Workspace

FAQs

Issue 06

Date 2024-06-13

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

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

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

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 FAQs for Administrators

1.1 Features and Advantages

1.1.1 What Are the Features and Advantages of Workspace?

You can purchase and unsubscribe from cloud desktops on the Workspace console and assign them to end users for immediate use.

Features of Workspace:

- Out-of-the-box usage: Unlike conventional private desktops that require days of deployment, Workspace allows for rapid provisioning of cloud desktops, ready for immediate use.
- Easy management: You can efficiently manage hundreds of desktops at the same time on the Workspace console.
- Elastic scaling: Workspace supports on-demand purchase and unsubscription of desktops and elastic scaling.
- Efficiency boost: Users can access their personal desktops from devices such as PCs and tablets anywhere, anytime, for an efficient and seamless mobile office.
- Enhanced security: Encrypted remote access, isolated tenant resources, and network and peripheral security control secure data access.

1.2 Billing and Purchase of Cloud Desktops

1.2.1 How Is Workspace Billed?

Yearly/Monthly: a prepaid billing mode. You pay in advance for a subscription term, and in exchange, you get a discounted rate.

Pay-per-use: a postpaid billing mode with a billing cycle of one hour. You are charged after using services, paying only for the resources consumed and their duration, and can unsubscribe from the services anytime.

NOTE

- You will **be charged for using NAT Gateway** to enable Internet access for user desktops.
- You can log in to the Huawei Cloud official website and choose **Billing & Costs** > **Bills** on the top of the page to view the fee details. For details, see **Bill Management** of Billing Center.

1.2.2 What If Desktop Purchase Failed?

If desktop purchase fails, rectify the fault by referring to the following cases. If the fault persists, **submit a service ticket** for technical support.

1.2.2.1 What If I Can't Add a Desktop to a Domain Due to a Locked Domain Administrator Account?

Scenarios

An AD domain is interconnected with. If desktop purchase fails and the error code 1909 appears, the domain administrator account is locked, preventing the desktop from joining the AD domain. To fix this, you need to unlock the domain administrator account following the procedure below.

Procedure

Step 1 **Log in to the console**.

Step 2 In the navigation pane, choose **Desktops** > **Desktops**.

The **Desktops** page is displayed.

Step 3 In the upper right corner of the **Desktops** page, click **Failed tasks**.

The page of failed tasks is displayed.

Step 4 If **1909** appears, the domain administrator account is locked. **Submit a service ticket** for technical support.

----End

1.2.2.2 What If Pooled Desktop Assignment Failed?

Scenarios

An AD domain is interconnected with. After you purchased a static desktop pool, assigning desktops in this pool failed. The cause is that the AD server's time and time zone are not synchronized with the standard ones. To fix this, you need to manually synchronize the AD server's time following the procedure below.

Procedure

Step 1 Log in to the AD server using the account and password.

Step 2 On the AD server, press **Win** + **R** to go to the **Run** dialog box.

Enter **cmd** to open the command line interface (CLI).

Step 3 Run the following command to synchronize the server's time:

w32tm /resync /rediscover

If the command execution succeeds, time synchronization is complete.

Step 4 Confirm that the server's time is the same as the standard time.

----End

1.2.2.3 What If Desktop Purchase Failed Due to an Invalid Desktop Name?

Scenarios

Desktop purchase on the console failed due to an invalid desktop name.

Procedure

Step 1 **Log in to the console**.

Step 2 In the navigation pane, choose **Desktops** > **Desktops**.

The **Desktops** page is displayed.

Step 3 In the upper right corner of the **Desktops** page, click **Failed tasks**.

The page of failed tasks is displayed.

Step 4 Find the failure cause: invalid desktop name.

Step 5 When re-purchasing a desktop, use a valid desktop name.

----End

1.2.2.4 What If Desktop Purchase Failed Due to Insufficient ECS Resources?

Scenarios

Desktop purchase failed due to insufficient ECS resources.

Procedure

Step 1 **Log in to the console**.

Step 2 In the navigation pane, choose **Desktops** > **Desktops**.

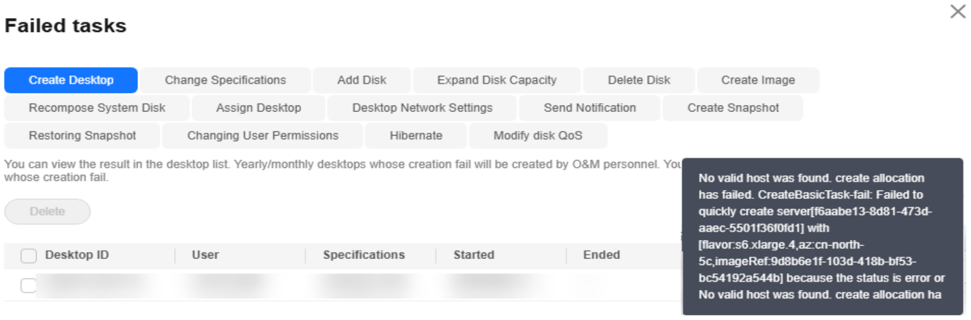
The **Desktops** page is displayed.

Step 3 In the upper right corner of the **Desktops** page, click **Failed tasks**.

The page of failed tasks is displayed.

Step 4 Find the failure cause: insufficient ECS resources, as shown in **Figure 1-1**.

Figure 1-1 Failure cause



You can view the result in the desktop list. Yearly/monthly desktops whose creation fail will be created by O&M personnel. You whose creation fail.

Desktop ID	User	Specifications	Started	Ended

No valid host was found. create allocation has failed. CreateBasicTask-fail: Failed to quickly create server[f6aabe13-8d81-473d-aaec-5501f36f0fd1] with [flavor:s6.xlarge.4,az:cn-north-5c,imageRef:9d8b6e1f-103d-418b-bf53-bc54192a544b] because the status is error or No valid host was found. create allocation ha

Step 5 Submit a service ticket for technical support.

----End

1.2.2.5 What If Desktop Purchase Failed in the AD Scenario Because a Common Domain User Was Configured?

Scenarios

An AD domain is interconnected with. A common domain user is configured as an AD domain user, but the number of VMs that can be added by a common domain user to the domain is limited. In this case, you need to replace the common domain user with another domain user or domain administrator.

Procedure

Step 1 Log in to the console.

Step 2 In the navigation pane, choose **Desktops** > **Desktops**.

The **Desktops** page is displayed.

Step 3 In the upper right corner of the **Desktops** page, click **Failed tasks**.

The page of failed tasks is displayed.

Step 4 Find the failure cause: failure of adding the VM to the domain.

----End

Assigning the domain user the permission to add a VM to the domain

Step 1 Log in to the AD server using the account and password.

Step 2 Press **Win** + **R**. In the **Run** dialog box displayed, enter **dsa.msc** and press **Enter**. The **Active Directory Users and Computers** page is displayed.

Step 3 On the page displayed, right-click the domain name and choose **Delegate Control**.

Step 4 Click **Next** and then **Add**.

Step 5 On the **Select User, Computer, or Group** page, enter the username such as **Administrator**, or click **Advanced** to select the desired user.

Step 6 Click **Check Names** and then **Add**.

Step 7 Click **Next**.

Step 8 Select the option of automatically creating a task for delegation and click **Next**.

Step 9 On the page of wizard for delegation control, select only the following objects in this folder.

Step 10 Then select computer objects, select the options of creating and deleting the selected objects in this folder, and click **Next**.

Step 11 Select the permission for reading, writing, and writing all attributes, and click **Finish**.

----End

1.2.3 How Do I Purchase Desktops in Batches?

Scenarios

You can purchase desktops in batches if a large number of desktops with the same specifications (including the OS image, memory, and disk) are needed.

Prerequisites

You have confirmed the desktop specifications and user information (including the username and email address).

If an AD domain is interconnected with, ensure that the desktop user information matches the user information on the AD domain.

Procedure

Step 1 Go to the **Huawei Cloud website**. Log in to the Huawei Cloud console as an administrator.

Step 2 Click 📍 in the upper left corner of the console and select a region and a project.

Step 3 Click ☰ and choose **Business Applications** > **Workspace** in the service list.

The **Dashboard** page is displayed.

Step 4 Click **Buy Desktop**.

The **Buy Desktop** page is displayed.

Step 5 Select the billing mode, project, AZ, CPU architecture, compute specifications, image file, system disk, and data disk specifications.

Step 6 Click **Next: Advanced Settings**.

The **Advanced Settings** page is displayed.

Step 7 Configure the network and determine whether to configure Internet access for desktops.

Step 8 Click **Next: Assign Desktop**.

The **Assign Desktop** page is displayed.

Step 9 Set **Desktop Assignment Type** to **Batch**.

Step 10 Click **Download User List Template** to obtain the user list template.

Step 11 Open the template on the local PC and enter user information by referring to **Table 1-1**.

NOTE

Each row in the template indicates one desktop.

Table 1-1 Parameters

Parameter	Description
No.	The number starts from 1 and increases row by row.
Username	User authentication for desktop login. Naming rules: ● A name can contain 1 to 32 characters. ● A name can contain letters, digits, periods (.), hyphens (-), and underscores (_). A username with letters can only start with a letter or digit. You can enter a digit-only username.
Email	Used to receive emails about desktop provisioning and related notifications. Email address rules: ● Enter a valid email address. ● The value can contain a maximum of 64 characters. ● The value cannot be empty.
Permission Group	Used to distinguish users' permissions on computers. Windows desktop permissions: ● **administrators**: indicates the administrator group. Group users have system administrator permissions, that is, full control permissions on a computer. They can perform all management tasks, including managing all users, on the computer. ● **users**: indicates the common user group. Group users have basic operation permissions on a computer, such as running applications. They cannot change the data of other users or the OS settings, or stop a server computer.

Parameter	Description
Desktop Name	Displayed desktop name. Do not use the name of a purchased desktop. If you do not customize the desktop name, the system automatically generates one. Naming rules: ● The value can contain only letters, digits, and hyphens (-). It must start with a digit or letter, and cannot end with a hyphen (-). ● The value can contain 1 to 15 characters.
Desktop IP Address	The entered IP addresses must be in the same subnet of the same VPC. If this parameter is left blank, an IP address is automatically allocated. Ensure that the IP address of each desktop is unique.

Step 12 Save and close the user list template file.

Step 13 Click **File**, select the user list template file saved in **Step 12**, and click **Open**.

Step 14 After the upload is successful, click **View Imported User Information** to confirm the user information.

If the upload fails, click **View error records** to check the user list template. After the modification, click **Upload** again.

Step 15 Click **Next: Confirm**.

The confirmation page is displayed.

Step 16 On the page displayed, select the required enterprise project from the **Enterprise Project** drop-down list.

Step 17 After confirming the desktop information, perform operations based on the selected billing mode.

- Yearly/Monthly
  a. Specify **Required Duration** and determine whether to enable auto-renewal.
  b. Read the disclaimer and check the box indicating your agreement to the disclaimer.
  c. Click **Buy Now**.
  d. Check the order information and select the required payment method.
- Pay-per-use
  a. Read the disclaimer and check the box indicating your agreement to the disclaimer.
  b. Click **Buy Now**.

----End

1.2.4 How Do I Add Resources to or Remove Resources from an Enterprise Project After Purchasing Workspace?

For details about how to add resources to enterprise projects, see **Adding Resources to Enterprise Projects**.

For details about how to remove resources from enterprise projects, see **Removing Resources from an Enterprise Project**.

1.2.5 What If a Message Appears Prompting Me to Cancel the Service and Re-Register or the Buttons Buy Desktop, Create User, Create Policy, and Enable Internet Are Grayed Out on the Workspace Console?

After you enable the service, it will be automatically locked if no desktop exists in the current project (without sub-projects) or sub-project for more than 14 days. This will disable the buttons **Buy Desktop**, **Create User**, **Create Policy**, and **Enable Internet**. You can cancel the service and re-register as prompted, or click **Reactivate** on the **Tenant Configuration** page to reactivate the service. After the service is reactivated, the preceding functions will become available.

1.2.6 Why Can't I Start a Pay-per-Use Cloud Desktop?

When a pay-per-use cloud desktop is shut down, its resources such as vCPUs and memory are released. When the cloud desktop is started again, the startup may fail due to insufficient resources.

If the cloud desktop startup fails, start it again later or modify the desktop specifications. For details about how to modify specifications, see operations for modifying specifications.

1.2.7 Do I Need to Enable the Snapshot Function After Purchasing a Cloud Desktop?

Workspace supports scheduled desktop snapshot creation. The purpose of desktop snapshot creation is to quickly back up and restore data. If a personal misoperation, software incompatibility, system breakdown or fault, or software conflict occurs, snapshot restoration can help quickly restore your desktop to the previous state, preventing data loss and work interruption.

- For details about creating a desktop snapshot, see **Scheduled Snapshot Creation**.
- For details about restoring a snapshot, see "Restoring a snapshot" in **Snapshots**.

1.3 Quotas

1.3.1 How Do I Check My Quotas?

NOTE

You can only check the quotas of the current administrator account.

Step 1 Go to the **Huawei Cloud official website**. Log in to the console as an administrator.

Step 2 Click 📍 in the upper left corner of the console and select a region and a project.

Step 3 In the upper right corner of the page, choose **Resources** > **My Quotas**.

The **Quotas** page is displayed.

----End

1.3.2 How Do I Increase My Quotas?

NOTE

You can only increase quotas of the current administrator account.

Step 1 Go to the **Huawei Cloud official website**. Log in to the console as an administrator.

Step 2 Click 📍 in the upper left corner of the console and select a region and a project.

Step 3 In the upper right corner of the page, choose **Resources** > **My Quotas**.

The **Quotas** page is displayed.

Step 4 Click **Increase Quota**.

Step 5 On the **Create Service Ticket** page, configure parameters as required.

Fill in the content to be adjusted in the **Problem Description** area. The following is an example:

- Name: **Workspace**
- Project ID: *xxxxxxxxxxxxxxxxxxxxxxxx*
- The quota is adjusted as follows: *xx* servers, *xx* cores, *xx* memory, and *xx* CPUs.

Step 6 Agree to the agreement and click **Submit**.

----End

1.4 Storage and Disks

1.4.1 How Do I Add a Disk?

NOTE

You can add data disks only to a desktop whose **Status** is **Running**.

Step 1 Go to the **Huawei Cloud official website**. Log in to the console as an administrator.

Step 2 Click 📍 in the upper left corner of the console and select a region and a project.

Step 3 Click ≡ and choose **Business Applications** > **Workspace** in the service list.

The **Dashboard** page is displayed.

Step 4 Click **Desktop management**.

The **Desktops** page is displayed.

Step 5 Select the desktop to which you need to add data disks, and choose **More** > **Disks** > **Add Disk**.

The page for adding data disks is displayed.

Step 6 Click **Add** and configure parameters.

- **High I/O**: uses serial attached SCSI (SAS) drives to store data. High I/O disks are suitable for common workloads.
- **Ultra-high I/O**: uses solid state disk (SSD) drives to store data. Ultra-high I/O disks are suitable for enterprise mission-critical services as well as workloads demanding high throughput and low latency.

NOTE

The maximum number of added data disks is 10 minus the number of existing data disks.

Step 7 Select **I understand the impact of this operation and will proceed.**

Step 8 Click **Next**.

Step 9 Confirm the information about the new disks and click **OK**. The data disks have been added.

----End

1.4.2 How Do I Copy Files Between a Desktop and a Local Storage Device?

Administrators can adapt different file, clipboard, and peripheral policies to different desktops to control the file copy permission between desktops and local storage devices.

The following lists several file copy scenarios and describes how to configure policies.

