Cloud Data Center (CloudDC)

User Guide

Issue	01
Date	2025-03-31

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property 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 Cloud 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 Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 Permissions

1.1 Creating an IAM User and Granting CloudDC Permissions

You can use **Identity and Access Management (IAM)** for fine-grained permissions control for your Cloud Data Center (DC). With IAM, you can:

- Create IAM users for personnel based on your enterprise's organizational structure. Each IAM user has their own identity credentials for accessing CloudDC resources.
- Grant only the permissions required for users to perform a specific task.
- Entrust a Huawei Cloud account or a cloud service to perform efficient O&M on your CloudDC resources.

If your Huawei Cloud account does not require individual IAM users, you may skip this section.

Figure 1-1 shows the procedure for granting permissions.

Prerequisites

Before granting permissions to user groups, learn about system-defined permissions in for CloudDC in **Table 1-1**.

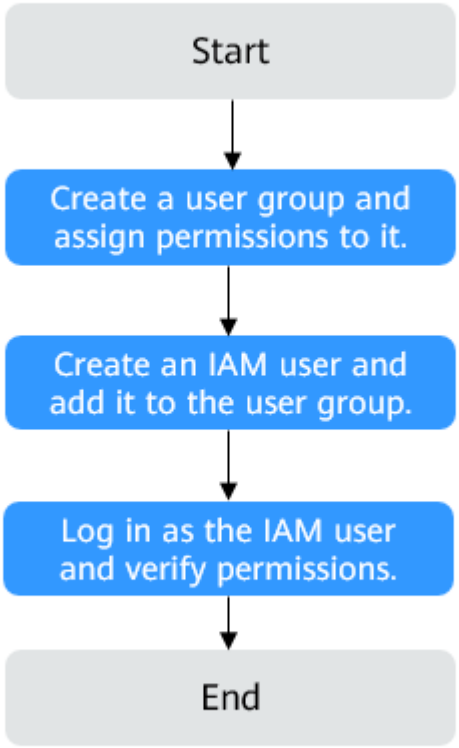
Table 1-1 System-defined permissions for CloudDC

Role/Policy Name	Description	Type	Dependencies
CloudDC FullAccess	Full permissions for CloudDC.	System-defined policy	None.

To grant permissions for other services, learn about all **system-defined permissions** supported by IAM.

Process Flow

Figure 1-1 Process for granting CloudDC permissions



1. On the IAM console, **create a user group and grant it permissions**.

   Create a user group on the IAM console and assign the **CloudDC FullAccess** permissions to the group.

2. **Create an IAM user and add it to the created user group**.

   Create a user on the IAM console and add the user to the group created in **1**.

3. **Log in as the IAM user** and verify permissions.

   In the authorized region, perform the following operations:

   Choose **Service List** > **Cloud Data Center**. Then click **Try Now** to go to the CloudDC overview page. If the page is displayed, the **CloudDC FullAccess** permissions are in effect.

2 CloudDC Scenario Differences and Resource Purchase Planning

CloudDC allows customers to purchase different types of resources based on service requirements to meet requirements in different scenarios. For details, see **Table 2-1**.

Table 2-1 Scenarios and resource purchase planning

Scenario	DC Cloud Adoption	Going Global
Description	You can deploy your servers to the Huawei public cloud for low-latency access to public cloud services. In addition, public cloud resources can be used to run workloads during service peaks.	By deploying your assets to Huawei Cloud equipment rooms, you can quickly get a highly reliable data center operating environment, eliminating the need for long-term investments in traditional data center site selection, infrastructure construction, facility reconstruction, O&M, and operations.

Scenario	DC Cloud Adoption	Going Global
Supported capabilities	• By deploying your assets to Huawei Cloud data centers, you can quickly get a highly reliable data center operating environment. • You can log in to, manage, and maintain servers through the CloudDC console. • A gateway between the CloudDC zone and Huawei Cloud is provided for the VPC network connectivity.	• By deploying your assets to Huawei Cloud data centers, you can quickly get a highly reliable data center operating environment. • The CloudDC console cannot be used to log in to, manage, and maintain servers. • Direct Connect is provided to connect your on-premises data centers to the Huawei Cloud data centers.
Purchasing resources	• Intelligent rack (iRack) • Intelligent bare metal (iMetal) • Cloud-based networks (CloudDCN)	Intelligent rack (iRack)

3 Servers

3.1 iMetal Server Overview

Introduction

You can manage your servers in Huawei Cloud data centers and access Huawei Cloud services as easily as using Huawei Cloud Bare Metal Server (BMS).

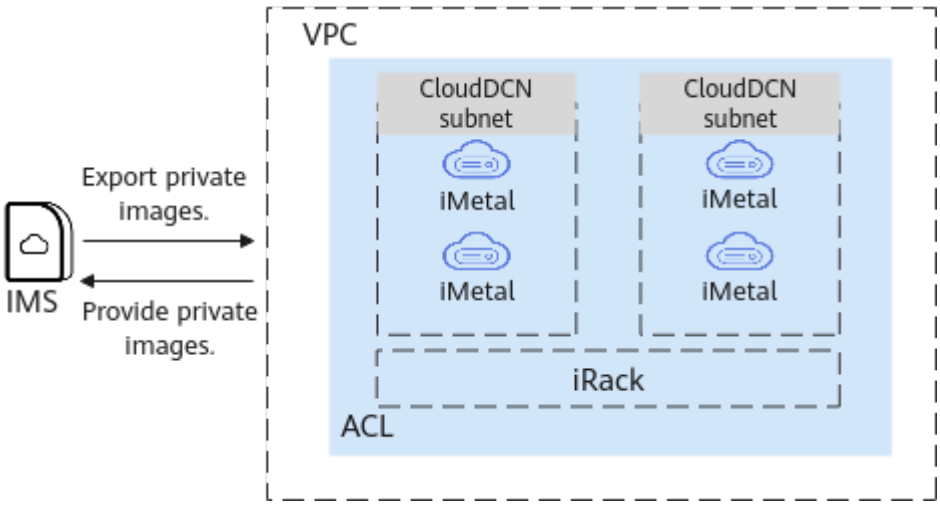
After deploying your servers in Huawei Cloud data centers, you can directly connect them to the Huawei Cloud private network to build a secure, dedicated network on the cloud. In addition, you can use the management console to maintain and manage servers.

Architecture

iMetal works with other cloud services to provide compute, storage, network, and image resources.

- iMetal servers are deployed in multiple availability zones (AZs) connected with each other through a private network. If an AZ becomes faulty, other AZs in the same region will not be affected.
- With Virtual Private Cloud (VPC), you can create a dedicated network for iMetal servers and configure subnets and network ACLs. iMetal servers in a VPC can communicate with public networks through EIPs (bandwidth support required).
- You can use Image Management Service (IMS) to install images on iMetal servers.
- Data is stored on the local disks of iMetal servers.

Figure 3-1 iMetal product architecture



Access Modes

The public cloud provides a web-based service management system (management console). You can access iMetal through the management console.

You can use the management console to access an iMetal server. Ensure that you have registered on Huawei Cloud. Then, log in to the management console and click **CloudDC**.

3.2 Creating an iMetal Server

3.2.1 Purchasing an iMetal Server

Scenarios

Leveraging Huawei Cloud's global compute, storage, and network capabilities, CloudDC provides stable and secure operating environment for data centers worldwide. You can deploy your own servers in the Huawei Cloud equipment rooms for low-latency access to public cloud services. In addition, public cloud resources can be used to run workloads when services are at their peaks.

After deploying your servers in Huawei Cloud, you can directly connect them to the Huawei Cloud private network to build a secure, dedicated network on the cloud. In addition, you can use the management console to maintain and manage servers.

If you want to deploy your own servers in CloudDC, you need to purchase resources on the management console.

Currently, the following resources can be purchased on the console:

- Intelligent rack (iRack)
- Intelligent bare metal (iMetal)
- Cloud-based networks (CloudDCN)

You can purchase iMetal servers separately or place a combined order to purchase iMetal servers and required racks and network resources.

This section describes how to purchase iRack, iMetal, and CloudDCN in a combined order.

NOTICE

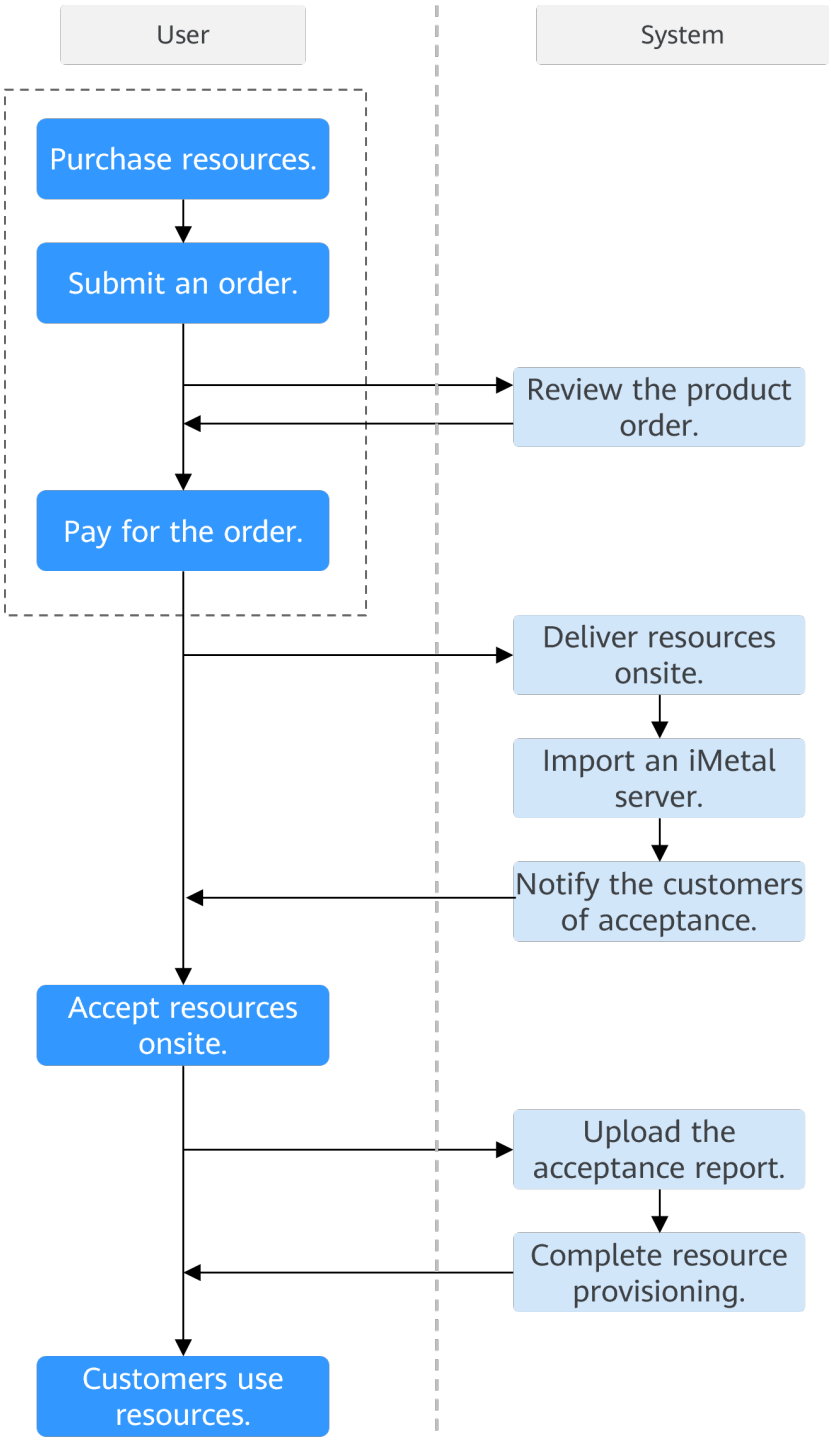
Offline operations and verification are required when you purchase iMetal servers. This section only describes how to purchase resources, submit orders, and pay for orders.

Constraints

- Currently, only the yearly/monthly billing mode is supported.
- If you place a combined order and want to cancel a sub-order, all sub-orders in the combined order will also be canceled.
- The resources purchased in a combined order must be in the same region.

Process

Figure 3-2 Process



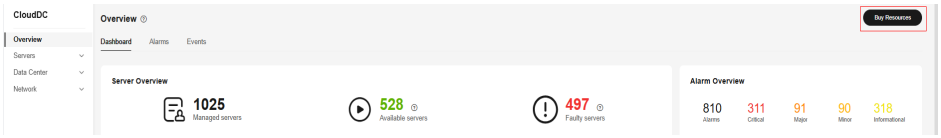
The following walks you through purchasing resources to paying for orders.

Procedure

1. Log in to the CloudDC console.

2. In the upper right corner of the **Overview** page, click **Buy Resources**. The **Buy Resources** page is displayed.

Figure 3-3 Purchasing resources



3. Set parameters for iRack and click **Add**.

Figure 3-4 iRack

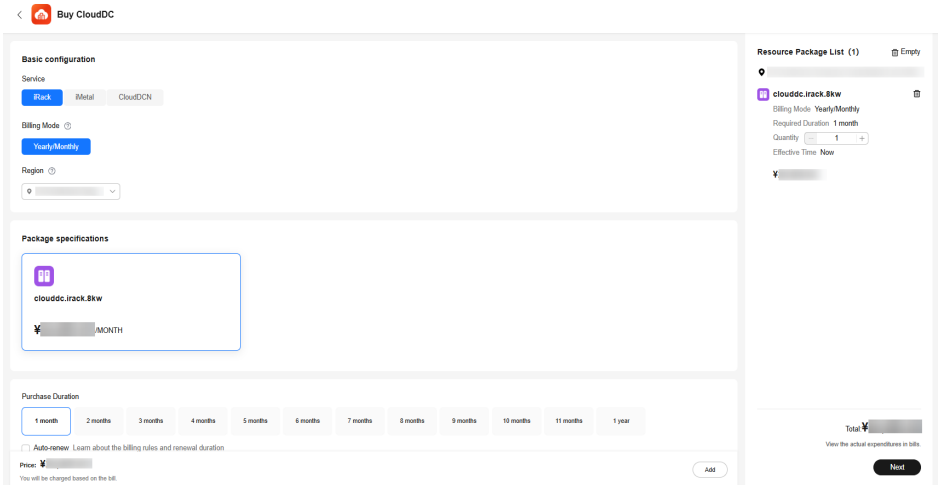


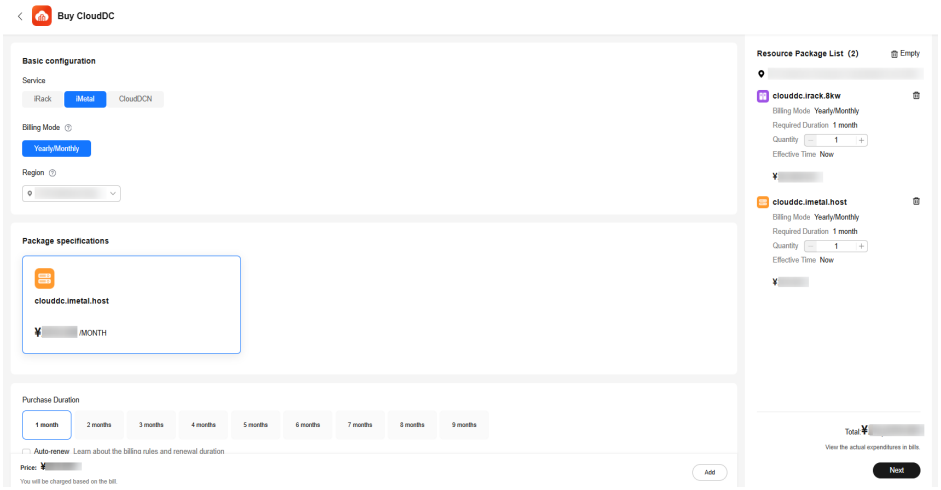
Table 3-1 Parameters

Parameter	Example Value	Description
Resource Type	iRack	Select the type of the resource to be purchased. Currently, the following resource types are supported: • iRack: used to deploy server hardware in Huawei Cloud equipment rooms. • iMetal: used to deploy your own servers in Huawei Cloud equipment rooms. • CloudDCN: used to connect servers deployed on Huawei Cloud to a private network on the cloud.
Billing Mode	Yearly/Monthly	Prepaid billing. You pay in advance for a subscription term, and in exchange, you get a discounted rate. Ensure that you have a top-up account with a sufficient balance or have a valid payment method configured first.

Parameter	Example Value	Description
Region	CN South-Guangzhou	For low network latency and quick resource access, select the region nearest to your target users. After the purchase, the region cannot be changed. The resources purchased in a combined order must be in the same region.
Specifications	clouddc.irack.8kw	Specifications of the resource package that can be purchased. The package specifications supported by different resource types are as follows: • iRack: clouddc.irack.8kw • iMetal: clouddc.imetal.host • CloudDCN: CloudDCN.GeneralNetwork.25G
Purchase Duration	1 month	Validity period of resources. The purchase duration varies depending on the resource type. For details, see the information displayed on the console. You can select **Auto-renew** to automatically renew yearly/monthly resources when they expire. For details about auto-renewal rules, see **Rules for Setting Auto-Renewal When Automatically Renewing a Cloud Service**.
Quantity	1	The number of resources to be purchased.

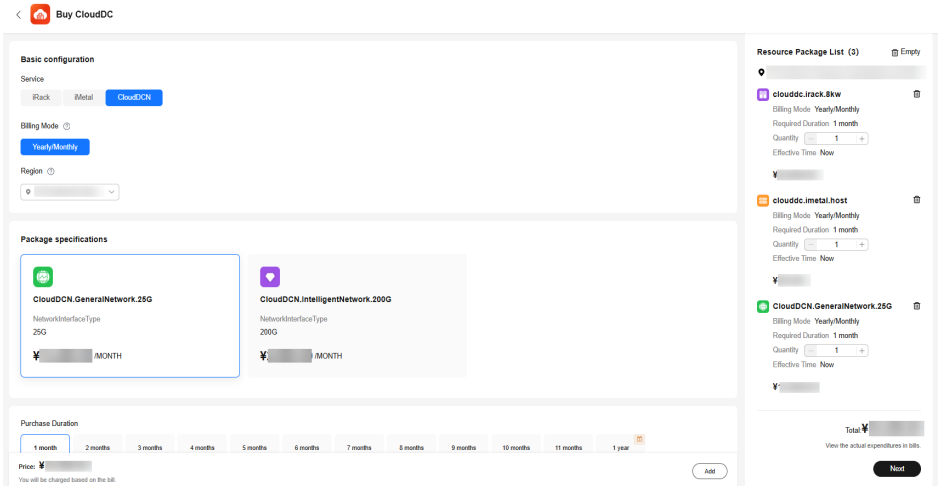
4. Set parameters for **iMetal** and click **Add**.
   For details about more parameters, see **Table 3-1**.

Figure 3-5 iMetal



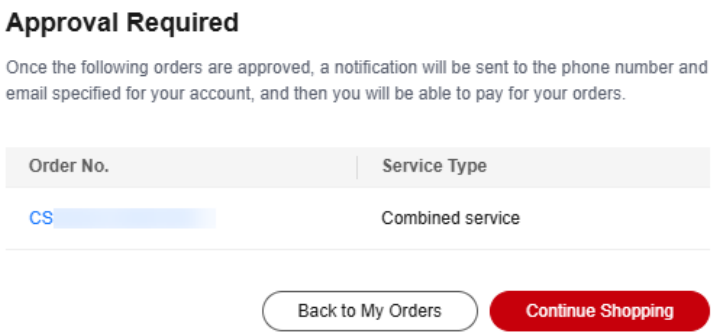
5. Set parameters for **CloudDCN** and click **Add**.
   For details about more parameters, see **Table 3-1**.

Figure 3-6 CloudDCN



6. In the lower right corner of the **Resource Package List** pane, click **Next**.
7. After confirming the configuration, click **Pay**.
   The resource purchase order can be paid only after it is approved.

Figure 3-7 Order review



8. On the menu bar of the console, choose **Billing** > **Unpaid Orders** and view the order status in the **Order Status** column.

   During the transaction, the order status changes as follows:

   a. **Pending approval**: The user has submitted an order and is waiting for the approval.

   b. **Pending payment**: After the order is approved, the user can pay for the order.

   c. **Processing**: After the payment is complete, the on-premises resource deployment phase starts.

   d. **Completed**: The offline acceptance is complete, resources are enabled, and the order is complete.

3.2.2 Importing an iMetal Server

Scenarios

iMetal allows you to import servers to the CloudDC console so that you can better maintain the iMetal servers on the console.

You need to confirm the serial numbers, models, vendors, racks in the equipment rooms, and BMC account of the servers, and import the iMetal server information using a template (.xlsx file).

This section describes how to import iMetal servers on the console.

Constraints

- A maximum of 500 records can be imported.
- New data will not overwrite the existing data. Duplicate records are not imported.
- After the iMetal servers are imported, the server information cannot be modified.
- Data can be imported again only when **Management Status** is **Verification failed**.

Prerequisites

- Ensure that you have applied for the OBT and have the required permissions to access the CloudDC console.
- Ensure that the information has been collected because you need to fill in server information using a template.

  For details about server information, see **Table 3-2**.

Procedure

1. Log in to the CloudDC console.
2. In the navigation pane, choose **Servers** > **iMetal Servers**.

   The **iMetal Servers** page is displayed.
3. In the upper part of the iMetal server list, choose **More** > **Import**. The **Import** dialog box is displayed.
4. Click **Download Template** to download the template.

   If you have filled in the server details based on the template requirements, go to step **6**.
5. Enter server information in the downloaded template based on the template requirements.

NOTICE

Once the iMetal server information is imported, it cannot be modified. If the information is incorrect, import it again.

Table 3-2 Server template information

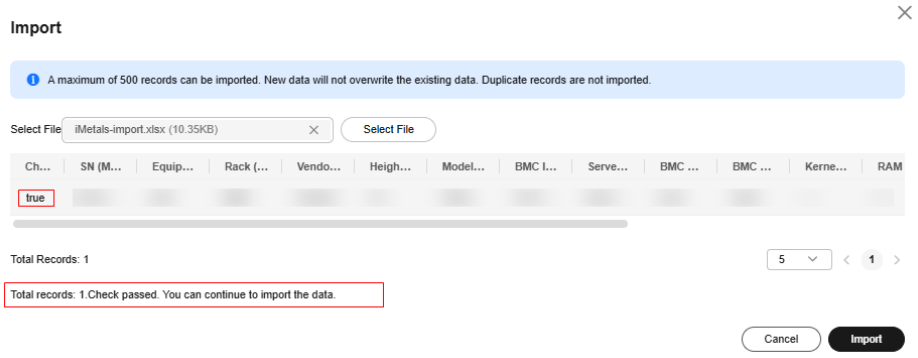
Parameter	Mandatory	Description
SN	Yes	Unique ID of an iMetal server.
Equipment Room	Yes	Equipment room where the iMetal server is located.
Rack	Yes	Rack where the iMetal server resides.
Vendor	Yes	Vendor of the iMetal server.
Height (U)	Yes	Physical storage space required by the iMetal server in the rack.
Model	Yes	Model of the iMetal server.
BMC IP Address	Yes	BMC IP address of the iMetal server.
Server Name	Yes	Name of the iMetal server.

Parameter	Mandatory	Description
BMC Username	Yes	BMC login username, which contains a maximum of 128 characters.
BMC Password	Yes	BMC login password, which contains a maximum of 64 characters.
Kernel Image ID	Yes	ID of the kernel image used by the iMetal server.
RAM Disk Image ID	Yes	ID of the ramdisk image used by the iMetal server.
Hardware Specifications	Yes	iMetal hardware specifications. The value can contain up to 256 characters, including letters, digits, plus signs (+), multiplication signs (x), parentheses (()), brackets ([]), hyphens (-), underscores (_), spaces, and periods (.).
Provision Subnet Gateway IP	Yes	Subnet gateway IP address of the Provision plane of the iMetal server.
Boot Mode	Yes	Boot mode of the iMetal server, which can be BIOS or UEFI. BIOS is used by default.
Skip Formatting	No	Used to control a formatting policy for a bare metal server during capacity expansion and commissioning. Value: True (skip formatting) or False (format). Default: False)
Formatting Policy Duration	No	Duration of the formatting policy, which must be a positive integer. If formatting is skipped, this parameter is mandatory. The maximum value is **120** and the unit is hours.

6. Click **Select File** and select the file where the server information has been configured.

   The system automatically checks whether the imported data is valid.

Figure 3-8 Checking data



7. After checking the data, click **Import** to import the server information.

   After the import is complete, you can view the imported server information in the iMetal list. If **Management Status** of the iMetal server is changed from **Onboard**, **Verifying**, to **Ready**, the import is successful. If it is **Verification failed**, check the server information in the uploaded file, modify the information, and upload the file again.

   It takes 10 to 15 minutes to verify the iMetal server.

Follow-up Operations

After an iMetal server is imported, you need to install an OS for the server. For details, see **Installing an OS on an iMetal Server**.

3.2.3 Installing an OS on an iMetal Server

Scenarios

After an iMetal server is imported and installed, no OS is installed. You need to install an OS for the iMetal server on the management console.

OS installation includes selecting an image for the iMetal server, configuring a network, and setting the remote login password.

After the OS is installed, **Management Status** of the iMetal server changes to **Running**. You can remotely log in to the iMetal server.

Constraints

- Currently, only Linux private images can be installed on an iMetal server.
- During the installation of an OS on an iMetal server, other operations on the server cannot be performed.

Prerequisites

An **iMetal server** has been imported, and **Management Status** of the iMetal server is **Ready**.

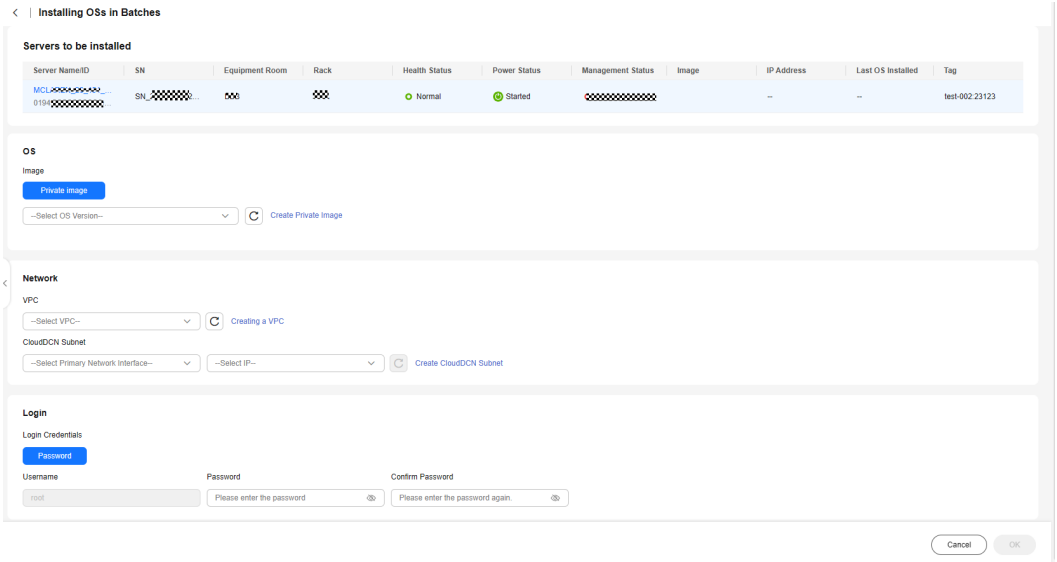
Procedure

1. Log in to the CloudDC console.
2. In the navigation pane, choose **Servers** > **iMetal Servers**.

   The **iMetal Servers** page is displayed.
3. In the iMetal server list, select the iMetal server where an OS is to be installed.
4. Click **Install OS** above the list.

   The **Install OS** page is displayed.

Figure 3-9 Batch OS installation



5. Configure parameters as follows.

Table 3-3 Parameters for installing an OS

Parameter		Description
OS	Image	Currently, only private images are supported. A private image is a personal image created or imported by a user and is visible only to the user who created or imported it. A private image contains an OS, preinstalled public applications, and a user's private applications. For details, see **Creating a Private Image for iMetal Servers**.
Network	VPC	With CloudDCN subnets, you can connect iMetal servers to an isolated, private, and high-performance cloud network. You can select an available VPC from the drop-down list or create a VPC as required. For details, see **Creating a VPC and Subnet** and **Creating a CloudDCN Subnet**.

Parameter		Description
	CloudDCN Subnet	After a VPC is selected, the system does not associate the CloudDCN subnet by default. You need to select a CloudDCN subnet and set the private IP address assignment mode. If no CloudDCN subnet is available, see **Creating a CloudDCN Subnet**.
Login	Login Credentials	Login credentials are used to set the mode for logging in to an iMetal server. • Password: The initial password is used to log in to an iMetal server. You can log in to the iMetal server using the username and password. •
	Password	Set **Password** and **Confirm Password**. The two values entered must be the same. The password must comply with the rules listed in **Table 3-4**.

Table 3-4 Password complexity requirements

Parameter	Requirement
Password	• Consists of 8 to 26 characters. • Must contain at least three of the following character types: – Uppercase letters – Lowercase letters – Digits – Special characters Linux: !@%^-_=+[]{}:,./? • Cannot be the username or the username spelled backwards. • Cannot contain the username or the username spelled backwards.

6. Click **OK** to start the installation.

   When the **Management Status** of the iMetal server changes to **Running**, the OS is installed successfully.

3.3 Viewing iMetal Servers

3.3.1 Checking the iMetal Server Status

Scenarios

After an iMetal server is created, you can view the server status in the **Management Status** column of the iMetal server.

The management status of the iMetal server is shown in **Table 3-5**.

Table 3-5 iMetal server management status

iMetal Server Status	iMetal Server Status Code	Description
Onboard	Onboard	The iMetal server has been imported.
Verifying	Verifying	The iMetal server data is being verified.
Ready	Ready	The iMetal server data has been verified.
Installing OS	Deploying	An OS is installing on the iMetal server.
Running	Running	An OS has been installed on the iMetal server.
Uninstalling OS	Undeploying	An OS of the iMetal server is being uninstalled.
Verification failed	RegisterError	The iMetal server failed to be registered.
OS installation failed	DeployError	An OS failed to be installed on the iMetal server.
OS uninstallation failed	UndeployError	The OS failed to be uninstalled on the iMetal server.
Deleting	Deleting	The iMetal server is being deleted.
Deletion failed	DeleteError	The iMetal server failed to be deleted.

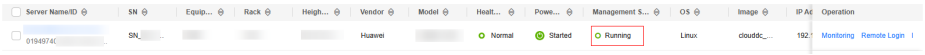
The following describes how to check the management status of an iMetal server.

Procedure

1. Log in to the CloudDC console.
2. In the navigation pane, choose **Servers** > **iMetal Servers**.

   The **iMetal Servers** page is displayed.
3. In the iMetal server list, locate the server to be checked and view its status in the **Management Status** column.

   Figure 3-10 Server management status



3.3.2 Querying iMetal Details

Scenarios

After you create an iMetal server, you can view and manage it on the management console.

This section describes how to check details about an iMetal server, including the server name/ID, OS, image, and IP address.

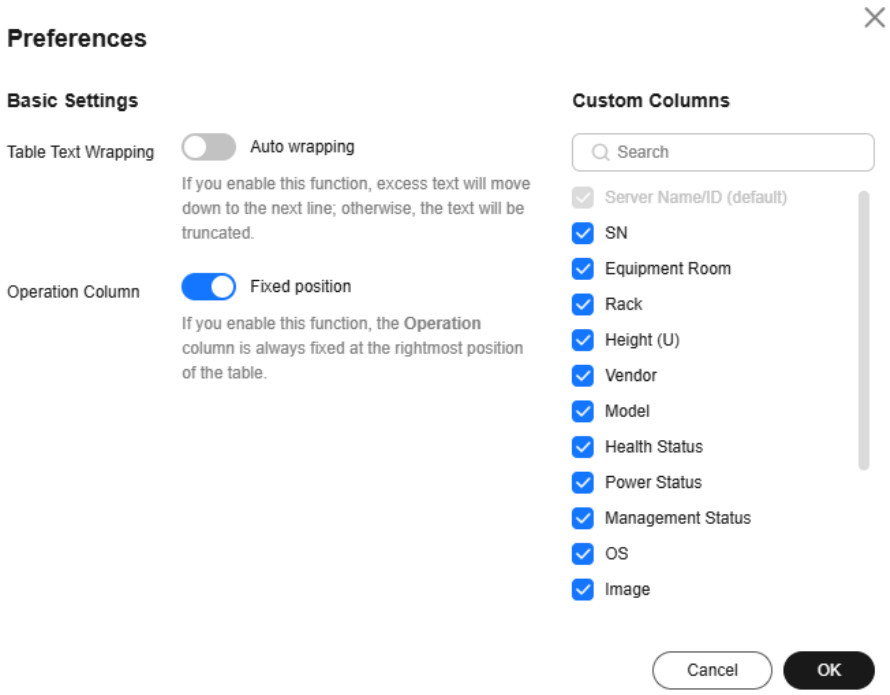
Procedure

1. Log in to the CloudDC console.
2. In the navigation pane, choose **Servers** > **iMetal Servers**.

   The **iMetal Servers** page is displayed.
3. In the iMetal server list, view the server name/ID, SN, and equipment room of the iMetal server.

   a. Click  on the right of the search box to customize the columns to be displayed in the list.

