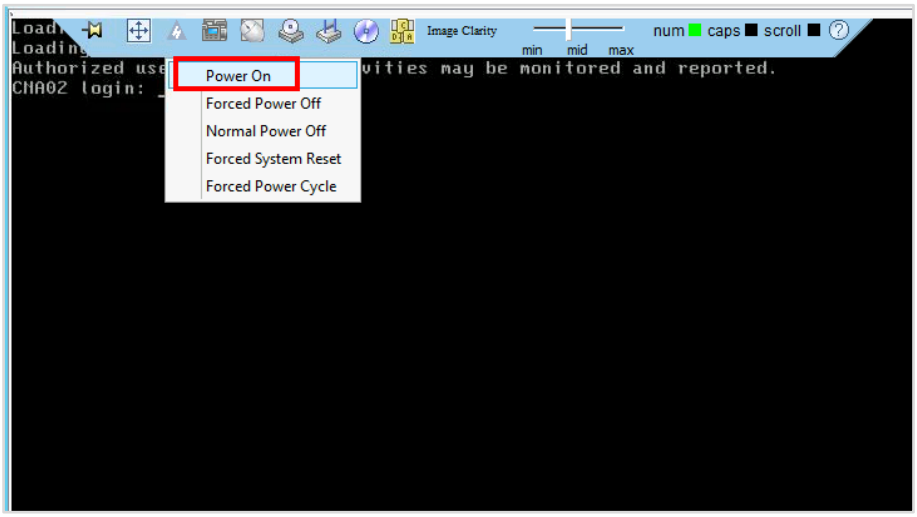


Figure 3-144 Powering on CNA02

3.3 Quiz

FusionCompute supports multiple VM creation methods, such as creating a VM using a template and creating a VM using a VM. What are the application scenarios of these two methods?

Answers:

If there is a proper template (with the same OS and hardware configurations as the VM to be created) in the system, you are advised to create the VM using the template. In this scenario, using the template can save your time.

4 Common O&M Management

4.1 Introduction

4.1.1 About This Exercise

This exercise illustrates how to manage the FusionCompute system, including loading license files, viewing alarms, configuring the system clock, and managing system permissions.

4.1.2 Objectives

- View the system ESN and load a license file.
- Manage system alarms.
- Configure the system clock.
- Configure system permissions.

4.1.3 Procedure

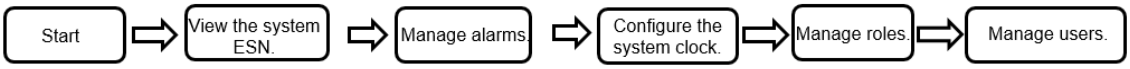


Figure 4-1 Procedure

4.2 Viewing the System ESN

The system has only a 90-day trial period because no license file is loaded. The system ESN is required for loading the license. This section only describes how to view the system ESN. For a commercial version, load the license.

Step 1 Choose **System** > **System Configuration** > **License Management**. Click **Load License File**.

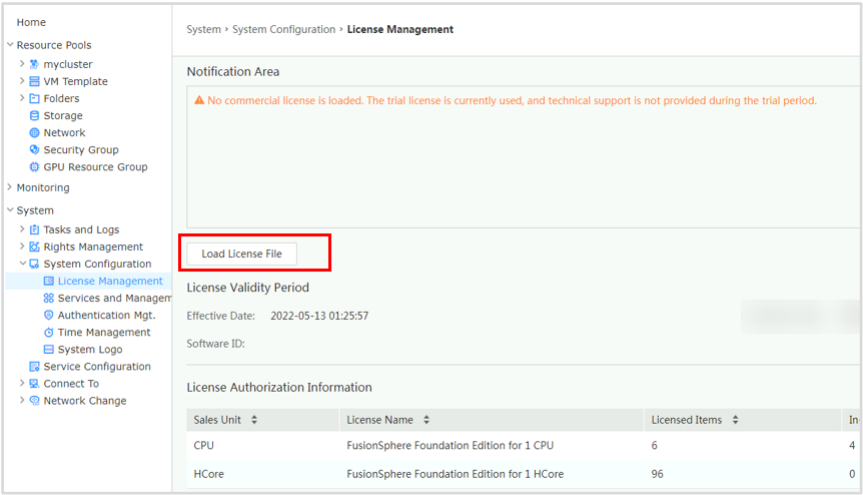


Figure 4-2 Clicking Load License File

Step 2 In the **Load License File** dialog box, select **Independent license** and click **Obtain ESN**. The ESN is displayed. Click **Cancel** to close the current dialog box. If a license file is available, click **Select**, select the license file, and click **OK** to load the commercial license.

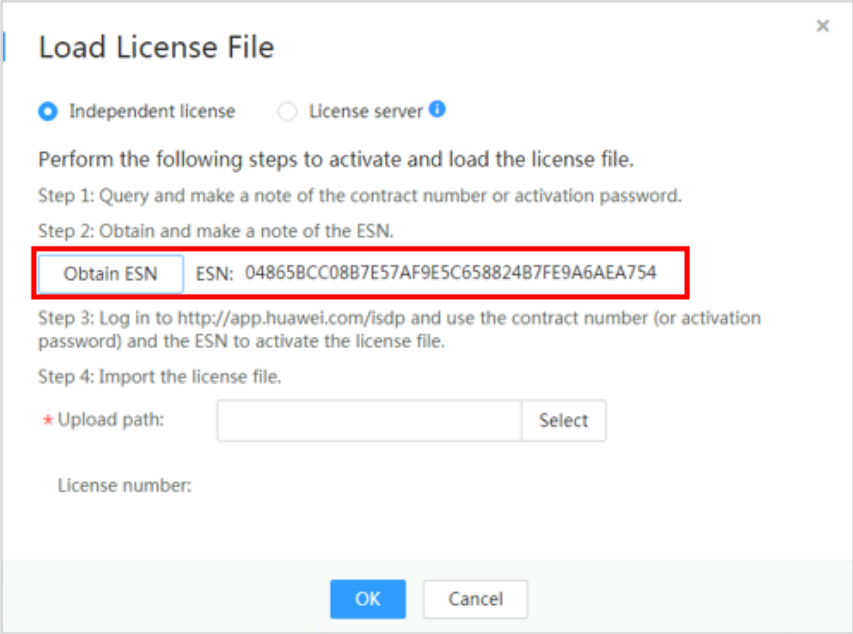


Figure 4-3 Loading a license

4.3 Managing Alarms

Step 1 Choose **Monitoring** > **Alarm** > **Alarms**. View alarm information such as **Alarm Severity**, **Alarm Name**, and **Alarm Object** of each alarm.

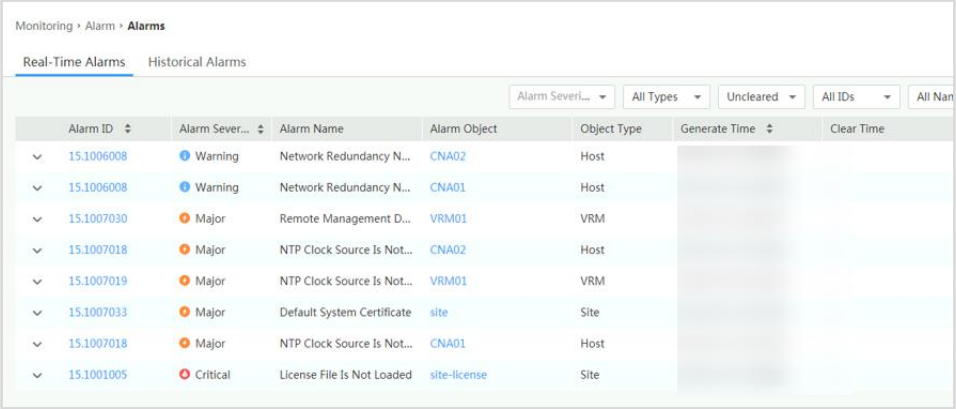


Figure 4-4 Viewing real-time alarms

Step 2 Click an alarm ID. A new page is displayed, showing the alarm description and handling procedure.

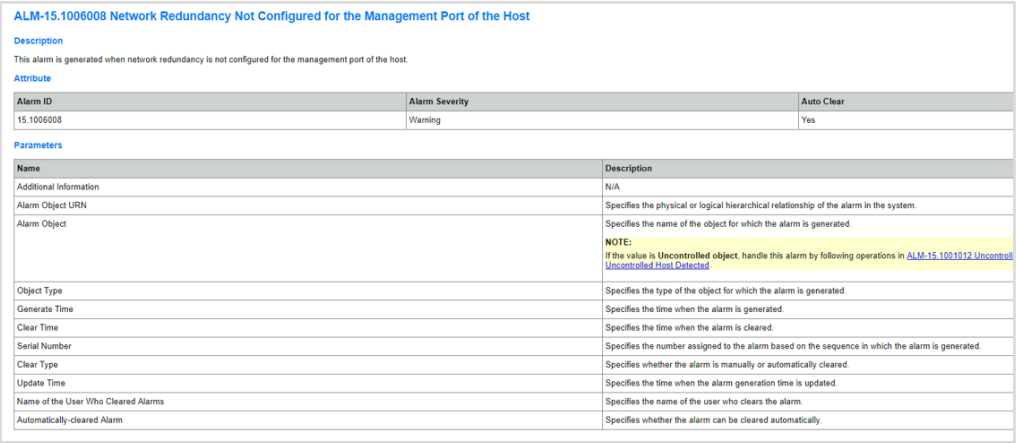


Figure 4-5 Alarm information

Step 3 Click **Clear** in the **Operation** column of the "License File Is Not Loaded" alarm. In the displayed dialog box, click **OK** to manually clear the alarm.

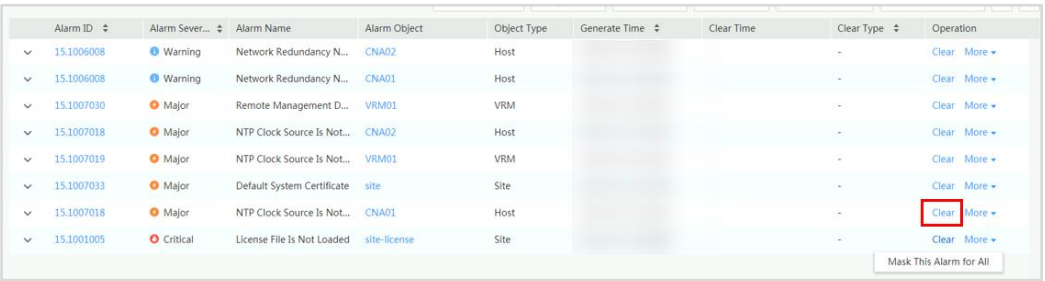


Figure 4-6 Manually clearing an alarm

Step 4 In the cleared alarms, locate the alarm named "License File Is Not Loaded", click **More** and choose **Mask This Alarm for All**. In the displayed dialog box, click **OK** to mask the alarm.

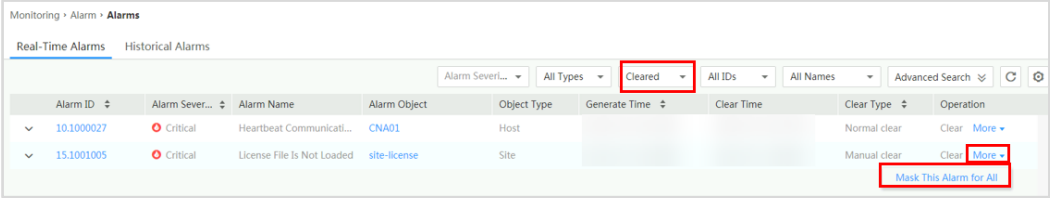


Figure 4-7 Masking an alarm

4.4 Configuring the System Clock

In a commercial environment, an NTP network clock must be configured to ensure consistent system clocks. This section uses CNA01 as the NTP server to demonstrate how to configure the time.

Step 1 Choose **System** > **System Configuration** > **Time Management**.

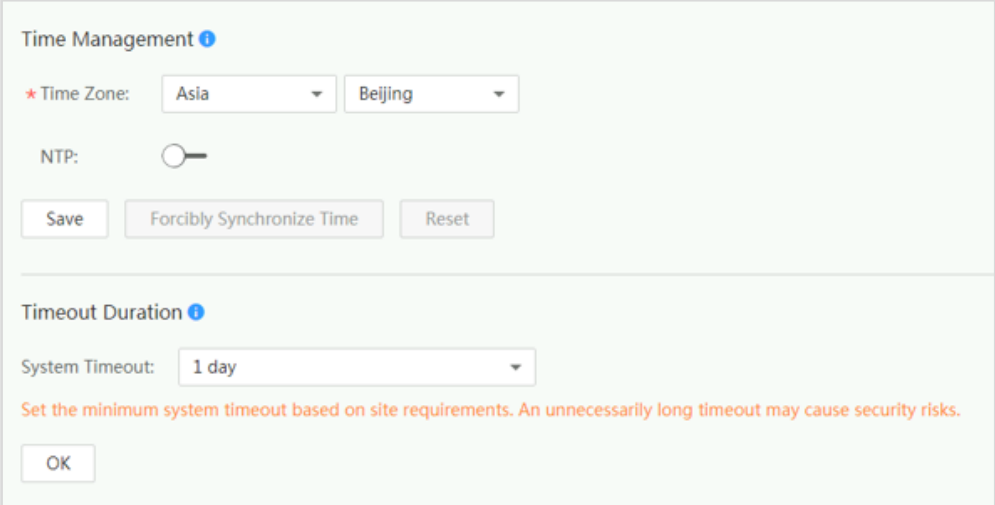


Figure 4-8 Time Management page

Step 2 Toggle on **NTP**, enter the IP address of the CNA01 node where VRM is located, and click **Save**. In the displayed dialog box, click **OK**. Wait until the system configuration is complete. If necessary, you can click **Forcibly Synchronize Time** to synchronize the time again. The system will stop for 1–2 minutes. Refresh the page until you can log in to FusionCompute.

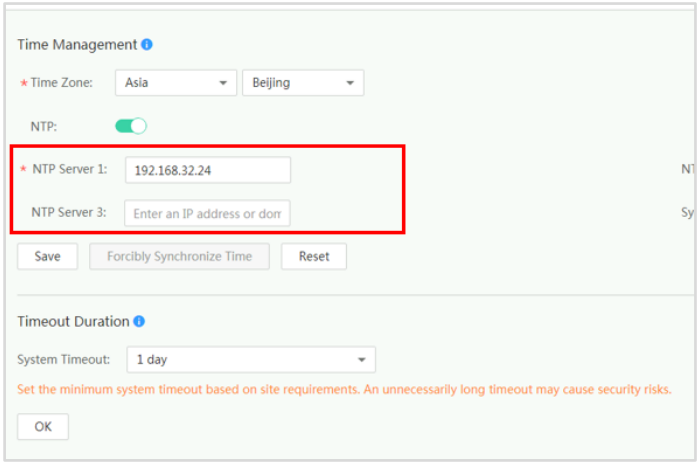


Figure 4-9 Configuring the clock server

4.5 Permission Management

4.5.1 Role Management

Step 1 If the default roles do not meet operation permission requirements, you can self-define a role and configure the required permissions for the role. Choose **System** > **Rights Management** > **Role Management**. On the **Role Management** page, view the permission list in the right pane.

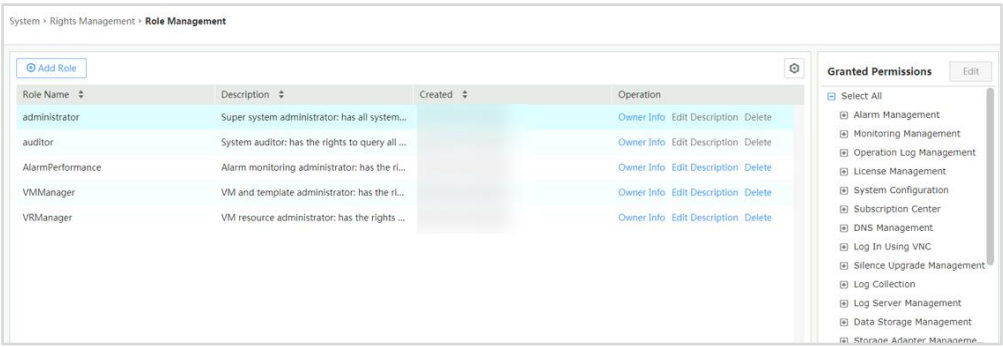


Figure 4-10 Permission management page

Step 2 Click **Add Role**. In the displayed dialog box, set **Role Name** to **vmmanager**, select **VM Management** for **Permission**, and click **OK**.

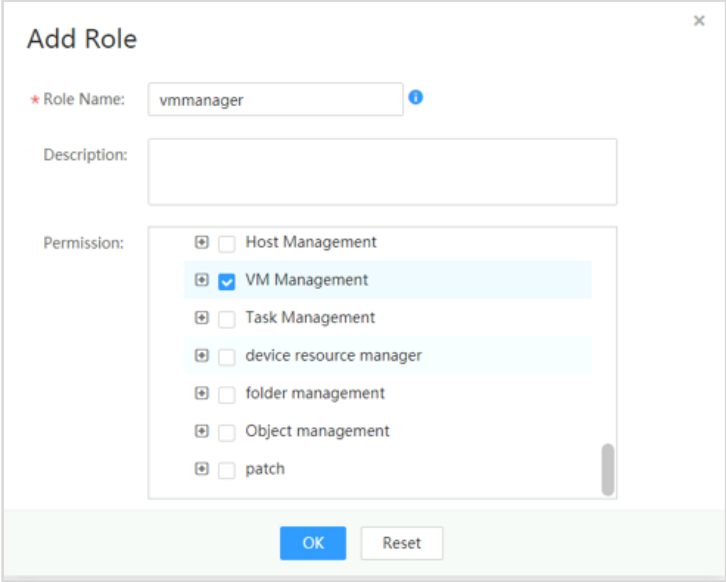


Figure 4-11 Adding a role

4.5.2 User Management

Step 1 FusionCompute allows you to create users and assign different roles to the users to meet different access control requirements. Choose **System** > **Rights Management** > **User Management**. Click **Add User**.

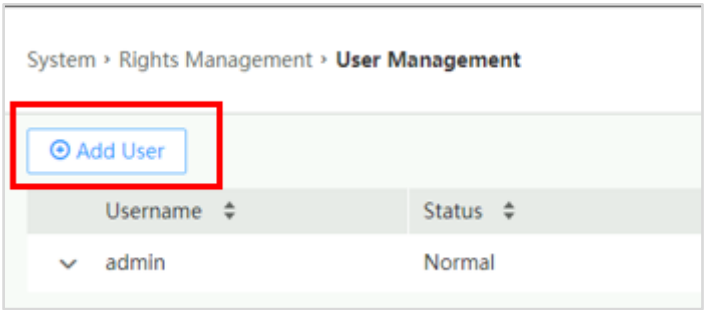


Figure 4-12 Adding a user

Step 2 In the **Add User** dialog box, set **User Type** to **Local user**, **Username** to **huawei**, **Password** to a customized string, and **Role** to **vmmanager**, set other parameters as required, and click **OK**.

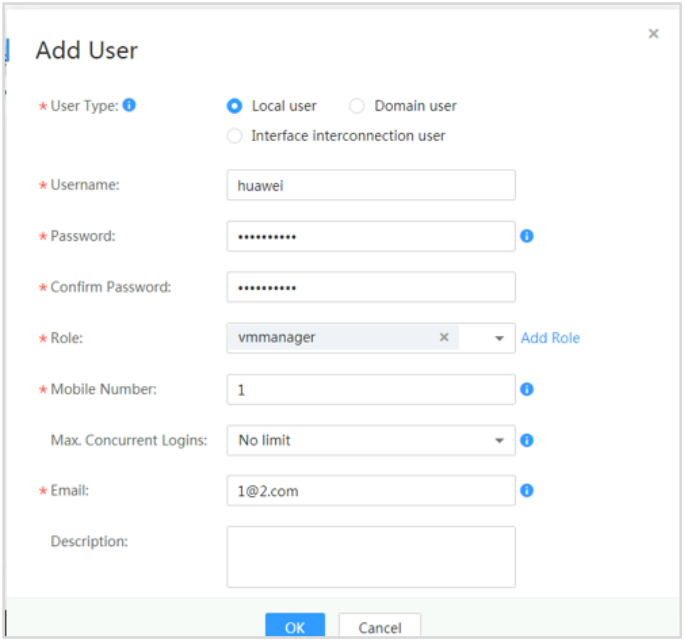


Figure 4-13 Configuring user information

Step 3 Log out of the current user and log in to the system as the **huawei** user. Change the password upon the first login.

4.5.3 Password Policy Management

Step 1 Log in to the system as the **admin** user and choose **System** > **Rights Management** > **Password Policy**. On the **Password Policy** page, view the password policy configuration of the system.

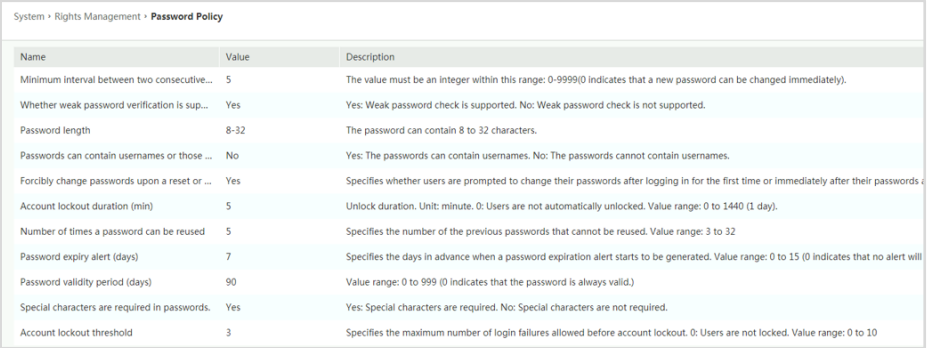


Figure 4-14 Password policy

Step 2 Click **Modify** in the lower left corner of the page. Set the parameters as follows: **Account lockout duration (min)** to **1**, **Number of times a password can be reused** to **3**, **Password expiry alert (days)** to **0**, **Password validity period (days)** to **0**, and **Account lockout threshold** to **1**. Click **Save**.

Name	Value	Description
Minimum interval between two consecutive...	5	The value must be an integer within this range: 0-9999(0 indicates that a new password can be changed immediately).
Local user passwords support weak passwo...	Yes	Yes: Weak password check is supported. No: Weak password check is not supported.
Password length	8-32	The password can contain 8 to 32 characters.
Passwords can contain usernames or those ...	No	Yes: The passwords can contain usernames. No: The passwords cannot contain usernames.
Forcibly change passwords upon a reset or ...	Yes	Specifies whether users are prompted to change their passwords after logging in for the first time or immediately after their passwords are reset.
Account lockout duration (min)	1	Unlock duration. Unit: minute. 0: Users are not automatically unlocked. Value range: 0 to 1440 (1 day).
Number of times a password can be reused	3	Specifies the number of the previous passwords that cannot be reused. Value range: 3 to 32
Password expiry alert (days)	0	Specifies the days in advance when a password expiration alert starts to be generated. Value range: 0 to 15 (0 indicates that no alert will be generated.)
Password validity period (days)	0	Value range: 0 to 999 (0 indicates that the password is always valid.)
Special characters are required in passwords.	Yes	Yes: Special characters are required. No: Special characters are not required.
Account lockout threshold	1	Specifies the maximum number of login failures allowed before account lockout. 0: Users are not locked. Value range: 0 to 10

Figure 4-15 Modifying a password policy

Step 3 Attempt to log in using an incorrect password.

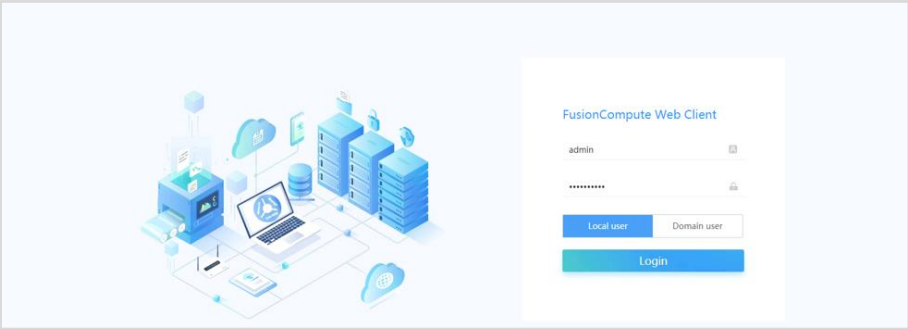


Figure 4-16 Test and verification 1

Step 4 Verify that the account is locked for 1 minute.

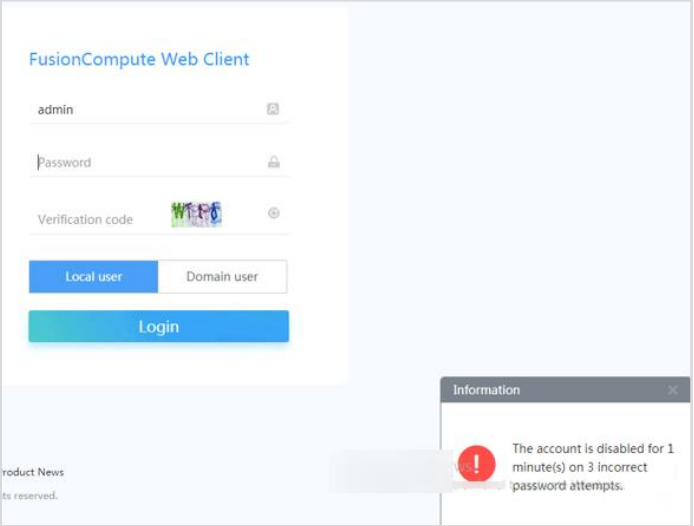


Figure 4-17 Test and verification 2

4.6 Quiz

What are the differences between major alarms and minor alarms on FusionCompute?

Answers:

A major alarm indicates a fault that affects the service at present, and if not rectified, could result in serious consequences. A minor alarm indicates a fault that does not affect the service at present, but if not rectified, could result in more severe faults.

Huawei Cloud Certification Training

HCIA-Cloud Computing

Lab Guide

(FusionAccess)

ISSUE: 5.0

HUAWEI TECHNOLOGIES CO., LTD

Copyright © Huawei Technologies Co., Ltd. 2022. All rights reserved.

No part of this document may be reproduced or transferred in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions

HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks or registered trademarks mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address:	Huawei Industrial Base, Bantian, Longgang, Shenzhen 518129 People's Republic of China
Website:	https://e.huawei.com

Huawei Certification System

The Huawei certification system is a platform for shared growth, part of a thriving partner ecosystem. There are two types of certification: one for ICT architectures and applications, and one for cloud services and platforms. There are three levels of certification available:

Huawei Certified ICT Associate (HCIA)

Huawei Certified ICT Professional (HCIP)

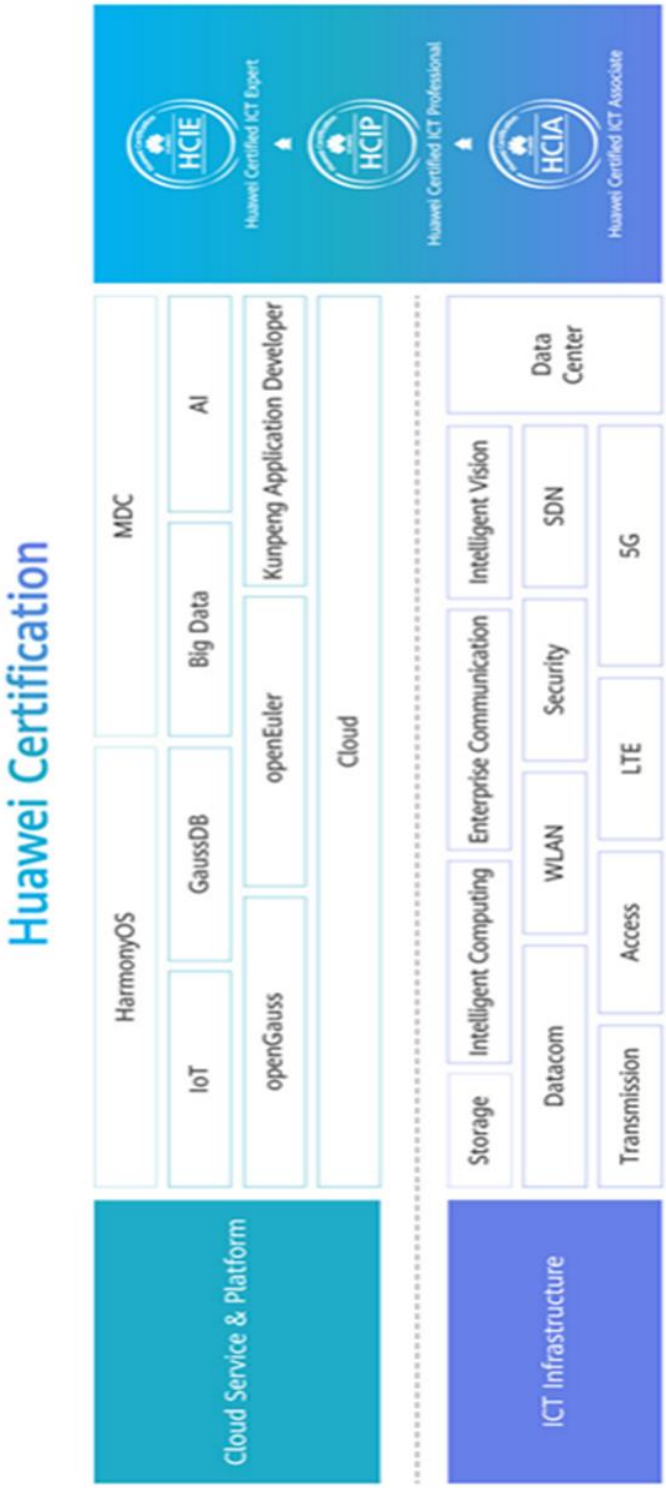
Huawei Certified ICT Expert (HCIE)

Huawei certification courses cover the entire ICT domain, with a focus on how today's architecture generates cloud-pipe-device synergy. The courses present the latest developments of all essential ICT aspects to foster a thriving ICT talent ecosystem for the digital age.

HCIA-Cloud Computing V5.0 is intended for beginners. Focusing on the virtualization technologies and FusionAccess of Huawei, this course aims to help you learn the basics of cloud computing and resource pooling, and to cultivate cloud computing engineers that are capable of using FusionCompute for virtualization and managing FusionAccess.

The HCIA-Cloud Computing V5.0 certification includes the following courses: basics of cloud computing (server, storage, network, and OS), overview of FusionCompute, routine management and troubleshooting of virtualization resource pools, overview of FusionAccess and related components, as well as their installation, deployment, service management, and troubleshooting.

Passing the HCIA-Cloud Computing V5.0 certification means that you are capable of designing, managing, and maintaining FusionCompute and FusionAccess.


Huawei Certification
Cloud Service & Platform
HarmonyOS
MDC
IoT
GaussDB
Big Data
AI
openGauss
openEuler
Kunpeng Application Developer
Cloud
ICT Infrastructure
Storage
Intelligent Computing
Enterprise Communication
Intelligent Vision
Datacom
WLAN
Security
SDN
Data Center
Transmission
Access
LTE
5G
HCIE
Huawei Certified ICT Expert
HCIP
Huawei Certified ICT Professional
HCIA
Huawei Certified ICT Associate

About This Document

Overview

This document is intended for trainees who are preparing for the HCIA-Cloud Computing V5.0 exam or those who want to understand and manage FusionAccess.

About the Exercises

This document introduces three exercises, including how to create bare VMs, install components, and perform service provisioning and O&M of virtual desktops.

- Exercise 1: FusionAccess component installation. In this exercise, you will learn how to create a bare VM on FusionCompute, install and configure the OS, install components on the VM, and set up FusionAccess that can be logged in to through the web. This exercise illustrates the logical networking, component functions, and installation process of virtual desktops.
- Exercise 2: FusionAccess service provisioning. In this exercise, you will learn how to create a VM user on the AD/DNS/DHCP server, create a VM template on FusionCompute (encapsulate the VM template using a Huawei dedicated tool), and configure the template, VM naming rule, and desktop group on FusionAccess, provision full copy desktops and linked clone desktops, log in to the vAG using a software client (SC), and connect to the provisioned desktops using the Huawei Desktop Protocol (HDP). Through this exercise, you will understand the virtual desktop provisioning process and the HDP, and can tell the difference between full copy and linked clone.
- Exercise 3: FusionAccess O&M and management. This exercise helps you learn about the virtual desktop O&M and troubleshooting in common O&M scenarios. This exercise consists of the following parts:
    - Service adjustment of virtual desktop VMs, such as modifying VM specifications, adding VM users, adding VMs, upgrading common desktops to VIP desktops, and unassigning virtual desktops or restoring virtual desktop assignment.
    - When a virtual desktop is faulty, users can use the self-service maintenance gateway (vAG) to rectify the fault.
    - FusionAccess also provides robust policy management functions. In this exercise, two common policies are used. The file redirection policy is used to control file transfer between clients and virtual desktops. The clipboard redirection policy is used to copy clipboard content (such as text and images) between clients and virtual desktops.
    - When a user uses a virtual desktop, the FusionAccess administrator can send notifications to the virtual desktop.

- The virtual desktop can be reclaimed once it is not used.

Background Knowledge Required

This course is a basic course of the Huawei certification system. To better understand this course, you should:

Have basic knowledge of the Linux OS, storage, network, and cloud computing, and be familiar with Huawei servers.

Lab Environment Overview

Scenarios

A training institution has deployed FusionCompute virtual environment resources as its infrastructure. Now it plans to optimize office work by using FusionAccess. The requirements are as follows: Some FusionAccess resources are used by teachers, and other FusionAccess resources are used by students in the classroom. Systems of the computers in the classroom are initialized each time after being shut down. As there are many students using computers, FusionAccess must be highly reliable. In addition, dedicated personnel are required to troubleshoot system problems.

Design

Based on the preceding requirements, the exercise is designed as follows:

1. The full copy desktop is used for trainers.
2. For trainees, the linked clone desktop is applied. The desktop group type is set to dynamic pool, and the desktop group VM behavior is set to support system restoration.
3. To improve system reliability and balance system resource usage, two ITA/GaussDB/HDC/WI/License/vAG/vLB nodes are deployed in active/standby mode, and the AD/DNS/DHCP nodes are deployed in standalone mode. The vLB implements load balancing when different users log in to the same WI, preventing overload caused by simultaneous login.

Networking Topology

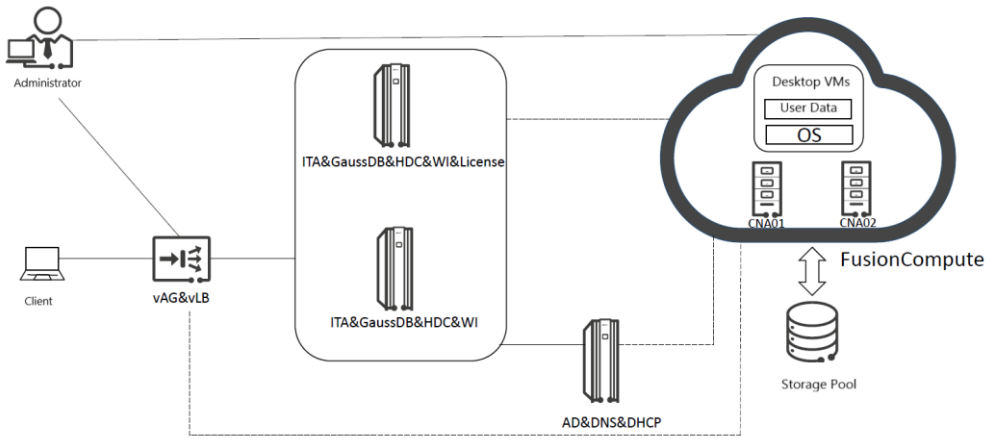


Figure 1-1 Networking diagram

Software and Tools

You need to install and use FusionAccess 8.0.2 in this exercise. You will need to use the following tools:

Table 1-1 Software and tools

Software	Description	How to Obtain
ADDNSDHCP_Template.ovf	AD/DNS/DHCP server template	The creation process is provided in the setup guide.
FusionAccess_Manager_Installer_8.0.2-x86_64.iso	FusionAccess installation software package (Linux OS component installation software)	https://support.huawei.com/enterprise/en/cloud-computing/fusionaccess-pid-19917528/software/251807361?idAbsPath=fixnode01%7C22658044%7C7919788%7C9856606%7C250416237%7C19917528
FusionAccess_WindowsDesktop_Installer_8.0.2.iso	FusionAccess installation software package (Windows OS component installation software)	
cn_windows_10_multiple_editions_x86_dvd_6846431.iso	Image files required for creating virtual desktops (Windows 10 images of different versions can be prepared as required.)	/
Putty	Used to log in to the Linux OS in SSH mode	/

VM Specifications

Table 1-2 VM specifications

VM Name	Specifications	NIC
FA-ADDNSDHCP	4-core/4 GB memory/50 GB hard disk (system disk)	NIC 1: service port group, for example, FA_Service_Portgroup
FA-ITADBHDCWILIcvAGvLB-01	8-core/16 GB memory/60 GB hard disk (system disk)	NIC 1: service port group, for example, FA_Service_Portgroup
FA-ITADBHDCWILIcvAGvLB-02	8-core/16 GB memory/60 GB hard disk (system disk)	NIC 1: service port group, for example, FA_Service_Portgroup

VM IP Address and VLAN Planning

- The actual network environment prevails.

Table 1-3 VM IP address and VLAN planning

VM Name	NIC	IP Address	VLAN	Gateway
FA-AD/DNS/DHCP	FA_Service_Portgroup	192.168.105.20/24	105	192.168.105.254
FA-ITADBHDCWILIvAGvLB-01 (active)	FA_Service_Portgroup	192.168.105.11/24 192.168.105.10/24 (floating IP address)	105	192.168.105.254
FA-ITADBHDCWIvAGvLB-02	FA_Service_Portgroup	192.168.105.12/24	105	192.168.105.254

FusionAccess Account List

Table 1-4 FusionAccess account list

Category	Account Description	Default Account
Linux infrastructure VM OS account	Linux server **root** account: used to install the programs for each component (excluding GaussDB). The account does not support	Username: **root** Password: For details, see "Note".

Category	Account Description	Default Account
	Secure Shell (SSH) login.	
	Linux server local common account.	Username: **gandalf** Password: For details, see "Note".
Password of the HA root certificate	Password of the HA root certificate	See "Note".
FusionAccess account	Default account of the FusionAccess Portal in common mode	Username: **admin** Password: For details, see "Note".
FusionCompute account	Northbound interface (NBI) account for interconnecting FusionCompute with FusionAccess	Username: **vdisysman** Password: user-defined. You are advised to set it to **VdiEnginE@234**.

Note: For details about the account and password, see FusionAccess Account List.

Contents

About This Document 3
Overview 3
About the Exercises 3
Background Knowledge Required 4
Lab Environment Overview 4
1 FusionAccess Component Installation 10
1.1 Overview 10
1.1.1 About This Exercise 10
1.1.2 Objectives 10
1.1.3 Procedure 10
1.2 Exercise Configuration 10
1.2.1 Creating a FusionAccess Port Group 10
1.2.2 Importing an AD/DNS/DHCP Server Template 12
1.2.3 Creating a Bare VM 16
1.2.4 Configuring Automatic Recovery for a VM 23
1.2.5 Installing an OS on the Bare VM 26
1.2.6 Installing FusionAccess Components 33
1.2.7 Modifying the Timestamp Configuration 40
1.2.8 Adding a System Account for Interconnecting with FusionAccess on FusionCompute 41
1.2.9 Completing the Configuration 43
1.3 Quiz 49
2 FusionAccess Service Provisioning 50
2.1 Overview 50
2.1.1 About This Exercise 50
2.1.2 Objectives 50
2.1.3 Procedure 50
2.2 Exercise Configuration 51
2.2.1 Creating a VM User 51
2.2.2 Creating a VM Template 58
2.2.3 Provisioning a Desktop 102
2.2.4 Logging In to a Desktop Using an SC 123
2.3 Quiz 125
3 FusionAccess O&M and Management 127
3.1 Overview 127

3.1.1 About This Exercise 127
3.1.2 Objectives 127
3.1.3 Procedure 127
3.2 Exercise Configuration 128
3.2.1 Policy Management 128
3.2.2 Service Adjustment 137
3.2.3 Viewing and Handling Alarms 156
3.3 Quiz 158

1 FusionAccess Component Installation

1.1 Overview

1.1.1 About This Exercise

This section describes how to create and configure bare Linux infrastructure VMs, install ITA/GaussDB/HDC/WI/License and vAG/vLB components on the VMs, and log in to FusionAccess using the web page when the AD, DNS, and DHCP servers are specified, complete initial configurations, such as interconnection between FusionAccess and FusionCompute and between FusionAccess and the AD/DNS/DHCP server.

1.1.2 Objectives

Upon completion of this exercise, you will understand:

- Functions of the ITA, GaussDB, HDC, WI, and License
- Functions of the vAG and vLB
- Installation and configuration processes of each component
- Initial configuration process of FusionAccess components
- Parameter settings for interconnecting FusionAccess with FusionCompute
- Parameter settings for interconnecting FusionAccess with the AD/DNS/DHCP server

1.1.3 Procedure

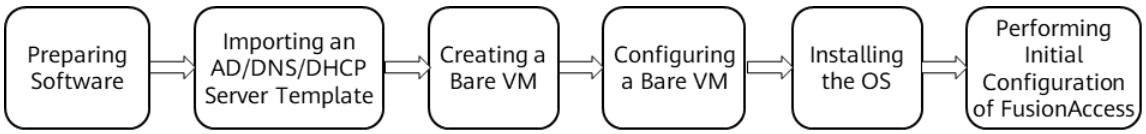


Figure 1-1 Flowchart

1.2 Exercise Configuration

1.2.1 Creating a FusionAccess Port Group

- If the FusionAccess port group has been created before the experiment, skip this step.

Step 1 Log in to FusionCompute and view DVS information.

- On FusionCompute, go to the **Resource Pools** page. Choose **Resource Pools** > **Network**, and click the distributed virtual switch (DVS). The DVS details are displayed in the lower part of the page.

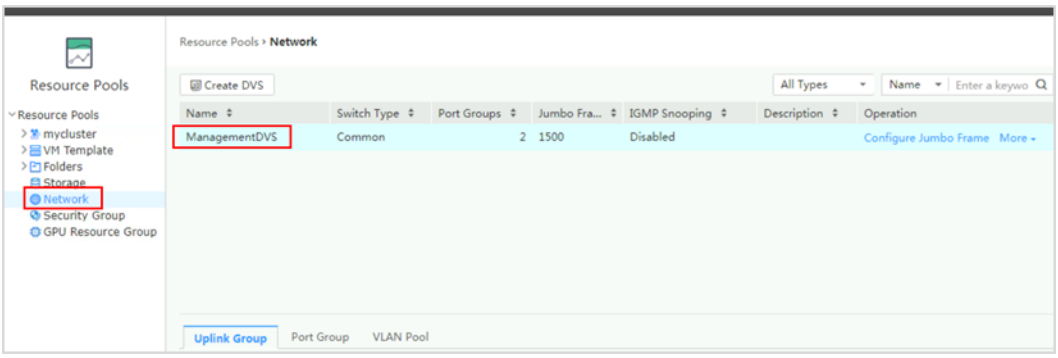


Figure 1-2 Viewing a DVS

Step 2 On the **VLAN Pool** tab page, click **Add**. Specify the start and end VLAN IDs.

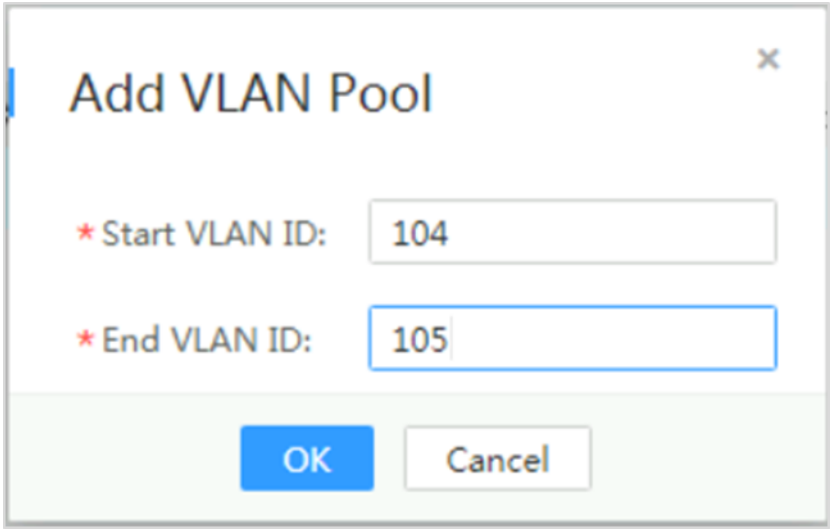


Figure 1-3 Adding a VLAN pool

Step 3 Click **OK**.

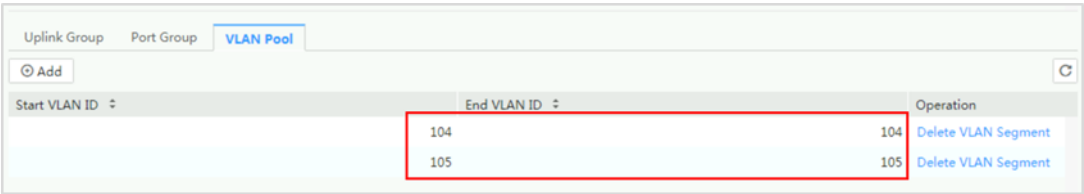


Figure 1-4 VLAN pool added

Step 4 Create the FusionAccess service port group **FA_Service_Portgroup**.

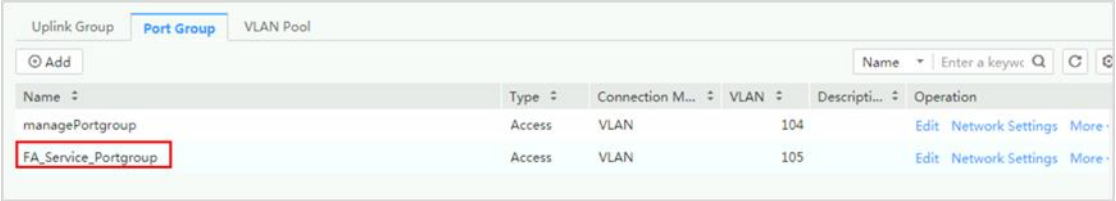


Figure 1-5 Adding a port group

1.2.2 Importing an AD/DNS/DHCP Server Template

Step 1 Log in to FusionCompute, right-click **Resource Pools**, and choose **Import** > **Import Template**. The **Create Template** dialog box is displayed.

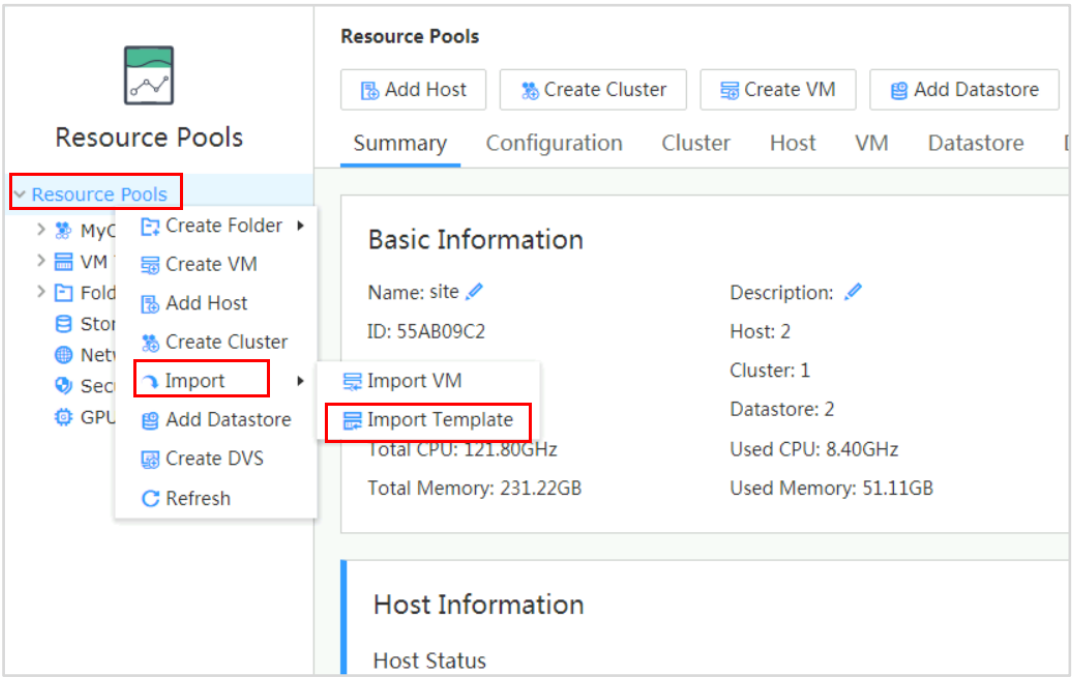


Figure 1-6 Importing a template

Step 2 Select **Import from Local PC**, select the path where the AD/DNS/DHCP server template (OVF template file) is stored, and click **Next**.

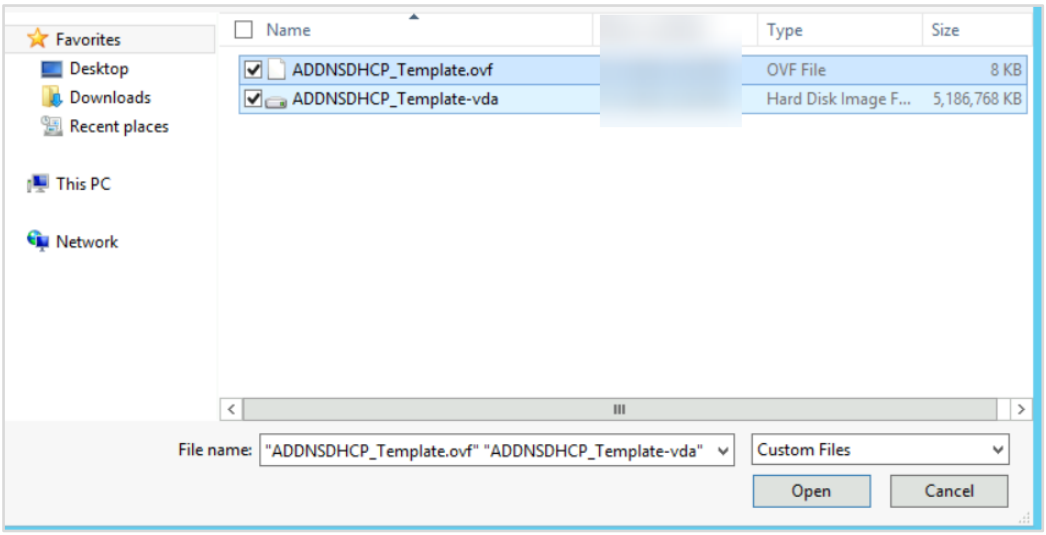


Figure 1-7 Selecting a template file

Note:

The AD/DNS/DHCP server template is created in the environment setup guide. The trainer creates and provides the template for trainees.

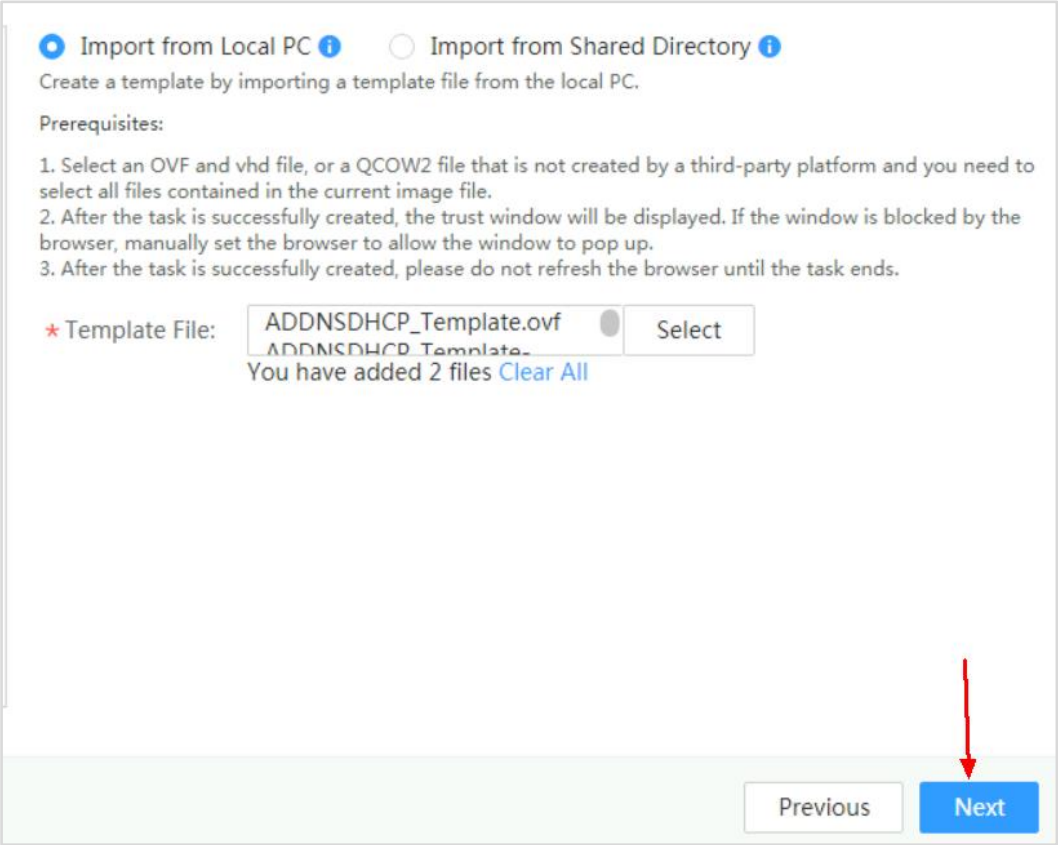


Figure 1-8 Confirming the template to be imported

Step 3 Set Name to FA-ADDNSDHCP, Select Template Location to site, and Set Compute Resource to MyCluster, and click **Next**.

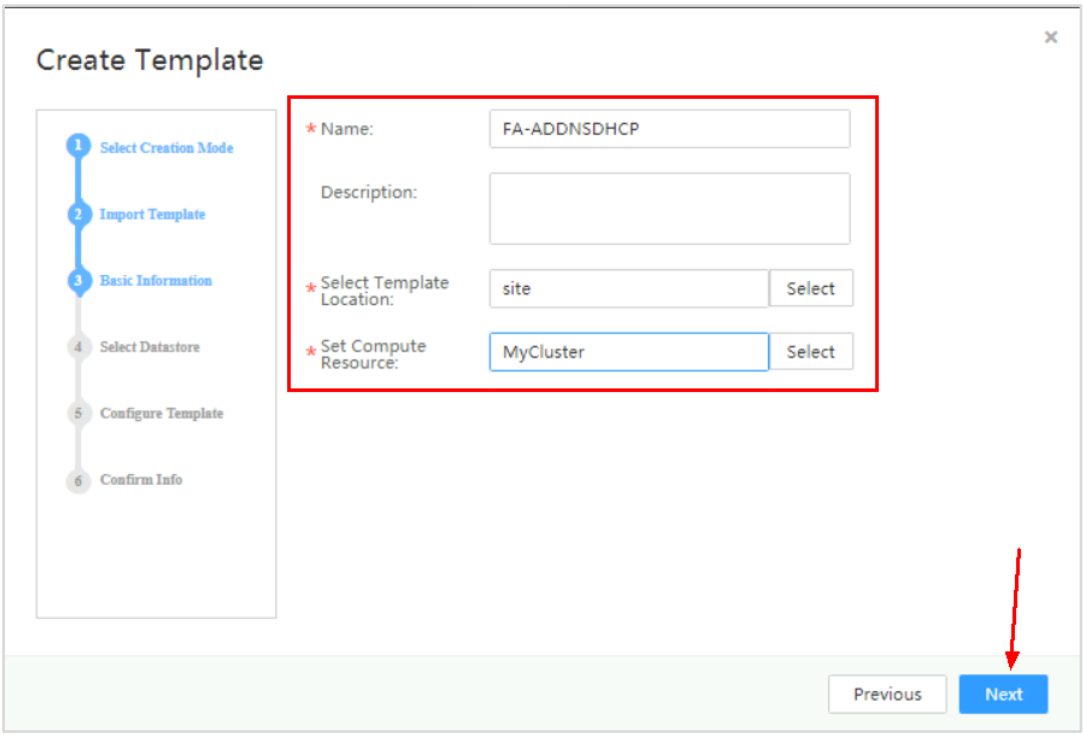


Figure 1-9 Basic information

Step 4 Select the datastore named **autoDS_CNA01** and click **Next**.

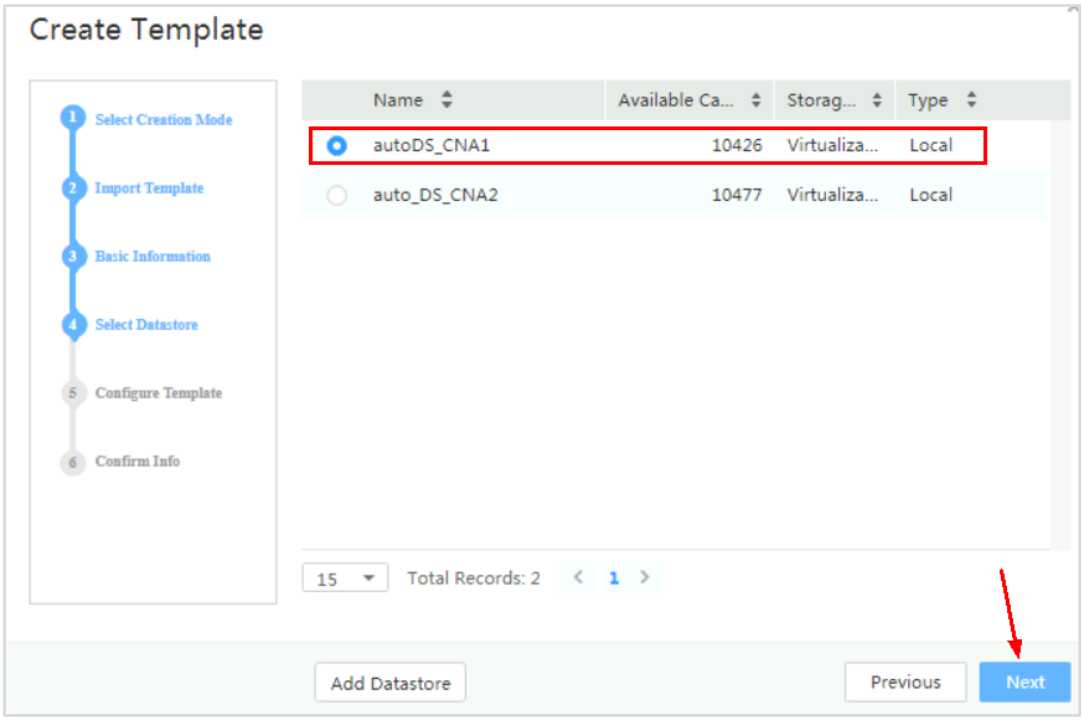


Figure 1-10 Selecting datastore

Note:

You can select any available data storage resource for the VM. The same applies to subsequent VM creation.

Step 5 For the **Configure Template** step, retain the default value and click **Next**.

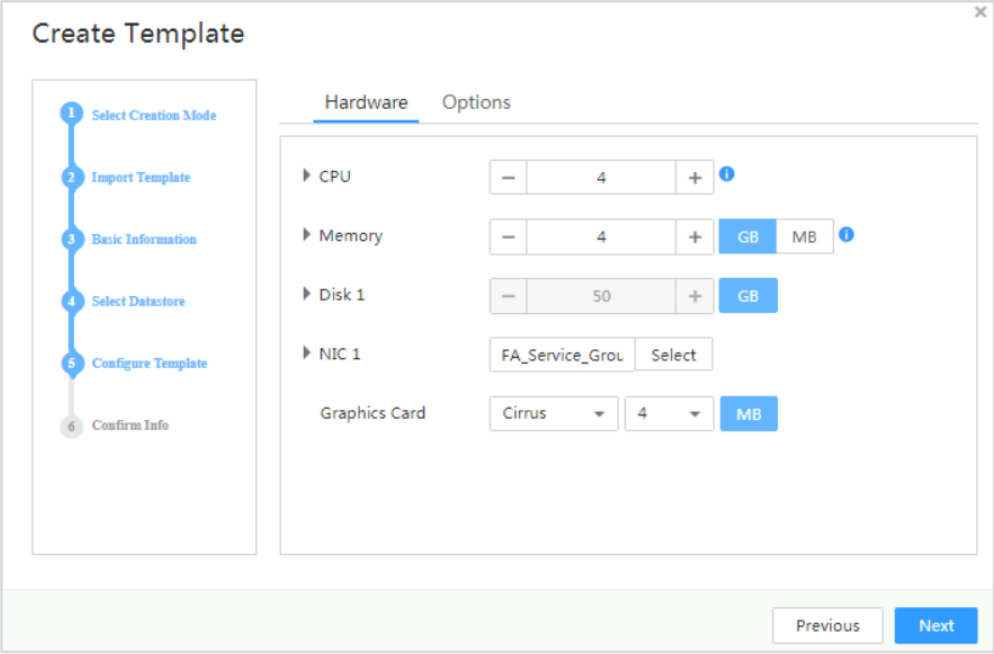


Figure 1-11 Configuring a template

Step 6 Confirm the information and click **OK**. The FA-ADDNSDHCP VM template has been created.

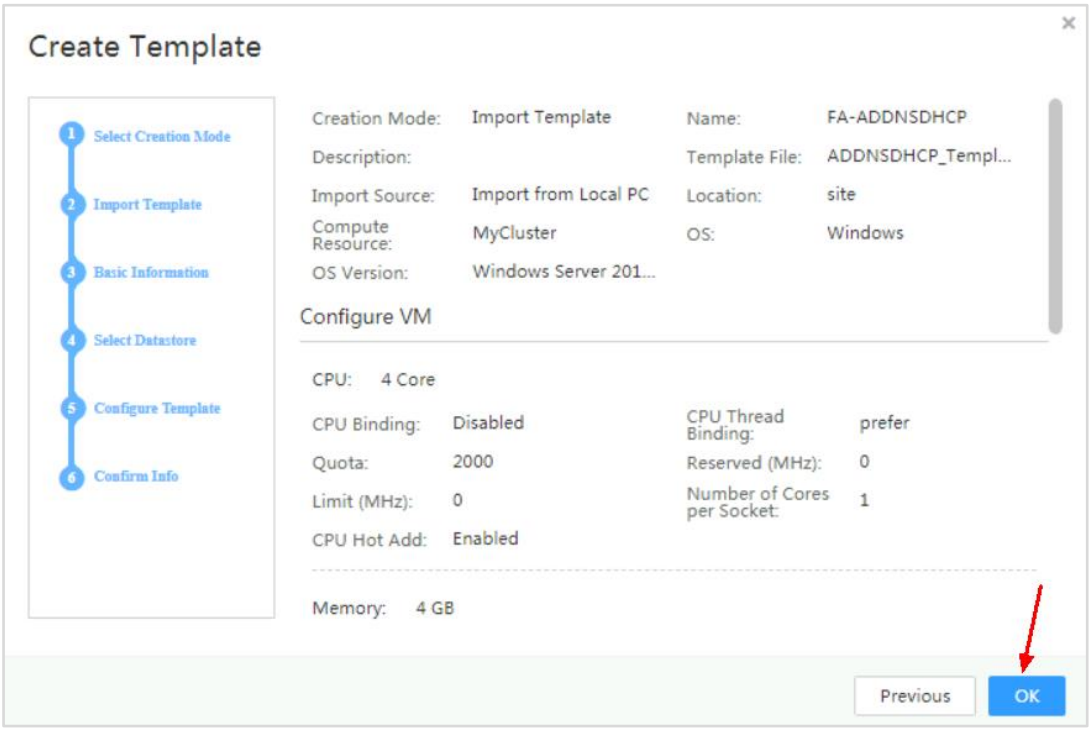


Figure 1-12 Confirming the information

Step 7 Create a new VM based on the VM template created in step 6.

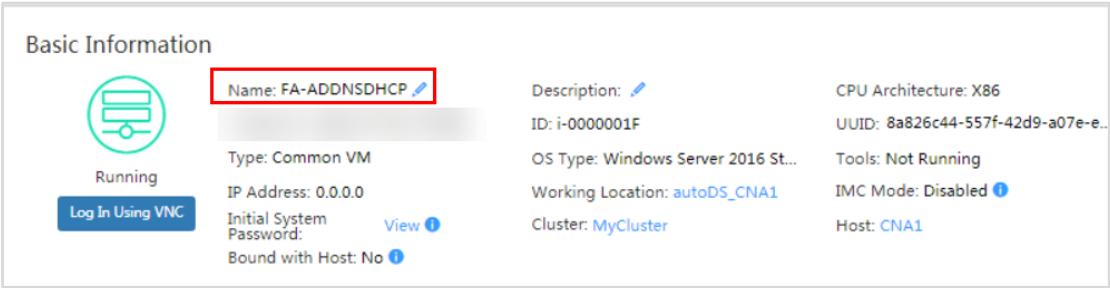


Figure 1-13 Checking the created VM

1.2.3 Creating a Bare VM

1.2.3.1 Creating the Active ITA/GaussDB/HDC/WI/vAG/vLB VM

Step 1 Log in to FusionCompute and choose **Common Operations** > **Create VM**.

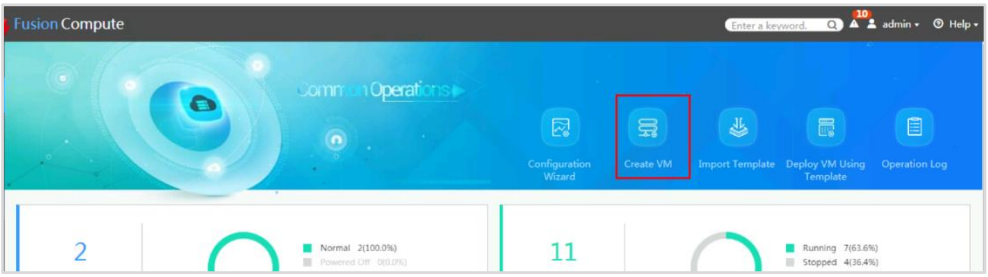


Figure 1-14 Creating a VM

Step 2 In the **Create VM** dialog box displayed, click **Next** in the **Select Creation Mode** step.

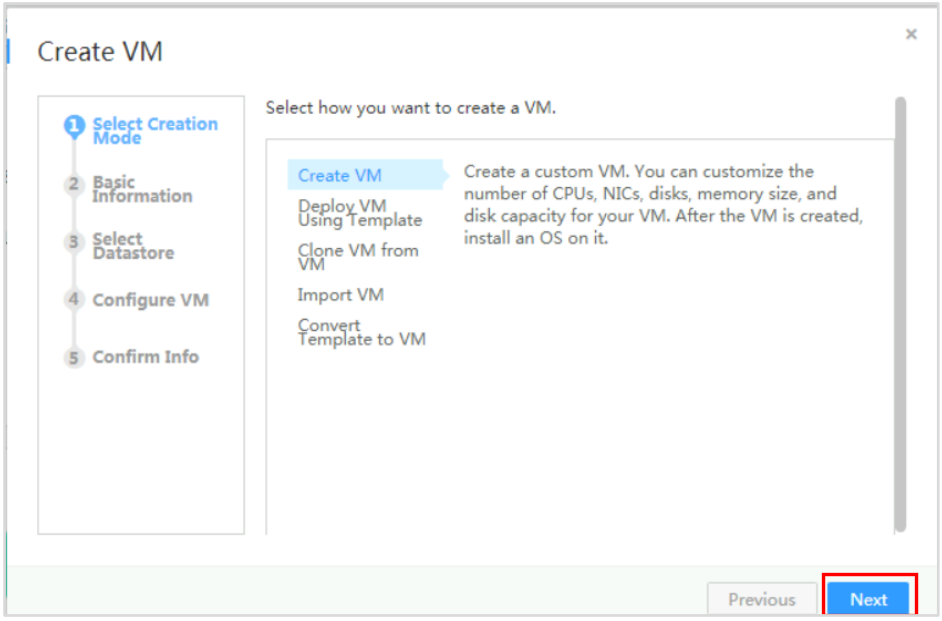


Figure 1-15 Creation mode

Step 3 When configuring **Basic Information**, change name to **FA-ITADBHDCWILIVAGVLB-01**. For **Set Compute Resource**, select **cna01** in **mycluster** and click **OK**. Set **OS** to **Linux** and **OS Version** to **EulerOS 2.5 64bit**, and click **Next**.

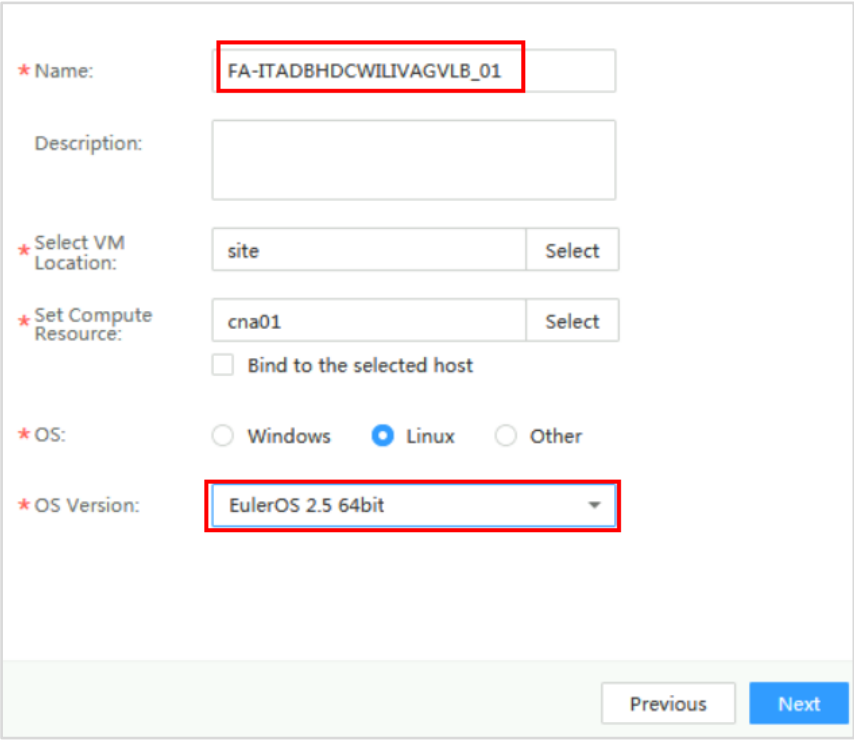


Figure 1-16 Basic information

Step 4 In the **Select Datastore** step, select **autoDS_cna01** and click **Next**.

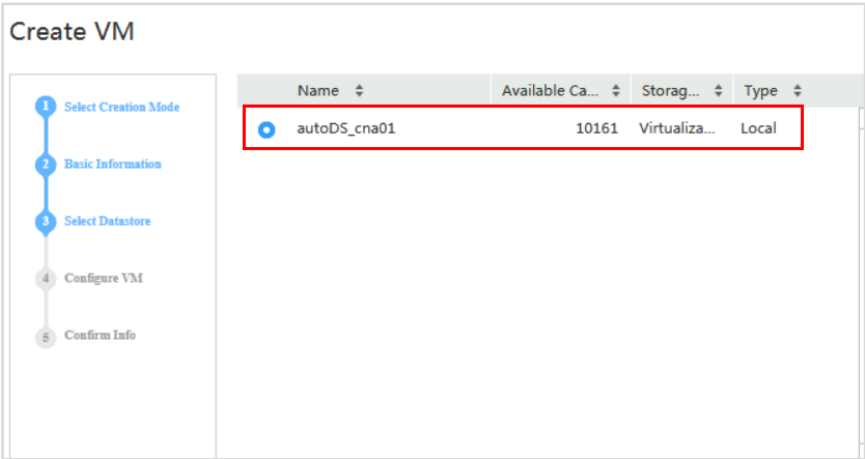


Figure 1-17 Selecting datastore

Note:

You can select any available datastore for the VM.

Step 5 In the **Configure VM** step, configure the VM hardware information and options, and click **Next**.

- Set **CPU** to **8**.
- Set **Memory** to **16 GB**.
- Set **Disk 1** to **60 GB** and **Configuration Mode** to **Thin provisioning**.
- Set **NIC 1** to a service port group, for example, **FA_Service_Portgroup**.

Note:

As the network planning adopts the integrated deployment mode and the physical switch has been configured, the FusionAccess infrastructure VM needs only one service NIC.