Copying Files from the Desktop to an External Storage Device

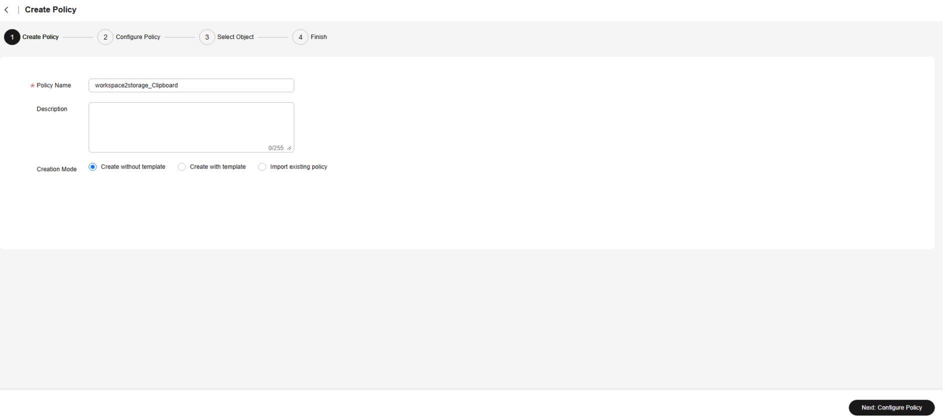
If Workspace desktops are used in offices and there are strict requirements for input data on office desktops, you can configure the clipboard policies for the desktops.

1. Log in to the console as an administrator.
2. Click 📍 in the upper left corner of the console and select a region and a project.
3. Click ≡ and choose **Business Applications** > **Workspace** in the service list.

   The **Dashboard** page is displayed.

4. In the navigation pane on the left, choose **Policies** > **Protocol Policies**.
5. Click **Create Policy** in the upper right corner.
6. Configure the policy name, description, and creation mode, and click **Next: Configure Policy**.
   - The policy name can contain up to 55 characters in digits, letters, and underscores (_), for example, **workspace2storage_Clipboard**.
   - The description can contain up to 255 characters, for example, **Clipboard redirection is used to copy files from a Workspace desktop to an external device**.
   - Retain the default creation mode.

Figure 1-2 Creating a policy



Create Policy

1 Create Policy — 2 Configure Policy — 3 Select Object — 4 Finish

* Policy Name: workspace2storage_Clipboard

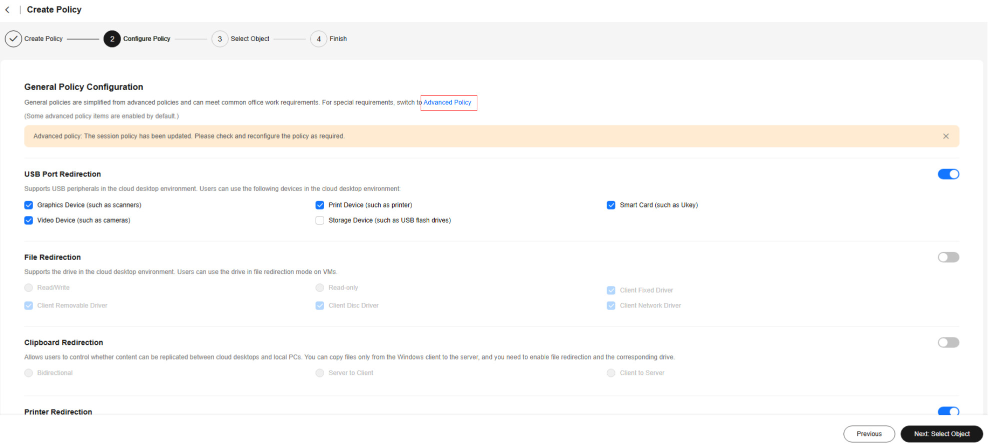
Description: 0/255

Creation Mode: ● Create without template ○ Create with template ○ Import existing policy

Next: Configure Policy

7. Click **Advanced Policies**.

Figure 1-3 Advanced policy entry



Create Policy

✓ Create Policy — 2 Configure Policy — 3 Select Object — 4 Finish

General Policy Configuration

General policies are simplified from advanced policies and can meet common office work requirements. For special requirements, switch to Advanced Policy

(Some advanced policy items are enabled by default.)

Advanced policy: The session policy has been updated. Please check and reconfigure the policy as required.

USB Port Redirection

Supports USB peripherals in the cloud desktop environment. Users can use the following devices in the cloud desktop environment:

☑ Graphics Device (such as scanners) ☑ Print Device (such as printer) ☑ Smart Card (such as Ukey)
☑ Video Device (such as cameras) □ Storage Device (such as USB flash drives)

File Redirection

Supports the drive in the cloud desktop environment. Users can use the drive in file redirection mode on VMs.

○ Read/Write ○ Read-only ☑ Client Fixed Driver
☑ Client Removable Driver ☑ Client Disc Driver ☑ Client Network Driver

Clipboard Redirection

Allows users to control whether content can be replicated between cloud desktops and local PCs. You can copy files only from the Windows client to the server, and you need to enable file redirection and the corresponding drive.

○ Bidirectional ○ Server to Client ○ Client to Server

Printer Redirection

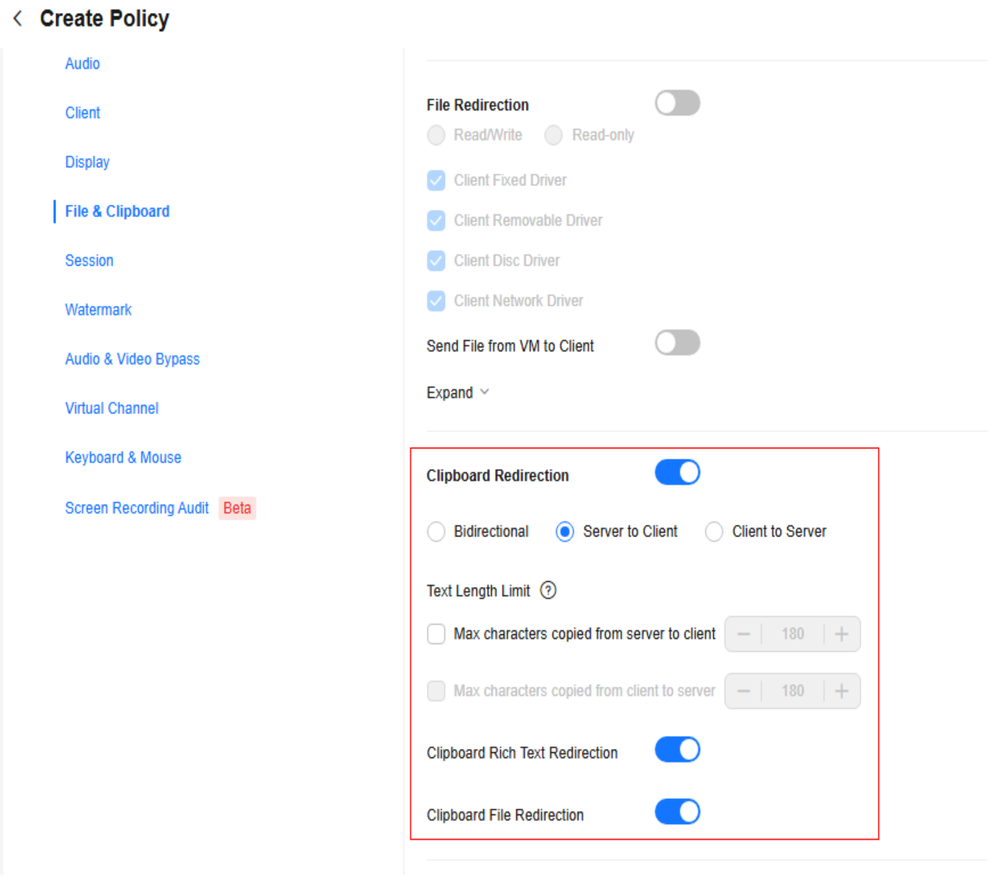
Previous | Next: Select Object

8. On the **Advanced Policies** page, click **Files and Clipboards**.
9. Enable the **Clipboard Redirection** policy and select **Server to client**, as shown in **Figure 1-4**.

   NOTE

   - Rich text copy and file copy are supported only when both the client (TC/SC) and desktop run Windows. A maximum of 500 files can be copied at a time.
   - If the OS of a client (TC/SC or mobile client) or desktop is not Windows, only text can be copied.

Figure 1-4 Configuring the clipboard redirection policy from the server to the client



< **Create Policy**

Audio
Client
Display
File & Clipboard
Session
Watermark
Audio & Video Bypass
Virtual Channel
Keyboard & Mouse
Screen Recording Audit Beta

File Redirection (off)
○ Read/Write ○ Read-only
☑ Client Fixed Driver
☑ Client Removable Driver
☑ Client Disc Driver
☑ Client Network Driver
Send File from VM to Client (off)
Expand

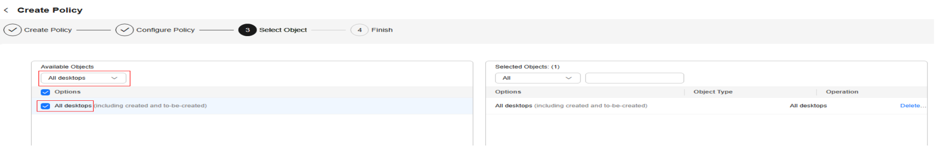
Clipboard Redirection (on)
○ Bidirectional ● Server to Client ○ Client to Server
Text Length Limit
□ Max characters copied from server to client 180
□ Max characters copied from client to server 180
Clipboard Rich Text Redirection (on)
Clipboard File Redirection (on)

10. Click **Next: Select objects**.

11. Select an object as required.

    For example, if you select **All desktops**, the policy applies to all desktops in the current project.

Figure 1-5 Selecting an object



< **Create Policy**

Create Policy — Configure Policy — 3 Select Object — 4 Finish

Available Objects
All desktops
☑ Options
☑ All desktops (including created and to-be-created)

Selected Objects: (1)
All

Options	Object Type	Operation
All desktops (including created and to-be-created)	All desktops	Delete...

12. Click **Next: Finish**.

Copying Files from an External Storage Device to the Desktop

If Workspace desktops are used in office and there are strict requirements for data transmission on office desktops, you can configure the **Clipboard Redirection**, **File Redirection** and **Send File in Virtual Machine to Client** policies for the desktops. You can select either of them.

- **Clipboard redirection**

  a. Log in to the console as an administrator.

b. Click in the upper left corner of the console and select a region and a project.

c. Click and choose **Business Applications** > **Workspace** in the service list.

   The **Dashboard** page is displayed.

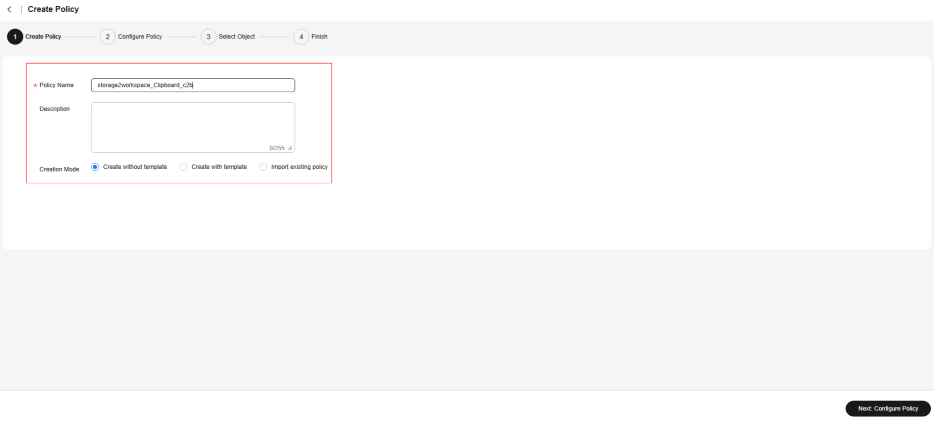
d. In the navigation pane on the left, choose **Policies** > **Protocol Policies**.

e. Click **Create Policy** in the upper right corner.

f. Configure the policy name, description, and creation mode, and click **Next: Configure Policy**.

   - The policy name can contain up to 55 characters in digits, letters, and underscores (_), for example, **workspace2storage_Clipboard_c2b**.
   - The description can contain up to 255 characters, for example, **Clipboard redirection is used to copy files from an external device to a desktop**.
   - Retain the default creation mode.

Figure 1-6 Creating a policy



< | Create Policy

1 Create Policy ——— 2 Configure Policy ——— 3 Select Object ——— 4 Finish

* Policy Name: storage2workspace_Clipboard_c2b

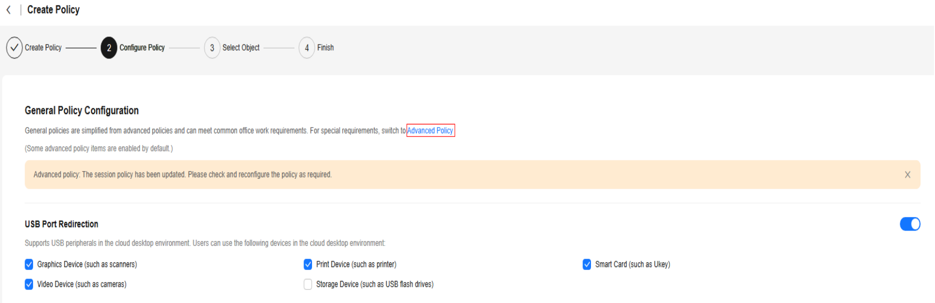
Description: 0/255

Creation Mode: ● Create without template ○ Create with template ○ Import existing policy

Next: Configure Policy

g. Click **Advanced Policies**.

Figure 1-7 Advanced policy entry



< | Create Policy

✓ Create Policy ——— 2 Configure Policy ——— 3 Select Object ——— 4 Finish

General Policy Configuration

General policies are simplified from advanced policies and can meet common office work requirements. For special requirements, switch to Advanced Policy

(Some advanced policy items are enabled by default.)

Advanced policy: The session policy has been updated. Please check and reconfigure the policy as required. X

USB Port Redirection

Supports USB peripherals in the cloud desktop environment. Users can use the following devices in the cloud desktop environment:

☑ Graphics Device (such as scanners) ☑ Print Device (such as printer) ☑ Smart Card (such as Ukey)

☑ Video Device (such as cameras) □ Storage Device (such as USB flash drives)

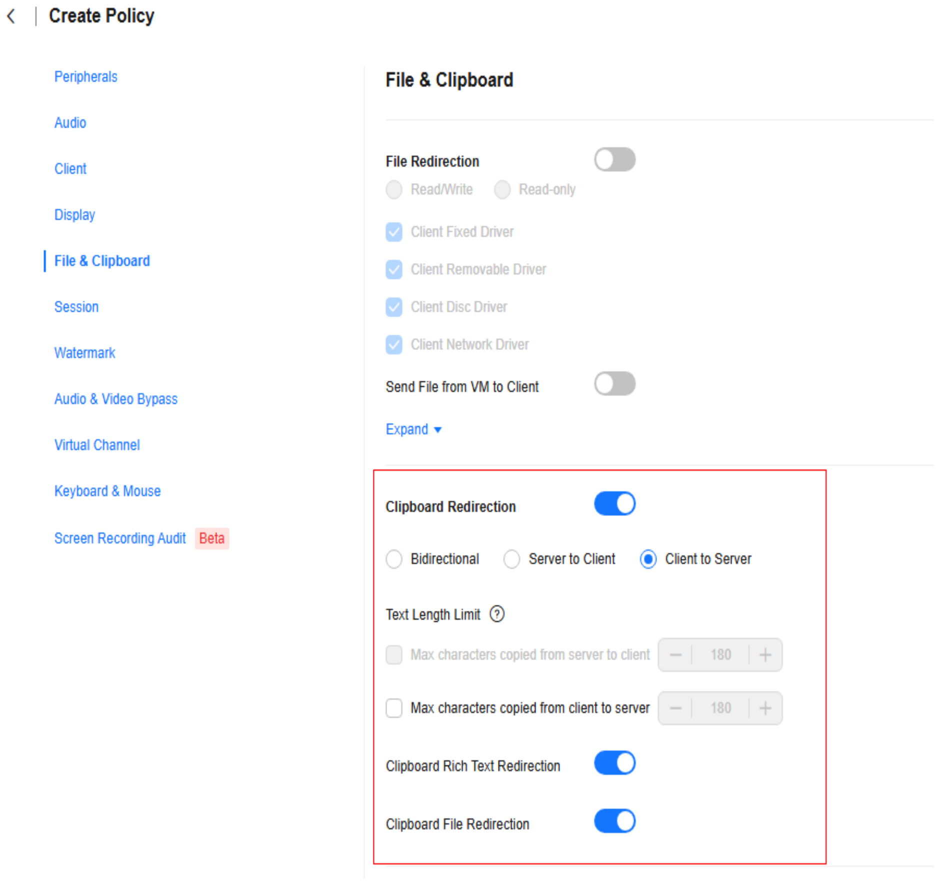
h. On the **Advanced Policies** page, click **Files and Clipboards**.

i. Enable the **Clipboard Redirection** policy and select **Client to server**, as shown in **Figure 1-8**.