Figure 3-11 Custom columns

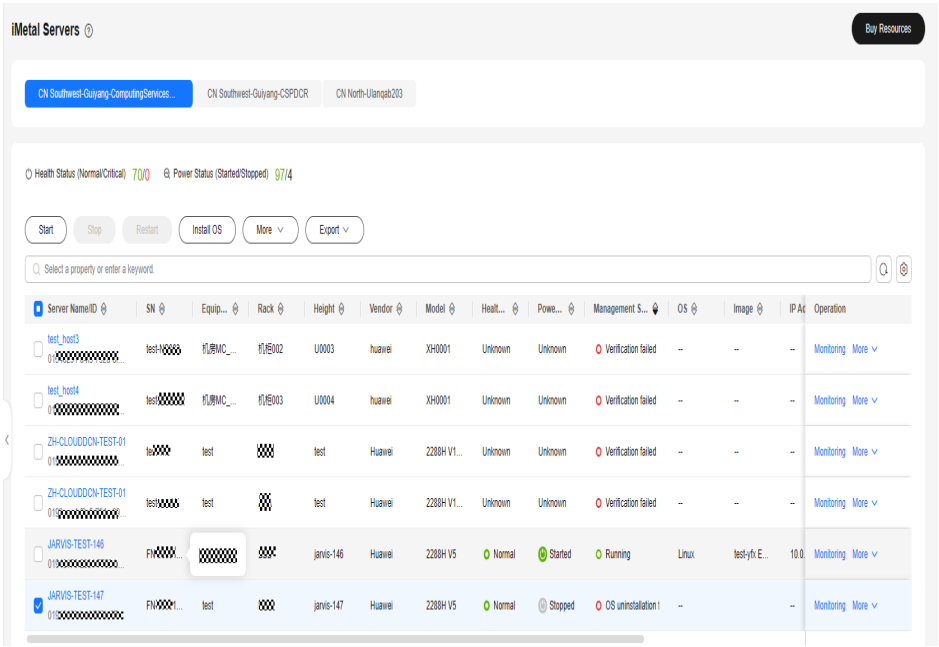


4. Search for the specified iMetal server in the search box.

   The iMetal server list displays all iMetal servers of the current account. You can enter a keyword in the search box to quickly search for an iMetal server.

   You can search for an iMetal server by attribute or by keyword. The attribute types include the SN, server name, equipment room, and rack.

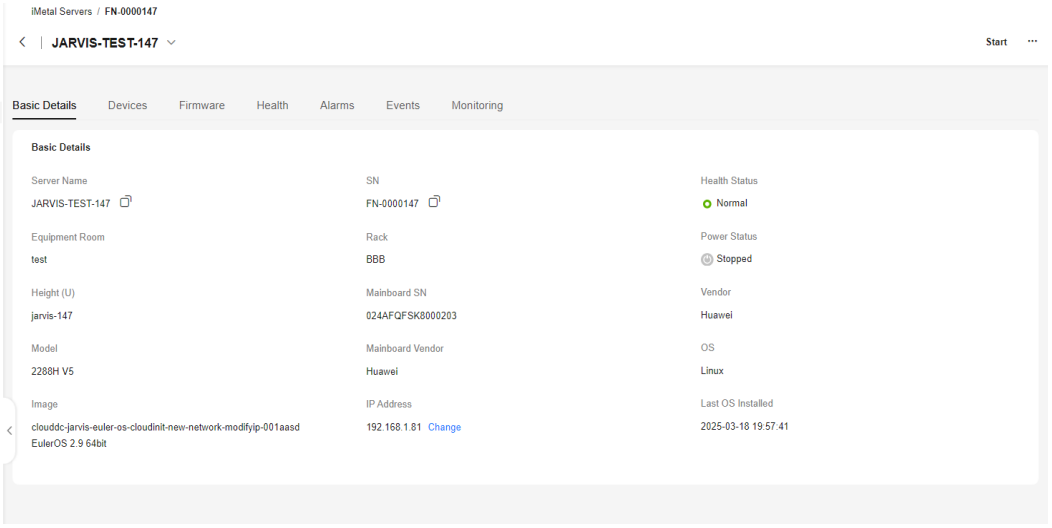
   Figure 3-12 iMetal server search box



5. Click the name of the iMetal server. The iMetal server details page is displayed.

6. On the iMetal server details page, view details about the iMetal server, such as the device and firmware information.

Figure 3-13 iMetal server details



3.3.3 Exporting the iMetal List

Scenarios

You can export the iMetal server information of your account to a local file in XLSX format. You can export all or specified iMetal servers.

The file is named in the format of "iMetal-Region-Current date" and records the name, status, and specifications of the iMetal server.

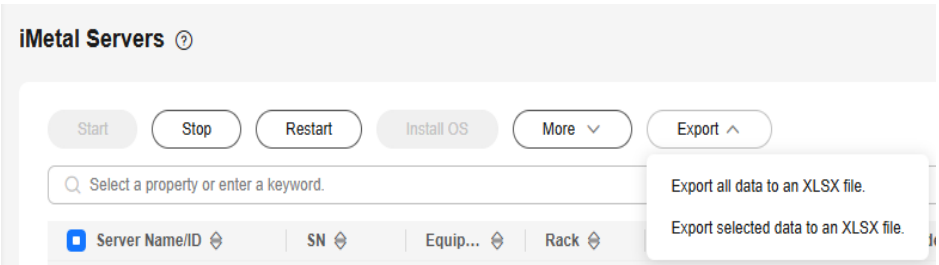
Procedure

1. Log in to the CloudDC console.
2. In the navigation pane, choose **Servers** > **iMetal Servers**.

   The **iMetal Servers** page is displayed.
3. Above the iMetal server list:
   - Export all iMetal servers.

     Choose **Export** > **Export all data to an XLSX file.** to export information about all iMetal servers of the current account and region to the local PC.

Figure 3-14 Exporting all iMetal servers



- Export a specified iMetal server.
  i. In the iMetal list, select the iMetal server to be exported.
  ii. Choose **Export** > **Export selected data to an XLSX file.** to export information about the specified iMetal server to the local PC.

3.4 Logging In to an iMetal Server

3.4.1 iMetal Server Login Methods

Choose an appropriate method to log in to an iMetal server based on the iMetal network configuration and your local PC OS.

- Use **Remote Login** on the management console and set **Login Credentials** to **Password**.
  For details, see **Logging In to an iMetal Server**.
- Use a remote connection tool, such as SSH, and set **Login Credentials** to **Password**.
  For details, see **Logging In to an iMetal Server Using an SSH Password**.

3.4.2 Logging In to an iMetal Server

Scenarios

If common remote connection software (such as SSH) is unavailable, you can use the remote login function on the management console to log in to an iMetal server.

Constraints

- Only Linux iMetal servers support remote login.
- When you log in to an iMetal server remotely, shortcut keys such as Ctrl and Alt are not well supported. For example, if you enter **Alt +** *ASCII code*, multiple special characters are displayed.
- Before exiting the management console, log out of the OS.

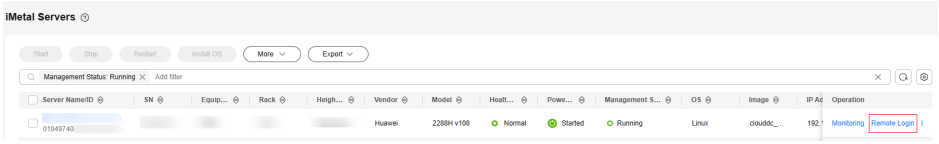
Prerequisites

- The iMetal server must be in **Running** state.
- You have set a login password when creating the iMetal server. If you do not set the password or forget the password, perform the operations as instructed in **Resetting the iMetal Password**.

Procedure

1. Log in to the CloudDC console.
2. In the navigation pane, choose **Servers** > **iMetal Servers**.
   The **iMetal Servers** page is displayed.

Figure 3-15 iMetal server list



3. In the iMetal server list, locate your iMetal server and click **Remote Login** in the **Operation** column.

   After about one minute, the login page is displayed. Press **Enter** and enter username **root** and password to log in.

   NOTE

   - If you do not log in within 10 minutes, the login page becomes invalid. You need to click **Remote Login** again.
   - If you do not perform any operation for 10 minutes after you log in, the page will expire, and you need to log in again.

3.4.3 Logging In to an iMetal Server Using an SSH Password

Scenarios

When a computer running Linux is connected to an iMetal server, you can log in to the iMetal server using the SSH password on the computer.

This section describes how to log in to an iMetal server from a Linux ECS using an SSH password via a VPC peering connection.

Constraints

- The iMetal server must be in **Running** state.
- The network connection between the login tool (such as SSH) and the target iMetal server is normal. For example, the default port 22 is not blocked by the firewall.

Prerequisites

- You have purchased a Linux ECS in the same region as the iMetal server.

  For details, see **Purchasing an ECS in Custom Config Mode**.
- An EIP has been bound to the ECS.

  For details, see **Binding an EIP**.

Logging In to the Server from a Linux PC

For an ECS running Linux, you can run the **ssh** command on the CLI to log in to the iMetal server.

1. Log in to the management console.
2. (Optional) Create a VPC peering connection.
   - If the VPC where the ECS is deployed is different from that of the iMetal server, you need to configure a VPC peering connection.

- If the VPC where the ECS is deployed is the same as that of the iMetal server, you do not need to configure a VPC peering connection. In this case, skip this step.

For details about how to create a VPC peering connection, see **Creating a VPC Peering Connection to Connect Two VPCs in the Same Account**.

NOTE

- When adding routes for the VPC peering connection, ensure that the destination of the VPC where the ECS is deployed is set to the CloudDCN subnet segment of the VPC where the iMetal server belongs.
- The security group of the ECS must allow traffic from port 22.

3. Remotely log in to the ECS.
4. Run the following command and log in to the iMetal server.

   ssh *<Private-IP-address-of-the-iMetal-server>*

3.5 Managing an iMetal Server

3.5.1 Resetting the iMetal Password

Scenarios

If you forget the password for logging in to an iMetal server or if you want to set a stronger password to improve the password security, you can reset the password on the console.

NOTE

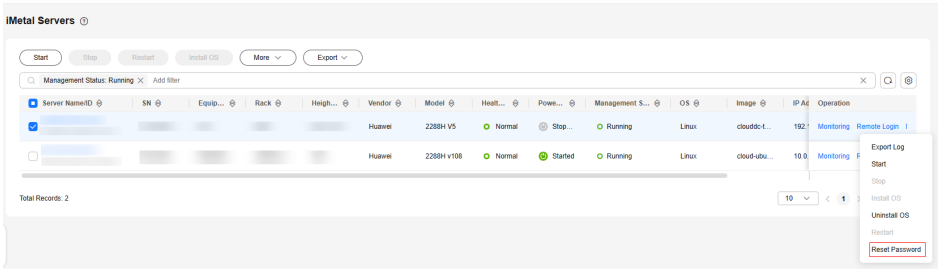
Before resetting the password, ensure that the iMetal server is stopped. After changing the password on the console, you need to manually restart the server. To prevent data loss, it is recommended that you reset the password during off-peak hours to minimize the impact on your services.

Procedure

1. Log in to the CloudDC console.
2. Choose **Servers** > **iMetal Servers**.

   The **iMetal Servers** page is displayed.
3. In the iMetal server list, select the iMetal server whose password is to be reset and choose **More** > **Reset Password** in the **Operation** column.

Figure 3-16 Resetting a password



4. Set and confirm a new password as prompted.

Figure 3-17 Resetting a password

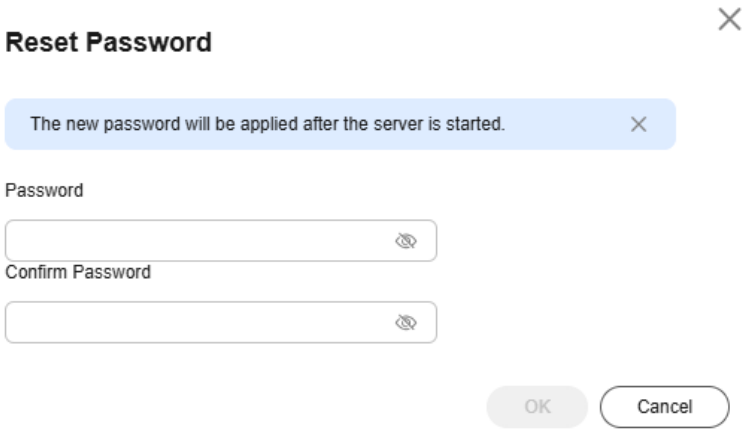


Table 3-6 Password complexity requirements

Parameter	Requirement
Password	• Consists of 8 to 26 characters. • Must contain at least three of the following character types: – Uppercase letters – Lowercase letters – Digits – Special characters Linux: !@%^-_=+[]{}:,./? • Cannot be the username or the username spelled backwards. • Cannot contain the username or the username spelled backwards.

5. Click **OK**.

   It takes about 10 minutes for the system to reset the password. Do not repeatedly perform this operation. After resetting the password, manually restart the iMetal server. After the iMetal server is restarted, use the new password to log in to the iMetal server to check whether the new password is applied.

3.5.2 Starting an iMetal Server

Scenarios

You can start an iMetal server only when the iMetal server is stopped.

Prerequisites

The iMetal server must be stopped.

Procedure

1. Log in to the CloudDC console.
2. In the navigation pane, choose **Servers** > **iMetal Servers**.

   The **iMetal Servers** page is displayed.
3. In the iMetal server list, locate your iMetal server and choose **More** > **Start** in the **Operation** column.

   To start multiple iMetal servers, select them and click **Start** at the top of the iMetal list.
4. In the **Start** dialog box, confirm the information and click **OK**.

   After the iMetal server is started, the **Power Status** of the iMetal server changes to **Started**.

3.5.3 Stopping an iMetal Server

Scenarios

You can stop an iMetal server as needed.

NOTE

- Stopping an iMetal server will forcibly interrupt services running on it. Before performing this operation, ensure that you have saved files on the iMetal server.
- You can stop an iMetal server only on the management console and cannot run **shutdown** to stop it. The **shutdown** and other commands attempting to stop an iMetal server will be regarded as unexpected operations and will not take effect.

Prerequisites

The iMetal server must be started.

Procedure

1. Log in to the CloudDC console.
2. In the navigation pane, choose **Servers** > **iMetal Servers**.

   The **iMetal Servers** page is displayed.
3. In the iMetal server list, locate your iMetal server and choose **More** > **Stop** in the **Operation** column.

   To stop multiple iMetal servers, select them and click **Stop** at the top of the iMetal server list.
4. In the **Stop** dialog box, confirm the information and click **OK**.

   After the iMetal server is stopped, the iMetal server is in the **Stopped** state.

3.5.4 Restarting an iMetal Server

Scenarios

You can restart an iMetal server on the management console.

NOTE

Restarting an iMetal server will interrupt your services. Exercise caution when performing this operation.

Prerequisites

The iMetal server must be started and its **Management Status** is **Running**.

Procedure

1. Log in to the CloudDC console.
2. In the navigation pane, choose **Servers** > **iMetal Servers**.

   The **iMetal Servers** page is displayed.
3. In the iMetal server list, locate your iMetal server and choose **More** > **Restart** in the **Operation** column.

   To restart multiple iMetal servers, select them and click **Restart** at the top of the iMetal list.
4. In the **Restart** dialog box, confirm the information and click **OK**.

3.5.5 Uninstalling the OS from an iMetal Server

Scenarios

If an iMetal server needs to be removed or the OS fails to be reinstalled, you can uninstall the iMetal server and reinstall the OS to rectify the fault.

- The OS cannot start.
- The OS is infected with viruses.
- The OS is running properly, but the system needs to be optimized to work in the optimal state.

This section describes how to uninstall the OS of an iMetal server.

Constraints

The management status of the iMetal server whose OS is to be uninstalled must be **Running** or **OS reinstallation failed**.

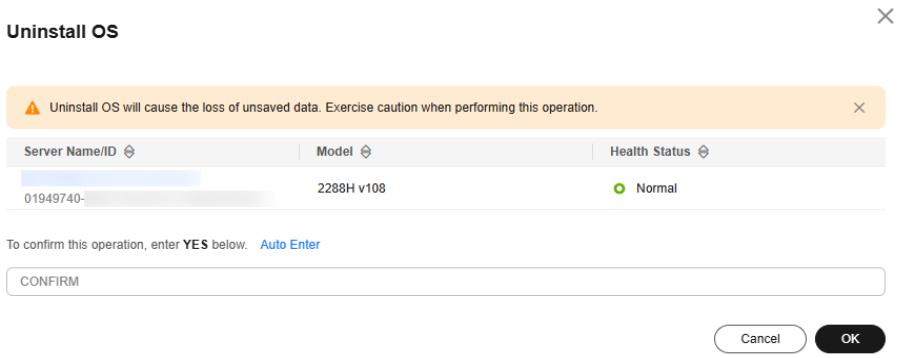
NOTICE

Uninstalling the OS will cause data loss on the iMetal server. Exercise caution when performing this operation.

Procedure

1. Log in to the CloudDC console.
2. In the navigation pane, choose **Servers** > **iMetal Servers**.
   The **iMetal Servers** page is displayed.
3. In the iMetal server list, select the iMetal server whose OS is to be uninstalled.
4. In the upper part of the list, click **More** > **Uninstall OS**.
   The **Uninstall OS** dialog box is displayed.
5. In the displayed dialog box, confirm the information about the server where the OS is to be uninstalled and click **OK**.

   Figure 3-18 Uninstalling the OS



   If the management status of the iMetal server changes to **Ready**, the OS installation is successful.

3.5.6 Exporting iMetal Server Logs

Scenarios

You can export iMetal server operation logs on the console for fault locating and troubleshooting.

This section describes how to export iMetal server logs.

Procedure

1. Log in to the CloudDC console.
2. Choose **Servers** > **iMetal Servers**.
   The **iMetal Servers** page is displayed.
3. In the iMetal server list, locate the iMetal server whose logs you want to export and choose **More** > **Export Log** in the **Operation** column.
   You can download the log information of the iMetal server to a local PC in the format of *{sn}*-**dump.tar.gz**.

3.6 Creating a Private Image for iMetal Servers

3.6.1 Overview

Introduction

To ensure an iMetal server can work properly on the management console, you need to install an OS for it. You can use an image for OS installation. Before that, you need to register an image file as an IMS private image on Huawei Cloud.

This section describes how to create a private image. You can create one based on your OS type.

You can also install software as needed to customize your private image.

Constraints

- Only Linux servers can be used to create images.
- Only x86 images are supported.
- You can create a private image for an iMetal server by importing an image file.

  The image file format can be VMDK, VHD, QCOW2, RAW, VHDX, QED, VDI, QCOW, ZVHD2, or ZVHD.
- The image file size cannot exceed 128 GB.

  If an image file is between 128 GB and 1 TB, convert it into RAW or ZVHD2 format and import it using fast import.
  - Convert the image file format by referring to **Converting the Image Format Using qemu-img-hw**.
  - For details about how to quickly import an image file, see **Fast Import of an Image File**.
- For details about the supported OSs, see **External Image File Formats and Supported OSs**.

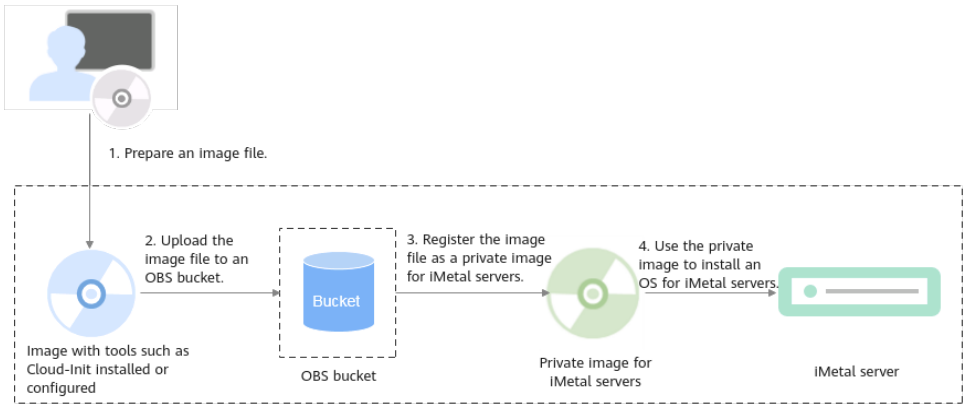
Procedure

You can create an image in either of the following ways:

- Scenario 1: If no image file has been exported from the original server or VM, install and configure Cloud-Init and network-related services on the original server or VM, export an image file, and upload the image file to an OBS bucket. Then register the image file as a private image for iMetal servers.

  Figure 3-19 shows the process of creating a private image.

Figure 3-19 Creating a system disk image (scenario 1)

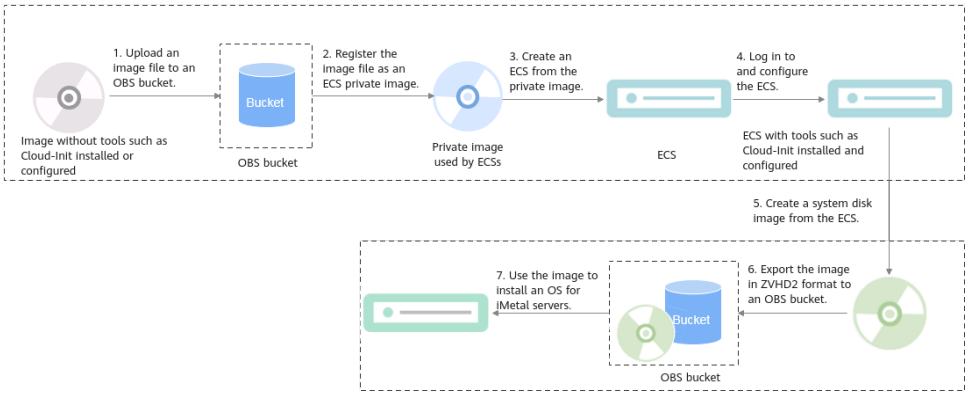


For details, see **Scenario 1: No Image File Exported from the Original Server or VM**.

- Scenario 2: An image file (in VMDK, VHD, QCOW2, RAW, VHDX, QED, VDI, QCOW, ZVHD2, or ZVHD format) has been exported from the original server or VM. You need to use the image file to create an ECS on Huawei Cloud. After installing and configuring tools such as Cloud-Init and network-related services on the ECS, use the ECS to create a private image for iMetal servers.

  Figure 3-20 shows the process of creating a private image.

Figure 3-20 Creating a system disk image (scenario 2)



For details, see **Scenario 2: External Image File Exported from the Original Server or VM**.

3.6.2 Scenario 1: No Image File Exported from the Original Server or VM

3.6.2.1 Preparing an External Image File

3.6.2.1.1 Process for Preparing an External Image File

Before exporting an external image file from the original platform, configure a server or VM on that platform as instructed in this section so that an iMetal server private image created from that server or VM can work properly.

You are strongly advised to configure a server or VM on the original platform and export an image file.

If you cannot configure a server or VM on the original platform, you are advised to create an image file by referring to **Scenario 2: External Image File Exported from the Original Server or VM**.

Preparing an Image File

Table 3-7 Initial configuration for an image file

No.	Configuration Item	Description	Reference
1	Network	Mandatory. If this item is not configured, the server startup or network capability will be abnormal.	• **Deleting Files from the Network Rule Directory** • **Configuring DHCP**
2	Tools	Cloud-Init is an open-source cloud initialization tool. When creating a server from an image that has Cloud-Init installed, you can inject custom information (such as the login password) into the server. You can also query and use metadata to configure and manage running servers. If Cloud-Init is not installed, custom information cannot be injected into your server and you can only log in to it using the password in the image file.	• **Installing Cloud-Init (SLES/RHEL/CentOS/ Oracle Linux/Ubuntu/ Debian)** • **Installing Cloud-Init (EulerOS/openEuler)**
3	Password reset plug-in	To ensure that the password of your server created from a private image can be reset, you are advised to install the password reset plug-in CloudResetPwdAgent. For details, see **Resetting the iMetal Password**.	**Installing the One-Click Password Reset Plug-In**
4	bms-network-config	It is used to automatically configure networks.	**Installing bms-network-config**

No.	Configuration Item	Description	Reference
5	Network service	By default, the network service is not installed for CentOS 8, EulerOS 2.9, RHEL 8, Ubuntu 20, or later. For iMetal servers using centralized gateways, the network service and network scripts are required to configure the network.	**Installing the Network Service**
6	Drivers	If KVM drivers are not installed, servers may fail to detect network interfaces and cannot communicate with external systems.	**Installing Native KVM Drivers**
7	File system	The root partition identified in the configuration file varies depending on the OS. It may be **root=/dev/xvda** or **root=/dev/disk**. The disk identifiers need to be changed to UUID.	• **Changing Disk Identifiers in the GRUB File to UUID** • **Changing Disk Identifiers in the fstab File to UUID**
8	Data disks	If multiple data disks are attached to the original server used to create a private image, the new servers created from the image may be unavailable. You need to detach all data disks from the original server before using it to create an image.	**Detaching Data Disks from an ECS**

3.6.2.1.2 Installing Cloud-Init (SLES/RHEL/CentOS/Oracle Linux/Ubuntu/Debian)

Scenarios

Cloud-Init is a tool developed to initiate VMs or iMetal servers in a cloud environment. It is used to customize the network configuration, hostname, hosts file, username, and password for a VM or an iMetal server. Cloud-Init is also required if the password of a VM is generated by the system at random.

The Cloud-Init installation file has requirements on Linux versions and can only be installed from the Internet. Therefore, ensure that the server or VM on the original platform can access the Internet.

Description

- The Cloud-Init installation procedures in the following sections are for reference only. You are advised to download the Cloud-Init from the official website. The Cloud-init version is updated on the official website in real time. Install the latest version.

- When you modify the **/etc/cloud/cloud.cfg** file, ensure that the file format (such as alignment and spaces) is consistent with the provided example that conforms to the YAML syntax.
- You can install Cloud-Init in any of the following ways: **(Recommended) Installing Cloud-Init Using the Official Installation Package**, **Installing Cloud-Init Using the Official Source Code Package and pip**, and **Installing Cloud-Init Using the Compiled Source Code**

(Recommended) Installing Cloud-Init Using the Official Installation Package

The method of installing Cloud-Init on a VM varies depending on the OS. Perform the installation operations as user **root**.

The following describes how to install Cloud-Init on VMs running SUSE Linux Enterprise Server (SLES), CentOS, Debian, or Ubuntu. For other OS types, install the required type of Cloud-Init. For example, you need to install coreos-cloudinit on VMs running CoreOS.

- SLES

  Paths for obtaining the Cloud-Init installation package for SLES

  http://ftp5.gwdg.de/pub/opensuse/repositories/Cloud:/Tools/

  http://download.opensuse.org/repositories/Cloud:/Tools/

  NOTE

  Select the required repo installation package in the provided paths.

  Take SLES 12 as an example. Perform the following steps to install Cloud-Init:

  a. Run the following command to install the network installation source for SLES 12:

     zypper ar http://ftp5.gwdg.de/pub/opensuse/repositories/Cloud:/Tools/SLE_12_SP3/Cloud:Tools.repo

  b. Run the following command to update the network installation source:

     zypper refresh

  c. Run the following command to install Cloud-Init:

     zypper install cloud-init

  d. Run the following commands to enable Cloud-Init to automatically start upon system boot:

     - SLES 11

       chkconfig cloud-init-local on; chkconfig cloud-init on; chkconfig cloud-config on; chkconfig cloud-final on

       service cloud-init-local status; service cloud-init status; service cloud-config status; service cloud-final status

     - SLES 12 and openSLES 12/13/42

       systemctl enable cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service

       systemctl status cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service

NOTICE

For SLES and openSUSE, perform the following steps to disable dynamic change of the hostname:

1. Run the following command to open the **dhcp** file using the vi editor:
   vi etc/sysconfig/network/dhcp
2. Change the value of **DHCLIENT_SET_HOSTNAME** in the **dhcp** file to **no**.

- CentOS

  Table 3-8 lists the Cloud-Init installation paths for CentOS. Select an address from the following table and download the EPEL release package.

  Table 3-8 Cloud-Init installation package addresses

OS	Version	How to Obtain
CentOS	6 32-bit	**https://archives.fedoraproject.org/pub/archive/epel/6/i386/Packages/e/**
	6 64-bit	**https://archives.fedoraproject.org/pub/archive/epel/6/x86_64/Packages/e/**
	7 64-bit	**https://archives.fedoraproject.org/pub/archive/epel/7/x86_64/Packages/e/**

  Run the following commands to install Cloud-Init for CentOS 6.5 64-bit (example):

  yum install https://archives.fedoraproject.org/pub/archive/epel/6/x86_64/Packages/e/epel-release-*xx-xx*.noarch.rpm

  yum install cloud-init

  NOTE

  xx-xx indicates the version of Extra Packages for Enterprise Linux (EPEL) release required by the OS.

- Debian

  Before installing Cloud-Init, ensure that the network installation source address has been configured for the OS by checking whether the **/etc/apt/sources.list** file contains the installation source address of the software package. If the file does not contain the address, configure the address by following the instructions on the Debian official website.

  Run the following commands to install Cloud-Init:

  apt-get update

  apt-get install cloud-init

  After Cloud-Init is installed in the Debian OS, run the following commands to install the vlan and ifenslave services:

  apt-get install vlan

apt-get install ifenslave

- Ubuntu

  Before installing Cloud-Init, ensure that the network installation source address has been configured for the OS by checking whether the **/etc/apt/sources.list** file contains the installation source address of the software package. If the file does not contain the address, configure the address by following the instructions on the Ubuntu official website.

  Run the following commands to install Cloud-Init:

  apt-get update

  apt-get install cloud-init

  After Cloud-Init is installed in the Ubuntu OS, perform the following operations to install tools and services:

  a. Install the SSH service.

     For x86, run the following commands:

     apt-get install openssh-client

     apt-get install openssh-server

     For ARM64, run the following commands:

     apt install openssh-client

     apt install openssh-server

  b. Install dkms.

     To ensure that SDI drivers can run properly, you need to install dkms for Ubuntu.

     Run the following command to install the tool:

     apt-get install dkms

     Then, run the following command:

     vi /usr/sbin/dkms

     Go to line 283 (press **shift** and **:** to enter the CLI mode. Then, type **283** and press **Enter**) and modify this line as follows:

     ```
     invoke_command "$mkinitrd -f $initrd_dir/$initrd $1" "$mkinitrd" background
     ```

  c. Install the vlan and ifenslave services.

     apt-get install vlan

     apt-get install ifenslave

  d. Install the ifupdown service.

     apt-get install ifupdown

Installing Cloud-Init Using the Official Source Code Package and pip

The following operations use Cloud-Init 0.7.9 as an example to describe how to install Cloud-Init.

1. Download the **cloud-init-0.7.9.tar.gz** source code package (version 0.7.9 is recommended) and upload it to the **/home/** directory of the VM.

   Download **cloud-init-0.7.9.tar.gz** from the following path:

   https://launchpad.net/cloud-init/trunk/0.7.9/+download/cloud-init-0.7.9.tar.gz

2. Create a **pip.conf** file in the **~/.pip/** directory and edit the following content:

   NOTE

   If the **~/.pip/** directory does not exist, run the **mkdir ~/.pip** command to create it.

   ```
   [global]
   index-url  = https://<$mirror>/simple/
   trusted-host = <$mirror>
   ```

   NOTE

   Replace *<$mirror>* with a public network PyPI source.

   Public network PyPI source: **https://pypi.python.org/**

3. Run the following command to install the downloaded Cloud-Init source code package (select **--upgrade** as needed during installation):

   pip install [--upgrade] /home/cloud-init-0.7.9.tar.gz

4. Run the **cloud-init -v** command. Cloud-Init is installed successfully if the following information is displayed:

   ```
   cloud-init 0.7.9
   ```

5. Enable Cloud-Init to automatically start upon system boot.
   - If the OS uses SysVinit to manage automatic start of services, run the following commands:

     chkconfig --add cloud-init-local; chkconfig --add cloud-init; chkconfig --add cloud-config; chkconfig --add cloud-final

     chkconfig cloud-init-local on; chkconfig cloud-init on; chkconfig cloud-config on; chkconfig cloud-final on

     service cloud-init-local status; service cloud-init status; service cloud-config status; service cloud-final status
   - If the OS uses Systemd to manage automatic start of services, run the following commands:

     systemctl enable cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service

     systemctl status cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service

NOTICE

If you install Cloud-Init using the official source code package and pip, pay attention to the following:

1. Add user **syslog** to the **adm** group during the installation. If user **syslog** exists, add it to the **adm** group. For some OSs (such as CentOS and SLES), user **syslog** may not exist. Run the following commands to create user **syslog** and add it to the **adm** group:

   useradd syslog

   groupadd adm

   usermod -g adm syslog

2. Change the value of **distro** in **system_info** in the **/etc/cloud/cloud.cfg** file based on the OS release version, such as **distro: ubuntu**, **distro: sles**, **distro: debian**, and **distro: fedora**.