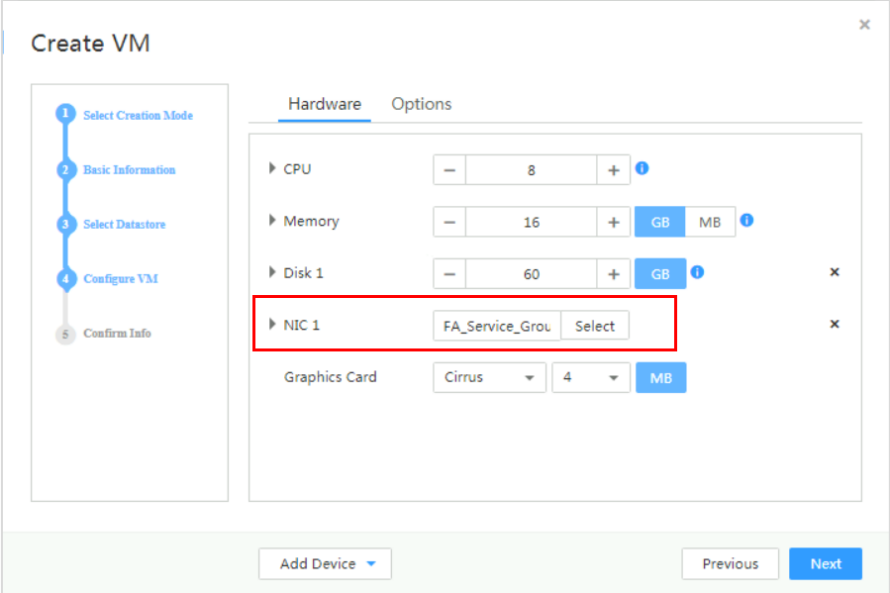


Figure 1-18 Configuring NICs

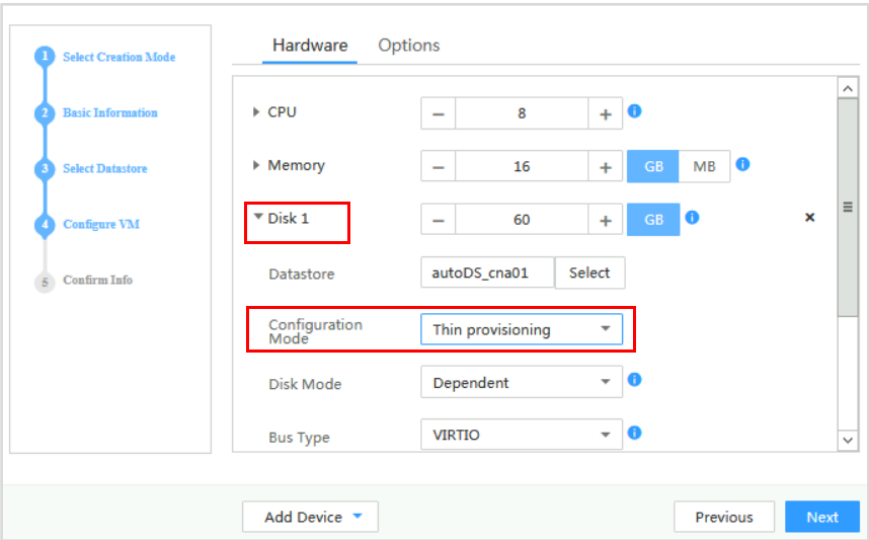


Figure 1-19 Configuring disks

Step 6 In the **Confirm Info** step, select **Start VM immediately after creation** and click **OK**. The VM tab page is displayed.

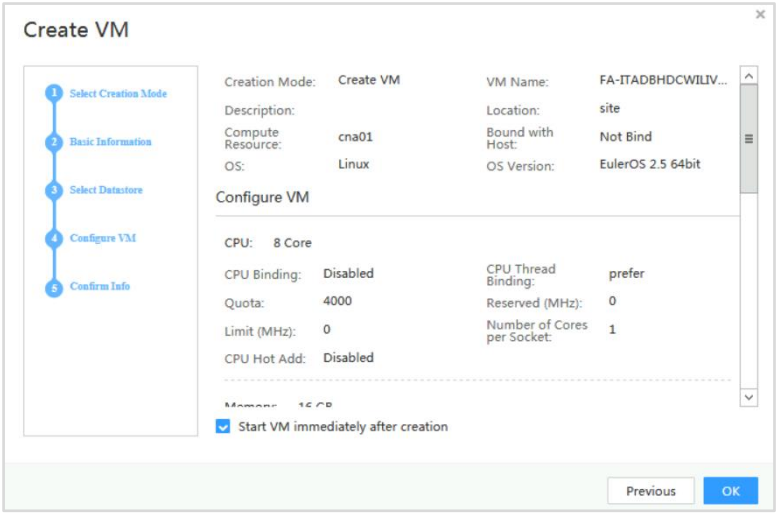


Figure 1-20 Confirming the information

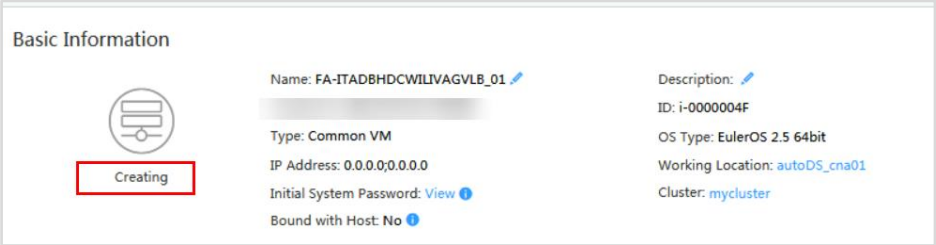


Figure 1-21 VM being created

1.2.3.2 Creating a Standby ITA/GaussDB/HDC/WI/vAG/vLB VM

Step 1 Log in to FusionCompute and choose **Common Operations** > **Create VM**.

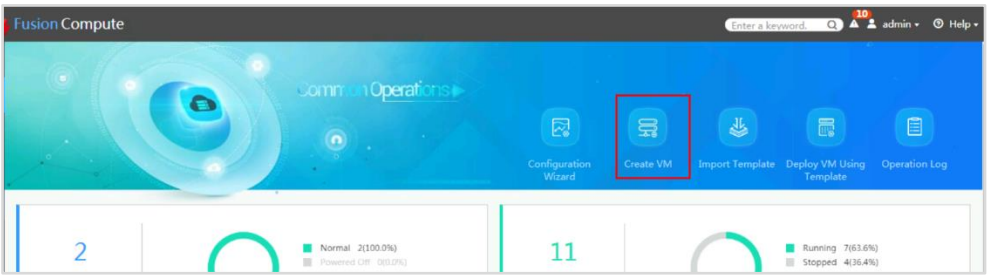


Figure 1-22 Creating a VM

Step 2 In the **Create VM** dialog box displayed, click **Next** in the **Select Creation Mode** step.

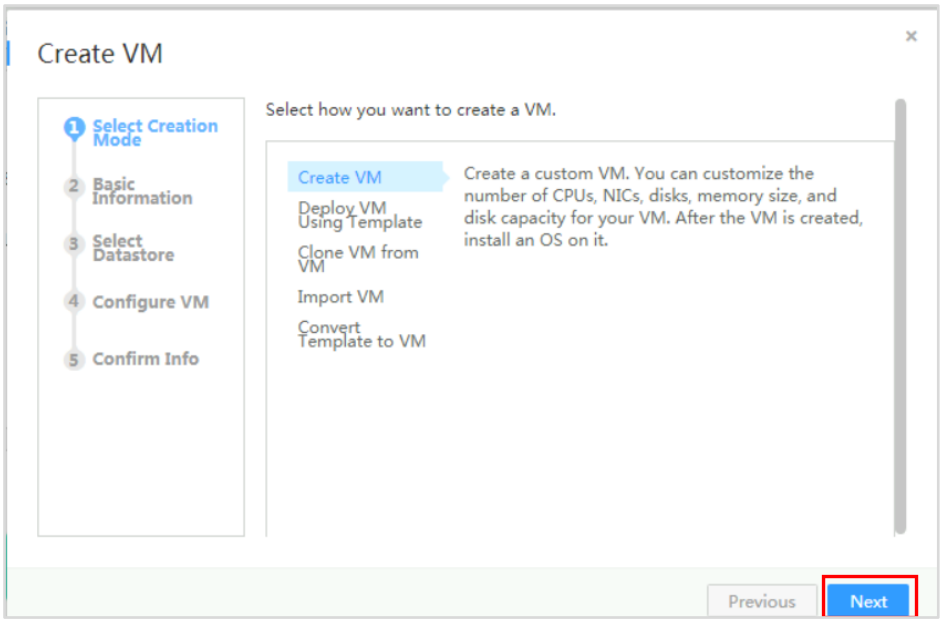


Figure 1-23 Creation mode

Step 3 When configuring **Basic Information**, change name to **FA-ITADBHDCWIVAGVLB-02**. For **Set Compute Resource**, select **cna02** in **mycluster** and click **OK**. Set **OS** to **Linux** and **OS Version** to **EulerOS 2.5 64bit**, and click **Next**.

Note:

- FA-ITADBHDCWILIVAGVLB-01 and FA-ITADBHDCWILIVAGVLB-02 adopt the active/standby deployment mode. Therefore, you are advised to deploy two VMs on two CNAs, respectively.
- As FA-ITADBHDCWILIVAGVLB-01 has been deployed on CNA01, deploy ITADBHDCWI-02 on CNA02.

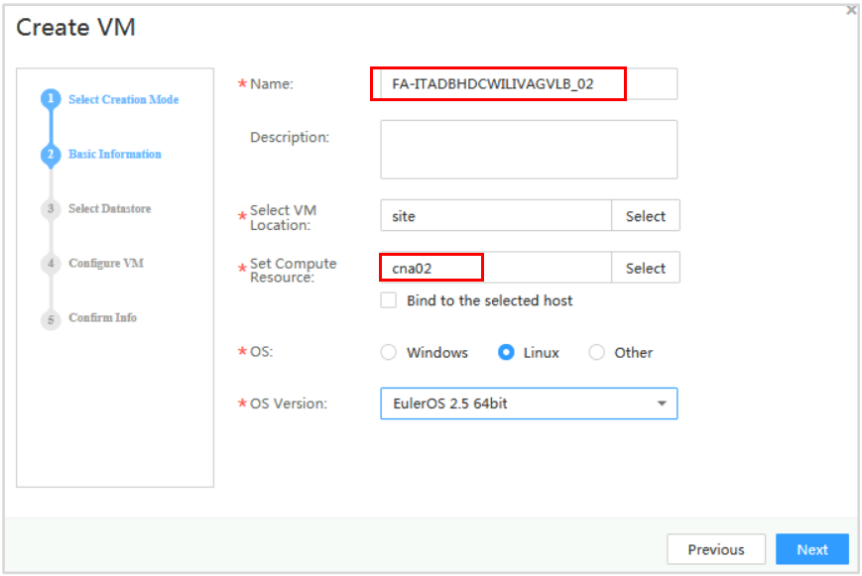


Figure 1-24 Basic information

Step 4 In the **Select Datastore** step, select **IP-SAN** and click **Next**.

Note:

- You can select any available datastore of the CNA host for the VM.
- If there is no specific requirement, you can select any available datastore when creating a VM.

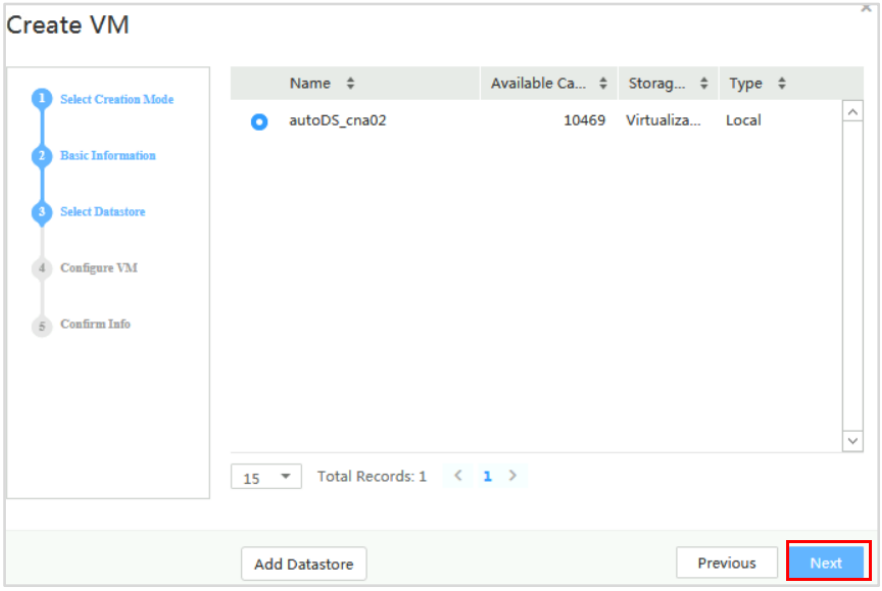


Figure 1-25 Selecting datastore

Step 5 In the **Configure VM** step, configure the VM hardware information and options, and click **Next**.

- Set **CPU** to **8**.
- Set **Memory** to **16 GB**.
- Set **Disk 1** to **60 GB** and **Configuration Mode** to **Thin provisioning**.
- Set **NIC 1** to a service port group, for example, **FA_Service_Portgroup**.

Note:

As the network planning adopts the integrated deployment mode and the physical switch has been configured, the FusionAccess infrastructure VM needs only one service NIC.

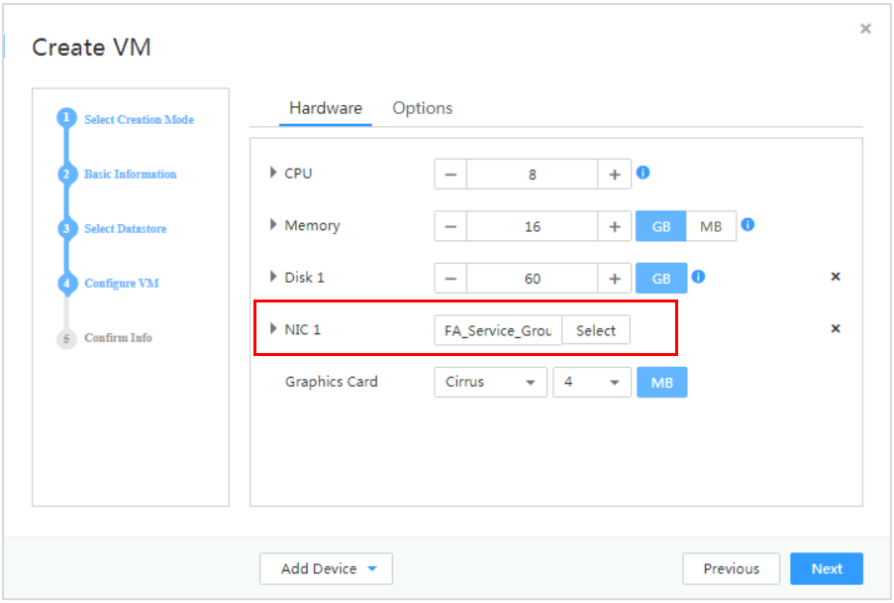


Figure 1-26 Configuring NICs

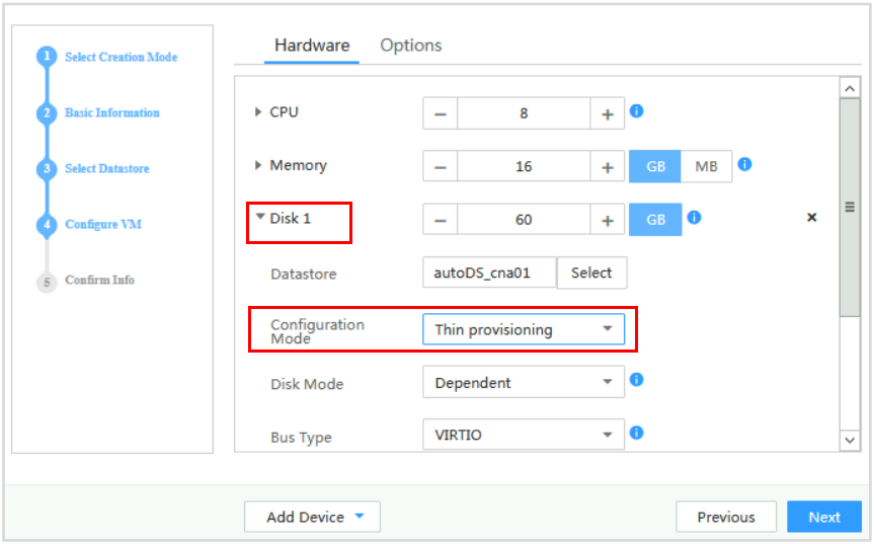


Figure 1-27 Configuring disks

Step 6 In the **Confirm Info** step, select **Start VM immediately after creation** and click **OK**. The VM tab page is displayed.

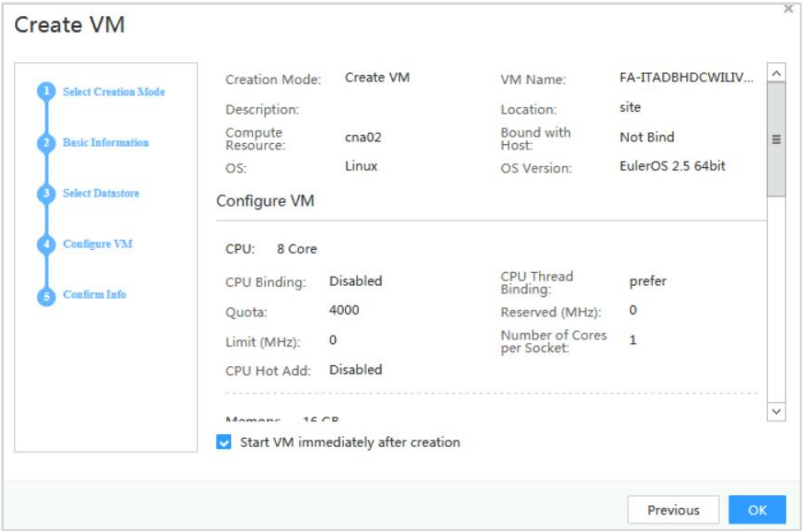


Figure 1-28 Confirming the information

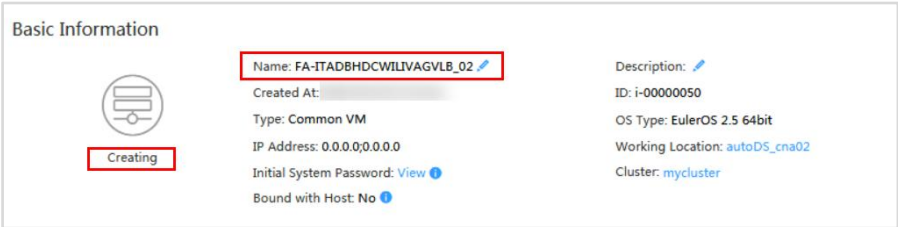


Figure 1-29 VM being created

1.2.4 Configuring Automatic Recovery for a VM

This section describes how to configure automatic recovery for a VM.

Step 1 Use an SSH tool (such as PuTTY) to log in to the active VRM node using the floating VRM IP address. The login account is **gandalf**, and the default password is the one set during initialization script execution after installation.

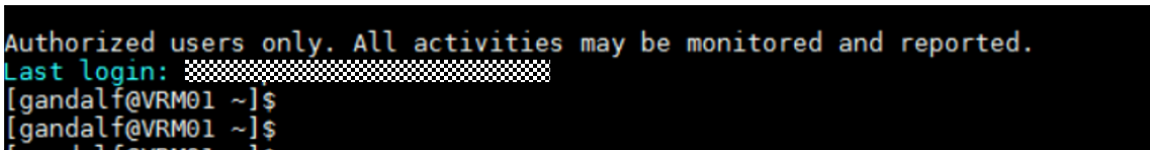


Figure 1-30 Logging in to the VRM node

Step 2 Run the following command to switch to user **root** and enter the **root** password as prompted. The default password is the one set during initialization script execution after installation.

```
su - root
```

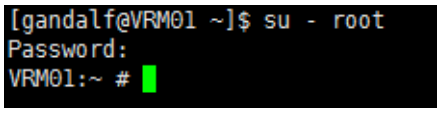


Figure 1-31 Switching to user root

Step 3 Run the following command to disable PuTTY logout upon timeout:

```
TMOUT=0
```

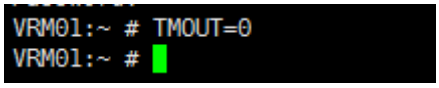


Figure 1-32 Setting the timeout duration

Step 4 On FusionCompute, query the ID of the created FA-ITADBHDCWILIVAGVLB-01 VM.

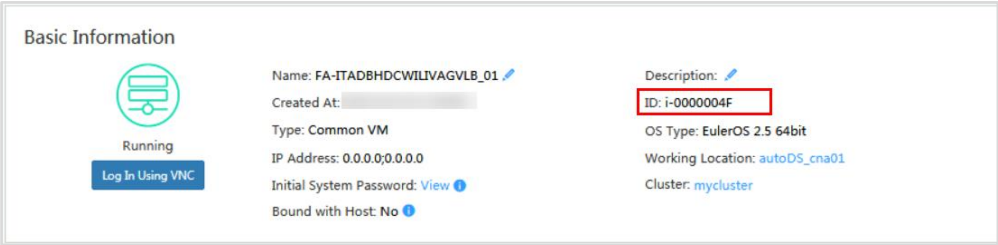


Figure 1-33 Querying a VM ID

Step 5 Run the following command for FA-ITADBHDCWILIvAGvLB-01 and FA-ITADBHDCWIvAGvLB-02, respectively. Replace **vmId** with the VM ID obtained in Step 4.

```
sh /opt/galax/vrm/tomcat/script/modifyRecover.sh vmId true
```

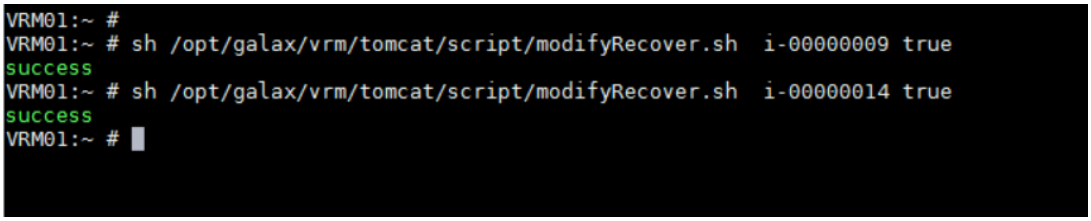


Figure 1-34 Configuring automatic recovery

Step 6 Restart the VRM process. If the process status is **active (running)**, the restart is complete.

```
service vrmd restart
```

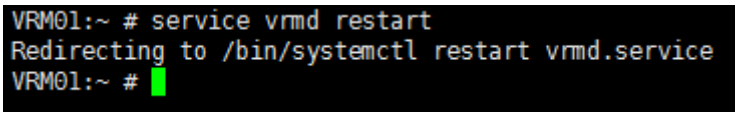


Figure 1-35 Restarting the VRM process

```
service vrmd status
```

```
VRM01:~ # service vrmd status
Redirecting to /bin/systemctl status vrmd.service
● vrmd.service - vrm Service
   Loaded: loaded (/usr/lib/systemd/system/vrmd.service; disabled; vendor preset: disabled)
   Active: active (running) since [redacted] CST; 1min 10s ago
  Process: 255897 ExecStop=/usr/bin/sh /opt/galax/vrm/tomcat/script/vrmd stop (code=exited, status=0/SUCCESS)
  Process: 255968 ExecStart=/usr/bin/sh /opt/galax/vrm/tomcat/script/vrmd start (code=exited, status=0/SUCCESS)
 Main PID: 256148 (java)
```

Figure 1-36 Viewing the process status

Step 7 After the VRM process is restarted, log in to FusionCompute again, right-click the name of the created bare VM, and choose **Power** > **Forcibly Stop** to stop the VM. After the VM is stopped, right-click the name of the created bare VM and choose **Power** > **Start** to start the VM.

Note:

Stop and restart both FA-ITADBHDCWILIvAGvLB-01 and FA-ITADBHDCWIvAGvLB-02.

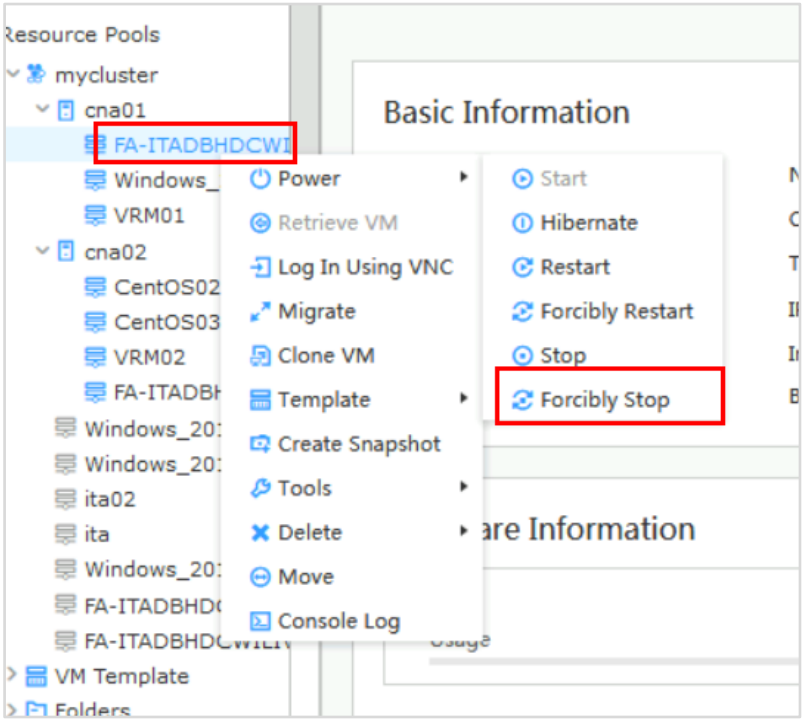


Figure 1-37 Stopping a VM

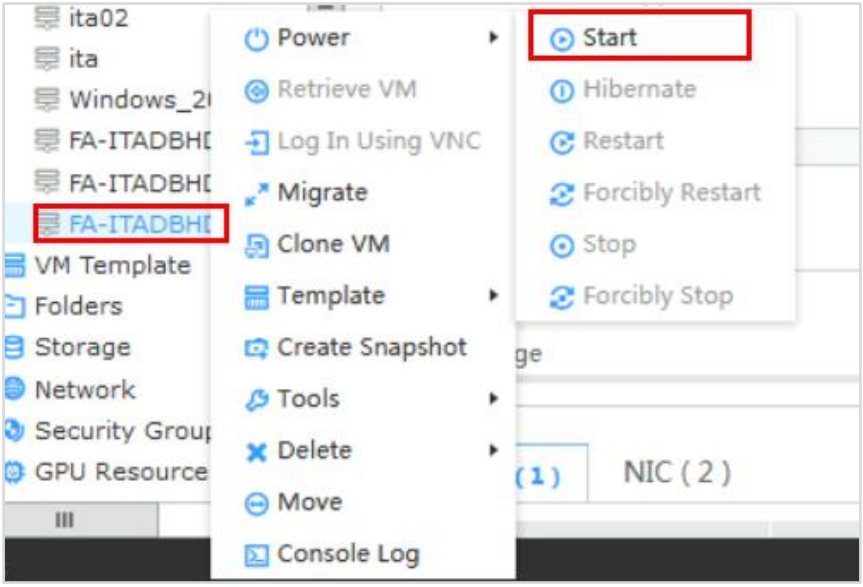


Figure 1-38 Restarting a VM

1.2.5 Installing an OS on the Bare VM

Step 1 Log in to FusionCompute. On the **Resource Pools** page, choose **mycluster** > **FA-ITADBHDCWILIVAGVLB-01**. Click the **Configuration** tab, choose **CD/DVD-ROM Drive**, set **Mount CD/DVD-ROM Drive Type** to **Mount Local CD/DVD-ROM Drive**, and click **OK**.

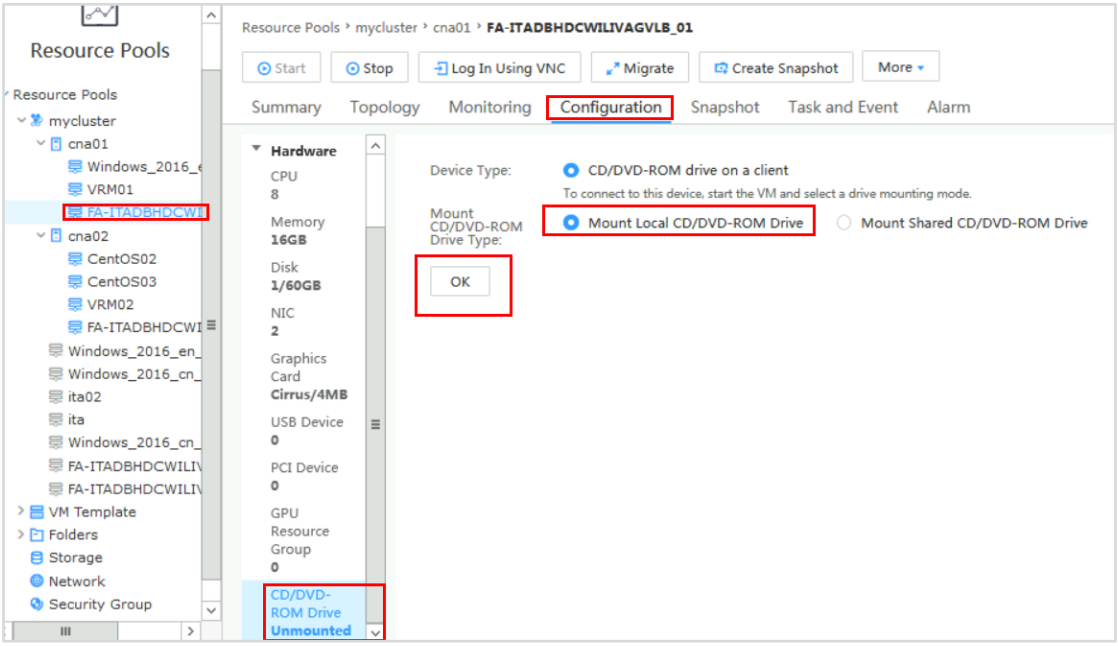


Figure 1-39 Mounting a CD/DVD-ROM drive

Step 2 In **File(*.iso)**, click **Browse**, select the ISO file **FusionAccess_Manager_Installer_8.0.2-x86_64.iso** stored in the local PC, select **Restart the VM now to install the OS**, and click **OK**.

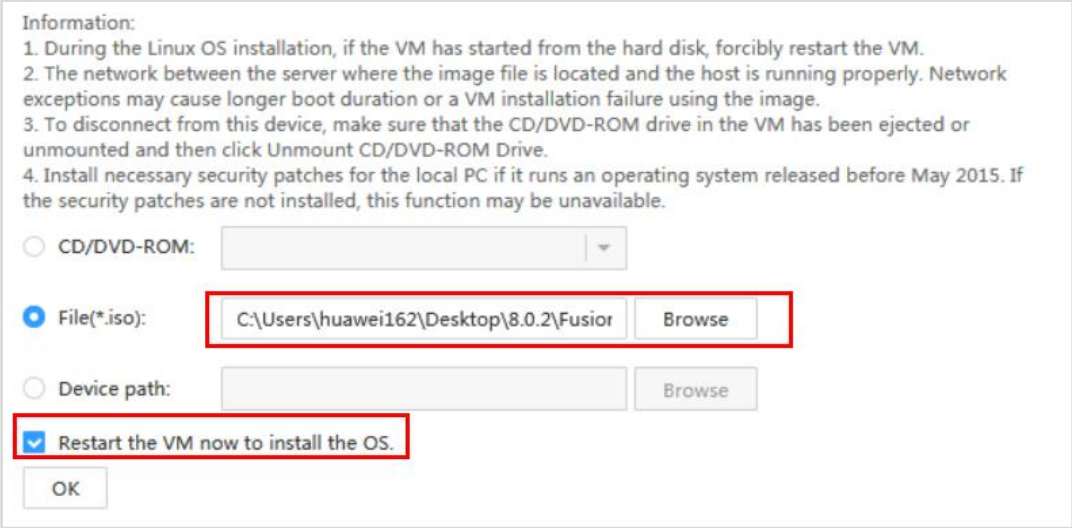


Figure 1-40 Selecting the ISO file

Step 3 After the CD/DVD-ROM drive is mounted, the **Information** dialog box is displayed. Click **OK**.

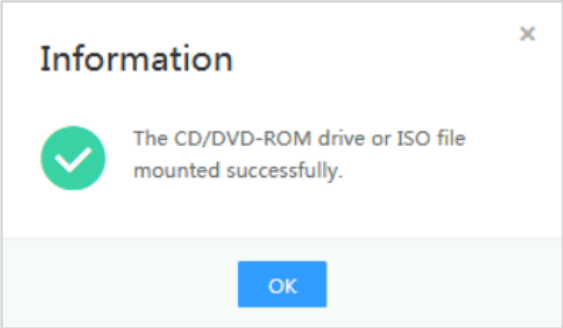


Figure 1-41 Successful mounting

Step 4 Return to the VM page and click **Log In Using VNC**.

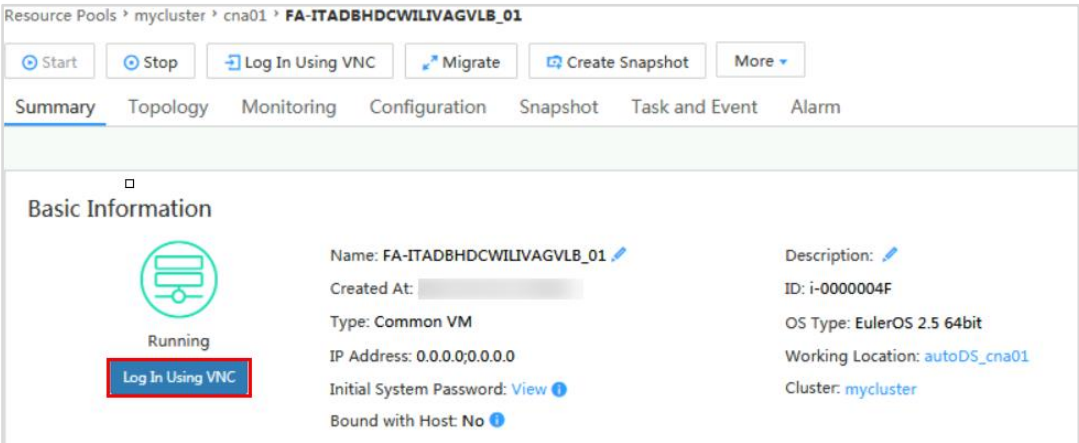


Figure 1-42 Logging in using VNC

Step 5 After the VM is restarted, select **Test this media & install EulerOS V2.0SP5** within 60 seconds after the EulerOS installation page is displayed, and press **Enter**.

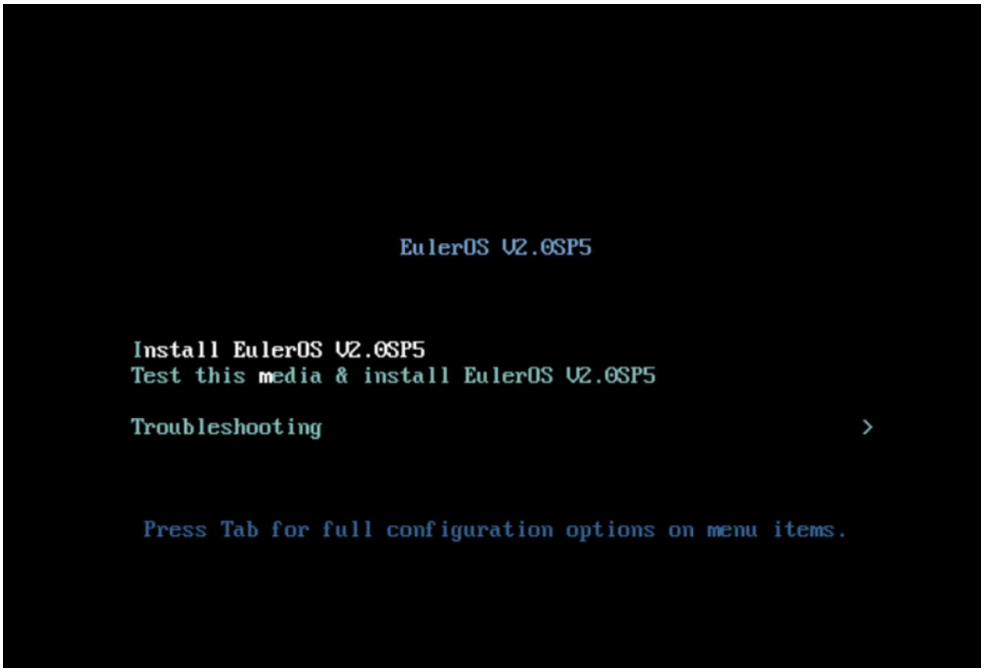


Figure 1-43 Selecting the OS to be installed

Note:

Press **Tab** or arrow keys (↑ and ↓) to move the cursor. Press **Enter** to select or execute a cursor-located item.

Step 6 The system automatically starts the installation based on the preconfiguration file.

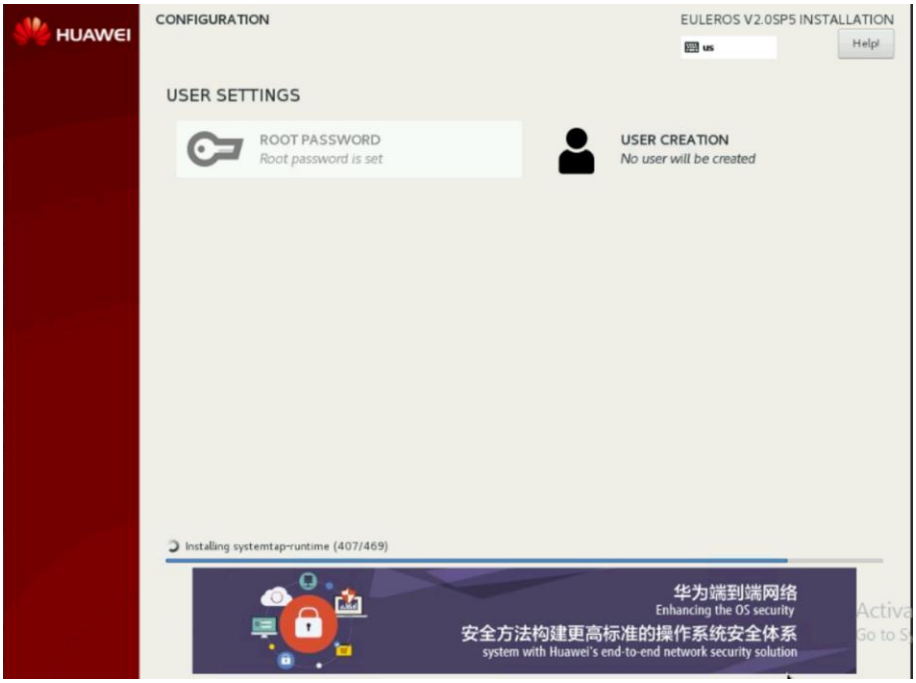


Figure 1-44 System installation started automatically

Step 7 After the installation is complete, the login page is displayed.

Note:

It takes about 30 minutes to install the OS.

Figure 1-45 Linux login page

Step 8 Unmount the CD/DVD-ROM drive.

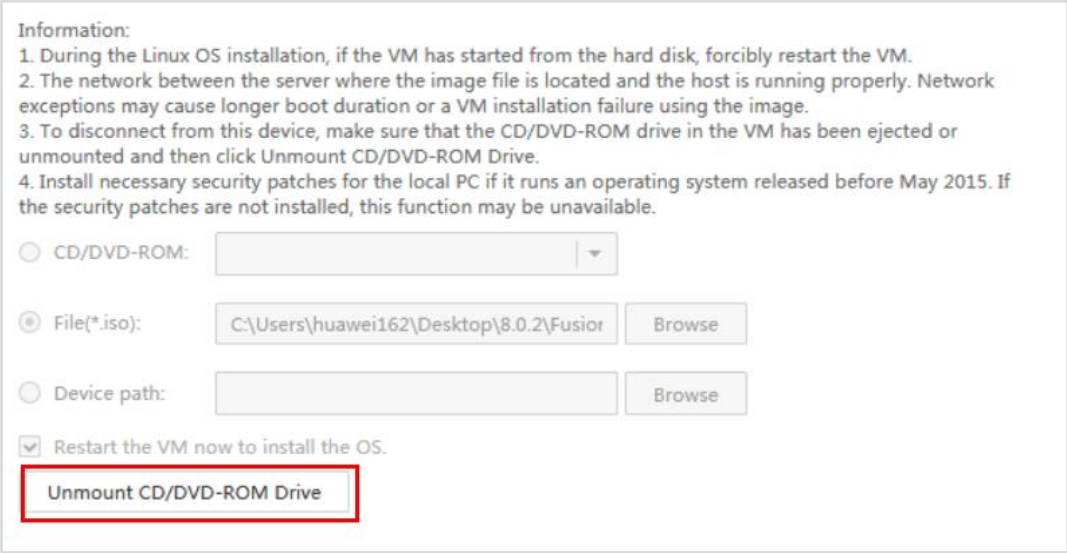


Figure 1-46 Unmounting the CD/DVD-ROM drive

Step 9 After the unmounting, the **Information** dialog box is displayed. Click **OK**.

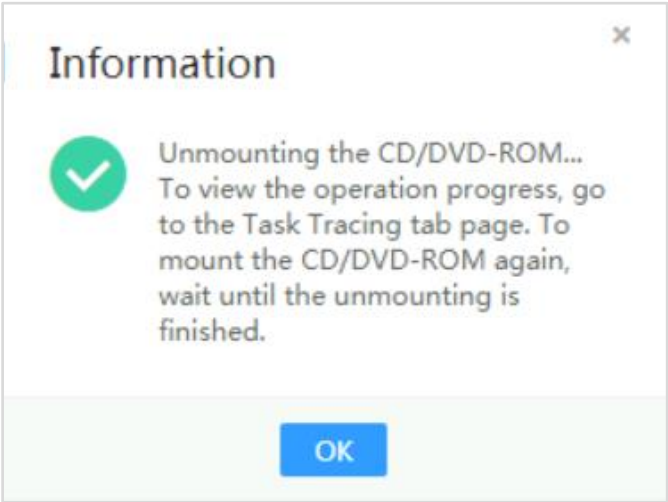


Figure 1-47 Successful uninstallation

Step 10 Return to FusionCompute. On the **Resource Pools** page, right-click the installed VM in **mycluster** and choose **Tools** > **Mount Tools**.

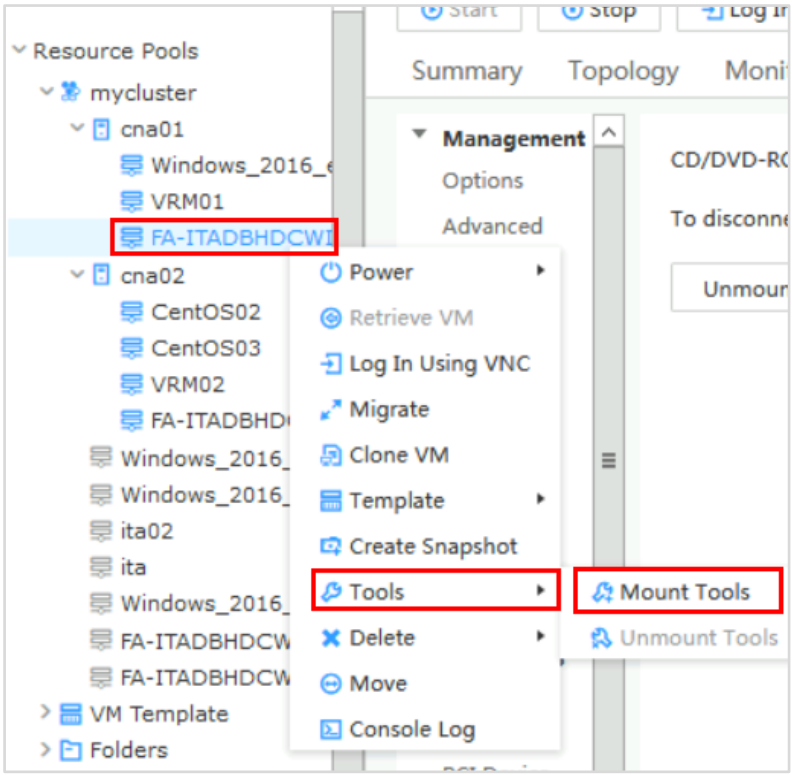


Figure 1-48 Mounting Tools

Step 11 In the **Information** dialog box displayed, click **OK**.

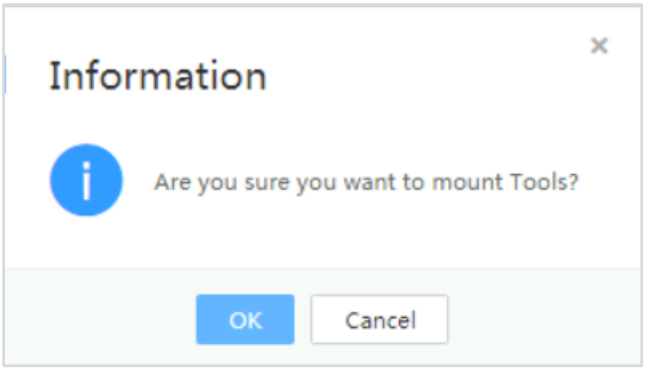


Figure 1-49 Confirming the mounting of Tools

Step 12 Log in to the VM using VNC as user **root**. Obtain the default password from FusionAccess Account List.

```
Authorized users only. All activities may be monitored and reported.
fusionaccess01 login: [  OK  ] Reached target Multi-User System.
         Starting Update UTMP about System Runlevel Changes...
[  OK  ] Started EulerOS Security Tool.
[  OK  ] Started Update UTMP about System Runlevel Changes.
         Mounting Arbitrary Executable File Formats File System...
[  OK  ] Mounted Arbitrary Executable File Formats File System.
[  OK  ] Started Crash recovery kernel arming.


Authorized users only. All activities may be monitored and reported.
fusionaccess01 login:
```

Figure 1-50 Logging in as user root

Step 13 Configure the IP address, subnet mask, and gateway of the infrastructure VM template. The FusionAccess page is displayed.

```
Authorized users only. All activities may be monitored and reported.
fusionaccess01 login: root
Password:

Authorized users only. All activities may be monitored and reported.
Redirecting to /bin/systemctl restart sshd.service
Please input ip address and press Enter: 192.168.105.10
Please input subnet mask like:255.255.255.0 and press Enter: 255.255.255.0
Please input gateway and press Enter: 192.168.105.254
```

Figure 1-51 Configuring the network

Step 14 Enter **1** to select **Driver Tools**, and press **Enter**.

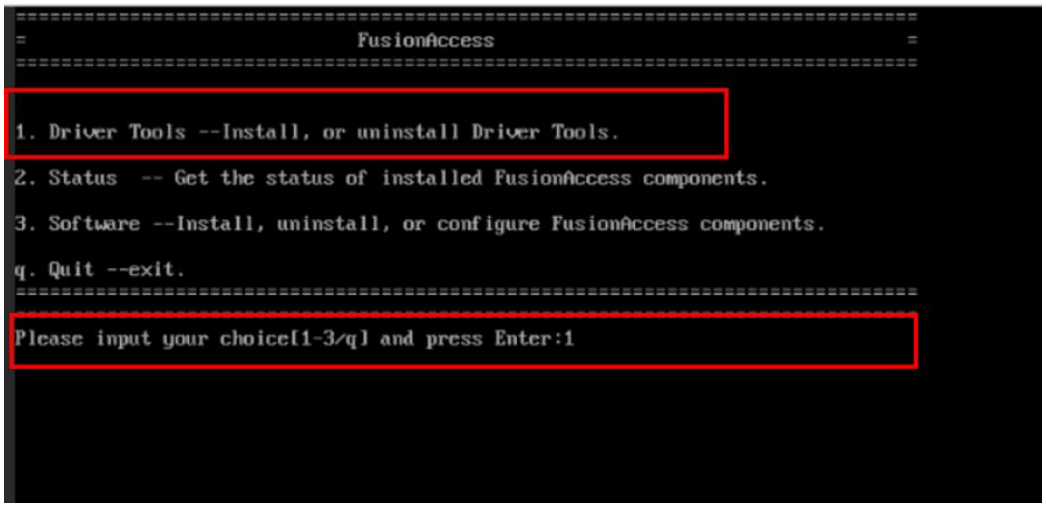


Figure 1-52 Opening the Tools installation program

Step 15 Enter **1** to select **Install Driver Tools**, and press **Enter** to start the installation.

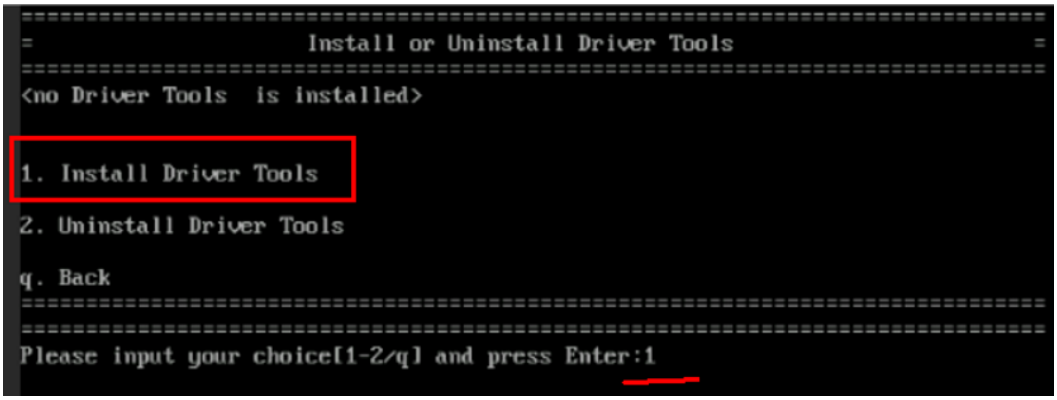


Figure 1-53 Starting installation

Step 16 After the installation is complete, enter **yes** and press **Enter** to restart the VM.

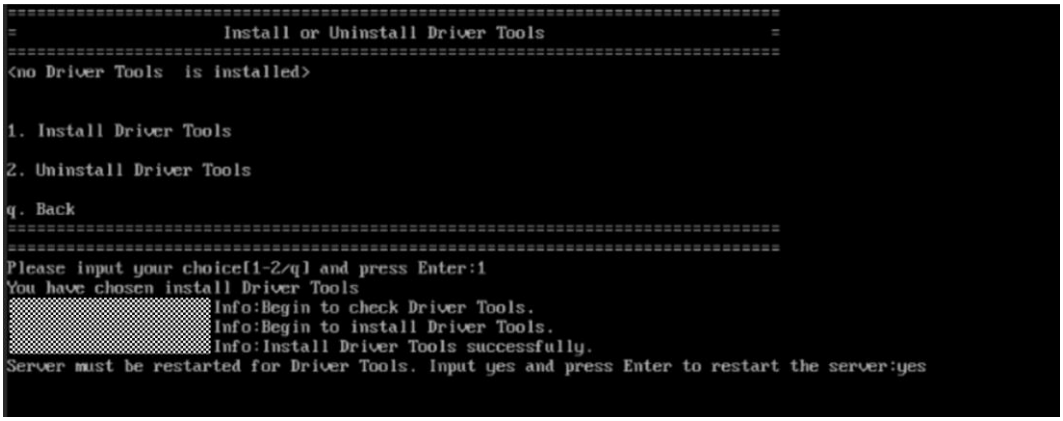


Figure 1-54 Restarting the VM

Step 17 Return to FusionCompute. Right-click the VM name and choose **Tools** > **Unmount Tools**. In the **Information** dialog box displayed, click **OK**.

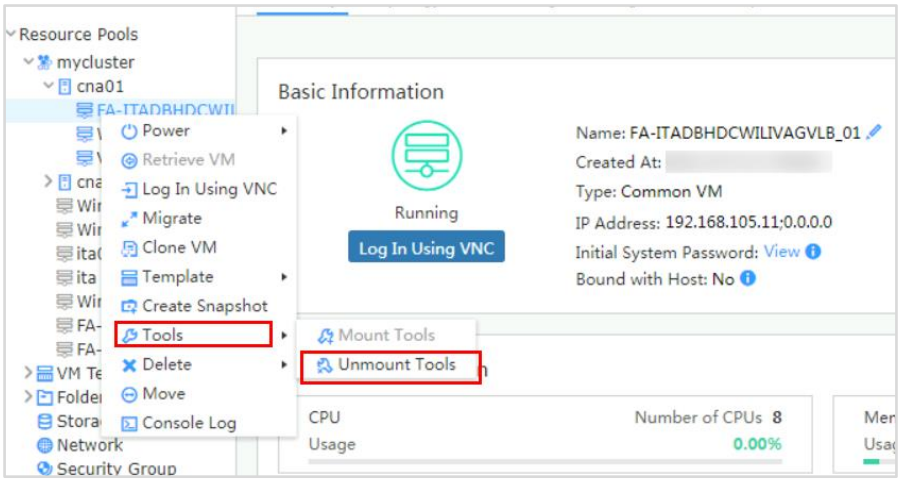


Figure 1-55 Unmounting Tools

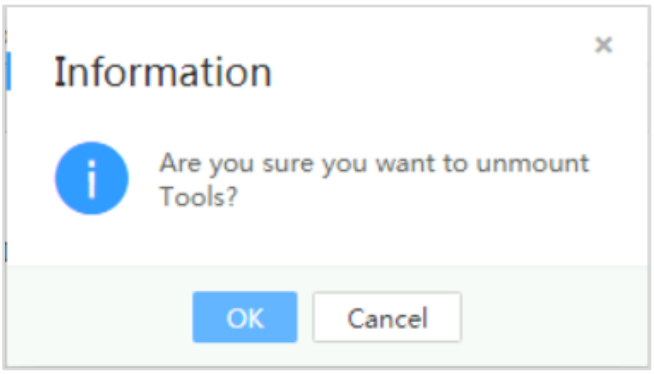


Figure 1-56 Confirming the unmounting

Step 18 Repeat steps 1 to 17 to install the OS and Tools on the other bare VM (FA-ITADBHDCWIvAGvLB-02).

Note:

For details about the IP address planning, see table VM IP address and VLAN planning in "Lab Environment Overview".

1.2.6 Installing FusionAccess Components

1.2.6.1 Installing Components on the Active ITA/DB/HDC/WI/License/vAG/vLB Server

Step 1 Log in to the active ITA/GaussDB/HDC/WI/License/vAG/vLB-01 VM as user **root** using VNC. Enter **startTools** and press **Enter**. The FusionAccess CLI is displayed.

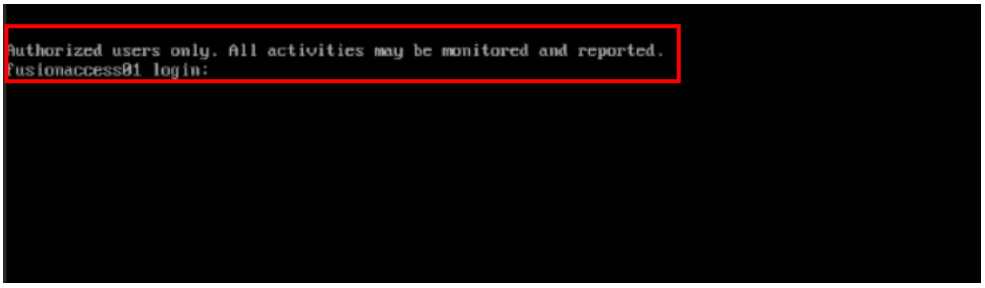


Figure 1-57 Logging in to the VM

Note:

If this is the first or second time for the **root** user to log in to the VM, the FusionAccess CLI is displayed.

Step 2 Enter **3** to select **Software** and press **Enter**.

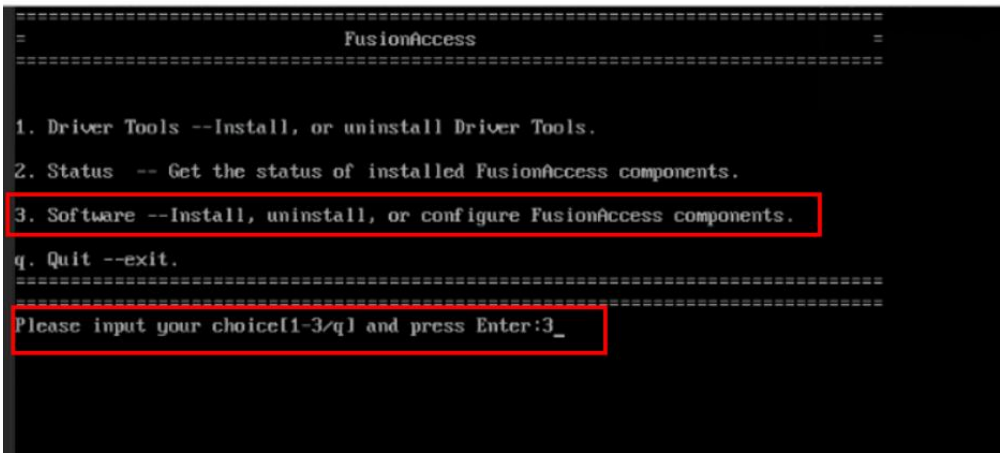


Figure 1-58 Installing FusionAccess component 1

Step 3 Enter **1** to select **All In One** and press **Enter**.

Figure 1-59 Installing FusionAccess component 2

Step 4 Enter **1** to select **Create a new node** and press **Enter**.

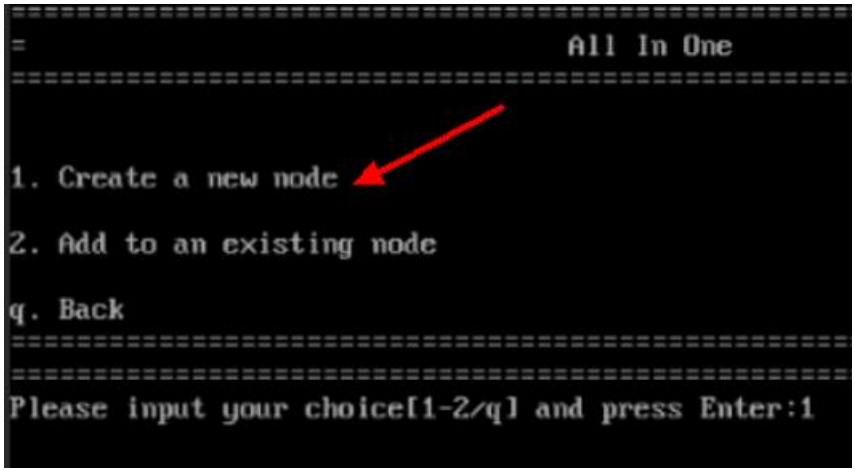


Figure 1-60 Installing FusionAccess component 3

Step 5 Enter **1** to select **Common mode** and press **Enter**.

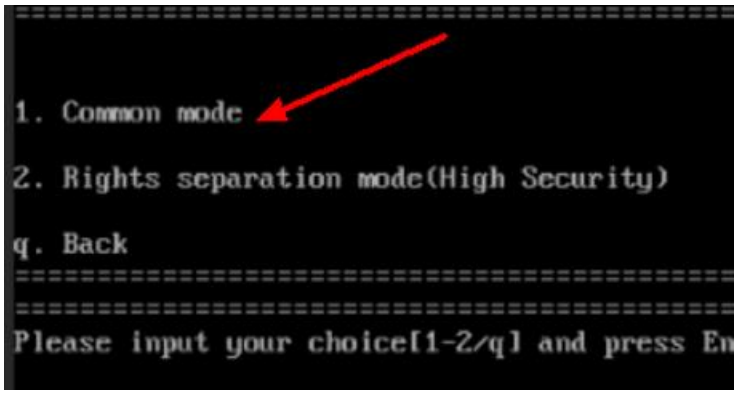


Figure 1-61 Installing FusionAccess component 4

Step 6 Specify the **Local Service IP** (the service plane IP address of the local server) and press **Enter**. The system starts installing and configuring components. After the message **Install all components successfully** is displayed, the components have been installed.

```
1. Common mode

2. Rights separation mode(High Security)

q. Back
================================================================================
================================================================================
Please input your choice[1-2/q] and press Enter:1
You have chosen Common mode
Local Service IP:192.168.105.10
                    Info:Begin to check FusionAccess component.
                    Info:No FusionAccess component are already installed.
                    Info:Begin to install ITA.
                    Info:Begin to install HDC.
                    Info:Begin to install WI.
                    Info:Begin to install License.
                    Info:Begin to install GaussDB.
                    Info:Begin to install vAG.
                    Info:Begin to install vLB.
                    Info:Begin to install LiteAS.
                    Info:Begin to install Cache.
                    Info:Configure LiteAS name...
                    Info:Configure LiteAS successfully.
                    Info:Start to config WIs to vLB...
                    Info:Config WIs to vLB successfully.
                    Info:Config ha to single mode...
                    Info:Config ha to single mode successfully.
                    Info:Restart ha...
                    Info:Restart successfully.
                    Info:Config Cache...
                    Info:Config Cache successfully.
                    Info:Config HDC...
                    Info:Config HDC successfully.
                    Info:Config WI...
                    Info:Config WI successfully.
                    Info:Configure ITA...
```

Figure 1-62 Installing FusionAccess component 5

Step 7 Enter **e** and press **Enter** to exit. Components have been installed and configured on the active VM.

```
                    Info:Config WI on local server...
                    Info:Config WI on local server successfully.
                    Info:Config WI on peer server...
                    Info:Config WI on peer server successfully.
                    Info:Start to config ITA on local node...
                    Info:Config ITA successfully.
                    Info:Write LiteAS info to ita database...
                    Info:Write LiteAS info to ita database successfully.
Install all components successfully.

Input e and press Enter to exit:e
[root@fusionaccess01 ~]#
[root@fusionaccess01 ~]#
[root@fusionaccess01 ~]#
[root@fusionaccess01 ~]#
[root@fusionaccess01 ~]#
[root@fusionaccess01 ~]#
[root@fusionaccess01 ~]#
[root@fusionaccess01 ~]#
[root@fusionaccess01 ~]#
```

Figure 1-63 Installing FusionAccess component 6

1.2.6.2 Installing Components on the Standby ITA/DB/HDC/WI Server

Step 1 Log in to the standby ITA/GaussDB/HDC/WI/License/vAG/vLB-02 VM as user **root** using VNC. Enter **startTools** and press **Enter**. The FusionAccess CLI is displayed.

```
Authorized users only. All activities may be monitored and reported.
fusionaccess01 login:
```

Figure 1-64 Logging in as user root

Note:

If this is the first or second time for the **root** user to log in to the VM, the FusionAccess CLI is displayed.

Step 2 Enter **3** to select **Software** and press **Enter**.

```
================================================================================
=                                FusionAccess                                  =
================================================================================


1. Driver Tools --Install, or uninstall Driver Tools.

2. Status  -- Get the status of installed FusionAccess components.

3. Software --Install, uninstall, or configure FusionAccess components.

q. Quit --exit.
================================================================================
================================================================================
Please input your choice[1-3/q] and press Enter:3_
```

Figure 1-65 Installing FusionAccess components 1

Step 3 Enter **1** to select **All In One** and press **Enter**.

```
================================================================================
=                                  Software                                    =
================================================================================


1. All In One

2. Custom Install

3. Install All(LiteAS/ITA/HDC/Cache/WI/License/GaussDB)

q. Back
================================================================================
================================================================================
Please input your choice[1-3/q] and press Enter:1_
```

Figure 1-66 Installing FusionAccess components 2

Step 4 Enter **2** to select **Add to an existing node** and press **Enter**.

Figure 1-67 Installing FusionAccess components 3

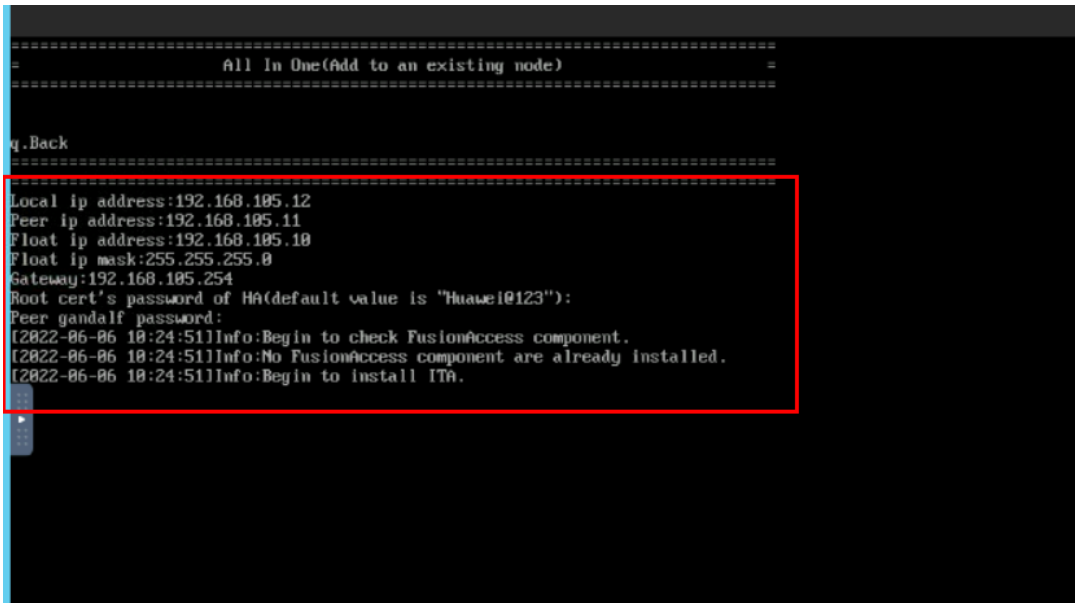


Figure 1-68 Installing FusionAccess components 4

Step 5 Configure related parameters.

Note:

- **Local ip address**: Enter the service plane IP address of the VM.
- **Peer ip address**: Enter the service plane IP address of the other VM in active/standby relationship with the VM.
- **Float ip address**: Enter the floating IP address of the VM.
- **Float ip subnet mask**: Enter the subnet mask of the VM.
- **Gateway**: Enter the service plane gateway of the VM.
- **Root cert's password of HA**: Enter the password of the HA root certificate. Obtain it from FusionAccess Account List.
- **Peer gandalf password**: Enter the **gandalf** password for logging in to the other VM in active/standby relationship with the VM. Obtain it from FusionAccess Account List.

Step 6 The system starts installing and configuring components. After the message **Install all components successfully** is displayed, the components have been installed.

```
Info:config ITA on peer server...
Info:Config ITA on peer successfully.
Info:Copy ITA config from peer server...
Info:Copy ITA config from peer server successfully.
Info:Config LiteAS on peer server...
Info:Configure LiteAS successfully.
Info:Copy LiteAS config from peer server...
Info:Copy LiteAS config from peer server successfully.
Info:Config HA on local server...
Info:Config HA successfully.
Info:Config GaussDB channel on local server...
Info:Config GaussDB channel successfully.
Info:Config float ip on local server...
Info:Config float ip successfully.
Info:Config WIs to vLB on local server...
Info:Config WIs to vLB successfully.
Info:Start to config LiteAS on local node...
Info:Config LiteAS successfully.
Info:Restart ha...
Info:Restart successfully.
Info:config Cache...
Info:config Cache successfully.
Info:Config HDC on local server...
Info:Config HDC on local server successfully.
Info:Config HDC on peer server...
Info:Config HDC on peer server successfully.
Info:Config WI on local server...
Info:Config WI on local server successfully.
Info:Config WI on peer server...
Info:Config WI on peer server successfully.
Info:Start to config ITA on local node...
Info:Config ITA successfully.
Info:Write LiteAS info to ita database...
Info:Write LiteAS info to ita database successfully.
Install all components successfully.
```

Figure 1-69 Installing FusionAccess components 5

Step 7 Enter **e** and press **Enter** to exit. Components have been installed and configured on the standby VM.

```
Info:Config WI on local server...
Info:Config WI on local server successfully.
Info:Config WI on peer server...
Info:Config WI on peer server successfully.
Info:Start to config ITA on local node...
Info:Config ITA successfully.
Info:Write LiteAS info to ita database...
Info:Write LiteAS info to ita database successfully.
Install all components successfully.

input e and press Enter to exit:e
[root@fusionaccess01 ~]#
[root@fusionaccess01 ~]#
[root@fusionaccess01 ~]#
[root@fusionaccess01 ~]#
[root@fusionaccess01 ~]#
[root@fusionaccess01 ~]#
[root@fusionaccess01 ~]#
[root@fusionaccess01 ~]#
[root@fusionaccess01 ~]#
```

Figure 1-70 Installing FusionAccess components 6

1.2.7 Modifying the Timestamp Configuration

Modifying the timestamp configuration can prevent failures caused by asynchronous desktop provisioning. Therefore, you need to modify the configuration file to disable time verification after a Linux infrastructure VM is installed.

Step 1 Log in to the active ITA/GaussDB/HDC/WI/License/vAG/vLB-01 VM as user **gandalf** using PuTTY.

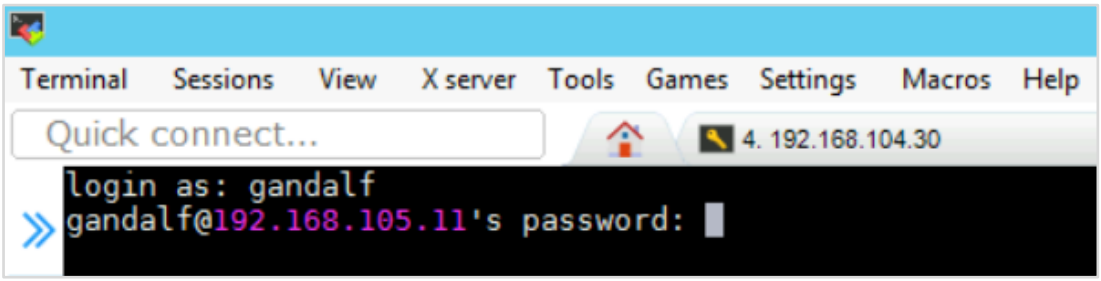


Figure 1-71 Logging in to the ITA VM

Step 2 Run the **su - root** command to switch to user **root** and enter the password.