NOTE

- Rich text copy and file copy are supported only when both the client (TC/SC) and desktop run Windows. A maximum of 500 files can be copied at a time.
- If the OS of a client (TC/SC or mobile client) or desktop is not Windows, only text can be copied.

Figure 1-8 Configuring the clipboard redirection policy from the client to the server



Create Policy

File & Clipboard

File Redirection: off
○ Read/Write ○ Read-only
☑ Client Fixed Driver
☑ Client Removable Driver
☑ Client Disc Driver
☑ Client Network Driver
Send File from VM to Client: off
Expand

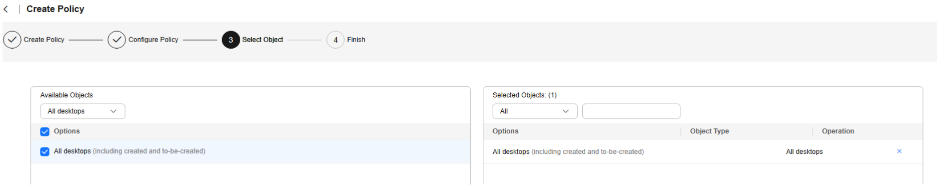
Clipboard Redirection: on
○ Bidirectional ○ Server to Client ● Client to Server
Text Length Limit
□ Max characters copied from server to client 180
□ Max characters copied from client to server 180
Clipboard Rich Text Redirection: on
Clipboard File Redirection: on

j. Click **Next: Select objects**.

k. Select an object as required.

For example, if you select **All desktops**, the policy applies to all desktops in the current project.

Figure 1-9 Selecting an object



Create Policy

Available Objects: All desktops
☑ Options
☑ All desktops (including created and to-be-created)

Selected Objects: (1) All

Options	Object Type	Operation
All desktops (including created and to-be-created)	All desktops	×

l. Click **Next: Finish**.

- **Sending files from VMs to clients**

a. Log in to the console as an administrator.

b. Click ⊙ in the upper left corner of the console and select a region and a project.

c. Click ☰ and choose **Business Applications** > **Workspace** in the service list.

   The **Dashboard** page is displayed.

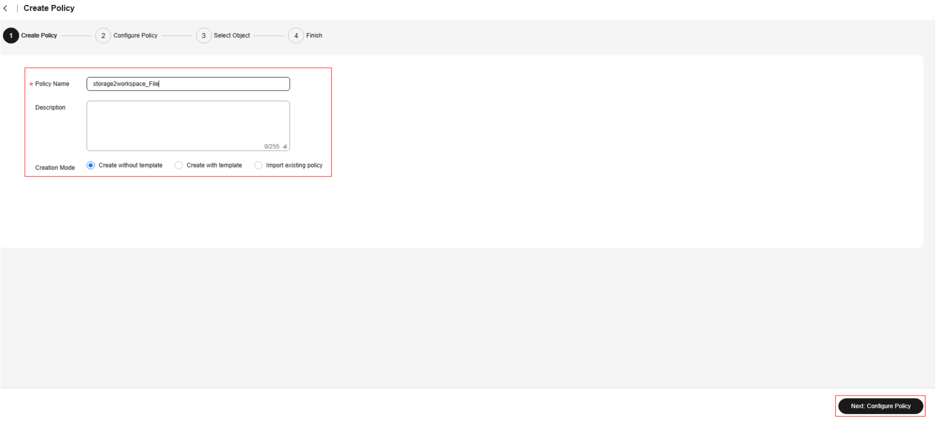
d. In the navigation pane on the left, choose **Policies** > **Protocol Policies**.

e. Click **Create Policy** in the upper right corner.

f. Configure the policy name, description, and creation mode, and click **Next: Configure Policy**.

   - The policy name can contain up to 55 characters in digits, letters, and underscores (_), for example, **storage2workspace_File**.
   - The description can contain up to 255 characters, for example, **Copying files from an external device to a desktop**.
   - Retain the default creation mode.

Figure 1-10 Creating a policy



< | Create Policy

1 Create Policy —— 2 Configure Policy —— 3 Select Object —— 4 Finish

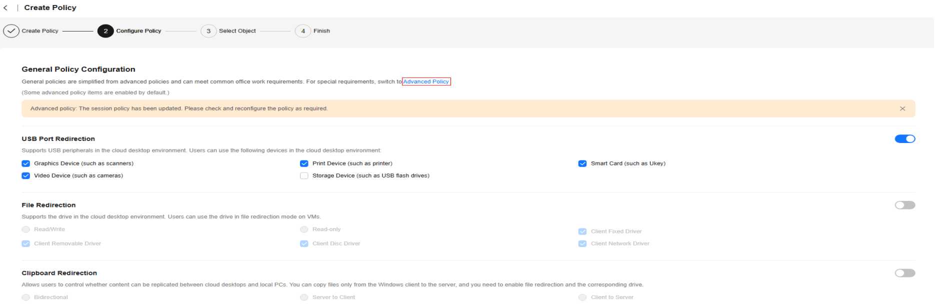
* Policy Name: storage2workspace_File

Description: 0/255

Creation Mode: ● Create without template ○ Create with template ○ Import existing policy

g. Click **Advanced Policies**.

Figure 1-11 Advanced policy entry



< | Create Policy

✓ Create Policy —— 2 Configure Policy —— 3 Select Object —— 4 Finish

General Policy Configuration

General policies are simplified from advanced policies and can meet common office work requirements. For special requirements, switch to Advanced Policy

(Some advanced policy items are enabled by default.)

Advanced policy: The session policy has been updated. Please check and reconfigure the policy as required. ×

USB Port Redirection

Supports USB peripherals in the cloud desktop environment. Users can use the following devices in the cloud desktop environment:

☑ Graphics Device (such as scanners) ☑ Print Device (such as printer) ☑ Smart Card (such as Ukey)
☑ Video Device (such as cameras) □ Storage Device (such as USB flash drives)

File Redirection

Supports the drive in the cloud desktop environment. Users can use the drive in file redirection mode on VMs.

○ Read/Write ○ Read-only ☑ Client Fixed Driver
☑ Client Removable Driver ☑ Client Disc Driver ☑ Client Network Driver

Clipboard Redirection

Allows users to control whether content can be replicated between cloud desktops and local PCs. You can copy files only from the Windows client to the server, and you need to enable file redirection and the corresponding drive.

○ Bidirectional ○ Server to Client ○ Client to Server

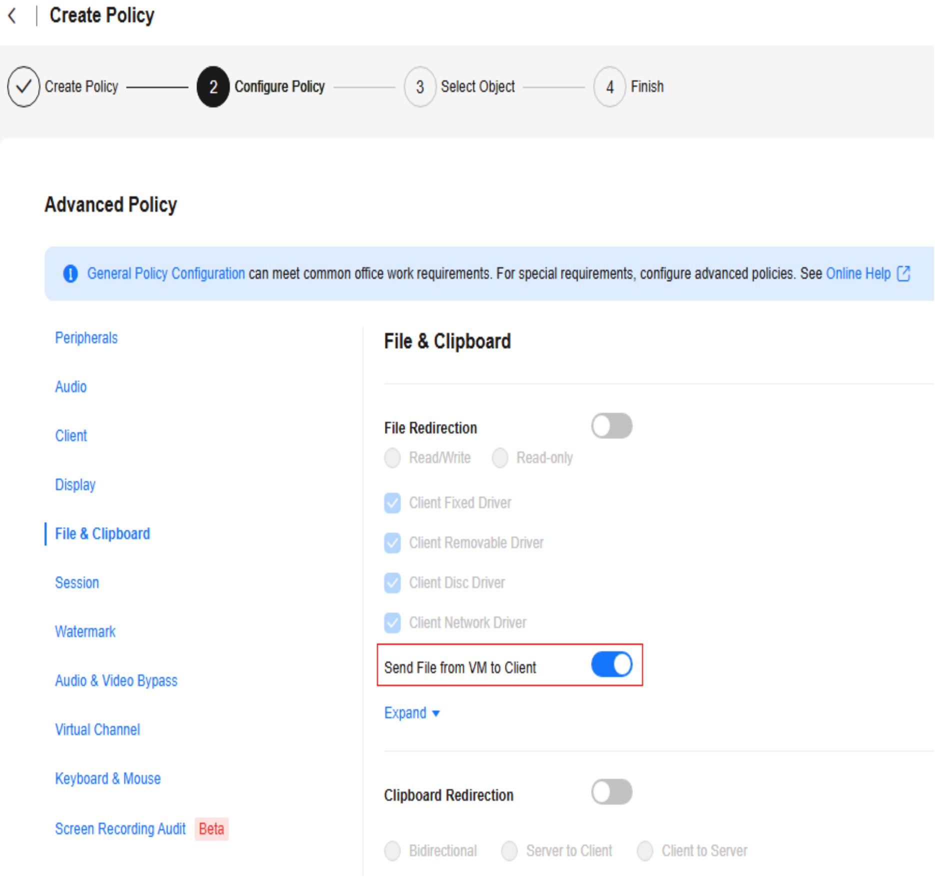
h. On the **Advanced Policies** page, click **Files and Clipboards**.

i. Enable **Send File In Virtual Machine to Client** as shown in **Figure 1-12**.

NOTE

If **Send File In Virtual Machine to Client** is enabled, you can copy files from an external storage device to the desktop by sending files only when both the client (TC/SC) OS and the desktop run Windows.

Figure 1-12 Configuring the policy



< | Create Policy

✓ Create Policy —— 2 Configure Policy —— 3 Select Object —— 4 Finish

Advanced Policy

General Policy Configuration can meet common office work requirements. For special requirements, configure advanced policies. See Online Help

File & Clipboard

File Redirection (off)
○ Read/Write ○ Read-only
☑ Client Fixed Driver
☑ Client Removable Driver
☑ Client Disc Driver
☑ Client Network Driver

Send File from VM to Client (on)

Expand ▾

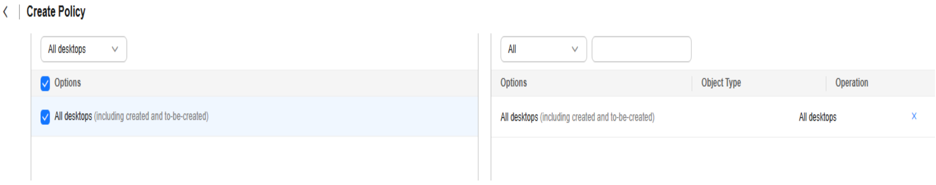
Clipboard Redirection (off)
○ Bidirectional ○ Server to Client ○ Client to Server

j. Click **Next: Select objects**.

k. Select an object as required.

For example, if you select **All desktops**, the policy applies to all desktops in the current project.

Figure 1-13 Selecting an object



< | Create Policy

All desktops ∨

☑ Options

☑ All desktops (including created and to-be-created)

All ∨

Options	Object Type	Operation
All desktops (including created and to-be-created)	All desktops	x

l. Click **Next: Finish**.

- **File redirection**

a. Log in to the console as an administrator.

b. Click in the upper left corner of the console and select a region and a project.

c. Click and choose **Business Applications** > **Workspace** in the service list.

   The **Dashboard** page is displayed.

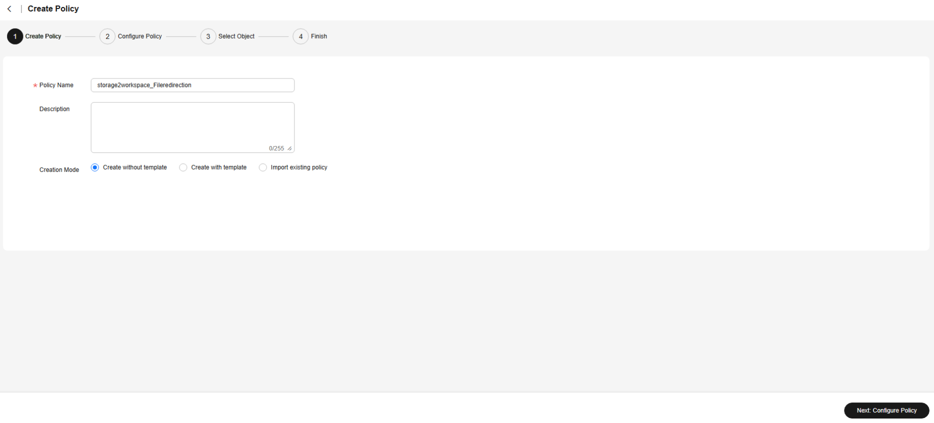
d. In the navigation pane on the left, choose **Policies** > **Protocol Policies**.

e. Click **Create Policy** in the upper right corner.

f. Configure the policy name, description, and creation mode, and click **Next: Configure Policy**.

   - The policy name can contain up to 55 characters in digits, letters, and underscores (_), for example, **storage2workspace_Fileredirection**.
   - The description can contain up to 255 characters, for example, **Copying files from an external device to a desktop**.
   - Retain the default creation mode.

Figure 1-14 Creating a policy



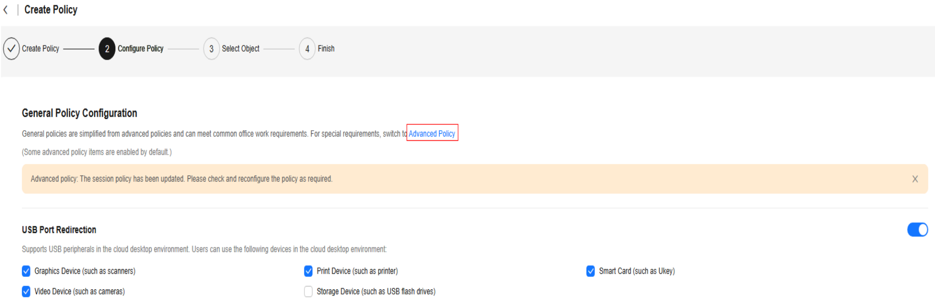
* Policy Name: storage2workspace_Fileredirection

Description: 0/255

Creation Mode: ● Create without template ○ Create with template ○ Import existing policy

g. Click **Advanced Policies**.

Figure 1-15 Advanced policy entry



General Policy Configuration

General policies are simplified from advanced policies and can meet common office work requirements. For special requirements, switch to Advanced Policy

(Some advanced policy items are enabled by default.)

Advanced policy: The session policy has been updated. Please check and reconfigure the policy as required.