Installing Cloud-Init Using the Compiled Source Code

The Cloud-Init configuration has been compiled in the source code. Therefore, you do not need to configure Cloud-Init after the installation. You can obtain the Cloud-Init source code from GitHub at **https://github.com/canonical/cloud-init/**

1. Run the following commands to download the Cloud-Init package and copy it to the **/tmp/CLOUD-INIT** folder:

   NOTE

   Cloud-Init 0.7.6: https://github.com/canonical/cloud-init/archive/refs/tags/0.7.6.zip
   Cloud-Init 0.7.9: https://github.com/canonical/cloud-init/archive/refs/tags/0.7.9.zip

   wget https://github.com/canonical/cloud-init/archive/refs/tags/0.7.9.zip

   mkdir /tmp/CLOUD-INIT

   cp cloud-init-0.7.9.zip /tmp/CLOUD-INIT

   cd /tmp/CLOUD-INIT

2. Run the following command to decompress the package:

   unzip cloud-init-0.7.9.zip

3. Run the following command to enter the **cloud-init-0.7.9** directory:

   cd cloud-init-0.7.9

4. Install the Cloud-Init package. The commands vary depending on the OS type.
   - For CentOS 6.*x* or SLES 11.*x*, run the following commands:

     python setup.py build

     python setup.py install --init-system sysvinit
   - For CentOS 7.*x*, SLES 12.*x*, or EulerOS 2.8 Arm, run the following commands:

     python setup.py build

     python setup.py install --init-system systemd

   NOTICE

   Add user **syslog** to the **adm** group during the installation. If user **syslog** exists, add it to the **adm** group. For some OSs (such as CentOS and SLES), user **syslog** may not exist. Run the following commands to create user **syslog** and add it to the **adm** group:

   useradd syslog

   groupadd adm

   usermod -g adm syslog

5. Enable Cloud-Init to automatically start upon system boot.
   - If the OS uses SysVinit to manage automatic start of services, run the following commands:

     chkconfig --add cloud-init-local; chkconfig --add cloud-init; chkconfig --add cloud-config; chkconfig --add cloud-final

     chkconfig cloud-init-local on; chkconfig cloud-init on; chkconfig cloud-config on; chkconfig cloud-final on

service cloud-init-local status; service cloud-init status; service cloud-config status; service cloud-final status

– If the OS uses Systemd to manage automatic start of services, run the following commands:

systemctl enable cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service

systemctl status cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service

6. Run the following commands to check whether Cloud-Init has been installed:

cloud-init -v

cloud-init init --local

Cloud-Init is successfully installed if the following information is displayed:

```
cloud-init 0.7.9
```

3.6.2.1.3 Installing Cloud-Init (EulerOS/openEuler)

Scenarios

Cloud-Init is a tool developed to initiate VMs or iMetal servers in a cloud environment. It is used to customize the network configuration, hostname, hosts file, username, and password for a VM or an iMetal server. Cloud-Init is also required if the password of a VM is generated by the system at random.

The Cloud-Init installation file has requirements on Linux versions and can only be installed from the Internet. Therefore, ensure that the server or VM on the original platform can access the Internet.

Description

- The Cloud-Init installation procedures in the following sections are for reference only. You are advised to download the Cloud-Init from the official website. The Cloud-init version is updated on the official website in real time. Install the latest version.
- When you modify the **/etc/cloud/cloud.cfg** file, ensure that the file format (such as alignment and spaces) is consistent with the provided example that conforms to the YAML syntax.

Procedure

1. Take EulerOS 2.2 as an example. Configure the Yum repository of EulerOS 2.2 and edit the **/etc/yum.repos.d/EulerOS-base.repo** file. For example, the configuration is:

```
[EulerOS-base]
name=EulerOS-base
baseurl=https://repo.huaweicloud.com/euler/2.2/os/x86_64/
enabled=1
gpgcheck=1
gpgkey=https://repo.huaweicloud.com/euler/2.2/os/RPM-GPG-KEY-EulerOS
```

Save the configuration.

2. Run the following command to update the yum source:

yum repolist

Run the following command to install Cloud-Init 0.7.6:

yum install cloud-init

Dependent packages of Cloud-Init 0.7.6 will be installed automatically.

```
Installed:
  cloud-init.x86_64 0:0.7.6-2

Dependency Installed:
  PyYAML.x86_64 0:3.10-11                                audit-libs-python.x86_64 0:2.4.1-5
  checkpolicy.x86_64 0:2.1.12-6                          libsemanage-python.x86_64 0:2.1.10-18
  libyaml.x86_64 0:0.1.4-11                              policycoreutils-python.x86_64 0:2.2.5-15.h1
  python-IPy.noarch 0:0.75-6                             python-backports.x86_64 0:1.0-8
  python-backports-ssl_match_hostname.noarch 0:3.4.0.2-4 python-jsonpatch.noarch 0:1.2-2
  python-jsonpointer.noarch 0:1.9-2                      python-prettytable.noarch 0:0.7.2-1
  python-requests.noarch 0:2.6.0-1                       python-six.noarch 0:1.9.0-2
  python-urllib3.noarch 0:1.10.2-2                       setools-libs.x86_64 0:3.3.7-46

Complete!
```

3. To inject the password of user **root**, run the following command to upgrade **selinux-policy** from h1 to h2.

   yum install selinux-policy

4. Run the **cloud-init -v** command. If the command output contains the Cloud-Init version number, the installation is complete.

3.6.2.1.4 Configuring Cloud-Init

After installing Cloud-Init, you need to edit the **cloud.cfg** file to configure Cloud-Init for iMetal server initialization.

Use the vi editor to modify the **/etc/cloud/cloud.cfg** file. The examples are for reference only. You can modify the file as you need.

Cloud-Init 0.7.9 or later is used as an example.

1. Add the following key-value pair with an empty line above and below it:
   ```
   no_ssh_fingerprints: true
   ```
2. Set **ssh_pwauth** to **false** or **0**, indicating that password login in SSH mode is disabled.
   ```
   ssh_pwauth: true
   ```
3. Set **disable_root** to **false**. This parameter specifies whether to allow SSH login of user **root**.
   ```
   disable_root: false
   ```
4. Add **preserve_hostname: false**.
   ```
   preserve_hostname: false
   ```
5. (Optional) Use the number sign (#) to comment out the following statements (skip this step if the statements do not exist):
   ```
   mount_default_fields: [~, ~, 'auto', 'defaults,nofail', '0', '2']
   resize_rootfs_tmp: /dev
   ssh_deletekeys:   0
   ```
6. Modify **ssh_genkeytypes** as follows (add it if it does not exist):
   ```
   ssh_genkeytypes: ['rsa', 'dsa']
   ```
7. Modify **syslog_fix_perms** as follows (add it if it does not exist):
   ```
   syslog_fix_perms: root:root
   ```
8. Add the following statements:
   ```
   network:
     config: disabled
   datasource_list: [ OpenStack ]
   datasource:
    OpenStack:
      metadata_urls: ['http://169.254.169.254/clouddc']
   ```



```
    max_wait: 120
    timeout: 10
    retries: 5
```

9. (Optional) In **/etc/cloud/cloud.cfg**, set **apply_network_config** to **False**.

   This step is only for Cloud-Init 18.3 or later.

```
network:
  config: disabled
datasource_list: [ OpenStack ]
datasource:
 OpenStack:
   metadata_urls: ['http://169.254.169.254/clouddc']
   max_wait: 120
   timeout: 10
   retries: 5
   apply_network_config: False
```

10. Add the following content after **- final-message** in **cloud_final_modules**:

```
- power_state_change
```

11. Modify **system_info** as follows:

```
system_info:
  distro: rhel
  default_user:
    name: root   //Username for OS login
   lock_passwd: False   //True indicates that login using a password is disabled. Note that some OSs use value 1 to disable the password login.
```

    In the preceding command, change the value of **distro** based on the OS, such as **distro: sles**, **distro: rhel**, **distro: ubuntu**, **distro: debian**, and **dustro: fedora**.

12. (Optional) For SLES 12 SP1 and SLES 12 SP2, modify **[Unit]** in the **/usr/lib/systemd/system/cloud-init-local.service** file.

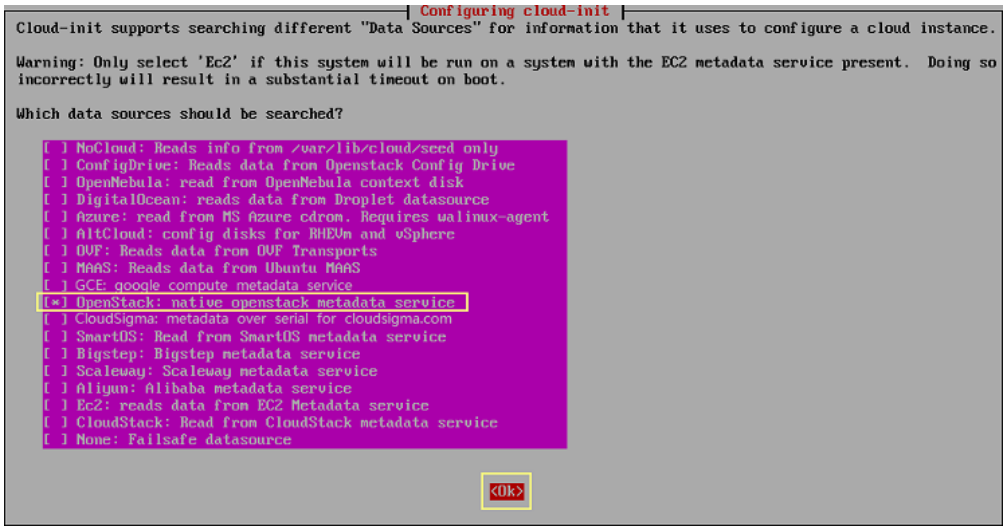
    vi /usr/lib/systemd/system/cloud-init-local.service

    Ensure that **[Unit]** is configured as follows:

```
[Unit]
Description=Initial cloud-init job (pre-networking)
DefaultDependencies=no
Wants=network-pre.target
Wants=local-fs.target
After=local-fs.target
Before=network-pre.target
Before=shutdown.target
Before=basic.target
Conflicts=shutdown.target
# Other distros use Before=sysinit.target. There is not a clearly identified
# reason for usage of basic.target instead.
```

13. (Optional) For Ubuntu 16.04, run the following command to configure the OpenStack source:

    dpkg-reconfigure cloud-init



Run the **vim /etc/cloud/cloud.cfg.d/90_dpkg.cfg** command to open the configuration file and check whether the items are correctly configured in the file.

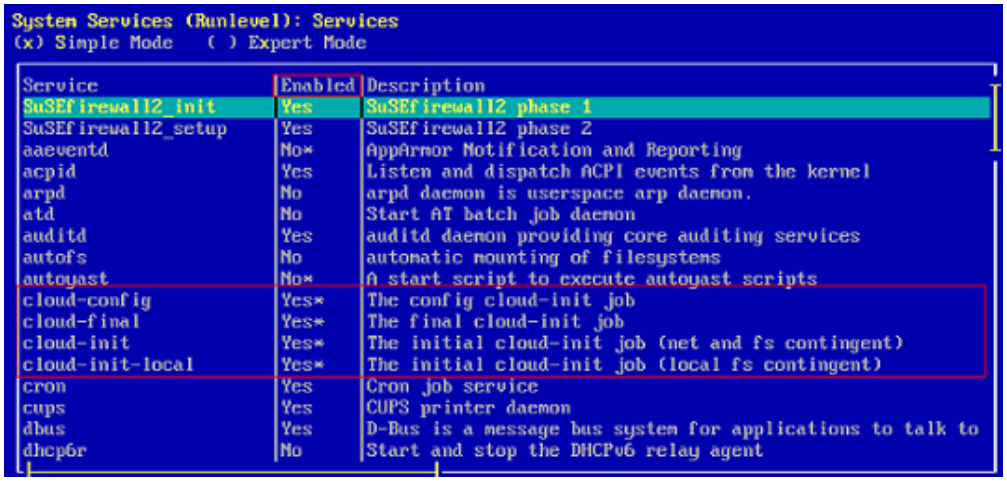
```
# to update this file, run dpkg-reconfigure cloud-init
datasource_list: [ OpenStack ]
~
~
~
```

If the configuration file content is consistent with the preceding command output, the configuration is successful.

3.6.2.1.5 Checking the Cloud-Init Status

SLES 11 SP4

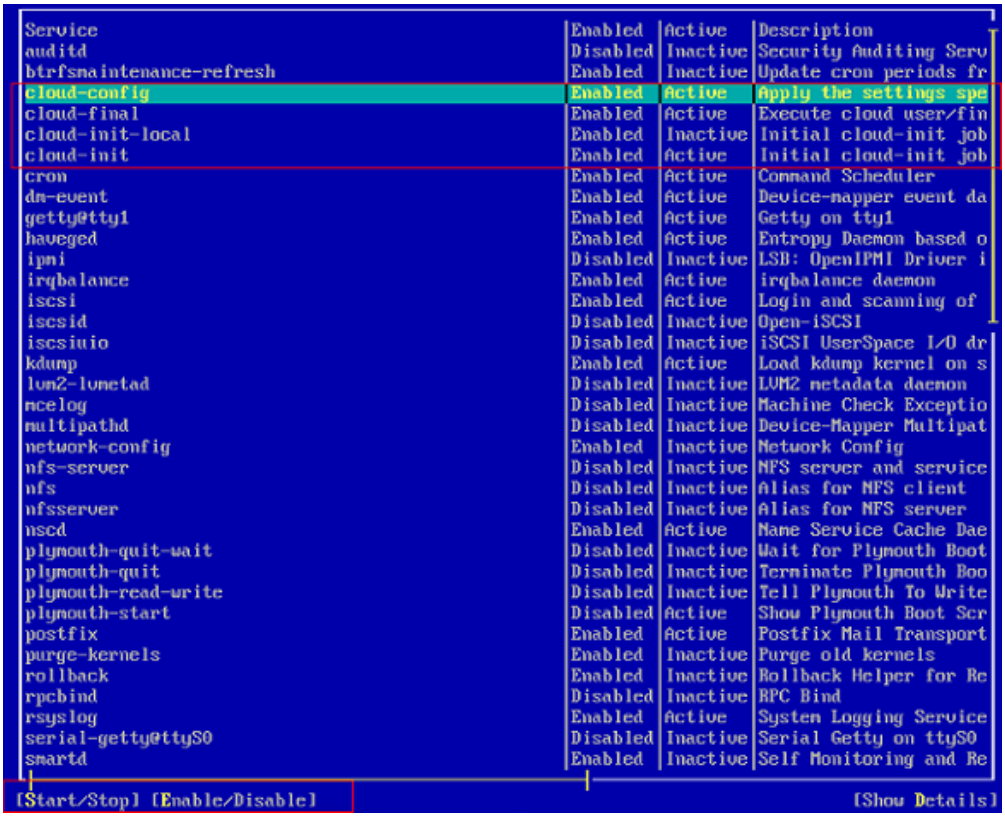
1. Run the **yast** command and select **System**.
2. Press **Tab** and select **System Services (Runlevel)**.
3. Press **Enter**. The following figure indicates that automatic startup has been enabled for the four services of Cloud-Init. If it is not enabled for any service, enable it.



SLES 12 SP1

1. Check whether the Cloud-init services will automatically start when the system starts.

   To query the Cloud-Init status, run the **yast** command and use up and down arrow keys to select **System**. Then, press **Tab** and use up and down arrow keys to select **System Manager**.



2. As shown in the preceding figure, automatic startup has been enabled for the four services of Cloud-Init. **Active** indicates that the service has been started. If automatic startup is not enabled for any service, select the service using up and down arrow keys, press **Tab**, and use the **Enable/Disable** option to enable it.

SLES 12 SP2/SLES 12 SP3/SLES 15/Oracle Linux 7/RHEL 7/CentOS 7/CentOS 8/XenServer 7

1. Check whether the Cloud-init services will automatically start when the system starts.

   systemctl status cloud-init-local

   systemctl status cloud-init

   systemctl status cloud-config

   systemctl status cloud-final

2. **enabled** indicates that the service will automatically start.


```
[root@localhost r74]# service cloud-init-local status
Redirecting to /bin/systemctl status cloud-init-local.service
● cloud-init-local.service - Initial cloud-init job (pre-networking)
   Loaded: loaded (/usr/lib/systemd/system/cloud-init-local.service; enabled; vendor preset: disabled)
   Active: inactive (dead)
[root@localhost r74]# service cloud-init status
Redirecting to /bin/systemctl status cloud-init.service
● cloud-init.service - Initial cloud-init job (metadata service crawler)
   Loaded: loaded (/usr/lib/systemd/system/cloud-init.service; enabled; vendor preset: disabled)
   Active: inactive (dead)
[root@localhost r74]# service cloud-config status
Redirecting to /bin/systemctl status cloud-config.service
● cloud-config.service - Apply the settings specified in cloud-config
   Loaded: loaded (/usr/lib/systemd/system/cloud-config.service; enabled; vendor preset: disabled)
   Active: inactive (dead)
[root@localhost r74]# service cloud-final status
Redirecting to /bin/systemctl status cloud-final.service
● cloud-final.service - Execute cloud user/final scripts
   Loaded: loaded (/usr/lib/systemd/system/cloud-final.service; enabled; vendor preset: disabled)
   Active: inactive (dead)
```

Otherwise, run the following commands to enable automatic startup for them.

systemctl enable cloud-init-local

systemctl enable cloud-init

systemctl enable cloud-config

systemctl enable cloud-final

3. Run the following commands to start Cloud-Init services:

   systemctl start cloud-init-local

   systemctl start cloud-init

   systemctl start cloud-config

   systemctl start cloud-final

4. Run the commands in **1** to check whether the Cloud-Init status is **active**.

```
[root@localhost ~]# systemctl start cloud-init-local
[root@localhost ~]# systemctl start cloud-init
[root@localhost ~]# systemctl start cloud-config
[root@localhost ~]# systemctl start cloud-final
[root@localhost ~]# systemctl status cloud-init-local
● cloud-init-local.service - Initial cloud-init job (pre-networking)
   Loaded: loaded (/usr/lib/systemd/system/cloud-init-local.service; enabled; vendor preset: disabled)
   Active: active (exited) since Tue 2022-10-18 14:15:13 CST; 3min 12s ago
  Process: 15945 ExecStart=/usr/bin/cloud-init init --local (code=exited, status=0/SUCCESS)
 Main PID: 15945 (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/system-hostos.slice/cloud-init-local.service
[root@localhost ~]# systemctl status cloud-init
● cloud-init.service - Initial cloud-init job (metadata service crawler)
   Loaded: loaded (/usr/lib/systemd/system/cloud-init.service; enabled; vendor preset: disabled)
   Active: active (exited) since Tue 2022-10-18 14:15:14 CST; 3min 28s ago
  Process: 15974 ExecStart=/usr/bin/cloud-init init (code=exited, status=0/SUCCESS)
 Main PID: 15974 (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/system-hostos.slice/cloud-init.service
[root@localhost ~]# systemctl status cloud-config
● cloud-config.service - Apply the settings specified in cloud-config
   Loaded: loaded (/usr/lib/systemd/system/cloud-config.service; enabled; vendor preset: disabled)
   Active: active (exited) since Tue 2022-10-18 14:15:14 CST; 3min 36s ago
  Process: 16019 ExecStart=/usr/bin/cloud-init modules --mode=config (code=exited, status=0/SUCCESS)
 Main PID: 16019 (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/system-hostos.slice/cloud-config.service
[root@localhost ~]# systemctl status cloud-final
● cloud-final.service - Execute cloud user/final scripts
   Loaded: loaded (/usr/lib/systemd/system/cloud-final.service; enabled; vendor preset: disabled)
   Active: active (exited) since Tue 2022-10-18 14:15:14 CST; 3min 53s ago
  Process: 16025 ExecStart=/usr/bin/cloud-init modules --mode=final (code=exited, status=0/SUCCESS)
 Main PID: 16025 (code=exited, status=0/SUCCESS)
```

EulerOS/OpenEuler

1. Check whether the Cloud-init services will automatically start when the system starts.

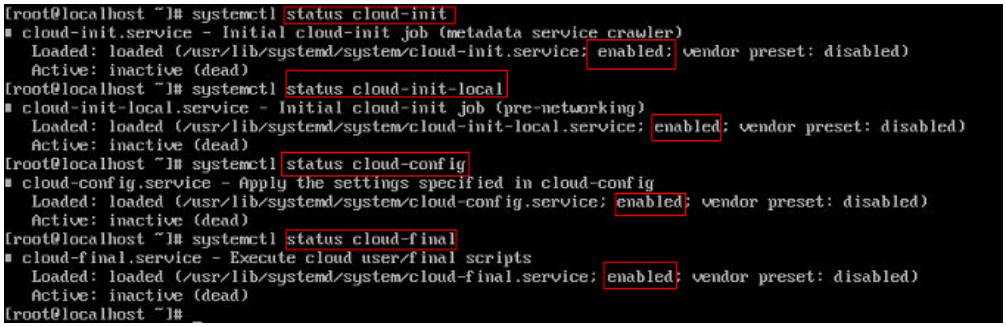
   systemctl status cloud-init-local

   systemctl status cloud-init

systemctl status cloud-config

systemctl status cloud-final

2. **enabled** indicates that the service will automatically start.



Otherwise, run the following commands to enable automatic startup for them.

systemctl enable cloud-init-local

systemctl enable cloud-init

systemctl enable cloud-config

systemctl enable cloud-final

3. Run the following commands to start Cloud-Init services:

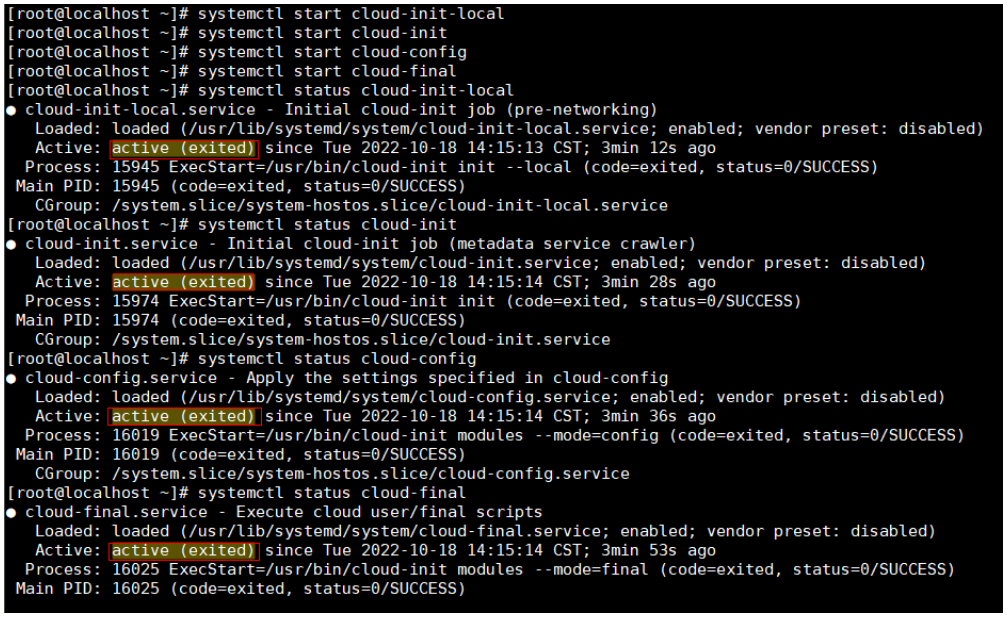
systemctl start cloud-init-local

systemctl start cloud-init

systemctl start cloud-config

systemctl start cloud-final

4. Run the commands in **1** to check whether the Cloud-Init status is **active**.

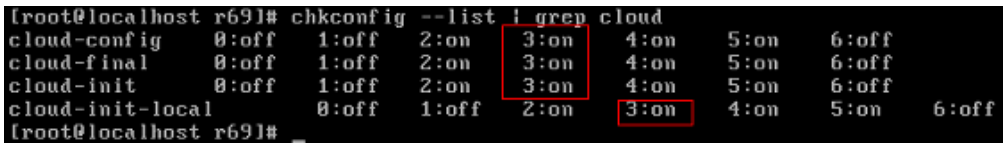


RHEL 6/CentOS 6/Oracle Linux 6

1. Run the following command:

chkconfig --list | grep cloud

As shown in the following figure, **on** indicates that automatic startup has been enabled for the service.



2. If automatic startup is not enabled for Cloud-Init services, run the following commands to enable it:

   chkconfig cloud-init on

   chkconfig cloud-init-local on

   chkconfig cloud-config on

   chkconfig cloud-final on

Ubuntu 16.04/Ubuntu 18.04

1. Run the following commands:

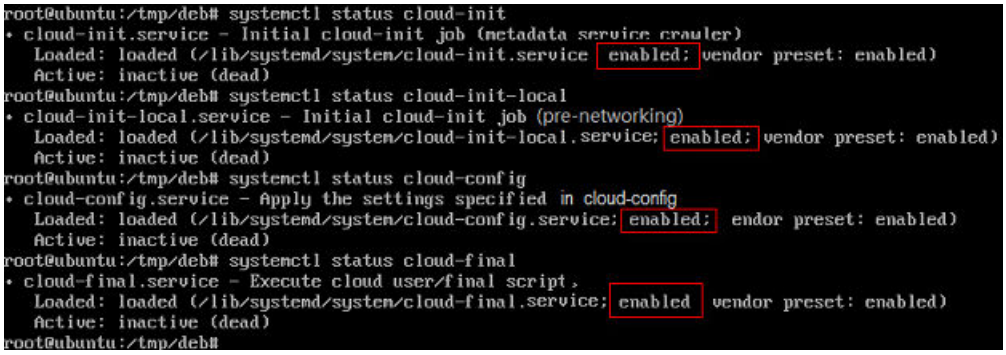
   systemctl status cloud-init

   systemctl status cloud-init-local

   systemctl status cloud-config

   systemctl status cloud-final

   As shown in the following figure, **enable** indicates that automatic startup has been enabled for the service.



2. If automatic startup is not enabled for Cloud-Init services, run the following commands to enable it:

   systemctl enable cloud-init

   systemctl enable cloud-init-local

   systemctl enable cloud-config

   systemctl enable cloud-final

3. Run the following commands to start Cloud-Init services:

   systemctl start cloud-init-local

   systemctl start cloud-init

   systemctl start cloud-config

   systemctl start cloud-final

4. Run the commands in **1** to check whether the Cloud-Init status is **active**.


```
[root@localhost ~]# systemctl start cloud-init-local
[root@localhost ~]# systemctl start cloud-init
[root@localhost ~]# systemctl start cloud-config
[root@localhost ~]# systemctl start cloud-final
[root@localhost ~]# systemctl status cloud-init-local
● cloud-init-local.service - Initial cloud-init job (pre-networking)
   Loaded: loaded (/usr/lib/systemd/system/cloud-init-local.service; enabled; vendor preset: disabled)
   Active: active (exited) since Tue 2022-10-18 14:15:13 CST; 3min 12s ago
  Process: 15945 ExecStart=/usr/bin/cloud-init init --local (code=exited, status=0/SUCCESS)
 Main PID: 15945 (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/system-hostos.slice/cloud-init-local.service
[root@localhost ~]# systemctl status cloud-init
● cloud-init.service - Initial cloud-init job (metadata service crawler)
   Loaded: loaded (/usr/lib/systemd/system/cloud-init.service; enabled; vendor preset: disabled)
   Active: active (exited) since Tue 2022-10-18 14:15:14 CST; 3min 28s ago
  Process: 15974 ExecStart=/usr/bin/cloud-init init (code=exited, status=0/SUCCESS)
 Main PID: 15974 (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/system-hostos.slice/cloud-init.service
[root@localhost ~]# systemctl status cloud-config
● cloud-config.service - Apply the settings specified in cloud-config
   Loaded: loaded (/usr/lib/systemd/system/cloud-config.service; enabled; vendor preset: disabled)
   Active: active (exited) since Tue 2022-10-18 14:15:14 CST; 3min 36s ago
  Process: 16019 ExecStart=/usr/bin/cloud-init modules --mode=config (code=exited, status=0/SUCCESS)
 Main PID: 16019 (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/system-hostos.slice/cloud-config.service
[root@localhost ~]# systemctl status cloud-final
● cloud-final.service - Execute cloud user/final scripts
   Loaded: loaded (/usr/lib/systemd/system/cloud-final.service; enabled; vendor preset: disabled)
   Active: active (exited) since Tue 2022-10-18 14:15:14 CST; 3min 53s ago
  Process: 16025 ExecStart=/usr/bin/cloud-init modules --mode=final (code=exited, status=0/SUCCESS)
 Main PID: 16025 (code=exited, status=0/SUCCESS)
```

Ubuntu 14.04

Run the following commands:

initctl status cloud-init

initctl status cloud-init-local

initctl status cloud-config

initctl status cloud-final

If Cloud-Init installation information is displayed, the installation is successful.

```
[root@ubuntu:~]# initctl status cloud-init
cloud-init stop/waiting
[root@ubuntu:~]# initctl status cloud-init-local
cloud-init-local stop/waiting
[root@ubuntu:~]# initctl status cloud-config
cloud-config stop/waiting
[root@ubuntu:~]# initctl status cloud-final
cloud-final stop/waiting
```

3.6.2.1.6 Installing bms-network-config

Scenarios

Install **bms-network-config** and use it with Cloud-Init to configure the network for iMetal servers.

Prerequisites

- You have logged in to the VM.
- Cloud-Init has been installed on the VM.
- You have downloaded the bms-network-config software package and SHA-256 verification code and verified the package integrity by referring to **Process for Preparing an External Image File**. For details, see **How Do I Verify Software Package Integrity?**

> **NOTE**
>
> Download the RPM package depending on the OS. Ubuntu and Debian use the .deb package, and CentOS and EulerOS (Arm) use the **aarch.rpm** package.

Procedure

1. Enter the directory where the bms-network-config software package is stored and run the **rpm -ivh** *bms-network-config-1.0-7.centosRedhat7.x86_64.rpm* command.

```
[root@localhost r74]# rpm -ivhbms-network-config-1.0-7.centosRedhat7.x86_64.rpm
Preparing...                          ################################# [100%]
Updating / installing...
   1:bms-network-config-1.0.7.centosRe################################# [100%]
```

> **NOTE**
>
> If the error shown in the following figure is displayed when you install bms-network-config for SLES 12/SLES 15, run the **rpm -ivh bms-network-config-1.0-9.suse12.x86_64.rpm --nodeps --force** command.

```
linux-dyqy:/home/bms-network-config_1.0.9 # rpm -ivh bms-network-config-1.0-9.suse12.x86_64.rpm
error: Failed dependencies:
        cloud-init is needed by bms-network-config-1.0-9.suse12.x86_64
linux-dyqy:/home/bms-network-config_1.0.9 #
```

   For Ubuntu/Debian, run the **dpkg -i***xxx* command (*xxx* indicates the .deb package name).

```
root@ubuntu:~/file# dpkg -i bms-network-config-1.0.7.ubuntu1604-918.deb
Selecting previously unselected package bms-network-config.
(Reading database ... 97630 files and directories currently installed.)
Preparing to unpack bms-network-config-1.0.7.ubuntu1604-918.deb ...
Unpacking bms-network-config (1.0) ...
Setting up bms-network-config (1.0) ...
root@ubuntu:~/file# dpkg -s bms-network-config
```

> **NOTE**
>
> The names of the .rpm and .deb packages vary according to the actual situation.

2. After the installation is complete, run the **rpm -qa | grep bms-network-config** command. The installation is successful if the following information is displayed:

```
[root@localhost r74]# rpm -qa | grep bms
bms-network-config-1.0.7.centosRedhat7.x86_64
```

   For Ubuntu/Debian, run the **dpkg -s bms-network-config** command.

3. Check the bms-network-config status.
   - For Oracle Linux 7, RHEL 7, CentOS 7, Ubuntu 16.04, Ubuntu 18.04, SLES 12, SLES 15, or EulerOS, run the **service bms-network-config status** command to check the service status. If the status is not **enabled**, run the **systemctl enable bms-network-config** command to enable the service.

```
[root@localhost r74]# service bms-network-config status
Redirecting to /bin/systemctl status bms-network-config.service
  bms-network-config.service - Network Config
  Loaded: loaded (/usr/lib/systemd/system/bms-network-config service; enabled vendor preset:
disabled)
  Active: inactive (dead)
```

   - For RHEL 6, CentOS 6, SLES 11 SP4, Oracle Linux 6.8, or Oracle Linux 6.9, run the **chkconfig --list | grep bms-network-config** command to check the service status. If the status is not **on**, run the **chkconfig bms-network-config on** command to enable the service.


```
[root@localhost r69]# chkconfig --list | grep bms
bms-network-config   0:off   1:off   2:on   3:on   4:off   5:on   6:off
```

– For Ubuntu 14.04/Debian, run the **initctl status bms-network_config** command to check the service status.

```
root@ubuntu:~# initctl status bms-network_config
bms-network_config stop/waiting
```

4. Check the startup dependencies between bms-network-config and other services.

   Run the **systemctl cat bms-network-config** command to check the configuration file and ensure that the file content is as follows:

```
[Unit]
Description=NetworkConfig
DefaultDependencies=no
After=dbus.service
Wants=dbus.service

[Service]
Type=oneshot
ExecStart=/usr/bin/bms-network_config rhel
RemainAfterExit=yes
TimeoutSec=0

[Install]
WantedBy=multi-user.target
```

   If the startup sequence is incorrect, use the **vim /usr/lib/systemd/system/bms-network-config.service** command to correct it.

3.6.2.1.7 Installing the Network Service

Scenarios

By default, the network service is not installed for CentOS 8, EulerOS 2.9, RHEL 8, Ubuntu 20, or later. For iMetal servers using centralized gateways, the network service and network scripts are required to configure the network. For iMetal servers using distributed gateways (that is, iMetal servers with SDI 3.0 or SDI 2.2 cards), skip this section.