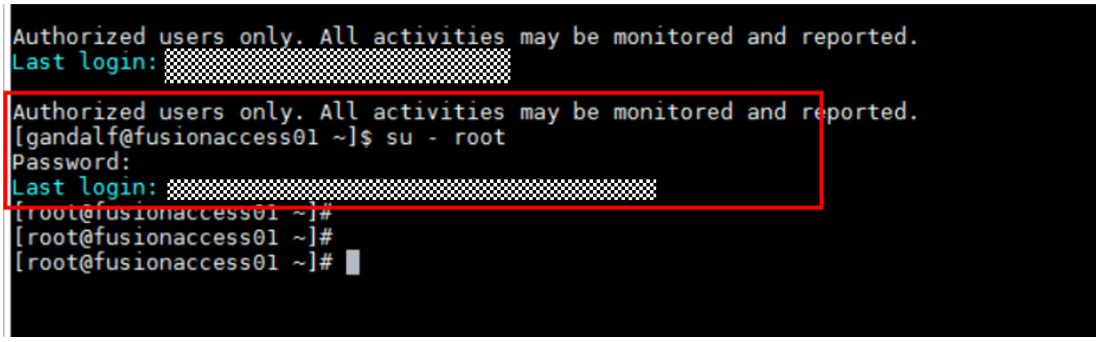


Figure 1-72 Switching to user root

Step 3 Run the following command to modify **SystemConf.xml**:

```
vim /opt/ITA/tomcat/ita/WEB-INF/conf/system/SystemConf.xml
```

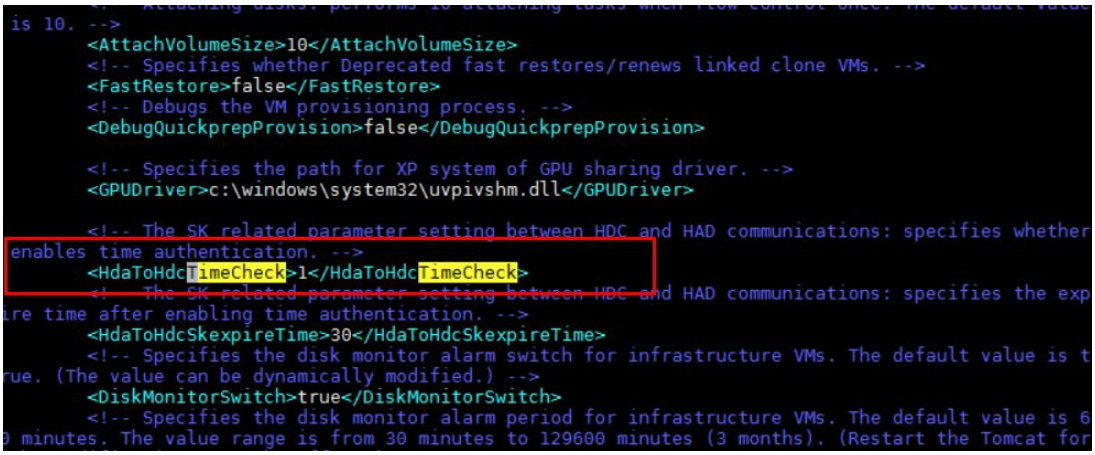


Figure 1-73 Opening SystemConf.xml

Step 4 Press **I** to enter the editing mode and change the value of **HdaToHdcTimeCheck** to **0**.

```
        <NicNumber>0</NicNumber>
        <!-- Attaching disks: performs 10 attaching tasks when flow control once. The default value
 is 10. -->
        <AttachVolumeSize>10</AttachVolumeSize>
        <!-- Specifies whether Deprecated fast restores/renews linked clone VMs. -->
        <FastRestore>false</FastRestore>
        <!-- Debugs the VM provisioning process. -->
        <DebugQuickprepProvision>false</DebugQuickprepProvision>

        <!-- Specifies the path for XP system of GPU sharing driver. -->
        <GPUDriver>c:\windows\system32\uvpivshm.dll</GPUDriver>

        <!-- The SK related parameter setting between HDC and HAD communications: specifies whether
 enables time authentication. -->
        <HdaToHdcTimeCheck>0</HdaToHdcTimeCheck>
        <!-- The SK related parameter setting between HDC and HAD communications: specifies the exp
ire time after enabling time authentication. -->
        <HdaToHdcSkexpireTime>30</HdaToHdcSkexpireTime>
        <!-- Specifies the disk monitor alarm switch for infrastructure VMs. The default value is t
rue. (The value can be dynamically modified.) -->
        <DiskMonitorSwitch>true</DiskMonitorSwitch>
        <!-- Specifies the disk monitor alarm period for infrastructure VMs. The default value is 6
0 minutes. The value range is from 30 minutes to 129600 minutes (3 months). (Restart the Tomcat for
 the modifications to take effect.) -->
        <DiskMonitorPeriod>60</DiskMonitorPeriod>
```

Figure 1-74 Modifying SystemConf.xml

Step 5 Press **Esc** to exit the editing mode. Enter **:wq** and press **Enter** to save the settings and exit.

Step 6 Run the following command to restart the ITA service:

```
service ITAService restart
```

```
[root@fusionaccess01 ~]# vim /opt/ITA/tomcat/ita/WEB-INF/conf/system/SystemConf.xml
[root@fusionaccess01 ~]#
[root@fusionaccess01 ~]#
[root@fusionaccess01 ~]# service ITAService restart
Using CATALINA_BASE:   /opt/ITA/tomcat
Using CATALINA_HOME:   /opt/ITA/tomcat
Using CATALINA_TMPDIR: /opt/ITA/tomcat/temp
Using JRE_HOME:        /opt/ITA/jre
Using CLASSPATH:       /opt/ITA/tomcat/bin/bootstrap.jar:/opt/ITA/tomcat/bin/tomcat-juli.jar
Using CATALINA_OPTS:
Using CATALINA_BASE:   /opt/ITA/tomcat
Using CATALINA_HOME:   /opt/ITA/tomcat
Using CATALINA_TMPDIR: /opt/ITA/tomcat/temp
Using JRE_HOME:        /opt/ITA/jre
Using CLASSPATH:       /opt/ITA/tomcat/bin/bootstrap.jar:/opt/ITA/tomcat/bin/tomcat-juli.jar
Using CATALINA_OPTS:
Tomcat started.
[root@fusionaccess01 ~]#
```

Figure 1-75 Restarting the ITA service

Step 7 Repeat steps 1 to 6 to modify the **HdaToHdcTimeCheck** configuration of the standby ITA/GaussDB/HDC/WI/License/vAG/vLB-02 VM. WIN-DSL1AQ8A17A

1.2.8 Adding a System Account for Interconnecting with FusionAccess on FusionCompute

Step 1 In the navigation pane on the right of the FusionCompute page, click **System**.

Step 2 Choose **Rights Management** > **User Management** and click **Add User**.

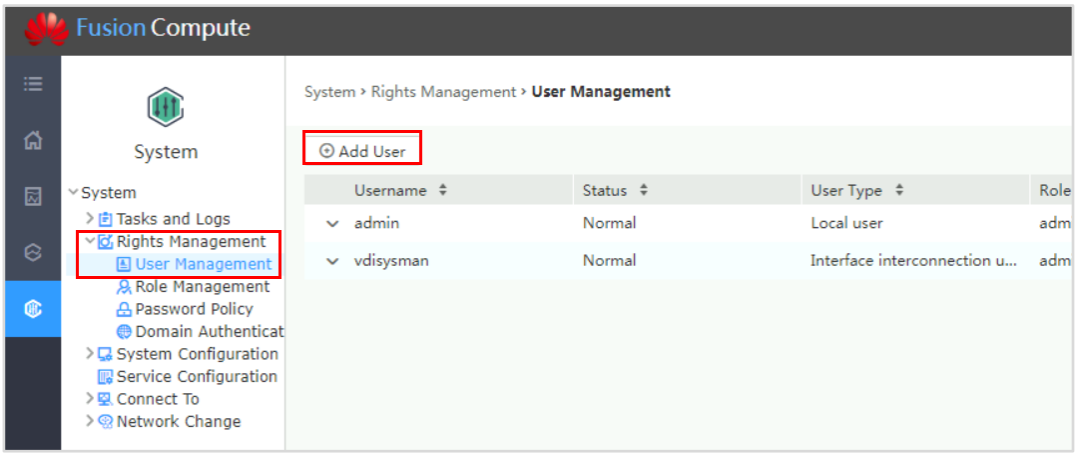


Figure 1-76 Adding a user

Step 3 On the **Add User** page, configure information about the user to be added and click **OK**.

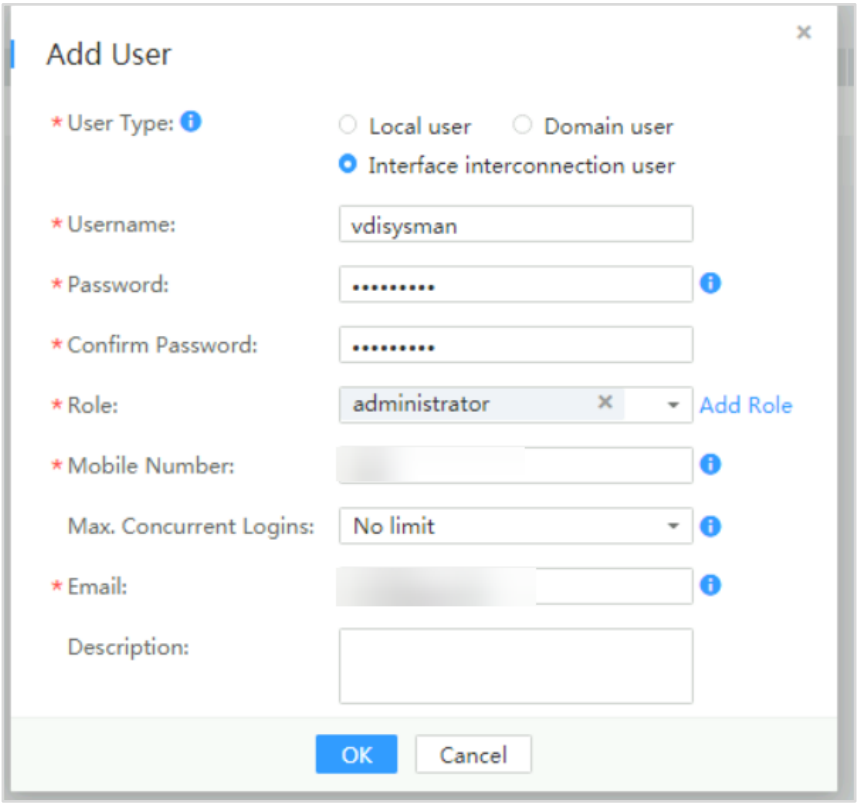


Figure 1-77 User configuration

Note:

- **User Type**: Select **Interface interconnection user**.
- **Username**: Enter **vdisysman**.
- **Role**: Select **administrator**.
- Configure other parameters.

Step 4 Verify that the user has been added.

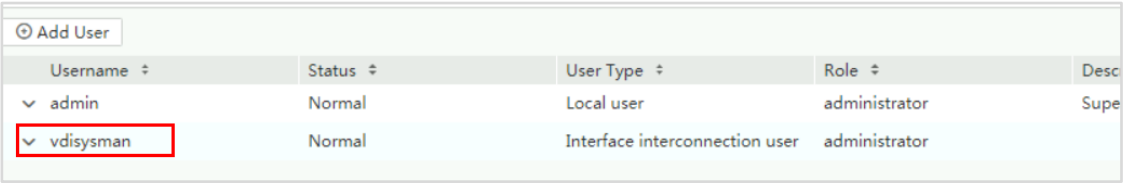


Figure 1-78 Verifying that the user has been added

1.2.9 Completing the Configuration

Configure the virtualization environment, vAGs/vLBs, and other necessary information after installing infrastructure components.

Step 1 In the address box of your web browser, enter **https://192.168.105.11:8448**, and press **Enter**. **192.168.105.11** is the service plane IP address of the active ITA VM. The **First login, please set admin password** page is displayed. Set a login password.

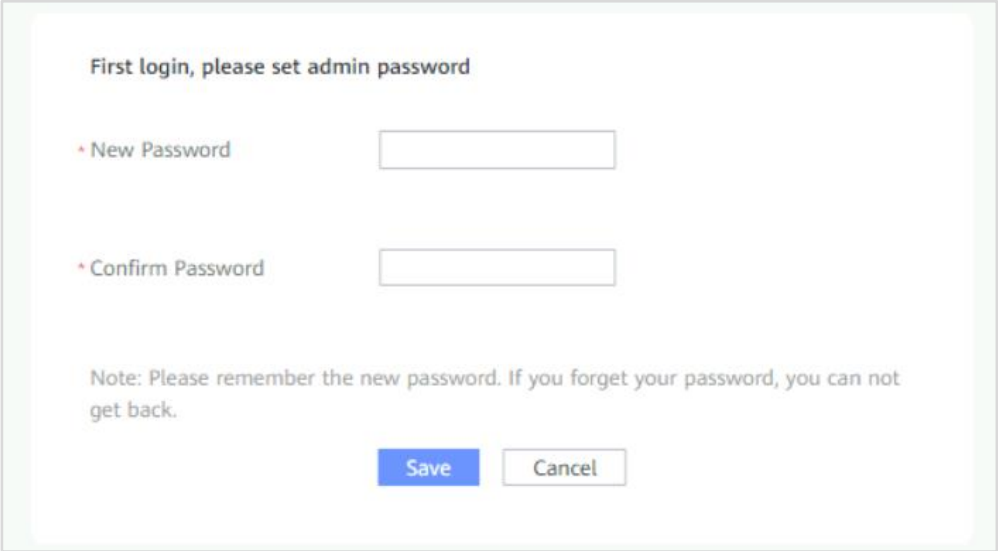


Figure 1-79 Changing the password

Step 2 Enter a password and click **Save**.

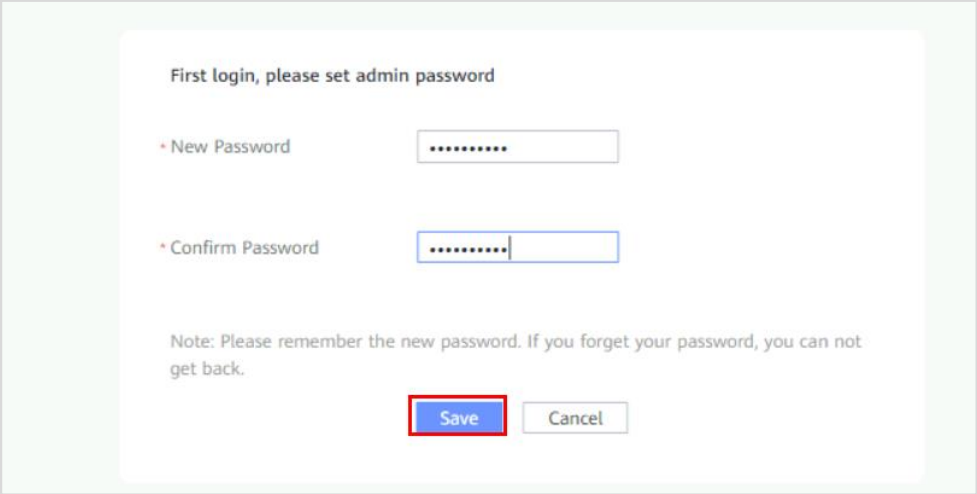


Figure 1-80 Saving the password

Step 3 After changing the password, go to the FusionAccess page.

Figure 1-81 Login page

Step 4 On the **Configure a virtualized environment** page, select **FusionCompute** for **Virtualization environment type**, configure related parameters as follows, and click **Next**.

Note:

- **Virtualization environment type**: Select **FusionCompute**.
- **FusionCompute IP Address**: Enter the IP address of the VRM node.
- **FusionCompute Port Number**: Enter **7070**.
- **SSL Port Number**: Enter **7443**.
- **Username**: Enter **vdisysman**.
- **Password**: Obtain it from FusionAccess Account List.
- **Protocol**: Select the protocol used for communication between FusionCompute and the ITA. You are advised to select **https**.

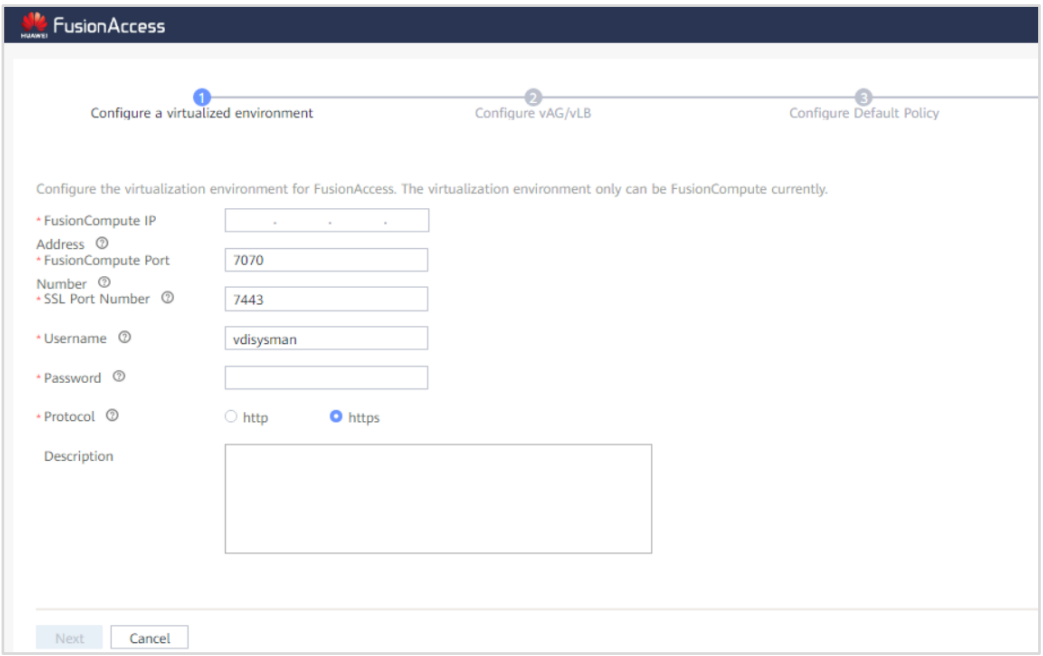


Figure 1-82 Interconnecting with the virtualization environment

Step 5 On the **Configure vAG/vLB** page, click **Add**. In the displayed dialog box, configure the parameters as follows and click **Next**.

Note:

- **Server IP Address**: Enter the service plane IP address of the vAG server.
- **Deployment Type**: Select **vAG+vLB**.
- **SSH Account**: The default value is **gandalf**.
- **Password**: Enter the password of the SSH account. Obtain it from "FusionAccess Account List".
- **Description**: (Optional) Describe the vAG.

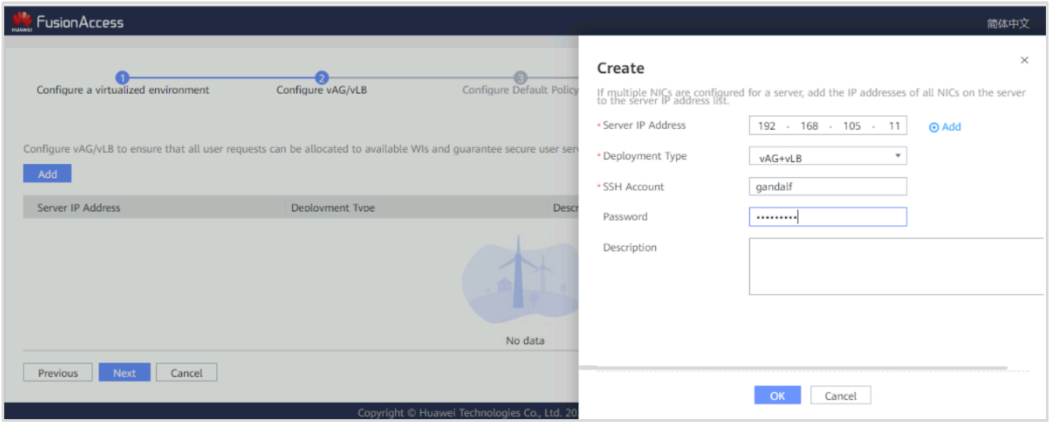


Figure 1-83 Configuring the vAG/vLB

Step 6 Configure the following parameters as required:

- **Service Access Gateway**: indicates whether to access a VM through the vAG. It is enabled by default.
- **Self-help Console Gateway**: indicates whether to access a VM from the self-help maintenance console. It is enabled by default.

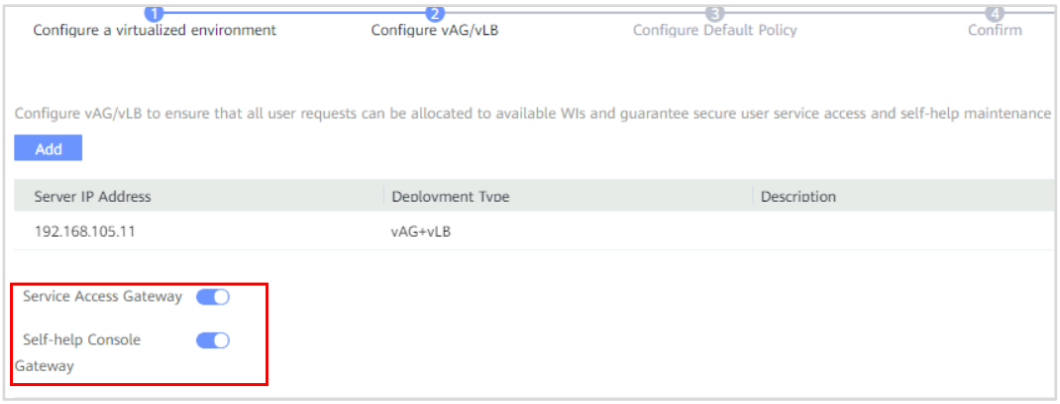


Figure 1-84 Configuring the service access gateway

Step 7 Configure the default policy.

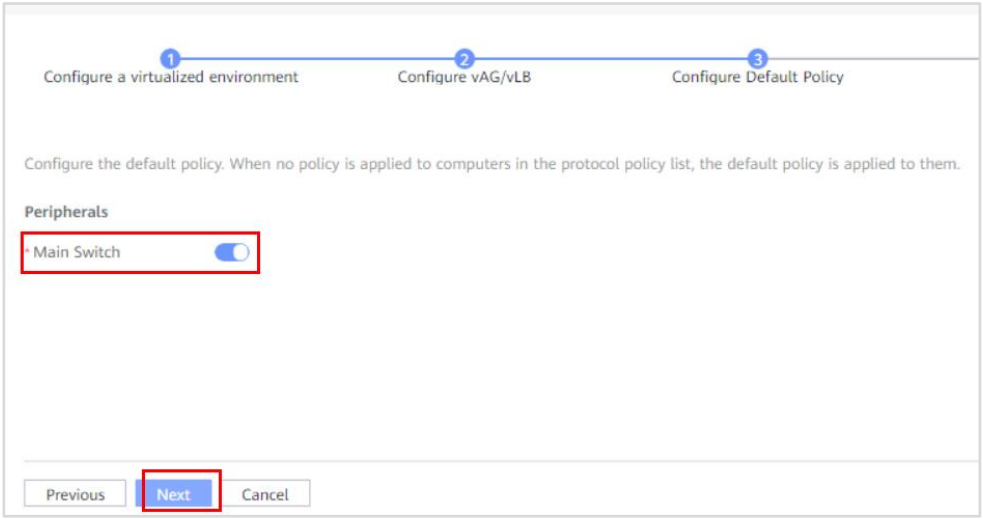


Figure 1-85 Configuring the default policy

Note:

By default, **Main Switch** for peripherals is enabled, and all peripherals can be directly used. You can modify the default policy.

Step 8 On the **Confirm** page, check each parameter and click **Next**. The system automatically performs the configuration. After the configuration is complete, the **FusionAccess Web Client** page is displayed.

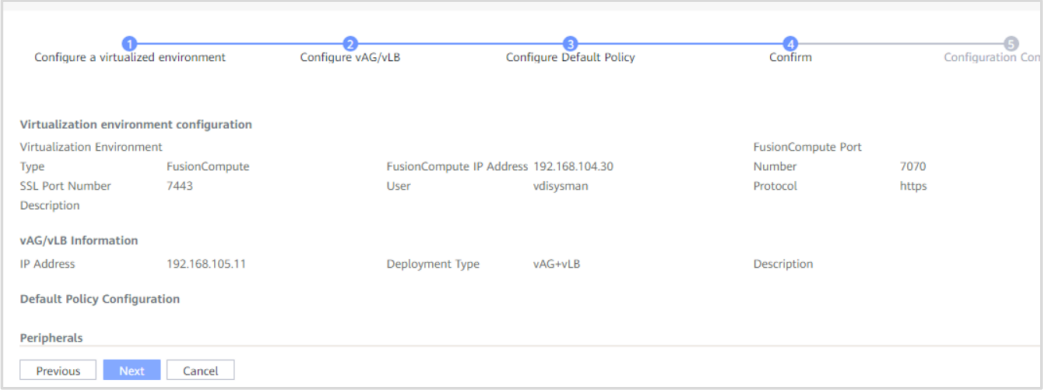


Figure 1-86 Confirming the configuration

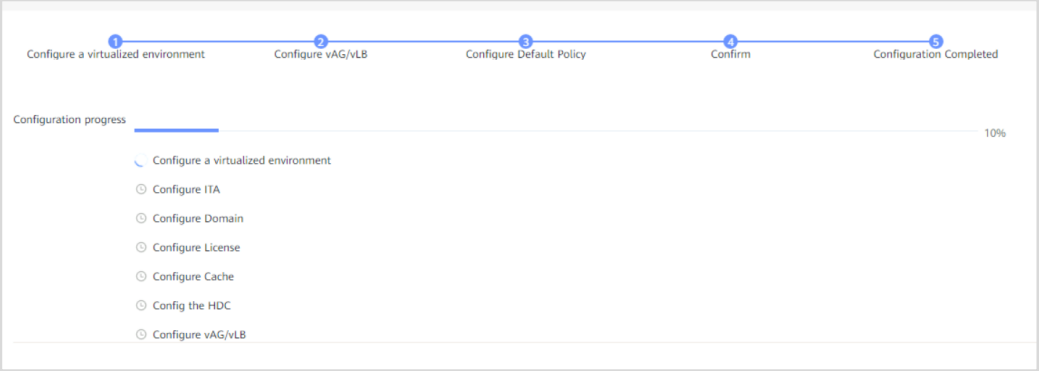


Figure 1-87 Configuration initialization started automatically

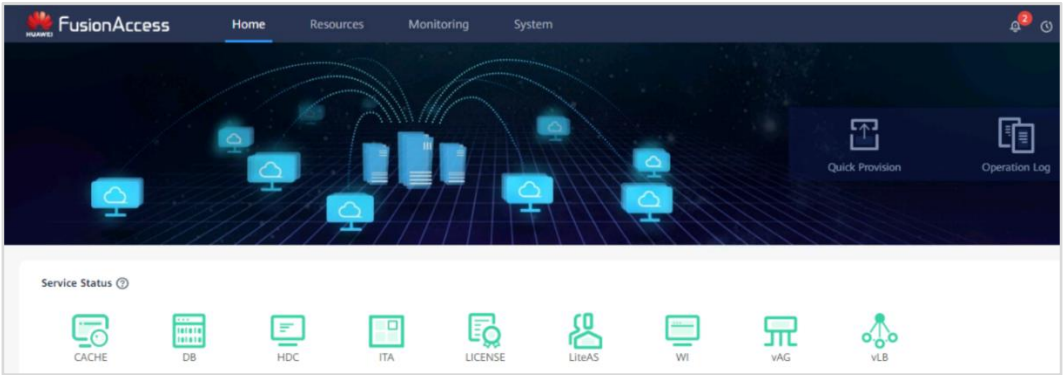


Figure 1-88 FusionAccess homepage

Step 9 On FusionAccess, choose **System** > **System Configuration** > **Authentication Configuration**, and click the **Windows AD** tab.

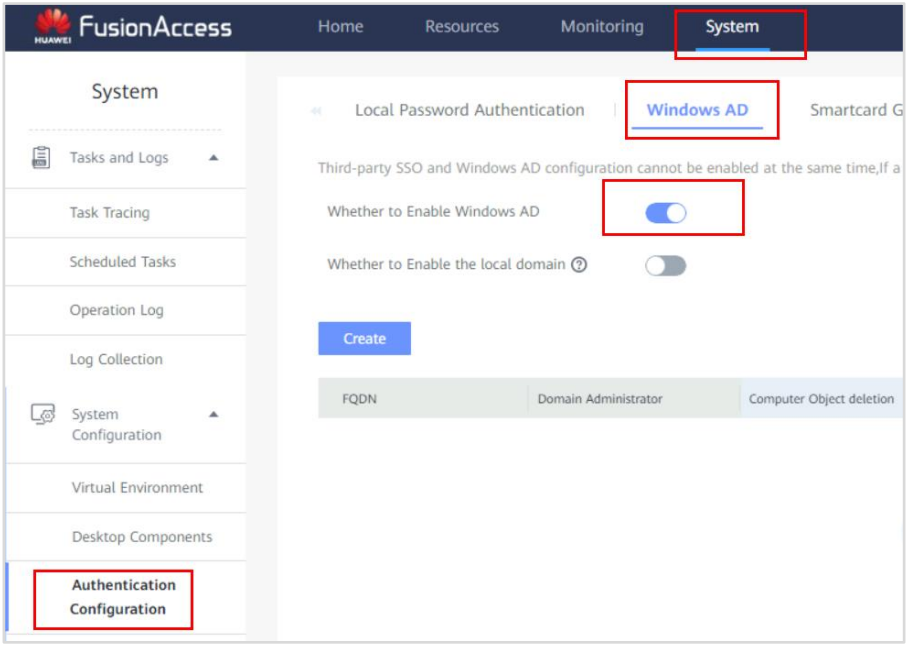


Figure 1-89 Accessing the Windows AD tab page

Step 10 Configure the connection to Windows AD.

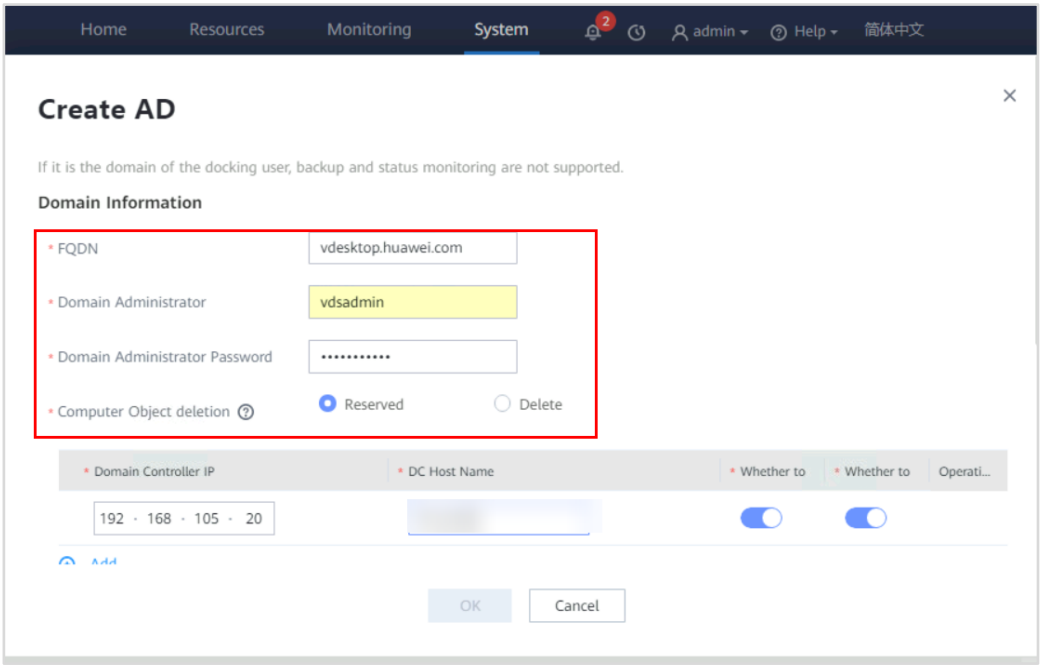


Figure 1-90 Configuring Windows AD

Note:

- **Whether to Enable Windows AD**: Enable this function.
- **FQDN**: Enter the name of the Windows AD domain controller.
- **Domain Administrator**: Enter the name of the administrator who accesses the Windows AD server.

- **Domain Administrator Password**: Enter the administrator password for login.
- **Domain Controller IP**: Enter the service plane IP address of the Windows AD server.
- **DC Host Name**: Enter the host name of the Windows AD server, for example, **FA-2016AD-01**.

1.3 Quiz

Why do we need to configure automatic recovery for a VM? What will happen if this function is not configured?

Answer: After the automatic recovery is configured for VMs, VMs can automatically recover if the FusionCompute storage network malfunctions, ensuring system reliability.

Otherwise, the VM may fail to recover automatically and the VM files cannot be read.

2 FusionAccess Service Provisioning

2.1 Overview

2.1.1 About This Exercise

This section describes how to create virtual desktop users on the AD/DNS/DHCP server, create VMs and install the system on FusionCompute, configure and encapsulate the VM system using Huawei tools (full copy and linked clone modes are available based on the encapsulation mode), and return to FusionCompute to create a template. After the template is created, create command rules, VM groups, and desktop groups on FusionAccess, and quickly provision desktops (including full copy and linked clone desktops). After the provisioning is successful, log in to the desktops from an SC.

2.1.2 Objectives

Upon completion of this exercise, you will understand:

- Functions of vAG and vLB
- Differences between linked clone desktops and full copy desktops
- Desktop group types: private desktop groups, static pool desktop groups, and dynamic pool desktop groups
- How to create a login user
- How to encapsulate linked clone and full copy templates
- How to perform operations on desktop groups
- How to name a VM
- How to perform operations on VM groups
- How to perform quick provisioning operations
- How to log in to the SC

2.1.3 Procedure

Figure 2-1 Flowchart

2.2 Exercise Configuration

2.2.1 Creating a VM User

2.2.1.1 Creating an Organizational Unit (OU)

Step 1 Log in to FusionCompute and log in to the VM where the AD/DNS/DHCP resides using VNC.

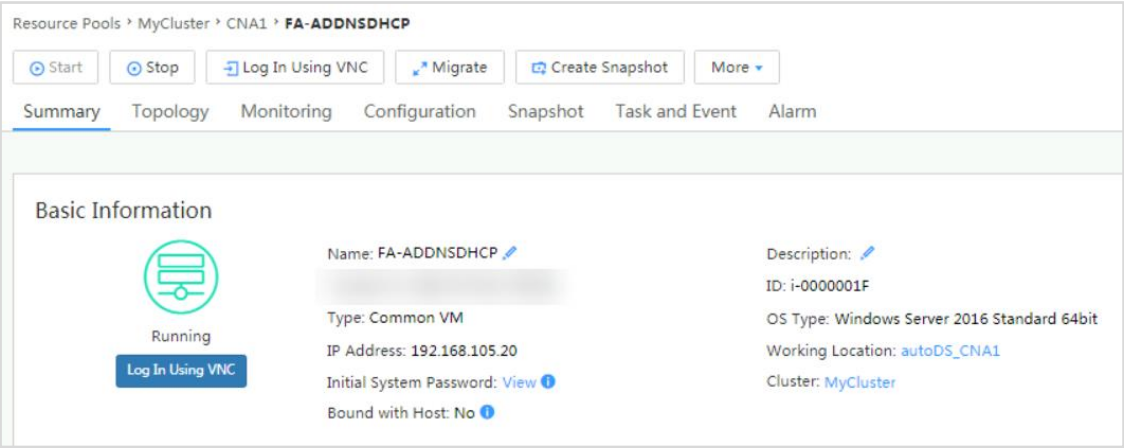


Figure 2-2 Logging in to the VM where the AD/DNS/DHCP resides using VNC

Step 2 Choose **Start** > **Administrative Tools** > **Active Directory Users and Computers**. The **Active Directory Users and Computers** window is displayed.

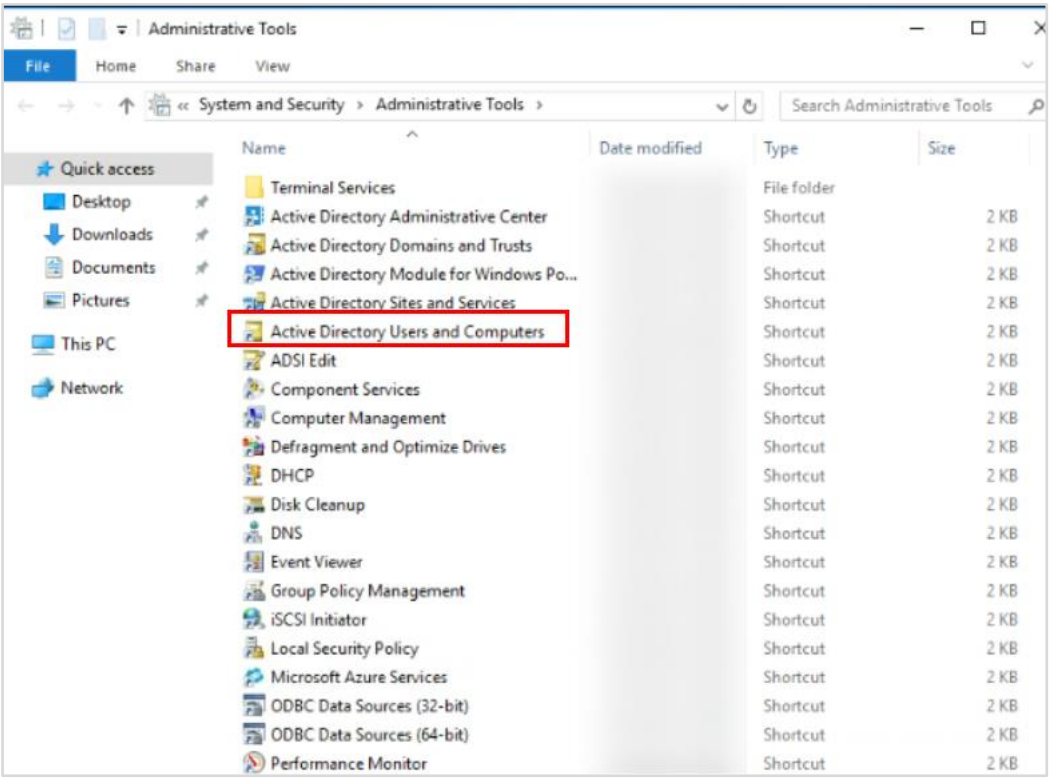


Figure 2-3 Opening the Active Directory Users and Computers window

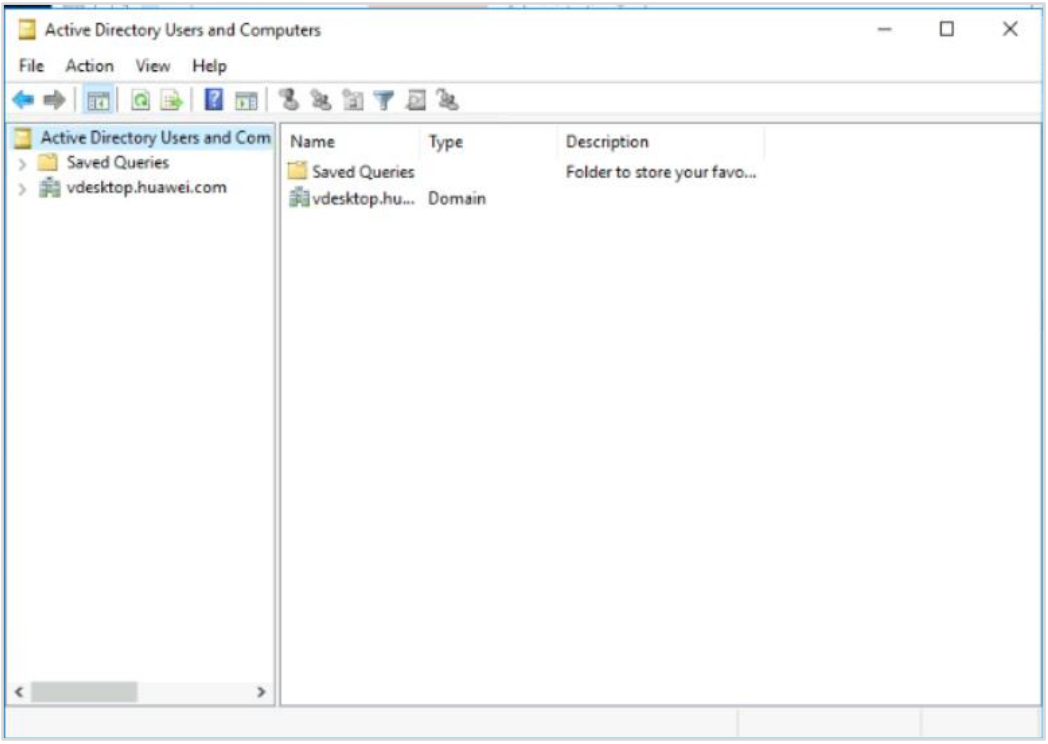


Figure 2-4 Active Directory Users and Computers window

Step 3 In the navigation pane on the left, right-click **vdesktop.huawei.com** and choose **New** > **Organizational Unit**.

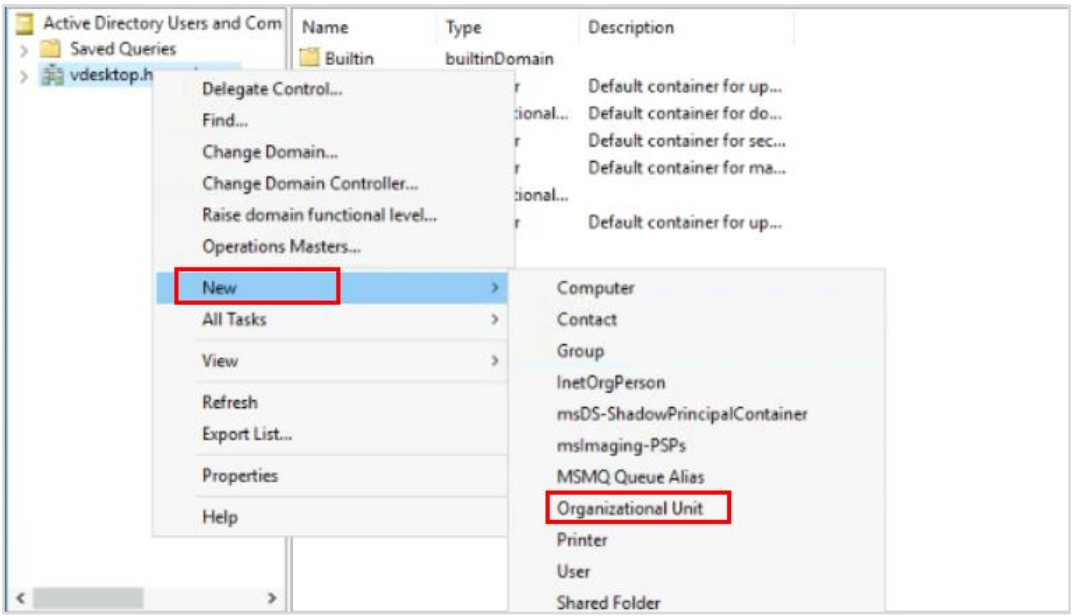


Figure 2-5 Creating an organizational unit

Step 4 The **New Object - Organizational Unit** window is displayed. Enter **UserOU** in the **Name** text box, select **Prevent container from being accidental deletion**, and click **OK**.

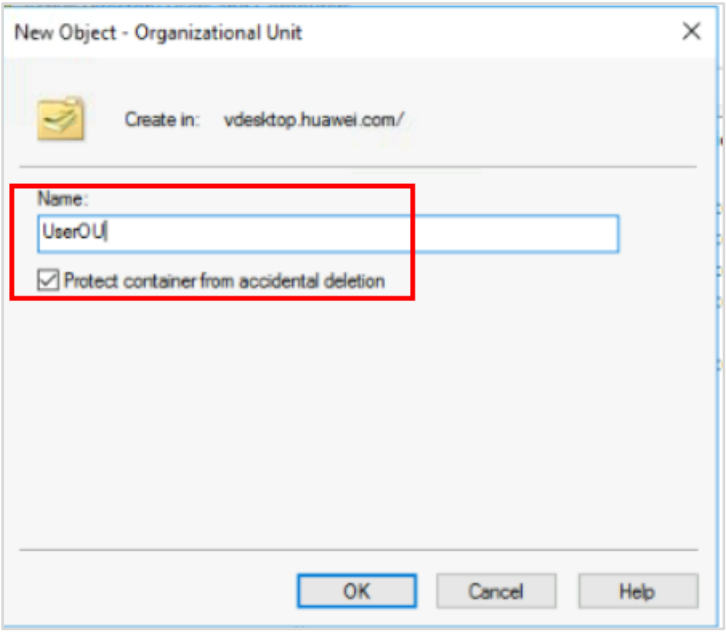


Figure 2-6 Creating an OU

Note:

If the system displays a message indicating that an OU named **UserOU** already exists, skip this step and proceed with the following steps to create a user group.

2.2.1.2 Creating a User Group

Step 1 In the navigation pane on the left of the **Active Directory Users and Computers** dialog box, right-click the name of the created user OU and choose **New** > **Group**.

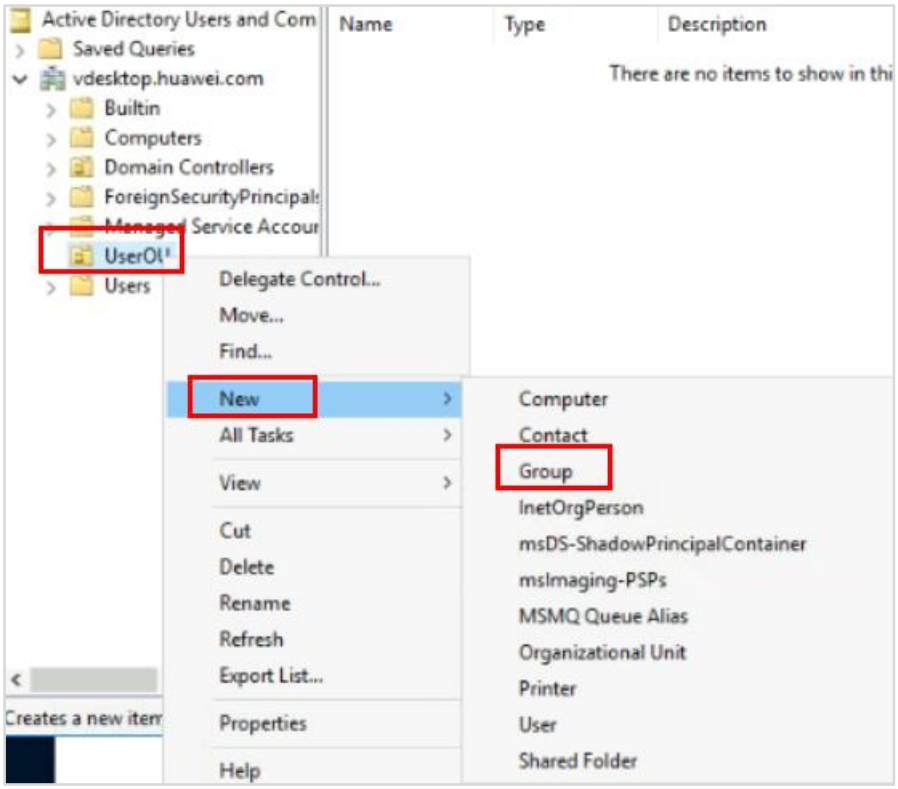


Figure 2-7 Creating a user group 1

Step 2 The **New Object - Group** window is displayed. Set **Group name**, retain the default values for **Group scope** and **Group type**, and click **OK**.

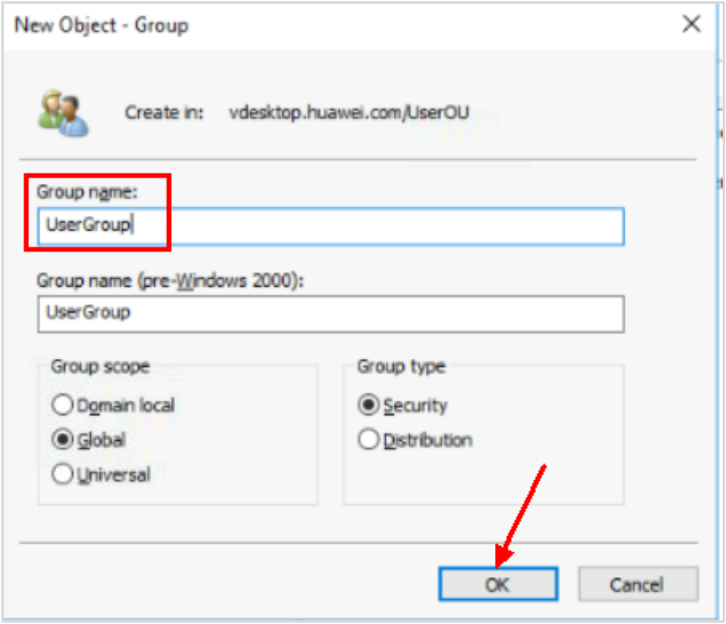


Figure 2-8 Creating a user group 2

2.2.1.3 Creating a Domain User

Step 1 In the navigation pane on the left of the **Active Directory Users and Computers** dialog box, right-click the name of the created user OU and choose **New** > **User**.

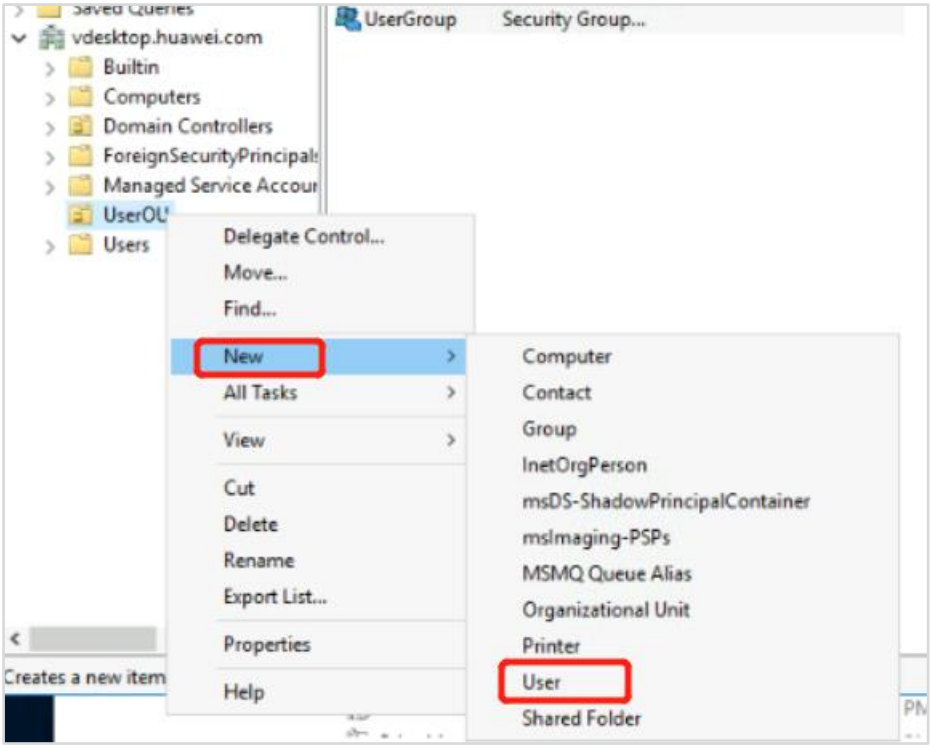


Figure 2-9 Creating a domain user

Step 2 In the displayed **New Object - User** window, configure registration information of the domain user and click **Next**.

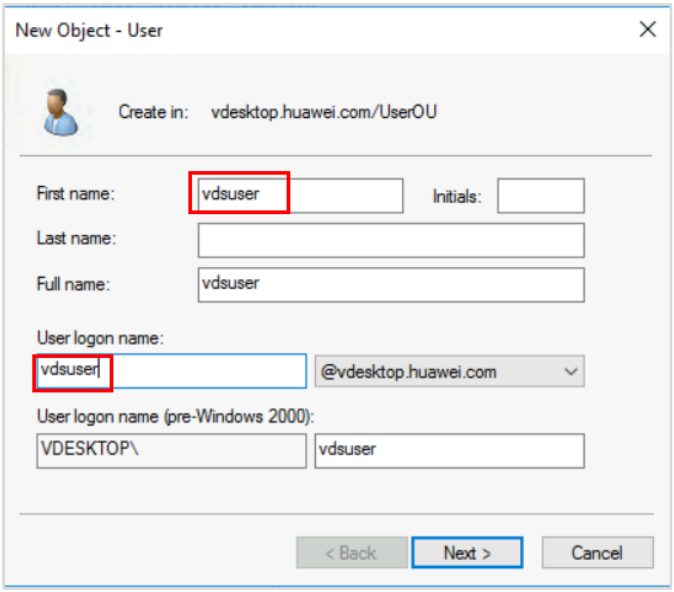


Figure 2-10 Configuring registration information of the domain user

Step 3 In **Password** and **Confirm password**, enter the password of the domain user. Deselect **User must change password at next logon**, select **User cannot change password** and **Password never expires**, and click **Next**.

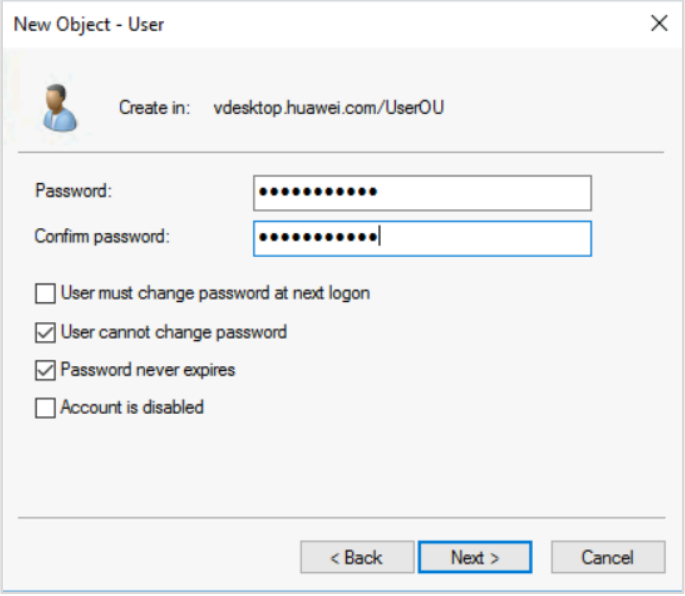


Figure 2-11 Entering the password of the domain user

Step 4 Confirm the information and click **Finish**.

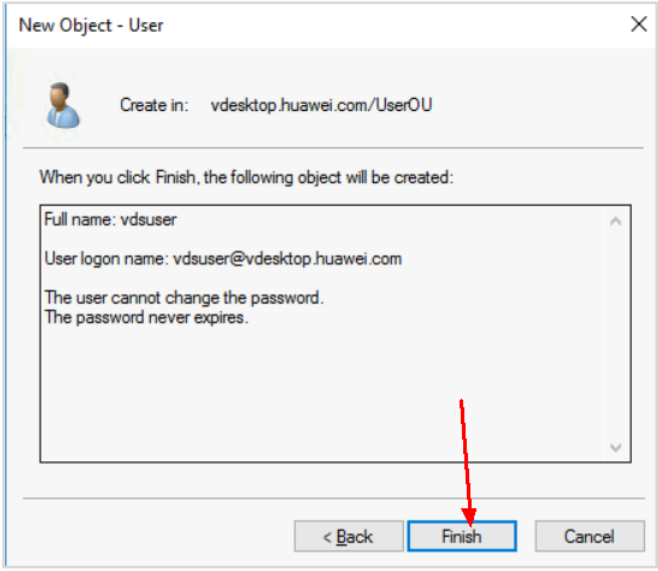


Figure 2-12 Confirming the information

Step 5 In the right pane of **UserOU**, right-click the target user and choose **Add to a group**.

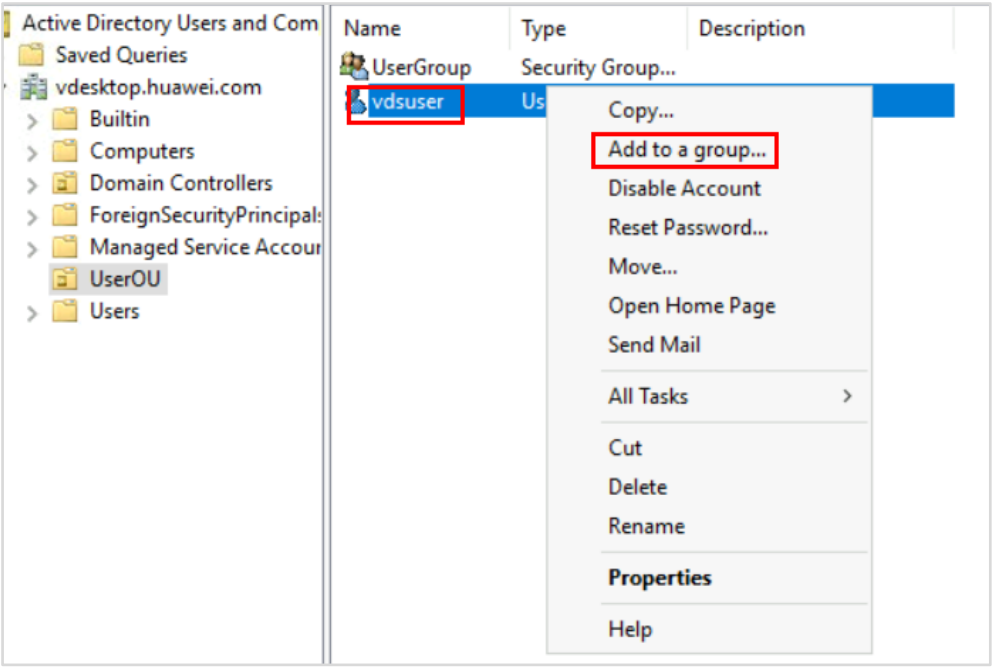


Figure 2-13 Adding the user to a group

Step 6 In the displayed **Select Groups** window, enter the user group name in **Enter the object names to select** and click **OK**.

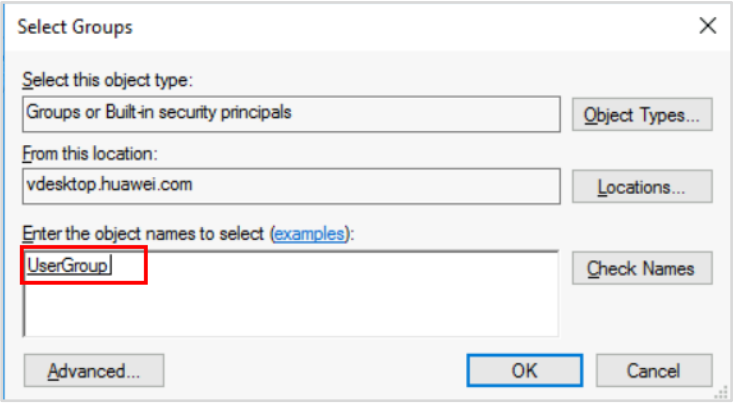


Figure 2-14 Entering a user group name

Step 7 In the displayed dialog box, click **OK**.

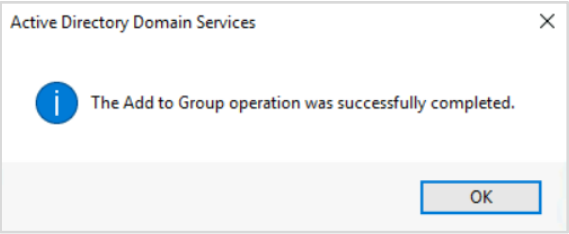


Figure 2-15 Completing the operation

2.2.2 Creating a VM Template

2.2.2.1 Creating a Bare VM

Step 1 Log in to FusionCompute and click **Create VM** on the homepage.

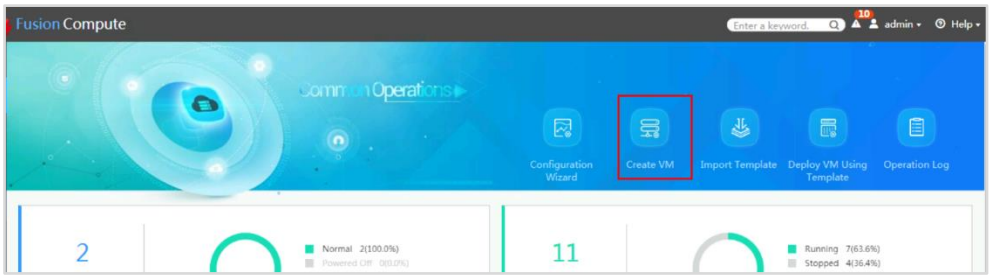


Figure 2-16 Creating a VM

Step 2 In the **Create VM** dialog box displayed, click **Next** in the **Select Creation Mode** step.

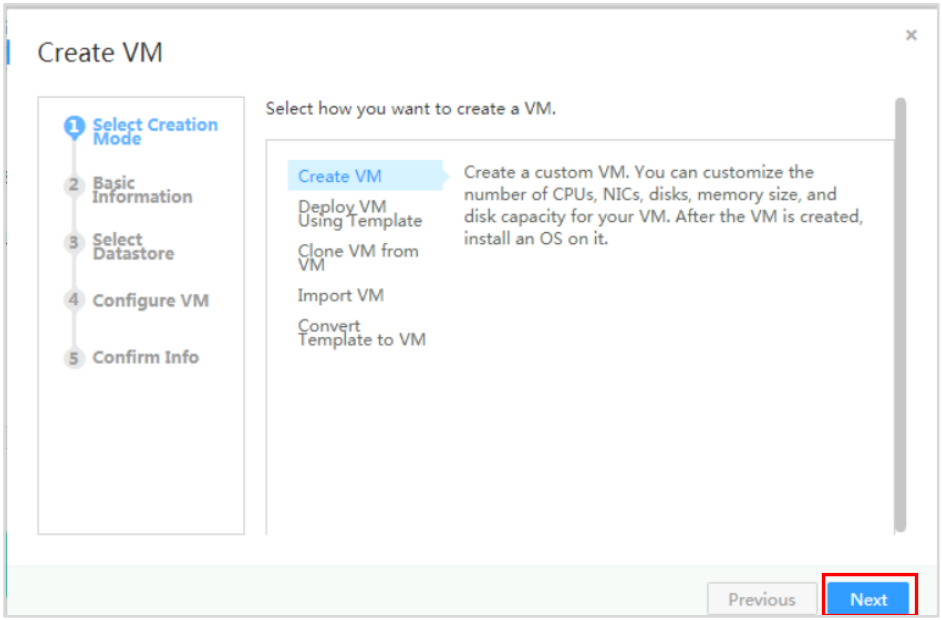


Figure 2-17 Creation mode

Step 3 When configuring **Basic Information**, change name to **vDesktop Template**. For **Set Compute Resource**, select **MyCluster** and click **OK**. Set **OS** to **Windows** and **OS Version** to **Windows 10 64bit**, and click **Next**.

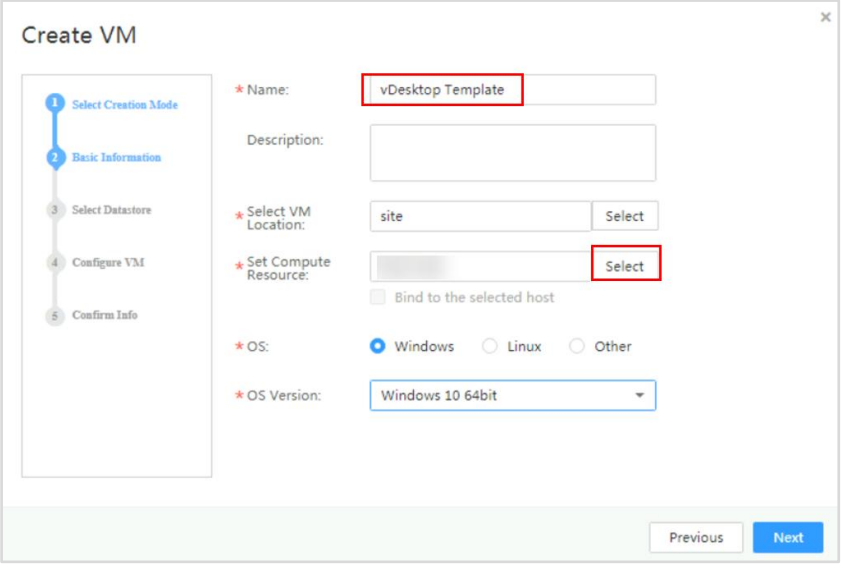


Figure 2-18 Basic information

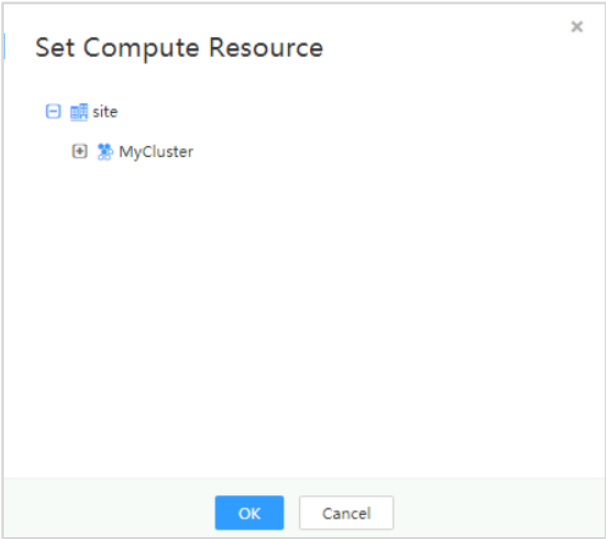


Figure 2-19 Selecting compute resources

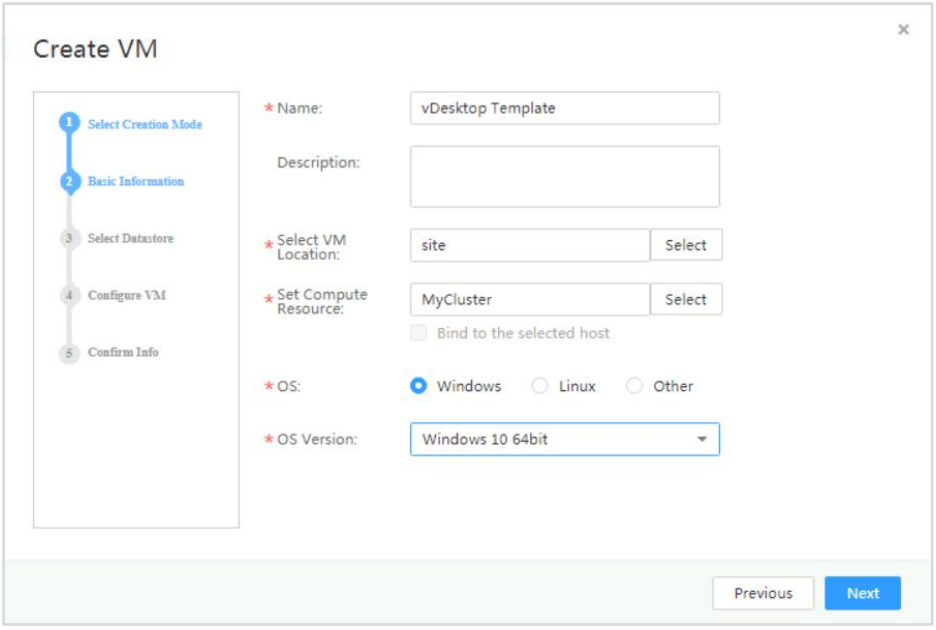


Figure 2-20 Confirming the basic information

Step 4 In the **Select Datastore** step, select **IP-SAN** and click **Next**.

Note:

You can select any available datastore for the VM.

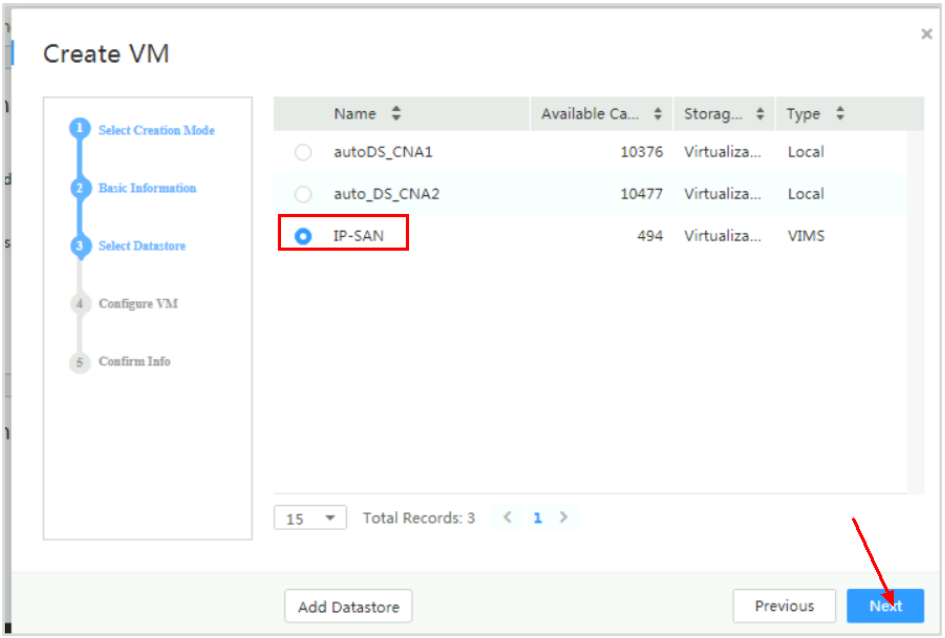


Figure 2-21 Selecting datastore

Step 5 In the **Configure VM** step, configure the VM hardware information and options, and click **Next**.

- **CPU**: Configure at least four CPUs for the VM.
- **Memory**: Configure at least 4 GB for the VM.

- **Disk 1**: Configure at least 40 GB for the VM and set **Configuration Mode** to **Thin provisioning**.
- **NIC 1**: Select a service port group.

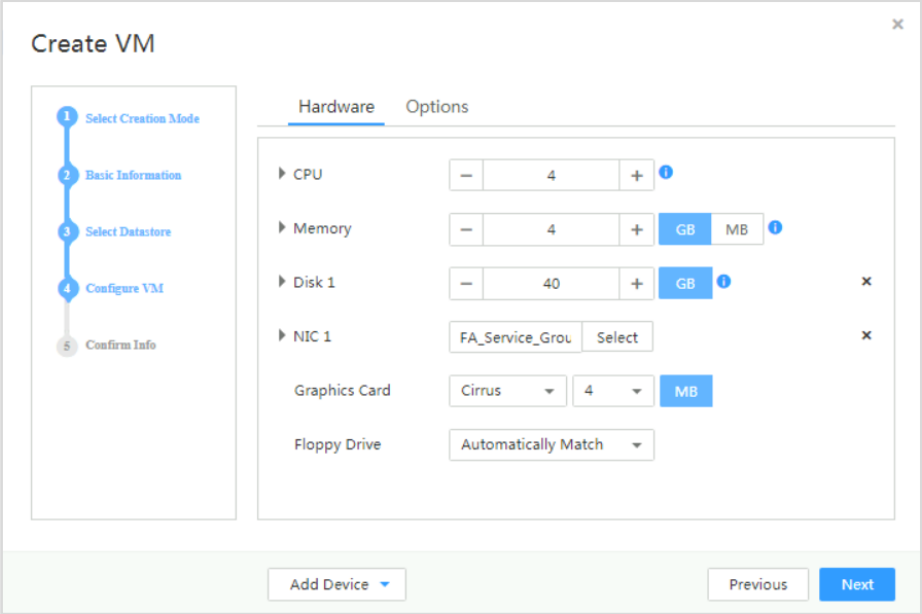


Figure 2-22 Configuring NICs

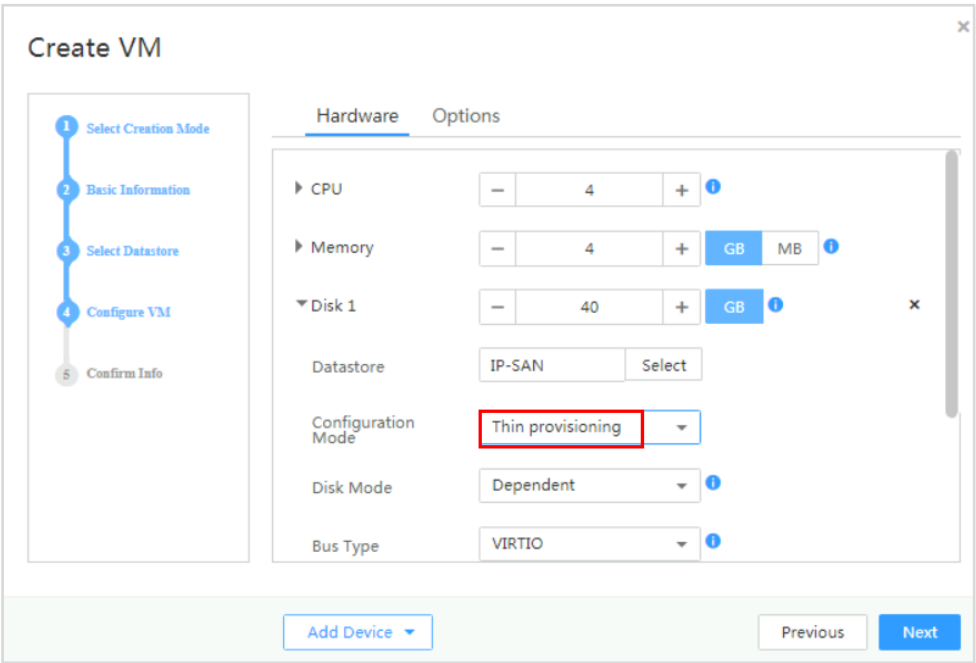


Figure 2-23 Configuring disks

Note:

If the number of CPU cores is adjusted to 4, a message is displayed indicating that the adjustment cannot be performed. In this case, you need to set **Number of Cores per Socket** to **2**.