USB Port Redirection

Supports USB peripherals in the cloud desktop environment. Users can use the following devices in the cloud desktop environment:

☑ Graphics Device (such as scanners) ☑ Print Device (such as printer) ☑ Smart Card (such as Ukey)

☑ Video Device (such as cameras) □ Storage Device (such as USB flash drives)

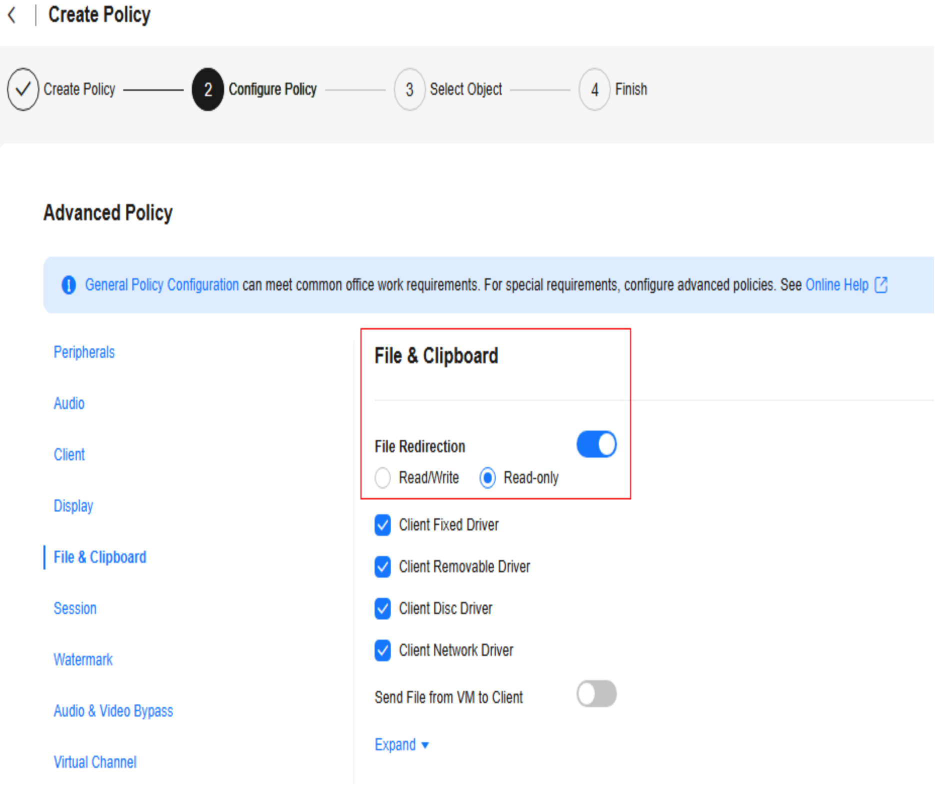
h. On the **Advanced Policies** page, click **Files and Clipboards**.

i. Enable the **File Redirection** policy and set it to **Read-only**, as shown in Figure 1-16.

NOTE

You do not need to configure other advanced policy parameters under **Files and Clipboards**. If you have strict requirements on the traffic and file size, configure them by referring to **Creating an Advanced Policy**. For a Linux terminal, expand **Advanced Policies** and set **Linux Root Directory Mounting** to . For an Android terminal, expand **Advanced Policies** and set **Mobile Client Redirection** to .

Figure 1-16 Configuring the policy



Create Policy

✓ Create Policy — 2 Configure Policy — 3 Select Object — 4 Finish

Advanced Policy

General Policy Configuration can meet common office work requirements. For special requirements, configure advanced policies. See Online Help

File & Clipboard

File Redirection: on
○ Read/Write ● Read-only

☑ Client Fixed Driver

☑ Client Removable Driver

☑ Client Disc Driver

☑ Client Network Driver

Send File from VM to Client: off

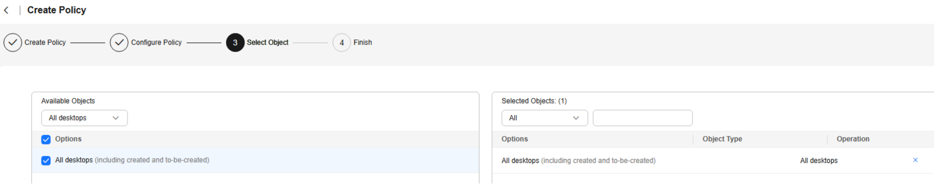
Expand ▾

j. Click **Next: Select objects**.

k. Select an object as required.

For example, if you select **All desktops**, the policy applies to all desktops in the current project.

Figure 1-17 Selecting an object



Create Policy

✓ Create Policy — ✓ Configure Policy — 3 Select Object — 4 Finish

Available Objects: All desktops

☑ Options

☑ All desktops (including created and to-be-created)

Selected Objects: (1)

All

Options	Object Type	Operation
All desktops (including created and to-be-created)	All desktops	×

l. Click **Next: Finish**.

Copying Files Between External Storage Devices and Desktops

If data is frequently transmitted between desktops and external storage devices without special requirements, you can configure USB port redirection, file redirection, or clipboard redirection as required. You can select one of them.

- **USB port redirection**

  USB port redirection allows files to be copied between mobile storage devices and desktops.

  a. Log in to the console as an administrator.

  b. Click in the upper left corner of the console and select a region and a project.

  c. Click ☰ and choose **Business Applications** > **Workspace** in the service list.

     The **Dashboard** page is displayed.

  d. In the navigation pane on the left, choose **Policies** > **Protocol Policies**.

  e. Click **Create Policy** in the upper right corner.

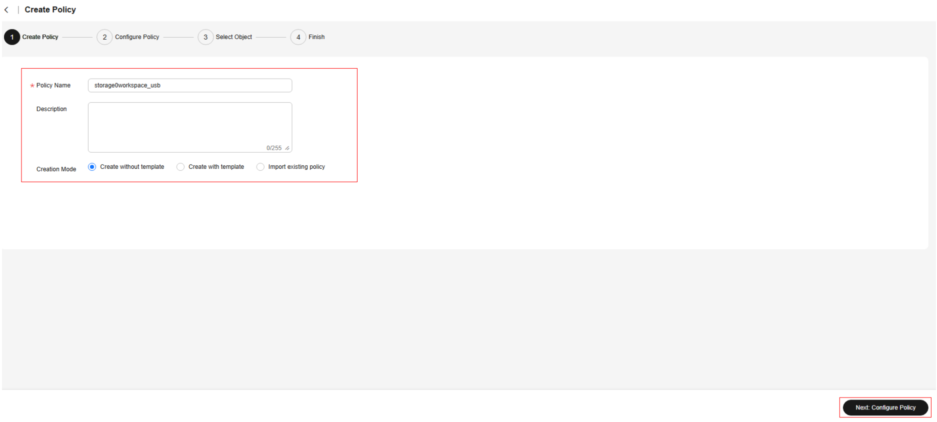
  f. Configure the policy name, description, and creation mode, and click **Next: Configure Policy**.

     - The policy name can contain up to 55 characters in digits, letters, and underscores (_), for example, **storage0workspace_usb**.

     - The description can contain up to 255 characters, for example, **USB port redirection is used to copy files between external devices and desktops**.

     - Retain the default creation mode.

     Figure 1-18 Creating a policy



Create Policy

1 Create Policy — 2 Configure Policy — 3 Select Object — 4 Finish

* Policy Name: storage0workspace_usb

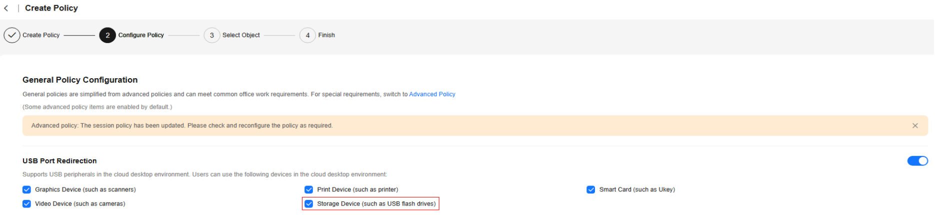
Description: 0/255

Creation Mode: ● Create without template ○ Create with template ○ Import existing policy

Next: Configure Policy

  g. Select **Storage Device (such as USB flash drives)** in **USB Port Redirection**, as shown in **Figure 1-19**.

Figure 1-19 Configuring the policy



Create Policy

Create Policy — 2 Configure Policy — 3 Select Object — 4 Finish

General Policy Configuration

General policies are simplified from advanced policies and can meet common office work requirements. For special requirements, switch to Advanced Policy

(Some advanced policy items are enabled by default.)

Advanced policy: The session policy has been updated. Please check and reconfigure the policy as required.

USB Port Redirection

Supports USB peripherals in the cloud desktop environment. Users can use the following devices in the cloud desktop environment:

☑ Graphics Device (such as scanners) ☑ Print Device (such as printer) ☑ Smart Card (such as Ukey)

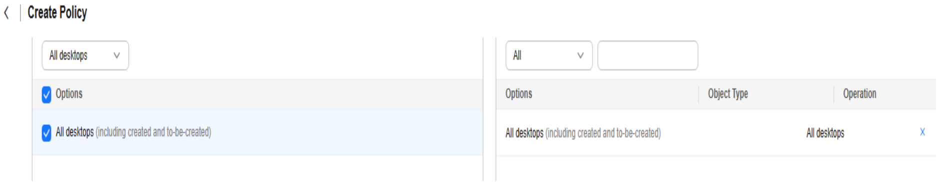
☑ Video Device (such as cameras) ☑ Storage Device (such as USB flash drives)

h. Click **Next: Select objects**.

i. Select an object as required.

   For example, if you select **All desktops**, the policy applies to all desktops in the current project.

Figure 1-20 Selecting an object



Create Policy

All desktops

☑ Options

☑ All desktops (including created and to-be-created)

All

Options	Object Type	Operation
All desktops (including created and to-be-created)	All desktops	X

j. Click **Next: Finish**.

- **File redirection**

  This feature supports the file copy between fixed drivers (such as local disks and TCs running Windows, Linux, and Android OSs) and removable drives (such as USB flash drives), CD-ROM drives, network drives, and desktops.

  a. Log in to the console as an administrator.

  b. Click ⊙ in the upper left corner of the console and select a region and a project.

  c. Click ☰ and choose **Business Applications** > **Workspace** in the service list.

     The **Dashboard** page is displayed.

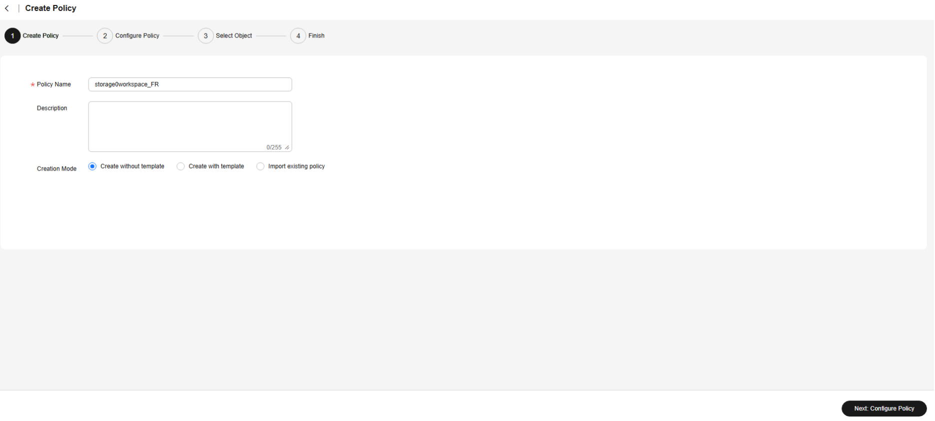
  d. In the navigation pane on the left, choose **Policies** > **Protocol Policies**.

  e. Click **Create Policy** in the upper right corner.

  f. Configure the policy name, description, and creation mode, and click **Next: Configure Policy**.

     - The policy name can contain up to 55 characters in digits, letters, and underscores (_), for example, **storage0workspace_FR**.
     - The description can contain up to 255 characters, for example, **File redirection for copying files between external devices and desktops**.
     - Retain the default creation mode.

Figure 1-21 Creating a policy



Create Policy

1 Create Policy — 2 Configure Policy — 3 Select Object — 4 Finish

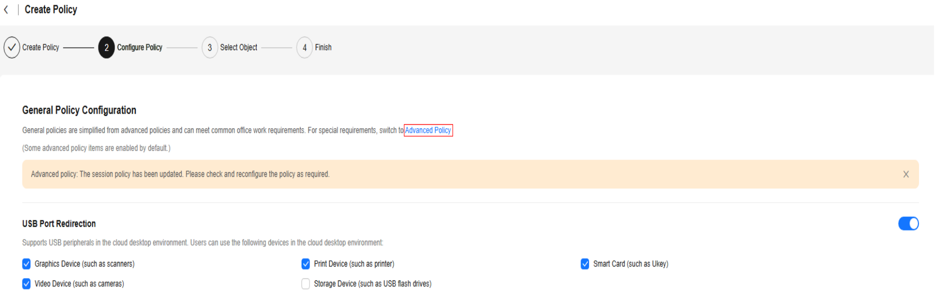
* Policy Name: storage0workspace_FR

Description: 0/255

Creation Mode: ● Create without template ○ Create with template ○ Import existing policy

g. Click **Advanced Policies**.

Figure 1-22 Advanced policy entry



Create Policy

✓ Create Policy — 2 Configure Policy — 3 Select Object — 4 Finish

General Policy Configuration

General policies are simplified from advanced policies and can meet common office work requirements. For special requirements, switch to Advanced Policy

(Some advanced policy items are enabled by default.)

Advanced policy: The session policy has been updated. Please check and reconfigure the policy as required.

USB Port Redirection

Supports USB peripherals in the cloud desktop environment. Users can use the following devices in the cloud desktop environment:

☑ Graphics Device (such as scanners) ☑ Print Device (such as printer) ☑ Smart Card (such as Ukey)

☑ Video Device (such as cameras) □ Storage Device (such as USB flash drives)

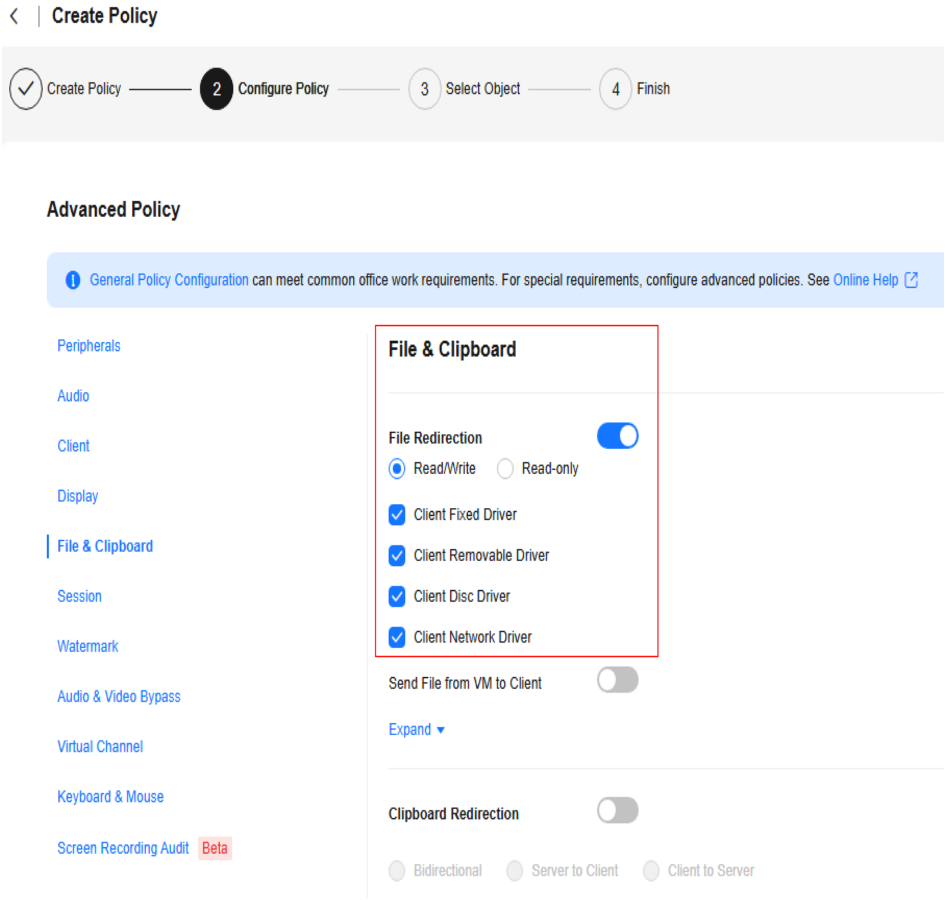
h. On the **Advanced Policies** page, click **Files and Clipboards**.

i. Enable the **File Redirection** policy and set it to **Read-write**, as shown in **Figure 1-23**.