Procedure

EulerOS 2.10 is used as an example.

1. Log in to the VM and query the network status.

   systemctl status network

```
Unit network.service could not be found.
```

2. Run the following command to install network-scripts using the Yum source:

   yum install network-scripts

3. After the installation is complete, run the following commands to check whether the network service is available:

   systemctl status network

```
● network.service - LSB: Bring up/down networking
Loaded: loaded (/etc/rc.d/init.d/network; generated)
Active: inactive (dead)
Docs: man:systemd-sysv-generator(8)
```


3.6.2.1.8 Deleting Files

Deleting Uploaded Files

Delete files uploaded to the VM, such as the .rpm packages of bms-network-config and SDI drivers.

Deleting Temporary Files

1. Run the following commands to delete user login records:

   echo > /var/log/wtmp

   echo > /var/log/btmp

2. Run the following commands to delete temporary files:

   rm -rf /var/log/cloud-init*

   rm -rf /var/lib/cloud/*

   rm -rf /var/log/network-config.log

   rm -rf /opt/huawei/network_config/network_config.json

3. Delete residual configurations.
   - SLES

     Check for the files whose names start with **ifcfg** in the **/etc/sysconfig/network-scripts/** folder and delete them except **ifcfg-lo** and **ifcfg.template**.

     - Run the following command to view files:

       ll /etc/sysconfig/network/

     - Run the following command to delete files:

       rm -rf /etc/sysconfig/network/ifcfg*xxx*

   - RHEL, CentOS, Oracle, or EulerOS

     Check for the files whose names start with **ifcfg** in the **/etc/sysconfig/network-scripts/** folder and delete them except **ifcfg-lo** and **ifcfg**.

     - Run the following command to view files:

       ll /etc/sysconfig/network-scripts/

     - Run the following command to delete files:

       rm -rf /etc/sysconfig/network-scripts/ifcfg*xxx*

   - Ubuntu

     rm -rf /etc/network/interfaces.d/50-cloud-init.cfg

4. Run the following command to delete operation records:

   history -w;echo > /root/.bash_history;history -c;history -c;history -c;

3.6.2.2 Uploading an Image File to an OBS Bucket

Constraints

- Only an unencrypted image file or an image file encrypted using SSE-KMS can be uploaded to an OBS bucket.

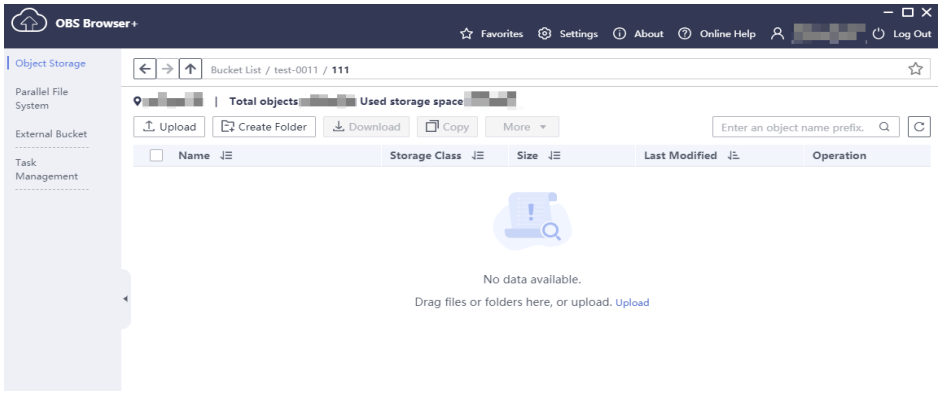
- When uploading an image file, you must select an OBS bucket with the storage class of Standard.

Procedure

Use OBS Browser+ to upload the image file. For details, see **OBS Browser+ Best Practices**.

For how to download OBS Browser+, see **Downloading OBS Browser+**.

Figure 3-21 Uploading an image file



3.6.2.3 Registering an Image File as a Private Image for iMetal Servers

1. Log in to the management console, click **Service List**, and choose **Compute** > **Image Management Service**.
2. Click **Create Image** in the upper right corner.
3. In the **Image Type and Source** area, set parameters as prompted.
   - **Region**: Set it to the region where your iMetal servers will be created.
   - **Type**: Select **Import Image**.
   - **Image Type**: Select **System disk image**.
   - **Select Image File**: Select the image file that has been uploaded to an OBS bucket in **Uploading an Image File to an OBS Bucket**.

     You can enter a bucket name in the search box in the upper right corner of the list to search for the bucket.
4. In the **Image Information** area, set parameters as prompted.

Table 3-9 Parameter description

Parameter	Example Value	Description
Function	BMS system disk image	Select **BMS system disk image**.
Architecture	x86	Currently, only the x86 architecture is supported. Select **x86**.

Parameter	Example Value	Description
Boot Mode	BIOS	This parameter is optional. The value can be **BIOS** or **UEFI**. For details about the differences between the two boot modes, see **How Is BIOS Different from UEFI?** For details about which OSs support UEFI boot, see **OSs Supporting UEFI Boot Mode**. The boot mode must be the same as that in the image file. You need to confirm which boot mode is used in the image file. After you select the right boot mode, the boot mode will be configured for the image at the background. Select a correct boot mode. Otherwise, the servers created from the image cannot be started.
OS	Ubuntu 20.04 server 64bit	To ensure that the image can be created and used properly, select an OS consistent with that in the image file. If you do not select an OS, the system attempts to automatically identify the OS in the image file. **NOTE** • If the system identifies that the OS in the image file is different from the one you select here, the identified OS prevails. • If the system fails to identify an OS, the OS you select will be used. • If the OS you selected or identified by the system is inconsistent with the actual one, servers created from the image file may be affected.
System Disk (GiB)	40	System disk capacity (value range: 40 GiB to 1024 GiB). Ensure that this value is not less than the system disk capacity in the image file. **NOTE** If you fail to upload a VHD image converted using qemu-img or other similar tools, see **Why Did My VHD Upload Fail? Why Does the System Say the System Disk in the VHD Image File Is Larger Than What I Specified on the Management Console?**

Parameter	Example Value	Description
Data Disk	Not added	You can also add data disks to the image. You need to obtain an image file containing data disks in advance. This function is used to migrate VMs and data disks from other platforms to the current platform. To add a data disk, click  , configure the data disk capacity, and click **Select Image File**. In the displayed dialog box, select a bucket and then an image file containing the data disk. A maximum of three data disks can be added.
Name	UbuntuImage	Set a name for the image.
Encryption	Not selected	(Optional) If you want to encrypt the image, select **KMS encryption** and select a key from the drop-down list. After you select **KMS encryption**, the system will create a default key **ims/default** for you. You can also select a key from the key list. For details about how to encrypt an image, see **Creating Encrypted Images**. **NOTE** If the encrypted image needs to be shared with other tenants, use a custom key to encrypt it. Otherwise, the key cannot be authorized to other tenants, causing a sharing failure.
Enterprise Project	default	Select an enterprise project from the drop-down list. This parameter is available only if you have enabled enterprise projects or your account is an enterprise account. An enterprise project can be used to centrally manage cloud resources and members by project.

Parameter	Example Value	Description
Tag	Tag key: usage Tag value: project	(Optional) Set a tag key and a tag value for the image to make identification and management of your images easier. You are advised to create predefined tags in TMS. For details, see **Creating Predefined Tags** . **NOTE** If your organization has configured tag policies for images, you need to add tags to your images based on the policies. If you add a tag that does not comply with the tag policies, images may fail to be created. Contact the organization administrator to learn more about the tag policies. • Each tag consists of a key and a value. A key contains a maximum of 36 characters, and a value contains a maximum of 43 characters. The key cannot be left blank or an empty character string. The value cannot be left blank but can be an empty character string. • An image can have a maximum of 10 tags.
Description	imageTest	(Optional) Describe the image.

5. Read and agree to the image disclaimer. Click **Next**.
6. Confirm the parameter settings and click **Submit**.
7. Go back to the private image list. When the image status changes to **Normal**, the image is created successfully.

3.6.3 Scenario 2: External Image File Exported from the Original Server or VM

3.6.3.1 Uploading an Image File to an OBS Bucket

Constraints

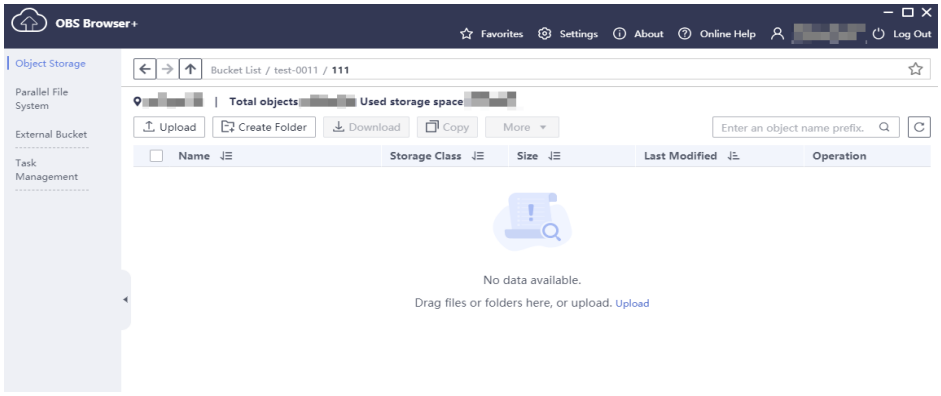
- Only an unencrypted image file or an image file encrypted using SSE-KMS can be uploaded to an OBS bucket.
- When uploading an image file, you must select an OBS bucket with the storage class of Standard.

Procedure

Use OBS Browser+ to upload the image file. For details, see **OBS Browser+ Best Practices**.

For how to download OBS Browser+, see **Downloading OBS Browser+**.

Figure 3-22 Uploading an image file



3.6.3.2 Registering an Image File as an ECS Private Image

1. Log in to the management console, click **Service List**, and choose **Compute** > **Image Management Service**.
2. Click **Create Image** in the upper right corner.
3. In the **Image Type and Source** area, set parameters as prompted.
   - **Region**: Set it to the region where your iMetal servers will be created.
   - **Type**: Select **Import Image**.
   - **Image Type**: Select **System disk image**.
   - **Select Image File**: Select the image file that has been uploaded to an OBS bucket in **Uploading an Image File to an OBS Bucket**.

     You can enter a bucket name in the search box in the upper right corner of the list to search for the bucket.
4. In the **Image Information** area, set parameters as prompted.

Table 3-10 Parameter description

Parameter	Example Value	Description
Enable automatic configuration	Selected	If you select this option, the system will automatically check and optimize the image file. For details, see **What Will the System Do to an Image File When I Use the File to Register a Private Image?**
Function	ECS system disk image	Select **ECS system disk image**.
Architecture	x86	Currently, only the x86 architecture is supported. Select **x86**.

Parameter	Example Value	Description
Boot Mode	BIOS	This parameter is optional. The value can be **BIOS** or **UEFI**. For details about the differences between the two boot modes, see **How Is BIOS Different from UEFI?** For details about which OSs support UEFI boot, see **OSs Supporting UEFI Boot Mode**. The boot mode must be the same as that in the image file. You need to confirm which boot mode is used in the image file. After you select the right boot mode, the boot mode will be configured for the image at the background. Select a correct boot mode. Otherwise, the iMetal servers created from the image cannot be started.
OS	Ubuntu 20.04 server 64bit	To ensure that the image can be created and used properly, select an OS consistent with that in the image file. If you do not select an OS, the system attempts to automatically identify the OS in the image file. **NOTE** • If the system identifies that the OS in the image file is different from the one you select here, the identified OS prevails. • If the system fails to identify an OS, the OS you select will be used. • If the OS you selected or identified by the system is inconsistent with the actual one, ECSs created from the image file may be affected.
System Disk (GiB)	40	System disk capacity (value range: 40 GiB to 1024 GiB). Ensure that this value is not less than the system disk capacity in the image file. **NOTE** If you fail to upload a VHD image converted using qemu-img or other similar tools, see **Why Did My VHD Upload Fail? Why Does the System Say the System Disk in the VHD Image File Is Larger Than What I Specified on the Management Console?**

Parameter	Example Value	Description
Data Disk	Not added	You can also add data disks to the image. You need to obtain an image file containing data disks in advance. This function is used to migrate VMs and data disks from other platforms to the current platform. To add a data disk, click  , configure the data disk capacity, and click **Select Image File**. In the displayed dialog box, select a bucket and then an image file containing the data disk. A maximum of three data disks can be added.
Name	UbuntuImage	Set a name for the image.
Encryption	Not selected	(Optional) If you want to encrypt the image, select **KMS encryption** and select a key from the drop-down list. After you select **KMS encryption**, the system will create a default key **ims/default** for you. You can also select a key from the key list. For details about how to encrypt an image, see **Creating Encrypted Images**. **NOTE** If the encrypted image needs to be shared with other tenants, use a custom key to encrypt it. Otherwise, the key cannot be authorized to other tenants, causing a sharing failure.
Enterprise Project	default	Select an enterprise project from the drop-down list. This parameter is available only if you have enabled enterprise projects or your account is an enterprise account. An enterprise project can be used to centrally manage cloud resources and members by project.

Parameter	Example Value	Description
Tag	Tag key: usage Tag value: project	(Optional) Set a tag key and a tag value for the image to make identification and management of your images easier. You are advised to create predefined tags in TMS. For details, see **Creating Predefined Tags** . **NOTE** If your organization has configured tag policies for images, you need to add tags to your images based on the policies. If you add a tag that does not comply with the tag policies, images may fail to be created. Contact the organization administrator to learn more about the tag policies. • Each tag consists of a key and a value. A key contains a maximum of 36 characters, and a value contains a maximum of 43 characters. The key cannot be left blank or an empty character string. The value cannot be left blank but can be an empty character string. • An image can have a maximum of 10 tags.
Description	imageTest	(Optional) Describe the image.

5. Read and agree to the image disclaimer. Click **Next**.
6. Confirm the parameter settings and click **Submit**.
7. Go back to the private image list. When the image status changes to **Normal**, the image is created successfully.

3.6.3.3 Creating and Configuring an ECS

1. In the private image list, locate the system disk image registered in **Registering an Image File as an ECS Private Image**, and click **Apply for Server** in the **Operation** column of the image.

2. For details about the parameters for creating an ECS, see **Purchasing an ECS in Custom Config Mode**.
3. Log in to the ECS and complete related configurations by referring to **Preparing an Image File**.

3.6.3.4 Creating a System Disk Image from an ECS

Constraints

The system disk capacity of the ECS used to create this system disk image must be no greater than 1 TB.

Prerequisites

The ECS from which this system disk image is created must meet the following requirements:

- Sensitive data has been deleted from the ECS to prevent data leaks.
- The ECS is running or stopped.

Procedure

Step 1 Access the IMS console.

1. Log in to the management console.
2. Under **Compute**, click **Image Management Service**.

   The IMS console is displayed.

Step 2 Register an external image file as a private image.

1. Click **Create Image** in the upper right corner.
2. Set image parameters.

   Table 3-11 and **Table 3-12** list the parameters in the **Image Type and Source** and **Image Information** areas, respectively.

Table 3-11 Image type and source

Parameter	Description
Type	Select **Create Image**.
Region	Select a region close to your business.
Type	Select **System disk image**.
Source	Select **ECS** and select the ECS created in **Creating and Configuring an ECS** from the list.

Table 3-12 Parameter description

Parameter	Description
Encryption	Specifies whether the image will be encrypted. The value is provided by the system and cannot be changed.
Name	Set a name for the image.
Enterprise Project	Select an enterprise project from the drop-down list. This parameter is available only if you have enabled enterprise projects or your account is an enterprise account. To enable this function, contact your customer manager. An enterprise project can be used to centrally manage cloud resources and members by project.

Parameter	Description
Tag	(Optional) Set a tag key and a tag value for the image to make identification and management of your images easier. You are advised to create predefined tags in TMS. For details, see **Creating Predefined Tags**. **NOTE** If your organization has configured tag policies for images, you need to add tags to your images based on the policies. If you add a tag that does not comply with the tag policies, images may fail to be created. Contact the organization administrator to learn more about the tag policies. – Each tag consists of a key and a value. A key contains a maximum of 36 characters, and a value contains a maximum of 43 characters. The key cannot be left blank or an empty character string. The value cannot be left blank but can be an empty character string. – An image can have a maximum of 10 tags.
Description	(Optional) Describe the image.

3. Read and select the check box, and click **Next**.
4. Confirm the parameter settings and click **Submit**.
5. Confirm the parameters and click **Submit Application**.

Step 3 Go back to the **Private Images** page and view the new system disk image.

The time required for creating an image depends on the system disk size, network status, and number of concurrent tasks. When the image status changes to **Normal**, the image is created successfully.

NOTE

- Do not perform any operations on the selected resources or its associated resources during image creation.
- An ECS created from an encrypted image is also encrypted. The key used for encrypting the ECS is the same as that used for encrypting the image.
- An image created from an encrypted ECS is also encrypted. The key used for encrypting the image is the same as that used for encrypting the ECS.

----End

3.6.3.5 Exporting a System Disk Image in ZVHD2 Format to an OBS Bucket

Export the system disk image created in **Creating a System Disk Image from an ECS** to an OBS bucket.

The exported file is in ZVHD2 format.

For details, see **Exporting an Image**.

3.6.3.6 Registering an Image File as a Private Image for iMetal Servers

1. Log in to the management console, click **Service List**, and choose **Compute** > **Image Management Service**.

2. Click **Create Image** in the upper right corner.
3. In the **Image Type and Source** area, set parameters as prompted.
   - **Region**: Set it to the region where your iMetal servers will be created.
   - **Type**: Select **Import Image**.
   - **Image Type**: Select **System disk image**.
   - **Select Image File**: Select the image file that has been uploaded to an OBS bucket in **Uploading an Image File to an OBS Bucket**.

     You can enter a bucket name in the search box in the upper right corner of the list to search for the bucket.
4. In the **Image Information** area, set parameters as prompted.

Table 3-13 Parameter description

Parameter	Example Value	Description
Function	BMS system disk image	Select **BMS system disk image**.
Architecture	x86	Currently, only the x86 architecture is supported. Select **x86**.
Boot Mode	BIOS	This parameter is optional. The value can be **BIOS** or **UEFI**. For details about the differences between the two boot modes, see **How Is BIOS Different from UEFI?** For details about which OSs support UEFI boot, see **OSs Supporting UEFI Boot Mode**. The boot mode must be the same as that in the image file. You need to confirm which boot mode is used in the image file. After you select the right boot mode, the boot mode will be configured for the image at the background. Select a correct boot mode. Otherwise, the servers created from the image cannot be started.

Parameter	Example Value	Description
OS	Ubuntu 20.04 server 64bit	To ensure that the image can be created and used properly, select an OS consistent with that in the image file. If you do not select an OS, the system attempts to automatically identify the OS in the image file. **NOTE** • If the system identifies that the OS in the image file is different from the one you select here, the identified OS prevails. • If the system fails to identify an OS, the OS you select will be used. • If the OS you selected or identified by the system is inconsistent with the actual one, servers created from the image file may be affected.
System Disk (GiB)	40	System disk capacity (value range: 40 GiB to 1024 GiB). Ensure that this value is not less than the system disk capacity in the image file. **NOTE** If you fail to upload a VHD image converted using qemu-img or other similar tools, see **Why Did My VHD Upload Fail? Why Does the System Say the System Disk in the VHD Image File Is Larger Than What I Specified on the Management Console?**
Data Disk	Not added	You can also add data disks to the image. You need to obtain an image file containing data disks in advance. This function is used to migrate VMs and data disks from other platforms to the current platform. To add a data disk, click ⊕, configure the data disk capacity, and click **Select Image File**. In the displayed dialog box, select a bucket and then an image file containing the data disk. A maximum of three data disks can be added.
Name	UbuntuImage	Set a name for the image.

Parameter	Example Value	Description
Encryption	Not selected	(Optional) If you want to encrypt the image, select **KMS encryption** and select a key from the drop-down list. After you select **KMS encryption**, the system will create a default key **ims/default** for you. You can also select a key from the key list. For details about how to encrypt an image, see **Creating Encrypted Images**. **NOTE** If the encrypted image needs to be shared with other tenants, use a custom key to encrypt it. Otherwise, the key cannot be authorized to other tenants, causing a sharing failure.
Enterprise Project	default	Select an enterprise project from the drop-down list. This parameter is available only if you have enabled enterprise projects or your account is an enterprise account. An enterprise project can be used to centrally manage cloud resources and members by project.
Tag	Tag key: usage Tag value: project	(Optional) Set a tag key and a tag value for the image to make identification and management of your images easier. You are advised to create predefined tags in TMS. For details, see **Creating Predefined Tags** . **NOTE** If your organization has configured tag policies for images, you need to add tags to your images based on the policies. If you add a tag that does not comply with the tag policies, images may fail to be created. Contact the organization administrator to learn more about the tag policies. • Each tag consists of a key and a value. A key contains a maximum of 36 characters, and a value contains a maximum of 43 characters. The key cannot be left blank or an empty character string. The value cannot be left blank but can be an empty character string. • An image can have a maximum of 10 tags.
Description	imageTest	(Optional) Describe the image.

5. Read and agree to the image disclaimer. Click **Next**.
6. Confirm the parameter settings and click **Submit**.
7. Go back to the private image list. When the image status changes to **Normal**, the image is created successfully.

3.7 Monitoring an iMetal Server

3.7.1 iMetal Server Monitoring Overview

Monitoring plays an important role for ensuring iMetal server performance, reliability, and availability. Using monitored data, you can understand the iMetal resource usage.

To better understand the operating status of an iMetal server, you can obtain the hardware information and fault information of the iMetal server through the BMC interface. This helps you detect hardware faults timely and better understand the performance metrics of the iMetal server.

iMetal servers only support the out-of-band monitoring mode.

3.7.2 iMetal Metrics

This section describes out-of-band monitoring metrics of iMetal servers.

iMetal Server Hardware Monitoring Metrics

Table 3-14 iMetal server hardware monitoring metrics

Metric Name	Metric	Description
Input Power	power_input_watts	Input power of the power supply
Output Power	power_output_watts	Output power of the power supply
Component Temperature	device_temperature	Temperature of the component
Server Health	host_health	The health of the server
CPU Health	cpu_health	The health of the CPU
Memory Health	memory_health	The health of the memory
Disk Health	disk_health	The health of the disk
Power Supply Health	power_health	The health of the power supply
Network Interface Health	nic_health	The health of the network interface
Fan Health	fan_health	The health of the fan

iMetal Server Alarm Trend Metrics

Table 3-15 iMetal server alarm trend metrics

Metric	Description
host	Collects the number of alarms generated for the entire system at a specified time. The value is the same as the number of alarms whose dimension is **host_health**.
type_cpu	Collects the number of alarms generated for a processor at a specified time. The value is the same as the number of alarms whose dimension is **cpu_health**.
type_memory	Collects the number of alarms generated for the memory at a specified time. The value is the same as the number of alarms whose dimension is **memory_health**.
type_disk	Collects the number of alarms generated for the disks at a specified time. The value is the same as the number of alarms whose dimension is **disk_health**.
type_power	Collects the number of alarms generated for the power supply at a specified time. The value is the same as the number of alarms whose dimension is **power_health**.
type_fan	Collects the number of alarms generated for the fans at a specified time. The value is the same as the number of alarms whose dimension is **fan_health**.
type_nic	Collects the number of alarms generated for the network interfaces at a specified time. The value is the same as the number of alarms whose dimension is **nic_health**.
level_critical	Collects the number of critical alarms generated at a specified time. The value is the same as the number of critical alarms in the alarms.
level_major	Collects the number of major alarms generated at a specified time. The value is the same as the number of major alarms in the alarms.

iRack Monitoring Metrics

Table 3-16 iRack monitoring metrics

Metric	Description
rack_power	Indicates the power of a rack.
rack_temp	Indicates the temperature of a rack.

3.7.3 Creating an Alarm Rule for an iMetal Server

Scenarios

You can set alarm rules for iMetal servers to customize the monitored objects and notification policies. Then, you can monitor your iMetal servers more carefully and get notifications in case of any failure.

An alarm rule includes the alarm rule name, monitored object, metric, threshold, monitoring interval, and whether to send notifications.

This section describes how to create an alarm rule for an iMetal server.

Prerequisites

To set alarm rules, you must be granted the CES FullAccess permissions. If a message appears indicating that you have insufficient permissions, contact the administrator to obtain permissions. For details, see **Permissions**.

Procedure

1. Log in to the management console.
2. Under **Management & Governance**, choose **Cloud Eye**.
3. In the navigation pane, choose **Alarm Management** > **Alarm Rules**.
4. On the displayed **Alarm Rules** page, click **Create Alarm Rule**.
5. On the **Create Alarm Rule** page, configure parameters as needed.

   The key parameters are as follows. For details, see **Creating an Alarm Rule**.

   - **Name**: Enter a name for the alarm rule. If you do not enter a name, the system generates a random one and you can modify it.
   - **Alarm Type**: Select **Metric**.
   - **Resource Type**: Select **CloudDC.iMetal**.
   - **Dimension**: Select **device,host**.

Table 3-17 Dimension values

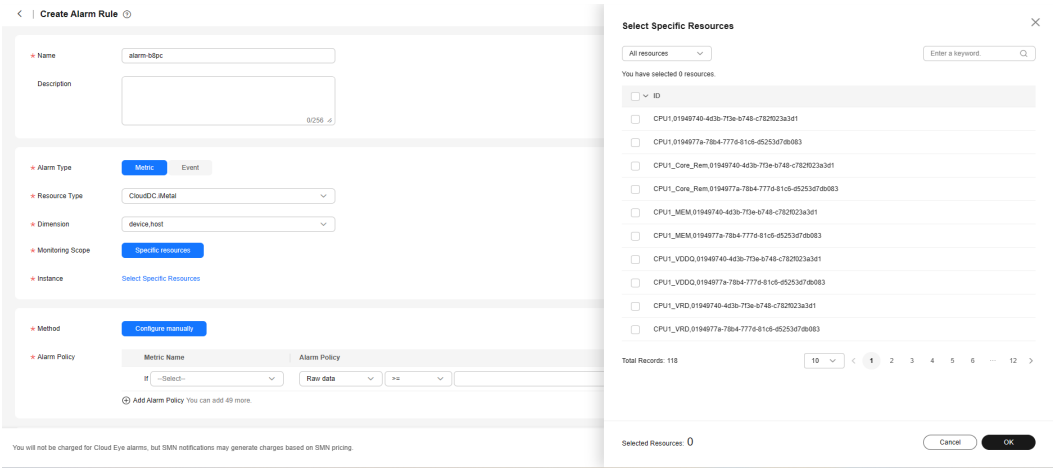
Dimension	Description
device,host	If this dimension is selected, you can specify a server component (such as the processor, memory, power supply, network interfaces, fans, or storage) as the monitored object.
host	If this dimension is selected, you can specify a server as the monitored object.
label	If this dimension is selected, you can specify a specific type of resources as the monitored object by label.
rack	If this dimension is selected, you can specify a rack as the monitored object.

NOTE

Currently, an iMetal server supports the following dimensions: **device,host**, **host**, **label**, and **rack**. You can select a dimension based on the object to be monitored.

- **Monitoring Scope**: Select **Specific resources**.
- **Instance**: Click **Select Specific Resources** and select the resources to be monitored.

Figure 3-23 Selecting specific resources



NOTE

The specified resources displayed in **Figure 3-23** vary according to the dimension. The following uses the **device,host** dimension as an example.

The content in the red box in **Figure 3-23** is the ID of the iMetal server. You can search for and select the resources of a specified iMetal service by ID for monitoring.

- **Method**: Select **Configure manually**.

- **Alarm Policy**: Specifies the policy for triggering an alarm. For details, see **Alarm Policies**.

6. Set alarm notification parameters.

   To send alarm notifications by email, SMS, HTTP, or HTTPS, enable **Alarm Notifications**.

   For details about the related parameters, see **Creating an Alarm Rule**.

7. Click **Create**.

   NOTE

   For more information about iMetal server alarm rules, see ***Cloud Eye User Guide*** .

3.7.4 Viewing Out-of-Band Monitoring Metrics (Alarms and Events) of iMetal Servers

Scenarios

After setting the alarm rules by referring to **Creating an Alarm Rule for an iMetal Server**, you can view the out-of-band monitoring metrics of an iMetal server on the overview page of the CloudDC console, including the server overview, alarm overview, server status, and server health status.

This section describes how to view the out-of-band monitoring information of all iMetal servers under the current account on the CloudDC overview page, including:

- **Viewing the iMetal Server Overview**
- **Viewing Alarms of the iMetal Servers**
- **Viewing Events of the iMetal Servers**

NOTE

- The out-of-band monitoring function of the iMetal servers is enabled by default. You do not need to manually enable it.
- You can also view the alarms and events of an iMetal server on the server details page. For details, see **Querying iMetal Details**.

Viewing the iMetal Server Overview

1. Log in to the CloudDC console.
2. Choose **Overview**.

   The **Overview** page of the CloudDC console is displayed.

   The iMetal server information is displayed by region on the **Overview** page, as shown in **Table 3-18**.

Table 3-18 Modules on the **Overview** page

Region	Description	Related Operation
Server Overview	Displays the number of servers, including: • Managed servers: the total number of servers under the current account. • Available servers: the number of servers whose **Health Status** is **Normal**. • Faulty servers: the number of servers whose **Health Status** is **Warning**, **Critical**, or **Unknown**.	You can move the pointer to the number of servers to view the number of servers in different equipment rooms.
Trends	Displays the change trends of server faults and alarms, including: • Daily New Faulty Servers: displays the number of daily new faulty servers. • Faulty Servers: displays the number of faulty servers. • Daily New Alarms (By Category): displays the number of daily new alarms by alarm category. • Alarms (By Category): displays the number of daily alarms by alarm category. • Daily New Alarms (By Severity): displays the number of daily new alarms by alarm severity. • Alarms (By Severity): displays the number of daily alarms by alarm severity.	• Setting the data display period: You can select a period from the drop-down list to view the data of the last 3 days, 7 days, 30 days, or a customized period. • Viewing detailed data: Hover the mouse pointer over the icon to view the number of faults or alarms on a day.
Alarm Overview	Displays the total number of alarms of the iMetal servers and the number of alarms by severity and that by category.	Click the number and type to view the alarm details.
Latest Alarms	Displays the latest alarms of the iMetal servers.	Click the alarm content link to view the alarm details.

Region	Description	Related Operation
Alarm Servers (Top 10)	Displays the top 10 servers that report alarms.	Click a server name to view the alarm time period and alarm duration of the server.
Server Status	Displays the numbers of iMetal servers whose **Power Status** is **Started**, **Stopped**, and **Unknown**.	Click a server status to view server details.
Server Health Status	Displays the numbers of iMetal servers whose **Health Status** is **Critical**, **Warning**, **Normal**, and **Unknown**.	Click a server status to view server details.

Viewing Alarms of the iMetal Servers

1. Log in to the CloudDC console.
2. Choose **Overview**.

   The **Overview** page of the CloudDC console is displayed.
3. Click the **Alarms** tab to view the alarm information of all iMetal servers under the current account.
   - Alarm query period: In the upper part of the alarm list, select a period from the drop-down list. You can view alarms in the last hour, last day, last 7 days, last 30 days, or a custom period.
   - Alarm query scope: You can search for alarms by server name, IP address, status, alarm subject, severity, server ID, and alarm content.

   View the alarm details in the alarm list, as shown in **Table 3-19**.

Table 3-19 Alarm information

Alarm Information	Description
Alarm Subject	Type of an alarm subject.
Alarm Content	Alarm details.
Severity	Alarm severity.
Server Name	Name of the iMetal server where an alarm was generated.
Server IP Address	IP address of the iMetal server where an alarm was generated.
Server ID	ID of the iMetal server where an alarm was generated.
Status	Alarm status.

Alarm Information	Description
Generated	Time when an alarm was generated.
Last Updated	Last time when an alarm was updated.

4. Click **View Server Status** in the **Operation** column of an alarm to go to the **Health** tab page on the details page of the iMetal server where the alarm was generated.

   On the **Health** tab page, you can view the health status of the iMetal server.
5. Click **View Events** in the **Operation** column of an alarm to go to the **Events** tab page.

   On the **Events** tab page, you can view the event details of the current iMetal server in the period when an alarm was generated.

Viewing Events of the iMetal Servers

1. Log in to the CloudDC console.
2. Choose **Overview**.

   The **Overview** page of the CloudDC console is displayed.
3. Click the **Events** tab to view the event information of all iMetal servers under the current account.
   - Event query period: In the upper part of the event list, select a period from the drop-down list. You can view events in the last hour, last day, last 7 days, last 30 days, or a custom period.
   - Event query scope: You can search for events by subject, event code, severity, server name, or server IP address in the search box.

   In the event list, you can view the event details, as shown in **Table 3-20**.

Table 3-20 Event information

Event Information	Description
Subject	Event subject.
Event Code	Reported event code.
Description	Event details.
Severity	Event severity.
Status	Event status.
Server Name	Name of the iMetal server where an event was reported.
Server IP Address	IP address of the iMetal server where an event was reported.
Server ID	ID of the iMetal server where an alarm was generated.

Event Information	Description
Generated	Time when an event was reported.