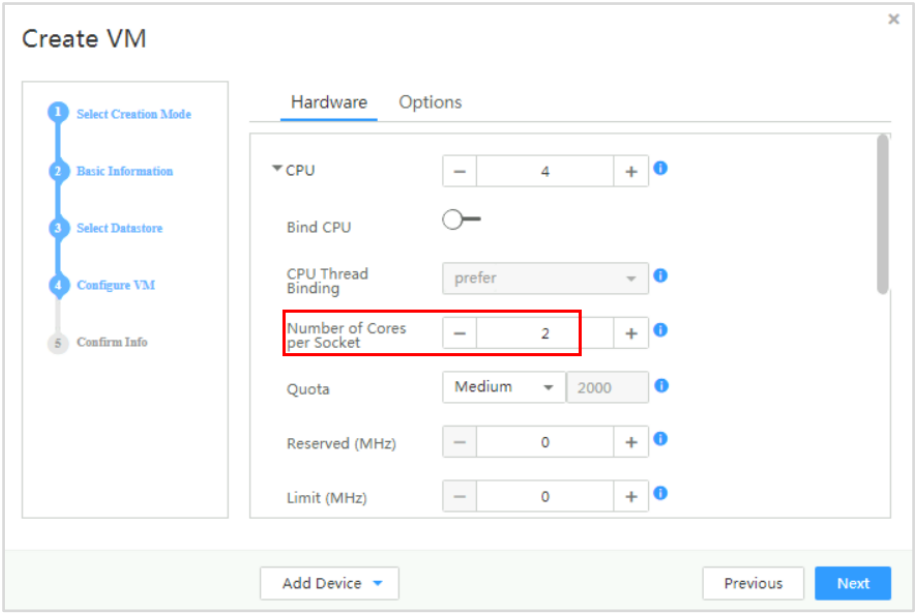


Figure 2-24 Configuring the CPU

Step 6 In the **Confirm Info** step, select **Start VM immediately after creation** and click **OK**. The VM tab page is displayed.

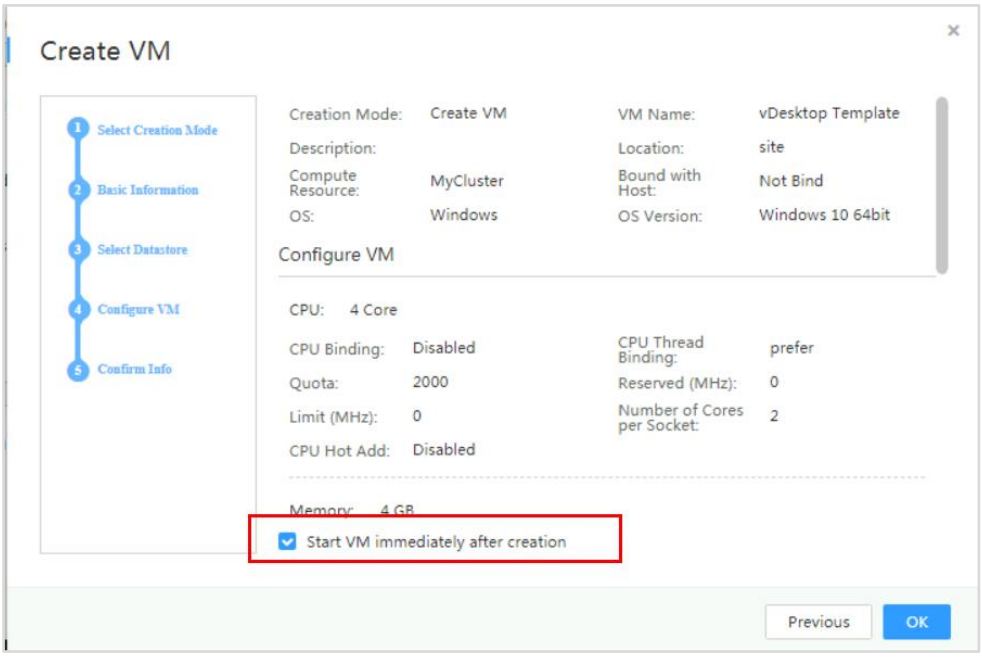


Figure 2-25 Confirming the information

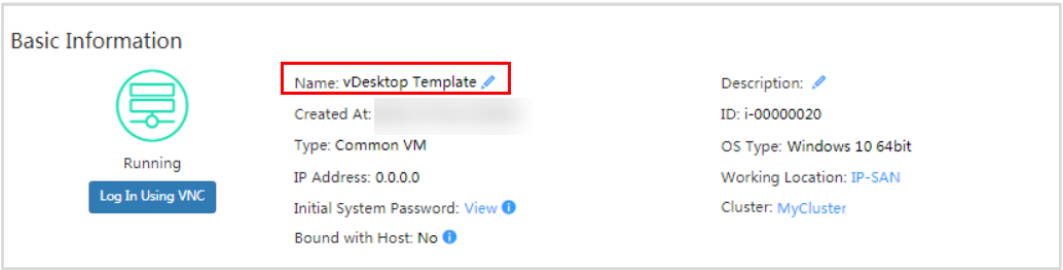


Figure 2-26 Confirming the creation

2.2.2.2 Installing an OS on the VM

Step 1 Log in to FusionCompute. On the **Resource Pools** page, choose **ManagementCluster** > **vDesktop Template**. Click the **Configuration** tab, choose **CD/DVD-ROM Drive**, set **Mount CD/DVD-ROM Drive Type** to **Mount Local CD/DVD-ROM Drive**, and click **OK**.

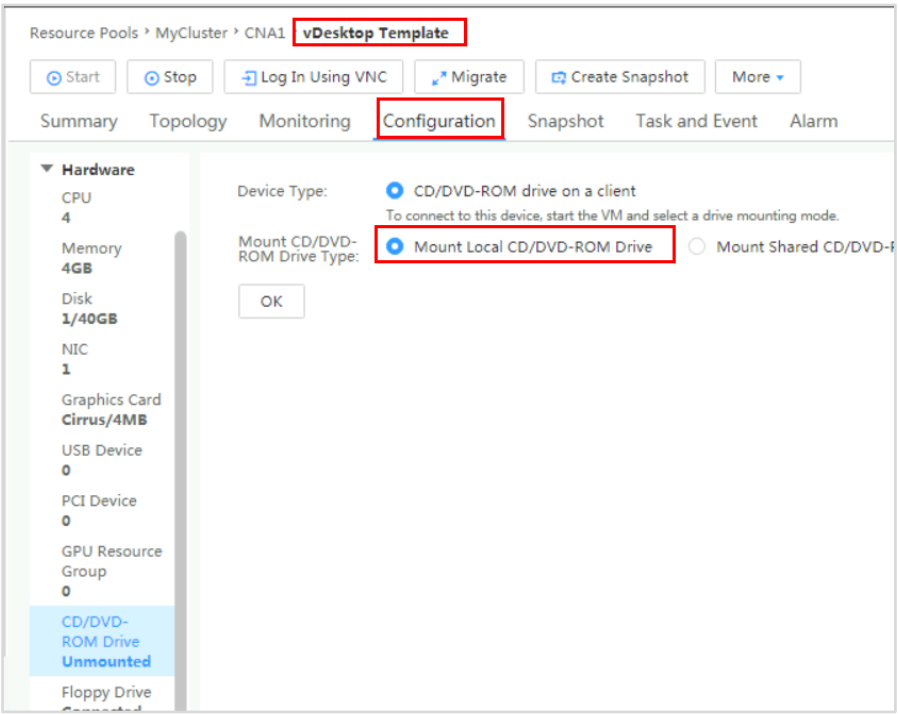


Figure 2-27 Mounting a CD/DVD-ROM drive

Step 2 In **File(*.iso)**, click **Browse**, select the ISO file stored in the local PC, select **Restart the VM now to install the OS**, and click **OK**.

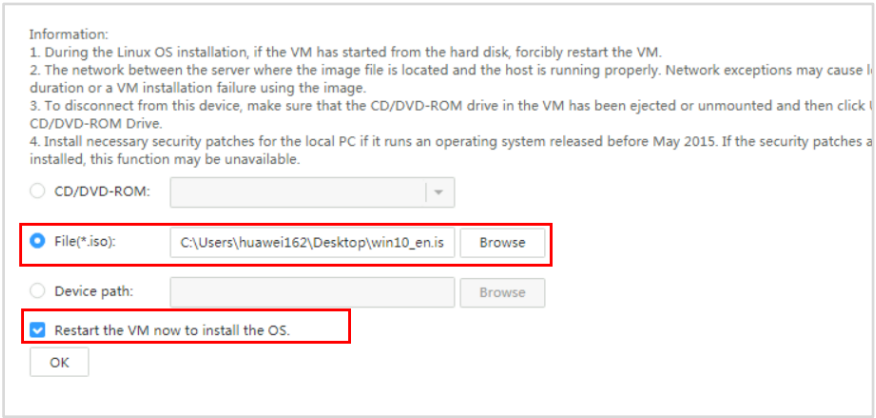


Figure 2-28 Selecting the ISO file

Step 3 After the CD/DVD-ROM drive is mounted, the **Information** dialog box is displayed. Click **OK**.

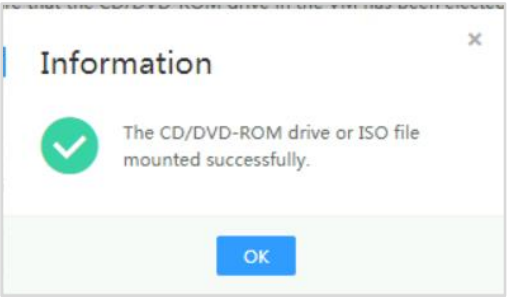


Figure 2-29 Confirming the mounting

Step 4 Return to the VM page and click **Log In Using VNC**.

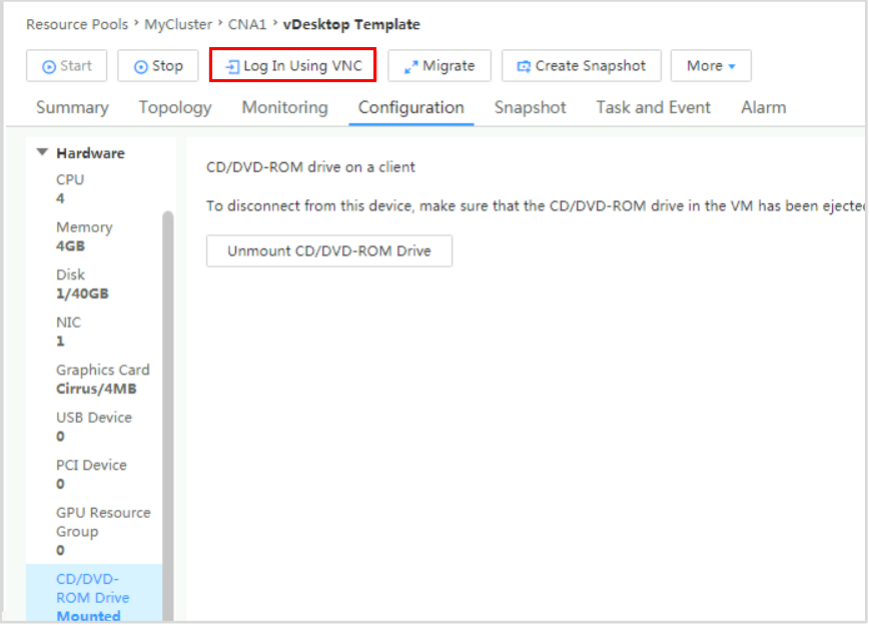


Figure 2-30 Logging in using VNC

Step 5 On the VM page, install the VM OS as prompted.

Step 6 Unmount the CD/DVD-ROM drive.

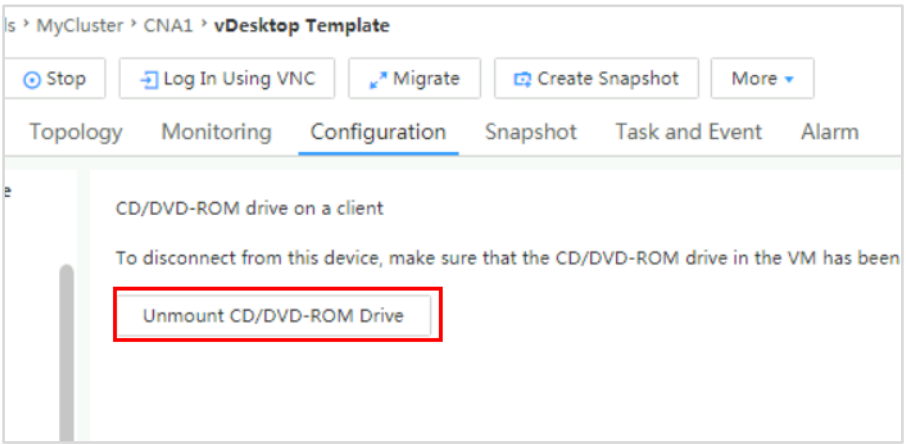


Figure 2-31 Unmounting the CD/DVD-ROM drive

Step 7 After the unmounting, the **Information** dialog box is displayed. Click **OK**.

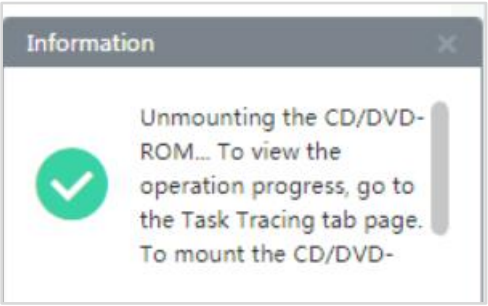


Figure 2-32 Confirming the unmounting

Step 8 On the VM OS, click **Start** in the lower left corner of the desktop and enter **compmgmt.msc** to open the **Computer Management** window.

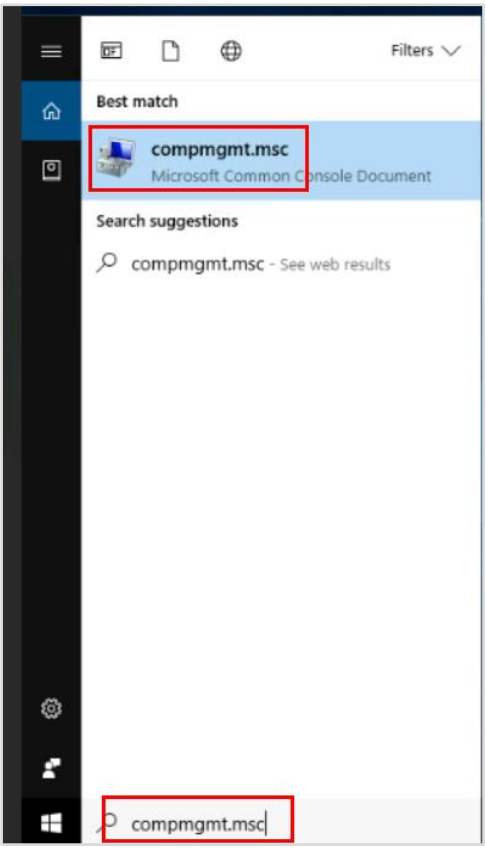


Figure 2-33 Opening the Computer Management window

Step 9 In the navigation pane on the left of the **Computer Management** window, choose **Computer Management (Local)** > **System Tools** > **Local Users and Groups**, and select **Users**. In the right pane, right-click **Administrator** and select **Properties**.

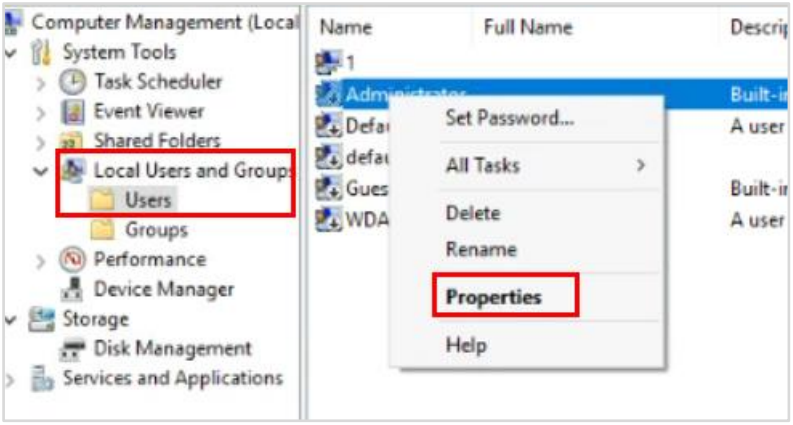


Figure 2-34 Selecting properties

Step 10 In the displayed **Administrator Properties** dialog box, deselect **Account is disabled** on the **General** tab and click **OK**. The administrator account has been activated, and its default password is empty.

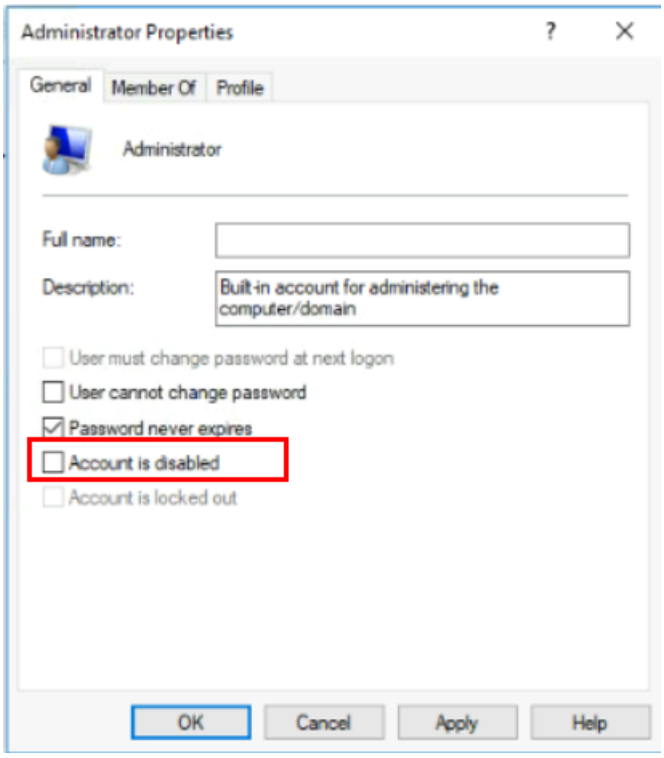


Figure 2-35 Activating the administrator account

Step 11 Right-click **Administrator** and select **Set Password**.

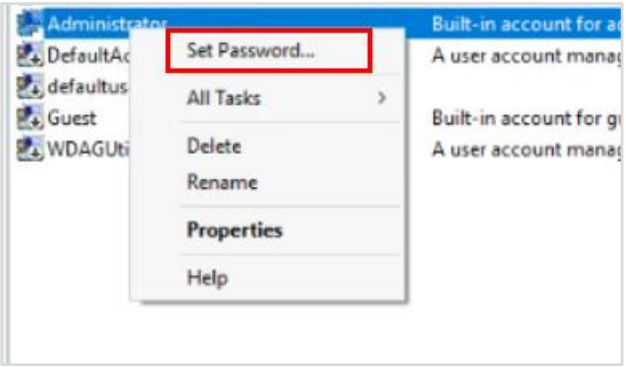


Figure 2-36 Setting a password

Step 12 In the displayed **Set Password for Administrator** dialog box, click **Proceed**.

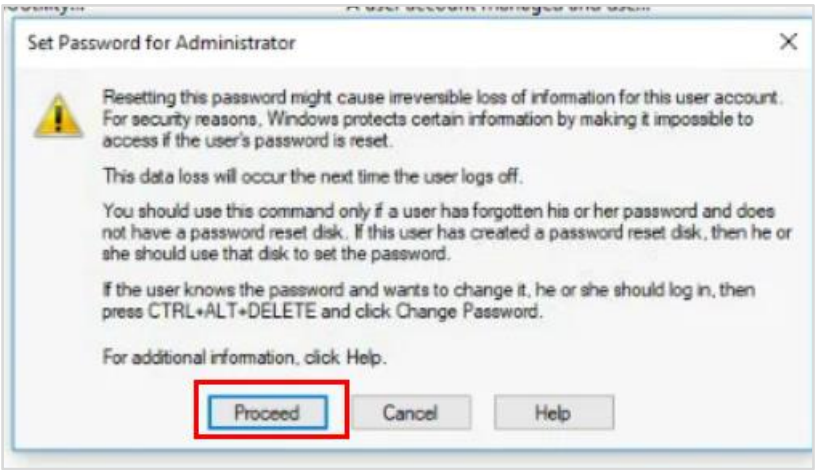


Figure 2-37 Clicking Proceed

Step 13 Set the password as required, and click **OK**.

Note: You are advised to set a simple password.

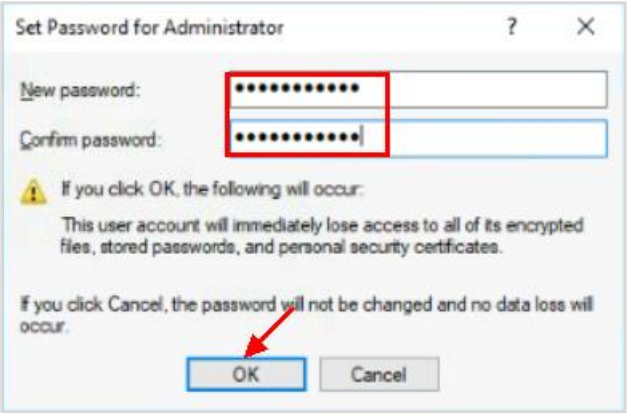


Figure 2-38 Setting a password for the administrator account

Step 14 On the displayed **Local Users and Groups** dialog box, click **OK**.

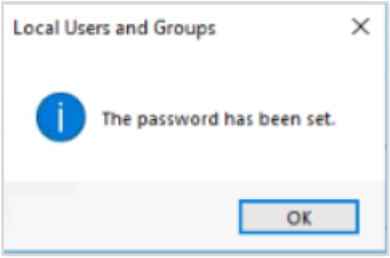


Figure 2-39 Completing the password settings

Step 15 Click **Start** in the lower left corner of the desktop. In the right pane, click the user button shown in the following figure and select **Sign Out**.

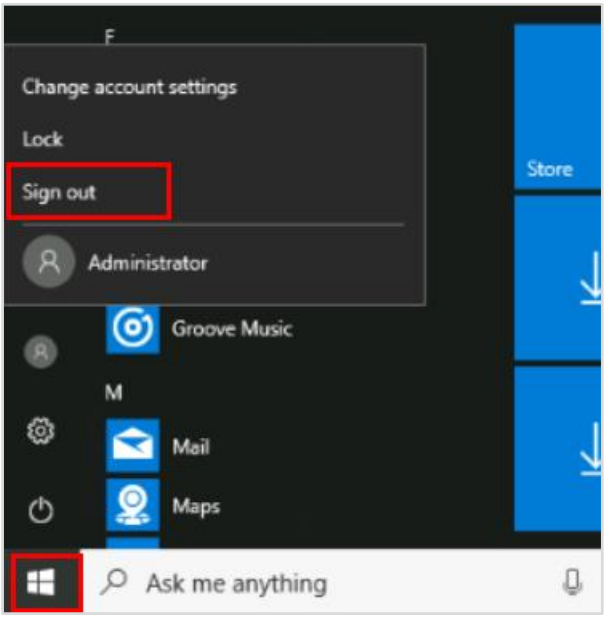


Figure 2-40 Selecting Sign out

Step 16 Log in to the VM as user **Administrator**.

2.2.2.3 Configuring the VM OS

Step 1 Log in to FusionCompute. On the **Resource Pools** page, right-click the installed VM in **mycluster** and choose **Tools** > **Mount Tools**.

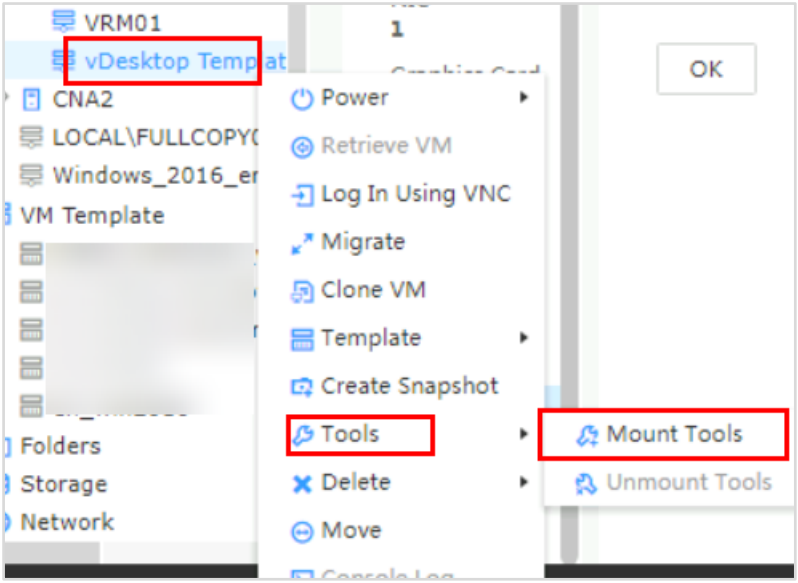


Figure 2-41 Mounting Tools

Step 2 In the **Information** dialog box displayed, click **OK**.

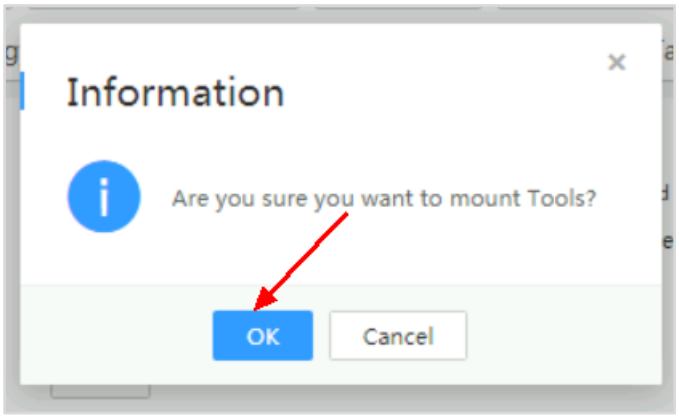


Figure 2-42 Confirming the mounting

Step 3 Go to the VM CD-ROM directory. Right-click **Setup** and select **Run as administrator**. Install the software as prompted. During the installation, retain the default settings.

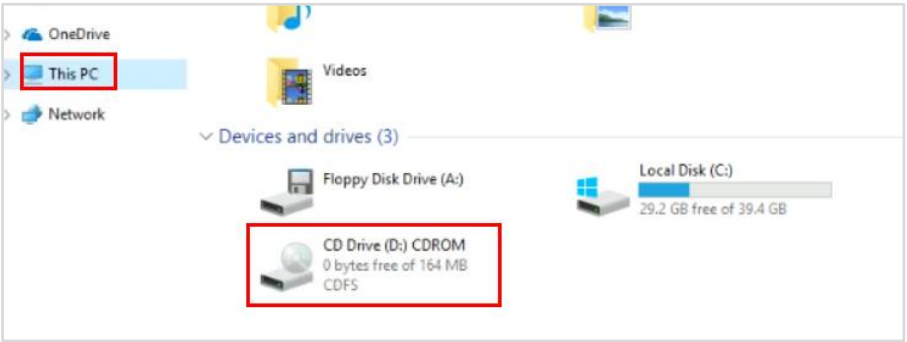


Figure 2-43 VM CD-ROM directory

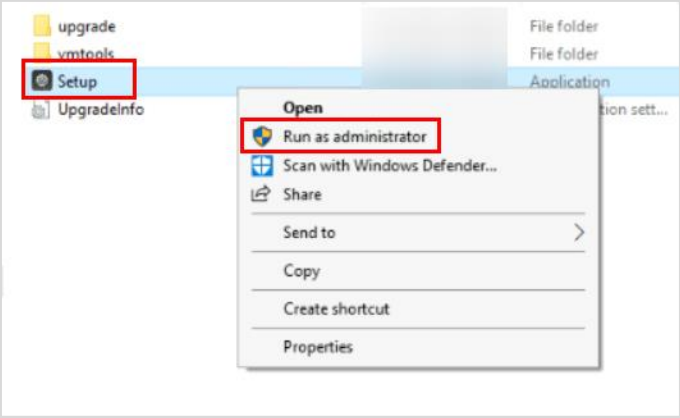


Figure 2-44 Running setup

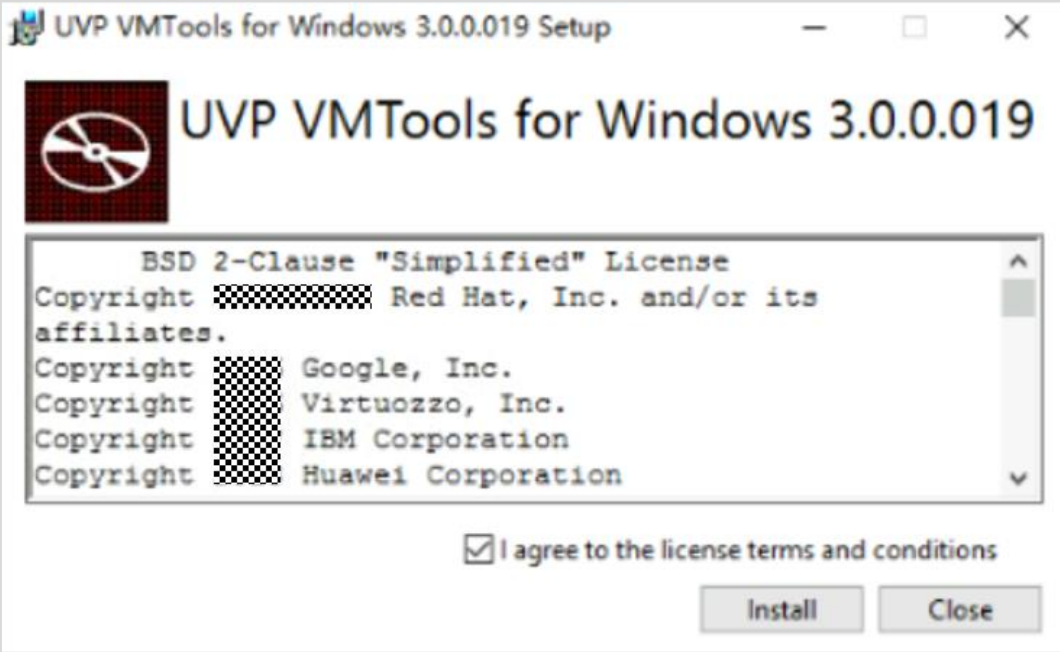


Figure 2-45 Starting the installation

Step 4 After the software is installed, restart the VM as prompted.

Figure 2-46 Reboot

Step 5 After the VM is restarted, shut down the VM.

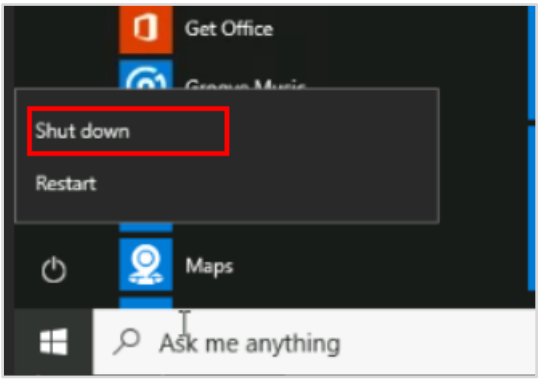


Figure 2-47 Powering off the VM

Step 6 On FusionCompute, right-click the stopped VM and choose **Template** > **Convert to Template**.

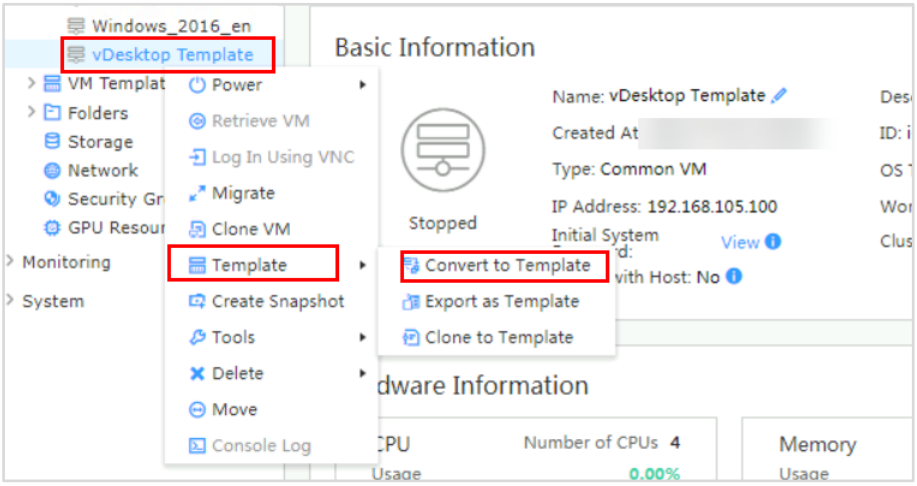


Figure 2-48 Converting a VM into a template

Step 7 In the **Information** dialog box displayed, click **OK**.

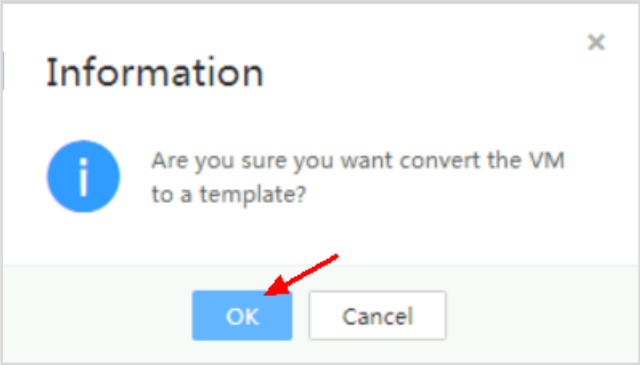


Figure 2-49 Completing the conversion

2.2.2.4 Creating a Full Copy VM Template

Step 1 In the navigation pane on the left of FusionCompute, click **VM Template**, right-click the template created in section 1.2.2, and click **Deploy VM Using Template**.

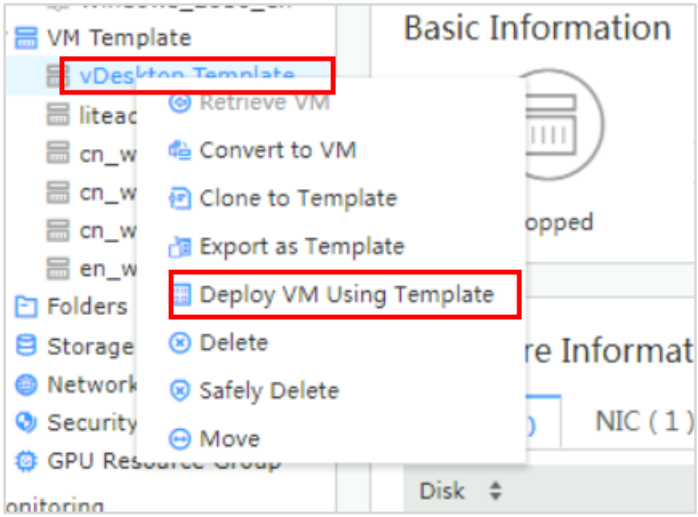


Figure 2-50 Deploying a VM using a template

Step 2 In the **Create VM** dialog box displayed, set **Name** to **FullyCopy Template** in the **Basic Information** step, and click **Next**.

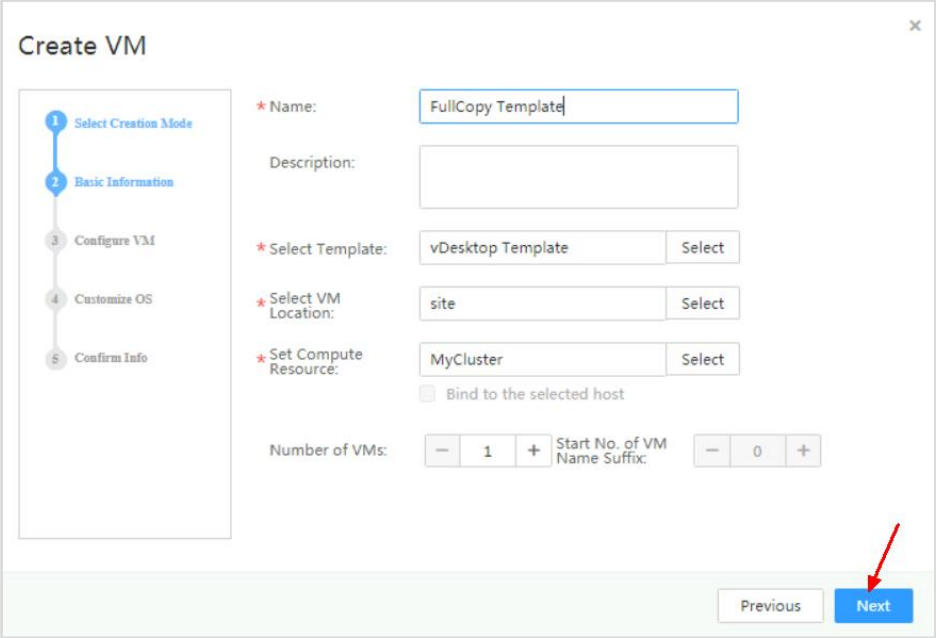


Figure 2-51 Basic information

Step 3 In the **Configure VM** step, retain the default values for other parameters. You can also modify the full copy VM specifications as planned (the disk specifications cannot be changed), and click **Next**.

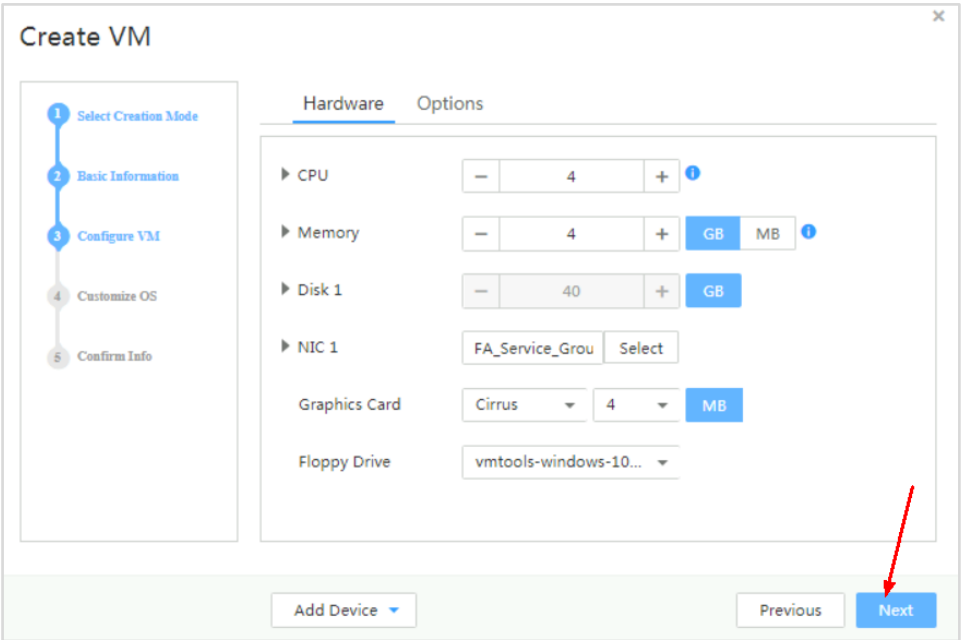


Figure 2-52 VM configuration

Step 4 In the **Customize OS** step, select **Do not customize** for **VM Attributes**, deselect **Generate Initial Password**, and click **Next**.

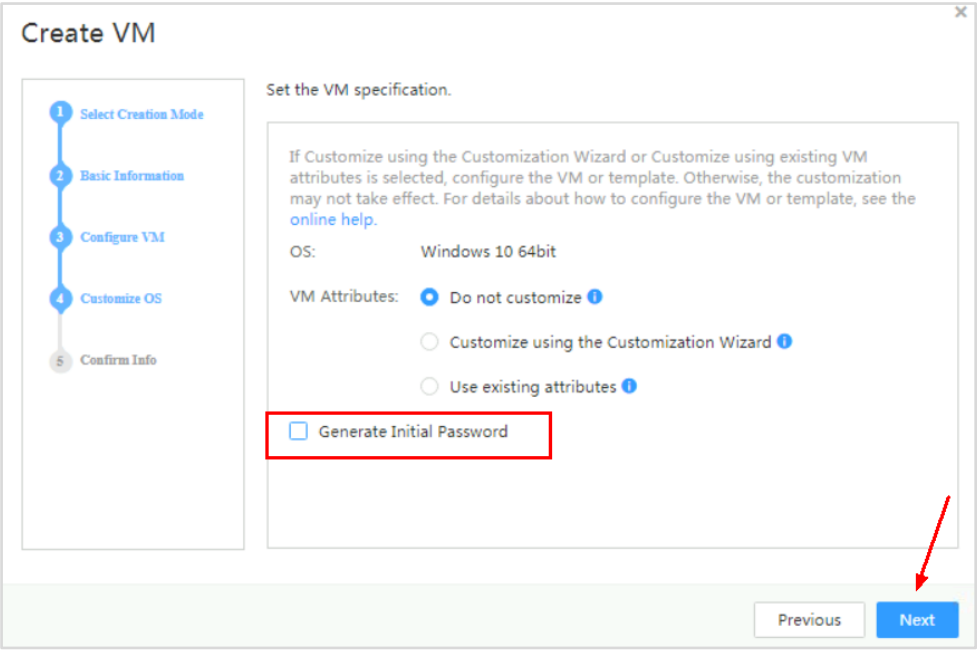


Figure 2-53 Customizing the OS

Step 5 In the **Confirm Info** step, select **Start VM immediately after creation** and click **OK**.

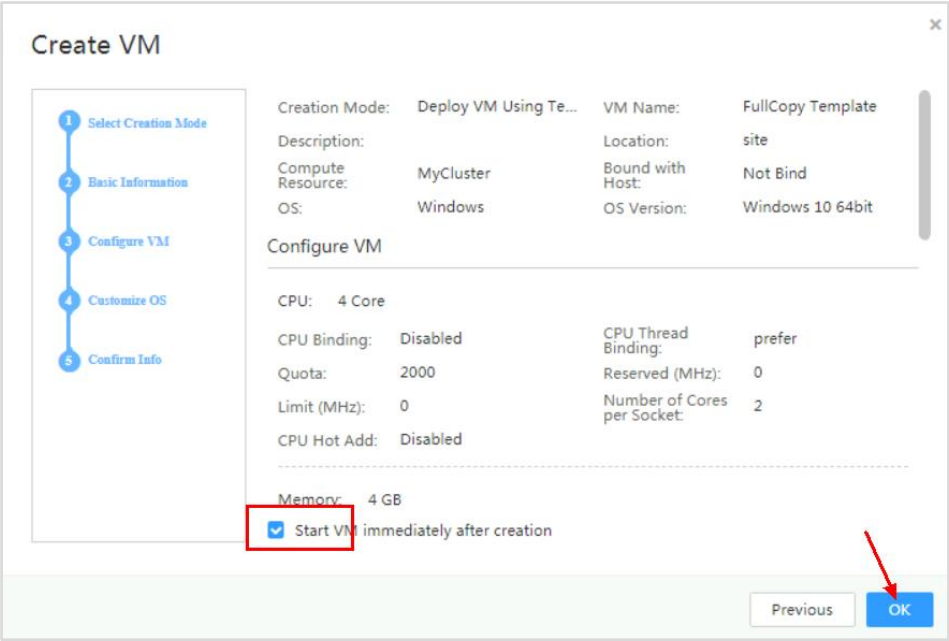


Figure 2-54 Confirming the information

Step 6 Log in to FusionCompute. On the **Resource Pools** page, select **ManagementCluster**, click the created VM, choose **Configuration** > **CD/DVD-ROM Drive**, set **Mount CD/DVD-ROM Drive Type** to **Mount Local CD/DVD-ROM Drive**, and click **OK**.

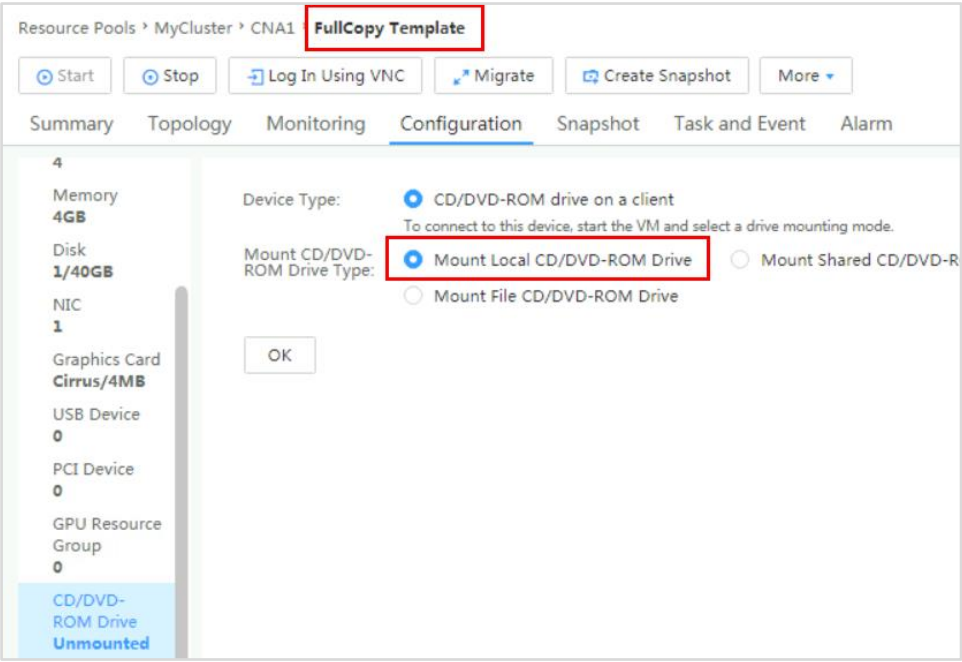


Figure 2-55 Mounting a CD/DVD-ROM drive

Step 7 In the displayed window, select **File(*.iso)**, click **Browse**, select the template tool image **FusionAccess_WindowsDesktop_Installer_8.0.2.iso** stored in the local PC, deselect **Restart the VM now to install the OS**, and click **OK**.

Figure 2-56 Selecting the ISO file

Step 8 In the displayed **Information** dialog box, click **OK**.

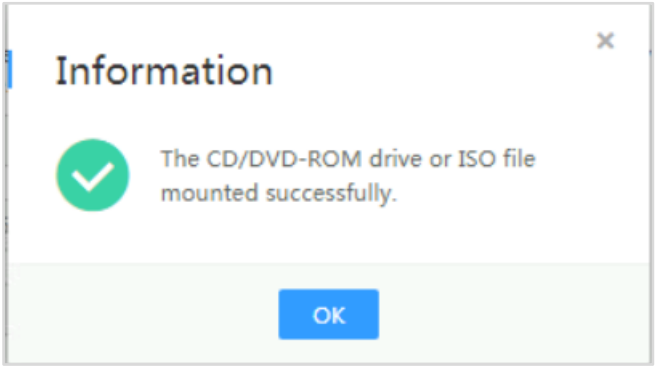


Figure 2-57 Successful mounting

Step 9 On the **FullCopy Template** tab page, click **Log In Using VNC** to log in to the VM as the **Administrator** user.

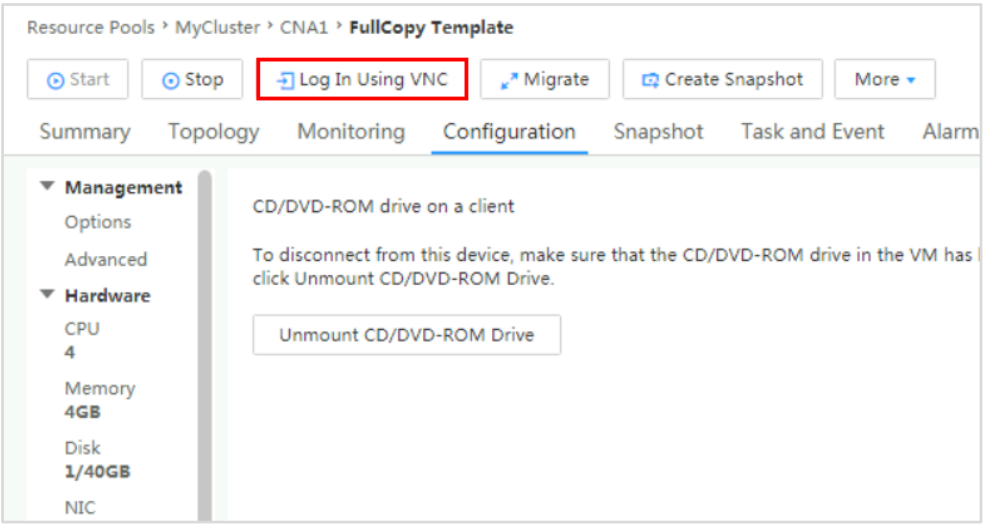


Figure 2-58 Logging in using VNC

Step 10 On the VM, right-click **CD Drive** and select **Open**.

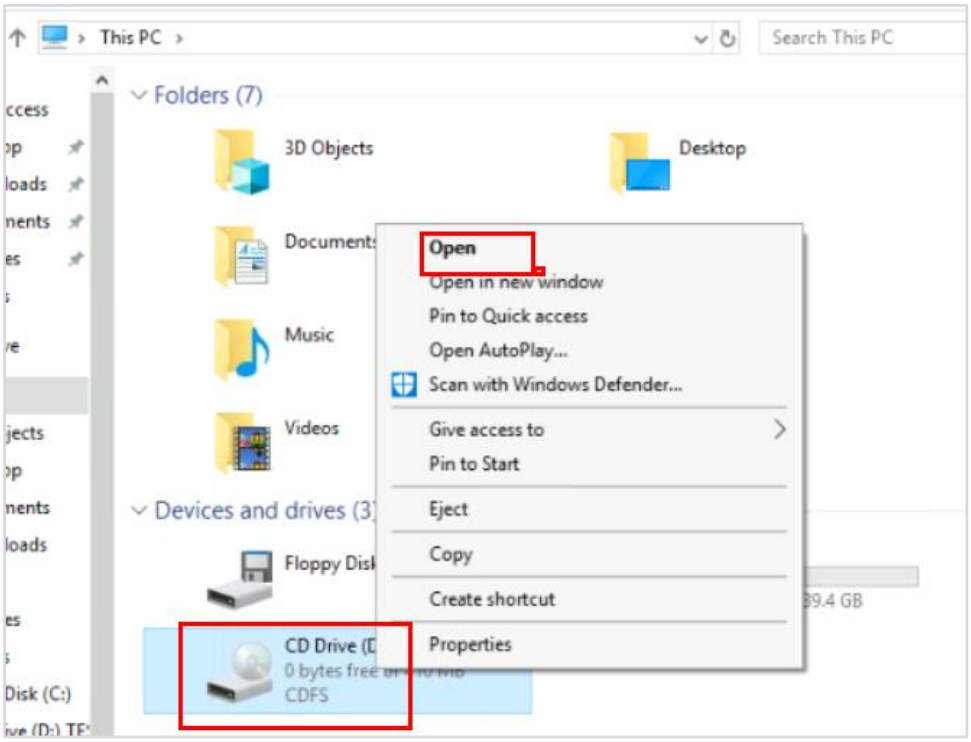


Figure 2-59 Opening the CD drive

Step 11 Double-click **run.bat**.

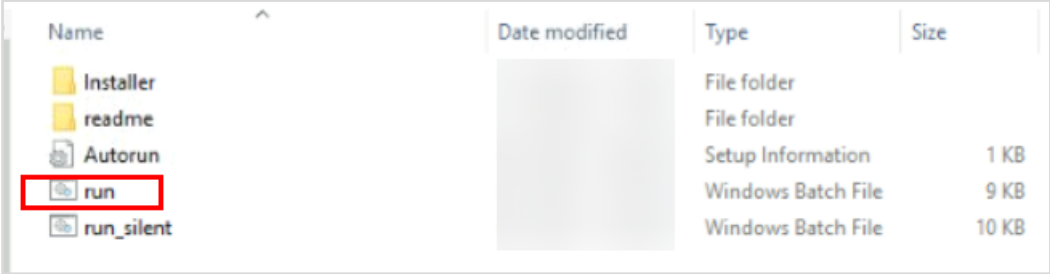


Figure 2-60 Double-clicking run.bat

Step 12 In the displayed **FusionAccess Windows Installer** window, click **Create Template**.

Figure 2-61 Template creation page

Step 13 In this exercise, set **Select a virtualization environment** to **FusionSphere(FusionCompute)** in the **Environment** step and click **Next**.

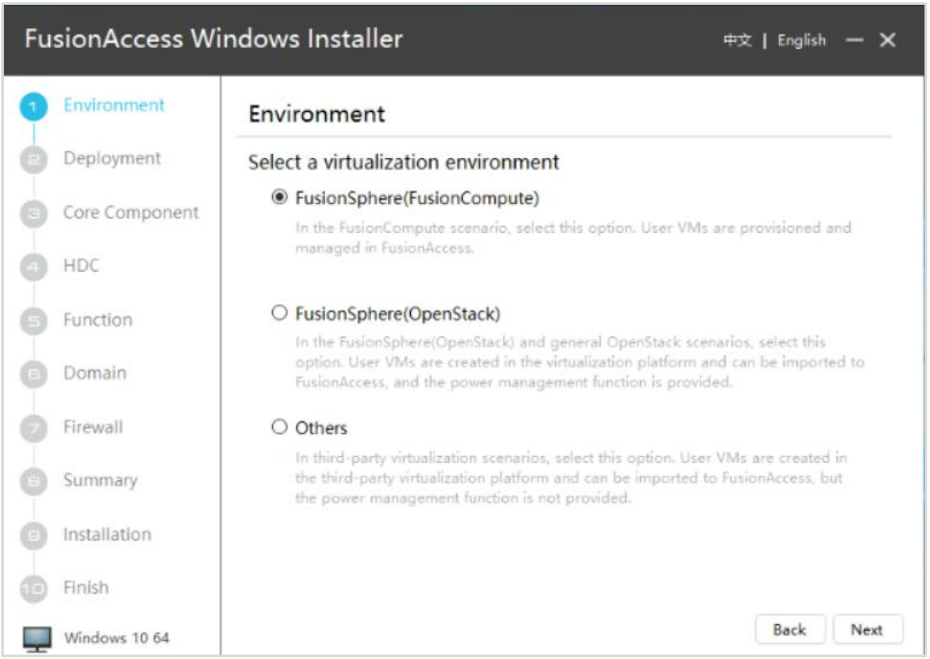


Figure 2-62 Process of creating a full copy template 1

Step 14 In the **Deployment step**, set **Select a template type** to **Full Copy** and click **Next**.

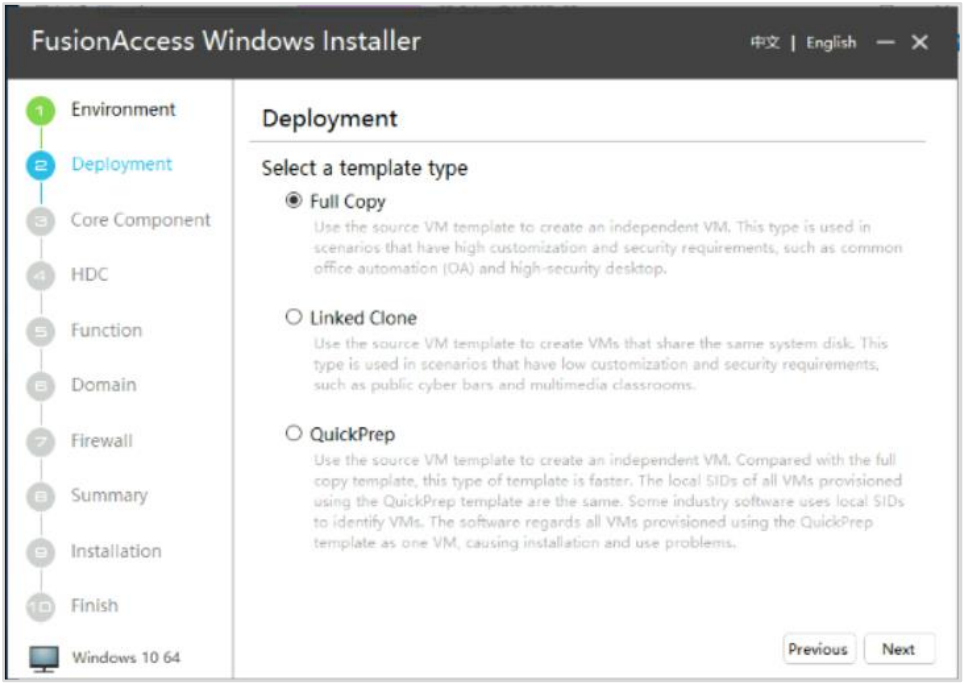


Figure 2-63 Process of creating a full copy template 2

Step 15 In the **Core Component** step, set **Select a Huawei Desktop Agent (HDA) Type** to **Common** and click **Next**.

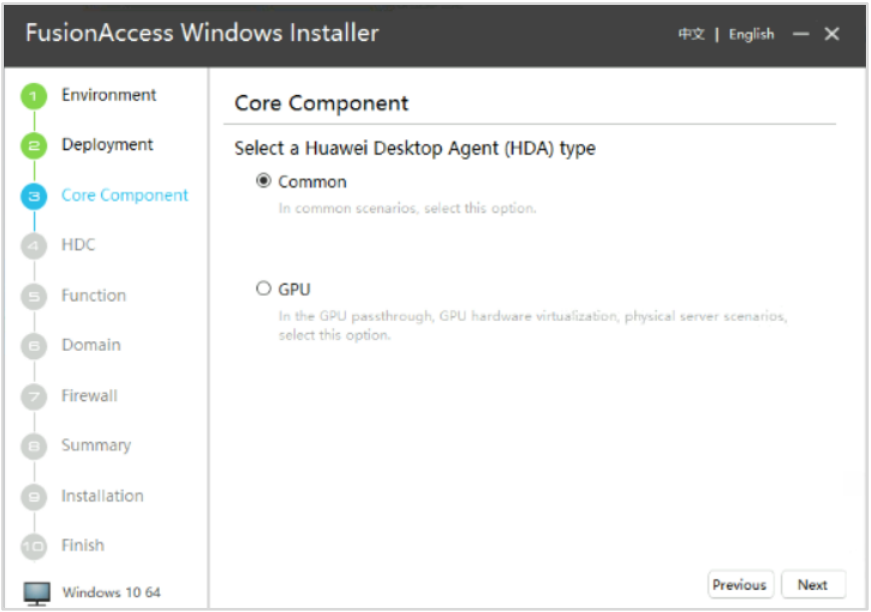


Figure 2-64 Process of creating a full copy template 3

Step 16 In the **HDC** step, set **Location of the Huawei desktop controller (HDC)** to **Automatic** and click **Next**.

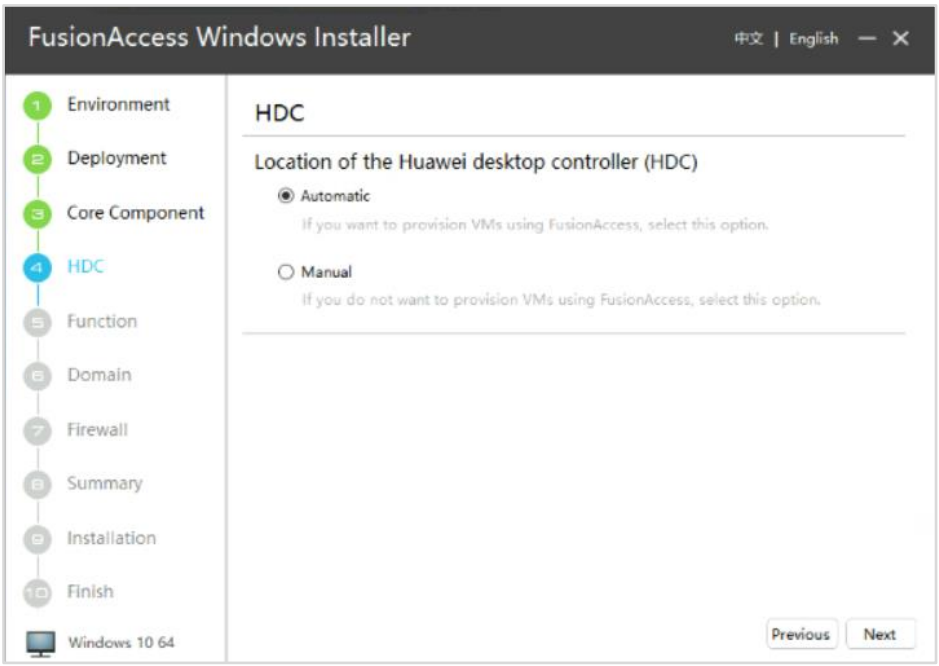


Figure 2-65 Process of creating a full copy template 4

Step 17 In the **Function** step, the **Optimize function** is selected by default. Click **Next**.

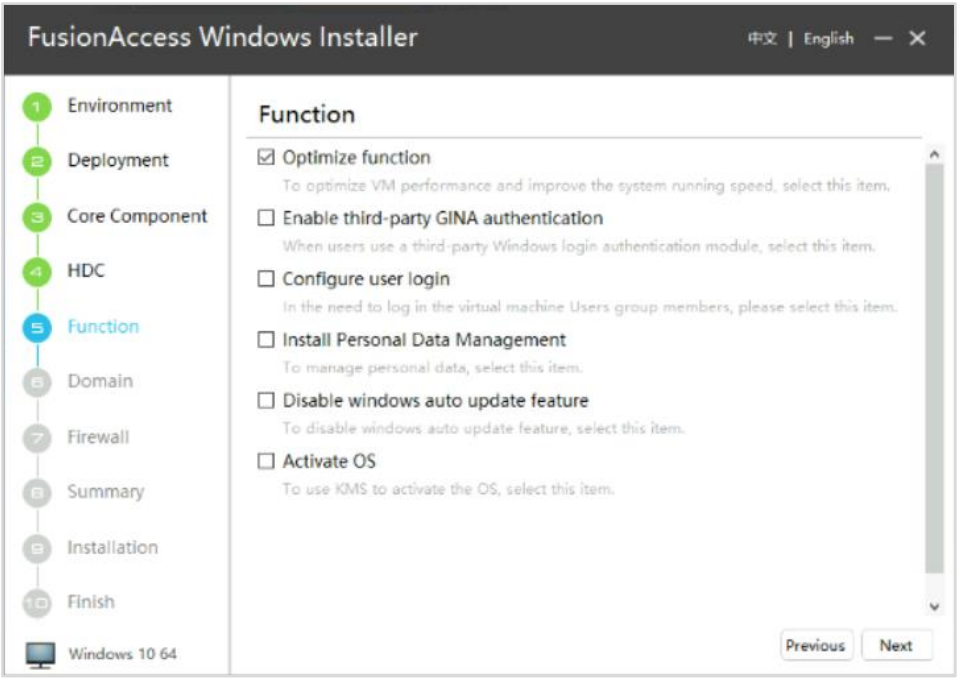


Figure 2-66 Process of creating a full copy template 5

Step 18 Skip the **Domain** step and click **Next**.

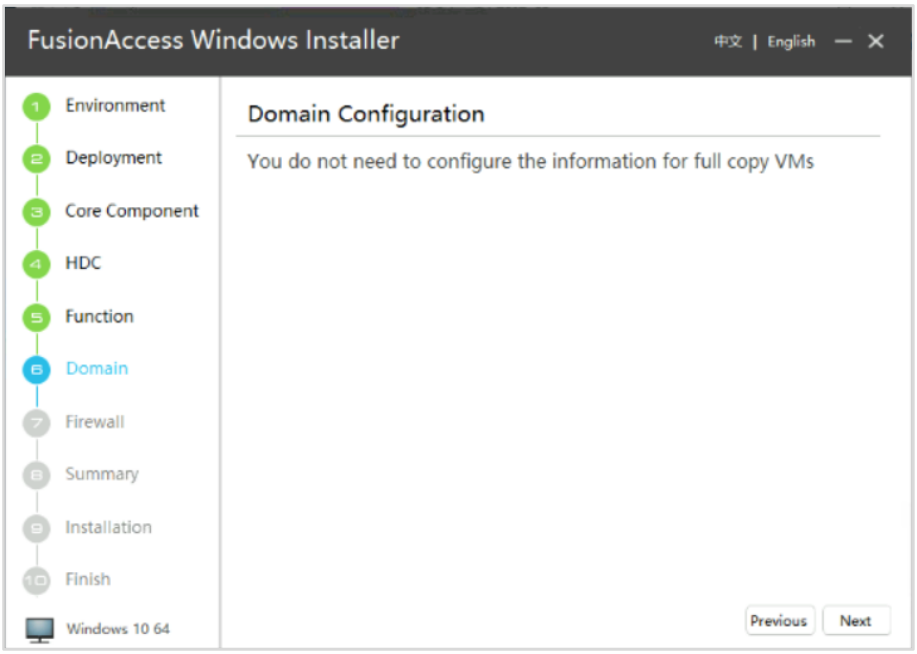


Figure 2-67 Process of creating a full copy template 6

Step 19 In the **Firewall** step, set **Configure firewall rules** to **Automatic** and click **Next**.

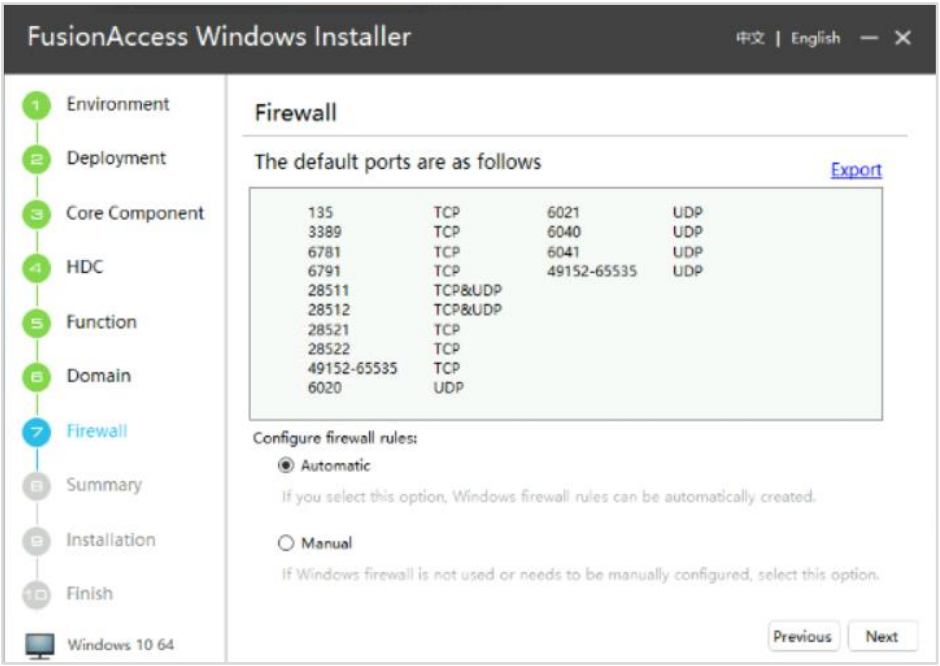


Figure 2-68 Process of creating a full copy template 7

Step 20 Confirm the information in the **Summary** step and click **Install**.

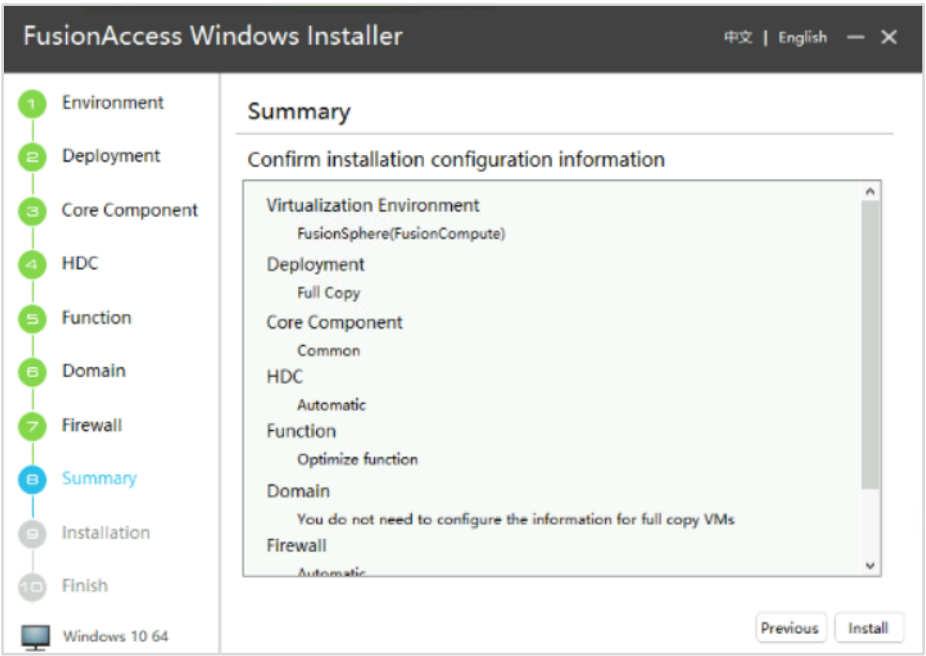


Figure 2-69 Process of creating a full copy template 8

Step 21 In the Installation step, a dialog box is displayed when the core component HDA is being installed. Click **OK** to restart the computer. After the restart, log in to the system as the **Administrator** user.

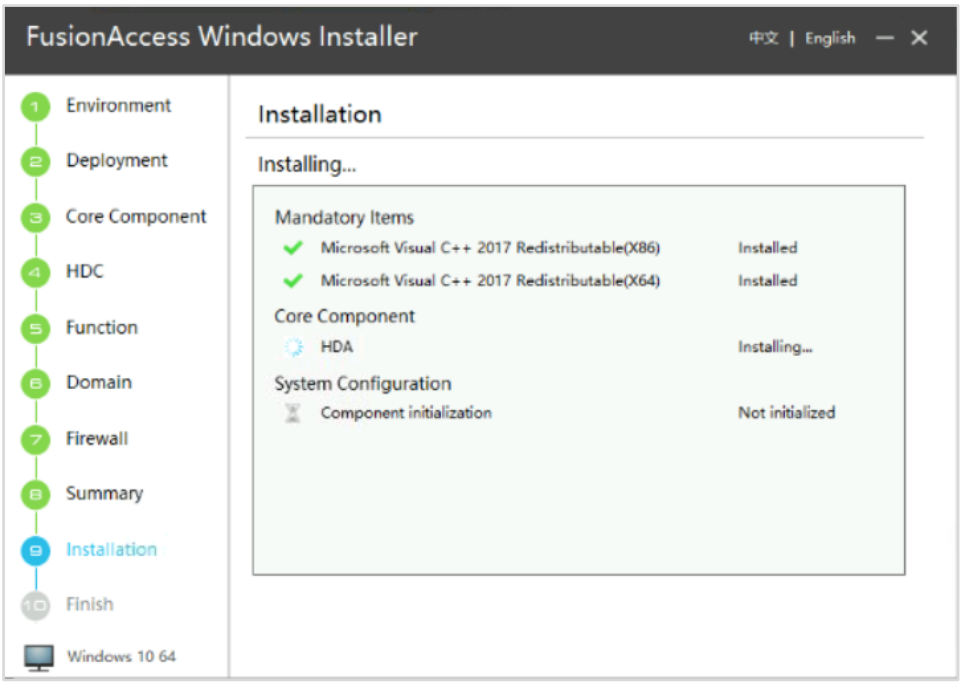


Figure 2-70 Process of creating a full copy template 9

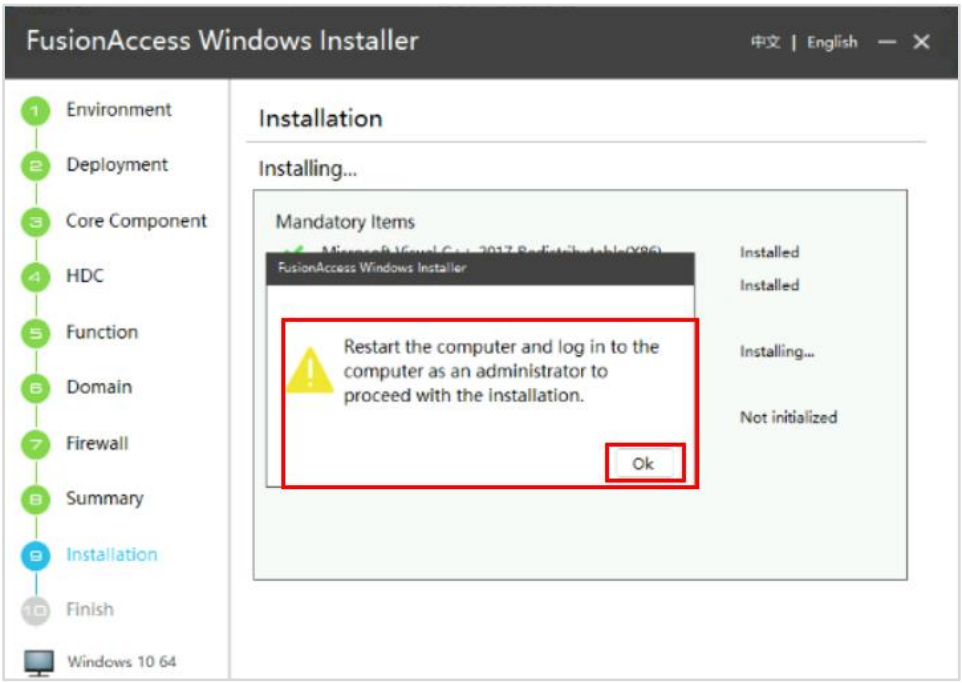


Figure 2-71 Process of creating a full copy template 10

Step 22 After the login is complete, the installation page is displayed. After the installation is complete, click **Next**.