NOTE

You do not need to configure other advanced policy parameters under **Files and Clipboards**. If you have strict requirements on the traffic and file size, configure them by referring to **Creating an Advanced Policy**. For a Linux terminal, expand **Advanced Policies** and set **Linux Root Directory Mounting** to ●. For an Android terminal, expand **Advanced Policies** and set **Mobile Client Redirection** to ●.

Figure 1-23 Configuring the policy



< | **Create Policy**

✓ Create Policy —— **2 Configure Policy** —— 3 Select Object —— 4 Finish

Advanced Policy

General Policy Configuration can meet common office work requirements. For special requirements, configure advanced policies. See Online Help

File & Clipboard

File Redirection: on

● Read/Write ○ Read-only

☑ Client Fixed Driver

☑ Client Removable Driver

☑ Client Disc Driver

☑ Client Network Driver

Send File from VM to Client: off

Expand ▾

Clipboard Redirection: off

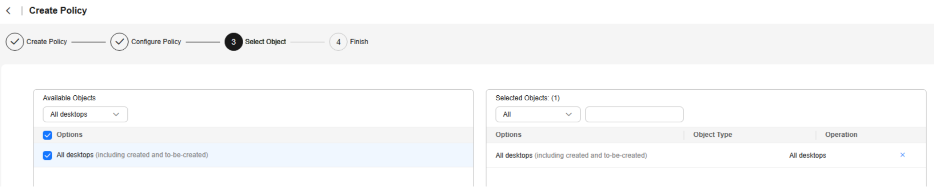
○ Bidirectional ○ Server to Client ○ Client to Server

j. Click **Next: Select objects**.

k. Select an object as required.

For example, if you select **All desktops**, the policy applies to all desktops in the current project.

Figure 1-24 Selecting an object



< | **Create Policy**

✓ Create Policy —— ✓ Configure Policy —— **3 Select Object** —— 4 Finish

Available Objects: All desktops

☑ Options

☑ All desktops (including created and to-be-created)

Selected Objects: (1) All

Options	Object Type	Operation
All desktops (including created and to-be-created)	All desktops	×

l. Click **Next: Finish**.

- **Clipboard redirection**

  Clipboard redirection supports file copy between storage devices and desktops.

  a. Log in to the console as an administrator.

  b. Click 📍 in the upper left corner of the console and select a region and a project.

  c. Click ☰ and choose **Business Applications** > **Workspace** in the service list.

The **Dashboard** page is displayed.

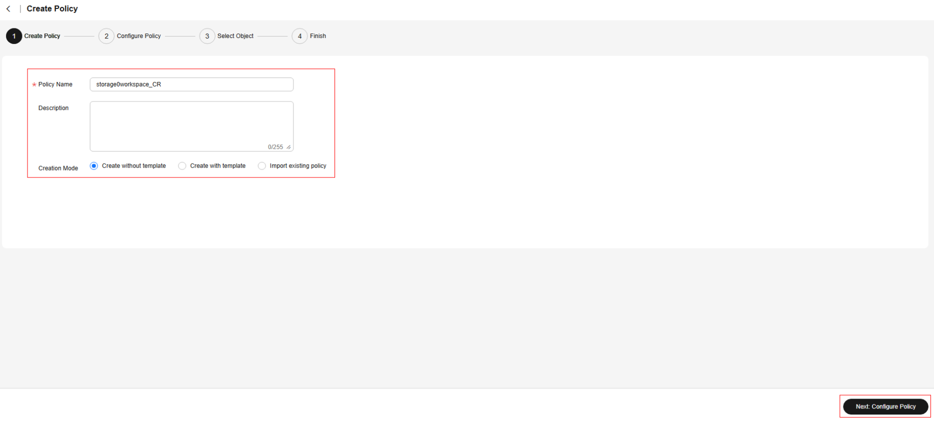
d. In the navigation pane on the left, choose **Policies** > **Protocol Policies**.

e. Click **Create Policy** in the upper right corner.

f. Configure the policy name, description, and creation mode, and click **Next: Configure Policy**.

- The policy name can contain up to 55 characters in digits, letters, and underscores (_), for example, **storage0workspace_CR**.
- The description can contain up to 255 characters, for example, **Clipboard redirection is used to copy files between external devices and desktops**.
- Retain the default creation mode.

Figure 1-25 Creating a policy



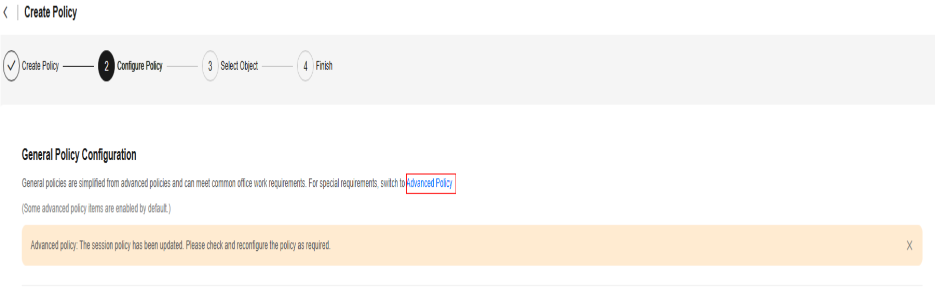
* Policy Name: storage0workspace_CR

Description:

Creation Mode: ● Create without template ○ Create with template ○ Import existing policy

g. Click **Advanced Policies**.

Figure 1-26 Advanced policy entry



General Policy Configuration

General policies are simplified from advanced policies and can meet common office work requirements. For special requirements, switch to Advanced Policy

(Some advanced policy items are enabled by default.)

Advanced policy: The session policy has been updated. Please check and reconfigure the policy as required.

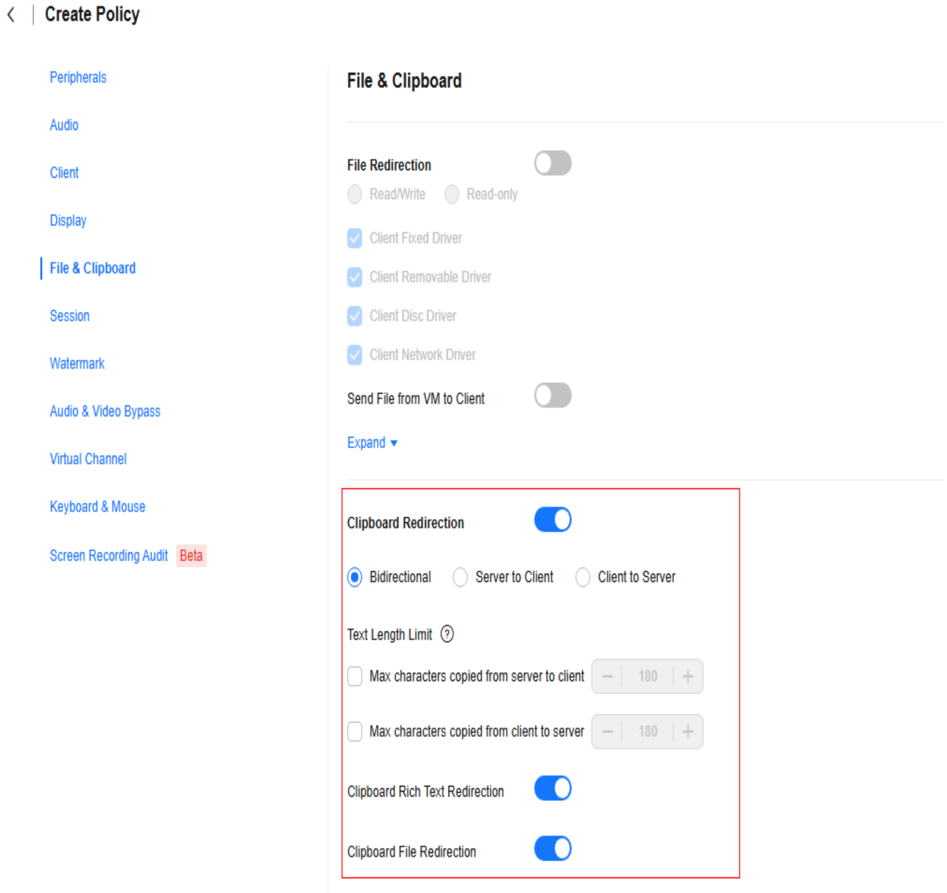
h. On the **Advanced Policies** page, click **Files and Clipboards**.

i. Enable the **Clipboard Redirection** policy and select **Bidirectional**, as shown in **Figure 1-27**.

NOTE

- Rich text copy and file copy are supported only when both the client (TC/SC) and desktop run Windows. A maximum of 500 files can be copied at a time.
- If the OS of a client (TC/SC or mobile client) or desktop is not Windows, only text can be copied.

Figure 1-27 Configuring the policy



< | Create Policy

Peripherals
Audio
Client
Display
File & Clipboard
Session
Watermark
Audio & Video Bypass
Virtual Channel
Keyboard & Mouse
Screen Recording Audit Beta

File & Clipboard

File Redirection (off)
○ Read/Write ○ Read-only
☑ Client Fixed Driver
☑ Client Removable Driver
☑ Client Disc Driver
☑ Client Network Driver

Send File from VM to Client (off)

Expand ▾

Clipboard Redirection (on)
● Bidirectional ○ Server to Client ○ Client to Server

Text Length Limit ?
□ Max characters copied from server to client − 180 +
□ Max characters copied from client to server − 180 +

Clipboard Rich Text Redirection (on)

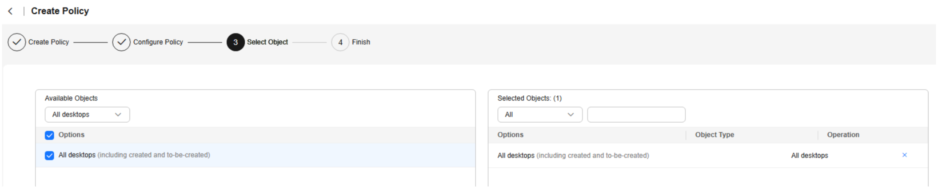
Clipboard File Redirection (on)

j. Click **Next: Select objects**.

k. Select an object as required.

For example, if you select **All desktops**, the policy applies to all desktops in the current project.

Figure 1-28 Selecting an object



< | Create Policy

✓ Create Policy — ✓ Configure Policy — 3 Select Object — 4 Finish

Available Objects
All desktops ▾
☑ Options
☑ All desktops (including created and to-be-created)

Selected Objects: (1)
All ▾

Options	Object Type	Operation
All desktops (including created and to-be-created)	All desktops	×

l. Click **Next: Finish**.

1.5 Networking

1.5.1 What Are the Network Requirements for Logging In to Desktops?

Table 1-2 lists the network requirements for logging in to desktops. To ensure good user experience, the network QoS should be at the good level or above. Enterprise customers are advised to access desktops through Direct Connect.

Table 1-2 Network QoS requirements

Level	Network QoS Requirement	User Experience
Excellent	● Packet loss rate ≤ 0.01% ● Round-trip latency ≤ 30 ms ● Network jitter ≤ 10 ms	1. Smooth office work (Word, Excel, Notepad, etc.) 2. Smooth audio/video playback 3. Smooth operations on peripherals such as USB flash drives
Good	● Packet loss rate ≤ 0.1% ● Round-trip latency ≤ 50 ms ● Network jitter ≤ 10 ms	1. Smooth office work (Word, Excel, Notepad, etc.) 2. Relatively smooth audio/video playback (occasional freezing) 3. Slow identification of peripherals and delayed response to operations on storage devices, such as slow data copy of USB flash drives
Acceptable	● Packet loss rate ≤ 0.3% ● Round-trip latency ≤ 100 ms ● Network jitter ≤ 40 ms	1. Office work (Word, Excel, Notepad, etc.) available 2. Audio/video playback (including QQ Music and Storm Player) freezing 3. Peripherals (such as USB flash drives and cameras) basically unusable

1.5.2 How Do I Configure Internet Access for a Cloud Desktop?

To configure Internet Access for a cloud desktop, see **Configuring Cloud Desktops to Access the Internet**.

1.5.3 How Do I Configure Enterprise Intranet Access for a Cloud Desktop?

To configure enterprise intranet access for a cloud desktop, see **Configuring Cloud Desktops to Access the Enterprise Intranet**.

1.5.4 What If My Desktop Cannot Access the Internet?

Checking whether Internet access has been enabled

Step 1 Log in to the console as an administrator.

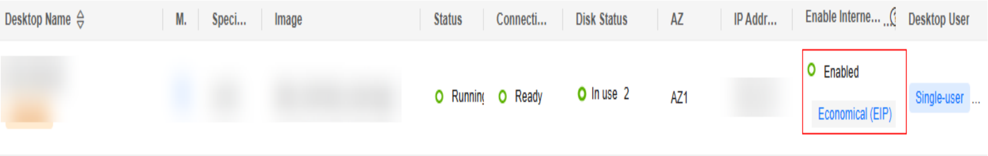
Step 2 Click 📍 in the upper left corner of the console and select a region and a project.

Step 3 Click ☰ and choose **Business Applications** > **Workspace** in the service list.

The **Dashboard** page is displayed.

Step 4 In the navigation pane, choose **Desktops**.

Figure 1-29 Desktop network status



Desktop Name	M.	Speci...	Image	Status	Connecti...	Disk Status	AZ	IP Addr...	Enable Interne...	Desktop User
[illegible]	[illegible]	[illegible]	[illegible]	○ Runnin	○ Ready	○ In use 2	AZ1	[illegible]	○ Enabled Economical (EIP)	Single-user ...

Check whether Internet access has been enabled for desktops in the service subnet.

- If **Enabled** is displayed in the **Internet Access** column, go to **Step 5**.
- If **Disabled** is displayed, **configure Internet access for the desktop** and ask the user to try again. If the Internet access still fails, go to **Step 5**.

Checking whether the network configuration is correct

Step 5 Check whether the network configuration is correct by referring to **Public NAT Gateway Troubleshooting**.

- If the network configuration is correct, go to **Step 6**.
- If the network configuration is incorrect, modify the configuration by referring to **Public NAT Gateway Troubleshooting** and ask the user to try again. If the Internet access still fails, go to **Step 6**.

Submitting a service ticket

Step 6 **Submit a service ticket** for technical support.

----End

1.5.5 How Do I Enable Internet Access on Other Cloud Service Pages?

Scenarios

After you purchase a cloud desktop, the cloud desktop is in the VPC subnet by default and cannot access the Internet. You need to configure the NAT gateway to share an EIP so that the cloud desktop can access the Internet. You can use the quick entry on Workspace to enable the Internet, or access the NAT and EIP consoles to purchase services.

NOTE

This section describes how to purchase NAT and EIP services to enable Internet access for cloud desktops. You can use the quick entry on Workspace to purchase NAT and EIP services to enable the Internet. For details, see **Configuring Cloud Desktops to Access the Internet**.

Prerequisites

- You have obtained the region, project, VPC, and subnet information of the desktop that needs to access the Internet.
- You have the permission for performing operations on the NAT and EIP services.

  NOTE

  - By default, self-registered Huawei accounts have the operation permissions of all services on Huawei Cloud.
  - To use NAT and EIP, the IAM account created under the Huawei account must be added to the **admin** user group or a user group with NAT and EIP operation permissions. You can go to the IAM page to check whether the account belongs to the **admin** user group. If the user group is not an **admin** user group, grant the IAM account the permission to use the NAT and EIP services. For details, see **Granting NAT Gateway Permissions** and **Granting EIP Permissions**.

Procedure (Not Interconnecting with Windows AD)

Creating an EIP

Step 1 Log in to the console as an administrator.

Step 2 Click 📍 in the upper left corner and select the region and project of the desktop that needs to access the public network.

Step 3 Click ☰ and choose **Networking** > **Elastic IP** in the service list.

Step 4 On the page displayed, click **Buy EIP**.

Step 5 Configure the parameters by referring to **Assigning an EIP**.

NOTE

Select the region and project of the desktop that needs to access the public network.

Step 6 Click **Next**.

Step 7 Confirm the configuration and click **Submit**.

Buying a public NAT gateway

Step 8 Click ☰ and choose **Networking** > **NAT Gateway** in the service list.