3.8 Auditing an iMetal Server Using CTS

3.8.1 Audit Traces Supported by iMetal Servers

Scenarios

With Cloud Trace Service (CTS), you can record traces associated with iMetal servers for future query, auditing, and backtracking.

Prerequisites

CTS has been enabled.

Key Operations Recorded by CTS

Operation	Resource Type	Trace
Downloading iMetal BMC logs from CTS	imetals	downloadLog
Setting the power supply	imetals	operatePower
Installing an OS	imetals	installOS
Uninstalling an OS	imetals	uninstallOS
Updating multiple intelligent racks	iracks	updateIracks
Updating a single iRack	iracks	updateIrack
Updating equipment room information	idcs	updateIdcs

3.8.2 Querying Audit Traces of the iMetal Servers

Scenarios

After you enable CTS and the management tracker is created, CTS starts recording operations on cloud resources. After a data tracker is created, the system starts recording operations on data in Object Storage Service (OBS) buckets. Cloud Trace Service (CTS) stores operation records (traces) generated in the last seven days.

This section describes how to query or export operation records of the last seven days on the CTS console.

- **Viewing Real-Time Traces in the Trace List of the New Edition**
- **Viewing Real-Time Traces in the Trace List of the Old Edition**

Constraints

- Traces of a single account can be viewed on the CTS console. Multi-account traces can be viewed only on the **Trace List** page of each account, or in the OBS bucket or the **CTS/system** log stream configured for the management tracker with the organization function enabled.
- You can only query operation records of the last seven days on the CTS console. To store operation records for longer than seven days, you must configure transfer to OBS or Log Tank Service (LTS) so that you can view them in OBS buckets or LTS log groups.
- After performing operations on the cloud, you can query management traces on the CTS console one minute later and query data traces five minutes later.
- These operation records are retained for seven days on the CTS console and are automatically deleted upon expiration. Manual deletion is not supported.

Viewing Real-Time Traces in the Trace List of the New Edition

1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. On the **Trace List** page, use advanced search to query traces. You can combine one or more filters.
   - **Trace Name**: Enter a trace name.
   - **Trace ID**: Enter a trace ID.
   - **Resource Name**: Enter a resource name. If the cloud resource involved in the trace does not have a resource name or the corresponding API operation does not involve the resource name parameter, leave this field empty.
   - **Resource ID**: Enter a resource ID. Leave this field empty if the resource has no resource ID or if resource creation failed.
   - **Trace Source**: Select a cloud service name from the drop-down list.
   - **Resource Type**: Select a resource type from the drop-down list.
   - **Operator**: Select one or more operators from the drop-down list.
   - **Trace Status**: Select **normal**, **warning**, or **incident**.
     - **normal**: The operation succeeded.
     - **warning**: The operation failed.
     - **incident**: The operation caused a fault that is more serious than the operation failure, for example, causing other faults.

- **Enterprise Project ID**: Enter an enterprise project ID.
- **Access Key**: Enter a temporary or permanent access key ID.
- Time range: Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range within the last seven days.

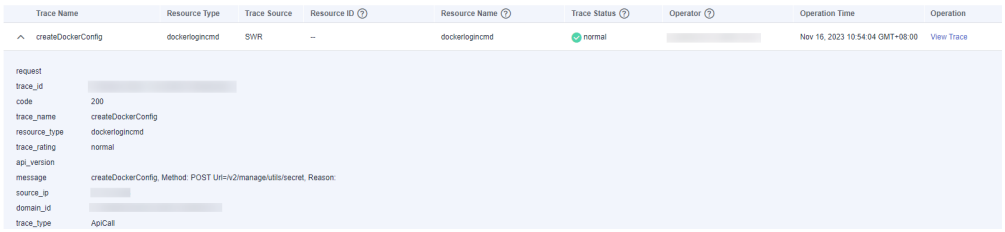
5. On the **Trace List** page, you can also export and refresh the trace list, and customize columns to display.
   - Enter any keyword in the search box and press **Enter** to filter desired traces.
   - Click **Export** to export all traces in the query result as an .xlsx file. The file can contain up to 5,000 records.
   - Click to view the latest information about traces.
   - Click to customize the information to be displayed in the trace list. If **Auto wrapping** is enabled ( ), excess text will move down to the next line; otherwise, the text will be truncated. By default, this function is disabled.
6. For details about key fields in the trace structure, see **Trace Structure** and **Example Traces**.
7. (Optional) On the **Trace List** page of the new edition, click **Go to Old Edition** in the upper right corner to switch to the **Trace List** page of the old edition.

Viewing Real-Time Traces in the Trace List of the Old Edition

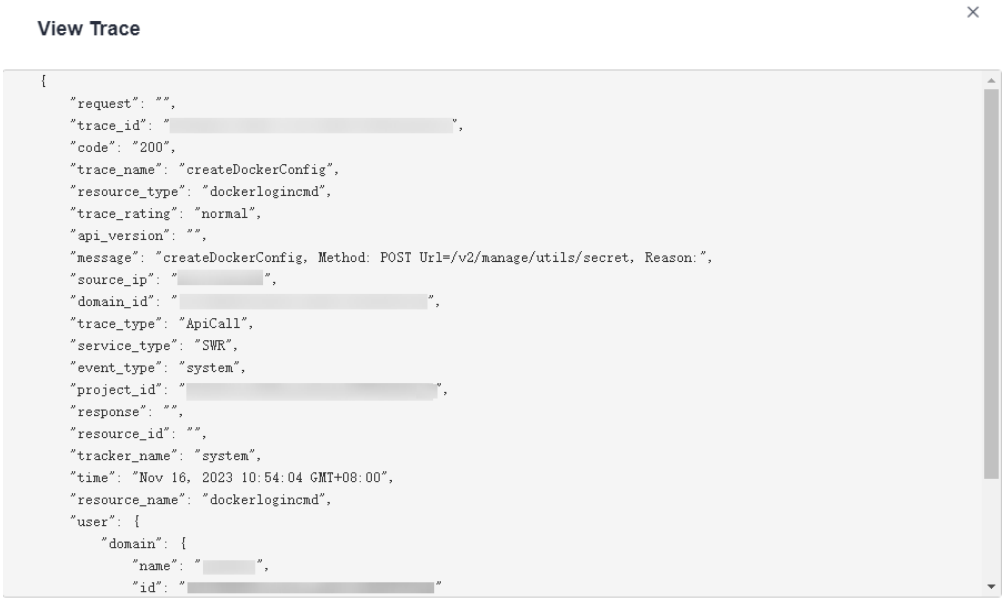
1. Log in to the management console.
2. Click in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. Each time you log in to the CTS console, the new edition is displayed by default. Click **Go to Old Edition** in the upper right corner to switch to the trace list of the old edition.
5. Set filters to search for your desired traces. The following filters are available.
   - **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**: Select a filter from the drop-down list.
     - If you select **Resource ID** for **Search By**, specify a resource ID.
     - If you select **Trace name** for **Search By**, specify a trace name.
     - If you select **Resource name** for **Search By**, specify a resource name.
   - **Operator**: Select a user.
   - **Trace Status**: Select **All trace statuses**, **Normal**, **Warning**, or **Incident**.
   - Time range: Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range within the last seven days.
6. Click **Query**.
7. On the **Trace List** page, you can also export and refresh the trace list.
   - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5,000 records.

- Click to view the latest information about traces.

8. Click on the left of a trace to expand its details.



9. Click **View Trace** in the **Operation** column. The trace details are displayed.



10. For details about key fields in the trace structure, see **Trace Structure** and **Example Traces** in the *CTS User Guide*.
11. (Optional) On the **Trace List** page of the old edition, click **New Edition** in the upper right corner to switch to the **Trace List** page of the new edition.

4 Data Center

4.1 Purchasing an Intelligent Rack

Scenarios

To get a highly reliable data center runtime environment quickly and eliminate the need for long-term investments in traditional data center site selection, infrastructure construction, facility reconstruction, O&M, and operations, you can purchase intelligent racks to deploy your own server hardware in Huawei Cloud equipment rooms.

The resources deployed in this mode must be used with Direct Connect to connect customers' on-premises data centers to Huawei Cloud equipment rooms.

If you want to deploy your own server hardware in Huawei Cloud equipment rooms, you need to purchase intelligent racks on the management console.

This section uses the separate order transaction as an example to describe how to purchase an intelligent rack.

NOTICE

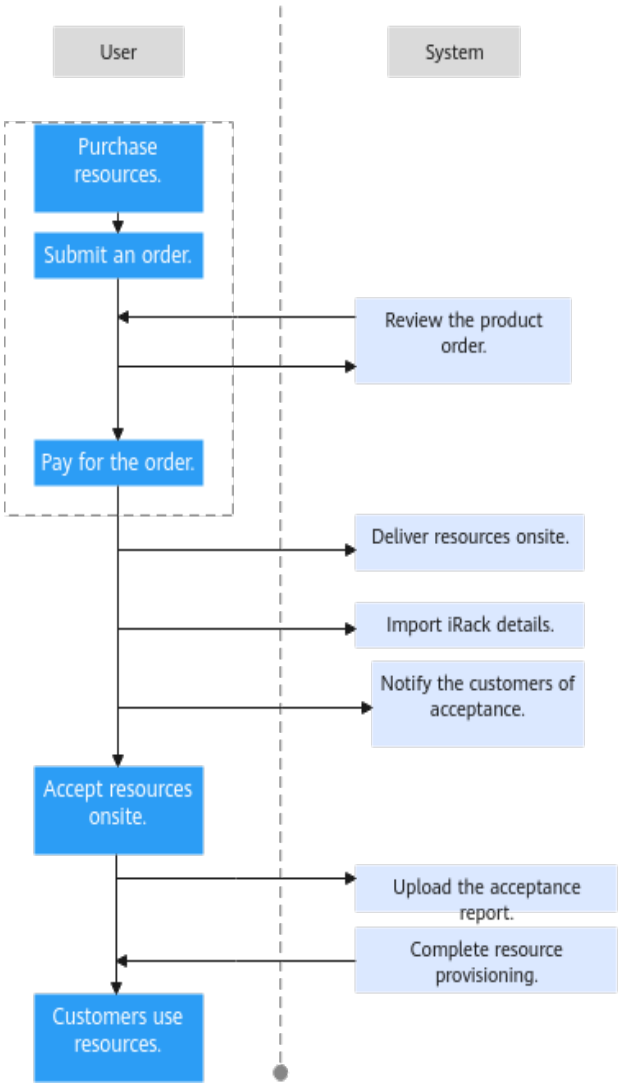
Offline operations and verification are required when you purchase an intelligent rack. This section describes only how to purchase racks, submit orders, and pay for orders.

Constraints

Currently, only the yearly/monthly billing mode is supported.

Process

Figure 4-1 Process

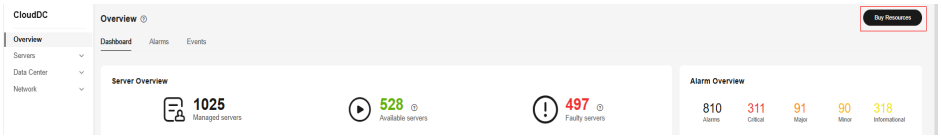


The following walks you through purchasing resources to paying for orders.

Procedure

1. Log in to the CloudDC console.
2. In the upper right corner of the **Overview** page, click **Buy Resources**. The **Buy Resources** page is displayed.

   Figure 4-2 Purchasing resources



3. Set parameters for iRack and click **Add**.

Figure 4-3 iRack

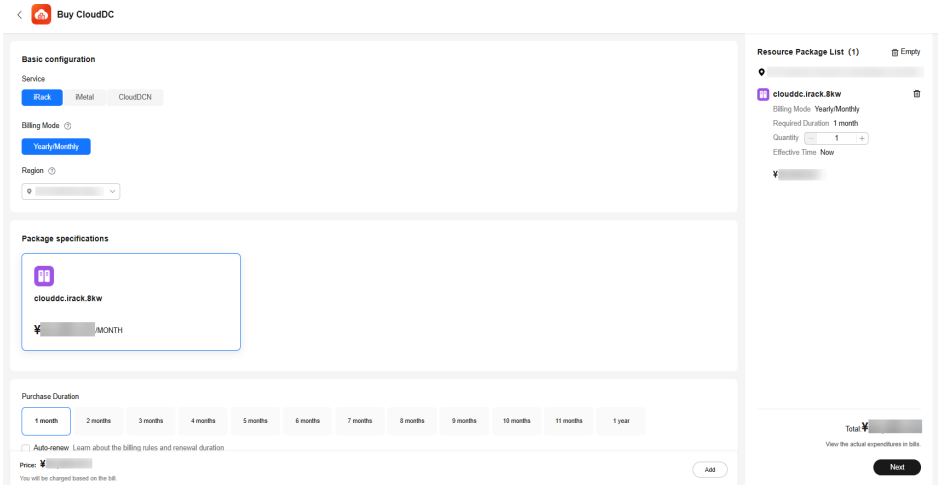


Table 4-1 Parameters

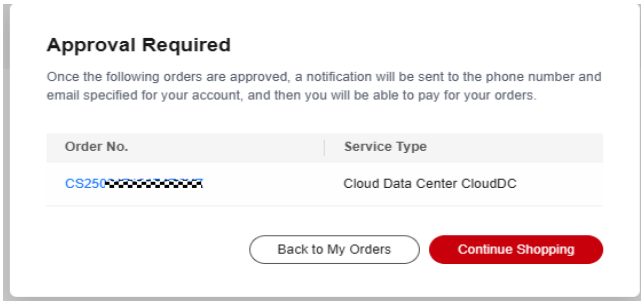
Parameter	Example Value	Description
Resource Type	iRack	Select the type of the resource to be purchased. Currently, the following resource types are supported: • iRack: used to deploy server hardware in Huawei Cloud equipment rooms. • iMetal: used to deploy your own servers in Huawei Cloud equipment rooms. • CloudDCN: used to connect servers deployed on Huawei Cloud to a private network on the cloud.
Billing Mode	Yearly/Monthly	Prepaid billing. You pay in advance for a subscription term, and in exchange, you get a discounted rate. Ensure that you have a top-up account with a sufficient balance or have a valid payment method configured first.
Region	CN South-Guangzhou	For low network latency and quick resource access, select the region nearest to your target users. After the purchase, the region cannot be changed.

Parameter	Example Value	Description
Specifications	clouddc.irack.8kw	Available resource package specifications The package specifications supported by different resource types are as follows: • iRack: clouddc.irack.8kw • iMetal: clouddc.imetal.host • CloudDCN: CloudDCN.GeneralNetwork.25G and CloudDCN.IntelligentNetwork.200G
Purchase Duration	1 month	Required duration of resources. The purchase duration varies depending on the resource type. For details, see the information displayed on the console. You can select **Auto-renew** to automatically renew yearly/monthly resources when they expire. For details about auto-renewal rules, see **Rules for Setting Auto-Renewal When Automatically Renewing a Cloud Service**.
Quantity	1	The number of resources to be purchased.

4. In the lower right corner of the **Resource Package List** pane, click **Next**.
5. After confirming the configuration, click **Pay**.

   The resource purchase order can be paid only after it is approved.

   Figure 4-4 Order review



6. On the menu bar of the console, choose **Billing** > **Unpaid Orders** and view the order status in the **Order Status** column.

   During the transaction, the order status changes as follows:

   a. **Pending approval**: The user has submitted an order and is waiting for the approval.

   b. **Pending payment**: After the order is approved, the user can pay for the order.

c. **Processing**: After the payment is complete, the on-premises resource deployment phase starts.

d. **Completed**: The offline acceptance is complete, resources are enabled, and the order is complete.

4.2 Managing an Intelligent Rack

Scenarios

You can use a web-based console to view the details of an intelligent rack where an iMetal server is deployed or view iMetal server details by iRack. You can also import or export iRack details on the console.

This section describes how to manage details of the iRack where an iMetal server is deployed.

Viewing iRack Details

1. Log in to the CloudDC console.
2. Choose **Data Center** > **iRack**.

   The **iRack** page is displayed. In the iRack list, view the rack details, as described in **Table 4-2**.

Table 4-2 iRack details

Parameter	Description	Related Operation
Rack Name	Name of an intelligent rack.	You can click a name in the **Rack Name** column to go to the iRack details page, which displays the basic details, temperature, and power of the rack.
Equipment Room	Name of the equipment room where an intelligent rack is located.	None.
Location	Physical location of an intelligent rack.	None.
Rack Size	Dimensions of an intelligent rack. The format is width × depth × height.	None.
Height (U)	Height of an intelligent rack.	None.
Rated Power	Rated power of an intelligent rack.	None.

Parameter	Description	Related Operation
Servers	Number of iMetal servers in an intelligent rack.	You can click a number in the **Servers** column of a rack to go to the **iMetal Servers** page and view details about all servers in the rack.
Tag	Tag of an intelligent rack, which is used to identify the iRack.	You can edit the tag.
Description	Description of an intelligent rack.	You can edit the description.
Billing Mode	Yearly/Monthly billing for an intelligent rack	None.

Importing iRack Details

1. Log in to the CloudDC console.
2. Choose **Data Center** > **iRack**.

   The **iRack** page is displayed.
3. Above the iRack list, click **Import**. The **Import** dialog box is displayed.
4. Click **Download Template** to download the template.

   If you have filled in the server details based on the template requirements, go to step 6.
5. Enter the rack details in the downloaded template based on the template requirements.

NOTICE

Once the iRack details are imported, they cannot be modified. If the information is incorrect, import it again.

Table 4-3 iRack template

Parameter	Mandatory	Description
Rack Name	Yes	Name of an intelligent rack. Maximum length: 128 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.

Parameter	Mandatory	Description
Equipment Room	Yes	Name of the equipment room where an intelligent rack is located. Maximum length: 256 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.
Location	Yes	Physical location of an intelligent rack. Maximum length: 128 characters.
Height (U)	Yes	Height of an intelligent rack. Maximum length: 128 characters.
Rack Size	Yes	Dimensions of an intelligent rack. The format is width × depth × height. Maximum length: 128 characters.
Rated Power	Yes	Rated power of an intelligent rack. Maximum length: 128 characters. It cannot contain spaces or line breaks.
Description	No	Description of an intelligent rack. Maximum length: 512 characters.

6. Click **Select File** and select the file where the iRack details have been filled in.

   The system automatically checks whether the imported data is valid.
7. After the import is verified, click **Import** to import iRack details.

   After the import is complete, you can view the imported iRack details in the list.

Exporting iRack Details

1. Log in to the CloudDC console.
2. Choose **Data Center** > **iRack**.

   The **iRack** page is displayed.
3. In the upper part of the iRack list, click **Export** > **Export all data to an XLSX file.**

   All iRack details will be downloaded locally in the format of "racks-Current date".

4.3 Managing an Equipment Room

Scenarios

You can use a web-based console to view information about the equipment room where an iMetal server is deployed. You can view iMetal server information by equipment room or export all equipment room data to a local file in XLSX format.

This section describes how to manage the equipment room where an iMetal server is deployed.

Viewing Equipment Room Details

1. Log in to the CloudDC console.
2. Choose **Data Center** > **Equipment Rooms**.

   The **Equipment Rooms** page is displayed. In the equipment room list, you can view the equipment room information, as shown in **Table 4-4**.

Table 4-4 Equipment room information

Parameter	Description	Related Operation
Equipment Room Name	Name of an equipment room.	None.
Racks	Number of intelligent racks in an equipment room.	You can click a number in the **Racks** column of an equipment room to go to the **iRack** page and view information about all racks in the equipment room.
Servers	Number of iMetal servers in an equipment room.	You can click a number in the **Servers** column of an equipment room to go to the **iMetal Servers** page and view information about all servers in the equipment room.
Description	Description about an equipment room.	You can modify the description.

Exporting Equipment Room Information

1. Log in to the CloudDC console.
2. Choose **Data Center** > **Equipment Rooms**.

   The **Equipment Rooms** page is displayed.
3. In the upper part of the equipment room list, click **Export** > **Export all data to an XLSX file.**

All iRack details will be downloaded locally in the format of "sites-Current date".

5 Network

5.1 CloudDCN Subnet

5.1.1 CloudDCN Subnet Overview

What Is a CloudDCN Subnet?

With CloudDCN subnets, you can connect your physical servers (iMetal servers) to an isolated, private, and high-performance cloud network.

When creating a VPC, you cannot create a CloudDCN subnet. You need to create a CloudDCN subnet in an existing VPC for deploying iMetal servers.

Notes and Constraints

Note the following when using CloudDCN subnets:

- The DHCP lease time is not supported.
- The DNS server address cannot be changed.
- Virtual IP addresses cannot be assigned.
- IPv6 addresses cannot be assigned.
- Each CloudDCN subnet comes with a default route table, which cannot be modified.
- Physical servers in a CloudDCN subnet cannot be associated with security groups.
- CloudDCN subnets cannot be shared.
- CloudDCN subnets does not support multicast.
- ECSs and BMSs cannot be created in CloudDCN subnets.
- CloudDCN subnets do not support flow logs. This means flow logs of the iMetal server in the CloudDCN subnet cannot be collected.
- CloudDCN subnets cannot be used as the frontend or backend subnet of load balancers.

- If you want to add an iMetal server in a CloudDCN subnet as the backend server of a load balancer, note the following:
  - When adding a backend server, you can only select **IP as a Backend**. For details, see **Adding Backend Servers in a Different VPC from a Load Balancer**.
  - When an iMetal server is added as a backend server, **Transfer Client IP Address** will not work even if it is enabled.

5.1.2 Creating a CloudDCN Subnet

Scenarios

A subnet is a unique CIDR block with a range of IP addresses in a VPC. All resources in a VPC must be deployed on subnets.

When creating a VPC, you cannot create a CloudDCN subnet. You can create a CloudDCN subnet on the **CloudDCN Subnets** page for deploying physical servers.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking** > **Virtual Private Cloud**.

   The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Virtual Private Cloud** > **CloudDCN Subnets**.
5. Click **Create CloudDCN Subnet**.

   The **Create CloudDCN Subnet** page is displayed.
6. Set the parameters based on the below table.

Table 5-1 Parameters for creating a CloudDCN subnet

Parameter	Description	Example Value
VPC	The VPC where you want to create a CloudDCN subnet. If no VPC is available, create one.	vpc-test
Subnet Name	The CloudDCN subnet name. The name: • Can contain 1 to 64 characters. • Can contain letters, digits, underscores (_), hyphens (-), and periods (.).	subnet-clouddcn-01

Parameter	Description	Example Value
AZ	An AZ is a geographic location with independent power supply and network facilities in a region. AZs are physically isolated, and AZs in the same VPC are interconnected through an internal network. Each region contains multiple AZs. If one AZ is unavailable, other AZs in the same region continue to provide services. • By default, all instances in different subnets of the same VPC can communicate with each other and the subnets can be in different AZs. For example, if you have a VPC with two subnets, subnet A01 in AZ1 and CloudDCN subnet A02 in AZ2. A01 and A02 can communicate with each other by default. • A cloud resource can be in a different AZ from its subnet. For example, a physical server in AZ1 can be in a CloudDCN subnet in AZ3. If AZ3 becomes faulty, physical servers in AZ1 can still use the CloudDCN subnet in AZ3, and your services are not interrupted. For details, see **Region and AZ**.	AZ1
IPv4 CIDR Block	The IPv4 CIDR block range of a CloudDCN subnet. A CloudDCN subnet is a unique CIDR block with a range of IP addresses in a VPC. A subnet mask can be between the netmask of its VPC CIDR block and /28 netmask. If a VPC CIDR block is 10.0.0.0/16, its subnet mask can between 16 to 28. If the VPC has a secondary CIDR block, you can select the primary or the secondary CIDR block that the subnet will belong to based on service requirements.	10.0.0.0/24

Parameter	Description	Example Value
Associated Route Table	The default route table with which the CloudDCN subnet will be associated. A route table contains a set of routes that are used to control the traffic routing for your subnets in a VPC. Each VPC comes with a default route table that will be automatically associated with CloudDCN subnets. This allows CloudDCN subnets in a VPC to communicate with each other.	-
Advanced Settings (Optional) > Gateway	The gateway address of the CloudDCN subnet. Click ⌄ to expand the configuration area and set this parameter. Retain the default value unless there are special requirements.	10.0.0.1
Advanced Settings (Optional) > DNS Server Address	The DNS server addresses of the CloudDCN subnet. Click ⌄ to expand the configuration area and set this parameter. A DNS server address is set by default to allow servers in a CloudDCN subnet to communicate with each other using private domain names. You can also directly access cloud services through private DNS servers. You can change the default DNS server address if needed. This may interrupt your access to cloud services. You can also click **Reset** on the right to restore the DNS server address to the default value. A maximum of two DNS server IP addresses can be configured. Multiple IP addresses must be separated using commas (,).	100.125.x.x
Advanced Settings (Optional) > Tag	The CloudDCN subnet tags. Click ⌄ to expand the configuration area and set this parameter. Add tags to help you quickly identify, classify, and search for your CloudDCN subnets. For details, see **Managing CloudDCN Subnet Tags**.	• Key: test • Value: 01

Parameter	Description	Example Value
Advanced Settings (Optional) > Description	Supplementary information about the CloudDCN subnet. Click to expand the configuration area and set this parameter. Enter a description about the CloudDCN subnet in the text box as required. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

7. Click **Create Now**.
   Return to the CloudDCN subnet list and view the subnet you have created.

5.1.3 Managing a CloudDCN Subnet

After a CloudDCN subnet is created, you can perform the following operations to manage a CloudDCN subnet:

- **Modifying the Basic Information of a CloudDCN Subnet**
- **Exporting CloudDCN Subnets**
- **Managing CloudDCN Subnet Tags**
- **Viewing IP Addresses in a CloudDCN Subnet**
- **Deleting a CloudDCN Subnet**

Modifying the Basic Information of a CloudDCN Subnet

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Click in the upper left corner and choose **Networking** > **Virtual Private Cloud**.
   The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Virtual Private Cloud** > **CloudDCN Subnets**.
   The **CloudDCN Subnets** page is displayed.
5. In the CloudDCN subnet list, locate the target subnet and click its name.
   The CloudDCN subnet details page is displayed.
6. On the **Summary** tab, click on the right of the parameter to be modified and modify the parameter.

Table 5-2 CloudDCN subnet parameters that can be modified

Parameter	Description	Example Value
Name	Name of the CloudDCN subnet. The name: • Can contain 1 to 64 characters. • Can contain letters, digits, underscores (_), hyphens (-), and periods (.).	Subnet
Description	Supplementary information about the CloudDCN subnet. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

Exporting CloudDCN Subnets

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Click in the upper left corner and choose **Networking** > **Virtual Private Cloud**.

   The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Virtual Private Cloud** > **CloudDCN Subnets**.

   The **CloudDCN Subnets** page is displayed.
5. In the upper left corner of the CloudDCN subnet list, click **Export**.
   - **Export selected data to an XLSX file**: Select one or more CloudDCN subnets and export information about the selected subnets.
   - **Export all data to an XLSX file**: Export information about all the CloudDCN subnets in the current region.

   The system will automatically export information about the CloudDCN subnets as an Excel file to a local directory.

Managing CloudDCN Subnet Tags

Tags help you identify and search for cloud resources easier.

- Each tag consists of a tag key and a tag value. Only the tag value can be edited.

  If you want to change the tag key, delete it and add one again.
- Each cloud resource can have a maximum of 20 tags.

For details about CloudDCN subnet tag requirements, see **Table 5-3**.

Table 5-3 Tag key and value requirements of a CloudDCN subnet

Parameter	Requirements	Example Value
Tag key	• For each CloudDCN subnet, each tag key must be unique, and each tag key can only have one tag value. • Cannot be left blank. • Can contain a maximum of 128 characters. • Can consist of letters, digits, underscores (_), and hyphens (-).	test
Tag value	• Can be left blank. • Can contain a maximum of 256 characters. • Can consist of letters, digits, underscores (_), periods (.), and hyphens (-).	01

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Click in the upper left corner and choose **Networking** > **Virtual Private Cloud**.

   The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Virtual Private Cloud** > **CloudDCN Subnets**.

   The **CloudDCN Subnets** page is displayed.
5. In the CloudDCN subnet list, locate the target subnet and click its name.

   The CloudDCN subnet details page is displayed.
6. On the **Tags** tab, click **Edit Tag** in the upper left corner above the tag list.

   The **Edit Tag** dialog box is displayed.
7. Perform the following operations on the tag as required:
   - Adding a tag: Click +, enter a tag key and value, and click **OK**.
   - Modifying a tag: Click × next to the target tag key or value, delete the original value, enter a new value, and click **OK**.
   - Deleting a tag: Click **Delete** next to the target tag and click **OK**.

Viewing IP Addresses in a CloudDCN Subnet

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Click in the upper left corner and choose **Networking** > **Virtual Private Cloud**.

   The **Virtual Private Cloud** page is displayed.

4. In the navigation pane on the left, choose **Virtual Private Cloud** > **CloudDCN Subnets**.

   The **CloudDCN Subnets** page is displayed.

5. In the CloudDCN subnet list, locate the target subnet and click its name.

   The CloudDCN subnet details page is displayed.

6. Click the **IP Addresses** tab to view the IP addresses in the CloudDCN subnet.

   In the private IP address list in the lower part of the page, you can view the private IP addresses, the resources that use the IP addresses of the CloudDCN subnet, and the resource ID.

Deleting a CloudDCN Subnet

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking** > **Virtual Private Cloud**.

   The **Virtual Private Cloud** page is displayed.

4. In the navigation pane on the left, choose **Virtual Private Cloud** > **CloudDCN Subnets**.

   The **CloudDCN Subnets** page is displayed.

5. In the CloudDCN subnet list, locate the target subnet and click **Delete** in the **Operation** column.

   A confirmation dialog box is displayed.

   If your CloudDCN subnet is used by other resources, you need to delete these resources before deleting this subnet.

6. Enter **DELETE** as prompted and click **OK**.

5.2 CloudDCN Subnet Network ACL

5.2.1 CloudDCN Subnet Network ACL Overview

What Is a CloudDCN Subnet Network ACL?

A network ACL is an optional layer of protection for your CloudDCN subnets. After you add inbound and outbound rules to a network ACL and associate CloudDCN subnets with it, you can control traffic in and out of the subnets.

Network ACL Rules for CloudDCN Subnets

- CloudDCN network ACLs has inbound and outbound rules that are used to control traffic in and out of CloudDCN subnets.
  - Inbound rules: control traffic sent to the instances in a CloudDCN subnet.
  - Outbound rules: control traffic from the instances in a CloudDCN subnet to external networks.

- You need to define the protocol, source and destination ports, source and destination IP addresses, and other information for network ACL rules.
  - Rule number: Network ACL rules are matched in ascending order, from the lowest to highest rule number.

    The default network ACL rule is marked with an asterisk (*) and is the very last rule that will be used for matching.
  - **Status**: **Enabled** or **Disabled**. Enabled rules are applied, while disabled rules are not.
  - **Action**: **Allow** or **Deny**. If a request matches a network ACL rule, the action defined in the rule is taken to allow or deny the request.
  - **Protocol**: The protocol to match traffic. The value can be **TCP**, **UDP**, or **ICMP**.
  - **Source**/**Destination**: The source or destination of the traffic.
  - **Source Port Range**/**Destination Port Range**: The source or destination port or port range, which ranges from 1 to 65535.

How Network ACL Rules Work

- After a network ACL is created, you can associate it with one or more CloudDCN subnets to control traffic in and out of the subnets. A network ACL can be associated with multiple CloudDCN subnets. However, a CloudDCN subnet can be associated with only one network ACL.
- The network ACLs dedicated for CloudDCN subnets are stateful. If the network ACL rule allows outbound traffic from your instance, you also need to set the inbound rule's action to **Allow** so that responses to outbound traffic to flow in. Similarly, if inbound traffic is allowed, you need to set the outbound rule's action to **Allow** so that responses to such inbound traffic to flow out.
- Each network ACL has the default inbound and outbound rules, as shown in **Table 5-4**. If a network ACL has no custom rules, the default inbound and outbound rules are applied, denying all traffic in and out of a CloudDCN subnet. You can use the default rules only when there is no need for traffic to go in and out of a CloudDCN subnet. If the traffic needs to go in and out of the subnet, you need to add custom rules to control traffic as required.

  Table 5-4 Default network ACL rules

Direction	Rule Number	Action	Protocol	Source	Source Port Range	Destination	Destination Port Range
Inbound	*	Deny	All	0.0.0.0/0	All	0.0.0.0/0	All
Outbound	*	Deny	All	0.0.0.0/0	All	0.0.0.0/0	All

- The default and custom rules of a network ACL does not block the traffic described in **Table 5-5**.