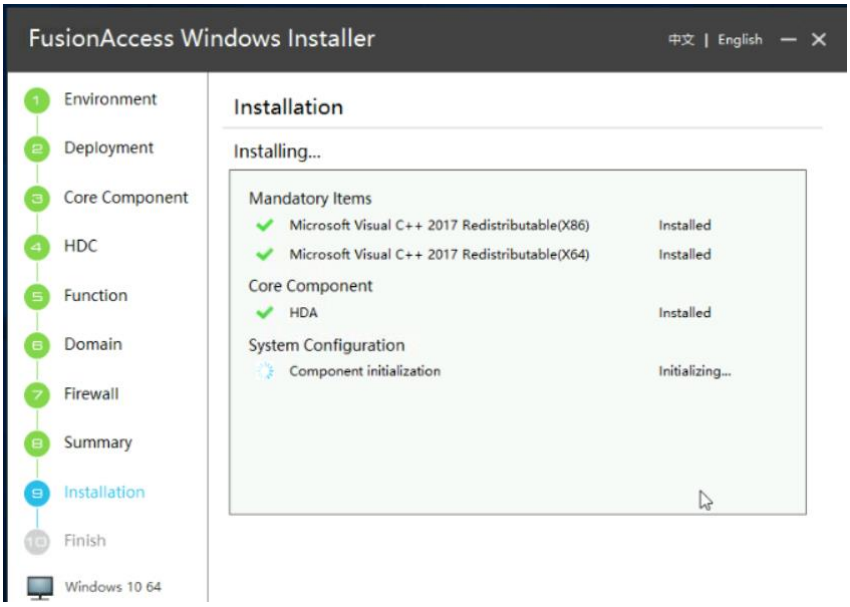


Figure 2-72 Process of creating a full copy template 11

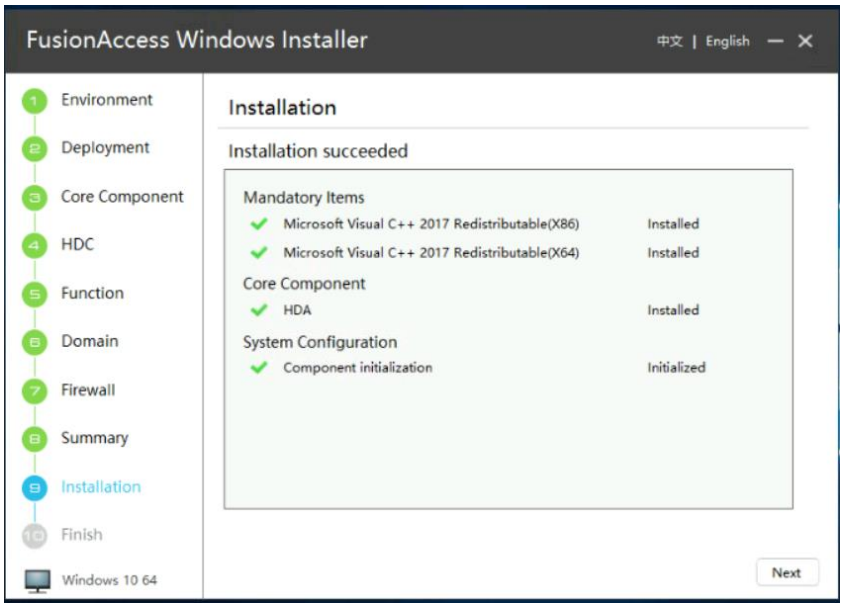


Figure 2-73 Process of creating a full copy template 12

Step 23 In the **Finish** step, click **Sysprep**. After the encapsulation is completed, click **Finish**.

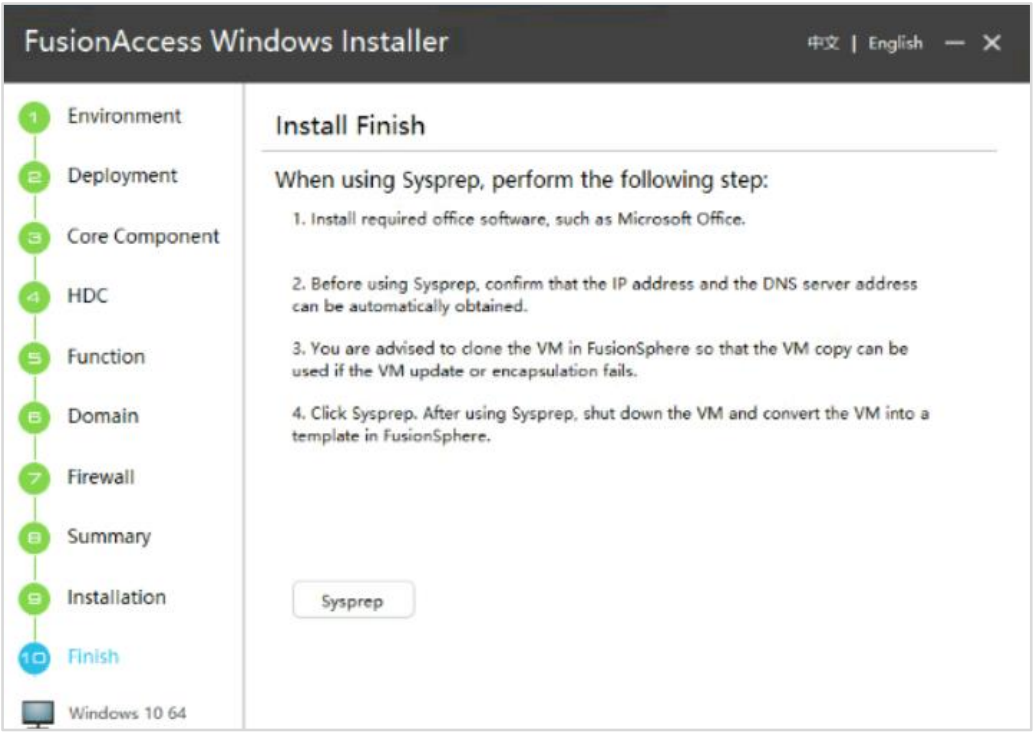


Figure 2-74 Process of creating a full copy template 13

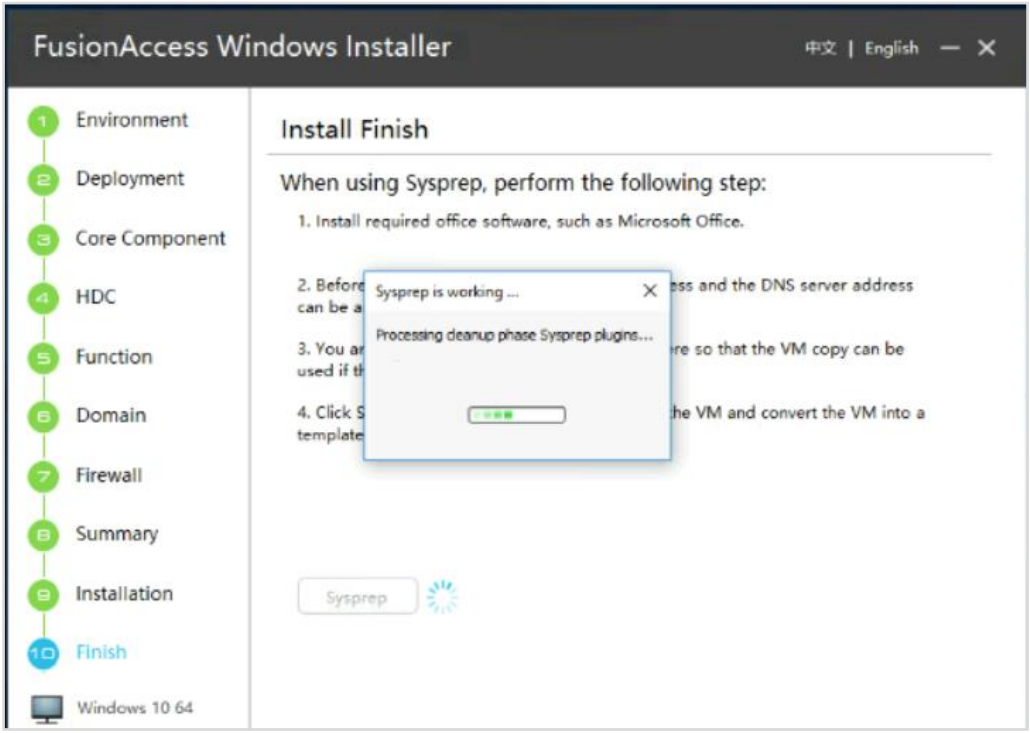


Figure 2-75 Process of creating a full copy template 14

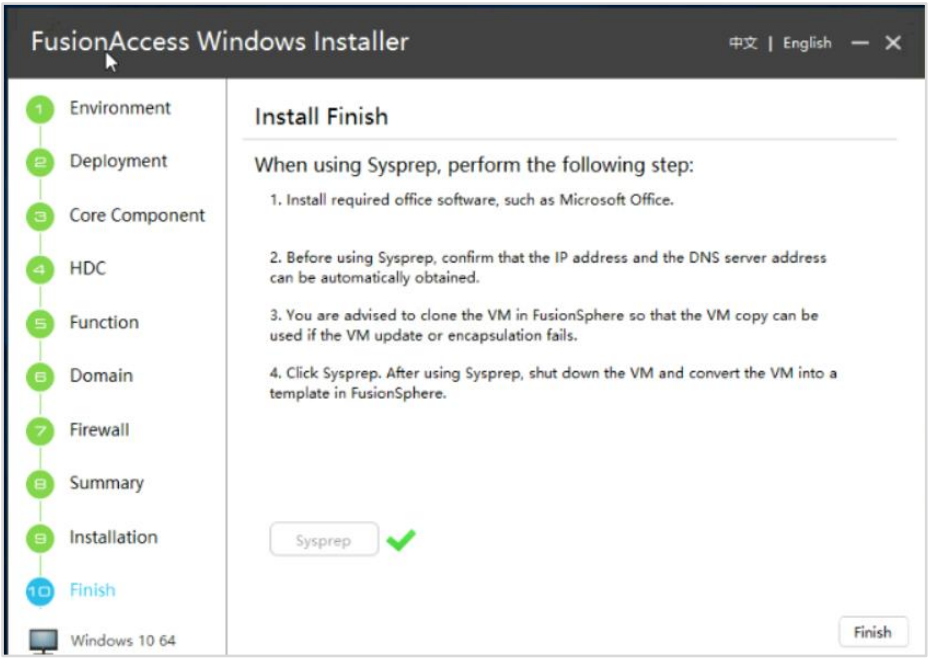


Figure 2-76 Process of creating a full copy template 15

Step 24 Unmount the CD-ROM drive. In the displayed **Information** dialog box, click **OK**.

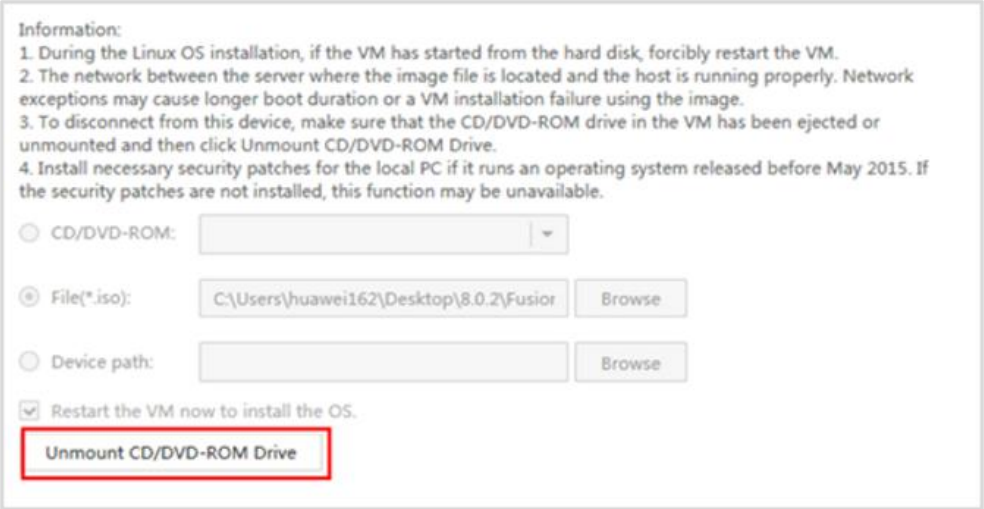


Figure 2-77 Unmounting the CD/DVD-ROM drive

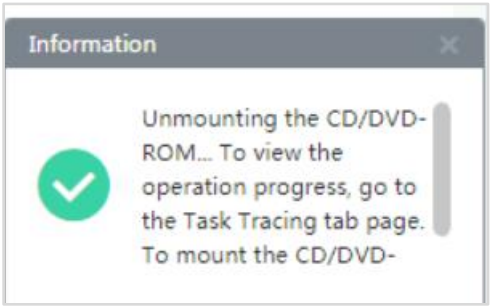


Figure 2-78 Confirming the unmounting

Step 25 On the VM tab page, click **Stop** to stop the VM.

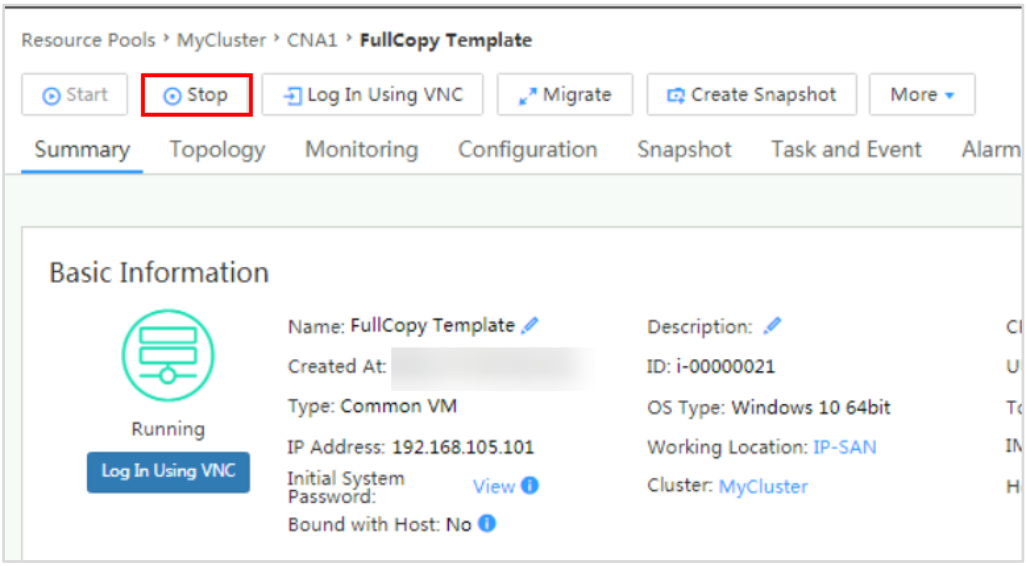


Figure 2-79 Stopping a VM

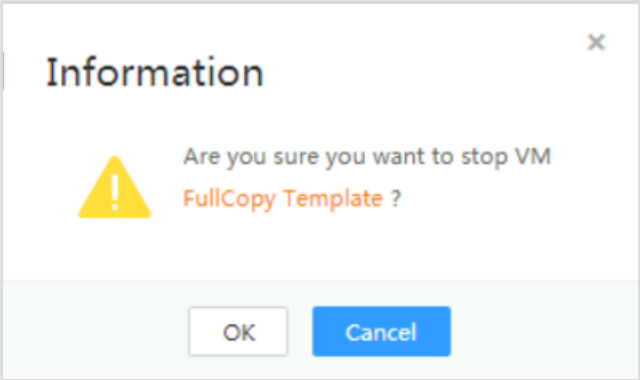


Figure 2-80 Confirming the operation

Step 26 On FusionCompute, right-click the stopped VM and choose **Template** > **Convert to Template**. In the displayed **Information** dialog box, click **OK**.

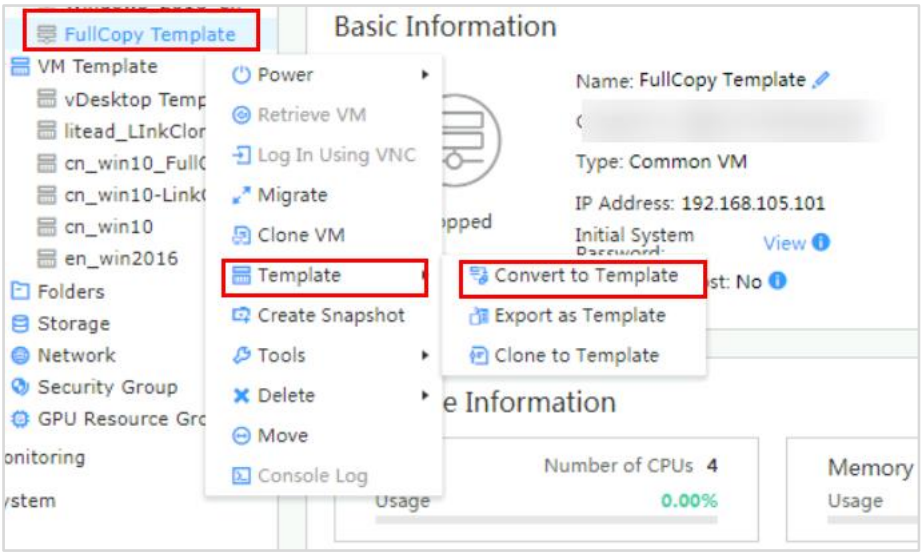


Figure 2-81 Converting a VM into a template

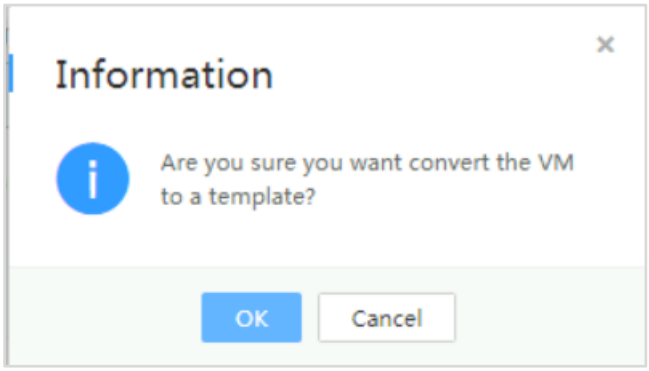


Figure 2-82 Confirming the operation

2.2.2.5 Creating a Linked Clone VM Template

Step 1 In the navigation pane on the left of FusionCompute, click **VM Template**, right-click the template created in step 7 in 2.2.2.3, and click **Deploy VM Using Template**.

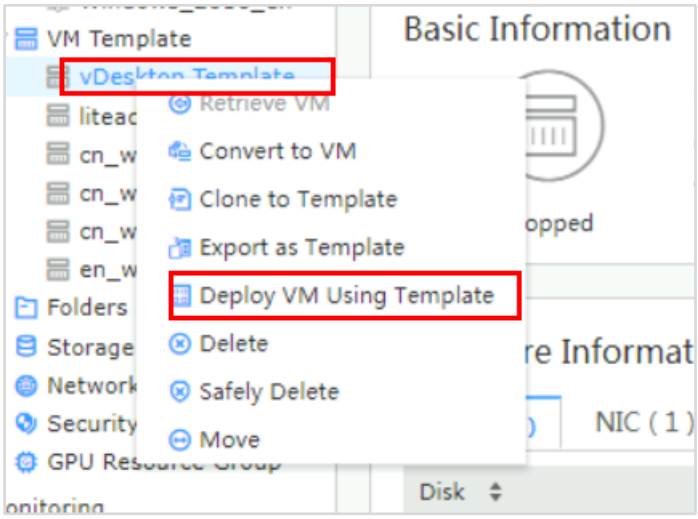


Figure 2-83 Deploying a VM using a template

Step 2 In the **Create VM** dialog box displayed, set **Name** to **LinkedClone Template** in the **Basic Information** step, and click **Next**.

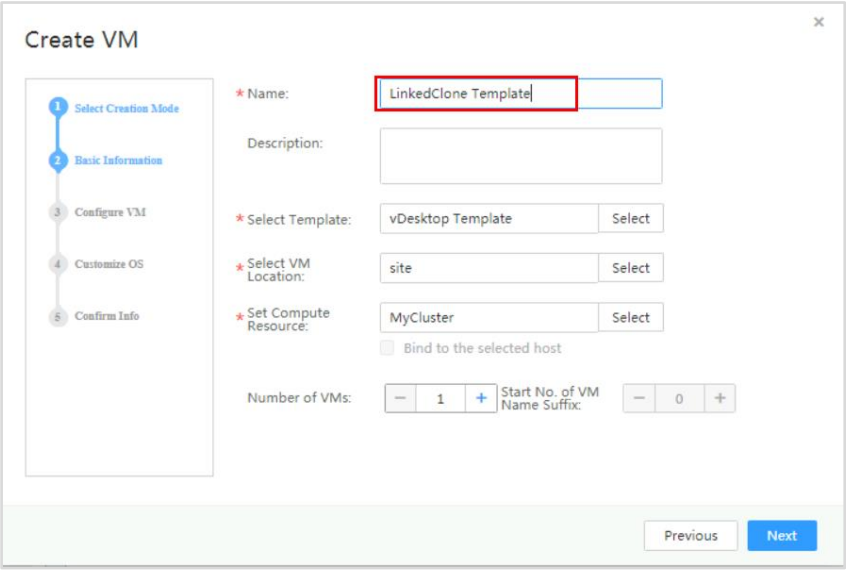


Figure 2-84 Basic information

Step 3 In the **Configure VM** step, retain the default values for other parameters. You can also modify the full copy VM specifications as planned (the disk specifications cannot be changed), and click **Next**.

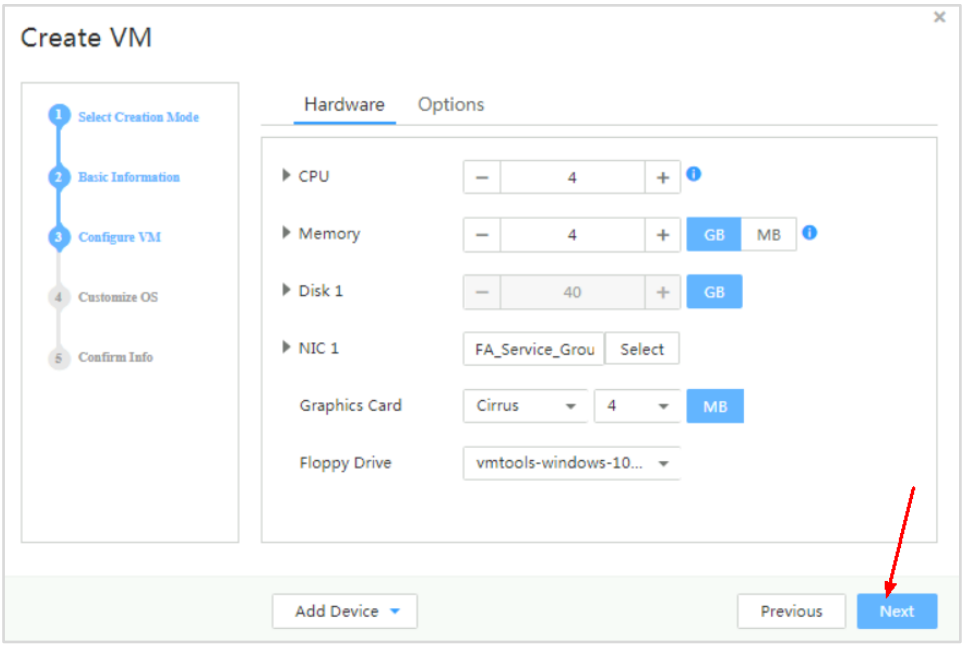


Figure 2-85 VM configuration

Step 4 In the **Customize OS** step, select **Do not customize** for **VM Attributes**, deselect **Generate Initial Password**, and click **Next**.

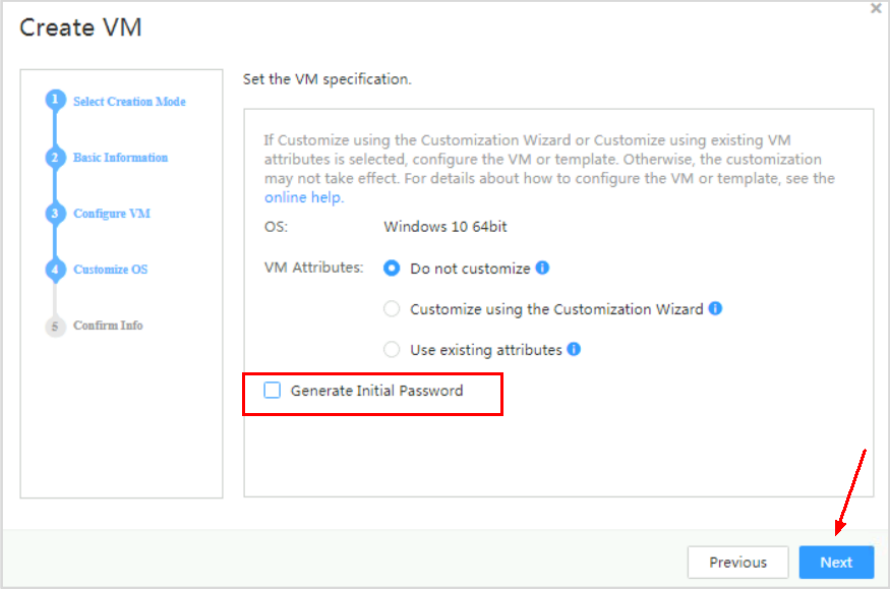


Figure 2-86 Customizing the OS

Step 5 In the **Confirm Info** step, select **Start VM immediately after creation** and click **OK**.

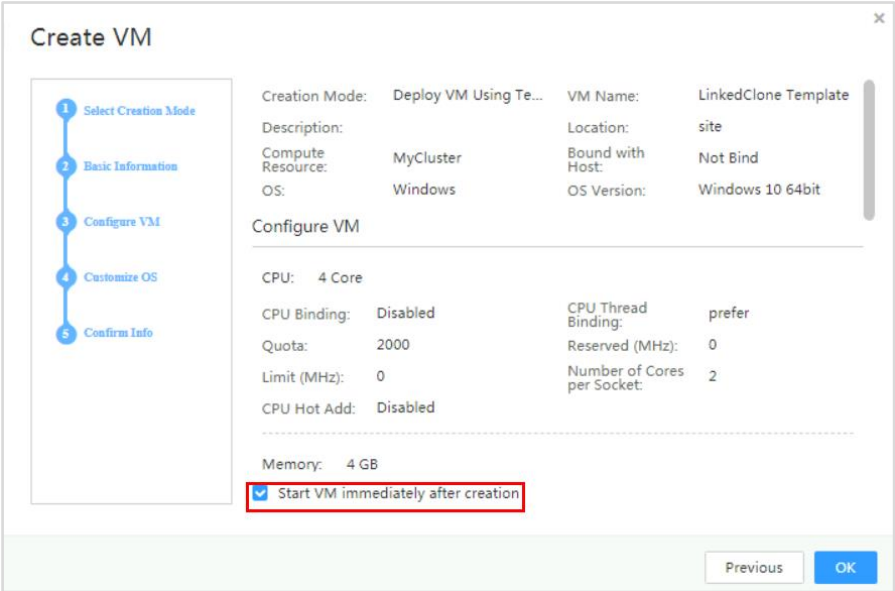


Figure 2-87 Confirming the information

Step 6 Log in to FusionCompute. On the **Resource Pools** page, select **ManagementCluster**, click the created VM, choose **Configuration** > **CD/DVD-ROM Drive**, set **Mount CD/DVD-ROM Drive Type** to **Mount Local CD/DVD-ROM Drive**, and click **OK**.

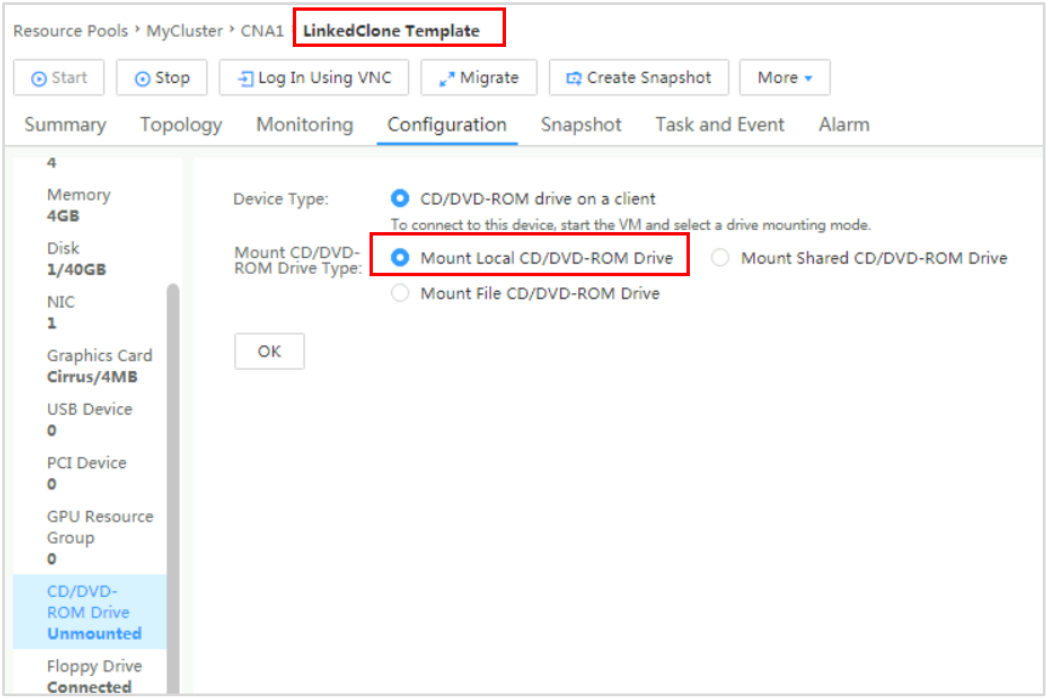


Figure 2-88 Mounting a CD/DVD-ROM drive

Step 7 In the displayed window, select **File(*.iso)**, click **Browse**, select the template tool image **FusionAccess_WindowsDesktop_Installer_8.0.2.iso** stored in the local PC, deselect **Restart the VM now to install the OS**, and click **OK**.

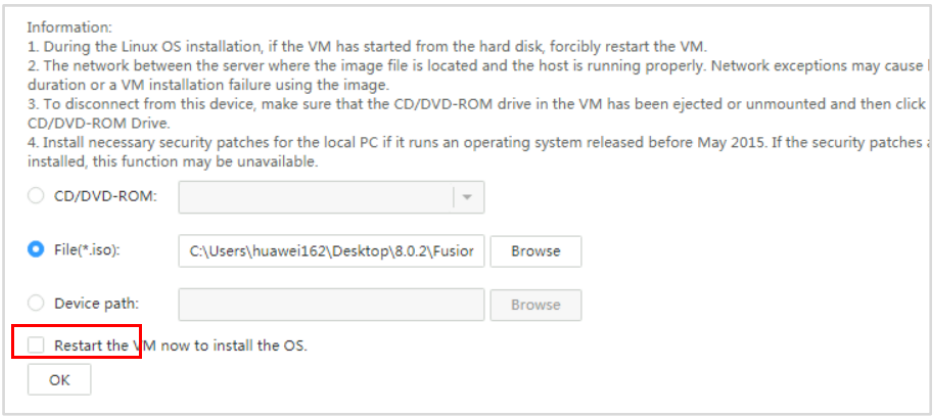


Figure 2-89 Selecting the ISO file

Step 8 In the displayed **Information** dialog box, click **OK**.

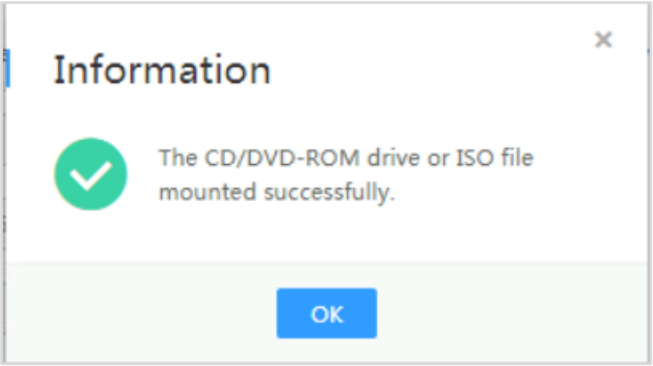


Figure 2-90 Successful mounting

Step 9 On the **LinkedClone Template** tab page, click **Log In Using VNC** to log in to the VM as the **Administrator** user.

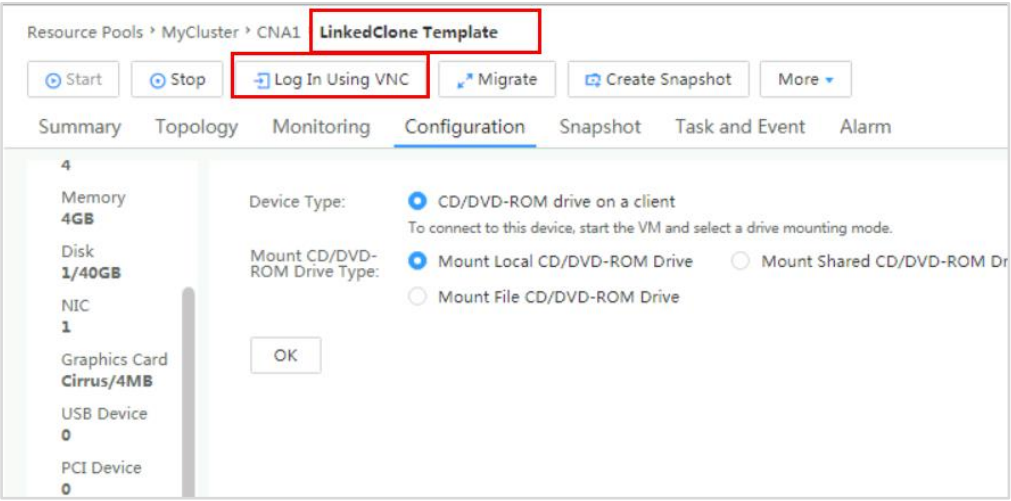


Figure 2-91 Logging in using VNC

Step 10 On the VM, right-click **CD Drive** and select **Open**.

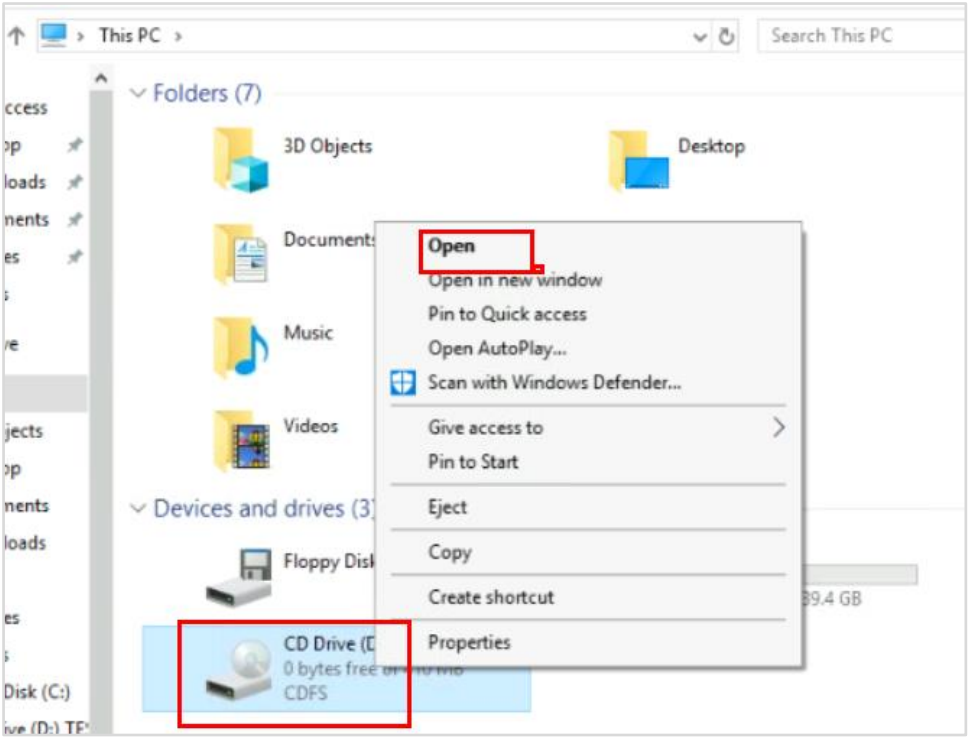


Figure 2-92 Opening the CD drive

Step 11 Double-click **run.bat**.

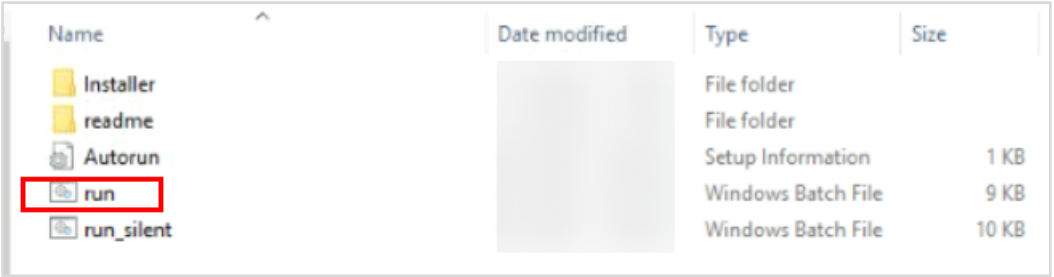


Figure 2-93 Double-clicking run.bat

Step 12 In the displayed **FusionAccess Windows Installer** window, click **Create Template**. The template creation page is displayed.

Figure 2-94 Template creation page

Step 13 In this exercise, set **Select a virtualization environment** to **FusionSphere(FusionCompute)** in the **Environment** step and click **Next**.

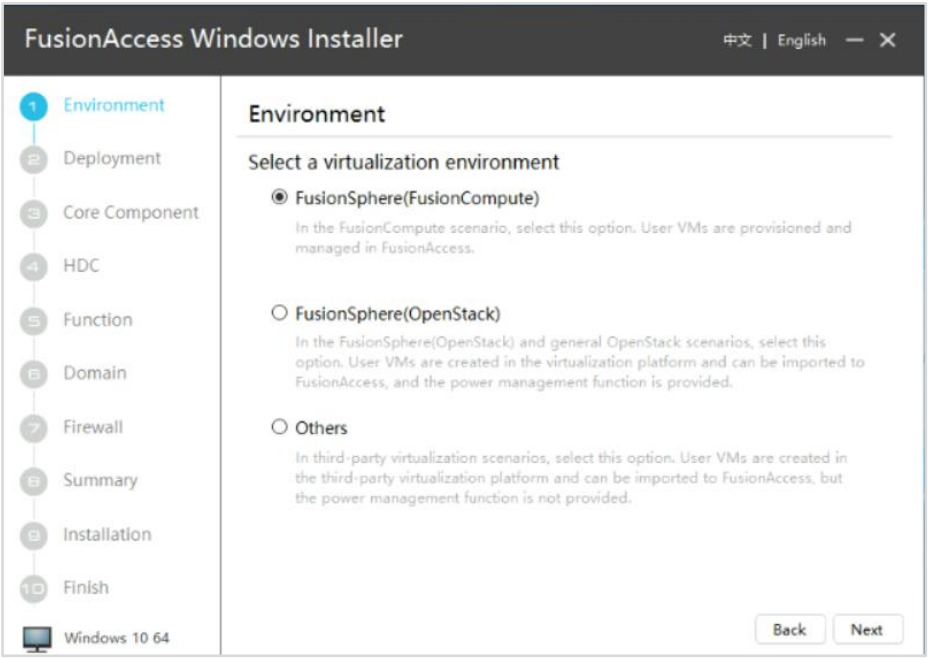


Figure 2-95 Process of creating a linked clone template 1

Step 14 In the **Deployment step**, set **Select a template type** to **Linked Clone** and click **Next**.

Figure 2-96 Process of creating a linked clone template 2

Step 15 In the **Core Component** step, set **Select a Huawei Desktop Agent (HDA) Type** to **Common** and click **Next**.

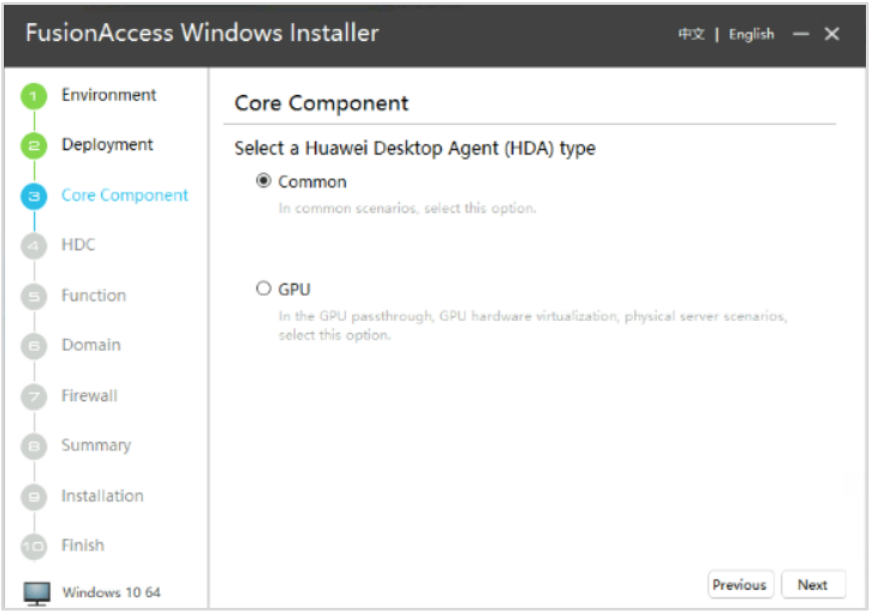


Figure 2-97 Process of creating a linked clone template 3

Step 16 In the **HDC** step, set **Location of the Huawei desktop controller (HDC)** to **Automatic** and click **Next**.

Figure 2-98 Process of creating a linked clone template 4

Step 17 In the **Function** step, the **Optimize function** and **Configure user login** are selected by default. Click **Next**.

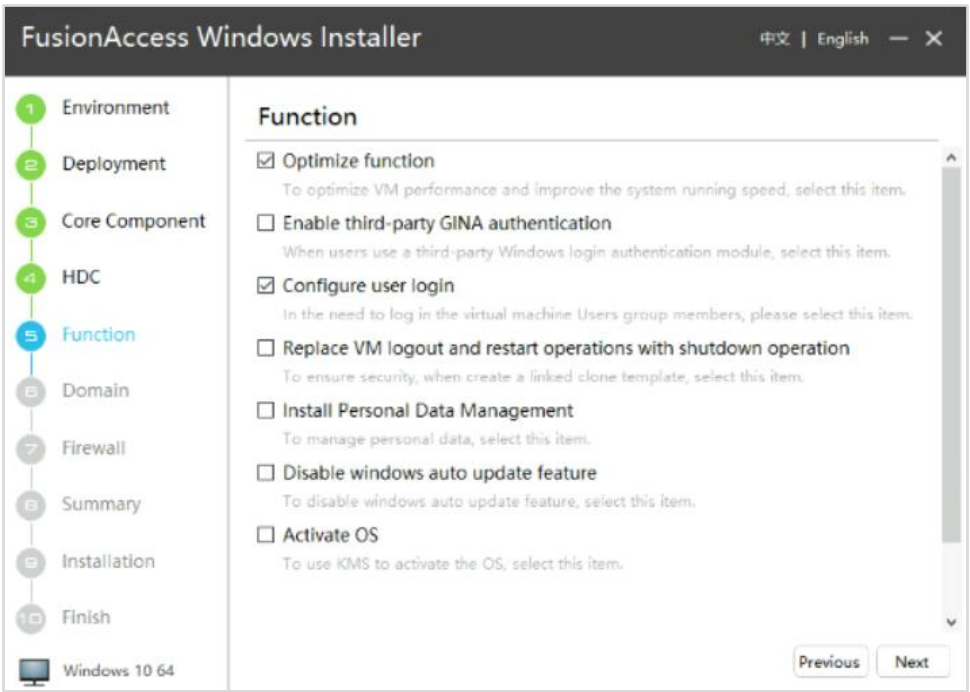


Figure 2-99 Process of creating a linked clone template 5

Step 18 In the **Domain** step, enter the following information and click **Next**.

Note:

- Set **Domain** to the domain to which the VM will be added, for example, **vdesktop.huawei.com**.
- Set **Account** to a domain account that has the permissions for adding other domain accounts.
- Set **Password** to the password of the domain account that has the permissions for adding other domain accounts.
- Set **OU** to the OU created on the AD server, for example, **UserOU**.
- Set **Domain user (group)** to the domain user (group) created on the AD server. You are advised to enter the security group name, for example, **UserGroup**.
- **Local user group**: VM users can be added to the **Users** group only when **Configure user login** is selected in the **Function** step. Users in the **Users** group do not have VM administrator permissions, so they cannot perform some operations. For example, the users cannot save files to the system disk.

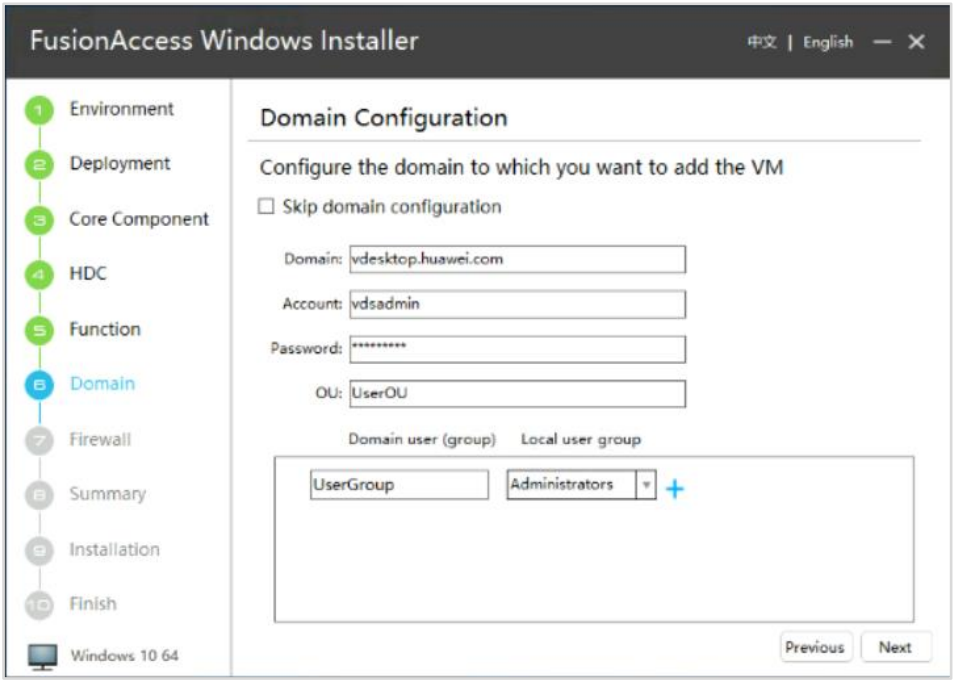


Figure 2-100 Process of creating a linked clone template 6

Step 19 In the **Firewall** step, set **Configure firewall rules** to **Automatic** and click **Next**.

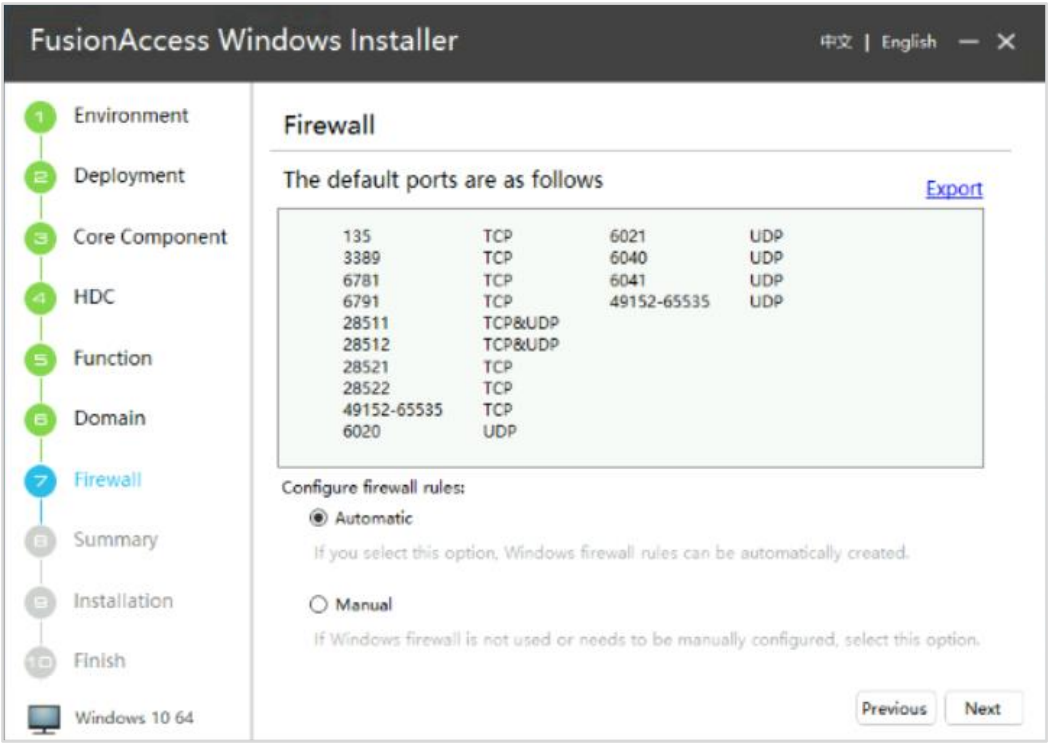


Figure 2-101 Process of creating a linked clone template 7

Step 20 Confirm the information in the **Summary** step and click **Install**.

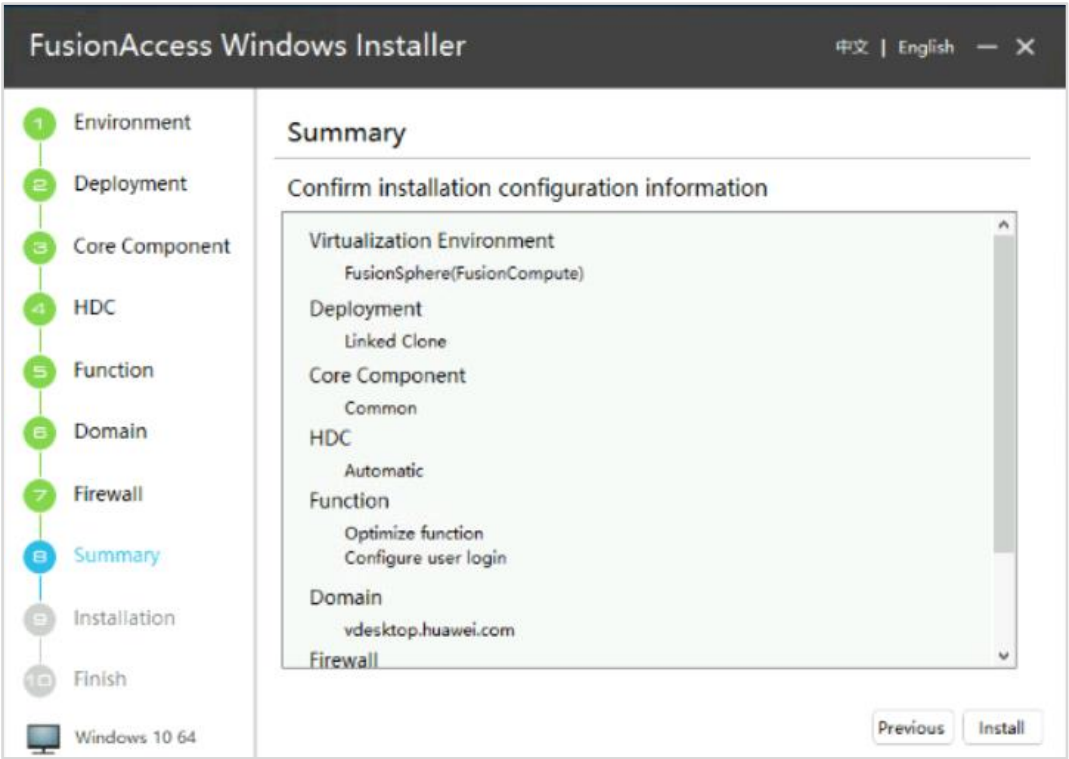


Figure 2-102 Process of creating a linked clone template 8

Step 21 In the Installation step, a dialog box is displayed when the core component HDA is being installed. Click **OK** to restart the computer. After the restart, log in to the system as the administrator.

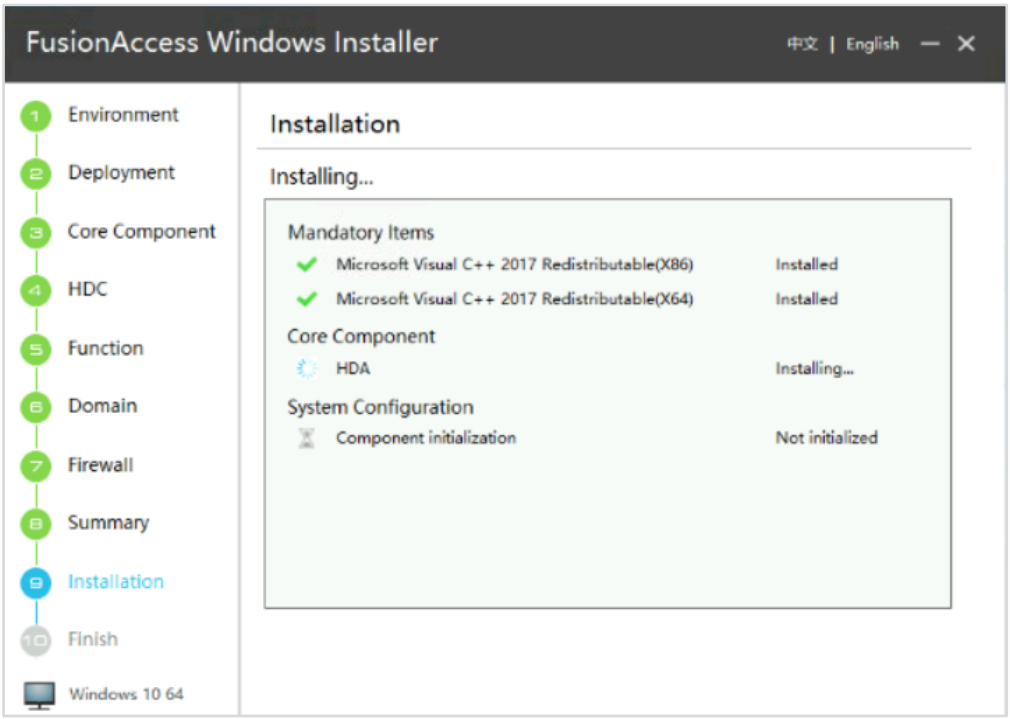


Figure 2-103 Process of creating a linked clone template 9

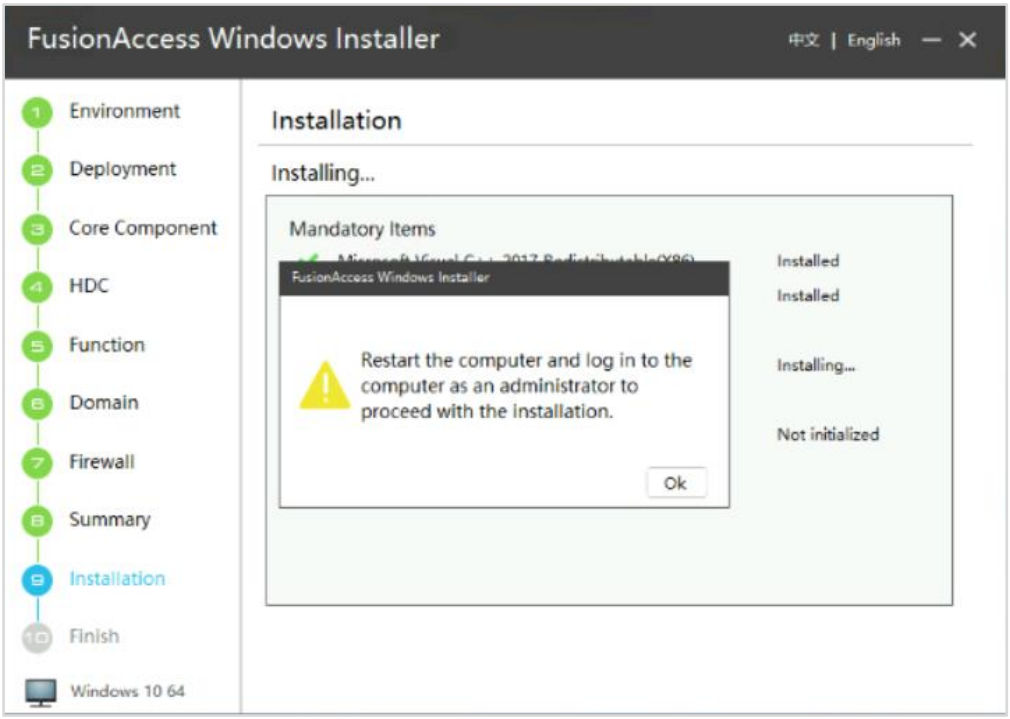


Figure 2-104 Process of creating a linked clone template 10

Step 22 After the login is complete, the installation page is displayed. After the installation is complete, click **Next**.

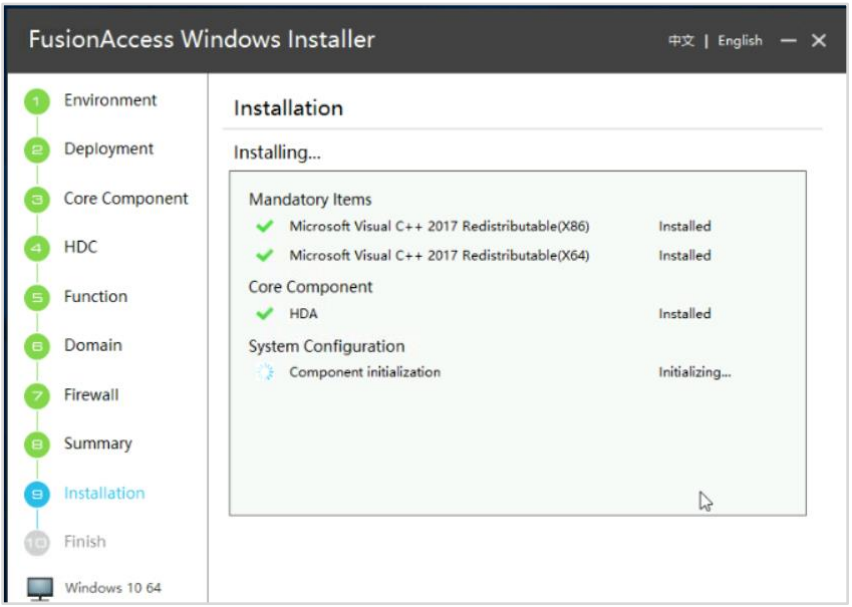


Figure 2-105 Process of creating a linked clone template 11

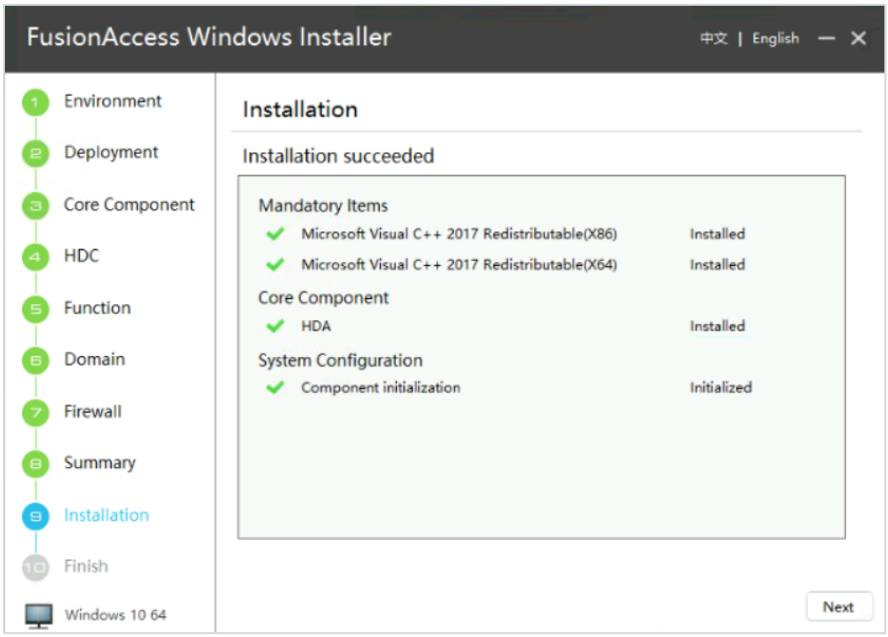


Figure 2-106 Process of creating a linked clone template 12

Step 23 In the **Finish** step, click **Finish**.

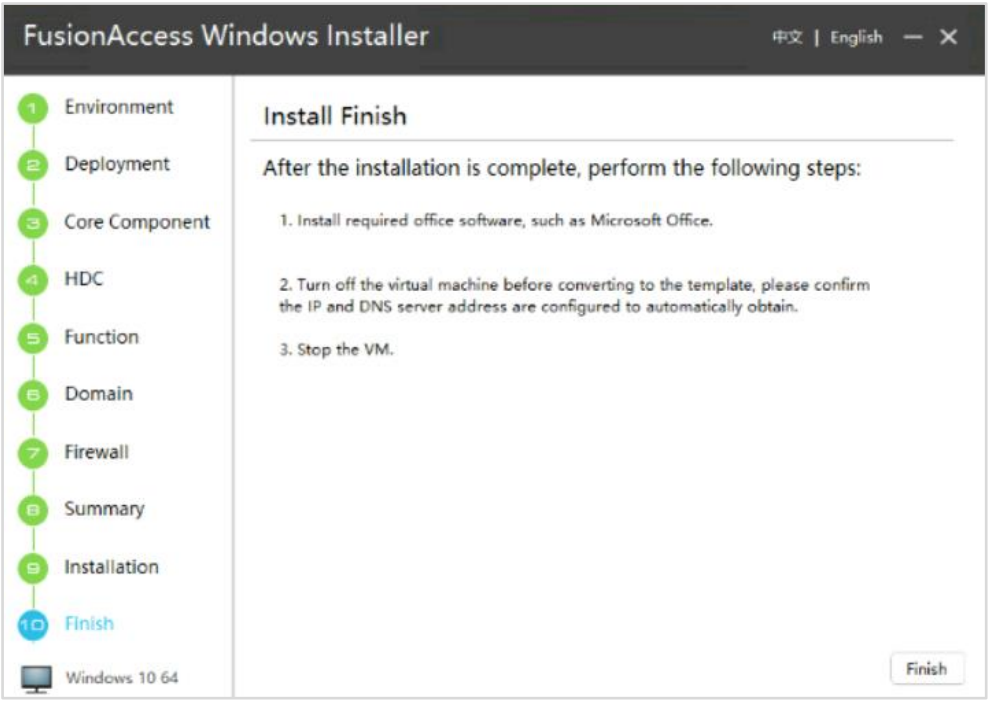


Figure 2-107 Process of creating a linked clone template 13

Step 24 Unmount the CD-ROM drive. In the displayed **Information** dialog box, click **OK**.

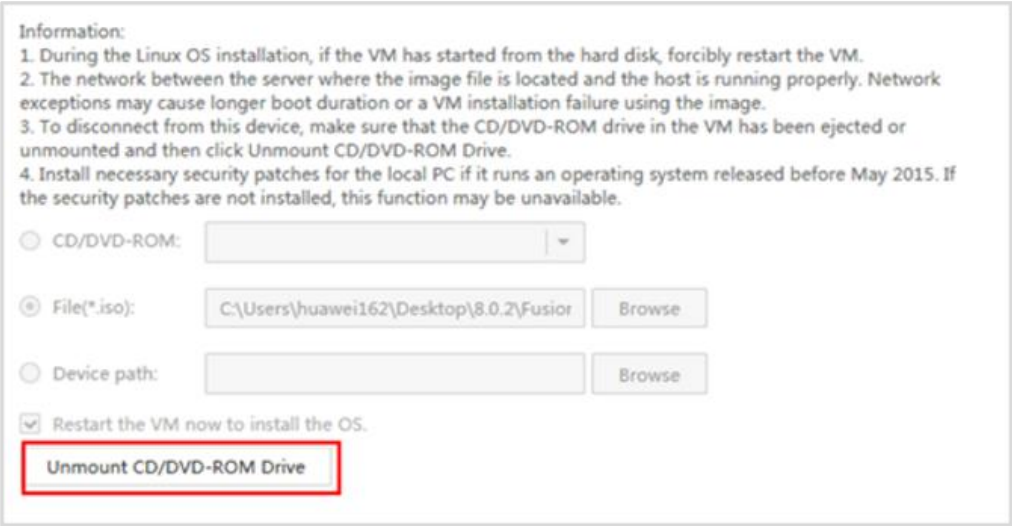


Figure 2-108 Unmounting the CD/DVD-ROM drive

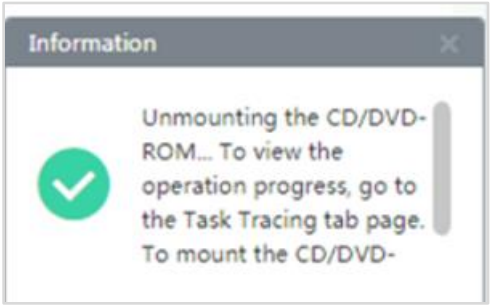


Figure 2-109 Confirming the unmounting

Step 25 On the VM tab page, click **Stop**. In the displayed **Information** dialog box, click **OK** to stop the VM.

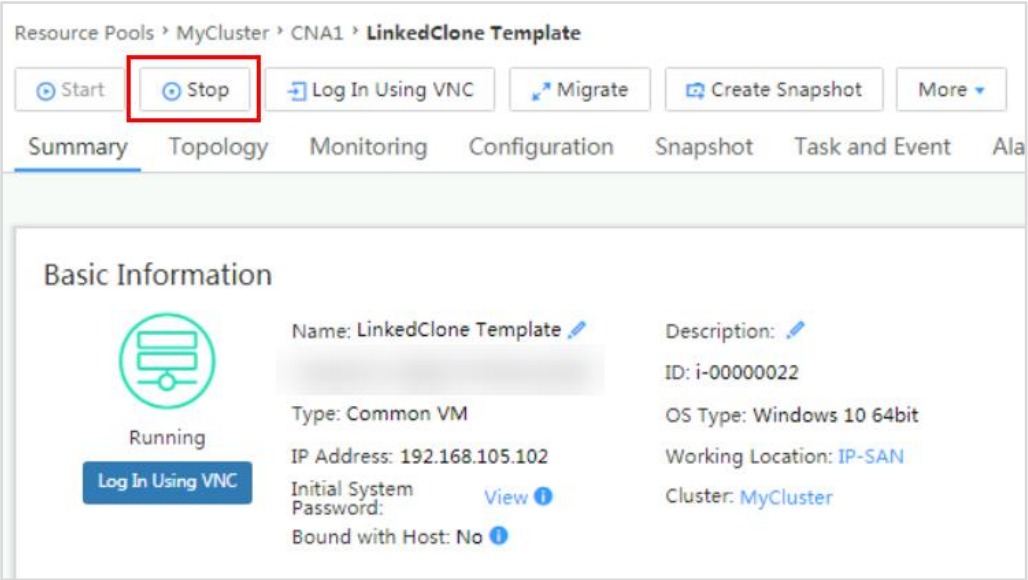


Figure 2-110 Stopping a VM

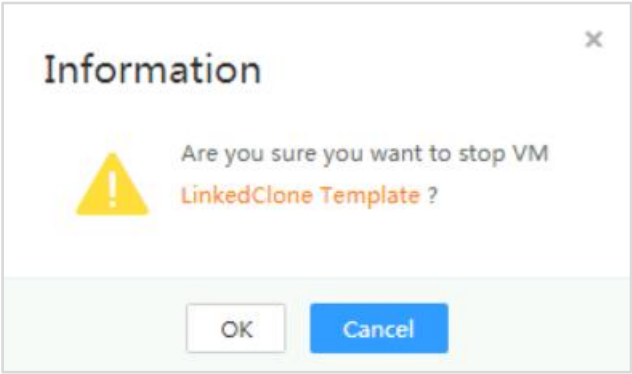


Figure 2-111 Confirming the operation

Step 26 On FusionCompute, right-click the stopped VM and choose **Template** > **Convert to Template**. In the displayed **Information** dialog box, click **OK**.

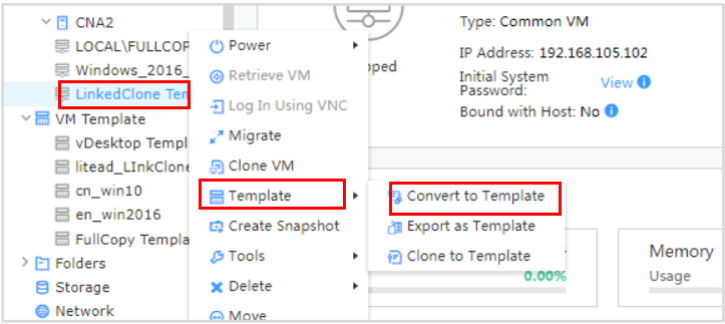


Figure 2-112 Converting a VM into a template

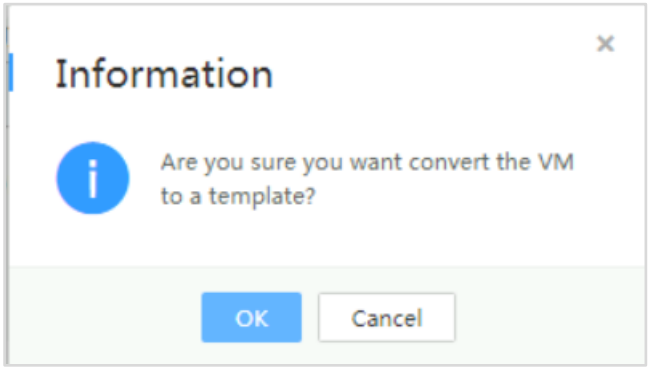


Figure 2-113 Confirming the conversion

2.2.3 Provisioning a Desktop

2.2.3.1 Configuring a Template

Step 1 In the address box of your web browser, enter **https://192.168.105.11:8448** to log in to FusionAccess. **192.168.105.11** is the service plane IP address of the active ITA server.

Step 2 On FusionAccess, choose **System** > **System Configuration** > **Virtual Environment**. On the displayed page, click **FusionCompute**.

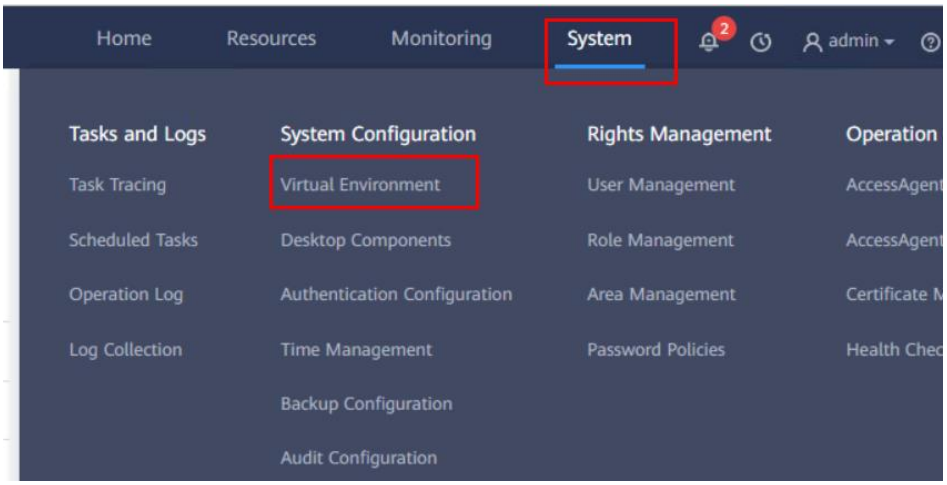


Figure 2-114 Virtual environment

Step 3 Choose **Operation** > **Template**. In the window displayed, locate the row containing the converted VM template, and configure parameters as required.