Step 9 Click **Buy Public NAT Gateway**.

Step 10 Configure the parameters by referring to **Purchasing a Public NAT Gateway**.

NOTE

Select the VPC and subnet of the desktop that needs to access the public network.

Step 11 Click **Next**.

Step 12 Confirm the configuration and click **Submit**.

Step 13 On the page for adding a rule, click **Cancel**.

Checking whether the VPC has a route to the NAT gateway

Step 14 Click ☰ and choose **Business Applications** > **Workspace** in the service list.

Step 15 Click **Tenant Configuration**.

Step 16 Click the VPC name of the tenant to go to its basic information page.

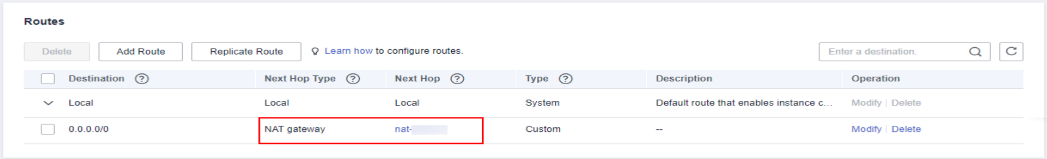
Step 17 In the **Networking Components** area on the right of the page, click the *number next to **Route Tables*** to go to the route table list page of the VPC.

Step 18 Click the *target route table name* to view the basic information list.

Step 19 Check whether there is a route whose next hop is the NAT gateway in the route list.

The NAT gateway automatically creates a route 0.0.0.0/0 from the VPC to the NAT gateway to allow traffic from the VPC to the NAT gateway, as shown in **Figure 1-30**.

Figure 1-30 Route to the NAT gateway



	Destination ⓘ	Next Hop Type ⓘ	Next Hop ⓘ	Type ⓘ	Description	Operation
∨	Local	Local	Local	System	Default route that enables instance c...	Modify | Delete
□	0.0.0.0/0	NAT gateway	nat-[redacted]	Custom	--	Modify | Delete

- If the route shown in **Figure 1-30** exists, go to **Step 20**.
- If the route shown in **Figure 1-30** does not exist, add such a route and go to **Step 20**.

Adding an SNAT rule

Step 20 Click ☰ and choose **Networking** > **NAT Gateway** in the service list.

Step 21 On the displayed page, locate the NAT gateway created in **Step 12** and click **Configure Rules** in the **Operation** column.

Step 22 On the **SNAT Rules** tab page, click **Add SNAT Rule**.

Step 23 Configure the parameters by referring to **Adding an SNAT Rule**.

> NOTE
>
> Set **Scenario** to **VPC**, **Subnet** to **Existing**, and **EIP** to the EIP purchased in **Step 7**.

Step 24 Click **OK**.

If the added SNAT rule is in the **Running** status, the rule has been added.

Verifying whether the desktop can access the public network through the NAT gateway

Step 25 Use a terminal user account and password to log in to the desktop from the client to check whether the desktop can access the public network.

----End

Procedure (Interconnecting with Windows AD)

Creating an EIP

Step 1 Log in to the console as an administrator.

Step 2 Click ⊙ in the upper left corner and select the region and project of the desktop that needs to access the public network.

Step 3 Click ☰ and choose **Networking** > **Elastic IP** in the service list.

Step 4 On the page displayed, click **Buy EIP**.

Step 5 Configure the parameters by referring to **Assigning an EIP**.

NOTE

Select the region and project of the desktop that needs to access the public network.

Step 6 Click **Next**.

Step 7 Confirm the configuration and click **Submit**.

Buying a public NAT gateway

Step 8 Click ☰ and choose **Networking** > **NAT Gateway** in the service list.

Step 9 Click **Buy Public NAT Gateway** to go to the **Buy Public NAT Gateway** page.

Step 10 Configure the parameters by referring to **Purchasing a Public NAT Gateway**.

NOTE

Select the VPC and subnet of the desktop that needs to access the public network.

Step 11 Click **Next**.

Step 12 Confirm the configuration and click **Submit**.

Step 13 On the page for adding a rule, click **Cancel**.

Checking whether the VPC has a route to the NAT gateway

Step 14 Click ☰ and choose **Business Applications** > **Workspace** in the service list.

Step 15 Click **Tenant Configuration**.

Step 16 Click the VPC name of the tenant to go to its basic information page.

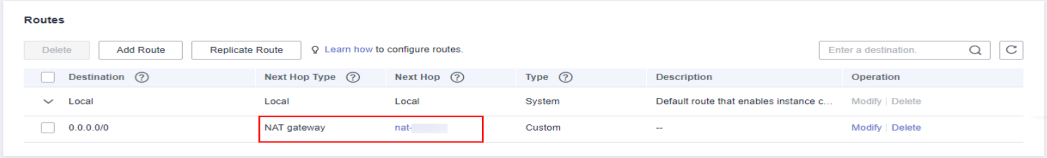
Step 17 In the **Networking Components** area on the right of the page, click the *number next to* ***Route Tables*** to go to the route table list page of the VPC.

Step 18 Click the *target route table name* to view the basic information list.

Step 19 Check whether there is a route whose next hop is the NAT gateway in the route list.

The NAT gateway automatically creates a route 0.0.0.0/0 from the VPC to the NAT gateway to allow traffic from the VPC to the NAT gateway, as shown in **Figure 1-30**.

Figure 1-31 Route to the NAT gateway



Routes

Delete | Add Route | Replicate Route | Learn how to configure routes. | Enter a destination.

□	Destination	Next Hop Type	Next Hop	Type	Description	Operation
﹀	Local	Local	Local	System	Default route that enables instance c...	Modify | Delete
□	0.0.0.0/0	NAT gateway	nat-[redacted]	Custom	--	Modify | Delete

- If the route shown in **Figure 1-30** exists, go to **Step 20**.
- If the route shown in **Figure 1-30** does not exist, add such a route and go to **Step 20**.

Adding an SNAT rule

Step 20 Click ☰ and choose **Networking** > **NAT Gateway** in the service list.

Step 21 On the displayed page, locate the NAT gateway created in **Step 12** and click **Configure Rules** in the **Operation** column.

Step 22 On the **SNAT Rules** tab page, click **Add SNAT Rule**.

Step 23 Configure the parameters by referring to **Adding an SNAT Rule**.

NOTE

Set **Scenario** to **VPC**, **Subnet** to **Existing**, and **EIP** to the EIP purchased in **Step 7**.

Step 24 Click **OK**.

If the added SNAT rule is in the **Running** status, the rule has been added.

Configuring DNS forwarding

Step 25 Log in to the DNS server as an administrator.

Step 26 On the taskbar in the lower left corner, click ⊞.

Step 27 Click on the right of the **Start** menu.

Step 28 The **Server Manager** window is displayed.

Step 29 In the navigation pane on the left, click **DNS**.

Step 30 In the **SERVERS** area, right-click a *Server name* and choose **DNS Manager** from the shortcut menu.

Step 31 The **DNS Manager** dialog box is displayed.

Step 32 Expand **DNS**. Right-click the computer name, and choose **Properties** from the shortcut menu.

Step 33 On the **Advanced** tab page, deselect **Disable recursion (also disable forwarders)** and click **Apply**.

Step 34 On the **Forwarder** tab page, click **Edit**, enter the default DNS server IP address of the desktop region in the text box, and click **OK**.

NOTE

Obtain the default DNS server IP address of the desktop region from **What Are Huawei Cloud Private DNS Server Addresses?**

Verifying whether the desktop can access the public network through the NAT gateway

Step 35 Use a terminal user account and password to log in to the desktop from the client to check whether the desktop can access the public network.

----End

1.5.6 How Do I Configure Security Group Rules When Using a Custom Security Group?

Scenarios

When changing a desktop security group, check whether the security group in use has allowed the inbound and outbound rules required for desktop access. If not, desktop access will be affected.

Procedure

Interconnected with an AD domain

NOTE

- Allow at least the IP addresses whose destination addresses are AD/DNS and ports of AD/DNS in the outbound rules of the security group. View the port list in **Configuring Network Connection Between Cloud Desktops and Windows AD**.
- If Workspace needs to access other service systems, configure security group rules as needed.

Direct Connect access

Step 1 **Log in to the console**.

In the navigation pane, choose **Desktops** > **Desktops**.

The **Desktops** page is displayed.

Step 2 Configure the desktop network.

- To check the security group configuration of a single desktop, perform **Step 3** and **Step 6** to **Step 11**.
- To batch check the security group configuration of desktops, perform **Step 4** to **Step 11**.

Step 3 Locate the row that contains the desktop whose security group is to be changed and choose **More** > **Network Settings** > **Desktop Network Settings** in the **Operation** column.

Step 4 Batch select multiple desktops whose security groups are to be changed and choose **More** > **Desktop Network Settings** in the upper left corner. The **Desktop Network Settings** page is displayed.

Step 5 Select **Use the new security group** for **Security Group**.

Step 6 Click **View existing security groups**. The **Security Groups** page of **Network Console** is displayed.

Step 7 Click **Manage Rules** in the **Operation** column of the desired security group.

Step 8 Check whether the ports listed in **Table 1-3** exist under the **Inbound Rules** tab.

Table 1-3 Ports

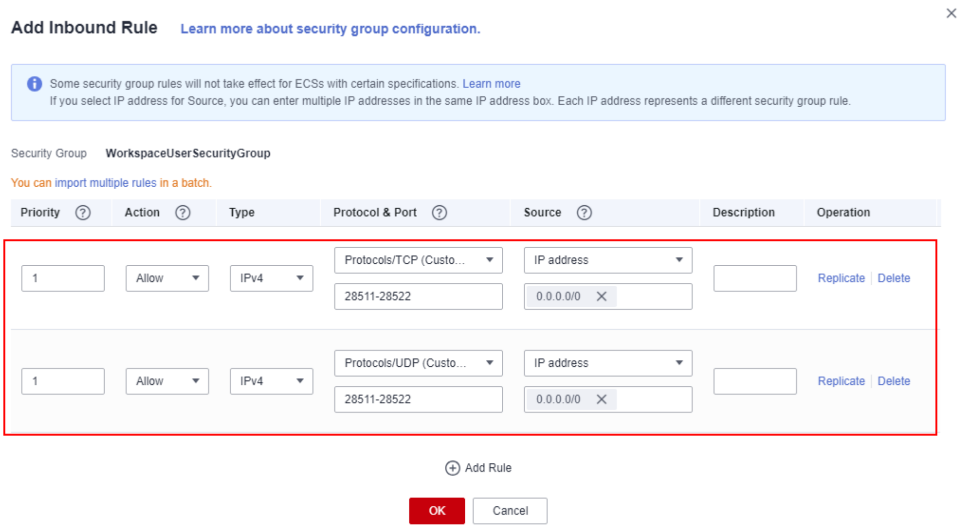
Port	Protocol	Description
28511–28512	TCP	Desktops are accessed through the gateway.
28511–28512	UDP	Desktops are accessed through the gateway.

- If yes, the security group has allowed the inbound rules required for desktop access. You do not need to add the rules again.
- If no, perform **Step 9** to **Step 11**.

Step 9 Under the **Inbound Rules** tab of the security group, click **Add Rule**. The **Add Inbound Rule** window is displayed.

Step 10 Click ⊕ to add a rule.

Figure 1-32 Adding an inbound rule



Add Inbound Rule Learn more about security group configuration.

Some security group rules will not take effect for ECSs with certain specifications. Learn more
If you select IP address for Source, you can enter multiple IP addresses in the same IP address box. Each IP address represents a different security group rule.

Security Group WorkspaceUserSecurityGroup

You can import multiple rules in a batch.

Priority	Action	Type	Protocol & Port	Source	Description	Operation
1	Allow	IPv4	Protocols/TCP (Custo... 28511-28522	IP address 0.0.0.0/0		Replicate | Delete
1	Allow	IPv4	Protocols/UDP (Custo... 28511-28522	IP address 0.0.0.0/0		Replicate | Delete

Step 11 Click **OK**.

----End

1.5.7 How Do I Allow Traffic to Pass Through Specified Service IP Addresses and Ports When There Is Access Control on Desktop Access?

Table 1-4 Service IP addresses and ports of Workspace

Access Scenario	IP Address	Port	Protocol	Description
Internet access	Access IP address	443	TCP	Internet access address
	Public IP address of the desktop access gateway	8443	TCP	Port for HDP data communication based on TCP
		8502–8509	UDP	Port for HDP data communication based on UDP
		8601	TCP	TCP port for WebSocket-based data communication between the browser and access gateway
	IP address of the network acceleration node accessed by desktops	20000–22000	UDP	IP address of the network acceleration node accessed by cloud desktops
		6447, 443	TCP	
	IP address for client software download	443	TCP	Address for downloading the Workspace client software package
	Log reporting	443	TCP	Log reporting
	IP address for reporting client metrics	8903	TCP	Reporting metrics such as the network latency, jitter, and packet loss rate during a desktop's network access
Direct Connect access	Access IP address	443	TCP	Direct Connect access address

Access Scenario	IP Address	Port	Protocol	Description
	Private IP address of the desktop access gateway	8443	TCP	Port for HDP data communication based on TCP
		8502-8509	UDP	Port for HDP data communication based on UDP
		8601	TCP	TCP port for WebSocket-based data communication between the browser and access gateway

NOTE

- The IP addresses in the preceding table may change. For access control such as firewalls and security groups, you are advised to allow traffic to pass through ports in the preceding table.
- If you need to allow traffic to pass through IP addresses in the preceding table, **submit a service ticket** for technical support.

1.5.8 Can My Desktops Use a Shared Bandwidth?

Yes. A shared bandwidth can be shared by multiple EIPs and controls the data transfer rate on these EIPs in a centralized manner. All cloud desktops that have EIPs bound in the same region can share a bandwidth. For details, see **Shared Bandwidth Overview**.

1.6 Identity Authentication and AD Configuration

1.6.1 How Do I Deploy a Windows AD Server?

Huawei does not provide Windows AD servers. Users need to purchase and configure Windows AD servers. If you need to use Windows AD authentication but do not have a Windows AD server, perform the following operations:

Buying an ECS

Step 1 For details, see **Buying an ECS**.

NOTE

- The server OS must be Windows Server 2016 or 2019.
- The SIDs of ECSs created using the same image are the same. As a result, some users cannot log in to the desktop. If you need to create multiple Windows AD servers, use different images.

Logging in to the ECS

Step 2 In the ECS list, click **Remote Login** in the **Operation** column of the created ECS.

Step 3 Click **Send CtrlAltDel** in the upper right corner of the remote login screen.

Step 4 Enter the password of the ECS to log in.

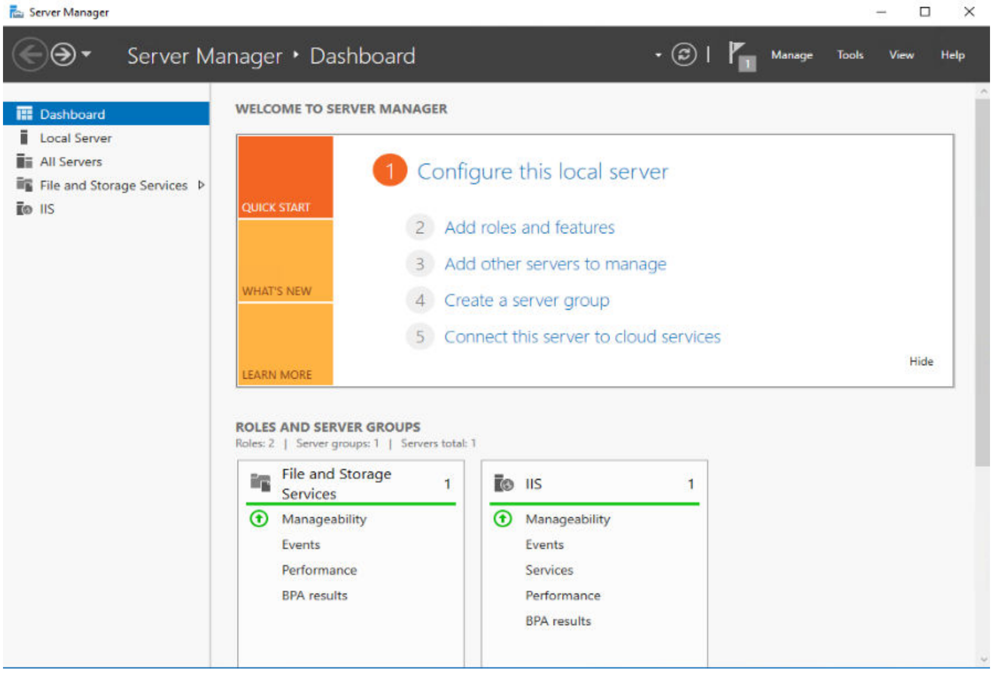
Adding the Windows AD role and backup feature

Step 5 On the taskbar in the lower left corner, click ⊞.