Table 5-5 Traffic not blocked by network ACL rules

Direction	Description
Inbound	Traffic between the source and destination in the same CloudDCN subnet
	Broadcast traffic to 255.255.255.255/32
	Multicast traffic to 224.0.0.0/24
Outbound	Traffic between the source and destination in the same CloudDCN subnet
	Broadcast traffic to 255.255.255.255/32
	Multicast traffic to 224.0.0.0/24
	TCP metadata traffic to 169.254.169.254/32 over port 80
	Traffic to 100.125.0.0/16 that is reserved for public services on the cloud, such as the DNS server address and NTP server address

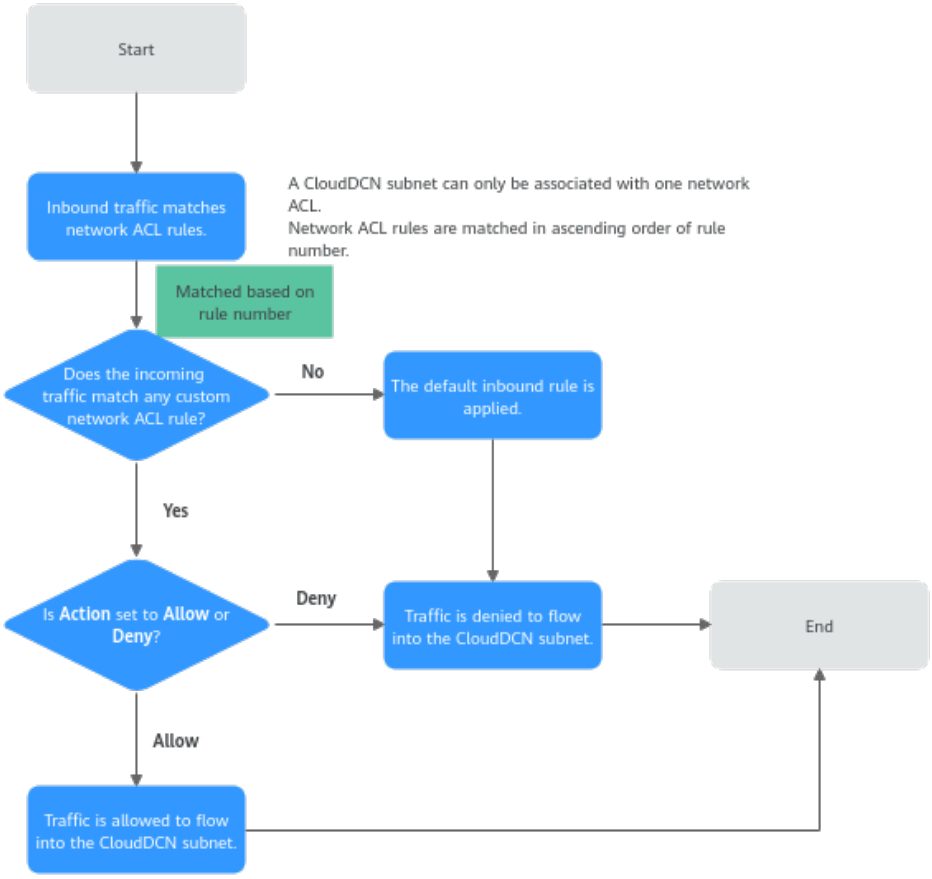
How Traffic Matches Network ACL Rules

A CloudDCN subnet can only be associated with one network ACL. If there are multiple rules on the network ACL, rules are matched in ascending order, from the lowest to highest rule number. The default network ACL rule is marked with an asterisk (*) and is the very last rule that will be used for matching.

The matching sequence of inbound traffic is the same as that of outbound traffic. The following takes inbound traffic as an example to describe how the rules are applied.

- If a custom rule is matched:
  - If **Action** is set to **Deny**, traffic is denied to flow into the CloudDCN subnet.
  - If **Action** is set to **Allow**, traffic is allowed to flow into the CloudDCN subnet.
- If no custom rule is matched, the default rule is applied, denying traffic to flow into the CloudDCN subnet.

Figure 5-1 Network ACL matching



Network ACL Configuration Procedure

Figure 5-2 Procedure for configuring a network ACL

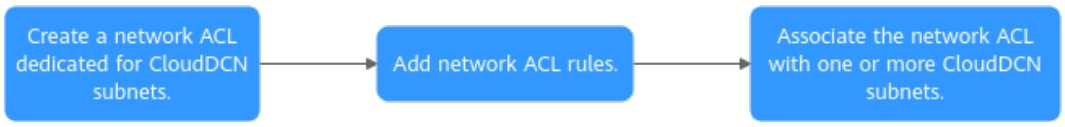


Table 5-6 Procedure for configuring a network ACL

No.	Step	Description	Procedure
1	Create a network ACL dedicated for CloudDCN subnets.	Each network ACL comes with default inbound and outbound rules that deny traffic in and out of a CloudDCN subnet. The default rules cannot be deleted or modified.	**Creating a Network ACL Dedicated for CloudDCN Subnets**

No.	Step	Description	Procedure
2	Add network ACL rules.	The default network ACL rules cannot be modified or deleted. You can add custom rules to control traffic in and out of a CloudDCN subnet. Traffic will be preferentially matched against the custom rules.	**Adding Network ACL Rules for CloudDCN Subnets**
3	Associate the network ACL with one or more CloudDCN subnets.	You can associate the network ACL with one or more CloudDCN subnets. If it is enabled, it controls traffic in and out of the subnets. A CloudDCN subnet can be associated with only one network ACL.	**Associating CloudDCN Subnets with a Network ACL**

Constraints on Using Network ACLs

- By default, each account can have up to 5 network ACLs in a region.
- A network ACL can have no more than 40 rules in one direction, or performance will deteriorate.

5.2.2 Creating a Network ACL Dedicated for CloudDCN Subnets

Scenarios

A network ACL protects all the instances in the associated CloudDCN subnets. You can create a network ACL by referring to this section.

Procedure

1. Go to the **network ACL list page**.
2. In the upper right corner of the Network ACL list, click **Create Network ACL**.
3. Set the parameters for as prompted.

Table 5-7 Parameters for configuring a network ACL dedicated for CloudDCN subnets

Parameter	Description	Example Value
Region	Mandatory A network ACL can only be associated with the CloudDCN subnets in the same region.	-

Parameter	Description	Example Value
Name	Mandatory The name of the network ACL. The name can contain a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot contain spaces.	fw-A
Type	Mandatory There are two options: • **General**: The network ACL can be associated with general subnets. • **CloudDCN**: The network ACL can be associated with CloudDCN subnets.	CloudDCN
Description	Supplementary information about the Network ACL. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	N/A

4. Click **Create Now**.

Follow-up Operations

1. A network ACL comes with default inbound and outbound rules that deny all traffic in and out of associated CloudDCN subnets. You can add custom rules to allow traffic by referring to **Adding Network ACL Rules for CloudDCN Subnets**. Traffic will preferentially match the custom rules.
2. You can associate the network ACL with one or more CloudDCN subnets by referring to **Associating CloudDCN Subnets with a Network ACL**. If it is enabled, it controls traffic in and out of the subnets.

5.2.3 Adding Network ACL Rules for CloudDCN Subnets

Scenarios

You can add inbound and outbound rules to a network ACL to control the traffic in and out of a CloudDCN subnet. Network ACL rules are matched in ascending order, either by the system-generated rule numbers or those you define.

- **Adding a Network ACL Rule (Default Rule Numbers)**: Rules are matched in order of their number, starting with the lowest. The rule number is automatically assigned based on the time when the rule is added.

  In **Table 5-8**, there are two custom inbound rules (rule A and rule B) and one default rule. The rule A number is 1 and rule B number is 2. The default rule is the last rule that is used for matching traffic. When you add rule C, the rule

number will be 3, which will be matched later than rules A and B but earlier than the default rule.

Table 5-8 Default rule numbers

Rule Number (Rules A and B)		Rule Number (Rules A, B, and C)	
Custom rule A	1	Custom rule A	1
--	--	Custom rule B	2
Custom rule B	2	**Custom rule C**	**3**
Default rule	*	Default rule	*

- **Adding a Network ACL Rule (Custom Rule Numbers)**: If you want a rule to be matched earlier or later than a specific rule, you can insert the rule above or below the specific rule.

  In **Table 5-9**, there are two custom inbound rules (rule A and rule B) and one default rule. The rule A number is 1 and rule B number is 2. The default rule is the last rule that is used for matching traffic. If you want rule C to be matched earlier than rule B, you can insert rule C above rule B. After rule C is added, the rule C number is 2, and rule B number is 3.

Table 5-9 Custom rule numbers

Rule Number (Rules A and B)		Rule Number (Rules A, B, and C)	
Custom rule A	1	Custom rule A	1
--	--	**Custom rule C**	**2**
Custom rule B	2	Custom rule B	3
Default rule	*	Default rule	*

Constraints

A network ACL can contain up to 40 rules in one direction, or performance will deteriorate.

Adding a Network ACL Rule (Default Rule Numbers)

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Click in the upper left corner and choose **Networking** > **Virtual Private Cloud**.

   The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Access Control** > **Network ACLs**.

   The Network ACL list is displayed.

5. In the Network ACL list, locate the target Network ACL and click its name.
   The Network ACL summary page is displayed.
6. On the **Inbound Rules** or **Outbound Rules** tab, click **Add Rule**.
   The **Add Inbound Rule** or **Add Outbound Rule** dialog box is displayed.
7. Configure required parameters.
   - Click ⊕ to add more rules.
   - Locate the row that contains the Network ACL rule and click **Replicate** in the **Operation** column to replicate an existing rule.

Table 5-10 Parameter descriptions

Parameter	Description	Example Value
Action	The action for the network ACL rule. There are two options: ● **Allow**: allows matched traffic in and out of a CloudDCN subnet. ● **Deny**: denies matched traffic in and out of a CloudDCN subnet.	Allow
Protocol	The protocol to match traffic. The value can be **TCP**, **UDP**, or **ICMP**.	TCP
Source	The source from which the traffic is allowed or denied. The source can be: ● Single IP address: IP address/mask Example IPv4 address: 192.168.10.10/32 ● An IP address range in CIDR notation: IP address/mask Example IPv4 address range: 192.168.52.0/24 ● All IP addresses 0.0.0.0/0 represents all IPv4 addresses.	192.168.0.0/24
Source Port Range	The source ports or port ranges used to match traffic. The value ranges from 1 to 65535. Enter ports in the following format: ● Individual port: Enter a port, such as **22**. ● Consecutive ports: Enter a port range, such as **22-30**. ● All ports: Leave it empty or enter **1-65535**.	22-30

Parameter	Description	Example Value
Destination	The destination to which the traffic is allowed or denied. The destination can be: • Single IP address: IP address/mask Example IPv4 address: 192.168.10.10/32 • An IP address range in CIDR notation: IP address/mask Example IPv4 address range: 192.168.52.0/24 • All IP addresses 0.0.0.0/0 represents all IPv4 addresses.	0.0.0.0/0
Destination Port Range	The destination ports or port ranges used to match traffic. The value ranges from 1 to 65535. Enter ports in the following format: • Individual port: Enter a port, such as **22**. • Consecutive ports: Enter a port range, such as **22-30**. • All ports: Leave it empty or enter **1-65535**.	22-30
Description	(Optional) Supplementary information about the network ACL rule. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	N/A

8. Click **OK**.

   Return to the rule list to check the new rule.

   – Rules are assigned a number based on the order they are added, with lower-numbered rule matched earlier.
   – If the status of the new rule is **Enabled**, the rule is applied.

Adding a Network ACL Rule (Custom Rule Numbers)

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Click in the upper left corner and choose **Networking** > **Virtual Private Cloud**.

   The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Access Control** > **Network ACLs**.

   The Network ACL list is displayed.
5. In the Network ACL list, locate the target Network ACL and click its name.

The Network ACL summary page is displayed.

6. Click the **Inbound Rules** or **Outbound Rules** tab and insert a rule.
   - Locate the target rule and choose **More** > **Insert Rule Above** in the **Operation** column. The new rule will be matched earlier than the current rule.
   - Locate the target rule and choose **More** > **Insert Rule Below** in the **Operation** column. The new rule will be matched later than the current rule.

5.2.4 Associating CloudDCN Subnets with a Network ACL

Scenarios

You can associate the network ACL with one or more CloudDCN subnets. If it is enabled, it controls traffic in and out of the subnets.

Associating CloudDCN subnets with a network ACL may affect how and where traffic is directed. Be careful with this operation as it may interrupt services.

Constraints

- A network ACL can be associated with multiple CloudDCN subnets. However, a CloudDCN subnet can be associated with only one network ACL.
- After a network ACL is associated with a CloudDCN subnet, the default rules deny all traffic to and from the subnet until you add custom rules to allow traffic. For details, see **Adding Network ACL Rules for CloudDCN Subnets**.
- A CloudDCN network ACL can only be associated with CloudDCN subnets.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Click in the upper left corner and choose **Networking** > **Virtual Private Cloud**.

   The **Virtual Private Cloud** page is displayed.
4. Associate a CloudDCN subnet with a network ACL using either of the following methods:
   - Method 1
     i. In the navigation pane on the left, click **CloudDCN Subnets**.

        The **CloudDCN Subnets** page is displayed.

     ii. In the CloudDCN subnet list, locate the target subnet and click **Associate** under the **Network ACL** column.

        The **Associate Network ACL** page is displayed.

     iii. Select a network ACL dedicated for CloudDCN subnets.

        If no network ACL is available, click in the drop-down list to create one.

iv. Click **OK**.

The CloudDCN subnet list is displayed. You can view the associated network ACL of the subnet.

– Method 2

i. In the navigation pane on the left, choose **Access Control** > **Network ACLs**.

The Network ACL list is displayed.

ii. In the network ACL list, locate the target network ACL and click **Associate Subnet** in the **Operation** column.

The **Associated Subnets** tab is displayed.

iii. On the **Associated Subnets** tab, click **Associate**.

The **Associate Subnet** dialog box is displayed.

iv. In the **Associate Subnet** dialog box, select the CloudDCN subnet from the subnet list and click **OK**.

In the associated subnet list, you can view all the CloudDCN subnets associated with the network ACL.

NOTE

A CloudDCN subnet with a network ACL associated will not be displayed in the subnet list of the **Associate Subnet** dialog box for you to select. If you want to associate such a subnet with another network ACL, you must disassociate the subnet from the network ACL first.

5.2.5 Disassociating CloudDCN Subnets from a Network ACL

Scenarios

You can disassociate a CloudDCN subnet from a network ACL based on your network requirements.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking** > **Virtual Private Cloud**.

   The **Virtual Private Cloud** page is displayed.
4. Disassociate a subnet from a network ACL using the following methods:
   – Method 1

   i. In the navigation pane on the left, click **CloudDCN Subnets**.

   The **CloudDCN Subnets** page is displayed.

   ii. In the CloudDCN subnet list, locate the target subnet and click its name.

   The CloudDCN subnet details page is displayed.

   iii. In the upper right corner of the CloudDCN subnet details page, click **Disassociate** next to the network ACL.

A confirmation dialog box is displayed.

iv. Confirm the information and click **OK**.

On the subnet details page, you can see that no network ACL is associated with the CloudDCN subnet.

- Method 2

i. In the navigation pane on the left, click **CloudDCN Subnets**.

The **CloudDCN Subnets** page is displayed.

ii. In the CloudDCN subnet list, locate the target subnet and click the name of the network ACL under the **Network ACL** column.

The network ACL details page is displayed.

iii. Click the **Associated Subnets** tab, select one or more CloudDCN subnets, and click **Disassociate** in the **Operation** column.

A confirmation dialog box is displayed.

iv. Click **OK** in the displayed dialog box.

On the **Associated Subnets** tab, you cannot see the disassociated subnets in the subnet list.

- Method 3

i. In the navigation pane on the left, choose **Access Control** > **Network ACLs**.

The Network ACL list is displayed.

ii. In the network ACL list, locate the target network ACL and click **Associate Subnet** in the **Operation** column.

The **Associated Subnets** tab is displayed.

iii. Select one or more CloudDCN subnets and click **Disassociate**.

A confirmation dialog box is displayed.

iv. Click **OK** in the displayed dialog box.

On the **Associated Subnets** tab, you cannot see the disassociated subnets in the subnet list.

5.3 Elastic Network Interface and Supplementary Network Interface

5.3.1 Overview

Elastic Network Interface

An elastic network interface (referred to as a network interface in this documentation) is a virtual network card. Each iMetal server comes with a network interface, which cannot be detached.

Supplementary Network Interface

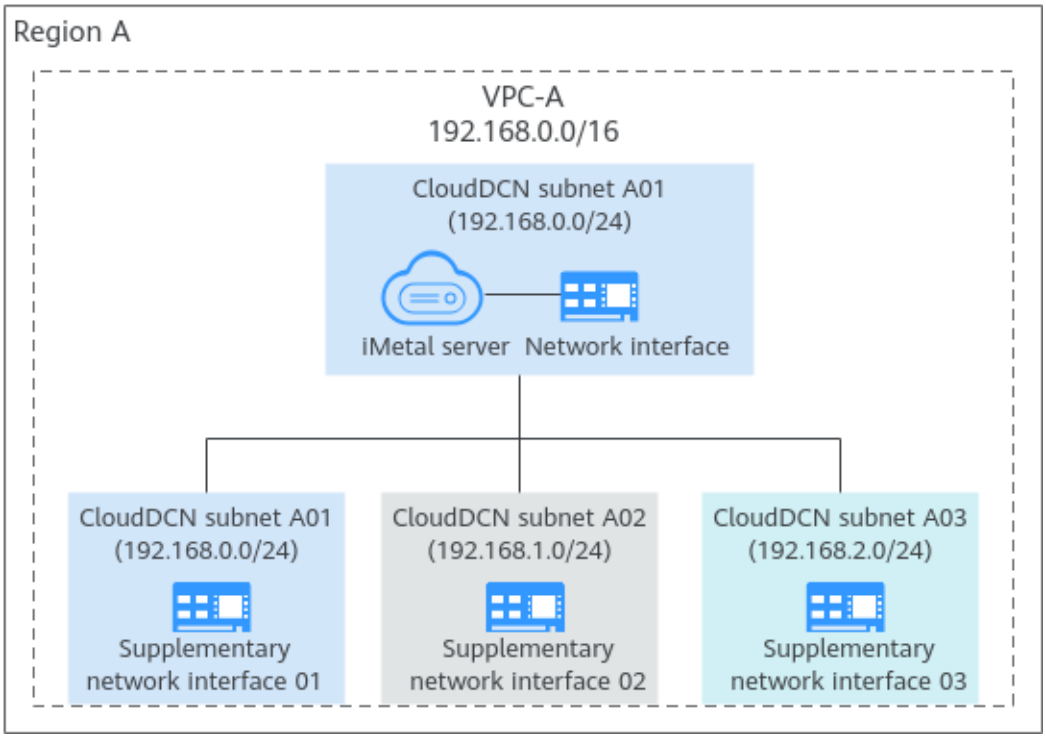
Supplementary network interfaces can be attached to VLAN sub-interfaces of network interfaces of an iMetal server for flexible and high-availability network configuration.

Application Scenario of Supplementary Network Interfaces

An iMetal server can have only one network interface. If you need more network interfaces, you can attach supplementary network interfaces to the network interface. These supplementary network interfaces can be in different subnets of the same VPC, each with a private IP address for internal communication.

Supplementary network interfaces are attached to VLAN sub-interfaces of network interfaces. **Figure 5-3** shows the networking diagram.

Figure 5-3 Supplementary network interface networking diagram



Constraints

- EIPs and virtual IP addresses cannot be bound to the network interfaces or supplementary network interfaces in a CloudDCN subnet.
- Security groups cannot be associated with supplementary network interfaces in a CloudDCN subnet.

5.3.2 Creating a Supplementary Network Interface

Scenarios

Supplementary network interfaces can be attached to network interfaces of an iMetal server for flexible and high-availability network configuration.

Constraints

- Supplementary network interfaces must be in the same VPC as the network interface they are attached to, but they can be in different subnets.
- After supplementary network interfaces are created, you need to create VLAN sub-interfaces on the network interface of the iMetal server and configure corresponding rules by referring to **Configuring a Supplementary Network Interface**.

Creating a Supplementary Network Interface

1. Go to the **supplementary network interface list page**.
2. In the upper right corner of the page, click **Create Supplementary Network Interface**.
3. Configure the parameters based on **Table 5-11**.

Table 5-11 Parameter descriptions

Parameter	Description	Example Value
Region	Region where the supplementary network interface will be created. Select the region nearest to you to ensure the lowest latency possible.	CN-Hong Kong
Network Interface	Network interface that you want the supplementary network interface to attach to. Select an elastic network interface from the drop-down list.	--(172.16.0.145)
VPC	VPC where the supplementary network interface will be created. The VPC of the network interface that the supplementary network interface is attached to is selected by default.	vpc-A
CloudDCN Subnet	CloudDCN subnet where the supplementary network interface will be created. The supplementary network interface and its network interface can be in different subnets.	subnet-clouddcn-01
Quantity	Number of supplementary network interfaces to be created.	1
Private IP Address	Whether to assign a private IPv4 address to the supplementary network interface. This parameter cannot be deselected in the current version.	-

Parameter	Description	Example Value
IPv4 Address	How a private IPv4 address will be assigned to the supplementary network interface. There are two options: • **Automatically assign IP address**: The system assigns an IP address from the subnet you have selected. • **Manually specify IP address**: You can specify an IP address. If you select **Manually specify IP address**, enter a private IPv4 address.	Automatically assign IP address
Description (Optional)	Description of the supplementary network interface. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-
Tag (Optional)	Optional Tags that are used to identify, classify, and search for supplementary network interfaces. For details, see **Managing Supplementary Network Interface Tags**.	**Tag key**: test **Tag value**: 01

4. Click **Create Now**.

NOTICE

To use a supplementary network interface, you need to create a VLAN sub-interface by referring to **Configuring a Supplementary Network Interface**.

Configuring a Supplementary Network Interface

After a supplementary network interface is created, you need to create a VLAN sub-interface for the network interface of the iMetal server and configure a private IP address and default routes for the supplementary network interface.

Before doing so, you need to obtain:

- The information described in **Table 5-12** when you configure a supplementary network interface for a Linux iMetal server.
- The information described in **Table 5-12** and **Table 5-13** when you configure a supplementary network interface for a Windows iMetal server.

Table 5-12 Information about the supplementary network interface and CloudDCN subnet

Item	How to Obtain
VLAN ID MAC address Private IP address	1. In the supplementary network interface list, click the private IP address of the target supplementary network interface. The **Summary** page is displayed. 2. On the displayed page, check and record the following information: • VLAN ID • MAC address • Private IP address
CloudDCN subnet mask Gateway address	1. In the supplementary network interface list, locate the target supplementary network interface and click the CloudDCN subnet name in the **Network** column. The **Summary** page of the subnet is displayed. 2. On the displayed page, check and record the following information: • CloudDCN subnet mask: subnet mask of the IPv4 CIDR block. For example, if the IPv4 CIDR block is 192.168.0.0/24, the mask is 24. • CloudDCN subnet gateway: In the **Gateway and DNS Information** area, check the gateway address.

Table 5-13 Information about the network interface and CloudDCN subnet to which the supplementary network interface belongs

Item	How to Obtain
Private IP address MAC address	1. In the iMetal server list, view and record the private IP address of the network interface. 2. On the **Network Interfaces** tab of the iMetal server details page, expand the details and view the MAC address.

Item	How to Obtain
CloudDCN subnet mask Gateway address	1. In the network interface list, locate the target network interface and click the CloudDCN subnet name in the **Network** column. The **Summary** page of the subnet is displayed. 2. On the displayed page, check and record the following information: • Subnet mask: subnet mask of the IPv4 CIDR block. For example, if the IPv4 CIDR block is 192.168.0.0/24, the mask is 24. • Subnet gateway: In the **Gateway and DNS Information** area, check the gateway address.

Configuring a Supplementary Network Interface for a Linux iMetal Server

The following describes how to create a VLAN sub-interface on the network interface of a Linux iMetal server. CentOS 7.8 is used as an example. In this example, the information about the supplementary network interface and CloudDCN subnet is as follows:

- VLAN ID: 1937
- MAC address: fa:16:3e:6d:c5:5a
- Private IP address: 192.168.0.149
- Subnet mask: 24
- Subnet gateway address: 192.168.0.1

1. Log in to the iMetal server.

   For details, see **iMetal Server Login Methods**.

2. Run the following command to view and record the network interface name of the iMetal server:

   ifconfig

   Information similar to the following is displayed. In this example, the network interface name is **eth0**.

```
[root@imetal-subeni-linux ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.125  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::f816:3eff:fe6d:c542  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:6d:c5:42  txqueuelen 1000  (Ethernet)
        RX packets 78131  bytes 111604802 (106.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8686  bytes 1422159 (1.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
...
```

3. Run the following command to create a VLAN sub-interface on the network interface:

   ip link add link *<network-interface-name>* **name** *<VLAN-sub-interface-name>* **type vlan id** *<VLAN-ID-of-the-supplementary-network-interface>*

   Variables in the preceding command are as follows:

- *network-interface-name*: the network interface name queried in **2**. In this example, the name is **eth0**.
- *VLAN-sub-interface-name*: Name the sub-interface in the format of *<network-interface-name>.<VLAN-ID-of-the-supplementary-network-interface>*. In this example, the VLAN sub-interface name is **eth0.1937**.
- *VLAN-ID-of-the-supplementary-network-interface*: In this example, the ID is **1937**.

Example command:

ip link add link eth0 name eth0.1937 type vlan id 1937

4. Run the following command to create a namespace:

   ip netns add *<namespace-name>*

   namespace-name: Name it in the format of **ns***<supplementary-network-interface-VLAN-ID>*. In this example, the name is **ns1937**.

   Example command:

   ip netns add ns1937

5. Run the following command to add the VLAN sub-interface to the namespace:

   ip link set *<VLAN-sub-interface-name>* **netns** *<namespace-name>*

   Example command:

   ip link set eth0.1937 netns ns1937

6. Run the following command to change the MAC address of the VLAN sub-interface to that of the supplementary network interface:

   ip netns exec *<namespace-name>* **ifconfig** *<VLAN-sub-interface-name>* **hw ether** *<MAC-address-of-the-supplementary-network-interface>*

   Example command:

   ip netns exec ns1937 ifconfig eth0.1937 hw ether fa:16:3e:6d:c5:5a

7. Run the following command to enable the VLAN sub-interface:

   ip netns exec *<namespace-name>* **ifconfig** *<VLAN-sub-interface-name>* **up**

   Example command:

   ip netns exec ns1937 ifconfig eth0.1937 up

8. Run the following command to configure a private IP address for the VLAN sub-interface:

   ip netns exec *<namespace-name>* **ip addr add** *<private-IP-address>* **dev** *<VLAN-sub-interface-name>*

   private-IP-address: private IP address of the supplementary network interface/subnet mask. In this example, the value is **192.168.0.149/24**.

   Example command:

   ip netns exec ns1937 ip addr add 192.168.0.149/24 dev eth0.1937

9. Run the following command to configure the default route for the VLAN sub-interface:

   ip netns exec *<namespace-name>* **ip route add default via** *<gateway-address-of-the-subnet-where-the-supplementary-network-interface-is-created>*

   Example command:

ip netns exec ns1937 ip route add default via 192.168.0.1

10. Check whether the supplementary network interface has worked.
    a. Run the following command to verify the connectivity between network interface **eth0** and the test iMetal server:

       ping *<private-IP-address-of-the-test-iMetal-server>*

       Plan the same VPC for the test iMetal server and the iMetal server with network interface **eth0** attached, so that the two iMetal servers can communicate with each other by default.

       Example command:

       ping 192.168.0.133

       If information similar to the following is displayed, the two iMetal servers can communicate with each other. If the communication is normal, proceed with **10.b**.

       ```
       [root@imetal-subeni-linux ~]# ping 192.168.0.133
       PING 192.168.0.133 (192.168.0.133) 56(84) bytes of data.
       64 bytes from 192.168.0.133: icmp_seq=1 ttl=64 time=0.302 ms
       64 bytes from 192.168.0.133: icmp_seq=2 ttl=64 time=0.262 ms
       ...
       --- 192.168.0.133 ping statistics ---
       2 packets transmitted, 2 received, 0% packet loss, time 999ms
       rtt min/avg/max/mdev = 0.262/0.282/0.302/0.020 ms
       ```

    b. Run the following command to verify the connectivity between the supplementary network interface and the test iMetal server.

       ip netns exec *<namespace-name>* **ping** *<private-IP-address-of-the-test-iMetal-server>*

       Plan the same VPC for the test iMetal server and the iMetal server that the supplementary network interface is attached to, so that the two iMetal servers can communicate with each other by default.

       Example command:

       ip netns exec ns1937 ping 192.168.0.133

       If information similar to the following is displayed, the two iMetal servers can communicate with each other. This means the supplementary network interface has worked.

       ```
       [root@imetal-subeni-linux ~]# ip netns exec ns1937 ping 192.168.0.133
       PING 192.168.0.133 (192.168.0.133) 56(84) bytes of data.
       64 bytes from 192.168.0.133: icmp_seq=1 ttl=64 time=0.420 ms
       64 bytes from 192.168.0.133: icmp_seq=2 ttl=64 time=0.233 ms
       ...
       --- 192.168.0.133 ping statistics ---
       2 packets transmitted, 2 received, 0% packet loss, time 999ms
       rtt min/avg/max/mdev = 0.233/0.326/0.420/0.095 ms
       ```

NOTICE

The route configured above is a temporary route that is applied once configured, and will be lost once the iMetal server is restarted. To avoid network disruptions, take step **11** to configure permanent routes instead.

11. Configure a permanent route for the supplementary network interface.
    a. Run the following command to open the **/etc/rc.local** file:

       vi /etc/rc.local

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

c. Add the following content to the end of the file.

The parameters and values must be the same as those in steps **3** to **9**.

```
ip link add link eth0 name eth0.1937 type vlan id 1937
ip netns add ns1937
ip link set eth0.1937 netns ns1937
ip netns exec ns1937 ifconfig eth0.1937 hw ether fa:16:3e:6d:c5:5a
ip netns exec ns1937 ifconfig eth0.1937 up
ip netns exec ns1937 ip addr add 192.168.0.149/24 dev eth0.1937
ip netns exec ns1937 ip route add default via 192.168.0.1
```

d. Press **ESC** to exit and enter **:wq!** to save the configuration.

e. Run the following command to assign execute permissions to the **/etc/rc.local** file:

chmod +x /etc/rc.local

NOTE

If your operating system is Red Hat or EulerOS, run the following command after you perform **11.e**:

chmod +x /etc/rc.d/rc.local

f. Run the following command to restart the iMetal server:

reboot

g. Check whether the permanent route has worked by referring to **10**.

Configuring a Supplementary Network Interface for a Windows iMetal Server

The following describes how to create a VLAN sub-interface on the network interface of a Windows iMetal server. Windows Server 2019 Standard 64bit is used as an example. In this example, the information about the supplementary network interface, primary network interface, and CloudDCN subnet is as follows:

- Supplementary network interface
  - VLAN ID: 2242
  - MAC address: fa:16:3e:6d:c5:db
  - Private IP address: 192.168.0.22
  - Subnet mask: 24 (255.255.255.0)
  - Subnet gateway address: 192.168.0.1
- Network interface
  - MAC address: fa:16:3e:6d:c5:d5
  - Private IP address: 192.168.0.16
  - Subnet mask: 24 (255.255.255.0)
  - Subnet gateway address: 192.168.0.1

NOTE

This example describes how to configure the supplementary network interface for the primary network interface of an ECS. If you want to do the same thing for the extended network interface of the ECS, follow the similar steps.

1. Login to the iMetal server.

   For details, see **iMetal Server Login Methods**.

2. Enter **Windows PowerShell** in the search box in the lower left corner of the desktop and press **Enter**.
3. On the displayed window, run the following command to query the Ethernet adapter information of the network interface:

   ipconfig

   Information similar to the following is displayed. In this example, the Ethernet adapter name is **tap7888b905-ee**.

   ```
   Windows PowerShell
   Copyright (C) Microsoft Corporation. All rights reserved.

   PS C:\Users\Administrator> ipconfig

   Windows IP Configuration


   Ethernet adapter tap7888b905-ee:

      Connection-specific DNS Suffix  . : openstacklocal
      Link-local IPv6 Address . . . . . : fe80::1e55:468d:da2a:e16%3
      IPv4 Address. . . . . . . . . . . : 192.168.0.16
      Subnet Mask . . . . . . . . . . . : 255.255.255.0
      Default Gateway . . . . . . . . . : 192.168.0.1
   ```

4. Create a bond group.
   a. Run the following command to create a bond group for the custom VLAN:

      New-NetLbfoTeam -Name *<bond-group-name>* **-TeamMembers "***<Ethernet-adapter-name-of-the-network-interface>***" -TeamingMode SwitchIndependent -LoadBalancingAlgorithm IPAddresses -Confirm:$false**

      Variables in the preceding command are as follows:

      - *bond-group-name*: the bond group name of the custom VLAN. In this example, the bond group name is **Team1**.
      - *Ethernet-adapter-name-of-the-network-interface*: information queried in **3**. In this example, the name is **tap7888b905-ee**.