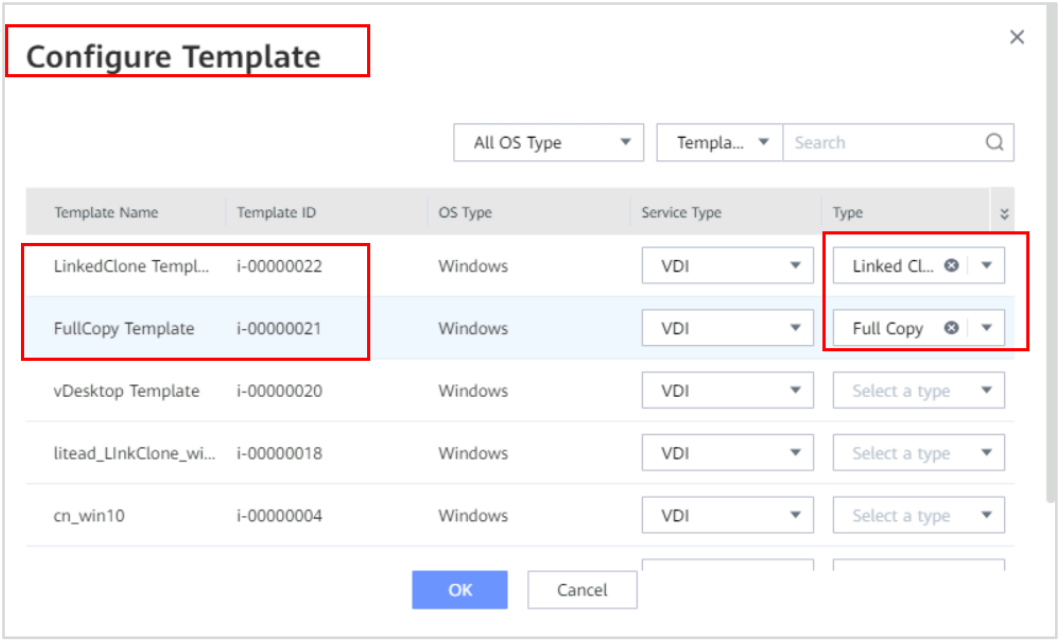


Figure 2-115 Configuring a template

Step 4 In the displayed confirmation dialog box, click **OK**. A message is displayed indicating that the configuration has been saved.

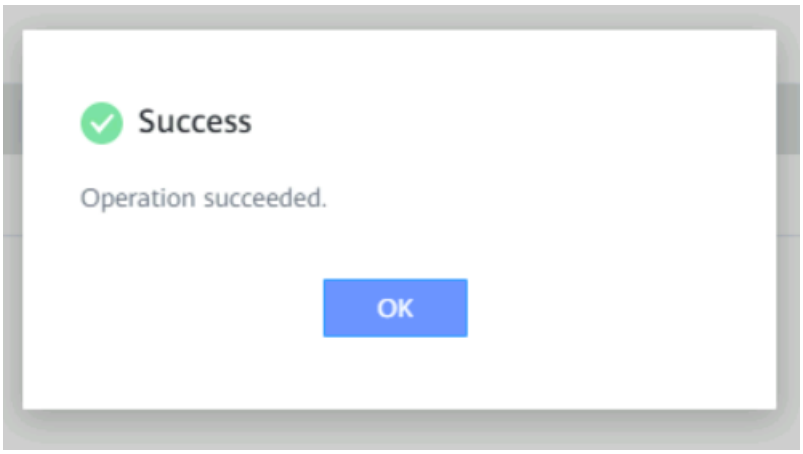


Figure 2-116 Successful template settings saving

2.2.3.2 Creating a Computer Group

Step 1 On FusionAccess, choose **Resources** > **Desktops** > **Computer Groups**.

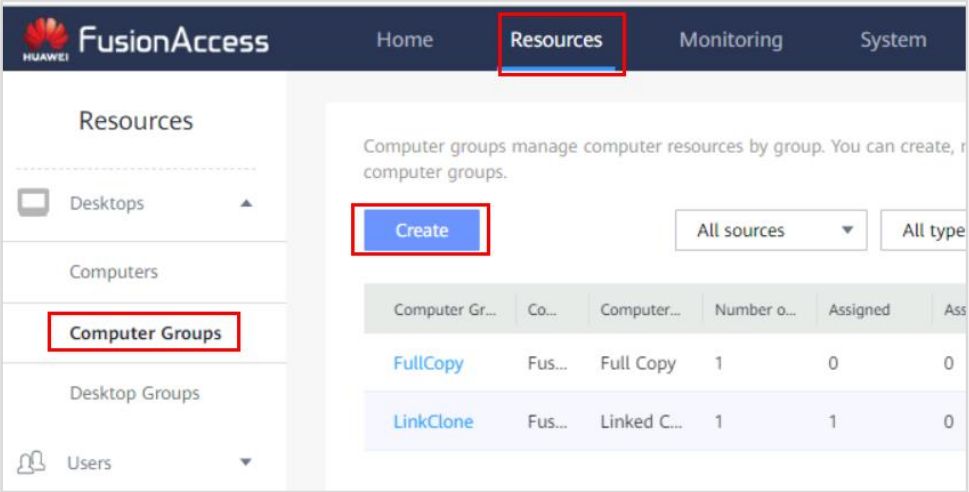


Figure 2-117 Computer group page

Step 2 Click **Create**. The **Create Computer Group** dialog box is displayed.

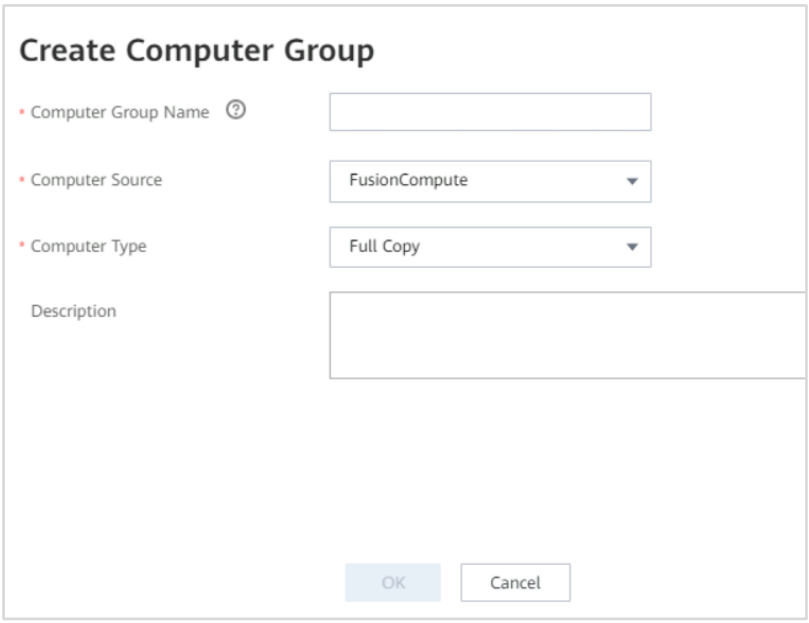


Figure 2-118 Creating a computer group

Step 3 Enter **FullCopy-VM-Group** in **Computer Group Name**, select **FusionCompute** from the **Computer Source** drop-down list and **Full Copy** from the **Computer Type** drop-down list, and click **OK**. If you select **Full Copy** for **Computer Type**, only full copy computers can be added to the computer group.

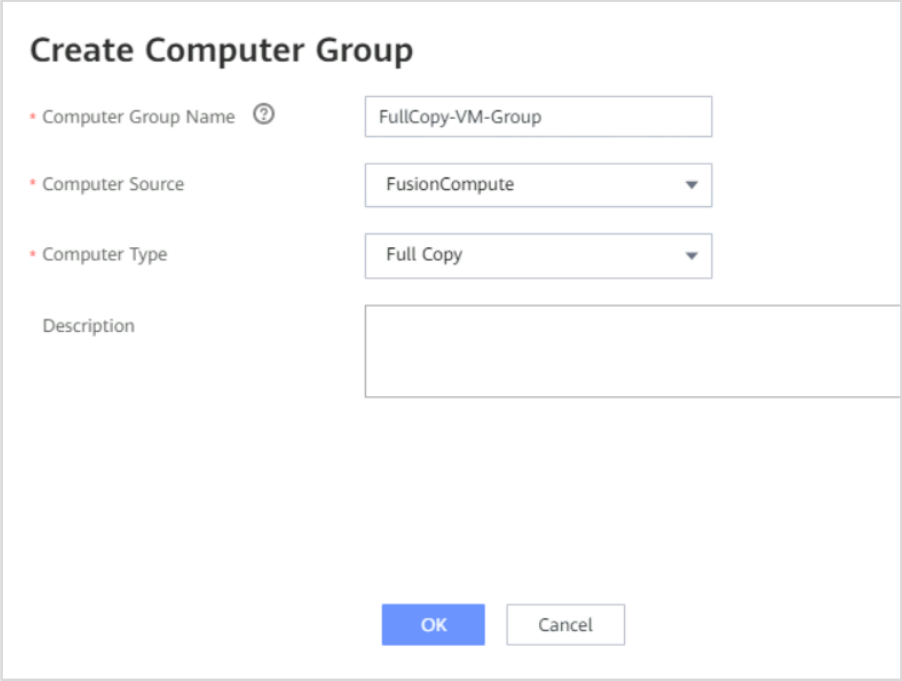


Figure 2-119 Configuring a computer group

Step 4 The message "Operation succeeded." is displayed. Click **OK**.

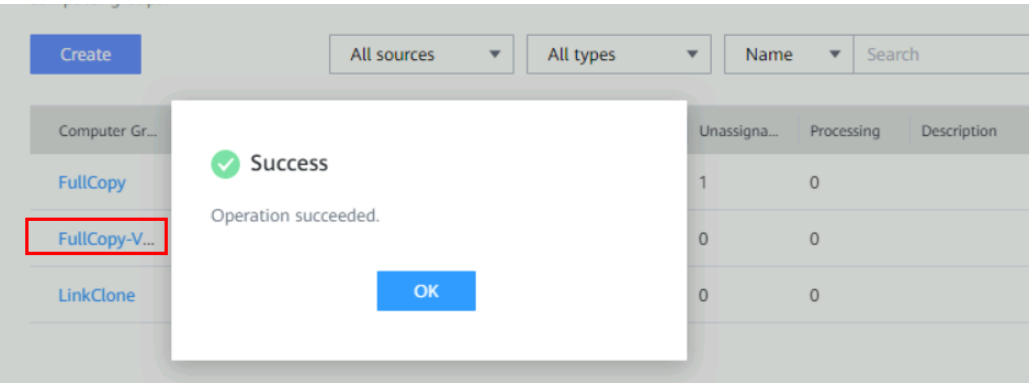


Figure 2-120 Successful operation

Step 5 On the **Computer Groups** page, click **Create** again.

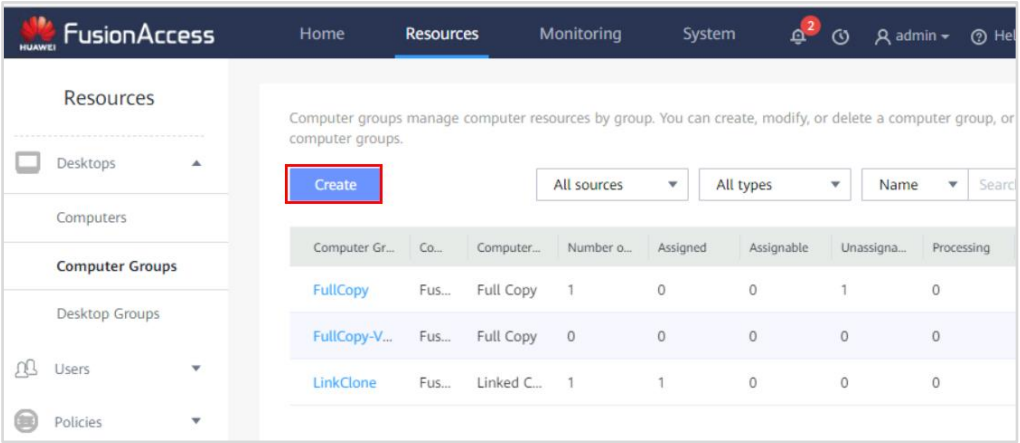


Figure 2-121 Creating a computer group

Step 6 Enter **LinkedClone-VM-Group** in **Computer Group Name**, select **FusionCompute** from the **Computer Source** drop-down list and **Linked Clone** from the **Computer Type** drop-down list, and click **OK**.

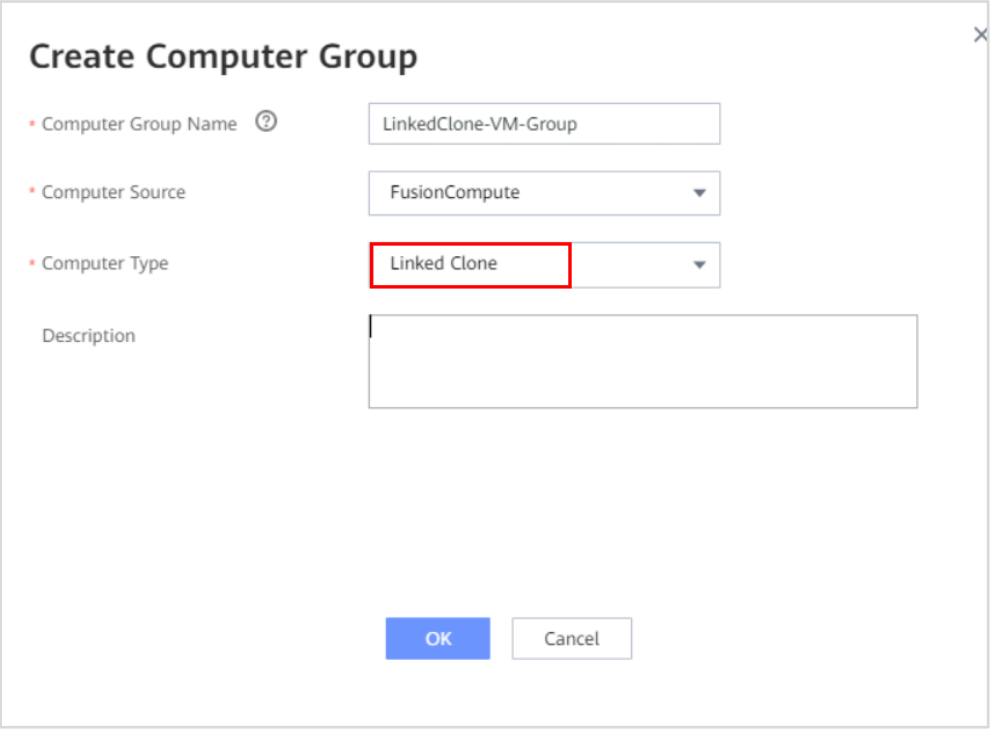


Figure 2-122 Configuring a computer group

Step 7 The message "Operation succeeded." is displayed. Click **OK**.

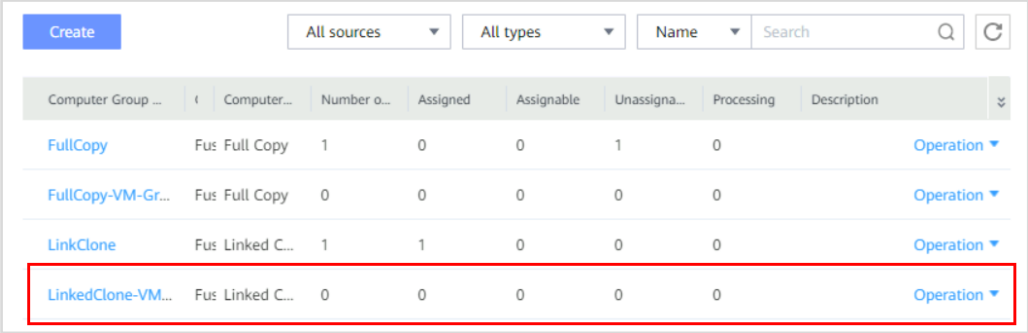


Figure 2-123 Successful operation

2.2.3.3 Create a Desktop Group

Step 1 On FusionAccess, choose **Resources** > **Desktops** > **Desktop Groups**.

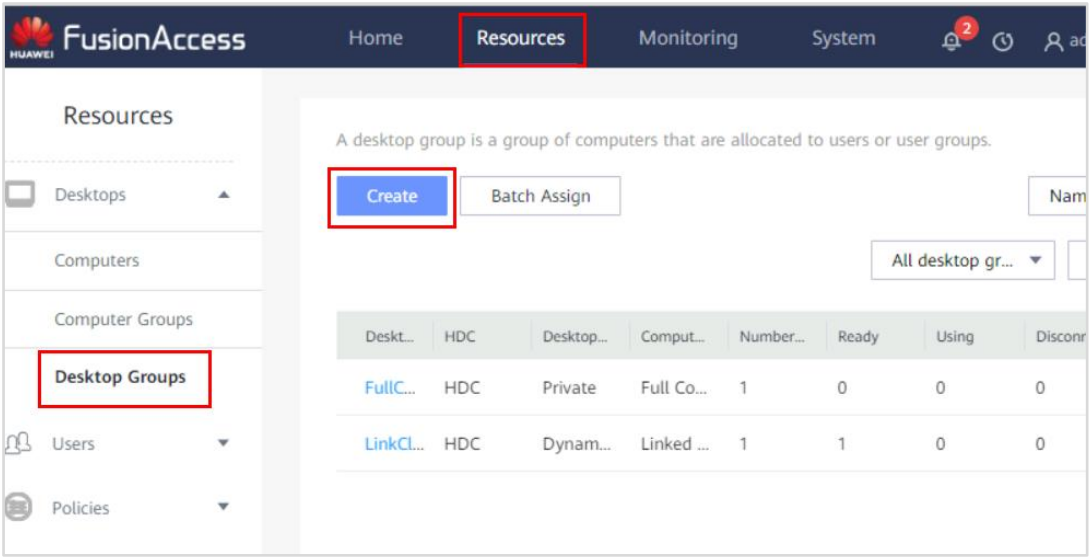


Figure 2-124 Creating a desktop group

Step 2 Click **Create**. The **Create Desktop Group** dialog box is displayed.

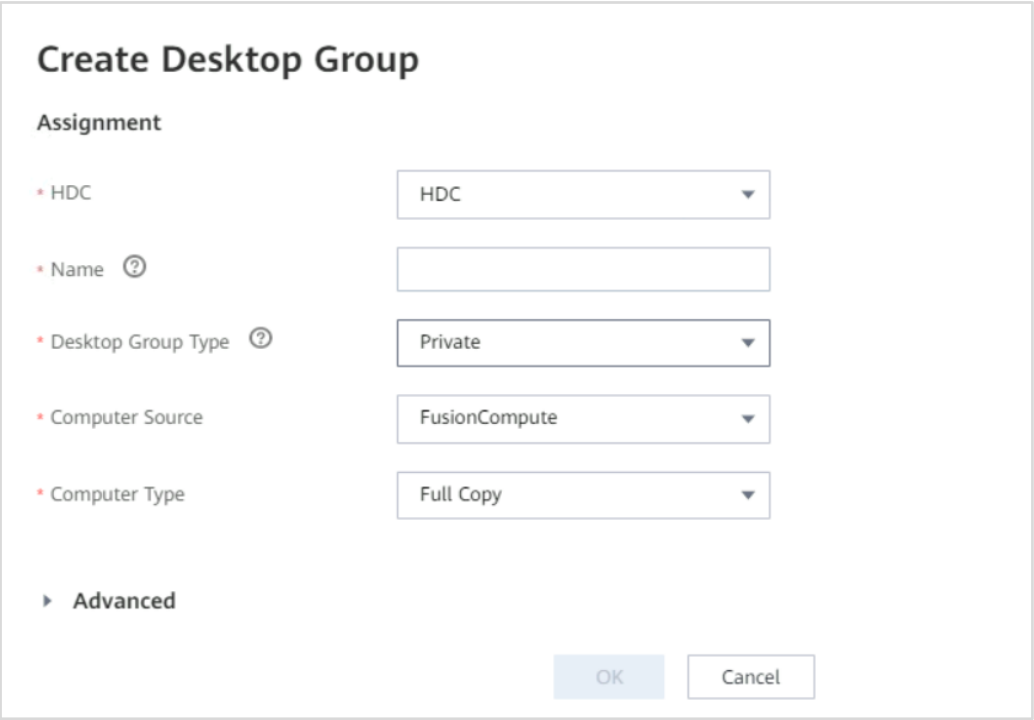


Figure 2-125 Configuring a desktop group 1

Step 3 In the displayed dialog box, select the configured HDC from the **HDC** drop-down list. HDC has been configured in **System** > **System Configuration** > **Desktop Components** > **HDC**. Set **Name** to **FullCopy-Desktop**. Set **Desktop Group Type** to **Private** and **Computer Type** to **Full Copy**, and click **OK**.

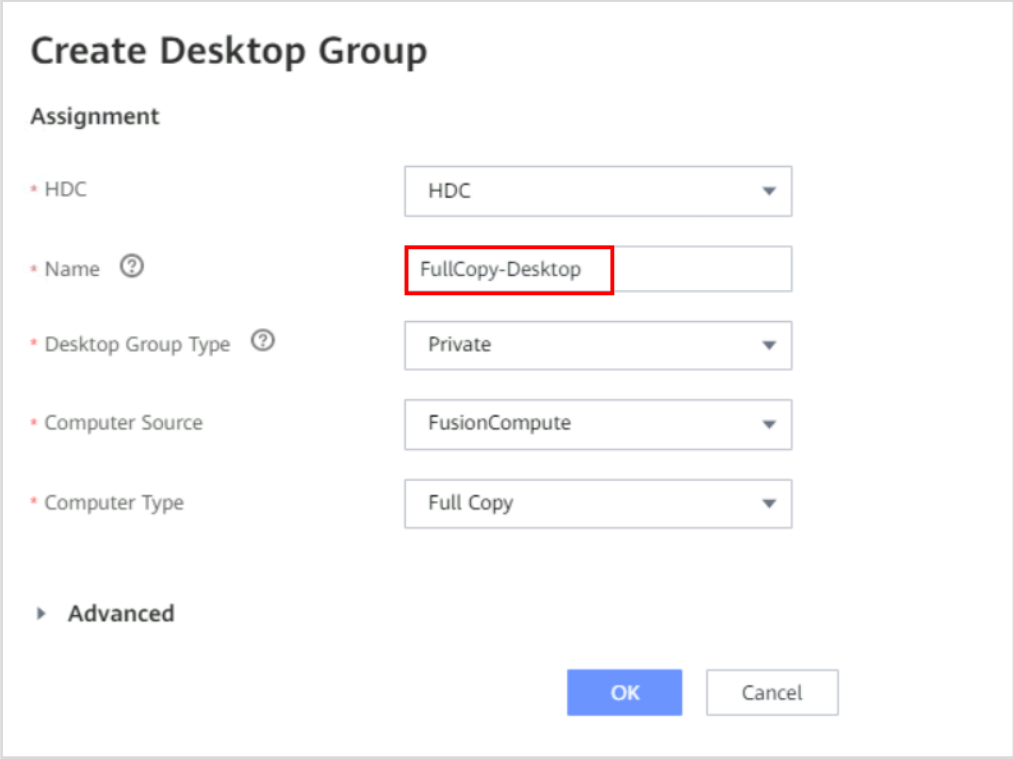


Figure 2-126 Configuring a desktop group 2

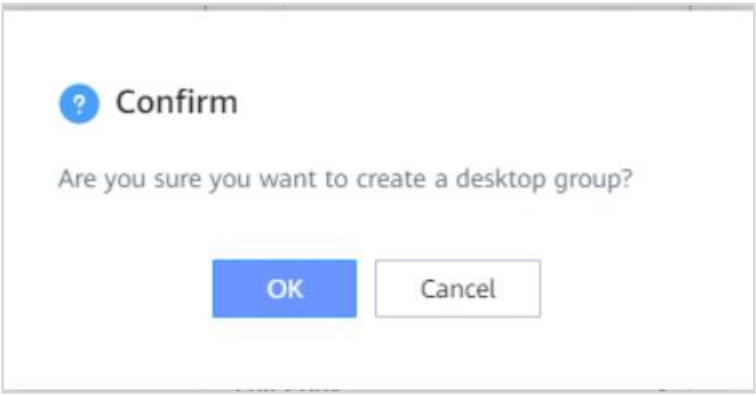


Figure 2-127 Confirming the creation

Step 4 Click **OK** in the **Confirm** dialog box. The message "Operation succeeded." is displayed. Click **OK** to return to the desktop group list.

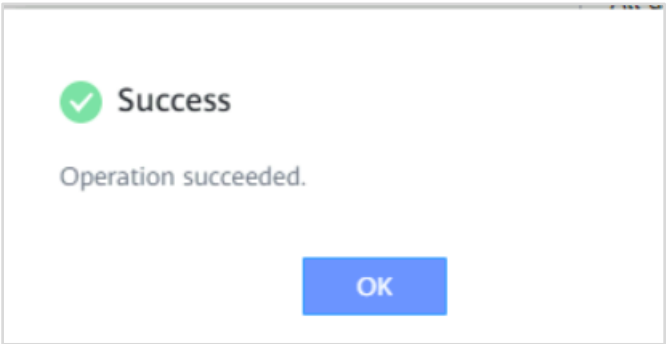


Figure 2-128 Successful operation

Step 5 On the **Desktop Groups** page, click **Create** again.

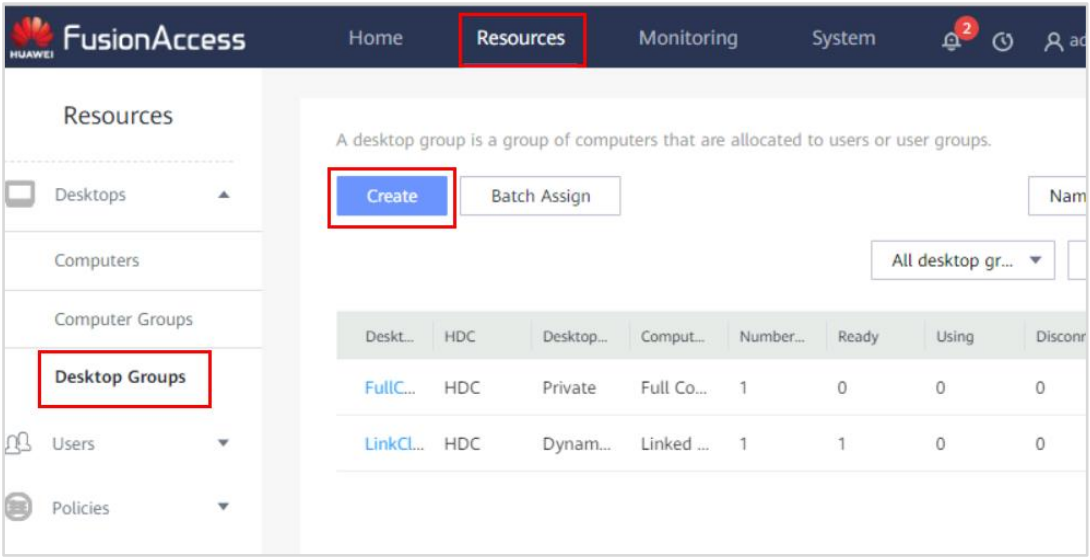


Figure 2-129 Creating a desktop group

Step 6 In the displayed dialog box, select the configured HDC from the **HDC** drop-down list. HDC has been configured in **System** > **System Configuration** > **Desktop Components** > **HDC**. Set **Name** to **LinkClone-Desktop**. Set **Desktop Group Type** to **Dynamic pool** and **Computer Type** to **Linked clone**, and click **OK**.

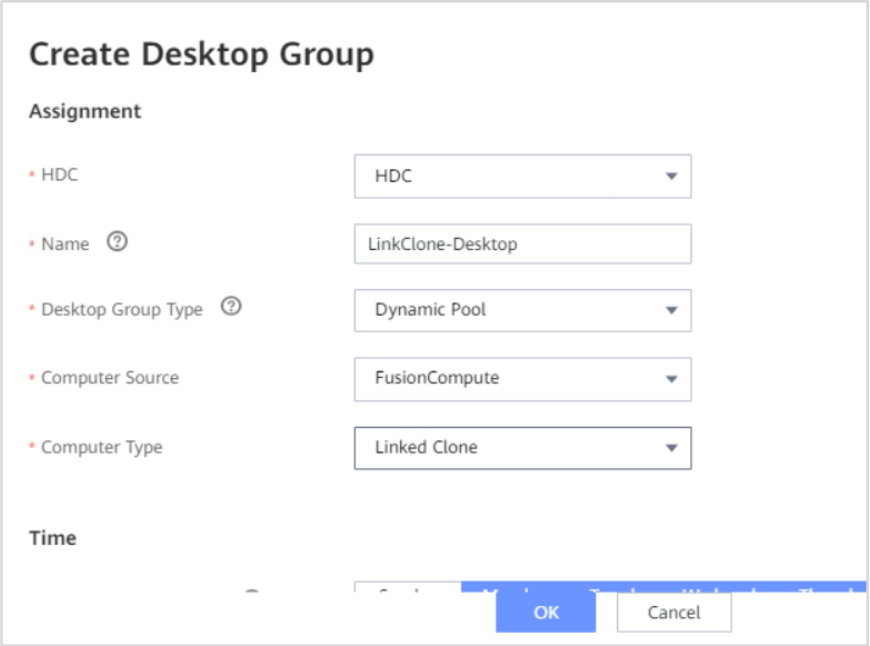


Figure 2-130 Configuring a desktop group

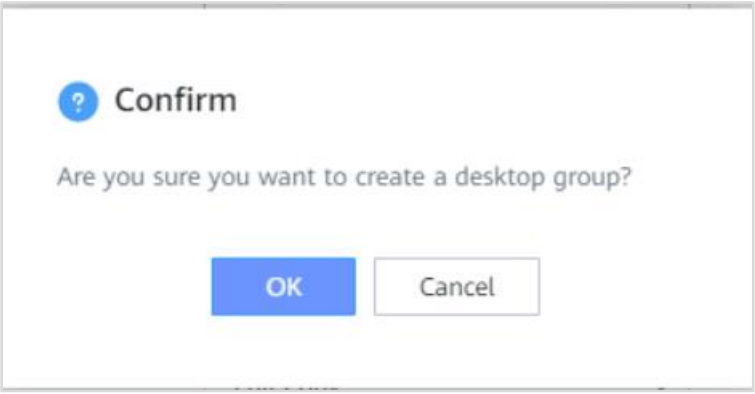


Figure 2-131 Confirming the creation

Step 7 Click **OK** in the **Confirm** dialog box. The message "Operation succeeded." is displayed. Click **OK** to return to the desktop group list.

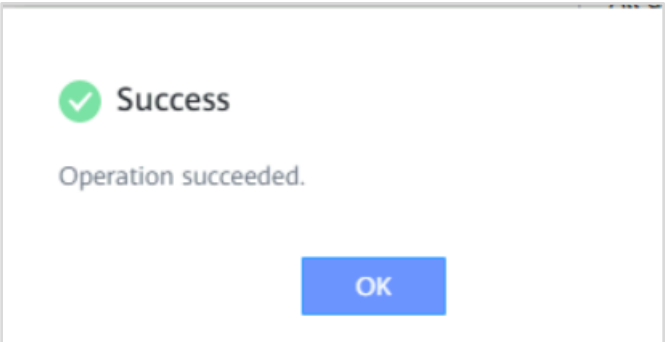


Figure 2-132 Successful operation

2.2.3.4 Provisioning a Full Copy Desktop

Step 1 On FusionAccess Web Client, click **Quick Provision**.

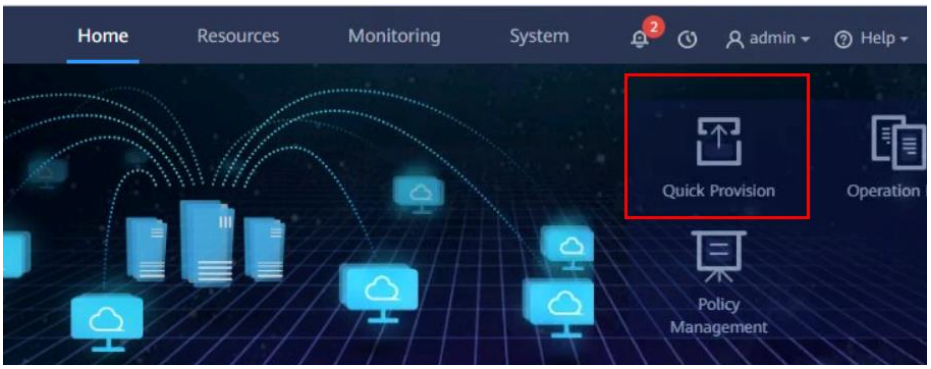


Figure 2-133 FusionAccess Web Client

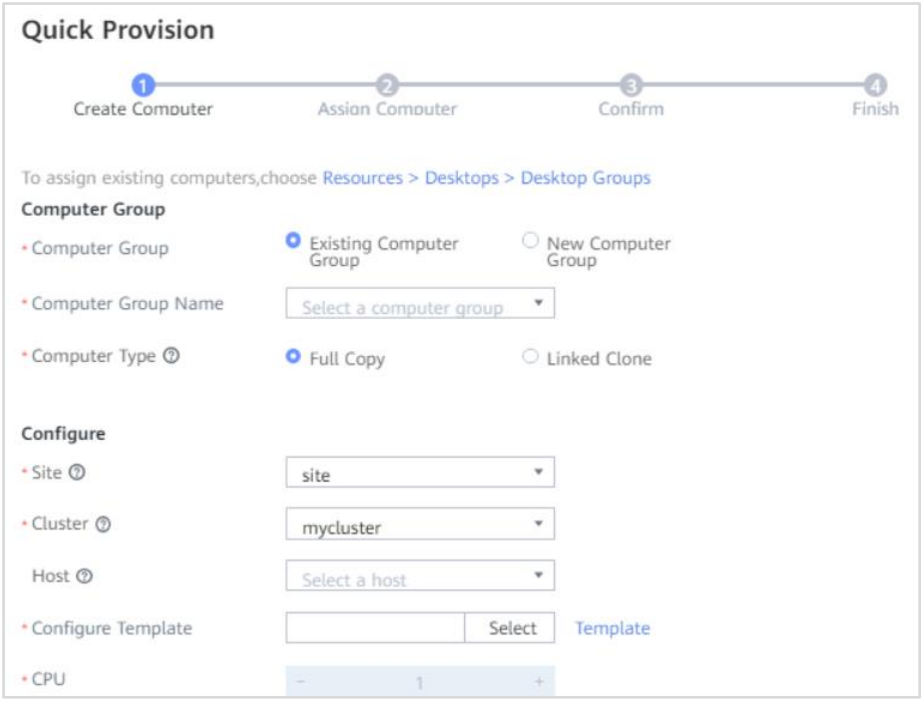


Figure 2-134 Quick provision

Step 2 Set **Computer Group** to **Existing Computer Group** and select **FullCopy-VM-Group** from the **Computer Group Name** drop-down list.

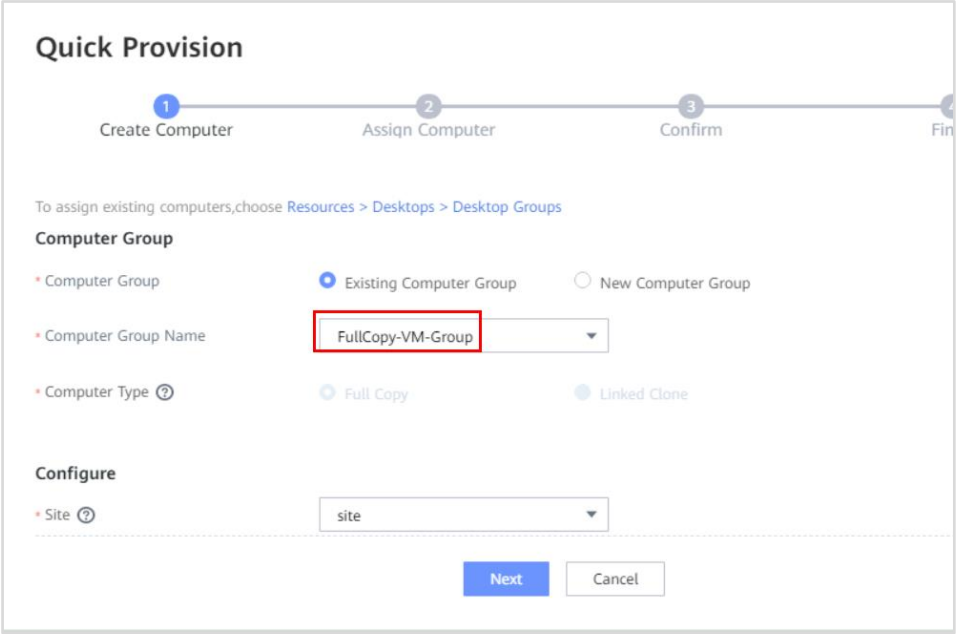


Figure 2-135 Computer group name

Step 3 Retain the default values for **Site** and **Cluster**. You do not need to set **Host**.

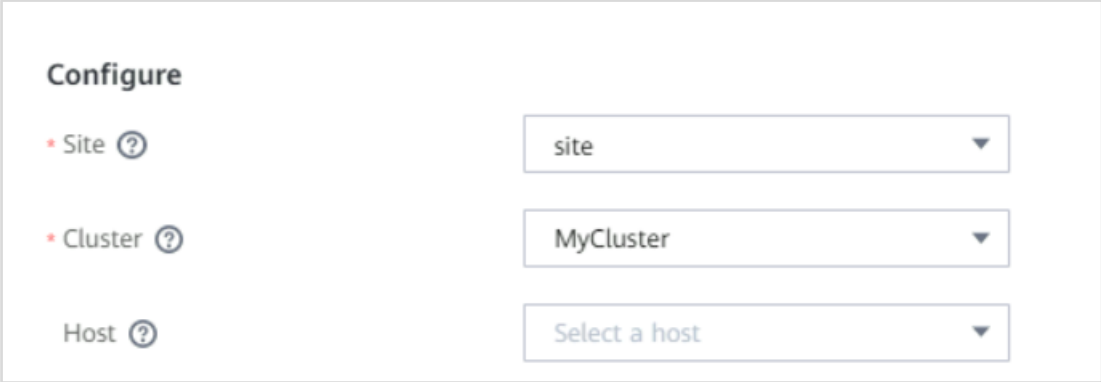


Figure 2-136 Configuring the site, cluster, and host

Step 4 In the **Configure Template** area, click **Template** to select a template and click **OK**.

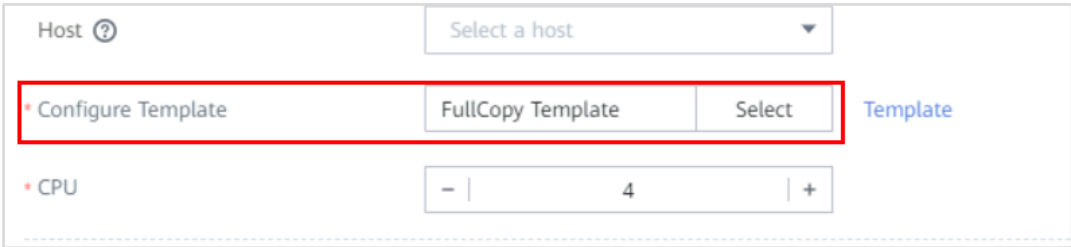


Figure 2-137 Selecting a VM template

Step 5 After you select a template, the **CPU**, **Memory (MB)**, **Disk**, and **NIC** information is automatically displayed. Retain the default values for CPU and memory or modify them as required.

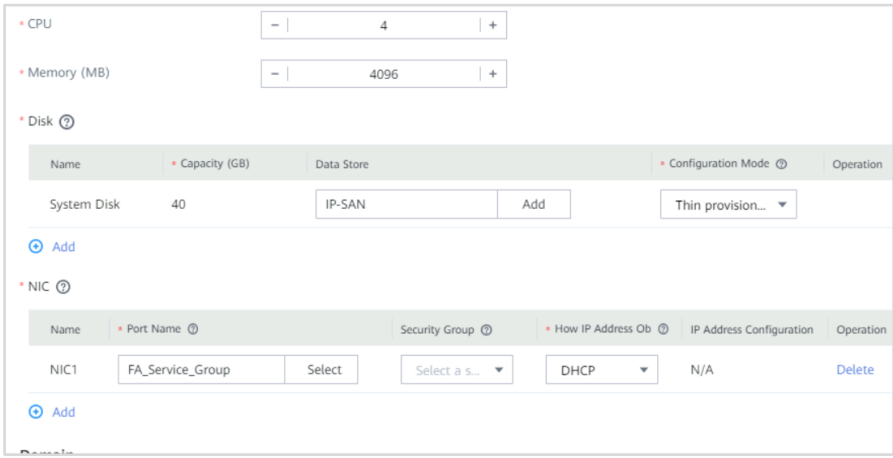


Figure 2-138 Specifications

Step 6 For a system disk, click **Add** in the **Data Store** column. In the displayed dialog box, select the desired data store and click **OK**. Select a configuration mode for the system disk. You are advised to select **Thick provisioning lazy zeroed**.

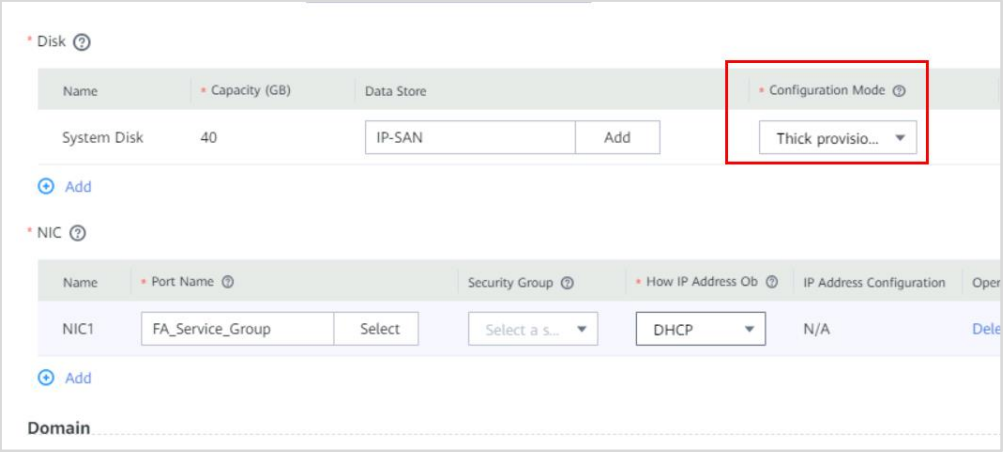


Figure 2-139 Configuring the system disk

Step 7 In the **NIC** area, click **Select** in the **Port Name** column. In the displayed dialog box, select the service-plane port group and click **OK**. Retain the default value for **Security Group**. Set **How IP Address Obtained** to **DHCP**.

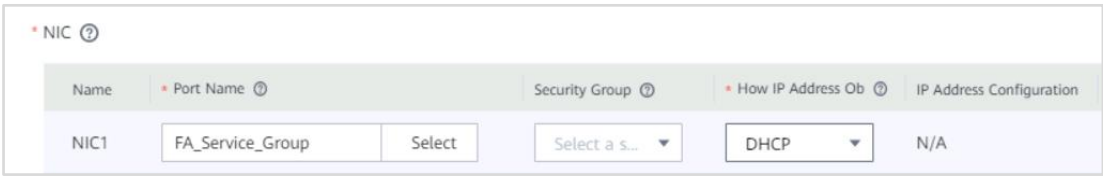


Figure 2-140 Setting a port group

Step 8 Set the number of computers to be provisioned in the **Quantity** area. You can create a maximum of 100 computers at a time.

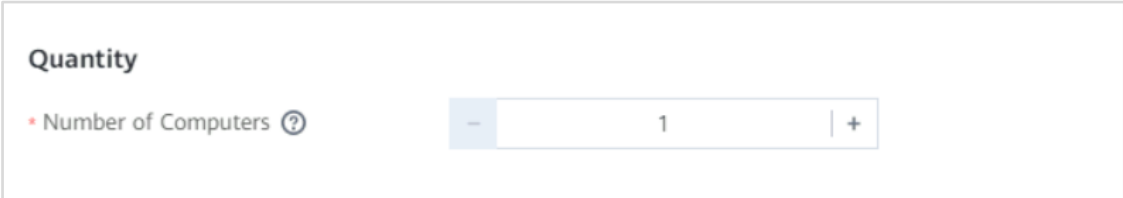


Figure 2-141 Setting the number of computers

Step 9 Configure a naming rule for computers. Click **Configure Naming Rule** and create a naming rule on the displayed **Configure Naming Rule** dialog box. After the configuration is complete, click **OK**

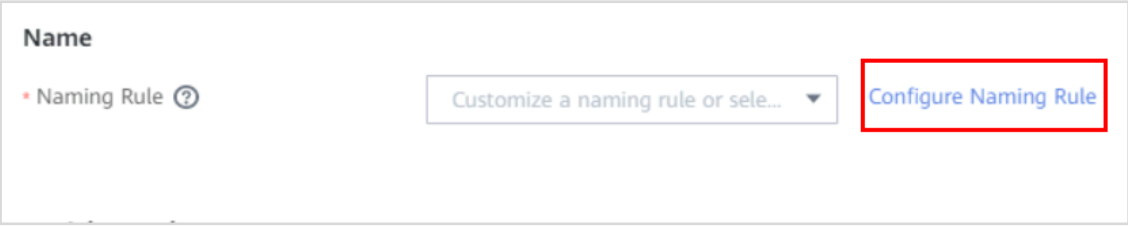


Figure 2-142 Configuring a naming rule

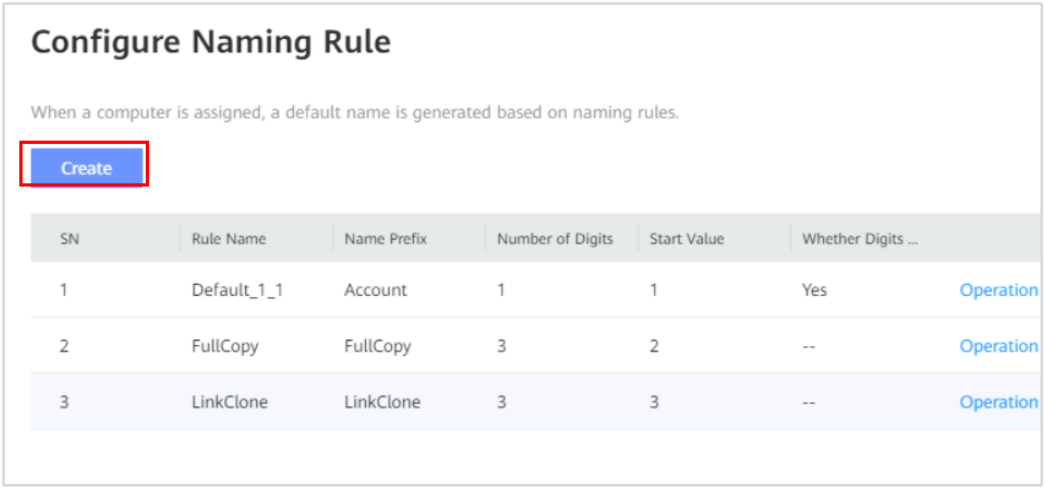


Figure 2-143 Adding a naming rule

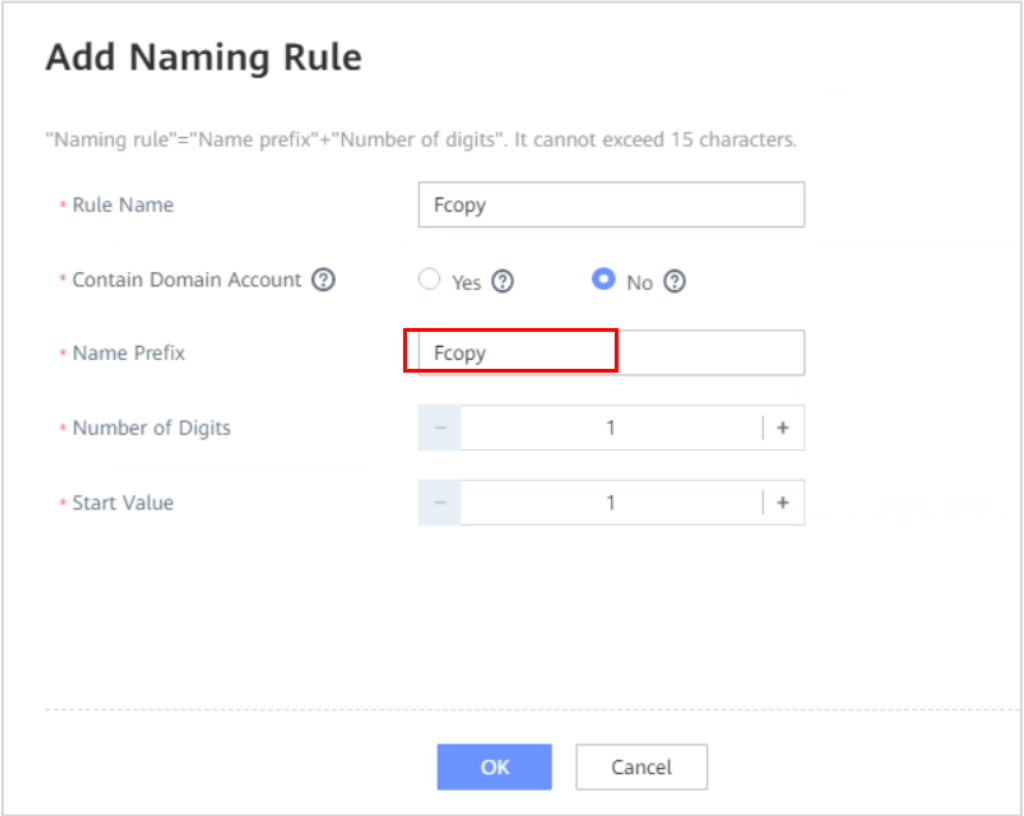


Figure 2-144 Configuring a VM naming rule

Set the VM naming rule to **Fcopy**.

The VM name prefix is the prefix of an unassigned VM. This parameter is optional when **VM Group Type** is set to **Full Copy**. In this exercise, set this parameter to **Fcopy**.

Step 10 In **Naming Rule**, select the naming rule configured in the previous step.

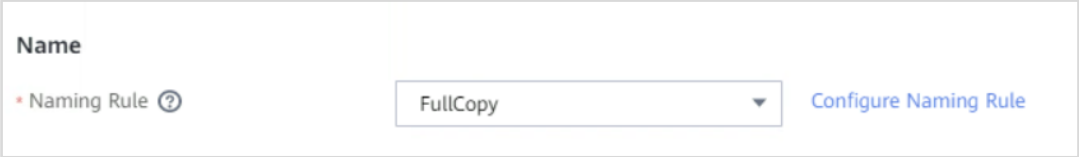


Figure 2-145 Selecting a naming rule

Step 11 Click **Next**. Select HDC information from the **HDC** drop-down list. Choose the HDC configured in **System** > **System Configuration** > **Desktop Components** > **HDC**.

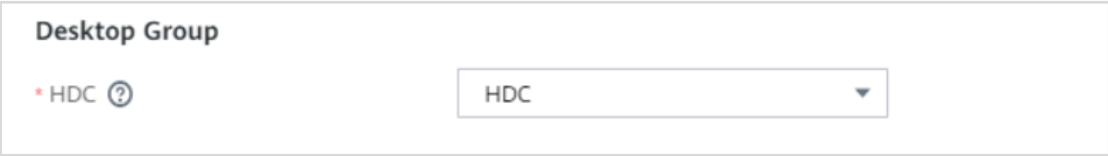


Figure 2-146 Selecting HDC

Step 12 Configure the desktop group to which the computer to be provisioned belongs. If you have configured a desktop group under **Resources** > **Desktops** > **Desktop Groups**, select **Existing Desktop Group**. Set **Desktop Group Type** to **Private**.

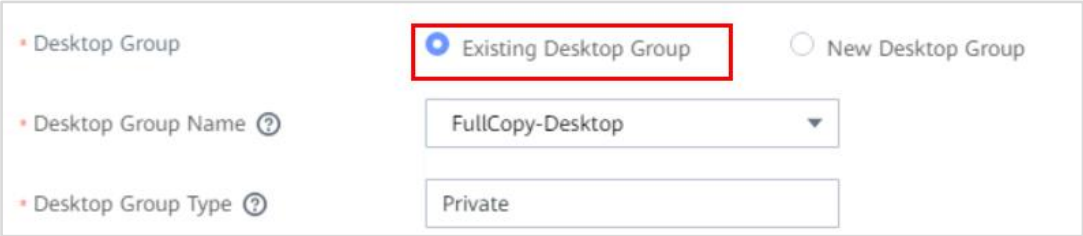


Figure 2-147 Selecting an existing desktop group

Step 13 Set **Assignment Type** to **Assign a Computer to a User**.

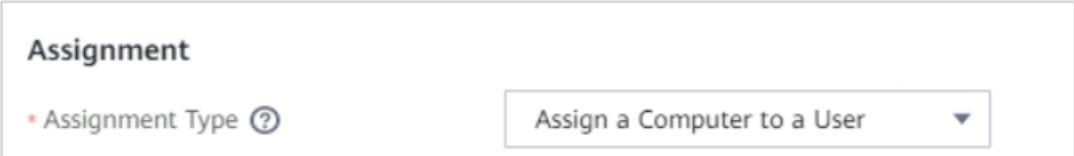


Figure 2-148 Selecting the assignment type

Step 14 In the **Add User (Group)** area, click **Add** to configure the domain user to which the computer is to be assigned. In the **Set User Group** area, set the user permissions on assigned computers as prompted.

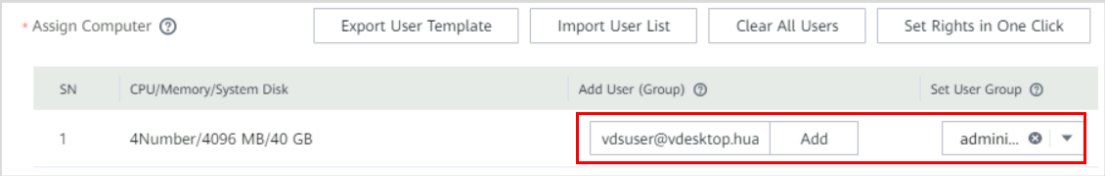


Figure 2-149 Adding a user (group)

Step 15 Click **Next**. Check the configuration of the computer to be provisioned. If the configuration is correct, click **OK**.

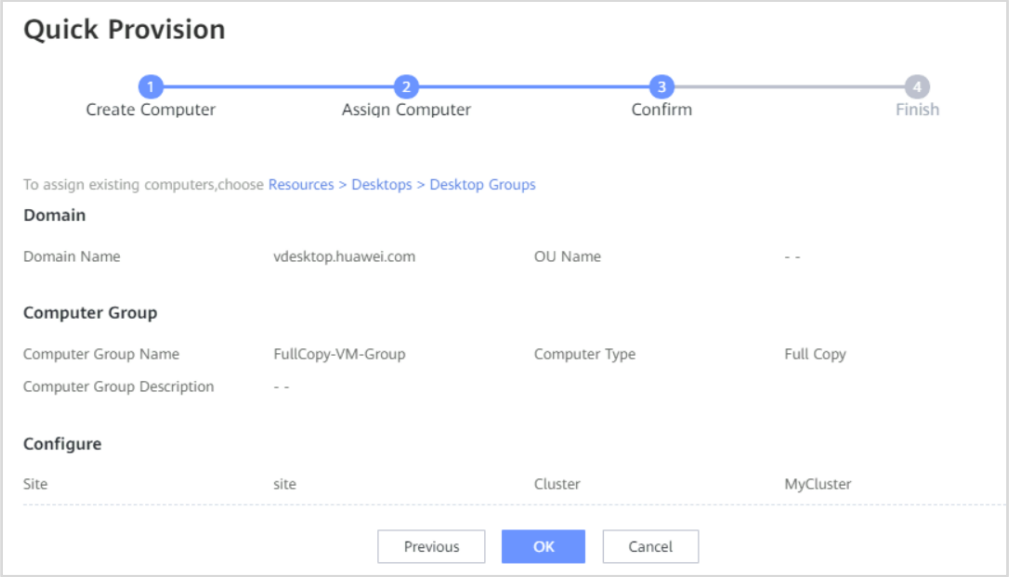


Figure 2-150 Checking the configuration of the computer to be provisioned

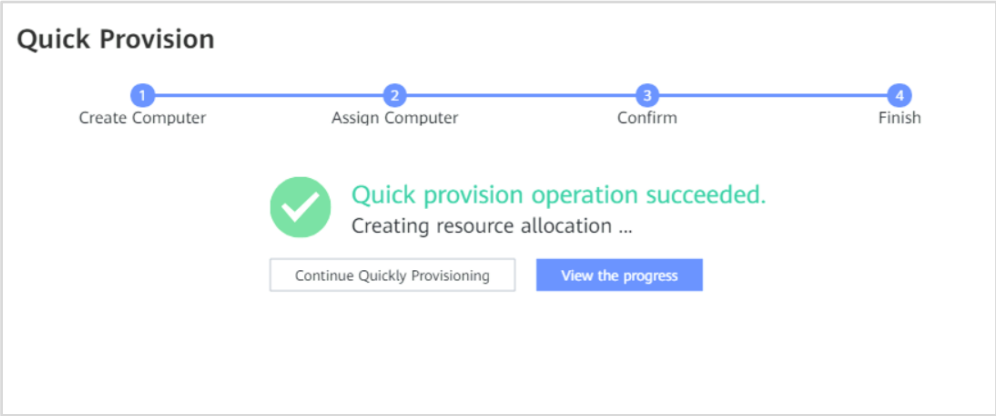


Figure 2-151 Confirming the provisioning

2.2.3.5 Provisioning a Linked Clone Desktop

Step 1 On FusionAccess Web Client, click **Quick Provision**.

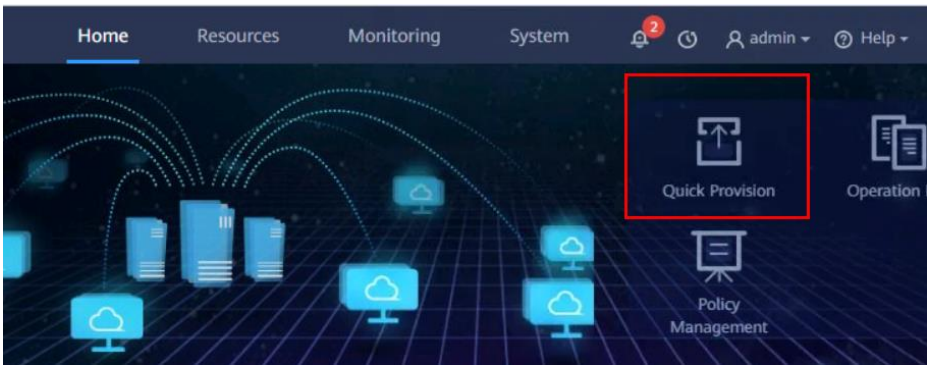


Figure 2-152 FusionAccess Web Client

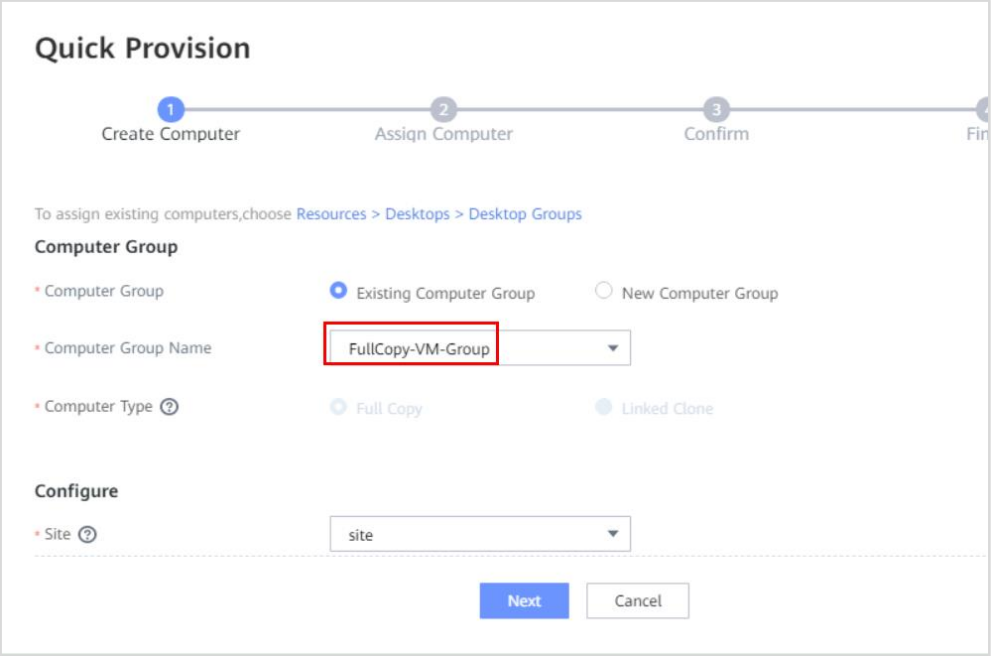


Figure 2-153 Quick provision

Step 2 Set **Computer Group** to **Existing Computer Group** and select **LinkClone-VM-Group** from the **Computer Group Name** drop-down list.

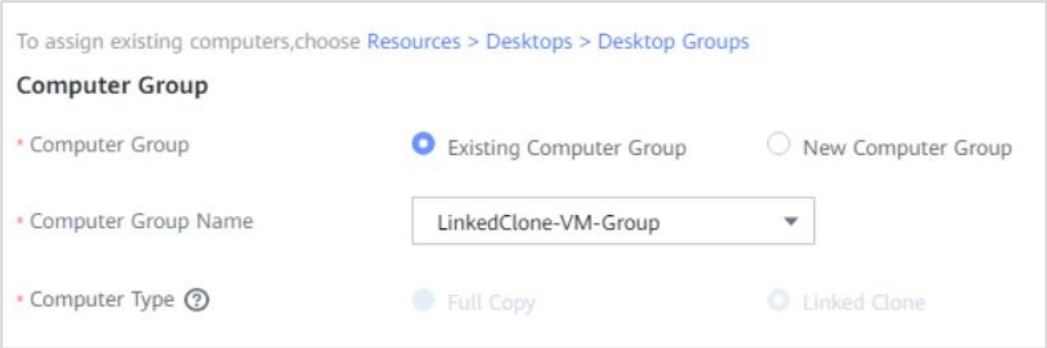


Figure 2-154 Selecting a computer group

Step 3 Retain the default values for **Site** and **Cluster**. You do not need to set **Host**.

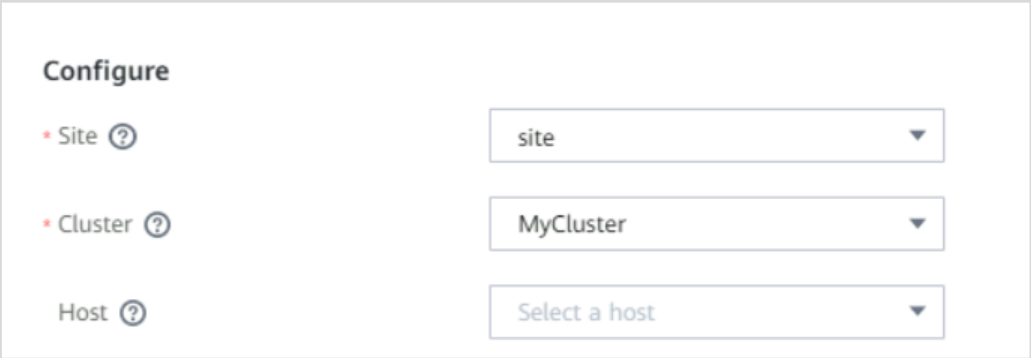


Figure 2-155 Configuring the site and cluster

Step 4 In the **Configure Template** area, click **Template** to select a template and click **OK**.

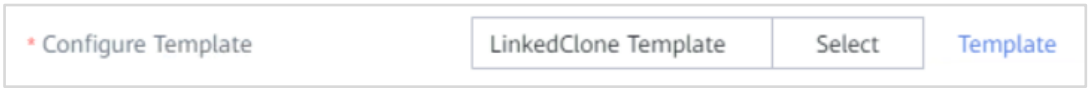


Figure 2-156 Selecting a VM template

Step 5 After you select a template, the **CPU**, **Memory (MB)**, **Disk**, and **NIC** information is automatically displayed. Retain the default values for CPU and memory or modify them as required.

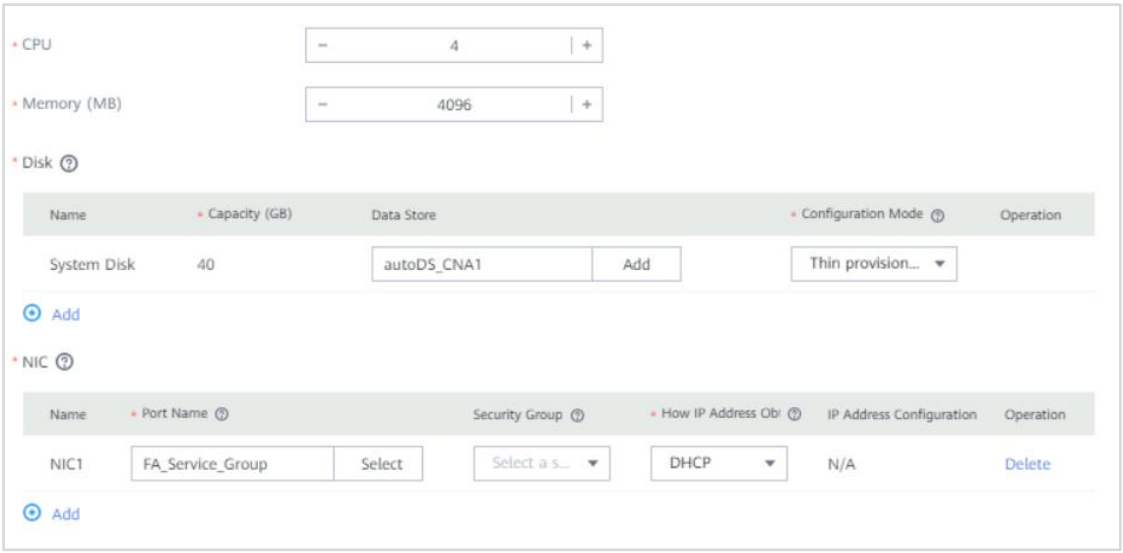


Figure 2-157 Specifications

Step 6 For a system disk, click **Add** in the **Data Store** column. In the displayed dialog box, select the desired data store and click **OK**. Set **Configuration Mode** to **Thin provisioning**.

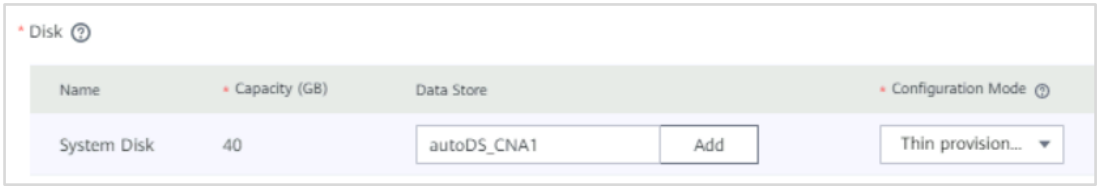


Figure 2-158 Configuring the system disk

Step 7 In the **NIC** area, click **Select** in the **Port Name** column. In the displayed dialog box, select the service-plane port group and click **OK**. Retain the default value for **Security Group**. Set **How IP Address Obtained** to **DHCP**.

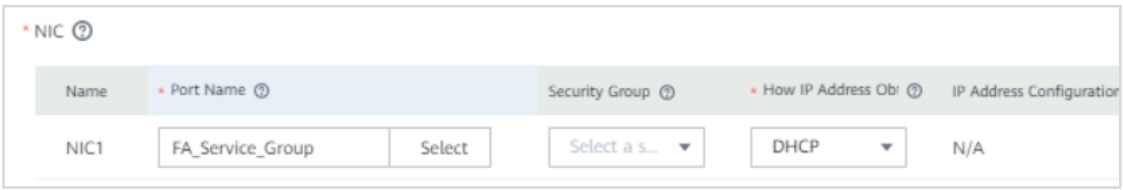


Figure 2-159 Setting a port group

Step 8 Set the number of computers to be provisioned in the **Quantity** area. You can create a maximum of 100 computers at a time.

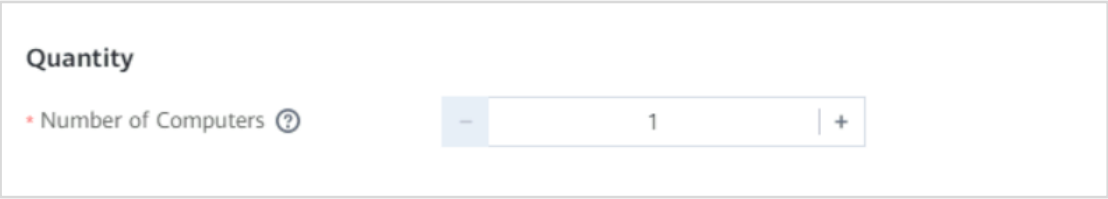


Figure 2-160 Setting the number of computers

Step 9 Configure a naming rule for computers. Click **Configure Naming Rule** and create a naming rule on the displayed **Configure Naming Rule** dialog box. After the configuration is complete, click **OK**

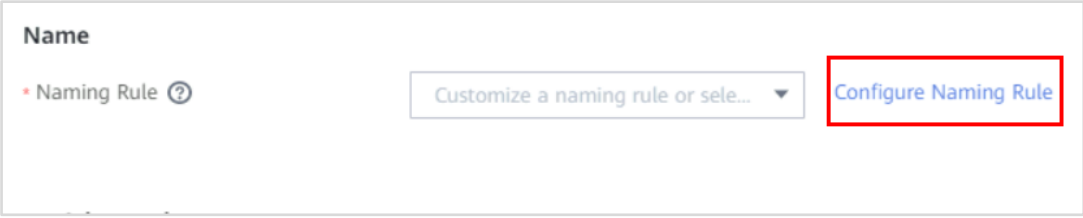


Figure 2-161 Configuring a naming rule

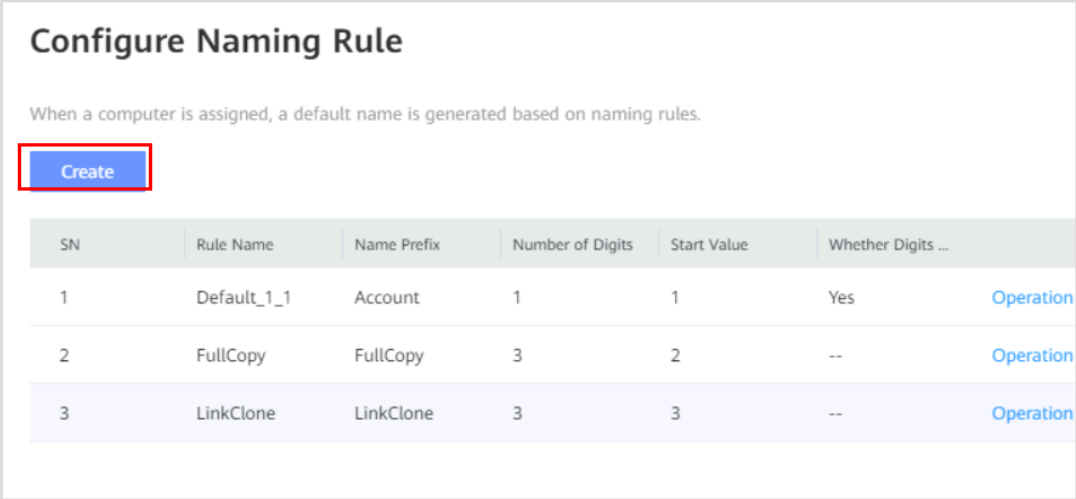


Figure 2-162 Adding a naming rule

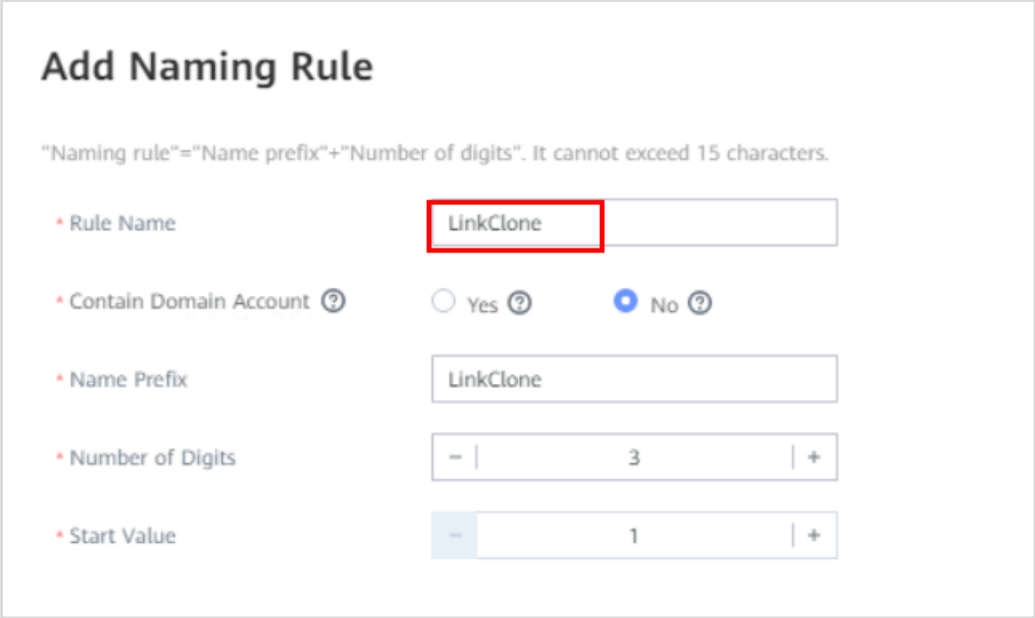


Figure 2-163 Modifying a naming rule

Set the VM naming rule to **LinkClone**.