Step 6 Click on the right of the **Start** menu.

The **Server Manager** window appears, as shown in **Figure 1-33**.

Figure 1-33 Server Manager



Step 7 In the middle of the page, click **Add roles and features**.

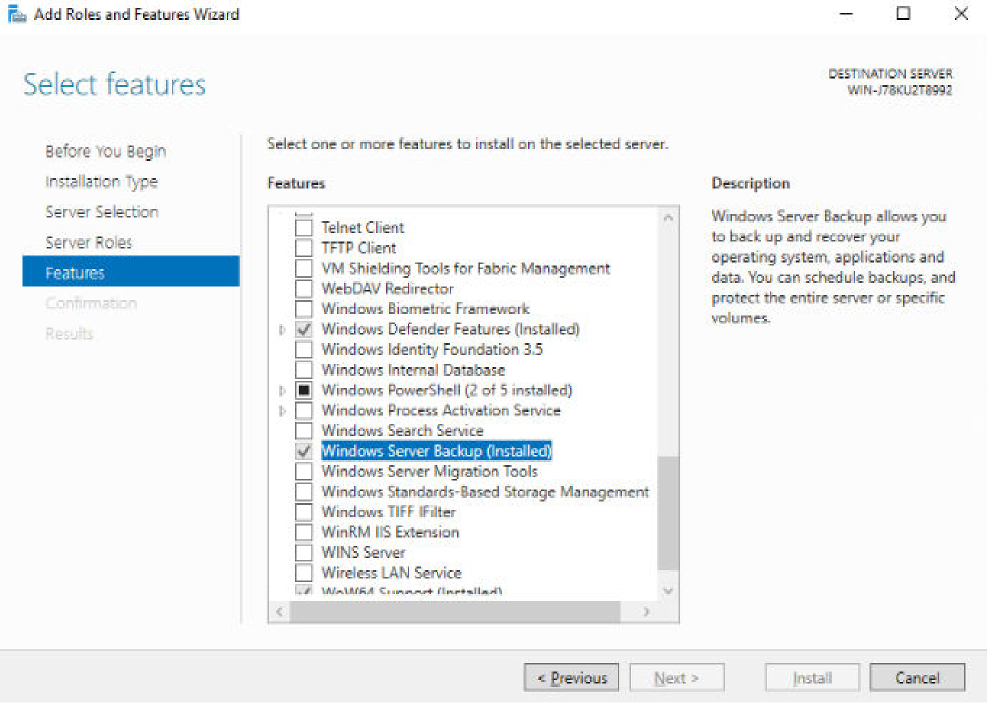
The **Add Roles and Features Wizard** dialog box is displayed.

Step 8 Click **Next** three times.

Step 9 In the **Roles** area, select **Active Directory Domain Services**. In the dialog box displayed, click **Add Features**. Then, click **Next**.

Step 10 In the **Features** area, select **Windows Server Backup**.

Figure 1-34 Enabling the backup feature



Add Roles and Features Wizard

Select features

DESTINATION SERVER
WIN-J78KU2T8992

Select one or more features to install on the selected server.

Features

- □ Telnet Client
- □ TFTP Client
- □ VM Shielding Tools for Fabric Management
- □ WebDAV Redirector
- □ Windows Biometric Framework
- ▷ ☑ Windows Defender Features (Installed)
- □ Windows Identity Foundation 3.5
- □ Windows Internal Database
- ▷ ■ Windows PowerShell (2 of 5 installed)
- ▷ □ Windows Process Activation Service
- □ Windows Search Service
- ☑ Windows Server Backup (Installed)
- □ Windows Server Migration Tools
- □ Windows Standards-Based Storage Management
- □ Windows TIFF IFilter
- □ WinRM IIS Extension
- □ WINS Server
- □ Wireless LAN Service
- ☑ WoW64 Support (Installed)

Description

Windows Server Backup allows you to back up and recover your operating system, applications and data. You can schedule backups, and protect the entire server or specific volumes.

Step 11 Click **Next** till the confirmation dialog box appears.

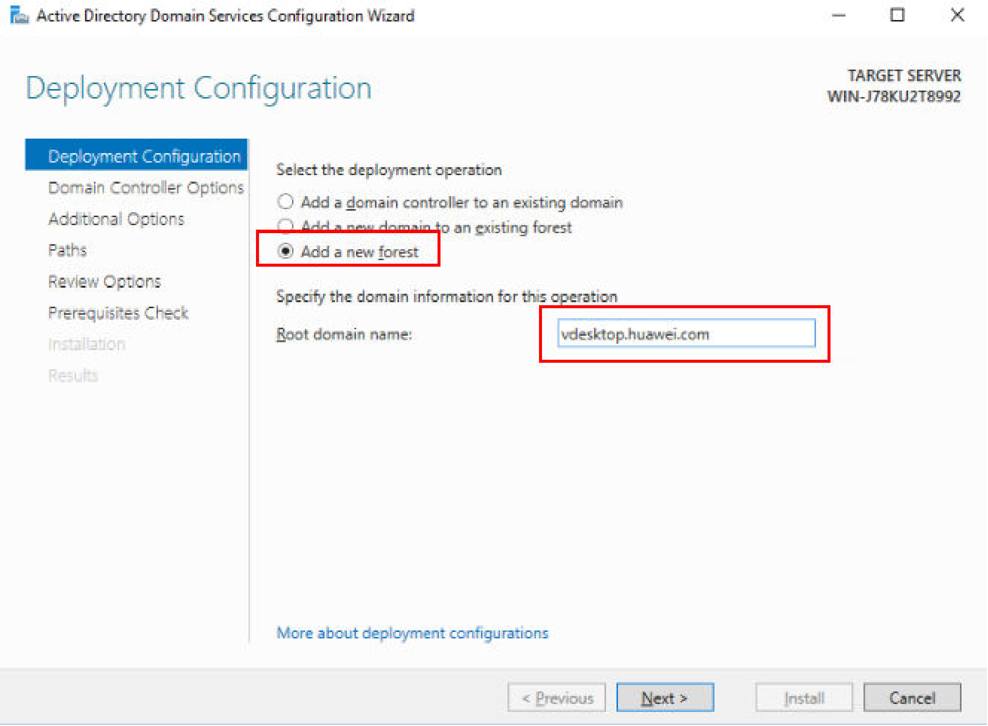
Step 12 Click **Install**.

You can see the installation progress bar. When **Installation succeeded** is displayed, the installation is successful.

Step 13 In the upper right corner of the **Server Manager** page, click ⚠, and select **Promote this server to a domain controller**.

The **Active Directory Domain Services Configuration Wizard** window appears, as shown in **Figure 1-35**.

Figure 1-35 Active Directory Domain Services Configuration Wizard


Active Directory Domain Services Configuration Wizard

Deployment Configuration

TARGET SERVER
WIN-J78KU2T8992

Select the deployment operation

○ Add a domain controller to an existing domain

○ Add a new domain to an existing forest

● Add a new forest

Specify the domain information for this operation

Root domain name: vdesktop.huawei.com

More about deployment configurations

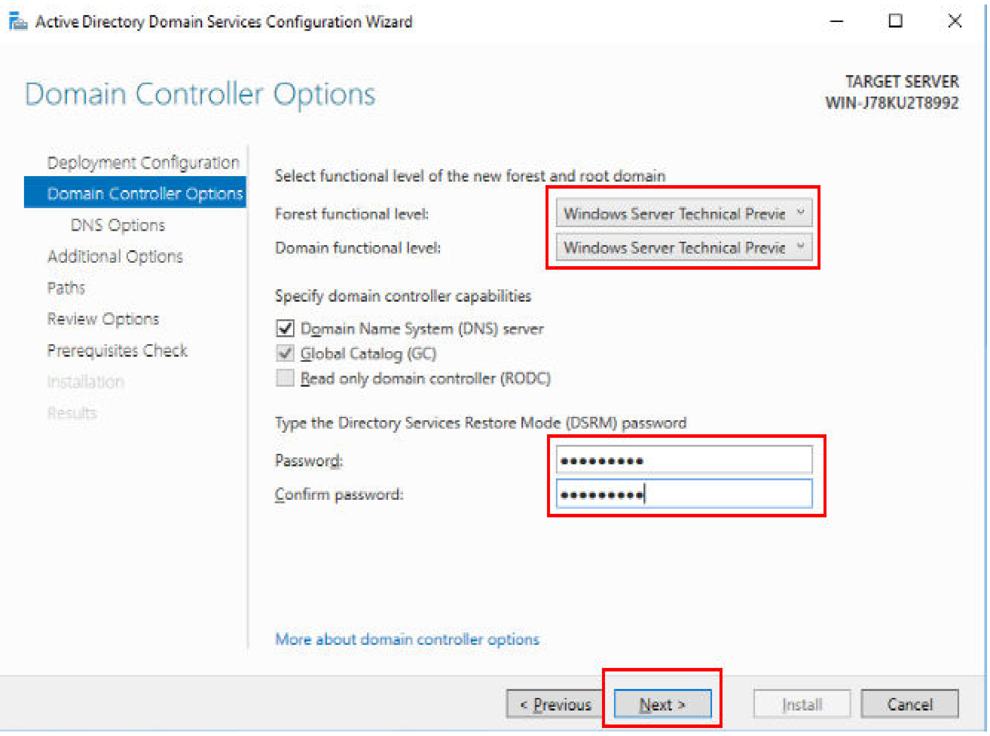
Step 14 Select **Add a new forest**, specify **Root domain name**, and click **Next**.

Step 15 Set both **Forest functional level** and **Domain functional level** to **Windows Server 2016**, set **Type the Directory Services Restore Mode (DSRM) password**, and click **Next**, as shown in **Figure 1-36**.

NOTE

In DSRM, only the DSRM administrator account can be used to log in to the system.

Figure 1-36 Configuring a domain controller



Domain Controller Options

TARGET SERVER
WIN-J78KU2T8992

Select functional level of the new forest and root domain

Forest functional level: Windows Server Technical Previe

Domain functional level: Windows Server Technical Previe

Specify domain controller capabilities

☑ Domain Name System (DNS) server

☑ Global Catalog (GC)

□ Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password: ●●●●●●●●●●

Confirm password: ●●●●●●●●●●

Step 16 Retain the default values, click **Next** four times, and click **Install**.

Install the Windows AD service and restart the VM as prompted.

Step 17 After the restart, log in to the Windows AD server using the administrator account.

The administrator account is in the *User domain name***\Administrator** format, for example, **vdesktop.huawei.com\Administrator**.

(Optional) Installing the Windows AD service on a standby server

Perform this operation only when a standby Windows AD server is required.

Step 18 Configure a standby Windows AD server by referring to **Step 2** to **Step 17**.

----End

1.6.2 What If the Interconnection Between a Desktop and an AD Domain Failed?

Step 1 Check whether the information on the interconnection page is consistent with that on the local Windows AD server.

- If yes, go to **Step 2**.
- If no, modify the parameters on the desktop interconnection page and try again. If the interconnection still fails, go to **Step 2**.

Step 2 Check whether the desktop and Windows AD are in the same VPC.

- If yes, go to **Step 3**.
- If no, **configure network connection between the desktop and Windows AD**. If the interconnection still fails, go to **Step 3**.

Step 3 Check whether the inbound security group rules of the Windows AD are correctly set.

- If yes, go to **Step 4**.
- If no, add inbound security group rules by referring to **Configuring Network Connection Between Cloud Desktops and Windows AD**. If the interconnection still fails, go to **Step 4**.

Step 4 **Submit a service ticket** for technical support.

----End

1.6.3 How do I Enable LDAPS on the AD Server?

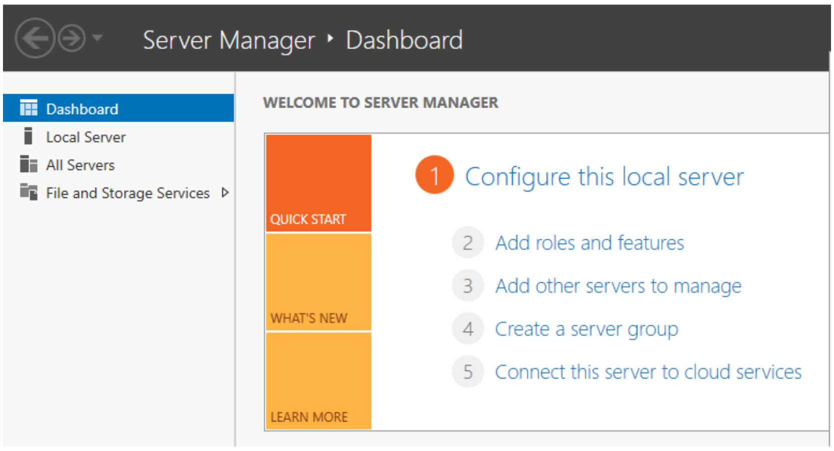
If an enterprise needs to enable LDAPS so that cloud desktops can communicate with AD server applications using LDAPS, perform the following operations:

- If an independent AD server is used, **enable LDAPS on the Active AD server** > **verify the connection between LDAPS and the active AD server**.
- If the AD servers work in active/standby mode, **enable LDAPS on the active AD server** > **verify the connection between LDAPS and the active AD server** > **enable LDAPS on the standby AD server** > **verify the connection between LDAPS and the standby AD server**.

Enabling LDAPS on the Active AD Server

Step 1 Log in to the active AD server. On the taskbar in the lower left corner, click ⊞ and click **Server Manager**. The server configuration page is displayed, as shown in **Figure 1-37**.

Figure 1-37 Server Manager



Server Manager ‣ Dashboard
Dashboard
Local Server
All Servers
File and Storage Services ▷
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services

Step 2 In the **Dashboard** tab page, click **Add roles and features**. The **Add Roles and Features Wizard** dialog box is displayed.

Step 3 Click **Next** until the **Select destination server** page is displayed.

Step 4 Select a destination server.

NOTE

To obtain the name and IP address of the destination server, choose **Tools** > **Active Directory Users and Computers** > **Domain Controllers** on the **Dashboard** tab page of **Server Manager**.

Step 5 Click **Next**. The **Select server roles** page is displayed.

Step 6 Click **Active Directory Certificate Services**.

Step 7 Retain the default settings and click **Add Features**.

Step 8 Click **Next** until the **Select role services** page is displayed.

Step 9 Select **Certification Authority Web Enrollment** and click **Add Features**.

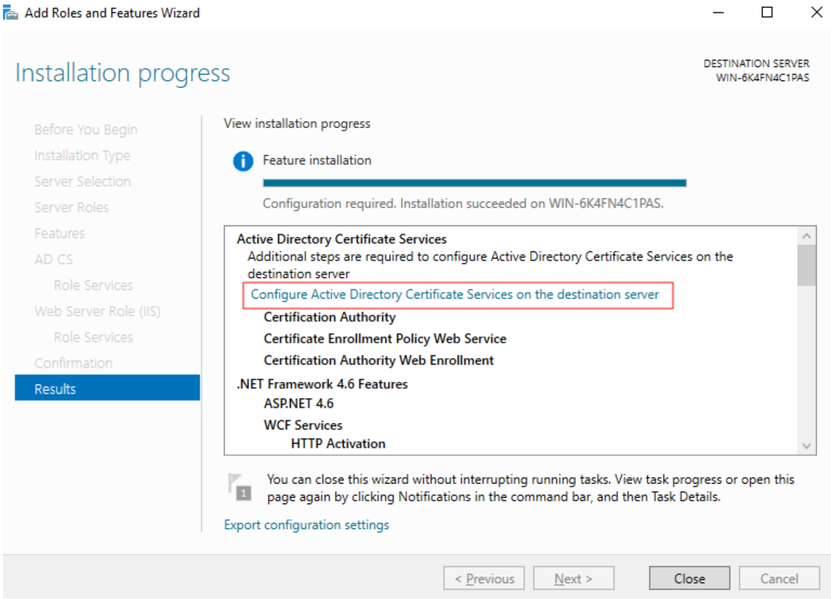
Step 10 Select **Certification Enrollment Policy Web Service** and click **Add Features**.