      Example command:

      New-NetLbfoTeam -Name Team1 -TeamMembers "tap7888b905-ee" -TeamingMode SwitchIndependent -LoadBalancingAlgorithm IPAddresses -Confirm:$false

      Information similar to the following is displayed:

      ```
      PS C:\Users\Administrator> New-NetLbfoTeam -Name Team1 -TeamMembers "tap7888b905-ee" -TeamingMode SwitchIndependent -LoadBalancingAlgorithm IPAddresses -Confirm:$false


      Name                   : Team1
      Members                : tap7888b905-ee
      TeamNics               : Team1
      TeamingMode            : SwitchIndependent
      LoadBalancingAlgorithm : IPAddresses
      Status                 : Up
      ```

   b. Run the following commands to query the bond group you have created:

      Get-NetLbfoTeamMember

      Information similar to the following is displayed:


```
PS C:\Users\Administrator> Get-NetLbfoTeamMember


Name                      : tap7888b905-ee
InterfaceDescription      : Red Hat VirtIO Ethernet Adapter
Team                      : Team1
AdministrativeMode        : Active
OperationalStatus         : Active
TransmitLinkSpeed(Gbps)   : 100
ReceiveLinkSpeed(Gbps)    : 100
FailureReason             : NoFailure
```

Get-NetAdapter

Information similar to the following is displayed:

```
PS C:\Users\Administrator> Get-NetAdapter

Name                      InterfaceDescription                ifIndex Status       MacAddress             LinkSpeed
----                      --------------------                ------- ------       ----------             ---------
Team1                     Microsoft Network Adapter Multiplexo...       9 Up           FA-16-3E-6D-C5-D5      100 Gbps
tap7888b905-ee            Red Hat VirtIO Ethernet Adapter               3 Up           FA-16-3E-6D-C5-D5      100 Gbps
```

5. Configure a custom VLAN network.

   a. Run the following command to create a VLAN sub-interface:

   Add-NetLbfoTeamNIC -Team "*<bond-group-name>***" -VlanID** *<VLAN-ID-of-the-supplementary-network-interface>* **-Confirm:$false**

   Example command:

   Add-NetLbfoTeamNIC -Team "Team1" -VlanID 2242 -Confirm:$false

   Information similar to the following is displayed:

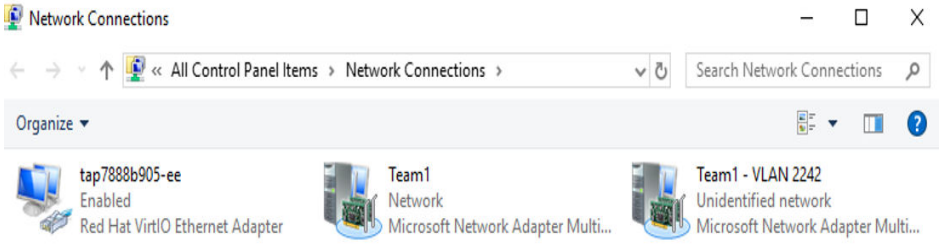
```
PS C:\Users\Administrator> Add-NetLbfoTeamNIC -Team "Team1" -VlanID 2242 -Confirm:$false


Name                      : Team1 - VLAN 2242
InterfaceDescription      : Microsoft Network Adapter Multiplexor Driver #2
Team                      : Team1
VlanID                    : 2242
Primary                   : False
Default                   : False
TransmitLinkSpeed(Gbps)   : 100
ReceiveLinkSpeed(Gbps)    : 100
```

   b. Run the following command to open the **Network Connections** page:

   ncpa.cpl

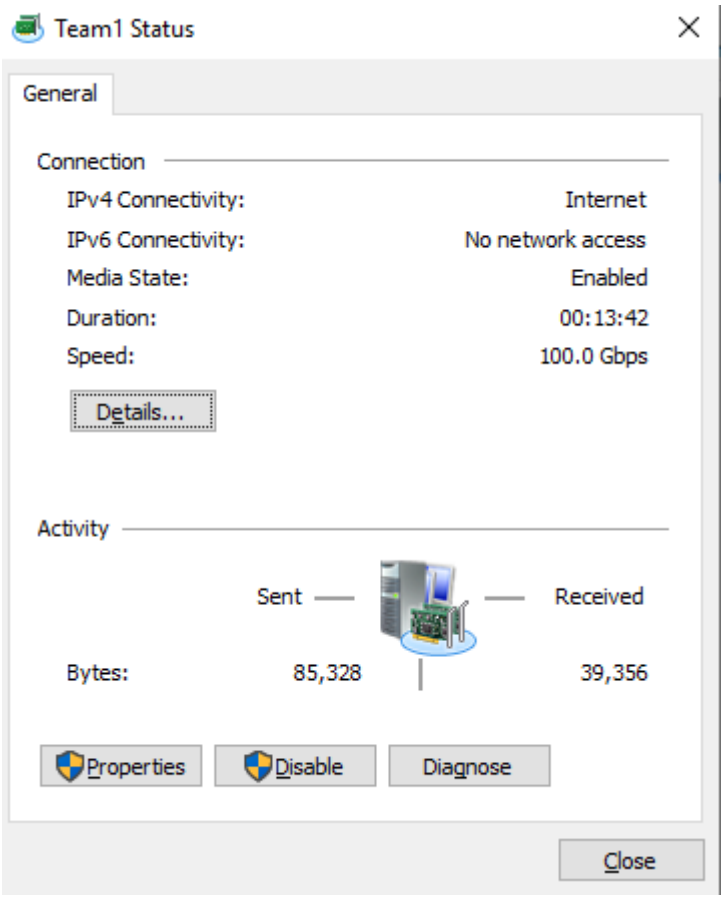
   On the displayed page, **Team1** is the bond group created in **4.a**, and **Team1 – VLAN 2242** is the VLAN sub-interface created in **5.a**.



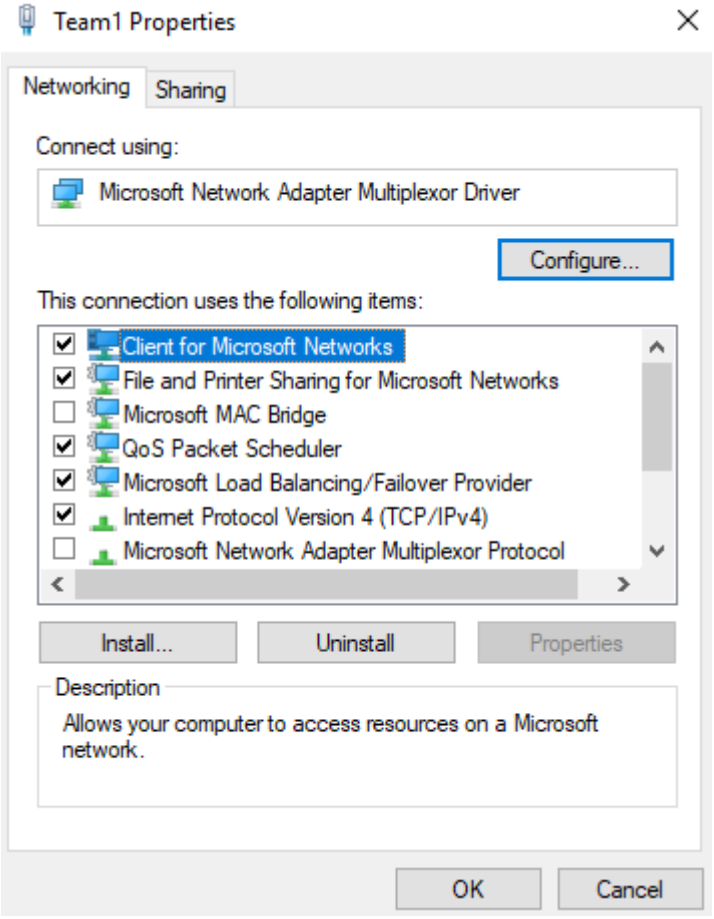
6. Configure the network for the network interface.

   a. On the **Network Connections** page, double-click **Team1**.

   The **Team1 Status** page is displayed.

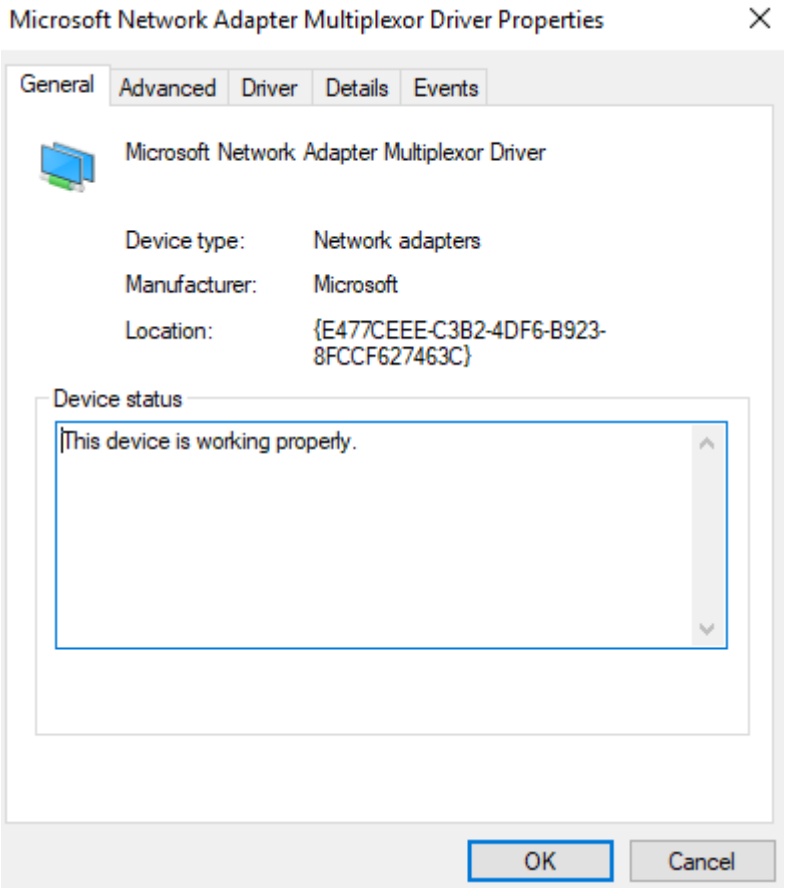


b. On the **Team1 Status** page, click **Properties**.
The **Team1 Properties** page is displayed.



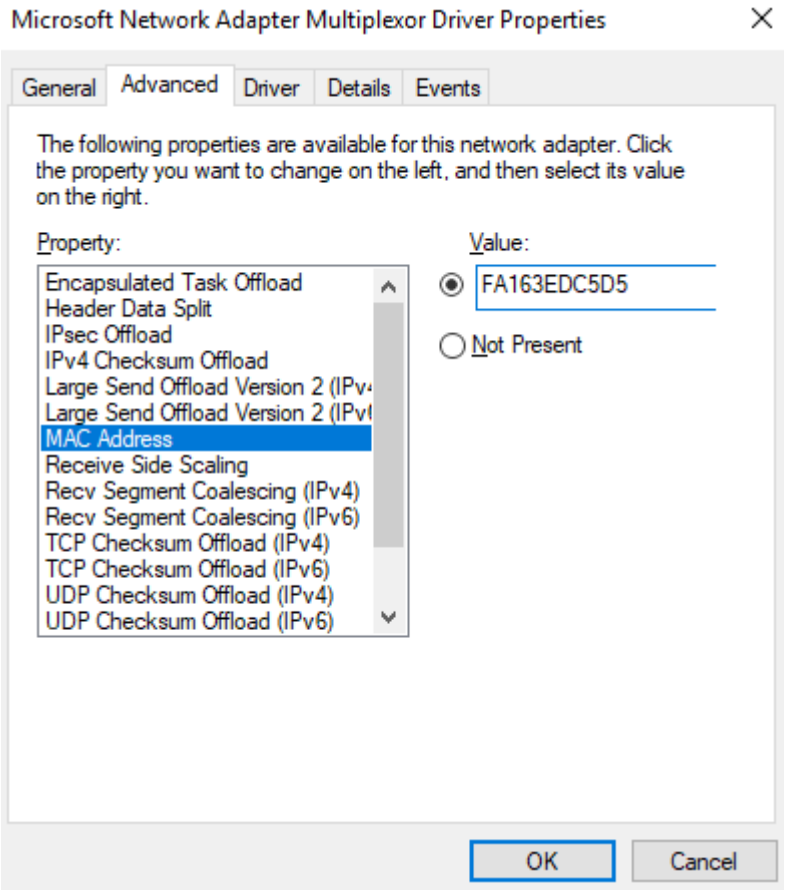
c. On the **Team1 Properties** page, click **Configure...**.

The **Microsoft Network Adapter Multiplexor Driver Properties** page is displayed.



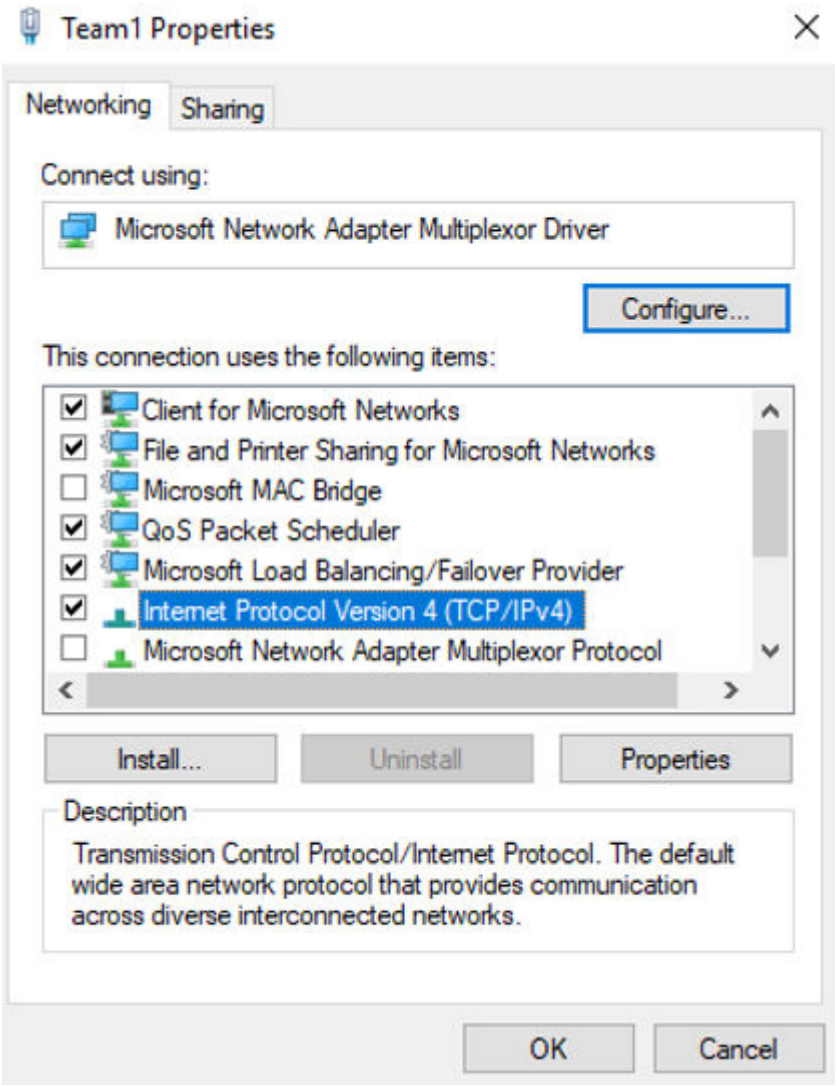
d. On the **Microsoft Network Adapter Multiplexor Driver Properties** page, choose the **Advanced** tab, click **MAC Address**, enter the MAC address of the network interface, and click **OK**.

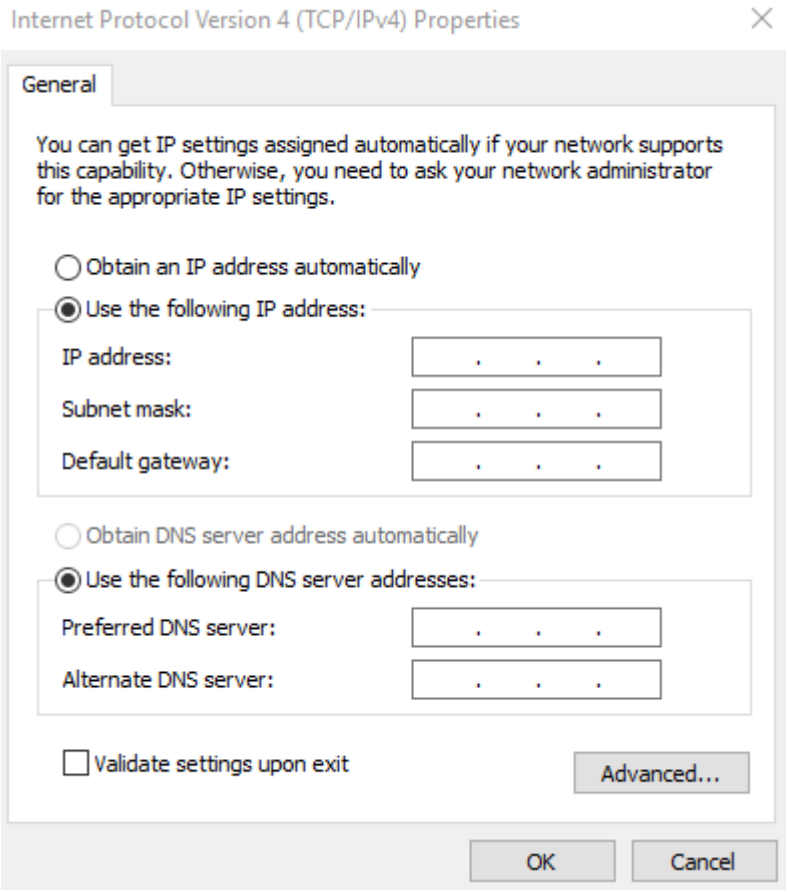
   When entering the MAC address, remove the colons (:) and use the uppercase letters. For example, if the MAC address of the network interface is **fa:16:3e:6d:c5:d5**, enter **FA163E6DC5D5**.



e. Return to the **Team1 Properties** page, double-click **Internet Protocol Version 4 (TCP/IPv4)**.

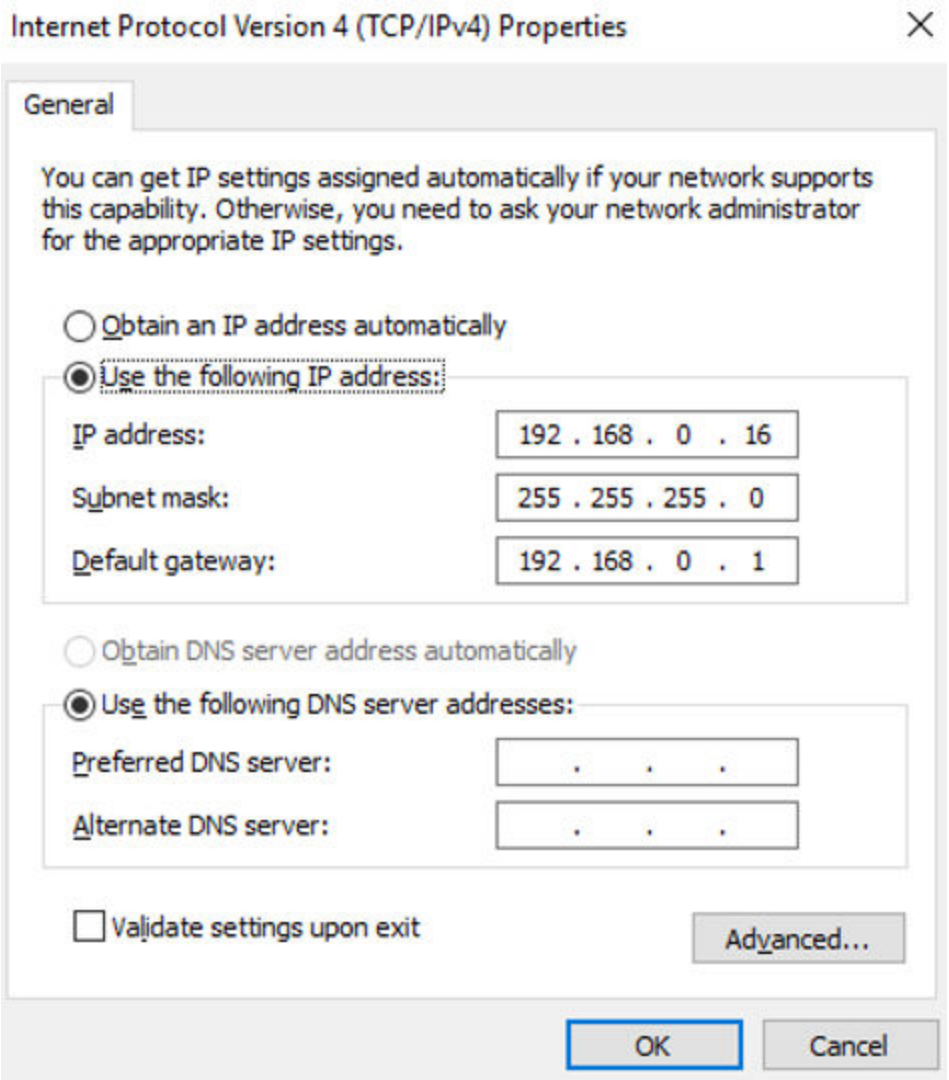
   The **Internet Protocol Version 4 (TCP/IPv4) Properties** page is displayed.



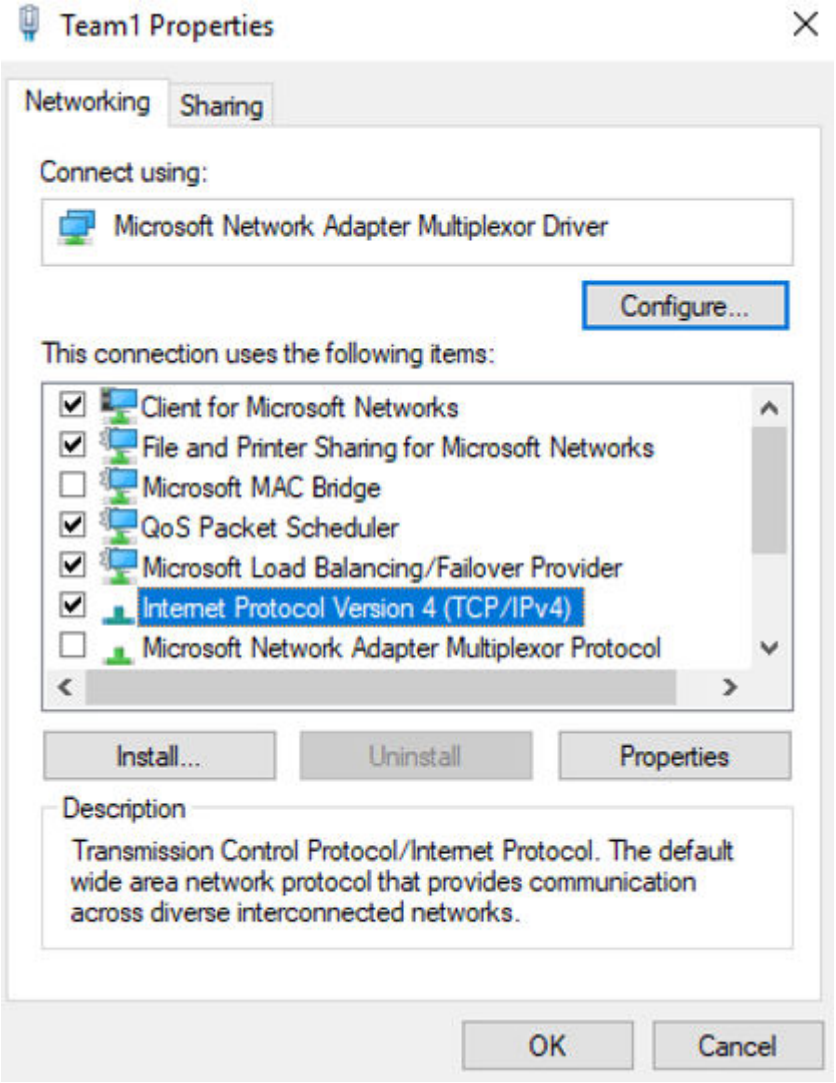


f. On the **Internet Protocol Version 4 (TCP/IPv4) Properties** page, configure the network information of the network interface and click **OK**.

- Select **Use the following IP address:**.
- **IP address**: Enter the private IP address of the network interface. In this example, the private IP address is **192.168.0.16**.
- **Subnet mask**: Enter the mask of the subnet where the network interface is created. In this example, the mask is **255.255.255.0**.
- **Default gateway**: Enter the gateway of the subnet where the network interface is created. In this example, the gateway is **192.168.0.1**.



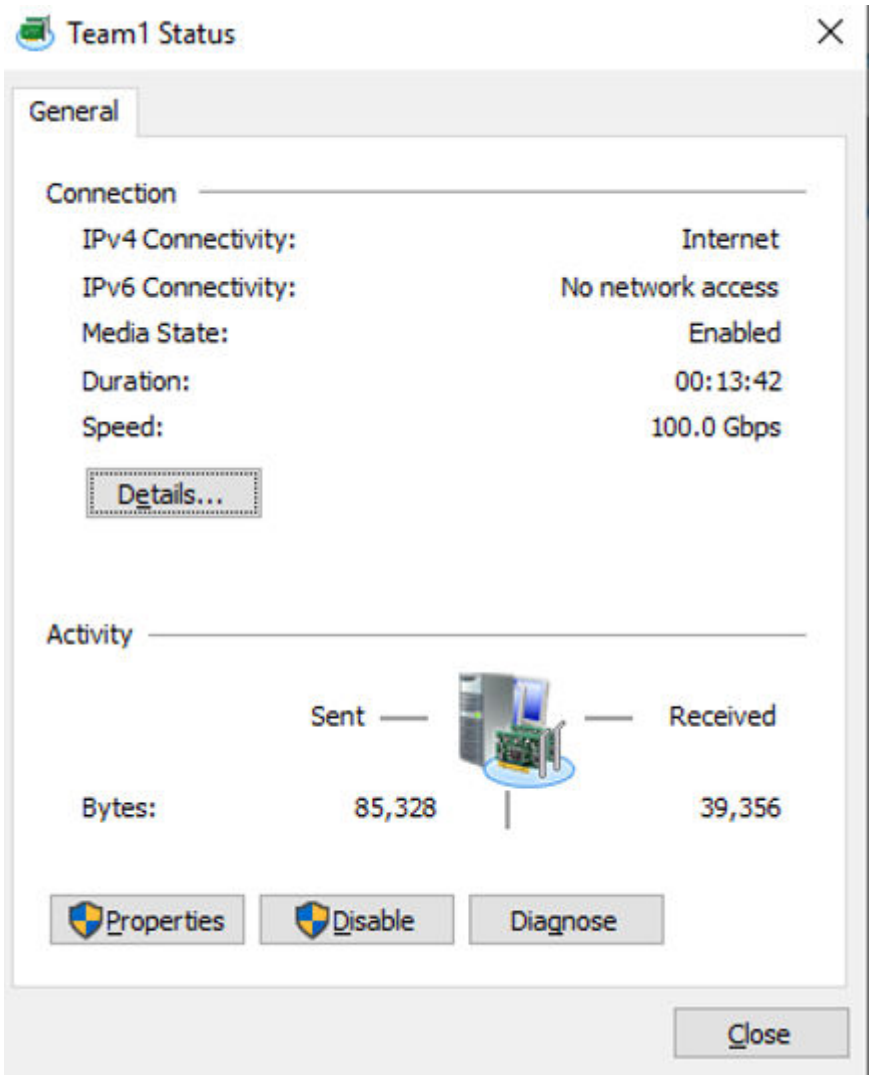
g. On the **Team1 Properties** page, click **OK** to save the settings.

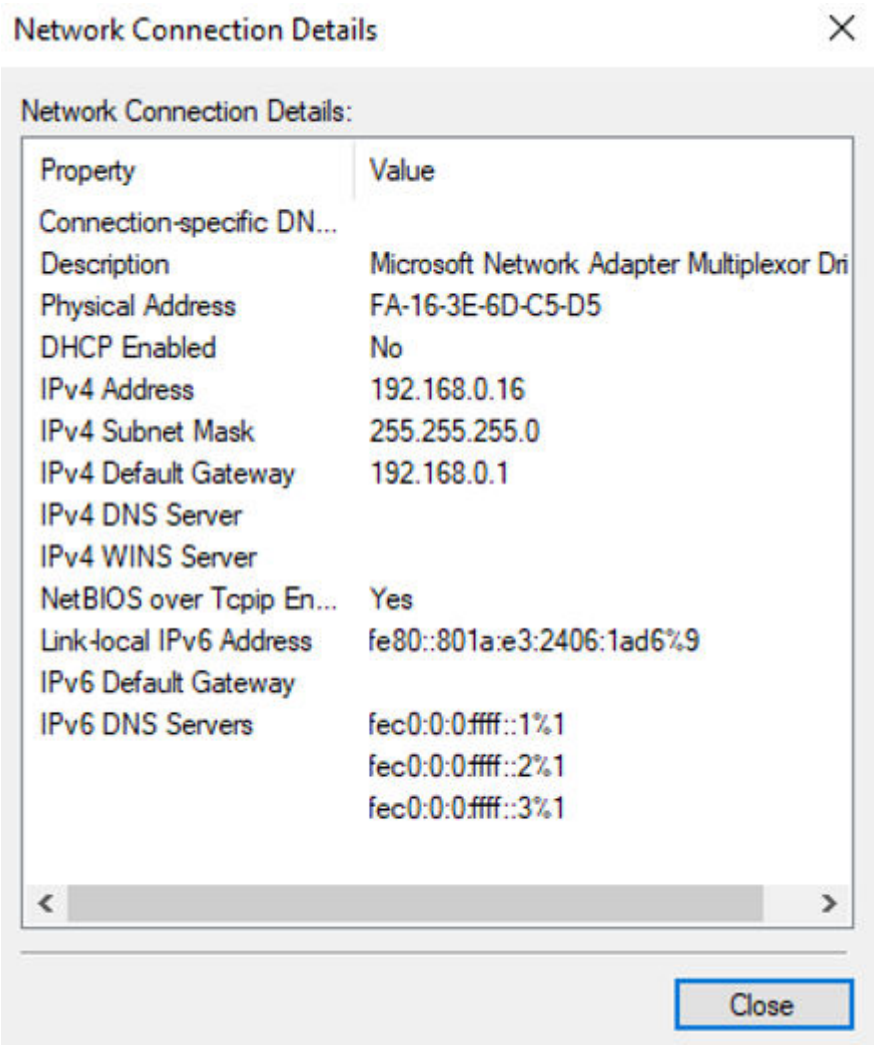


h. Return to the **Team1 Status** page and click **Details...**.

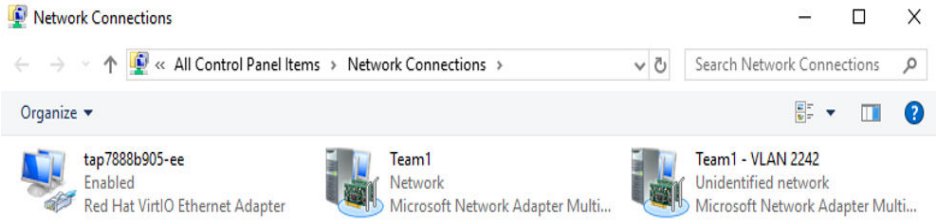
On the **Network Connection Details** page, check whether the following information is correctly configured:

- **Physical Address**: MAC address of the network interface.
- **IPv4 Address**: the private IP address of the network interface.
- **IPv4 Subnet Mask**: the mask of the subnet where the network interface is created.
- **IPv4 Default Gateway**: the gateway of the subnet where the network interface is created.