The VM name prefix is the prefix of an unassigned VM. If **VM Group Type** is set to **Linked Clone**, set this parameter to **LinkClone**.

Step 10 In **Naming Rule**, select the naming rule configured in the previous step.

Figure 2-164 Selecting a naming rule

Step 11 Click **Next** and select HDC information from the **HDC** drop-down list. Choose the HDC configured in **System** > **System Configuration** > **Desktop Components** > **HDC**.

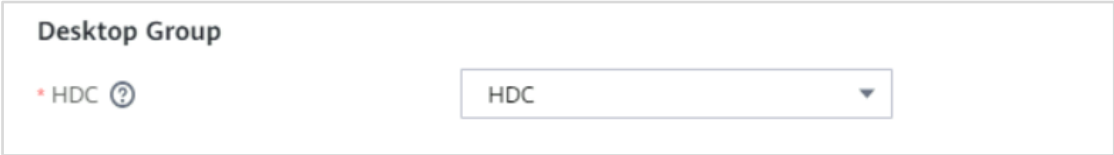


Figure 2-165 Selecting HDC

Step 12 Configure the desktop group to which the computer to be provisioned belongs. If you have configured a desktop group under **Resources** > **Desktops** > **Desktop Groups**, set **Desktop Group** to **Existing Desktop Group** and **Desktop Group Name** to **LinkClone-Desktop**. Set **Desktop Group Type** to **Dynamic Pool**.

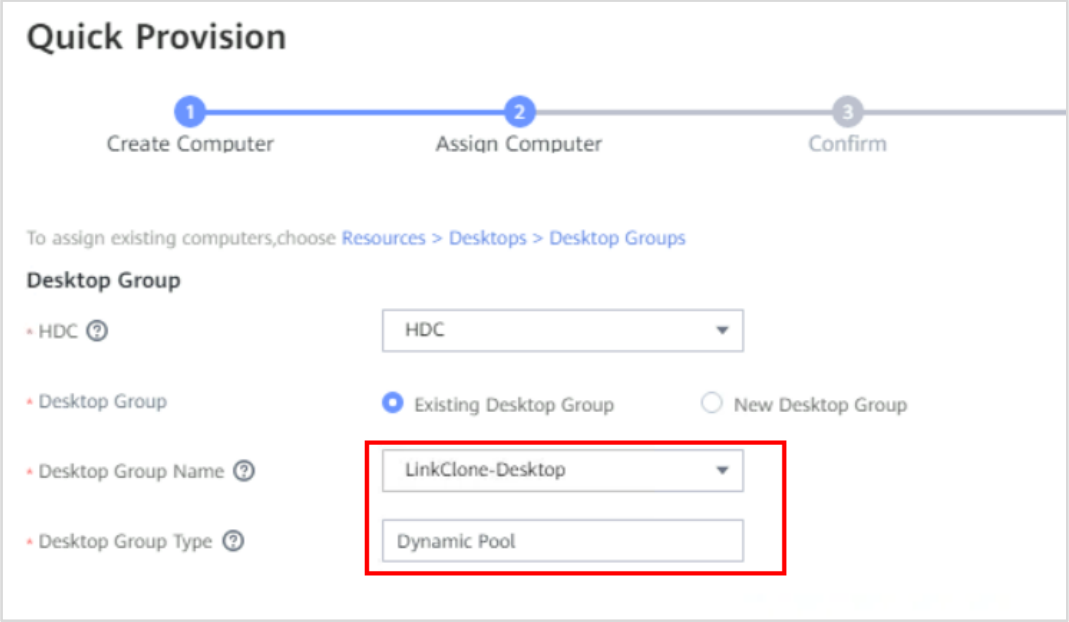


Figure 2-166 Selecting an existing desktop group

Step 13 In the **Add User (Group)** area, click **Add** to configure the domain user to which the computer is to be assigned. In the **Set User Group** area, set the user permissions on assigned computers as prompted.

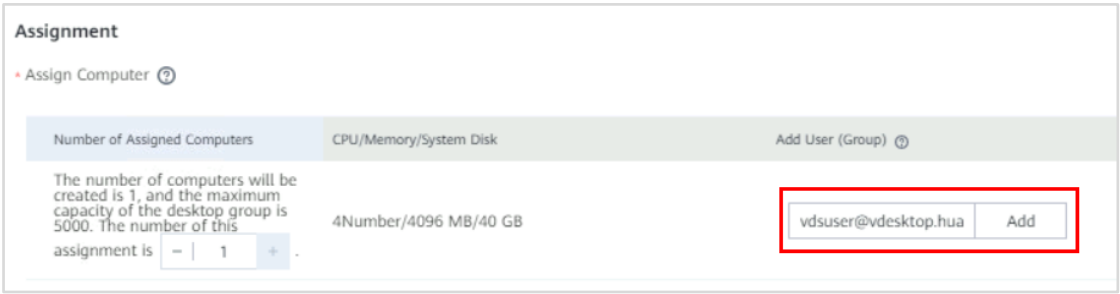


Figure 2-167 Adding a user (group)

Step 14 Click **Next**. Check the configuration of the computer to be provisioned. If the configuration is correct, click **OK**.

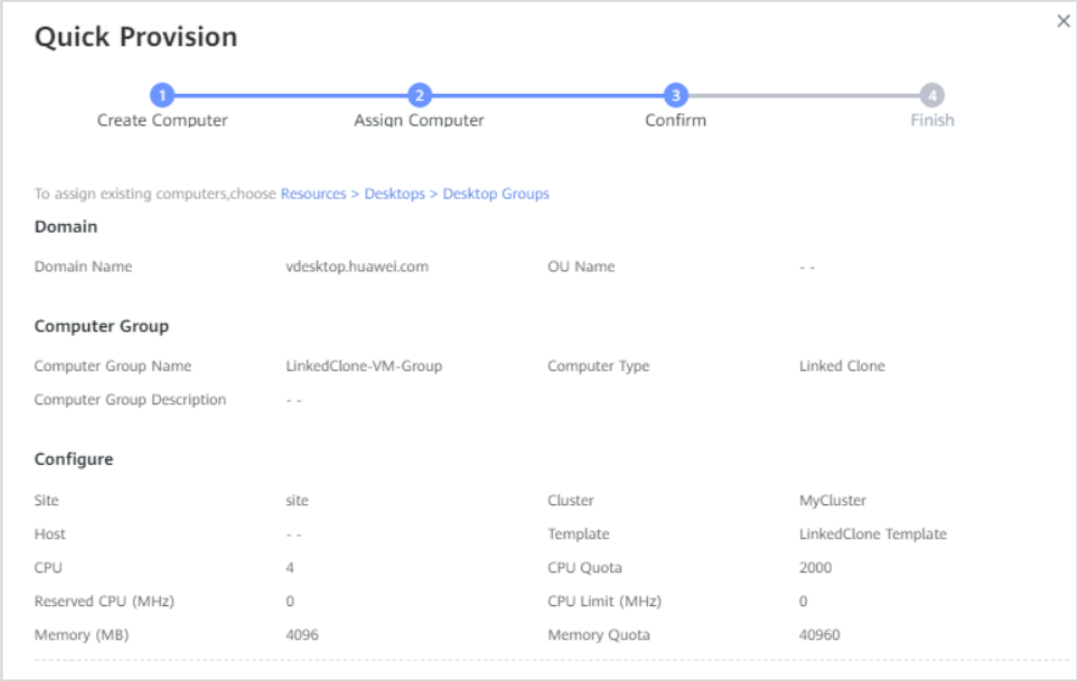


Figure 2-168 Checking the configuration of the computer to be provisioned

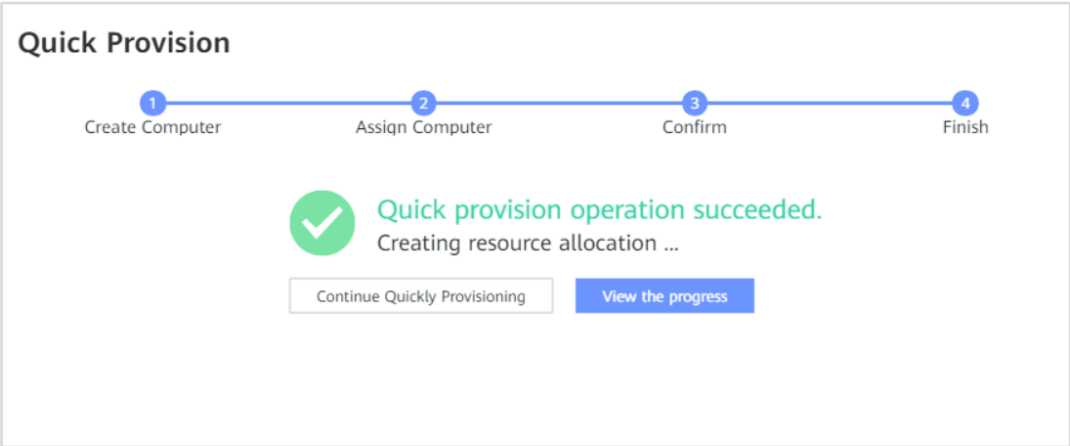


Figure 2-169 Confirming the provisioning

Step 15 Choose **System** > **Task Tracing** and click **View** of the corresponding task to check the progress. You can also view the process on the **Task Center** of FusionCompute.

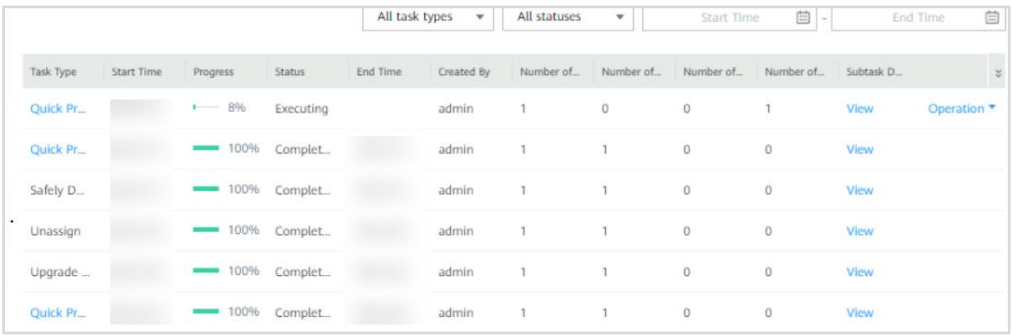


Figure 2-170 Viewing the VM creation process

Step 16 After the task has been executed, you can view the linked clone VM on FusionCompute.

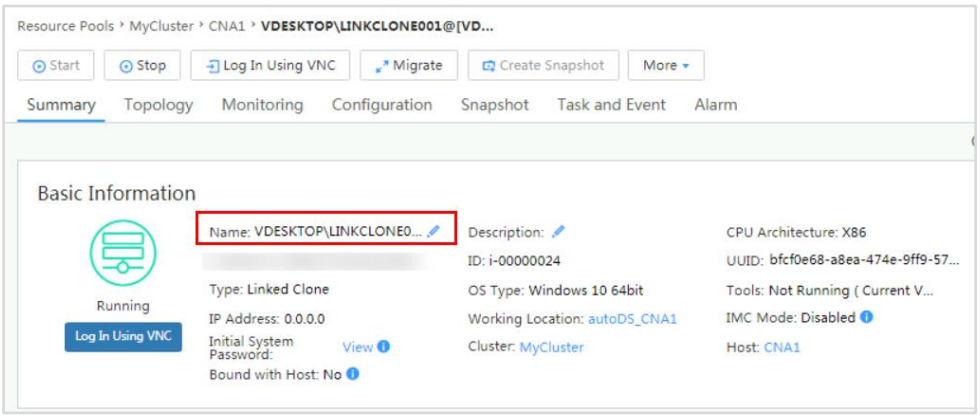


Figure 2-171 Viewing the linked clone VM

2.2.4 Logging In to a Desktop Using an SC

Step 1 Ping the IP address of the vAG server on the test device (PC). If the address cannot be pinged, check the local IP address configuration of the test device (PC).

Step 2 In the test device (PC) browser, enter the IP address of the vAG server, for example, **192.168.105.10**, and press **Enter**.

Note:

When you access the address for the first time, the message "Your connection is not private" is displayed. Choose **HIDE ADVANCED** > **Proceed to 192.168.105.10 (unsafe)**.

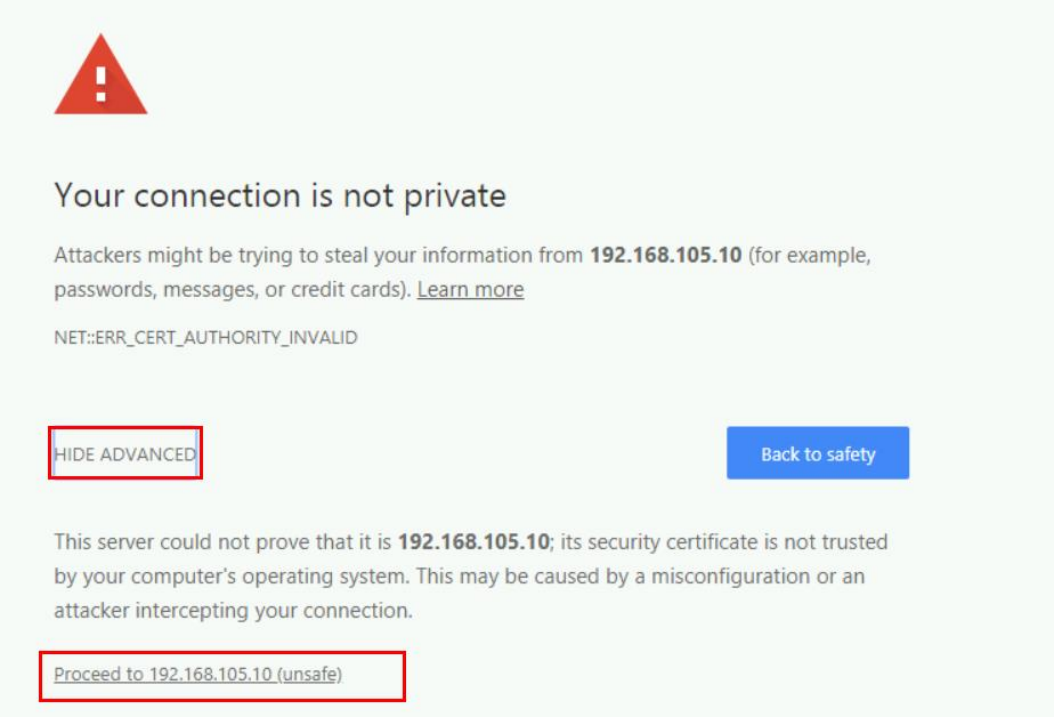


Figure 2-172 Accepting the risk and proceeding

Step 3 On the login page, enter the domain username and password to log in to the system.

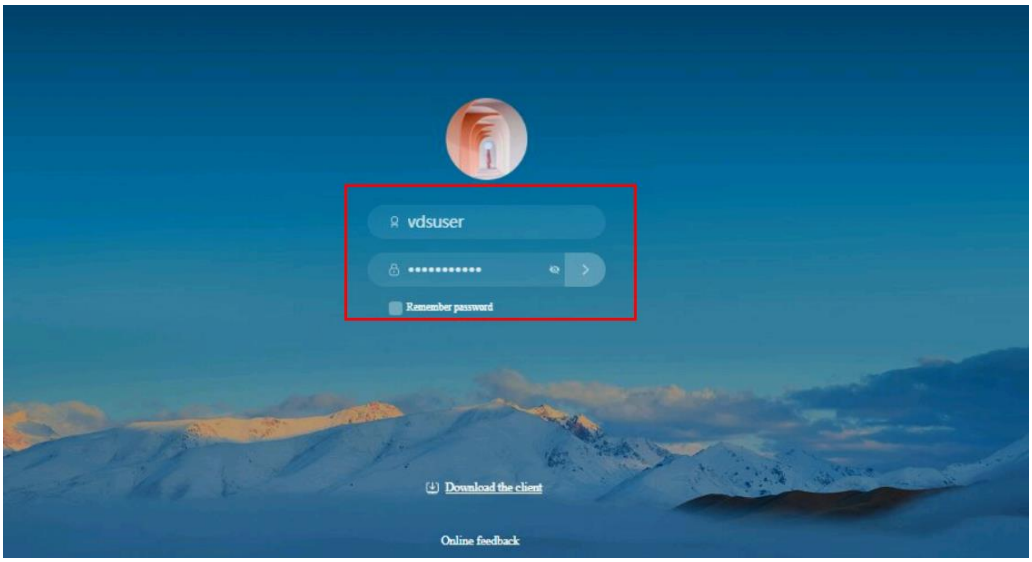


Figure 2-173 Login page

Step 4 After logging in, you can view the available cloud desktops. You can also click **Download the client** at the bottom of the page to download and install the cloud client.

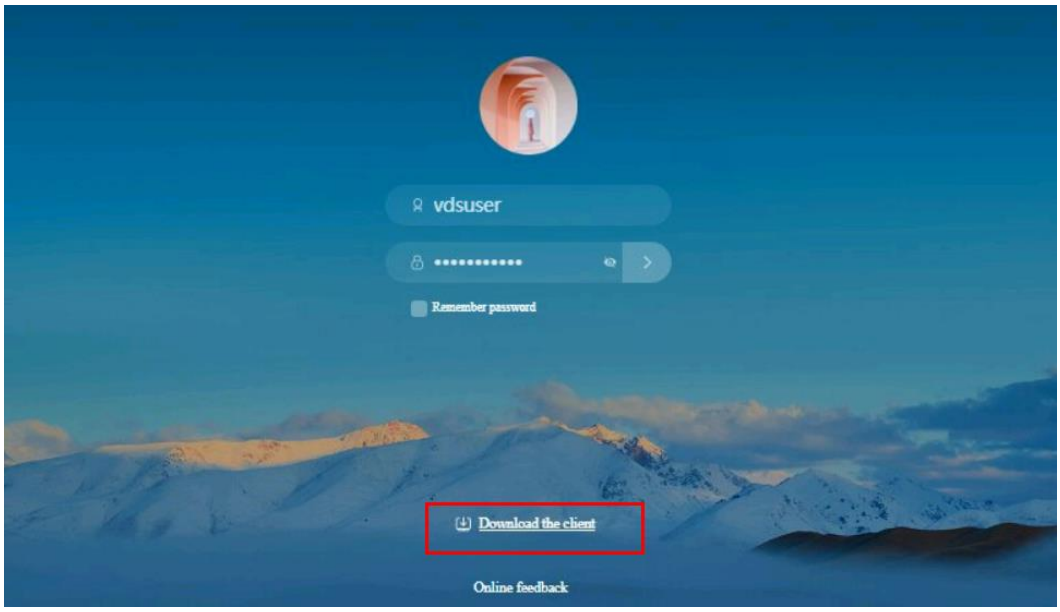


Figure 2-174 Downloading a client

Step 5 After the installation is complete, the VM to be logged in to is automatically selected from the VM list.

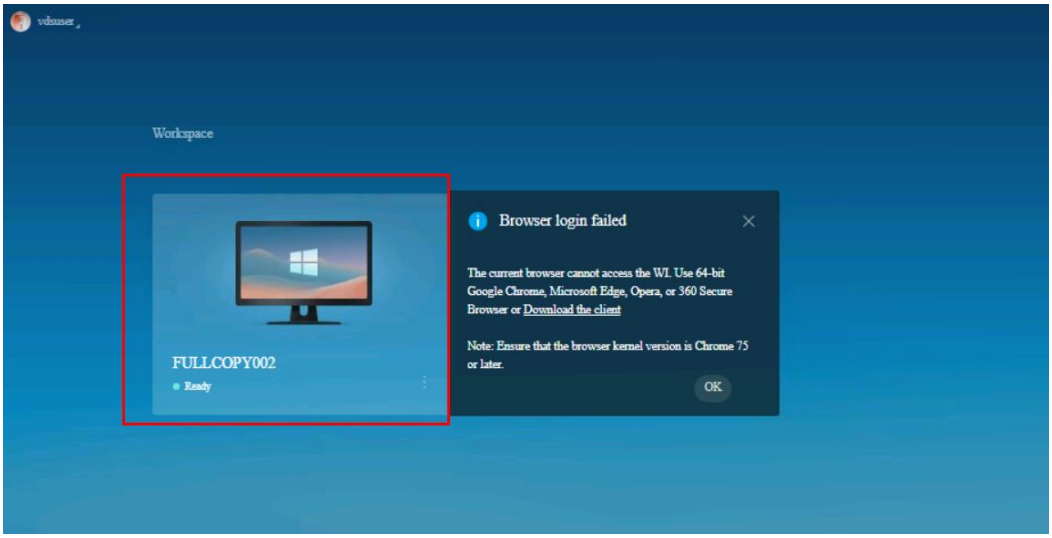


Figure 2-175 Available VMs

Step 6 After the login is successful, the virtual desktop is automatically displayed.

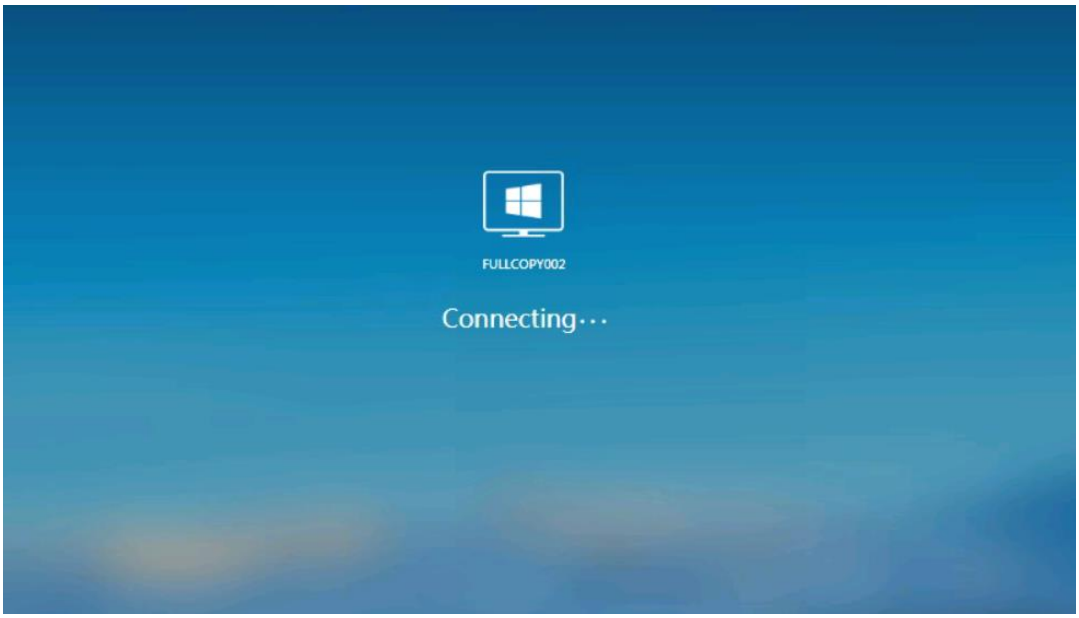


Figure 2-176 Virtual desktop

2.3 Quiz

Why is an organizational unit (OU) required before creating user groups and users? Must an OU be created?

Answers:

OUs are created to facilitate the management of users and user groups stored on the AD domain controller. If the domain controller is directly used to manage resources such as users, the organizational structure cannot be clearly presented. However, the OU can.

If you do not create an OU, you can proceed with the subsequent steps.

Can the disk configuration mode be common or thick provisioning lazy zeroed when you provision a linked clone desktop? If not, why?

Answer: No. The configuration mode of linked clone desktop disks must be thin provisioning. Multiple linked clone desktops of a source computer template can share the same disk space (typically the system disk, that is, the base volume).

3 FusionAccess O&M and Management

3.1 Overview

3.1.1 About This Exercise

This section describes how to perform virtual desktop O&M, including virtual desktop service adjustment, self-service maintenance, policy control, notification sending, and user desktop reclaiming.

3.1.2 Objectives

Upon completion of this exercise, you will understand:

- How to modify the virtual desktop specifications
- How to add users
- How to add virtual desktops
- How to upgrade a common desktop to a VIP desktop
- How to unassign virtual desktops and restore virtual desktop assignment
- How to perform self-service maintenance
- How to manage the virtual desktop policy

3.1.3 Procedure

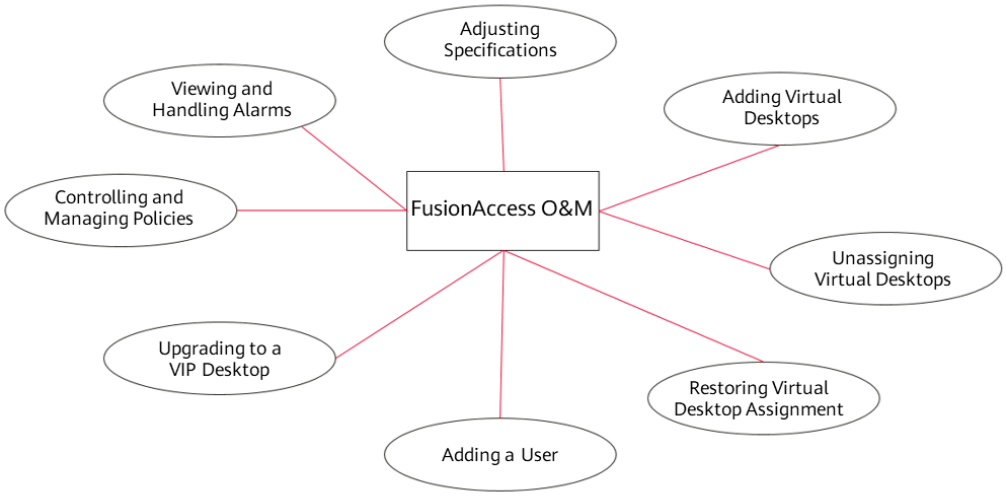


Figure 3-1 Flowchart

3.2 Exercise Configuration

3.2.1 Policy Management

3.2.1.1 File Redirection

Set a file redirection policy and apply it to the created user **vdsuser**. Drives installed on the local client are redirected to the virtual desktop. The virtual desktop is read-only for the user. That is, users are allowed to copy files from clients to virtual desktops but not from virtual desktops to clients.

Step 1 On FusionAccess, choose **Resources** > **Policies** > **Protocol Policies**, and click **Create**.

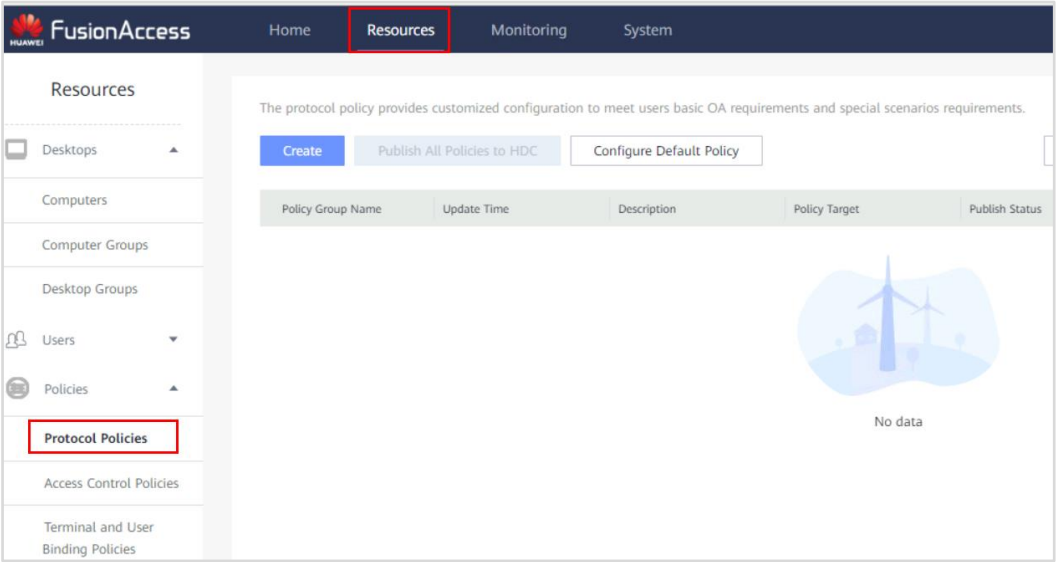


Figure 3-2 Creating a policy group

Step 2 On the **Create Policy Group** page, specify **Policy Group Name**, set **Creation Mode** to **New Policy Group**, and click **Next**.

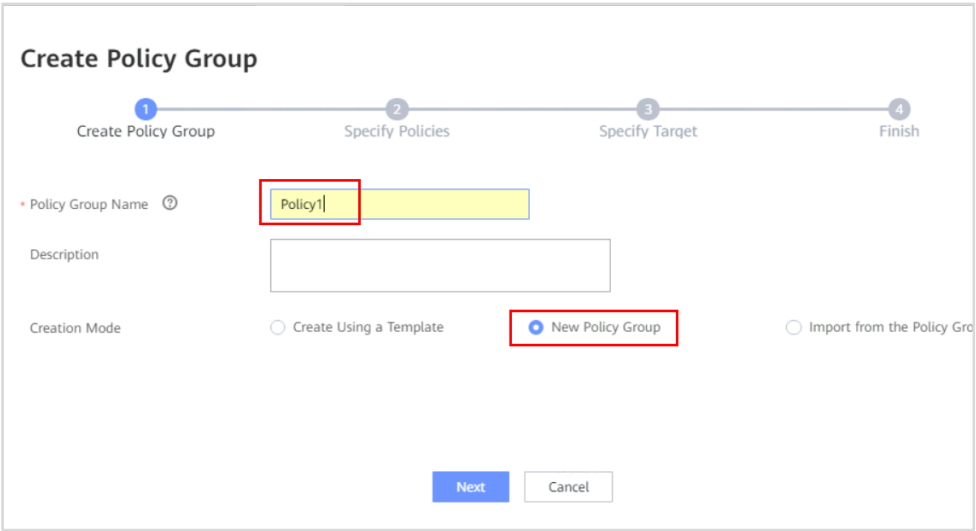


Figure 3-3 Creating a policy group

Step 3 On the **Specify Policies** page, click **File&Clipboard**. In the right pane, set **File Redirection** to **Read-only**, enable **Client Fixed Drive (such as local disk)**, and click **Next**.

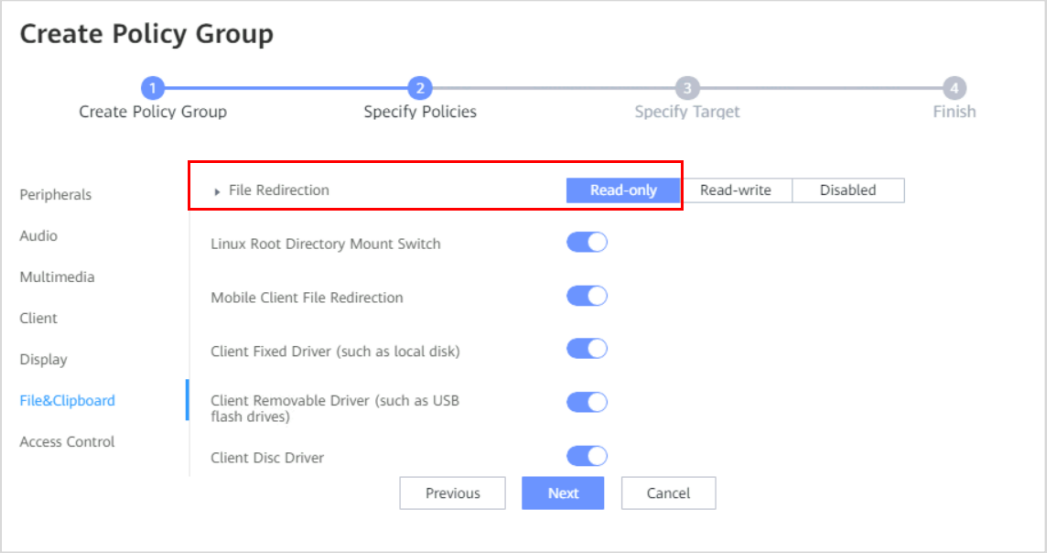


Figure 3-4 Specifying a policy

Step 4 On the **Specify Target** page, set **Target Type** to **User**, **Target Name** to a domain user, for example, **vdsuser**, and click the query icon. Select a target name from the target name list and add it to **Already Chosen**.

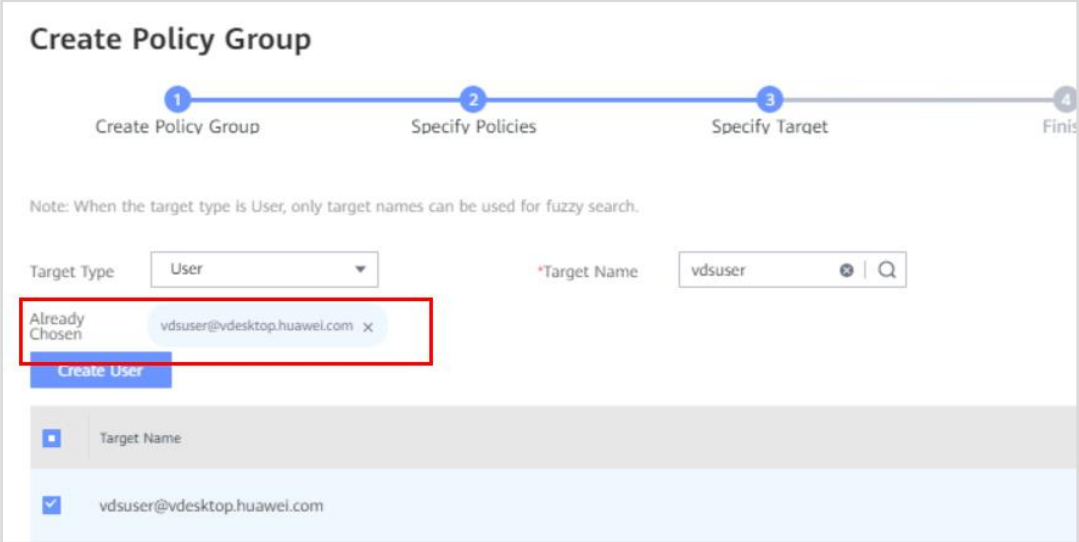


Figure 3-5 Specifying a target

Step 5 Click **Submit**. The policy configuration will take effect. When a message is displayed indicating that the policy group has been created, click **Back**.

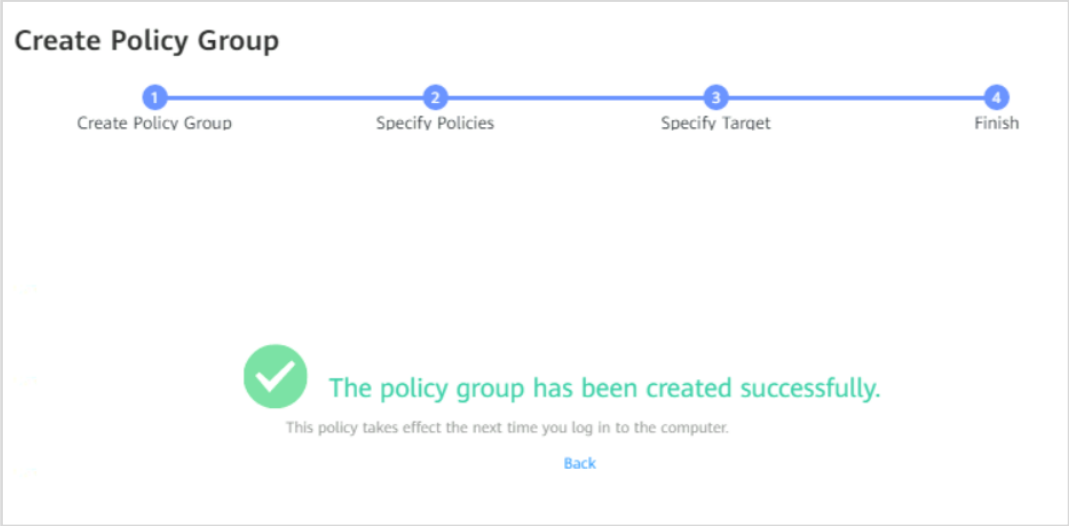


Figure 3-6 Specifying a target

Step 6 Log in to the virtual desktop as user **vdsuser**. Click **This PC** and ensure that the disk drive on the local client has been redirected to the virtual desktop.

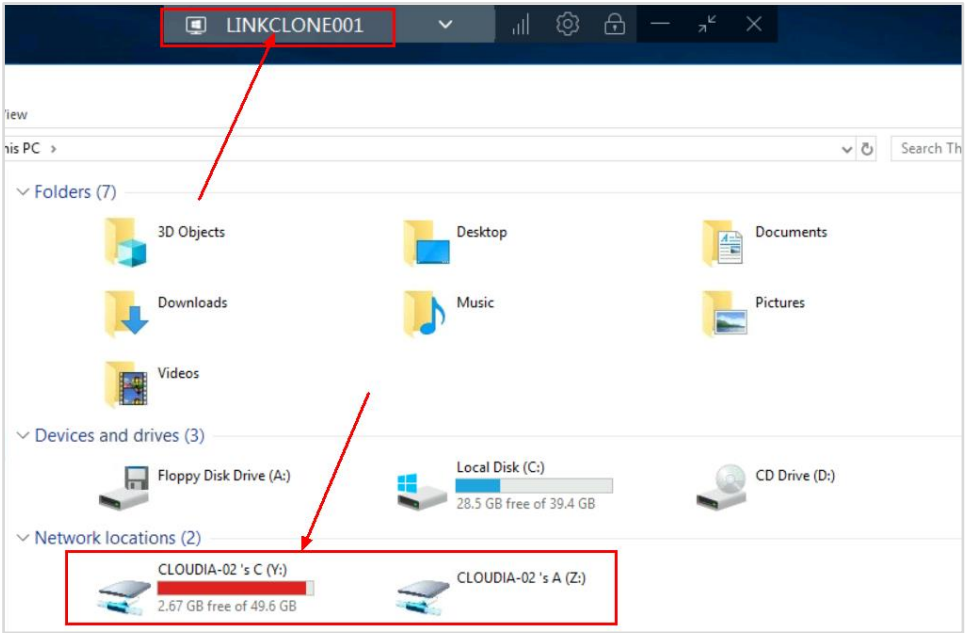


Figure 3-7 Viewing the local disk drive

Step 7 Copy a file from the local drive on the client and paste it to the drive of the virtual desktop. Check whether the operation is successful.

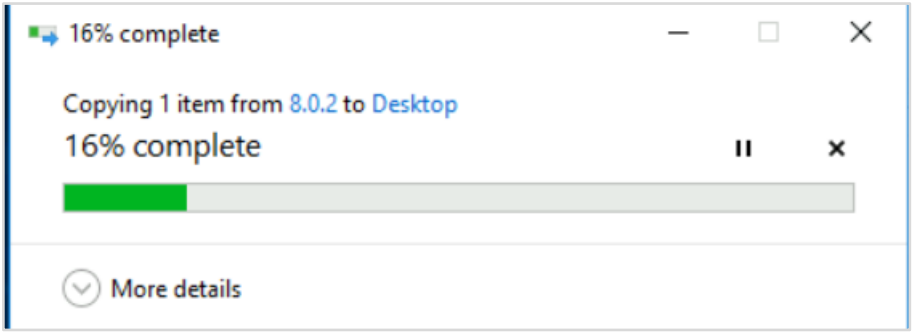


Figure 3-8 Checking the operation

Note:

Destination path of the file to be pasted:

- If the desktop VM has only one system disk, select a folder named after the domain user in the **User** folder or a folder in the **Public** path as the destination path.

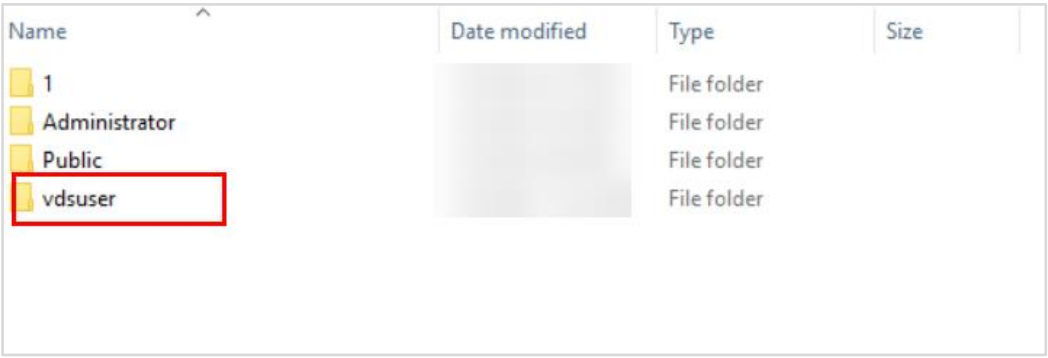


Figure 3-9 File path

- If the desktop VM has at least two disks, you are advised to select a non-system disk as the destination path.

Step 8 Copy a file from the virtual desktop to the client drive and check whether the operation is denied.

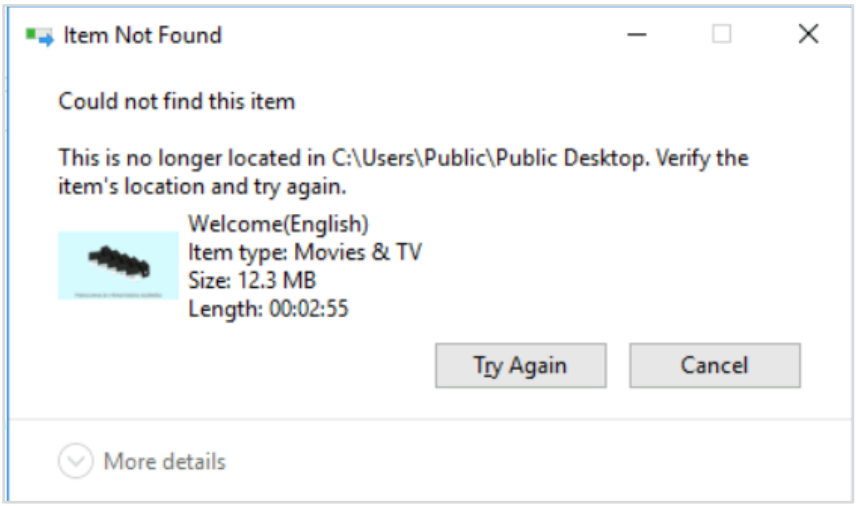


Figure 3-10 Checking the copy result

3.2.1.2 Clipboard Redirection

Set the clipboard redirection policy and apply it to the created user **vdsuser**. The clipboard content can be bidirectionally copied between clients and virtual desktops. That is, local files or folders on the client can be directly copied and pasted on the virtual desktop.

Step 1 On FusionAccess, choose **Resource** > **Policies** > **Protocol Policies**. On the page that is displayed, click **Policy1** created in 3.2.3.1 to view its details.

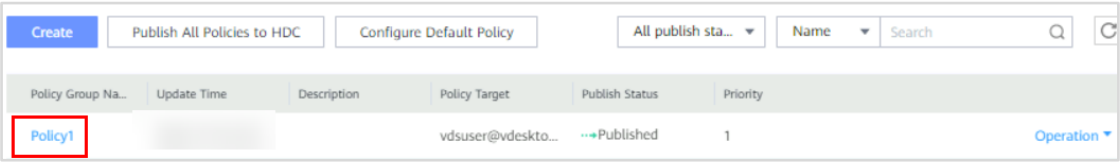


Figure 3-11 Policy details page

Step 2 Drag the policy details page to the right and choose **Operation** > **Edit**.

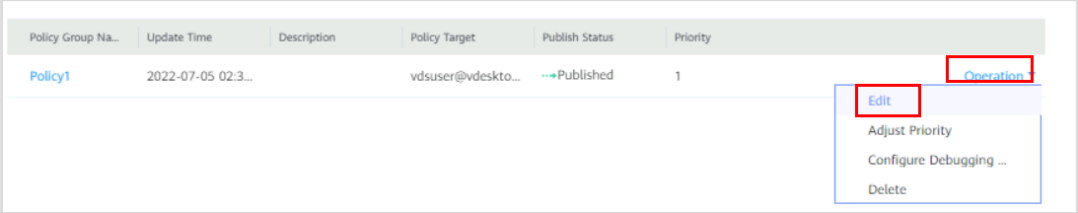


Figure 3-12 Editing a policy

Step 3 On the **Edit Policy Group** page, set **Edit Mode** to **Edit Current Policy Group** and click **Next**.

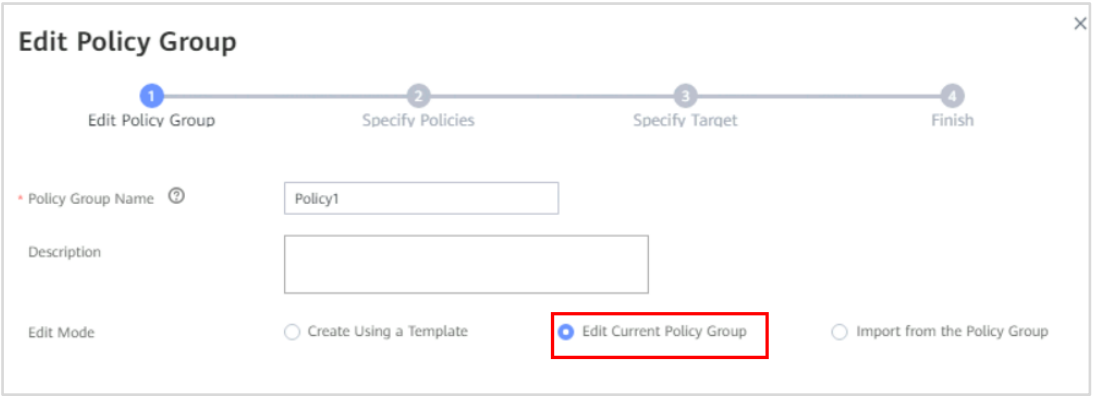


Figure 3-13 Editing a policy group

Step 4 The **Specify Policies** page is displayed. Click **File&Clipboard**. In the right pane:

- Set **File Redirection** to **Read-write**.
- Enable **Client Fixed Driver (such as local disk)**.
- Set **Clipboard Redirection** to **Bidirectional**.
- Enable **Clipboard Rich Text Redirection**.
- Enable **Clipboard File Redirection**.

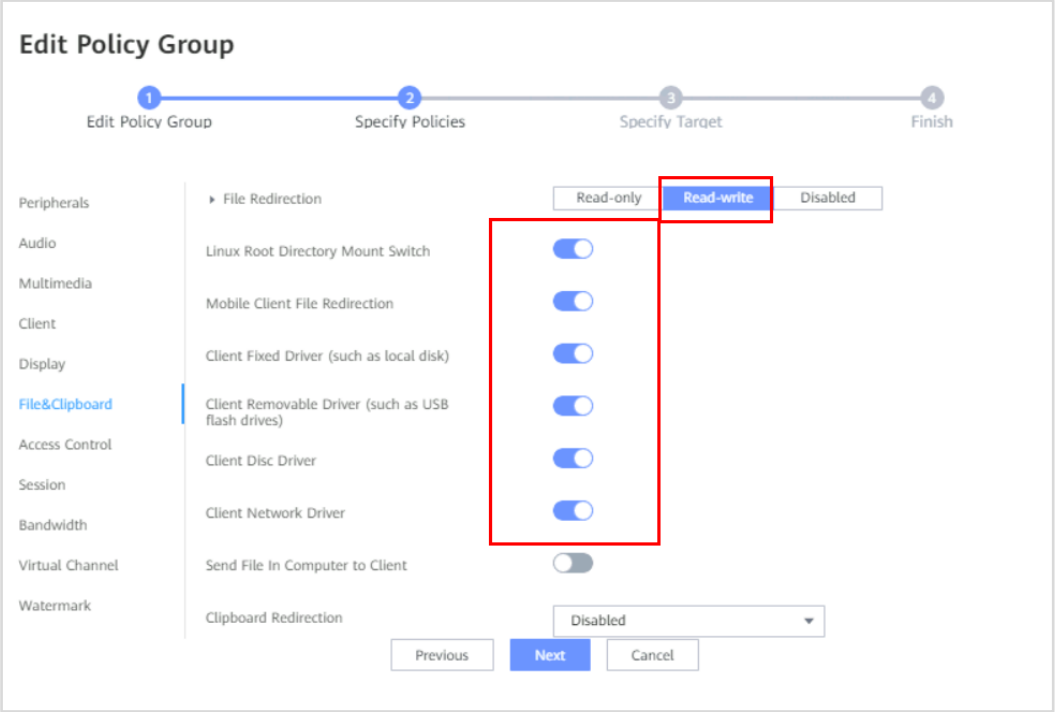


Figure 3-14 Specifying a policy

Figure 3-15 Setting clipboard redirection

Step 5 Click **Next**. The **Specify Target** page is displayed.

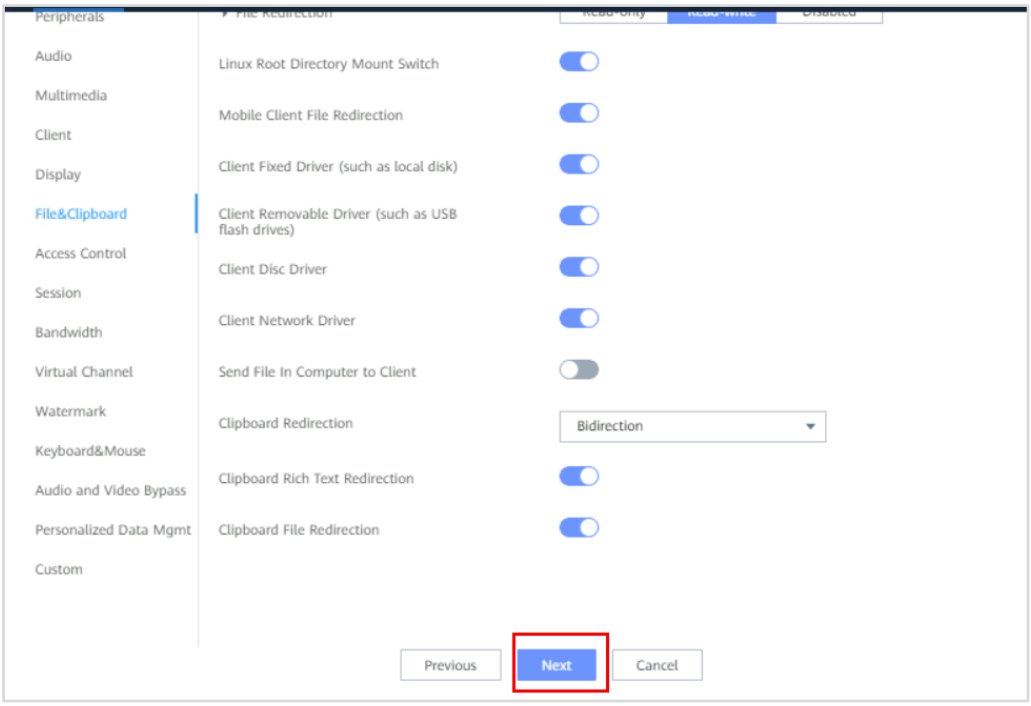


Figure 3-16 Going to specify a target

Step 6 Retain the default settings and click **Submit**. In the displayed dialog box, click **Back**.

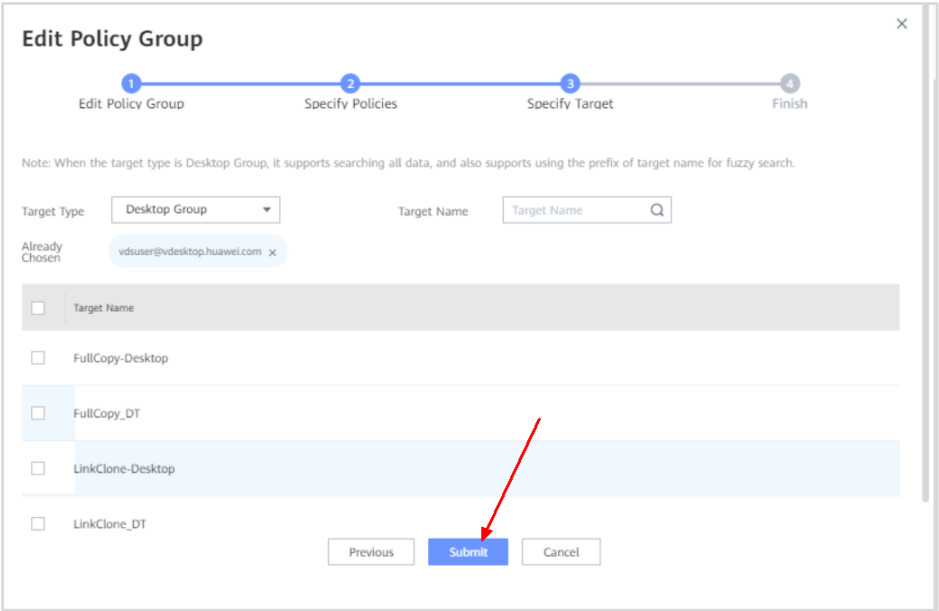


Figure 3-17 Specifying a target

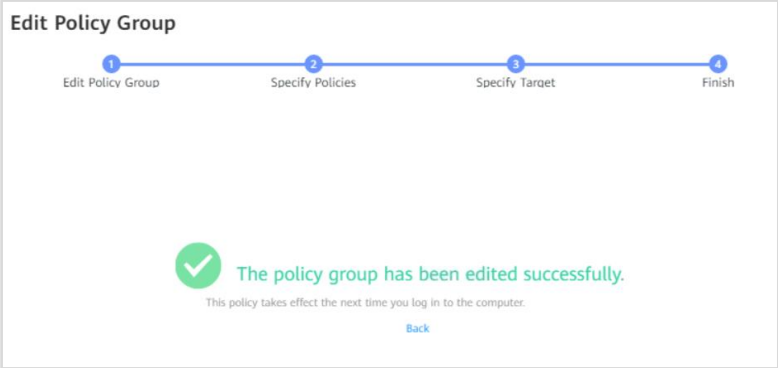


Figure 3-18 Successful editing

Step 7 Open a Word document containing text or images and copy the content.

Figure 3-19 Example

Step 8 Log in to the virtual desktop as user **vdsuser** and open the WordPad. Paste content to the WordPad created on the virtual desktop and check whether the operation can be performed.

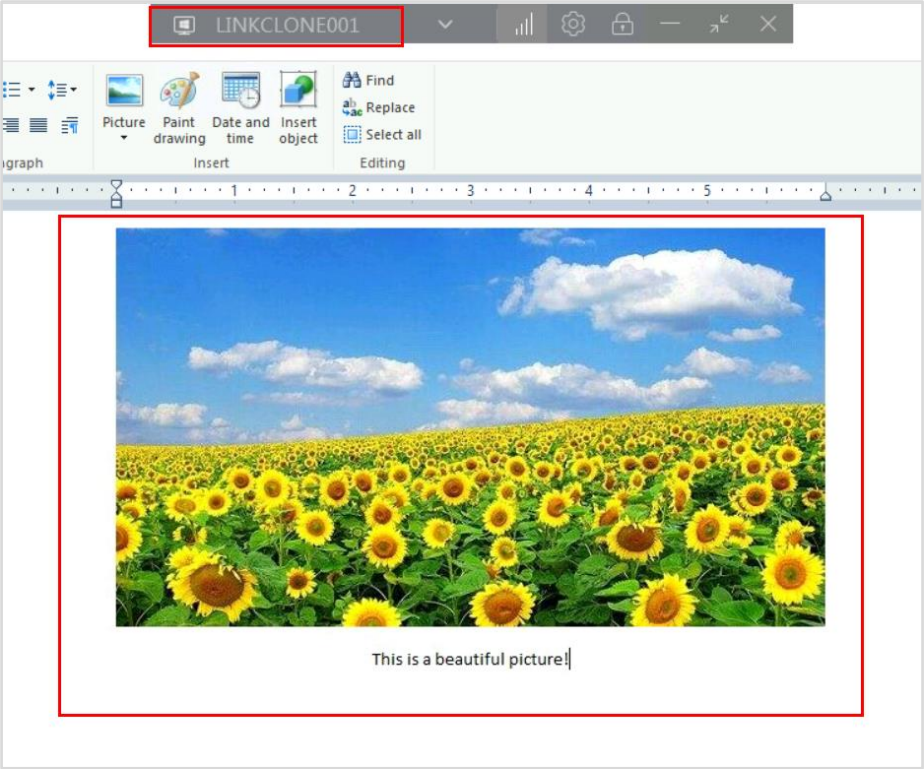


Figure 3-20 Verifying the clipboard redirection

Note:

You can select any content.

Step 9 On the virtual desktop, create a WordPad that contains text and images.

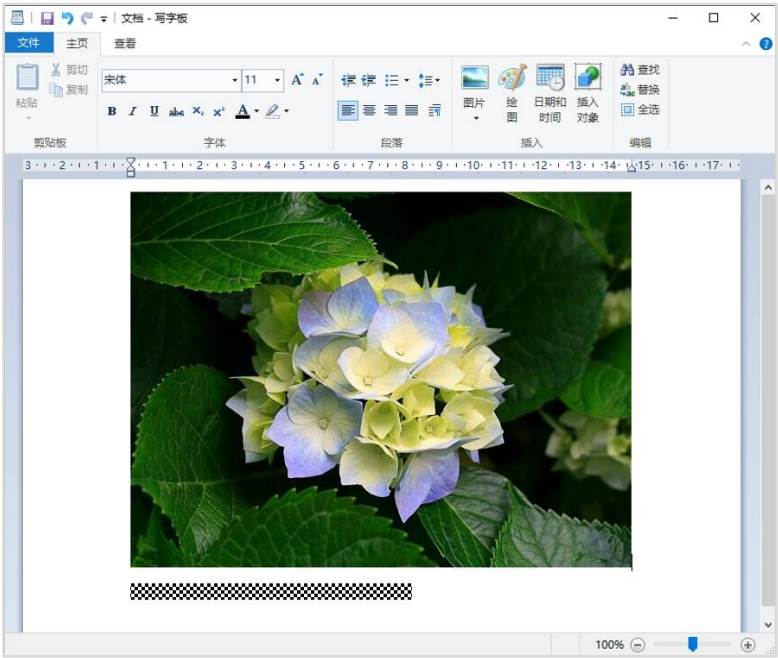


Figure 3-21 Example

Step 10 Copy and paste the content to the client WordPad and check whether the operation can be performed.

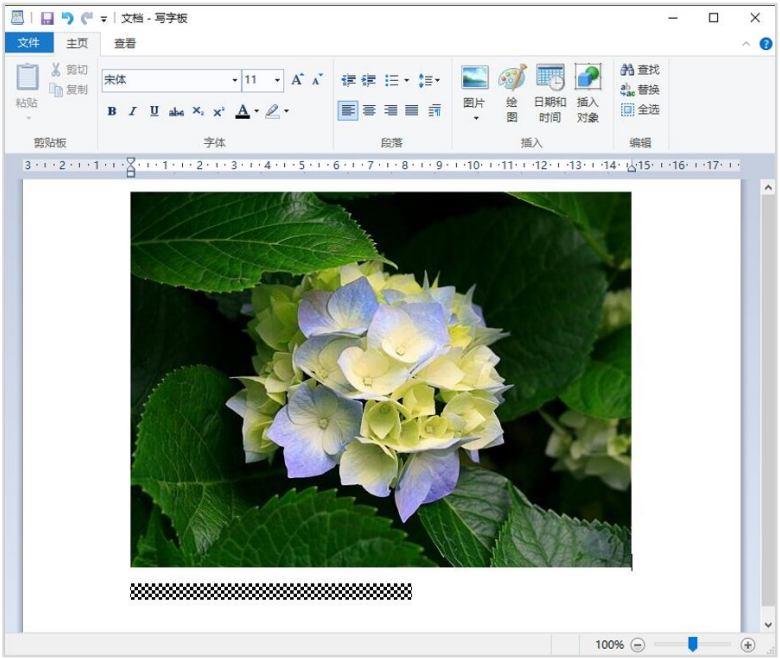


Figure 3-22 Verifying the clipboard redirection

3.2.2 Service Adjustment

3.2.2.1 Modifying Computer Specifications

This section describes how to modify computer specifications.

Step 1 On FusionAccess, choose **Resources** > **Desktops** > **Computers**.

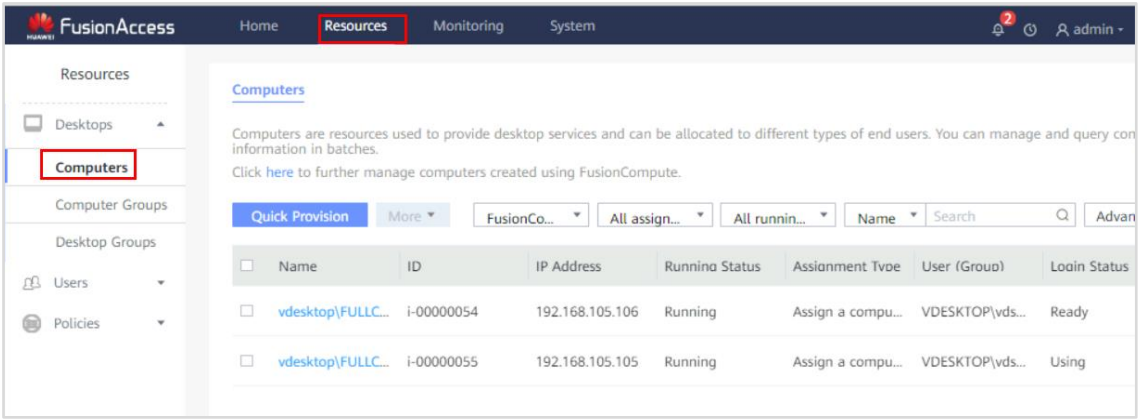


Figure 3-23 Computers

Step 2 In the computer list, select the target computer, click **Operation**, and choose **Change** > **Modify Computer**. The **Modify Computer** page is displayed.

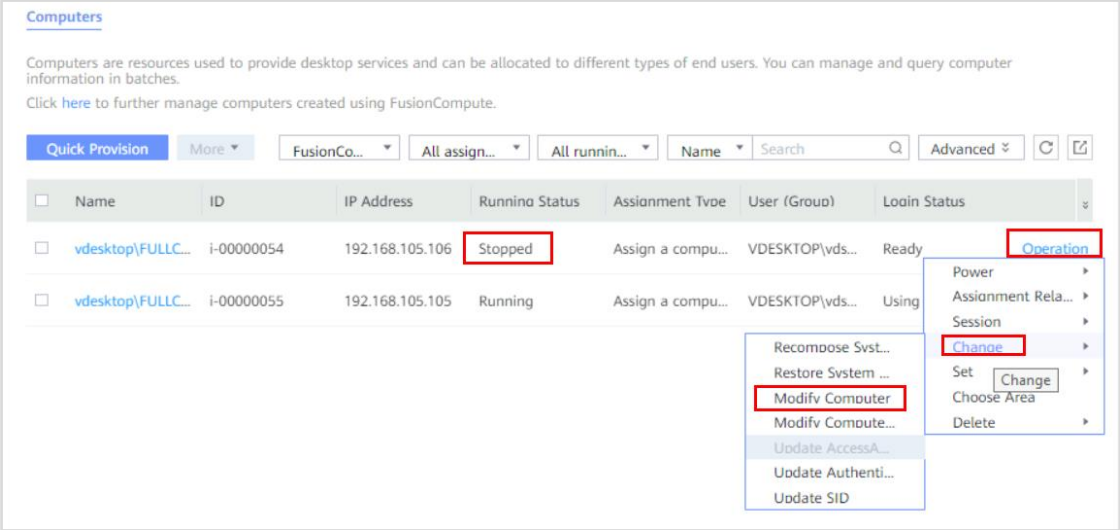


Figure 3-24 Going to modify a computer

Step 3 Change the CPU and memory of the computer to **8** and **8192** respectively, and click **OK**. In the displayed **Confirm** dialog box, click **OK** to return to the computer list. The computer specifications have been modified.

Note:

Computers that are in the **Running** state need to be restarted for the new CPU and memory specifications to take effect. For computers in other states, the modification will take effect upon startup.

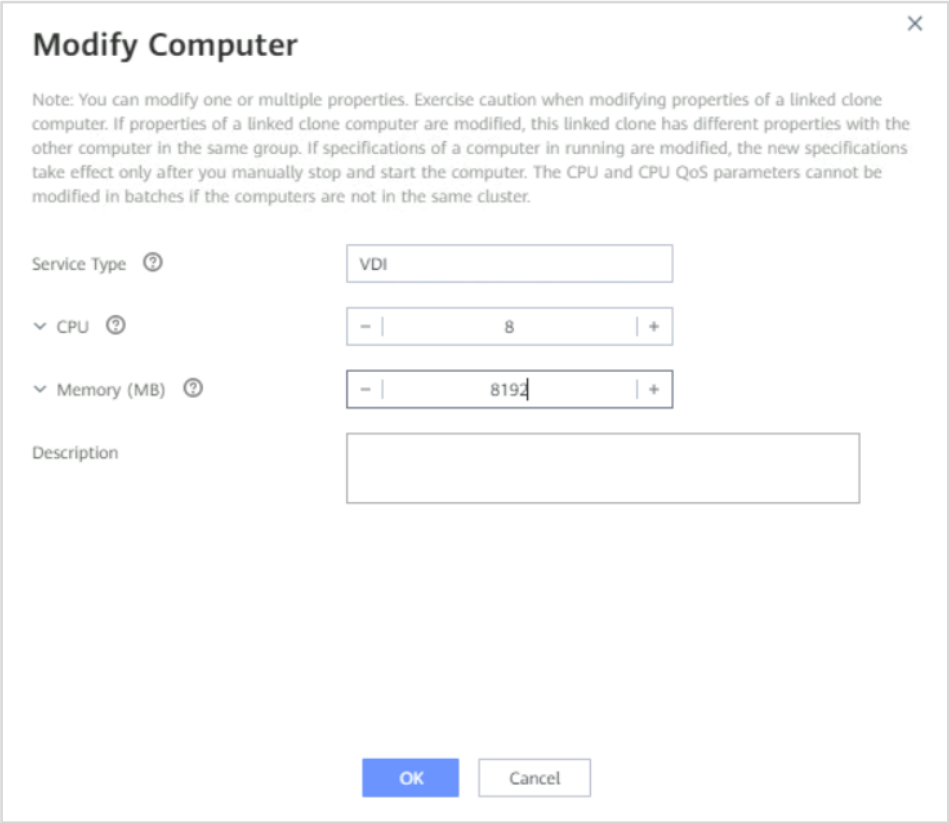


Figure 3-25 Modifying a computer

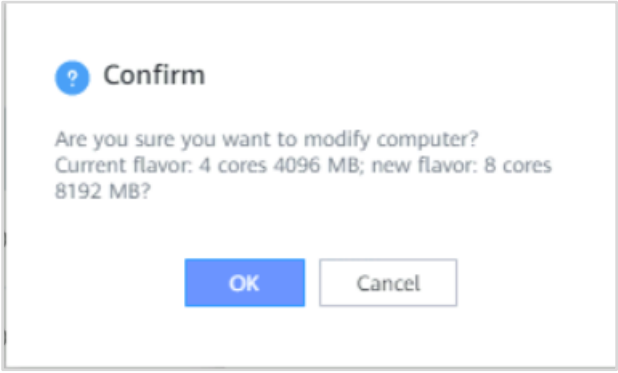


Figure 3-26 Confirming the modification

Step 4 In the displayed computer list, you can view the modified computer information.

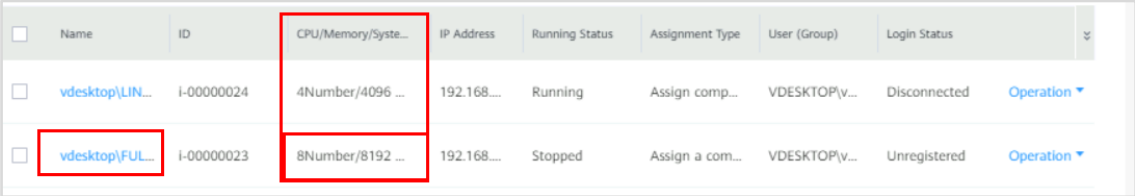


Figure 3-27 Computer list

Step 5 After the computer is started and the login status is **Ready**, log in to the virtual desktop using VNC by referring to section 2.2.4 or find the computer on FusionCompute. Go to **Processors** and **System** to check whether the configuration has been modified.

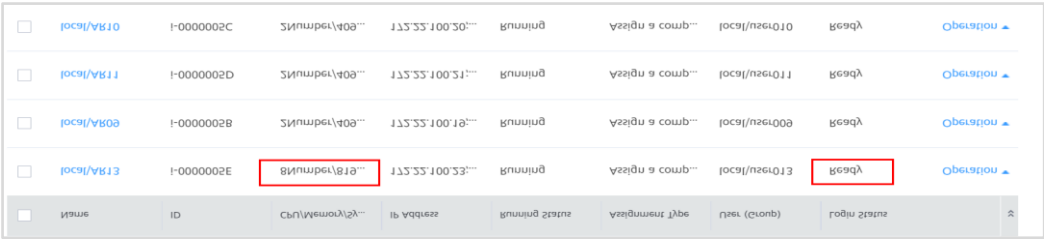


Figure 3-28 Computer list

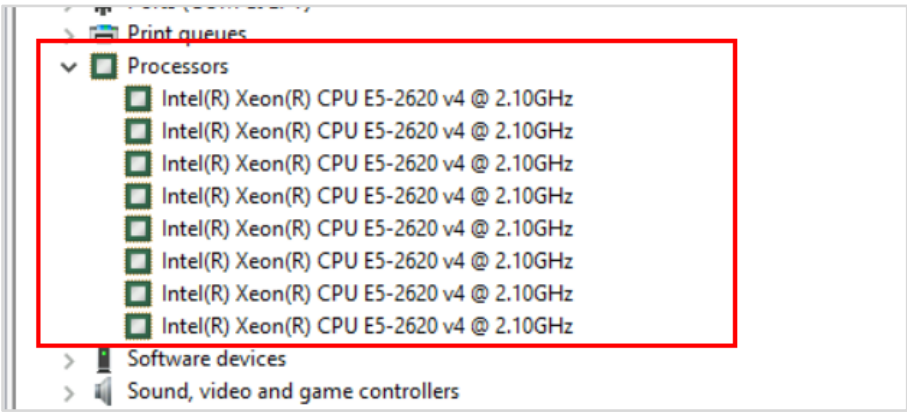


Figure 3-29 Processors

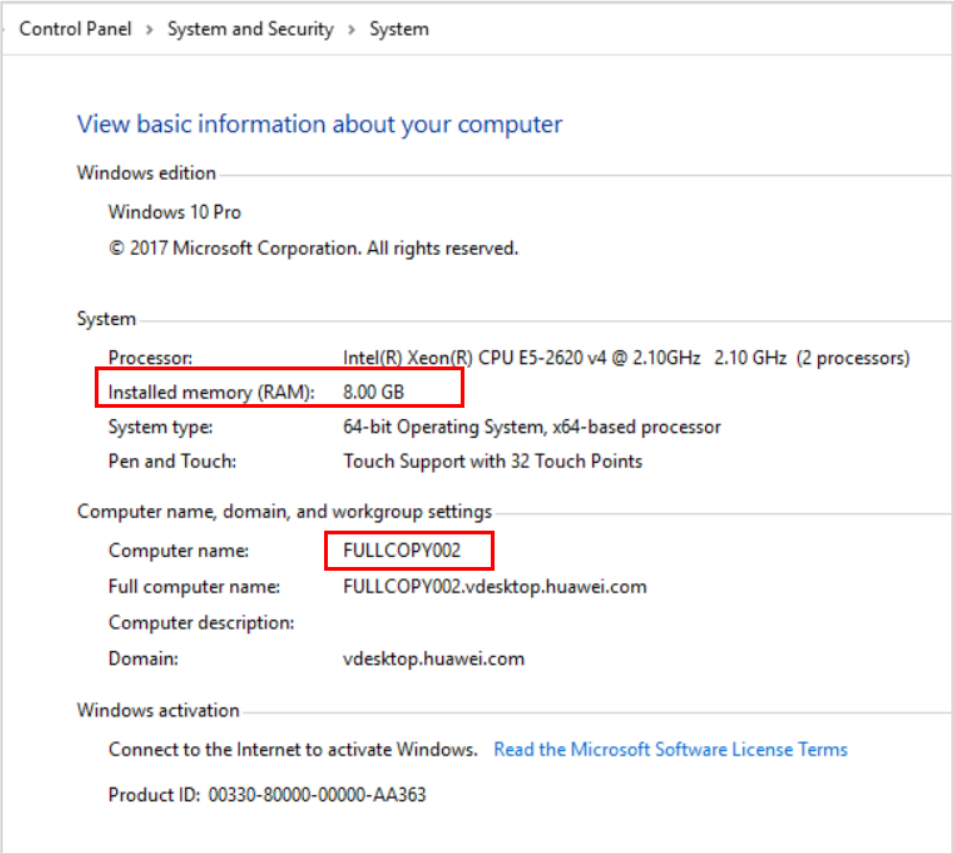


Figure 3-30 System

3.2.2.2 Adding a Computer Domain User

This section describes how to add a user to a computer whose **Assignment Type** is **Assign a Computer to Multiple Users**.

Step 1 On FusionAccess, choose **Resources** > **Desktops** > **Computers**.

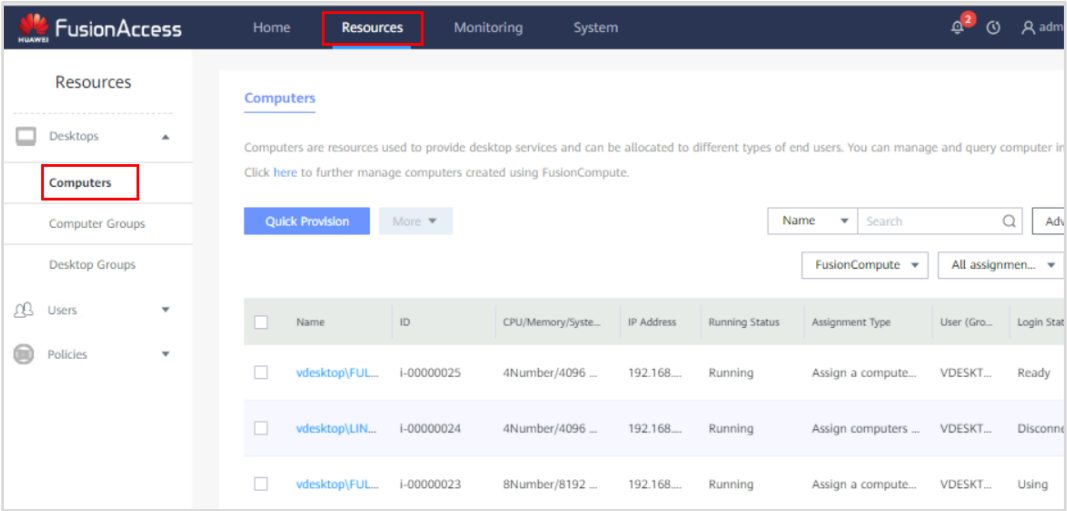


Figure 3-31 Computers

Step 2 Select a computer whose **Assignment Type** is **Assign a Computer to Multiple Users**. Choose **Operation** > **Assignment Relationship** > **Add User**. The page for adding a user to the computer is displayed.

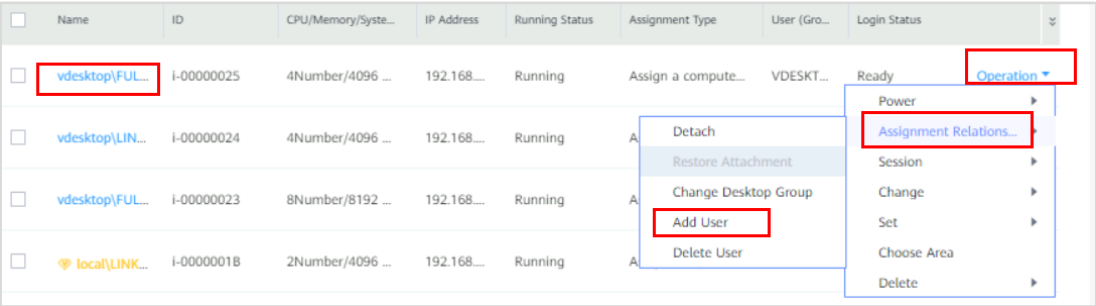


Figure 3-32 Adding a user

Note:

When the assignment type is **Multiple Users**:

- If user A has logged in to a VM, user B cannot log in to the VM.
- If user A disconnects from a VM without logging out, user B can log in to the VM and user A will be forcibly logged out of the VM at that time.
- To ensure all users in user group A can log in to the pool desktop that is assigned to this group, all these users must directly belong to user group A.
- For example, if user A belongs to department A and department A belongs to department C, user A can directly log in to the pool desktop if it is assigned to department A, but cannot log in to the pool desktop if it is assigned to department C.

Step 3 In the displayed **Add User** page, add a user.

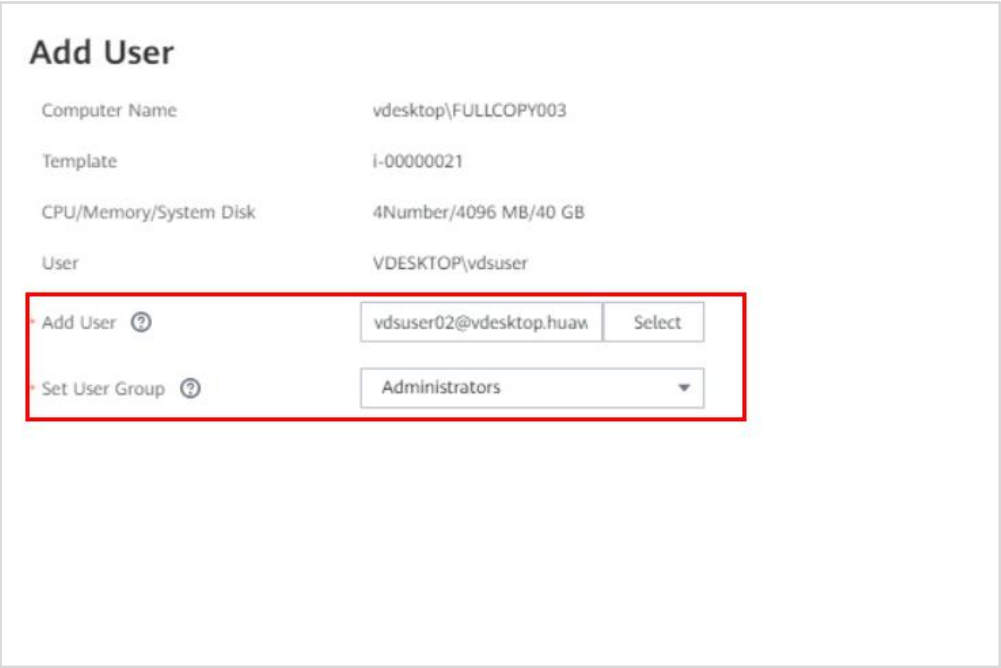


Figure 3-33 Adding a user

Note:

Specify the added user's user group. If the user group **Users** was configured during computer template creation, set this parameter to **Users**. Otherwise, set it to **Administrators**.

Step 4 In the displayed **Confirm** dialog box, click **OK**. The VM list is displayed.

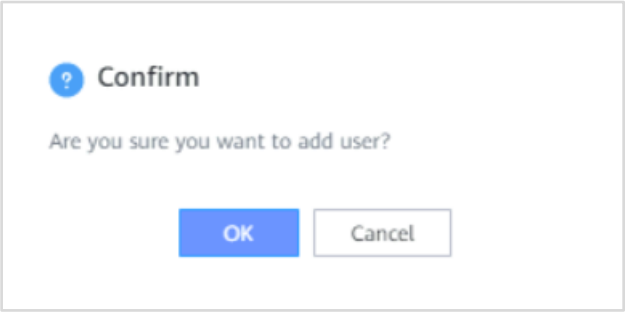


Figure 3-34 Confirming the operation of adding users

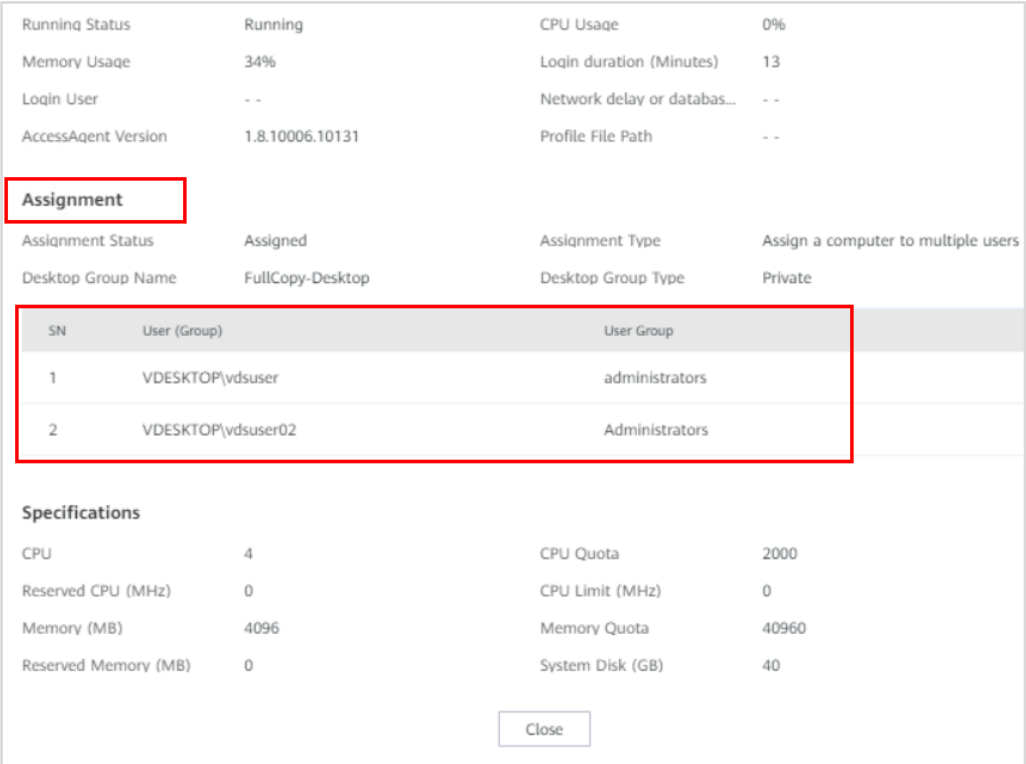


Figure 3-35 VM list

Step 5 In the test device (PC) browser, enter the IP address of the vAG server, for example, http://192.168.105.11, and press **Enter**.

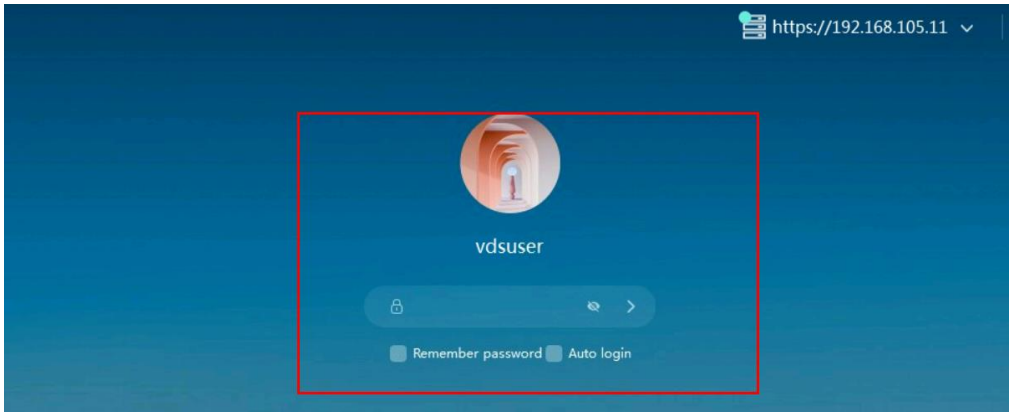


Figure 3-36 Login page

Step 6 Enter the username and password of the added user to log in to the system. The VM of the added user is displayed.

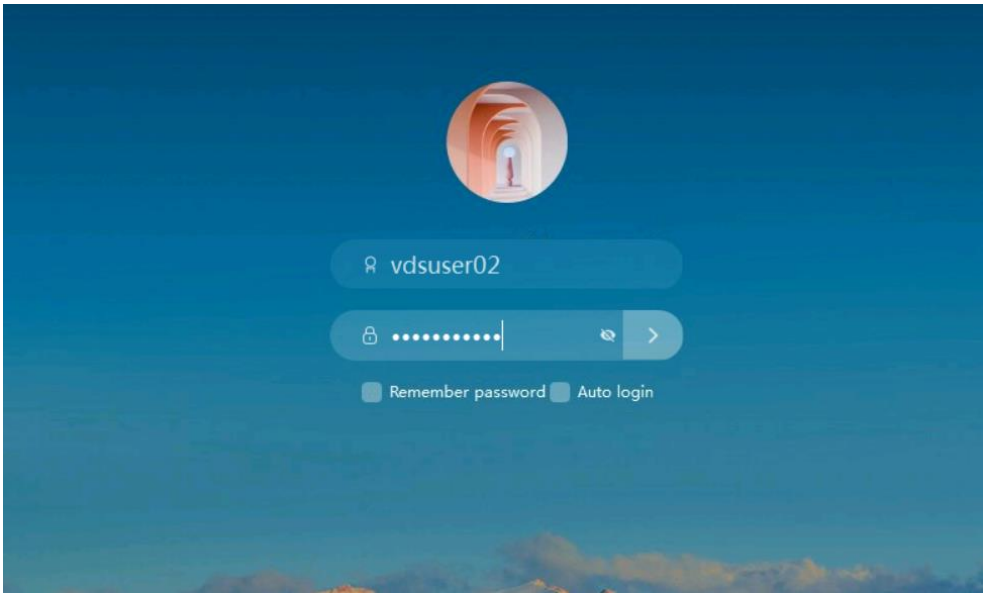


Figure 3-37 Login information

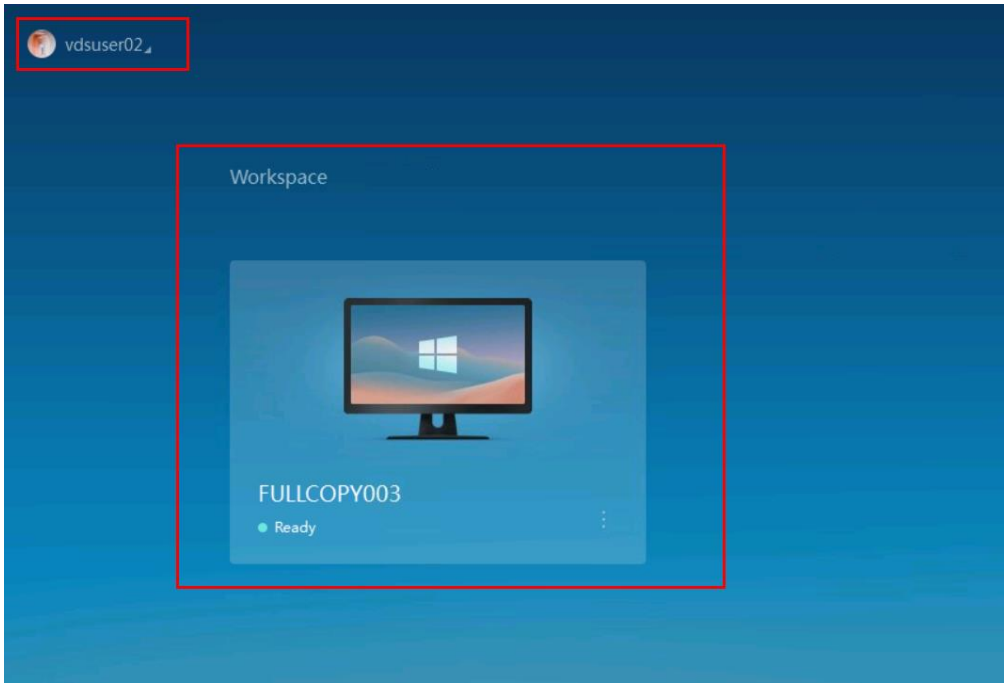


Figure 3-38 VM of the added user

3.2.2.3 Adding a Computer (Full Copy)

This section describes how to add a computer to a computer group and assign the computer in a desktop group.

Step 1 On FusionAccess, choose **Resources** > **Desktops** > **Computer Groups**. The **Computer Groups** page is displayed.

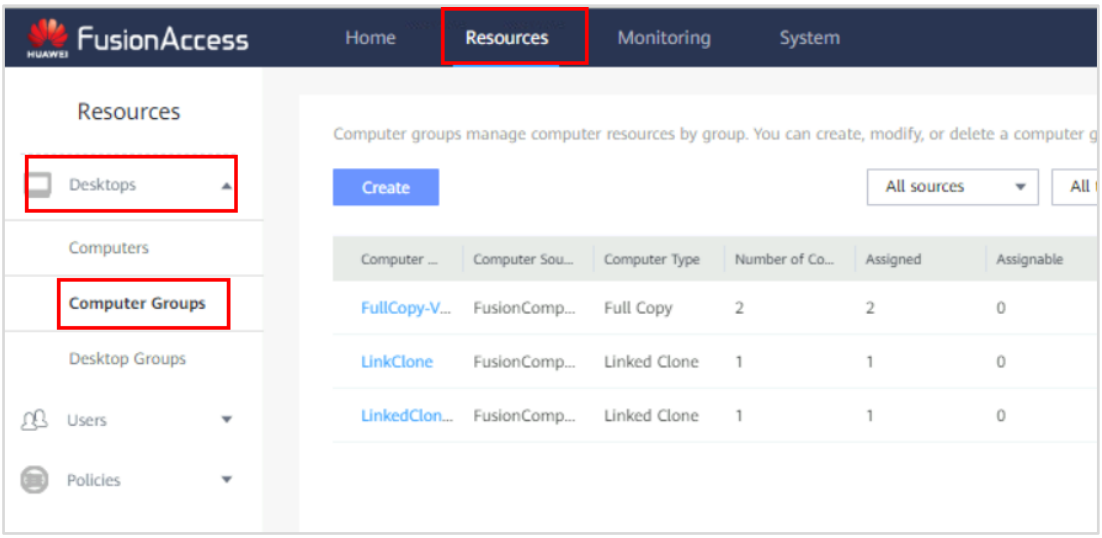


Figure 3-39 Computer groups

Step 2 On the right of the computer group to be added, choose **Operation** > **Add Computer**. The **Add Computer** page is displayed.

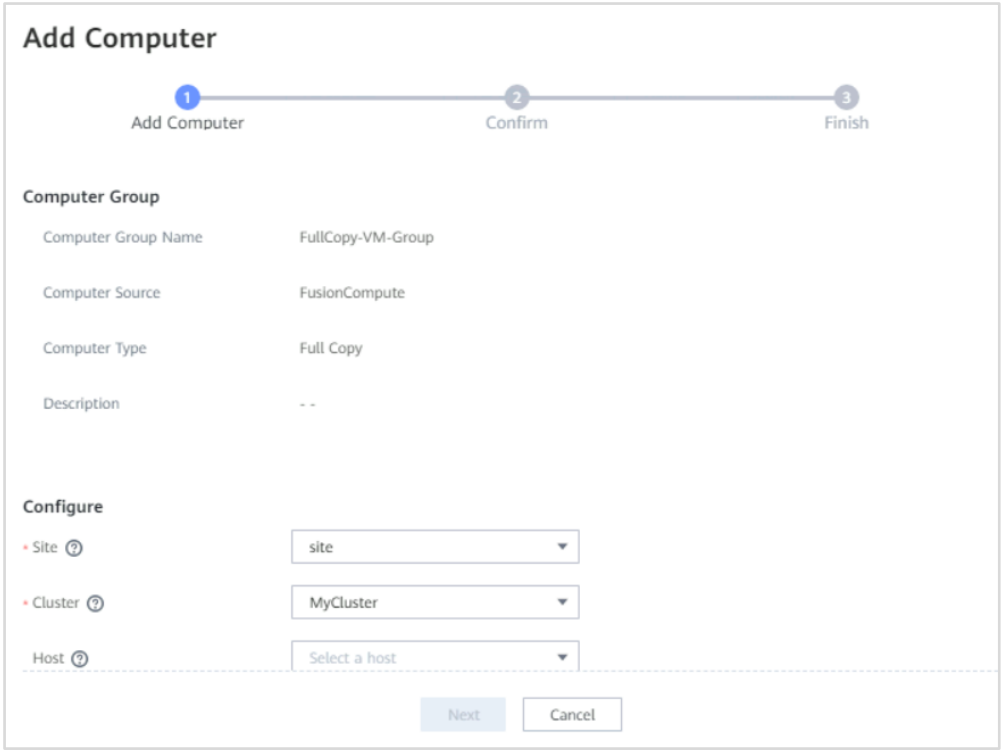


Figure 3-40 Adding a computer

Step 3 Retain the default values for **Site** and **Cluster**. You do not need to set **Host**.

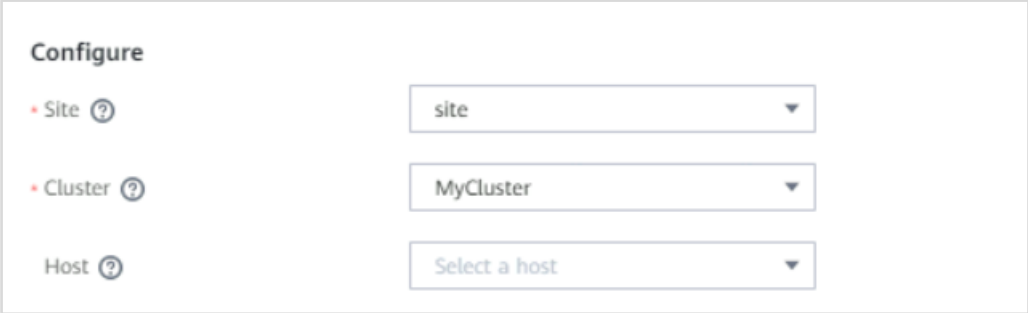


Figure 3-41 Configuring the site and cluster

Step 4 In the **Configure Template** area, click **Template** to select a template and click **OK**.

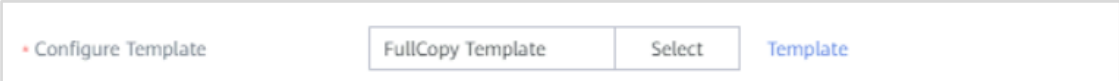


Figure 3-42 Selecting a VM template

Step 5 After you select a template, the **CPU**, **Memory (MB)**, **Disk**, and **NIC** information is automatically displayed. Retain the default values for CPU and memory or modify them as required.

Figure 3-43 Configuring a computer

Step 6 For a system disk, click **Add** in the **Data Store** column. In the dialog box that is displayed, select the desired data store and click **OK**. Select a configuration mode for the system disk. You are advised to select **Thick provisioning lazy zeroed**.

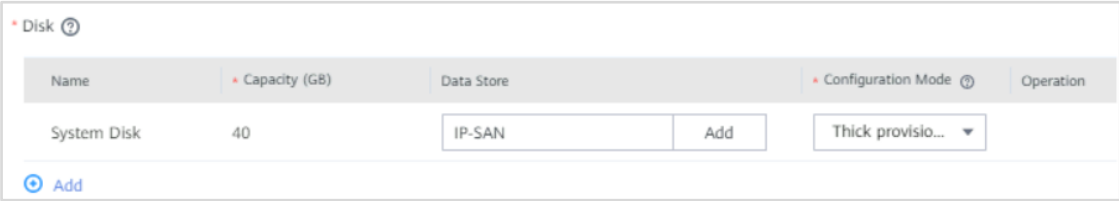


Figure 3-44 Configuring the system disk

Step 7 In the **NIC** area, click **Select** in the **Port Name** column. In the displayed dialog box, select the service-plane port group and click **OK**. Retain the default value for **Security Group**. Set **How IP Address Obtained** to **DHCP**.

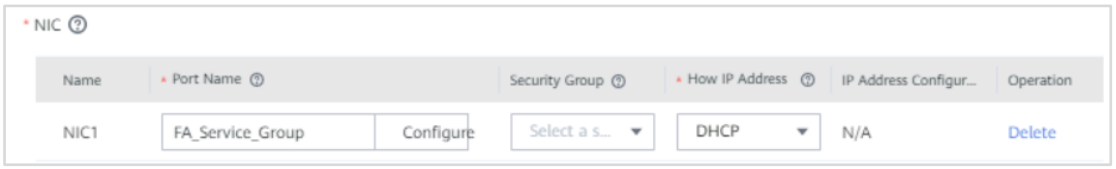


Figure 3-45 Configuring the NIC

Step 8 Set the number of computers to be provisioned in the **Quantity** area. You can create a maximum of 100 servers at a time.

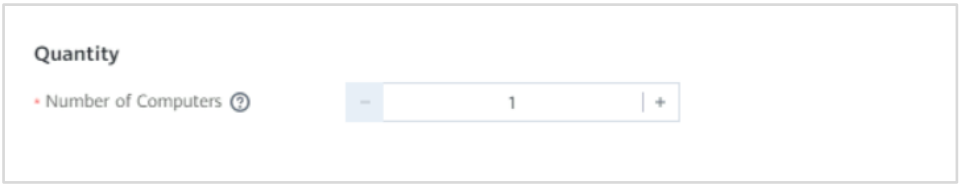


Figure 3-46 Setting the number of computers

Step 9 Select the full copy naming rule configured in **Naming Rule**.

Figure 3-47 Selecting a naming rule

Step 10 Click Next and select HDC information from the HDC drop-down list. Choose the HDC configured in **System** > **System Configuration** > **Desktop Components** > **HDC**.

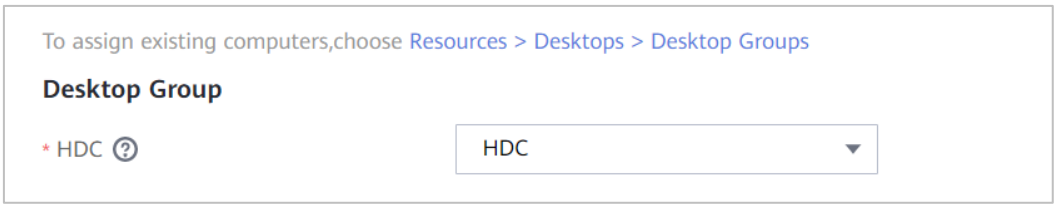


Figure 3-48 Selecting HDC information

Step 11 Click **Next**. Check the configuration of the computer to be provisioned. If the configuration is correct, click **OK**.

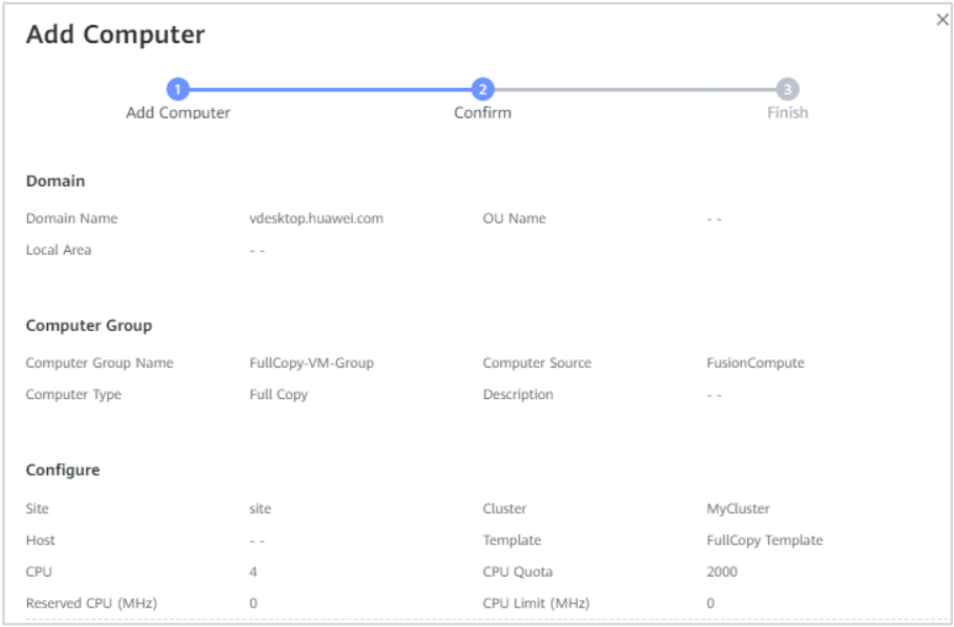


Figure 3-49 Checking the configuration of the computer to be provisioned

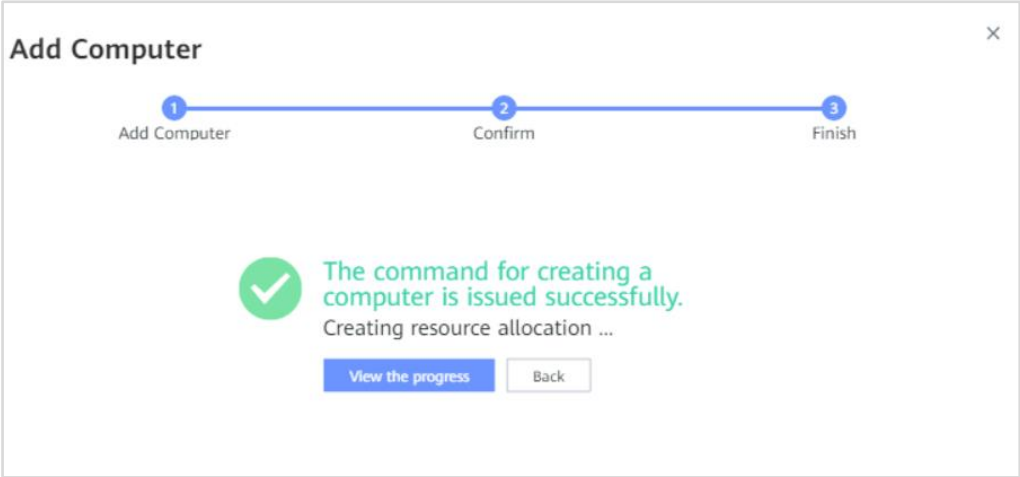


Figure 3-50 Successful provisioning

Step 12 You can view the task progress in the task center.

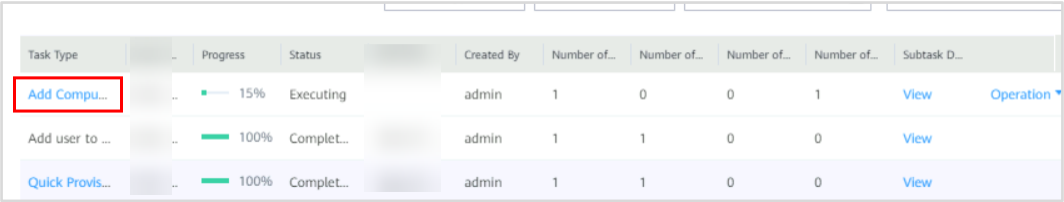


Figure 3-51 Viewing the progress

Step 13 On FusionAccess, choose **Resources** > **Desktops** > **Desktop Groups**. The **Desktop Groups** page is displayed.

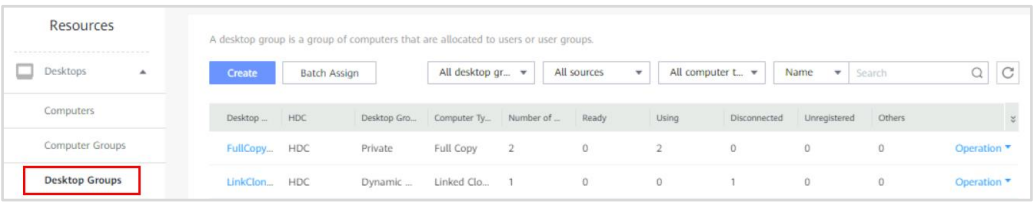


Figure 3-52 Desktop groups

Step 14 Select a desktop group in the list and choose **Operation** > **Assign Computer**. The **Assign Computer** page is displayed.

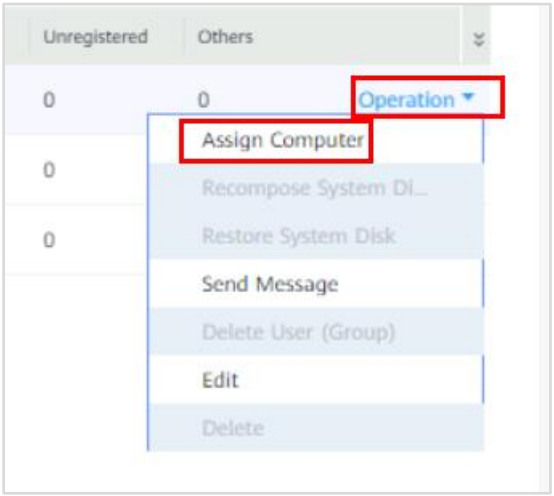


Figure 3-53 Assigning a computer

Step 15 Set **Naming Rule** to **FullCopy**, retain the default values for other parameters, and click **OK**.

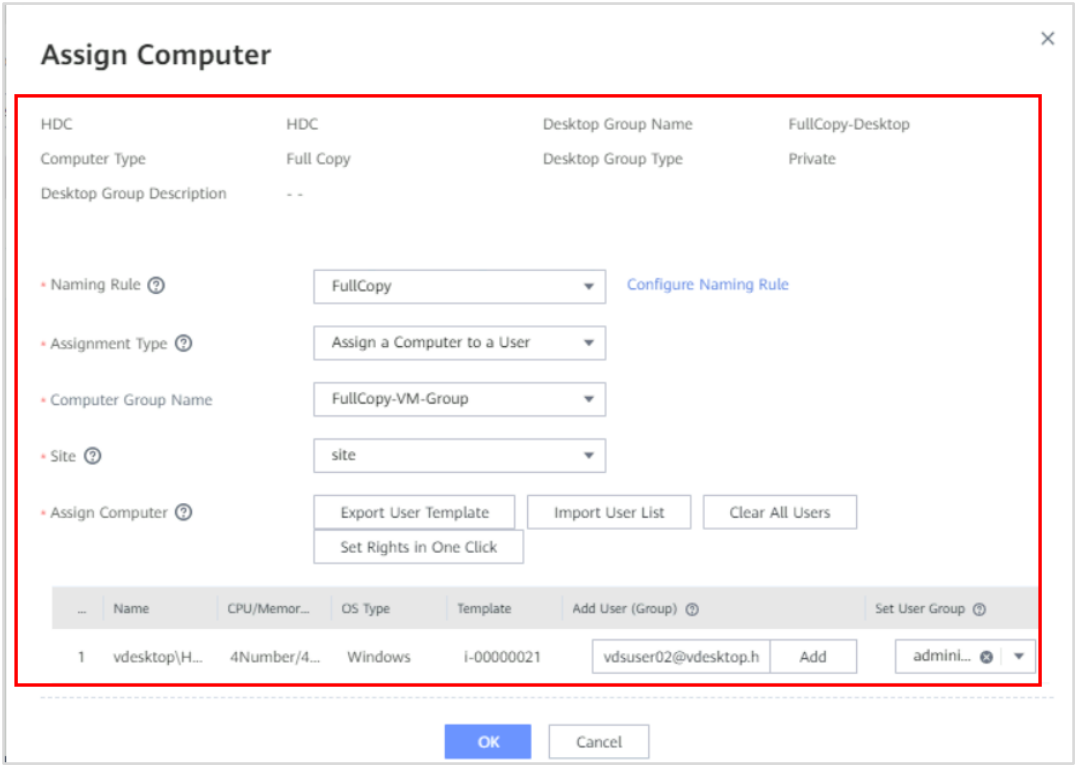


Figure 3-54 Configuring a desktop group

Step 16 In the displayed window, click **View the progress**. You can view the task progress in the task center.

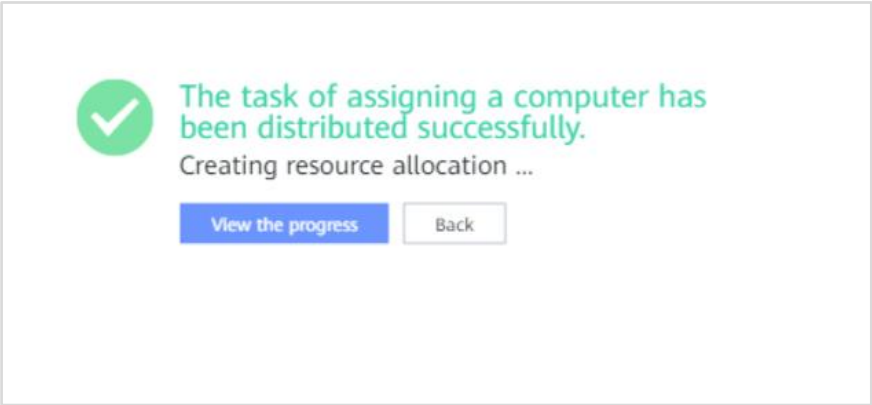


Figure 3-55 Successful assigning

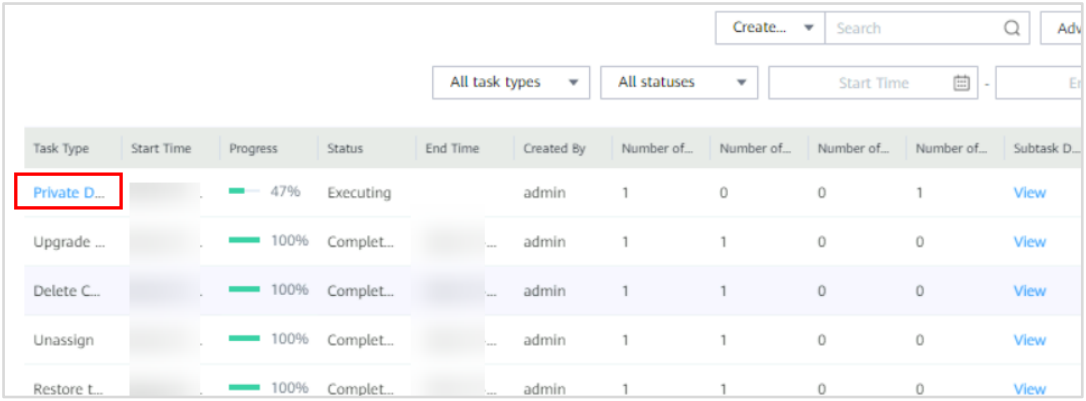


Figure 3-56 Desktop group list

Step 17 In the desktop group list, the total number of VMs in the **FullCopy Desktop group** changes from **1** to **2**.

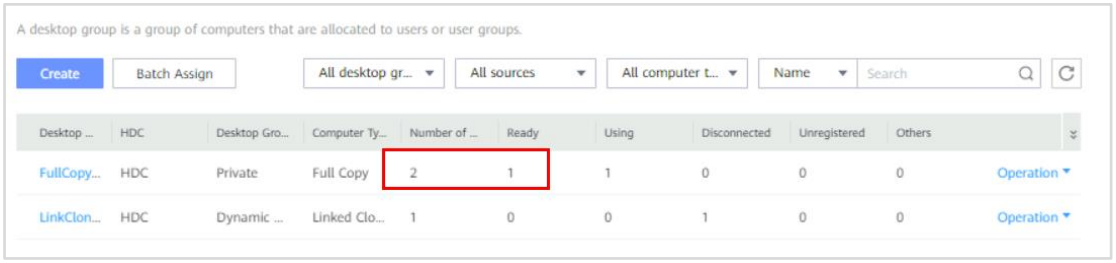


Figure 3-57 Desktop group list

3.2.2.4 Upgrading a Common Desktop to a VIP Desktop

In a common office scenario, all VMs request resources at the same priority. In specific scenarios, some virtual desktops have higher priorities for resource supply. In this case, you can upgrade these common desktops to VIP desktops so that users of these virtual desktops can enjoy faster CPU and memory resource supply, real-time VM status monitoring, and better experience. Administrators can flexibly upgrade common desktops to VIP desktops as required.

Note:

- Only assigned full copy and linked clone VMs can be upgraded to VIP desktops.
- Retain default values for VIP desktop resource assurance and real-time monitoring policies for all VIP users.
- During the operation, the user VM will be shut down and restarted. The VM will be available after it is restarted.

Step 1 On FusionAccess, choose **Resources** > **Desktops** > **Computer Groups**. The **Computer Groups** page is displayed.

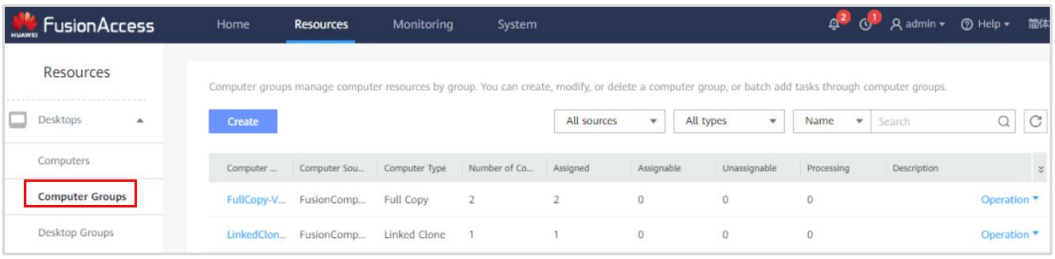


Figure 3-58 Computer groups

Step 2 In the computer list, select one or more computers that have been assigned and need to be upgraded to VIP desktops. Then, choose **Operation** > **Set** > **Upgrade to VIP Desktop**.

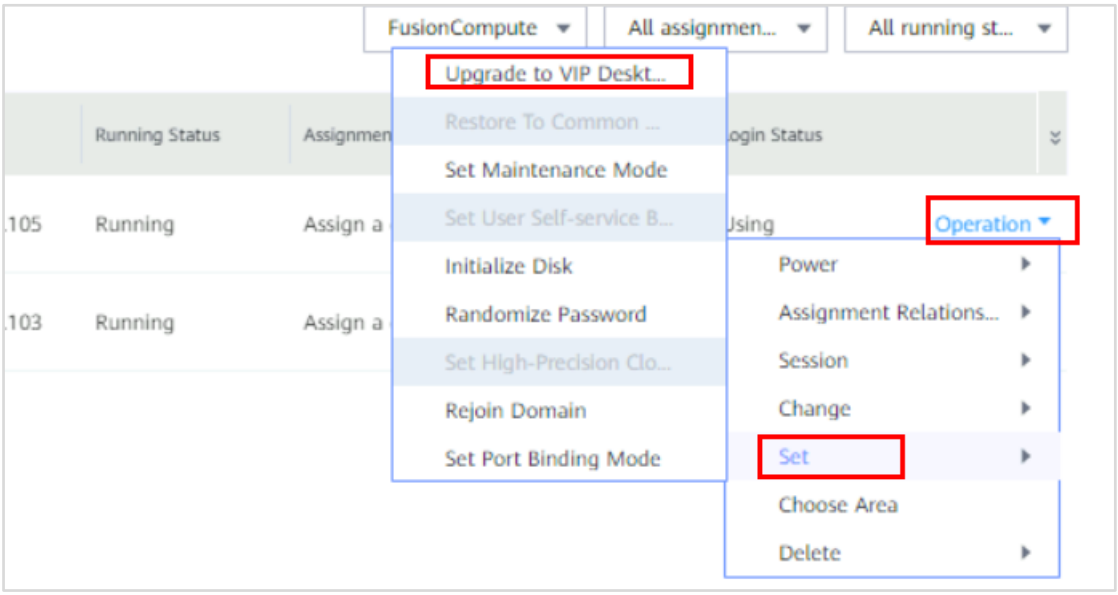


Figure 3-59 Upgrading to a VIP desktop

Step 3 In the displayed **Confirm** dialog box, click **OK**. In the displayed **Success** dialog box, click **OK**.

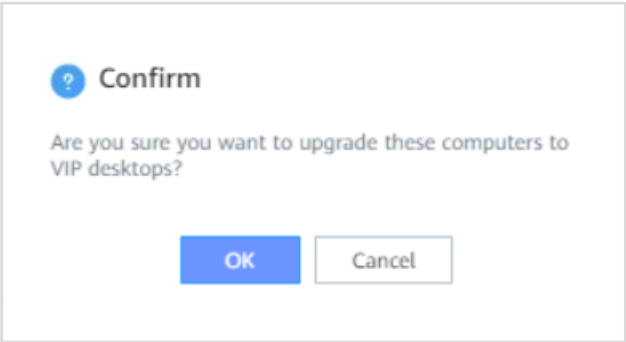


Figure 3-60 Confirming the upgrade

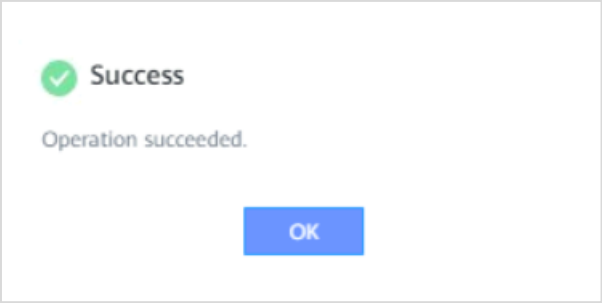


Figure 3-61 Successful upgrading

Step 4 The computer automatically restarts. After the restart is complete, the computer name is displayed in yellow.

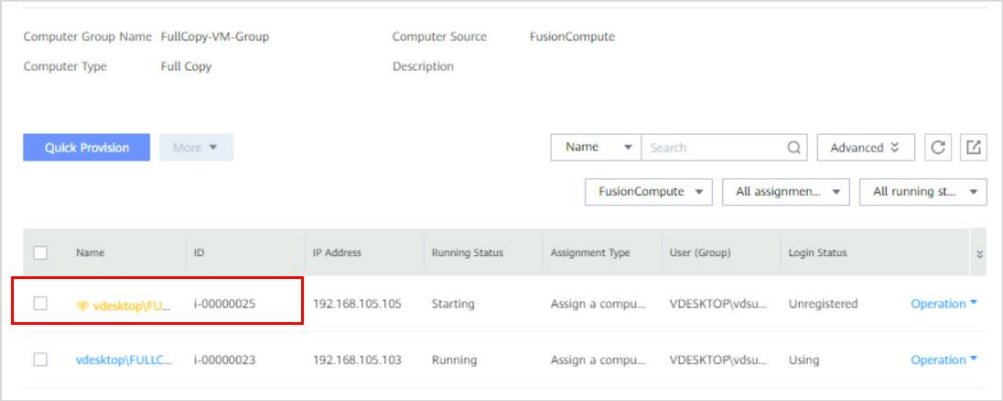


Figure 3-62 Checking the color of the computer name

3.2.2.5 Unassigning or Restoring a Virtual Desktop Assignment

This section describes how to unassign a computer from a user or user group and restore the assignment relationship. A full copy computer whose **Assignment Type** is **Assign a Computer to Multiple Users** is automatically shut down after being unassigned.

Note:

- After a full copy computer whose assignment type is **Assign a computer to a user** is unassigned, you can choose **Operation** > **Assignment Relationship** > **Restore Attachment** to assign the computer again. However, the computer can only be assigned to the original user and the user group permissions remain unchanged. Once the unassigned computer is assigned and started, the computer icon on the WI is lightened. Wait 3 minutes before logging in.
- An unassigned full copy VM whose assignment type is **Assign a computer to multiple users** cannot be re-assigned.

Step 1 On FusionAccess, choose **Resources** > **Desktops** > **Computers**.

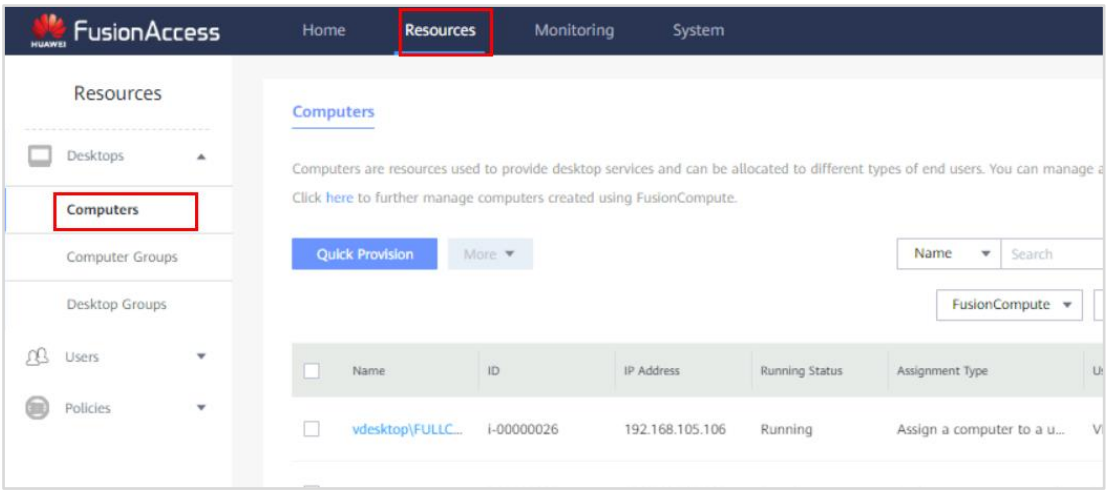


Figure 3-63 Computers

Step 2 In the computer list, select one or more computers to be unassigned and choose **Operation** > **Assignment Relationship** > **Detach**. A dialog box is displayed.

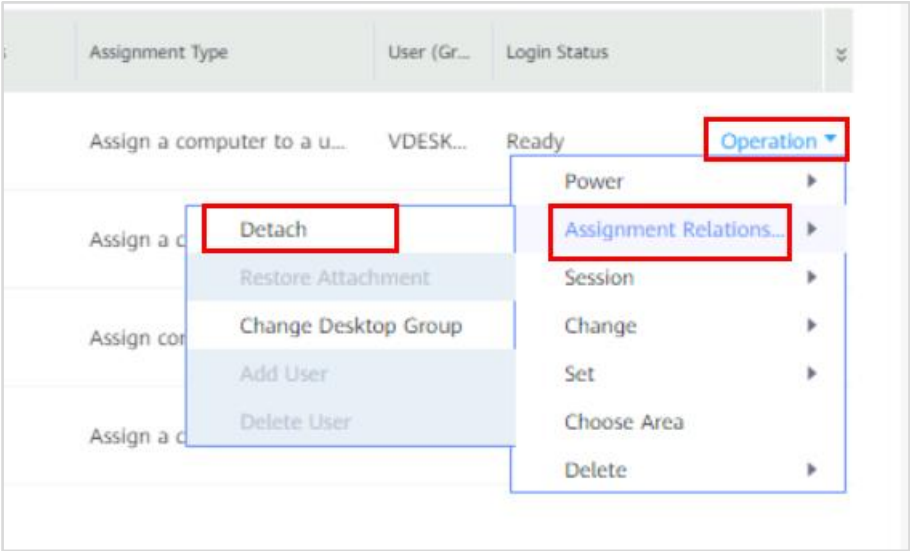


Figure 3-64 Unassigning a computer

Step 3 In the displayed confirmation dialog box, click **OK**.

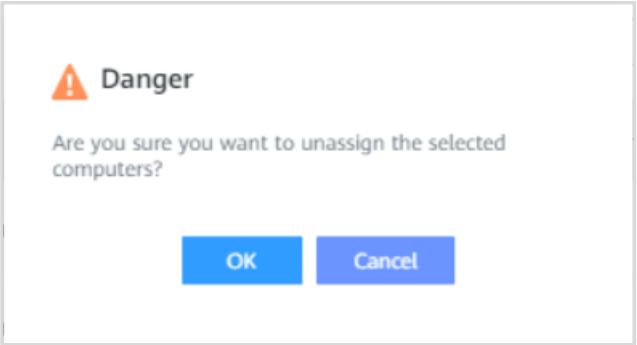


Figure 3-65 Confirming the unassignment

Step 4 In the **Unassigned List** dialog box displayed, click **OK**.

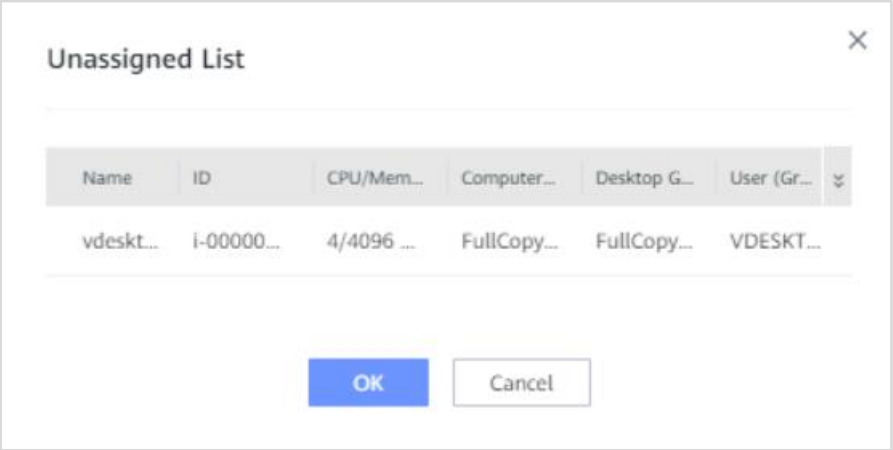


Figure 3-66 List of unassigned computers

Step 5 In the displayed dialog box, click **OK**.

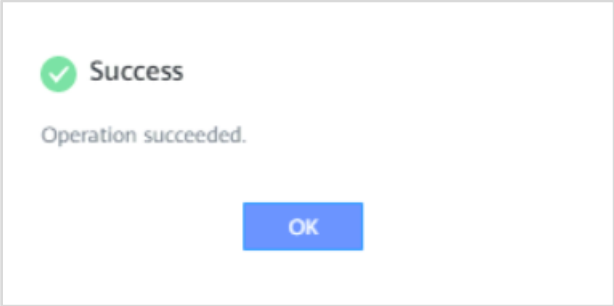


Figure 3-67 Confirming the unassignment

Step 6 Enter the search criteria to search for the unassigned computer. Check the operation result in the computer list. If the assignment status is **Unassigned**, the computer has been unassigned.

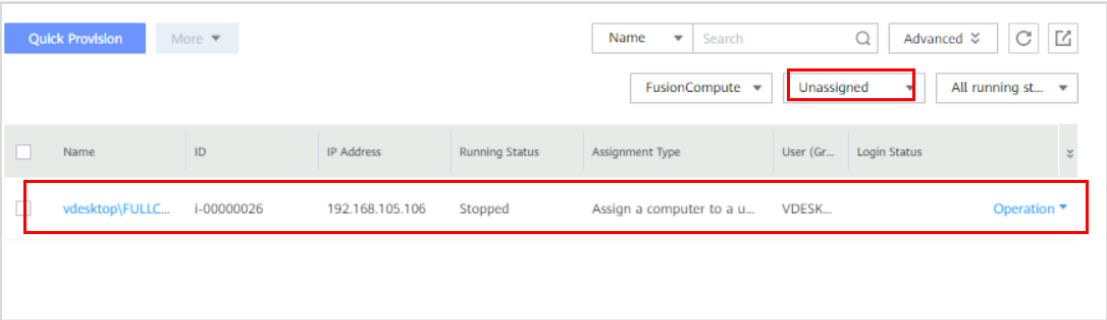


Figure 3-68 Querying the assignment status of a computer

Step 7 Search for the unassigned computer by relevant criteria. Select the computer from the result list.

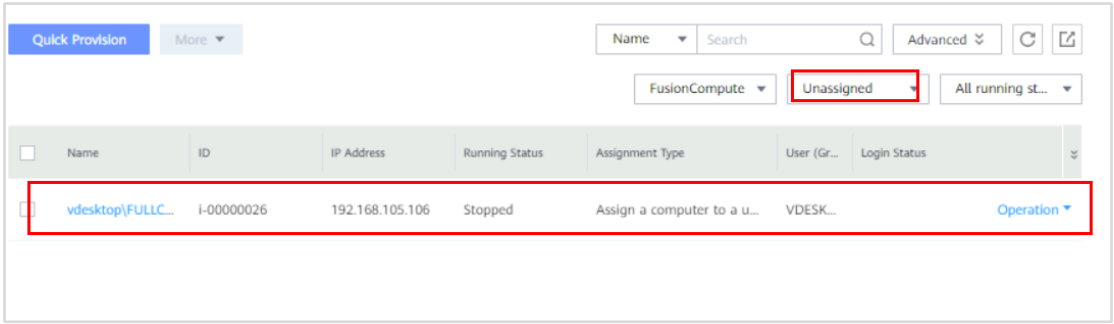


Figure 3-69 Searching for unassigned computers

Step 8 Choose **Operation** > **Assignment Relationship** > **Restore Attachment**.

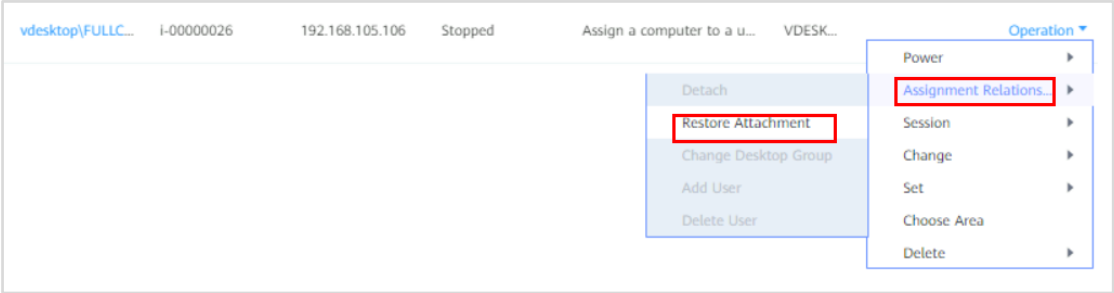


Figure 3-70 Restoring assignment

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

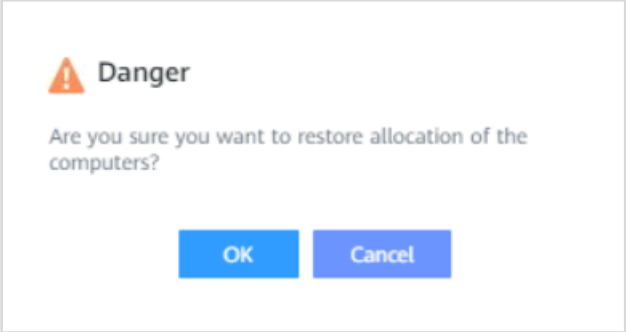


Figure 3-71 Confirming the assignment restoration

Step 10 In the **Restore Allocated List** dialog box, click **OK**.

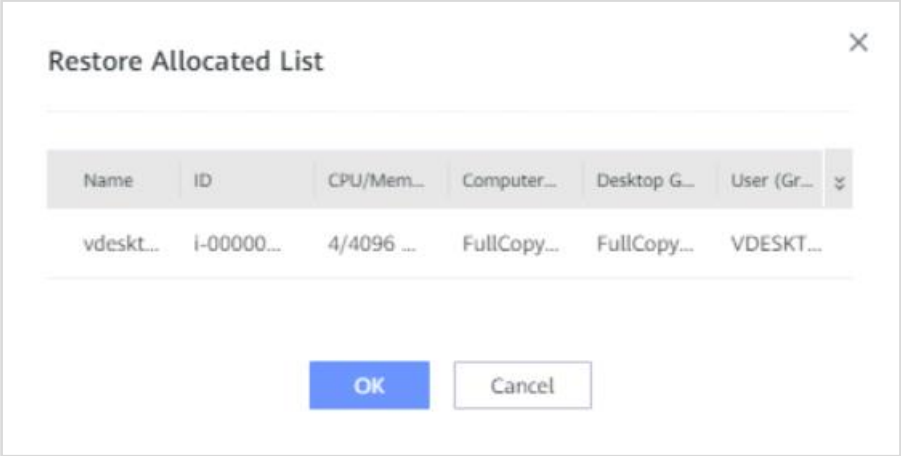


Figure 3-72 List of restored assignment

Step 11 In the displayed dialog box, click **OK**.

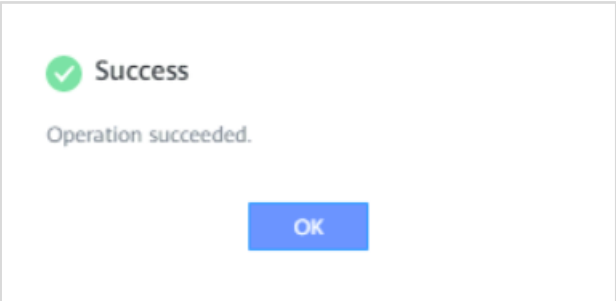


Figure 3-73 Confirming the operation

Step 12 Enter the search criteria to search for the assigned computer. Check the operation result in the computer list. If the assignment status is **Assigned**, the computer has been unassigned.

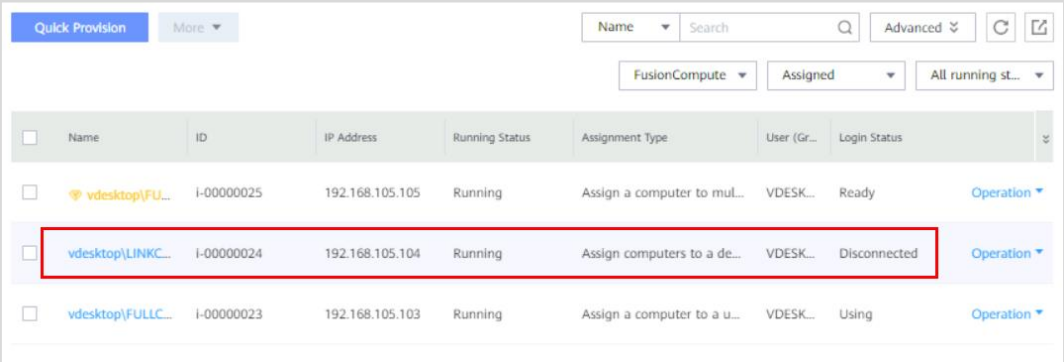


Figure 3-74 Assignment status

3.2.3 Viewing and Handling Alarms

Step 1 Log in to FusionAccess Web Client, choose **Monitoring** > **Alarms** > **System Alarms** to view and collect FusionAccess alarms.

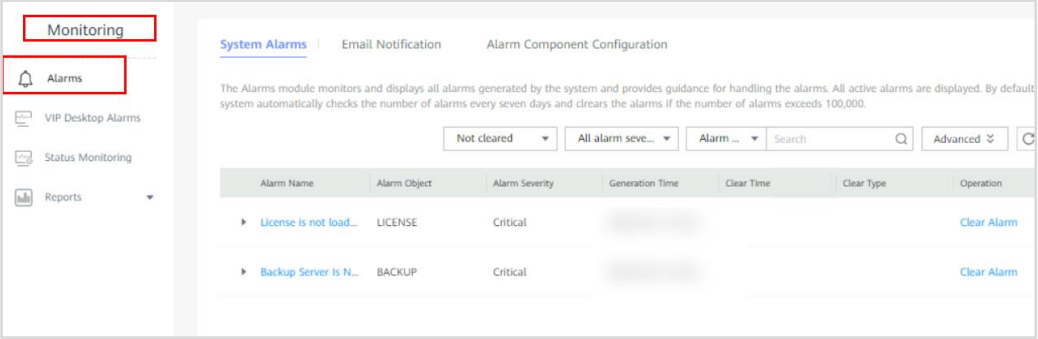


Figure 3-75 Alarm information

Step 2 Log in to FusionAccess Web Client, choose **Monitoring** > **Status Monitoring**, and view the status of each FusionAccess component.

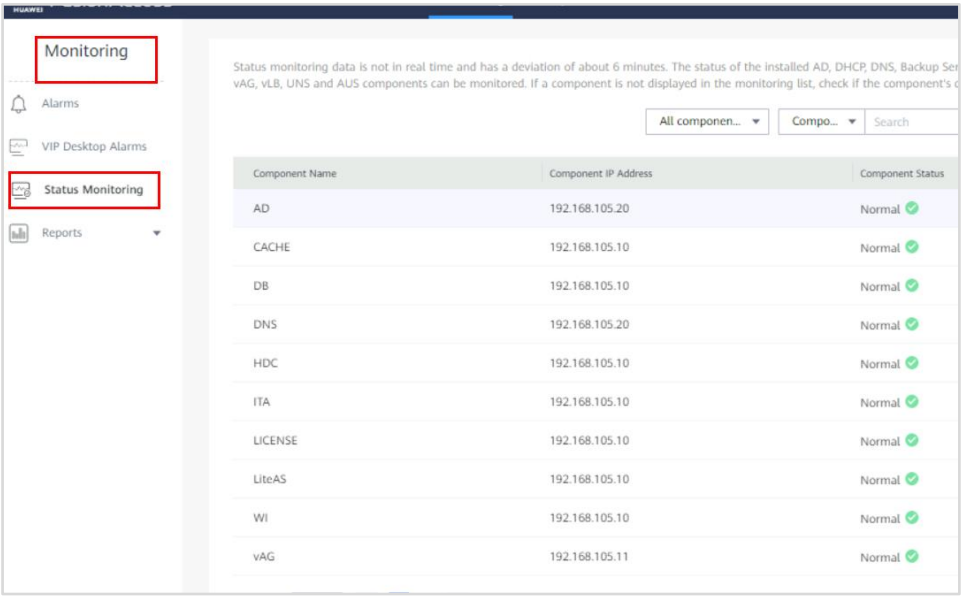


Figure 3-76 Status of each component

Step 3 Log in to FusionAccess Web Client, choose **Monitoring** > **VIP Desktop Alarms**, and view the VIP desktop alarm information.

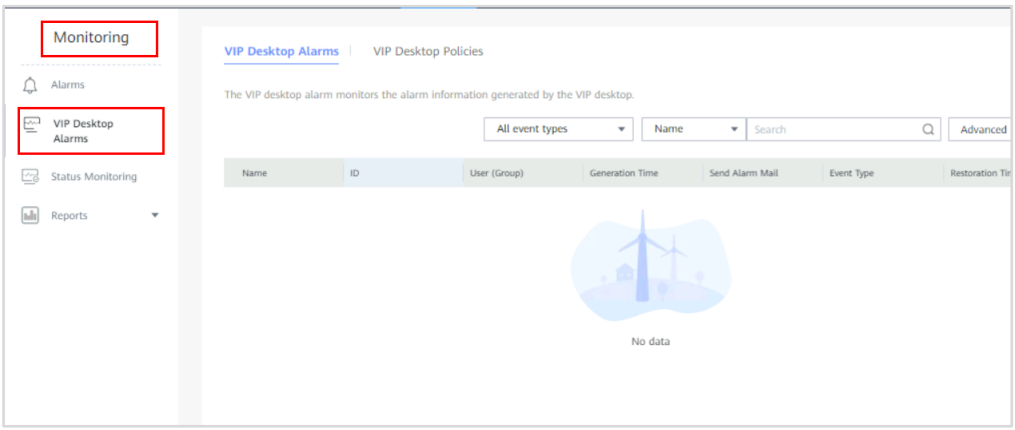


Figure 3-77 VIP desktop alarms

Step 4 Log in to FusionAccess Web Client, choose **Home** > **Computer Status Statistics**, and view the status statistics of computers used by users.

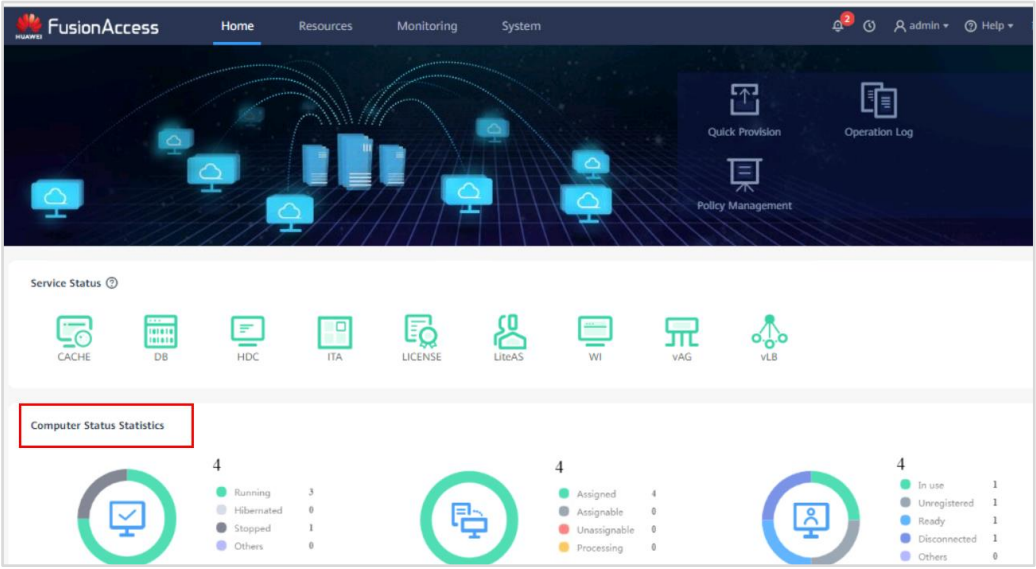


Figure 3-78 Computer status statistics

Step 5 Log in to FusionAccess Web Client, choose **Monitoring** > **Reports** > **vAG Information**, and view the gateway status.

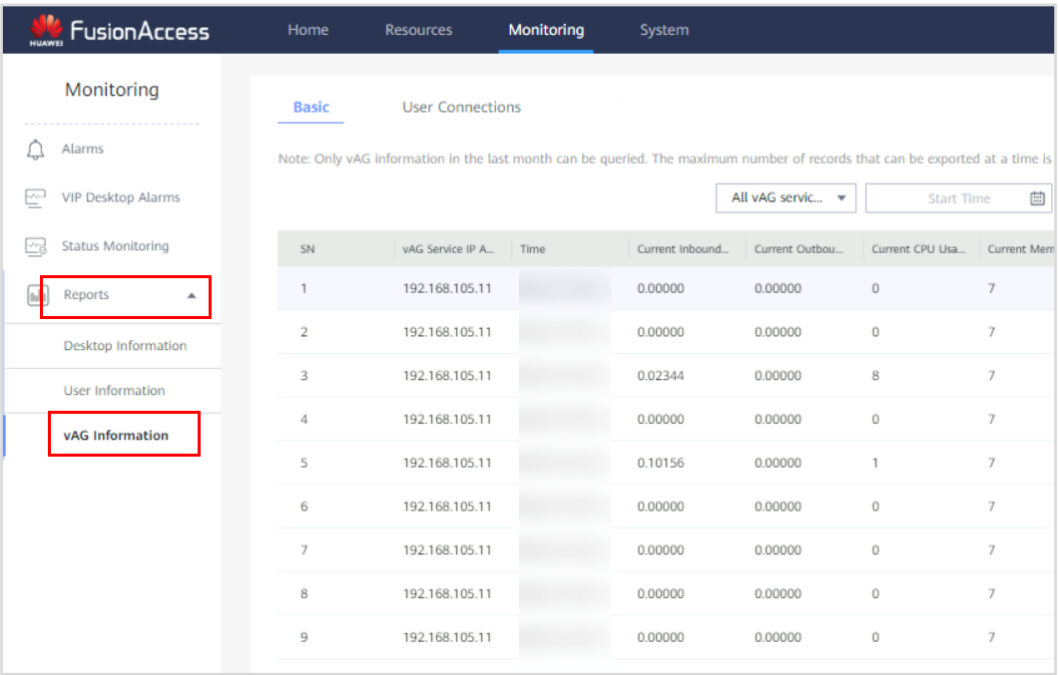


Figure 3-79 Gateway status

3.3 Quiz

What should I pay attention to when adding a computer user?

Answers:

To ensure that a computer user can be added, the following requirements must be met:

1. The assignment type of the computer must be **Assign a computer to multiple users**.
2. The running status of the computer is **Running**.