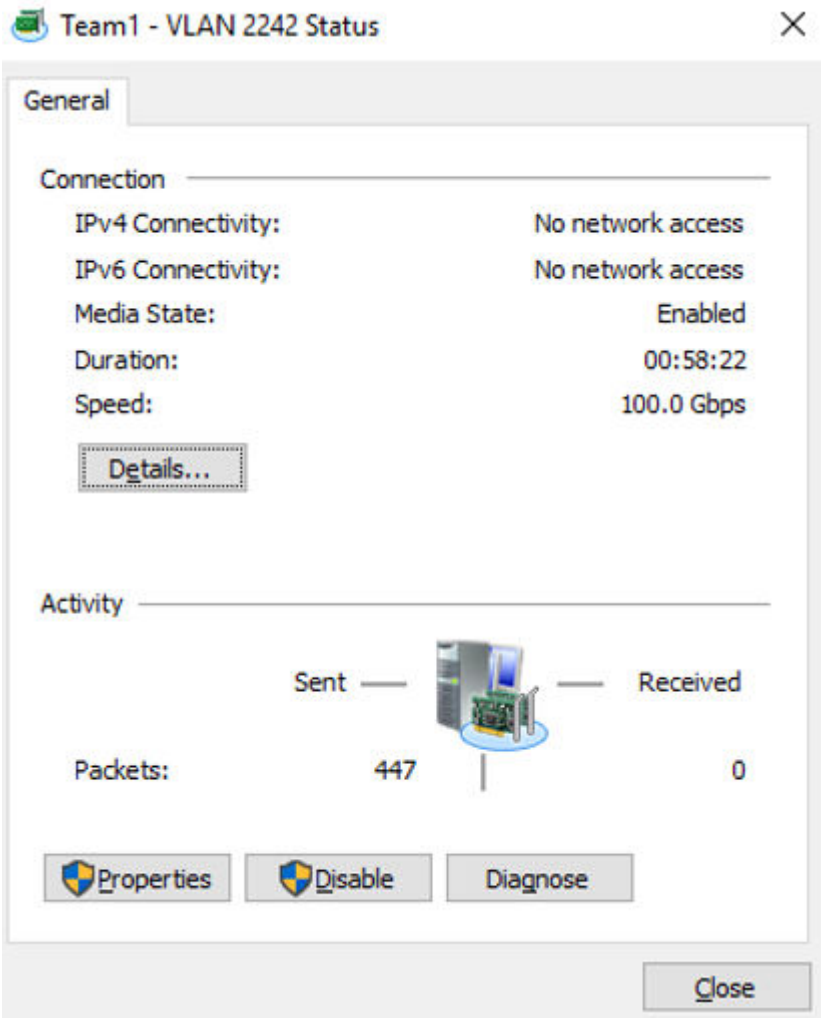




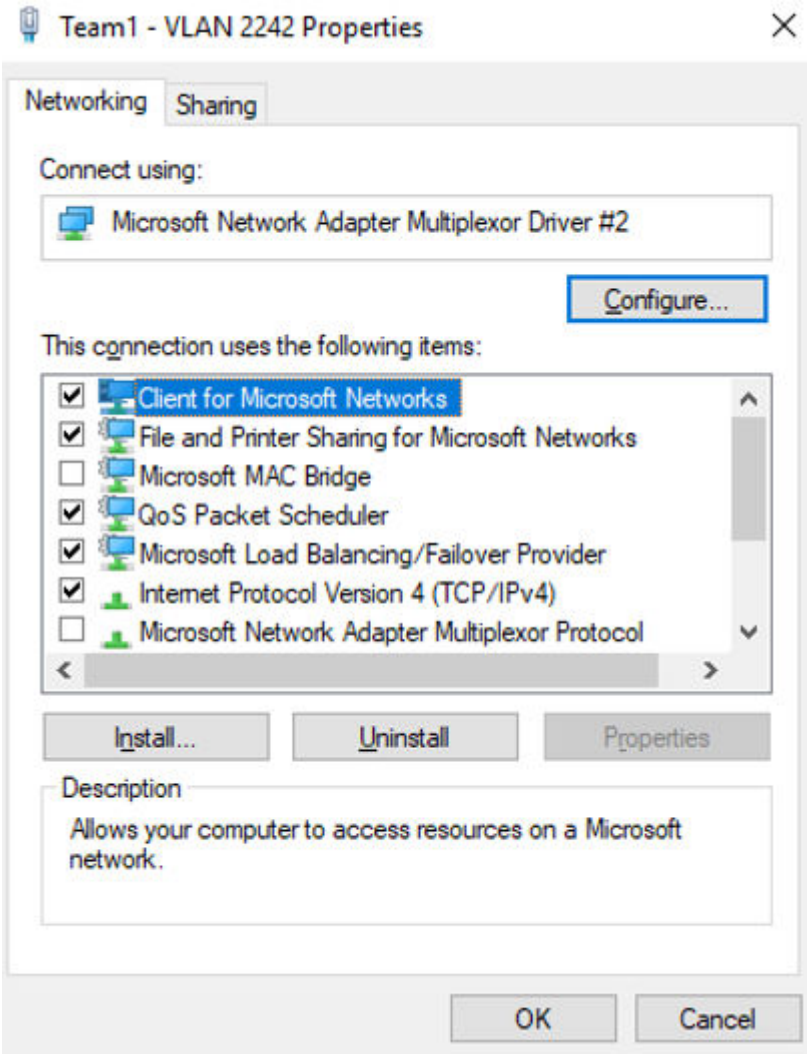
i. Check the settings and click **Close**.
The **Network Connections** page is displayed.



7. Configure the network for the supplementary network interface.
   a. On the **Network Connections** page, double-click **Team1 - VLAN 2242**.
   The **Team1 - VLAN 2242 Status** page is displayed.

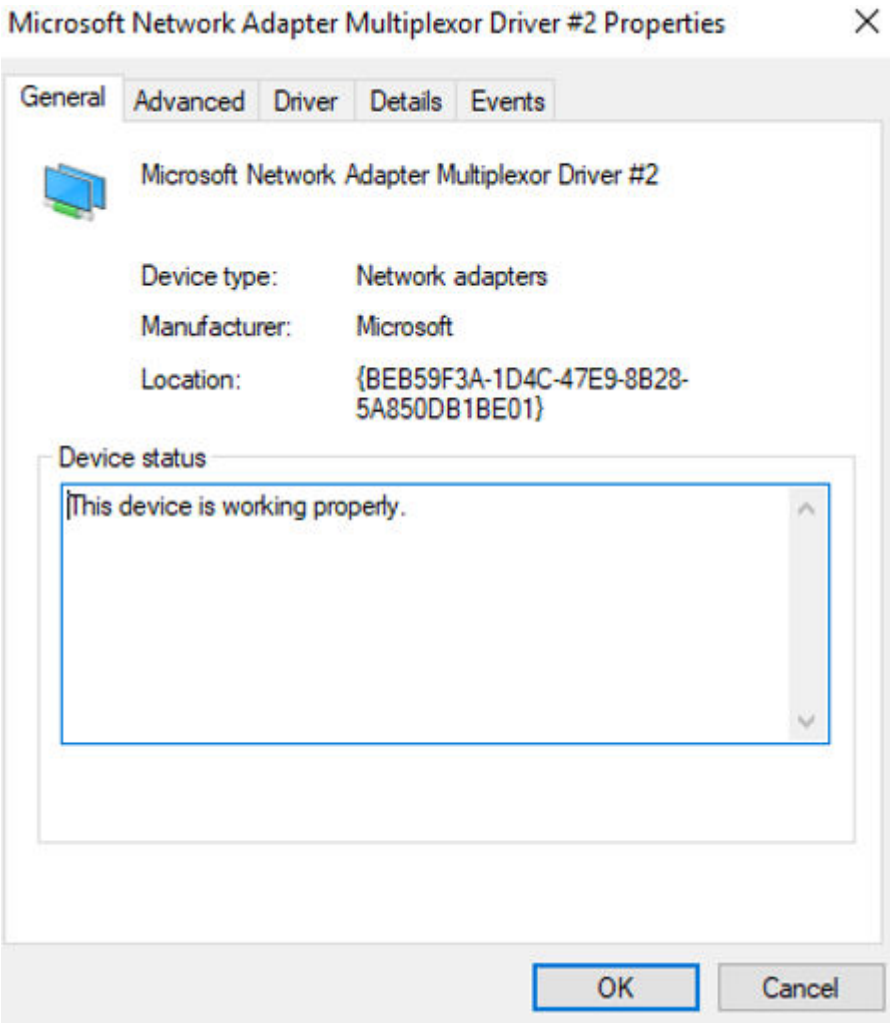


b. On the **Team1 - VLAN 2242 Status** page, click **Properties**.
The **Team1 - VLAN 2242 Properties** page is displayed.



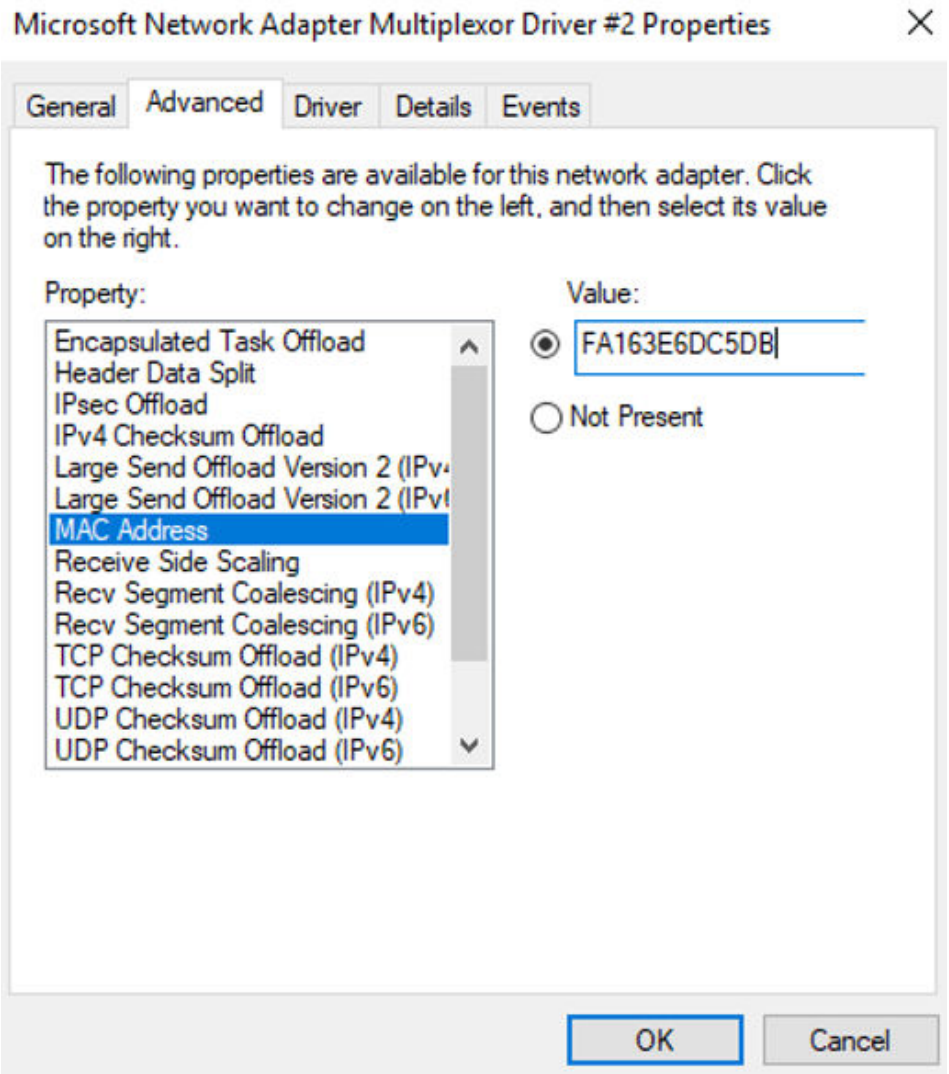
c. On the **Team1 - VLAN 2242 Properties** page, click **Configure...**.

The **Microsoft Network Adapter Multiplexor Driver #2 Properties** page is displayed.



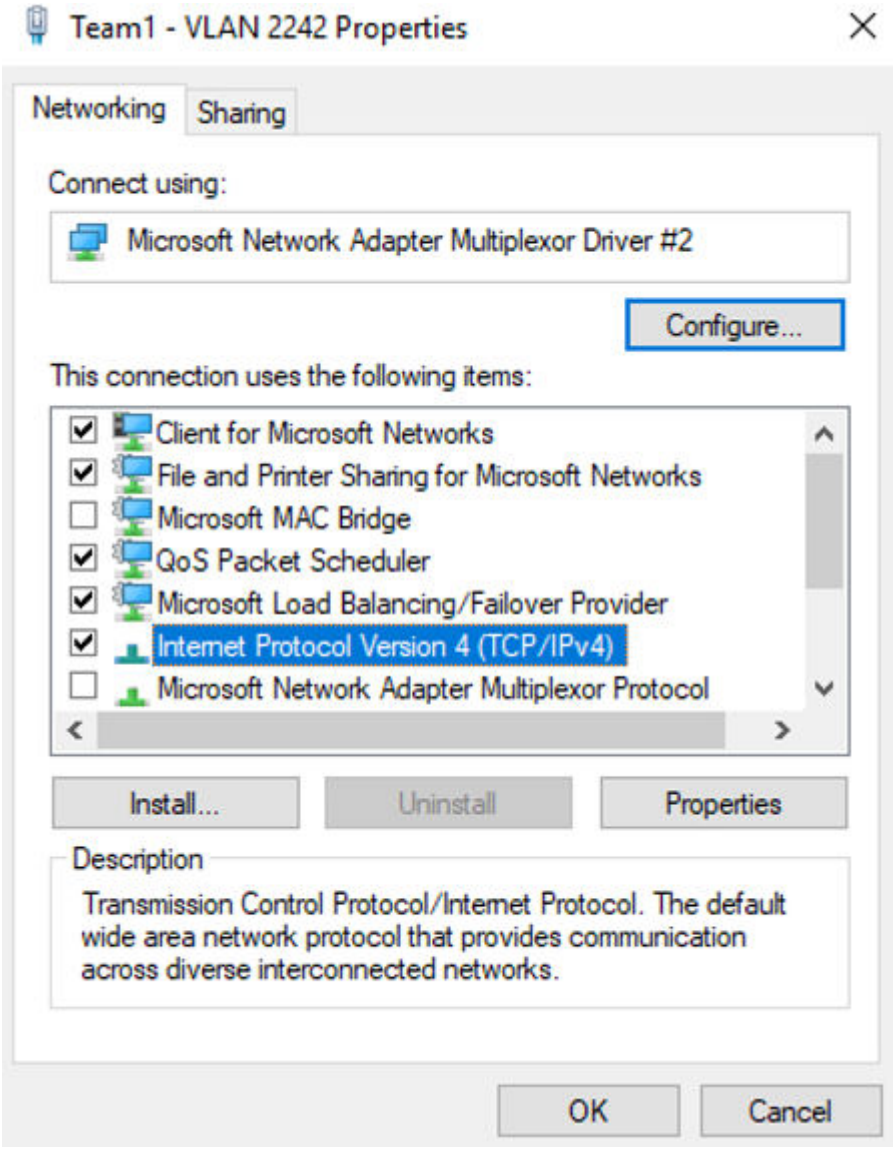
d. On the **Microsoft Network Adapter Multiplexor Driver #2 Properties** page, choose the **Advanced** tab, click **MAC Address**, enter the MAC address of the supplementary network interface, and click **OK**.

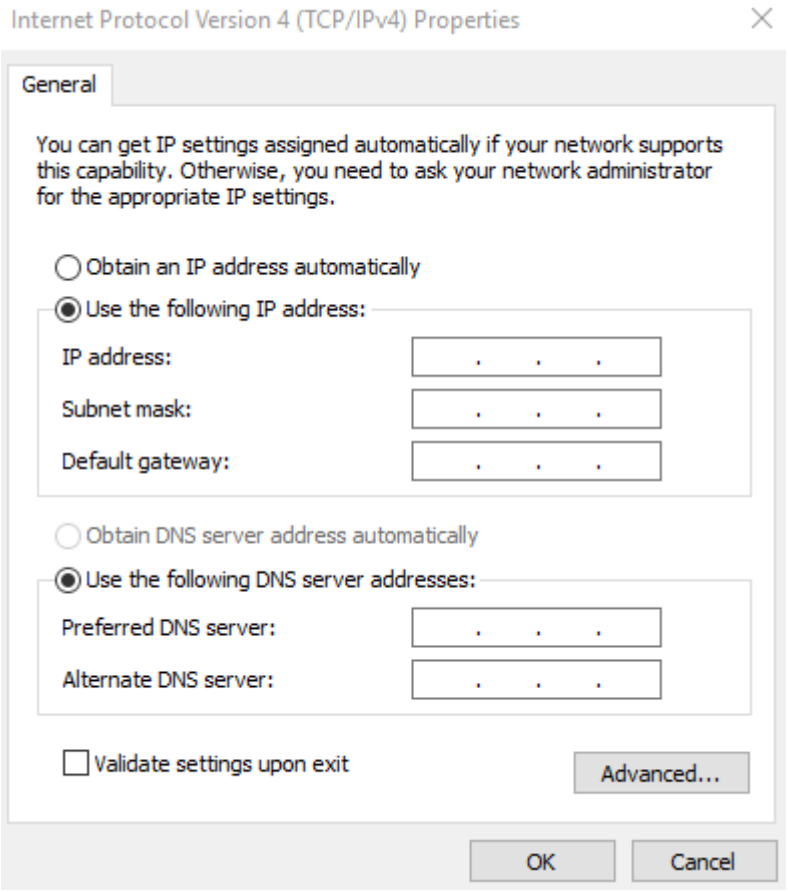
   When entering the MAC address, remove the colons (:) and use the uppercase letters. For example, if the MAC address of the supplementary network interface is **fa:16:3e:6d:c5:db**, enter **FA163E6DC5DB**.



e. Return to the **Team1 - VLAN 2242 Properties** page, double-click **Internet Protocol Version 4 (TCP/IPv4)**.

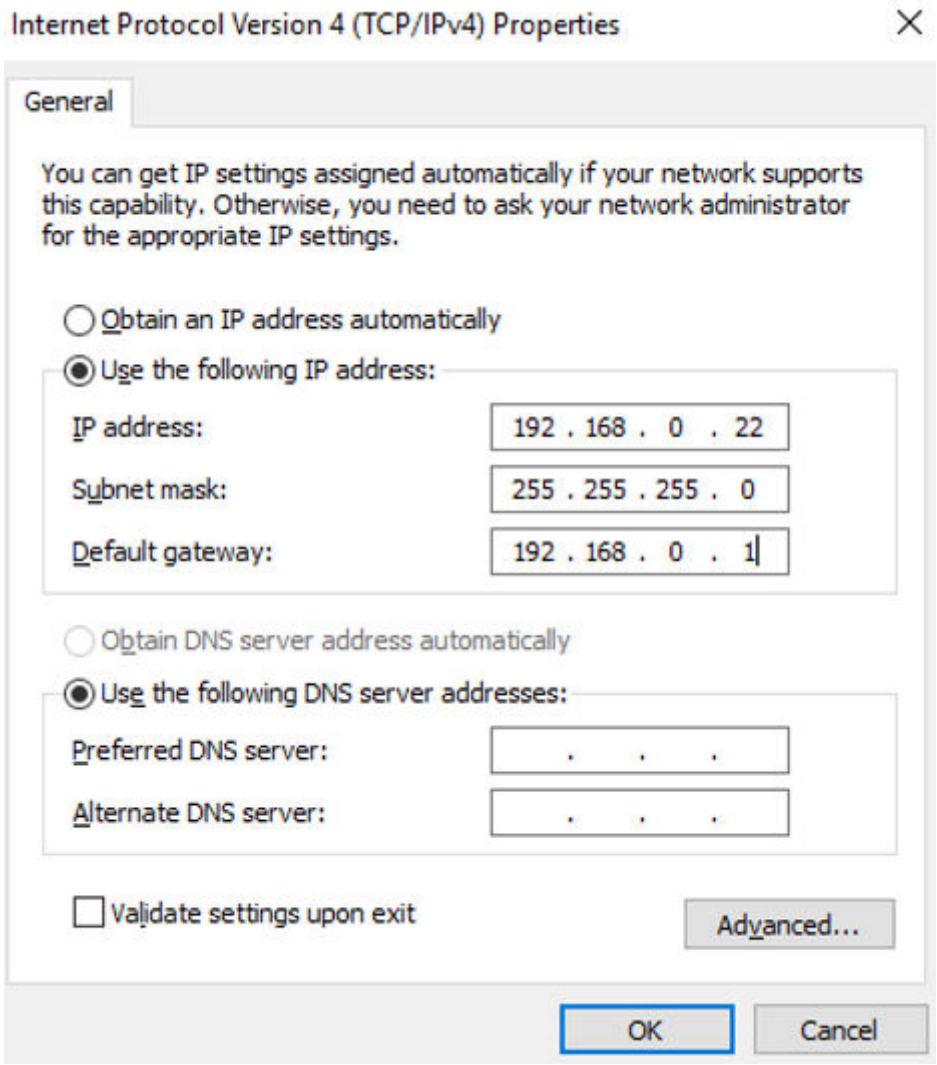
   The **Internet Protocol Version 4 (TCP/IPv4) Properties** page is displayed.



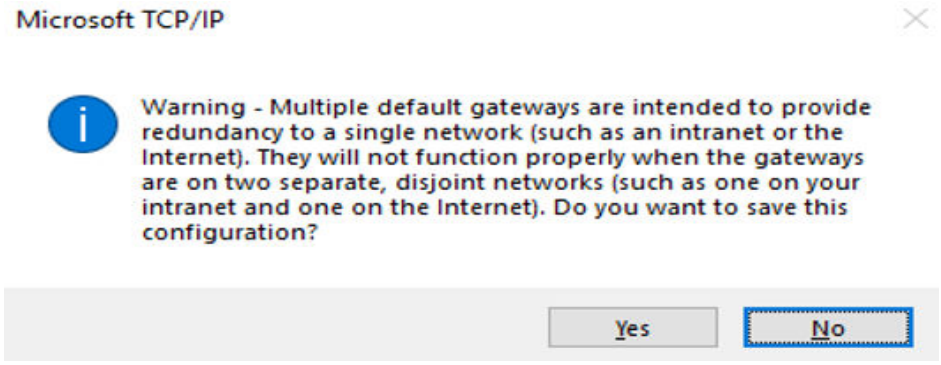


f. On the **Internet Protocol Version 4 (TCP/IPv4) Properties** page, configure the network information of the supplementary network interface and click **OK**.

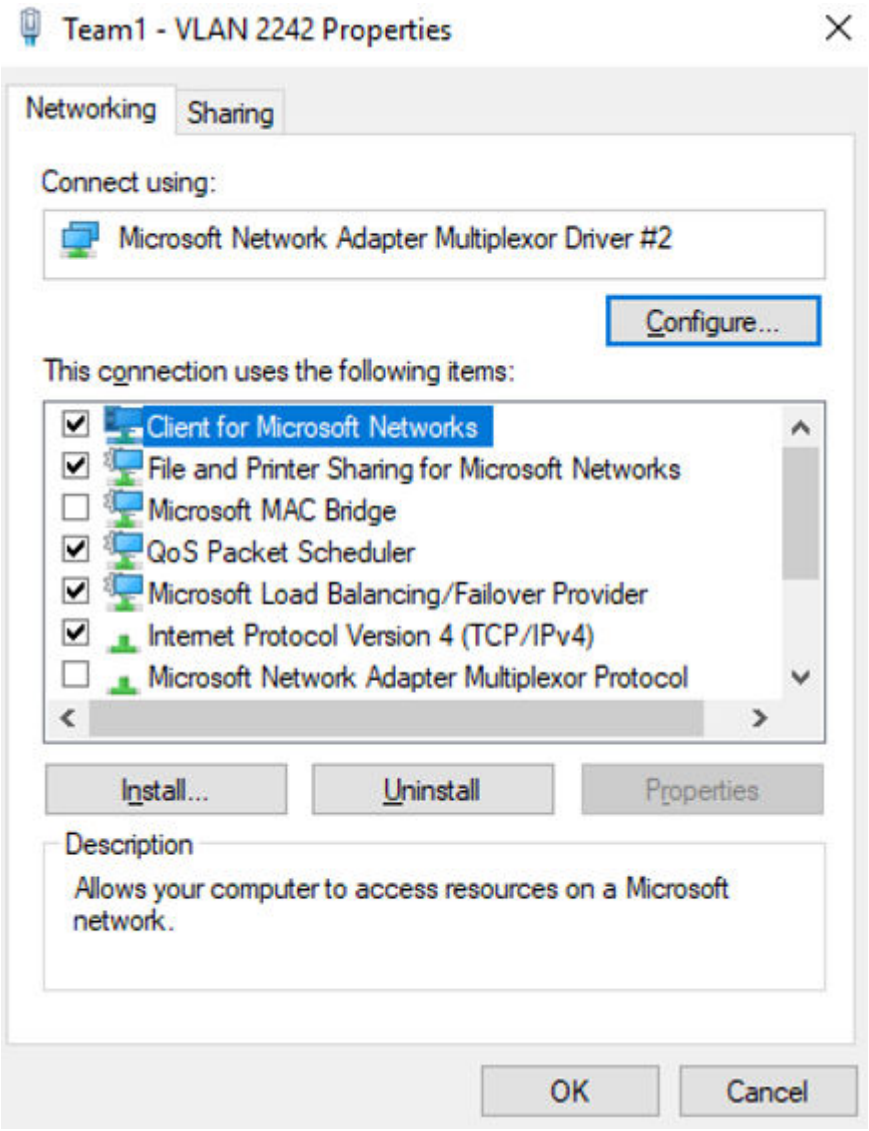
- Select **Use the following IP address:**.
- **IP address**: Enter the private IP address of the supplementary network interface. In this example, the private IP address is **192.168.0.22**.
- **Subnet mask**: Enter the mask of the subnet where the supplementary network interface is created. In this example, the mask is **255.255.255.0**.
- **Default gateway**: Enter the gateway of the subnet where the supplementary network interface is created. In this example, the gateway is **192.168.0.1**.



If the following warning is displayed, click **Yes** to close the dialog box.



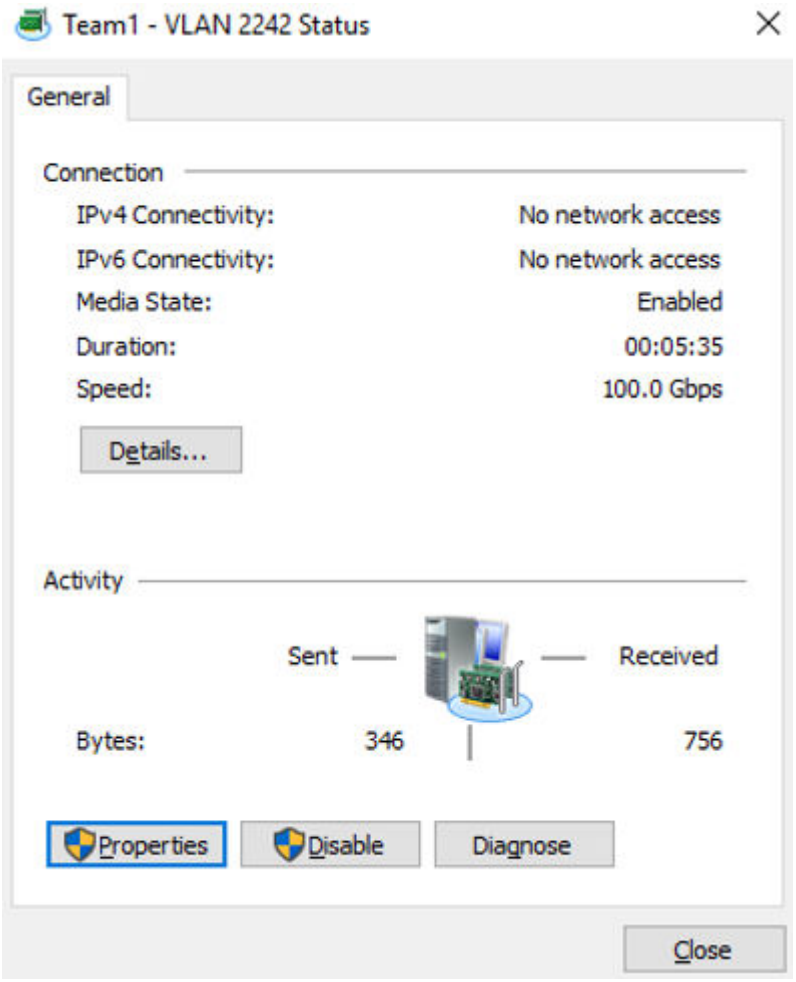
g. On the **Team1 - VLAN 2242 Properties** page, click **OK** to save the settings.

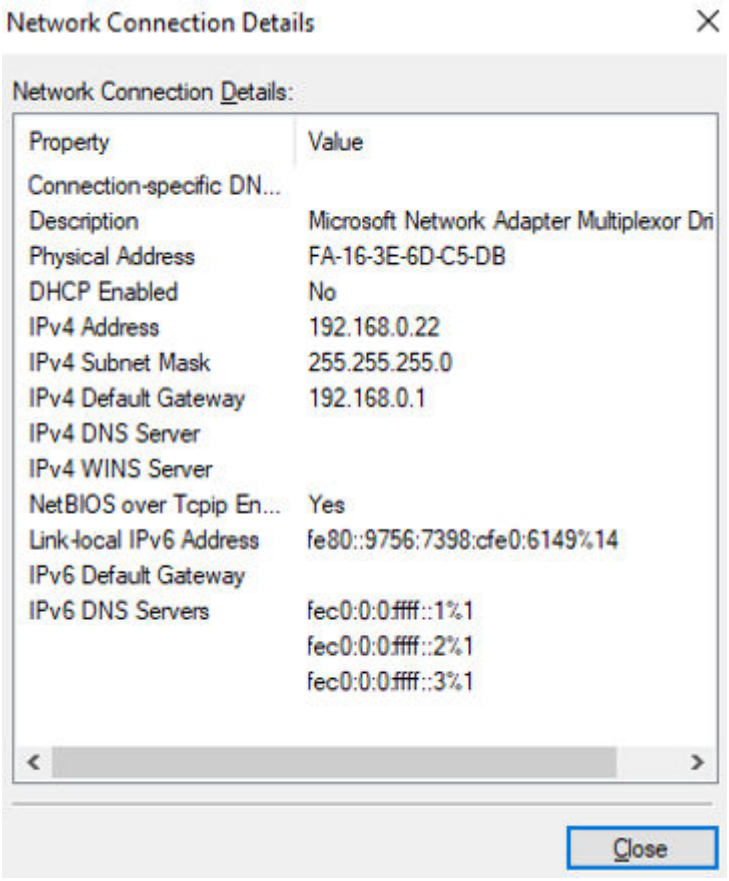


h. Return to the **Team1 - VLAN 2242 Status** page and click **Details...**.

On the **Network Connection Details** page, check whether the following information is correctly configured:

- **Physical Address**: MAC address of the supplementary network interface.
- **IPv4 Address**: the private IP address of the supplementary network interface.
- **IPv4 Subnet Mask**: the mask of the subnet where the supplementary network interface is created.
- **IPv4 Default Gateway**: the gateway of the subnet where the supplementary network interface is created.





i. Check the settings and click **Close**.

8. On the Windows PowerShell CLI page, check whether the network interface and supplementary network interface are connected to the test iMetal server.

   a. Run the following command to verify the network connectivity between the network interface and the test iMetal server.

      Ping *<private-IP-address-of-the-test-iMetal-server>* **-S** *<private-IP-address-of-the-network-interface>*

      Plan the same VPC for the test iMetal server and the iMetal server that the network interface is attached to, so that the two iMetal servers can communicate with each other by default.

      Example command:

      Ping 192.168.0.133 -S 192.168.0.16

      If information similar to the following is displayed, the two iMetal servers can communicate with each other.

```
PS C:\Users\Administrator> Ping 192.168.0.133 -S 192.168.0.16

Pinging 192.168.0.133 from 192.168.0.16 with 32 bytes of data:
Reply from 192.168.0.133: bytes=32 time=1ms TTL=64
Reply from 192.168.0.133: bytes=32 time<1ms TTL=64
Reply from 192.168.0.133: bytes=32 time<1ms TTL=64
Reply from 192.168.0.133: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.133:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```


b. Run the following command to verify the connectivity between the supplementary network interface and the test iMetal server.

Ping *<private-IP-address-of-the-test-iMetal-server>* **-S** *<private-IP-address-of-the-supplementary-network-interface>*

Plan the same VPC for the test iMetal server and the iMetal server that the supplementary network interface is attached to, so that the two iMetal servers can communicate with each other by default.

Example command:

Ping 192.168.0.133 -S 192.168.0.22

If information similar to the following is displayed, the two iMetal servers can communicate with each other.

```
PS C:\Users\Administrator> Ping 192.168.0.133 -S 192.168.0.22

Pinging 192.168.0.133 from 192.168.0.22 with 32 bytes of data:
Reply from 192.168.0.133: bytes=32 time=1ms TTL=64
Reply from 192.168.0.133: bytes=32 time<1ms TTL=64
Reply from 192.168.0.133: bytes=32 time<1ms TTL=64
Reply from 192.168.0.133: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.133:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

5.3.3 Managing Supplementary Network Interface Tags

Scenarios

Tags help you identify, classify, and search for supplementary network interfaces. You can perform the following operations to manage the tags of a supplementary network interface:

- Add a tag to a supplementary network interface.
- Modify a supplementary network interface tag.
- Delete a supplementary network interface tag.

For details about supplementary network interface tag requirements, see **Table 5-14**.

Table 5-14 Tag key and tag value requirements

Parameter	Requirements	Example Value
Tag key	• For each resource, each tag key must be unique, and each tag key can only have one tag value. • Cannot be left blank. • Can contain a maximum of 128 characters. • Can contain letters in any language, digits, spaces, underscores (_), periods (.), colons (:), equal signs (=), plus signs (+), minus signs (-), and at signs (@). • Cannot start with _sys_ or a space or end with a space.	test
Tag value	• Can be left blank. • Can contain a maximum of 255 characters. • Can contain letters in any language, digits, spaces, underscores (_), periods (.), colons (:), slashes (/), equal signs (=), plus signs (+), minus signs (-), and at signs (@). • Cannot start or end with a space.	01

Notes and Constraints

Each cloud resource can have a maximum of 20 tags.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Click in the upper left corner to display the service list and choose **Networking** > **Virtual Private Cloud**.

   The **Virtual Private Cloud** page is displayed.
4. Go to the **supplementary network interface list page**.
5. In the supplementary network interface list, click the private IP address of the target supplementary network interface.

   The supplementary network interface details page is displayed.
6. On the **Tags** tab, click **Edit Tag** in the upper left corner above the tag list.

   The **Edit Tag** dialog box is displayed.
7. Perform the following operations on the tag as required:
   - Adding a tag: Click , enter a tag key and value, and click **OK**.
   - Modifying a tag: Click next to the target tag key or value, delete the original value, enter a new value, and click **OK**.

- Deleting a tag: Click **Delete** next to the target tag and click **OK**.

5.3.4 Deleting a Supplementary Network Interface

Scenarios

You can delete a supplementary network interface that is no longer used.

Constraints

Deleting a supplementary network interface will also detach it from its network interface.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner to display the service list and choose **Networking** > **Virtual Private Cloud**.

   The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Virtual Private Cloud** > **Network Interfaces**.
5. On the **Network Interfaces** page, click **Supplementary Network Interfaces** tab.
6. Locate the row that contains the supplementary network interface and click **Delete** in the **Operation** column.

   A confirmation dialog box is displayed.
7. Confirm the information and click **OK**.

   Deleting a supplementary network interface will also delete the VLAN sub-interfaces configured on the iMetal server.