Step 11 Click **Next** until the confirmation page is displayed.

Step 12 Click **Install**.

Step 13 After the installation is complete, click **Configure Active Directory Certificate Services on the destination server** under **Active Directory Certificate Services**, as shown in **Figure 1-38**. The **AD CS Configuration** page is displayed.

Figure 1-38 Configuring the Active Directory certificate service



View installation progress

Feature installation

Configuration required. Installation succeeded on WIN-6K4FN4C1PAS.

Active Directory Certificate Services
Additional steps are required to configure Active Directory Certificate Services on the destination server
Configure Active Directory Certificate Services on the destination server
Certification Authority
Certificate Enrollment Policy Web Service
Certification Authority Web Enrollment
.NET Framework 4.6 Features
ASP.NET 4.6
WCF Services
HTTP Activation

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

Step 14 Retain the default settings and click **Next**. The **Role Services** page is displayed.

Step 15 Select **Certificate Authority**, **Certificate Authority Web Enrollment**, and **Certificate Enrollment Policy Web Service**, and click **Next**. The **Setup Type** page is displayed.

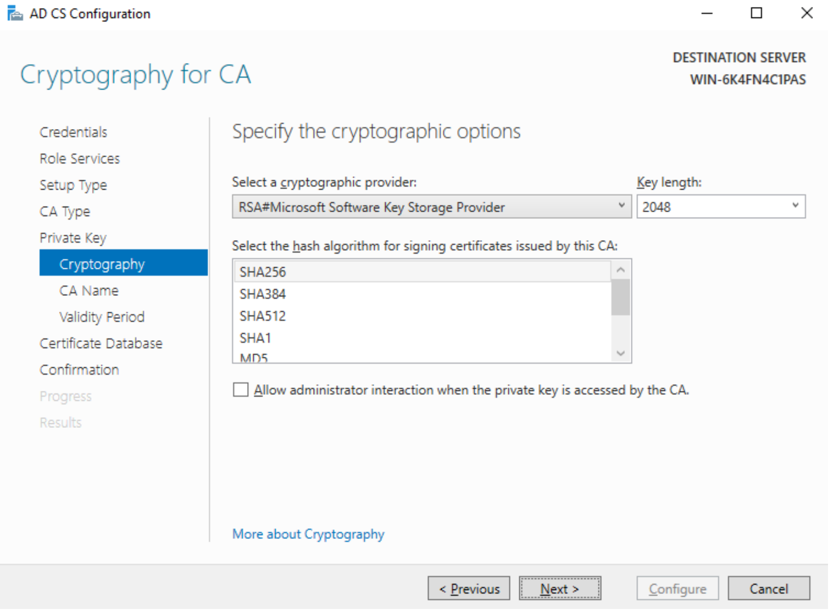
Step 16 Select **Enterprise CA** and click **Next**. The **Specify the type of the CA** page is displayed.

Step 17 Select **Root CA** and click **Next**. The **Specify the type of the private key** page is displayed.

Step 18 Select **Create a new private key** and click **Next**. The encryption configuration page is displayed.

Step 19 Set **Key length** to **2048** and select **SHA256** for the hash algorithm for signing certificates issued by the CA. Retain the default values for other parameters, as shown in **Figure 1-39**.

Figure 1-39 Cryptography settings



AD CS Configuration

Cryptography for CA

DESTINATION SERVER
WIN-6K4FN4C1PAS

Specify the cryptographic options

Select a cryptographic provider: RSA#Microsoft Software Key Storage Provider

Key length: 2048

Select the hash algorithm for signing certificates issued by this CA:

SHA256
SHA384
SHA512
SHA1
MD5

□ Allow administrator interaction when the private key is accessed by the CA.

Step 20 Click **Next**.

Step 21 Select **Select a certificate and assign it later for SSL** and click **Next**. The confirmation page is displayed.

Step 22 Click **Configure**.

Step 23 After the configuration is complete, click **Close**.

Step 24 Restart the active AD server.

----End

Verifying the LDAPS Connection of the Active AD Server

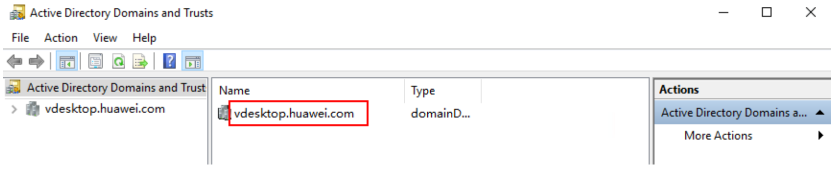
Step 1 On the desktop of the active AD server, click 🔍 and enter **Ldp** to start Ldp.

Step 2 On **Connection**, click **Connect**.

Step 3 In **Server**, enter the domain name to be connected, for example, **vdesktop.domain.com**.

To obtain the target domain name, choose **Tools** > **Active Directory Domains and Trusts** on the **Dashboard** tab page of **Server Manager**. The domain list page is displayed. The required domain name is displayed in the **Name** column, as shown in **Figure 1-40**.

Figure 1-40 Domain name


Active Directory Domains and Trusts
File Action View Help
Active Directory Domains and Trust
vdesktop.huawei.com
Name
Type
vdesktop.huawei.com
domainD...
Actions
Active Directory Domains a...
More Actions

Step 4 Enter **636** in **Port**.

Step 5 Select **SSL**.

Step 6 Click **OK**.

If RootDSE information is displayed in the right pane, the connection is successful.

----End

Enabling LDAPS on the Standby AD Server

Step 1 On the desktop of the active AD server, click 🔍 and enter **Run** to start the application.

Step 2 Enter **mmc** in **Open** to go to **Console Root**.

Step 3 Choose **File** > **Add/Remove Snap-ins**.

Step 4 In the **Available snap-ins** list, double-click **Certificates**.

Step 5 Select **Computer account** and click **Next** to select a computer.

Step 6 Select **Local computer: (the computer this console is running on)**, click **Finish**, and click **OK**.

Step 7 Under the **Console Root**, expand **Certificates**.

Step 8 Choose **Personal** > **Certificates**.

Step 9 Right-click the certificate whose **Intended Purposes** is **All** and choose **All Tasks** > **Export**. The certificate export wizard page is displayed.

Step 10 Click **Next**.

Step 11 Select **Yes, export the private key** and click **Next**.

Step 12 Select **Personal Information Exchange-PKCS#12(.PFX)**, select **Include all certificates in the certification path if possible**, and click **Next**. The security configuration page is displayed.

Step 13 Select **Group or user names**, select **Password**, and set the password. Click **Next**.

NOTE

Record the password, which will be used when you import a certificate.

Step 14 Click **Browse**, select a path for storing the certificate, set the certificate name, click **Save**, and click **Next**. The information confirmation page is displayed.

Step 15 Confirm the information and click **Finish**.

Step 16 Log in to the standby AD server.

Step 17 Copy the active AD server certificate exported from **Step 15** to the standby AD server.

Step 18 Open **Server Manager**.

Step 19 In the **Dashboard** tab page, click **Add roles and features**. The **Add Roles and Features Wizard** dialog box is displayed.

Step 20 Click **Next** until the **Select destination server** page is displayed.

Step 21 Select a destination server.

> NOTE
>
> To view the name and IP address of the destination server, choose **Tools** > **Active Directory Users and Computers** > **Domain Controllers** on the **Dashboard** tab page of **Server Manager**.

Step 22 Click **Next**. The **Select server roles** page is displayed.

Step 23 Click **Active Directory Certificate Services**.

Step 24 Retain the default settings and click **Add Features**.

Step 25 Click **Next** until the **Select role services** page is displayed.

Step 26 Select **Certification Authority Web Enrollment** and click **Add Features**.

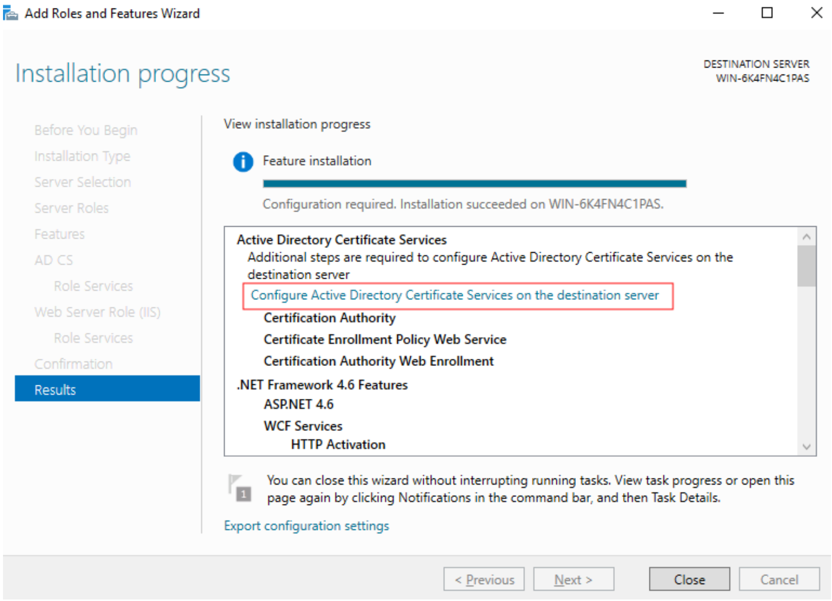
Step 27 Select **Certification Enrollment Policy Web Service** and click **Add Features**.

Step 28 Click **Next** until the confirmation page is displayed.

Step 29 Click **Install**.

Step 30 After the installation is complete, click **Configure Active Directory Certificate Services on the destination server** under **Active Directory Certificate Services**, as shown in **Figure 1-41**. The **AD CS Configuration** page is displayed.

Figure 1-41 Configuring the Active Directory certificate service



Add Roles and Features Wizard

Installation progress

DESTINATION SERVER
WIN-6K4FN4C1PAS

View installation progress

Feature installation

Configuration required. Installation succeeded on WIN-6K4FN4C1PAS.

Active Directory Certificate Services
Additional steps are required to configure Active Directory Certificate Services on the destination server
Configure Active Directory Certificate Services on the destination server
Certification Authority
Certificate Enrollment Policy Web Service
Certification Authority Web Enrollment
.NET Framework 4.6 Features
ASP.NET 4.6
WCF Services
HTTP Activation

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

Step 31 Retain the default settings and click **Next**. The **Role Services** page is displayed.

Step 32 Select **Certificate Authority**, **Certificate Authority Web Enrollment**, and **Certificate Enrollment Policy Web Service**, and click **Next**. The **Setup Type** page is displayed.

Step 33 Select **Enterprise CA** and click **Next**. The **Specify the type of the CA** page is displayed.

Step 34 Select **Root CA** and click **Next**. The **Specify the type of the private key** page is displayed.

Step 35 Select **Use existing private key**, select **Select a certificate and use its associated private key**, and click **Next**.

Step 36 Click **Import**, select the certificate file copied to the standby AD server in **Step 17**, enter the password set in **Step 13**, and click **OK**.

Step 37 After the certificate is imported, select the certificate in the **Certificates** list and click **Next**.

Step 38 Select **Select a certificate and assign it later for SSL** and click **Next**. The confirmation page is displayed.

Step 39 Click **Configure**.

Step 40 After the configuration is complete, click **Close**.

Step 41 Restart the standby AD server.

----End

Verifying the LDAPS Connection of the Standby AD Server

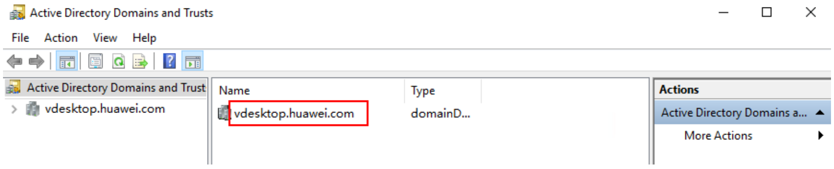
Step 1 On the desktop of the standby AD server, click 🔍 and enter **Ldp** to start Ldp.

Step 2 On **Connection**, click **Connect**.

Step 3 In **Server**, enter the domain name to be connected, for example, **vdesktop.domain.com**.

To obtain the target domain name, choose **Tools** > **Active Directory Domains and Trusts** on the **Dashboard** tab page of **Server Manager**. The domain list page is displayed. The required domain name is displayed in the **Name** column, as shown in **Figure 1-42**.

Figure 1-42 Domain name


Active Directory Domains and Trusts
File
Action
View
Help
Active Directory Domains and Trust
vdesktop.huawei.com
Name
Type
vdesktop.huawei.com
domainD...
Actions
Active Directory Domains a...
More Actions

Step 4 Enter **636** in **Port**.

Step 5 Select **SSL**.

Step 6 Click **OK**.

If RootDSE information is displayed in the right pane, the connection is successful.

----End

1.6.4 How do I Export the Root Certificate of an LDAPS-enabled AD server?

After LDAPS is enabled on the AD server, the administrator needs to configure the root certificate exported from the AD server on the management console for LDAPS to take effect.

NOTE

The LDAPS root certificates on the active and standby AD servers are the same. If the active and standby AD servers are used, you can log in to either AD server to obtain the certificate.

Step 1 Log in to the AD server, click 🔍, and enter **Run** to start the application.

Step 2 Enter **mmc** in **Open** to go to **Console Root**.

Step 3 Choose **File** > **Add/Remove Snap-ins**.

Step 4 In the **Available snap-ins** list, double-click **Certificates**.

Step 5 Select **Computer account** and click **Next** to select a computer.

Step 6 Select **Local computer: (the computer this console is running on)**, click **Finish**, and click **OK**.

Step 7 Under the **Console Root**, expand **Certificates**.

Step 8 Choose **Personal** > **Certificates**.

Step 9 Right-click the certificate whose **Certificate Template** is **Domain Controllers** and choose **All Tasks** > **Export**. The certificate export wizard page is displayed.

Step 10 Click **Next**.

Step 11 Select **No, do not export the private key** and click **Next**.

Step 12 Select **Base-64 encoded X.509 (.CER)** and click **Next**.

Step 13 Click **Browse**, select a path for storing the certificate, set the certificate name, click **Save**, and click **Next**. The information confirmation page is displayed.

Step 14 Confirm the configurations and click **Finish**.

----End

1.6.5 Can I Change the User Authentication Mode of the Desktop?

The user authentication mode cannot be changed for purchased desktops.

If the authentication mode of the purchased desktop is incorrect, purchase a desktop in another project that has no desktop and configure the required user authentication mode for the new desktop. Determine whether to interconnect the purchased desktop with an AD domain:

- If the enterprise does not deploy the Windows AD used for user authentication, select **No interconnection with AD** when purchasing desktops. That is, the desktop uses the account authentication system of Huawei for user authentication.
- If the enterprise deploys the Windows AD used for user authentication and the desktop also needs this authentication mode, select **Interconnection with AD** when purchasing the desktop. That is, the desktop uses the enterprise's Windows AD for user authentication.

NOTE

- For details about how to purchase a desktop, see **Purchasing Yearly/Monthly-billed Desktops**.
- For details about project-related operations, see **Project Management**.

1.7 Accounts and Permissions

1.7.1 What If I Lost the Administrator Password?

If you lost the password for logging in to the Workspace console, retrieve the password by referring to **What Can I Do If I Forgot My Password?** in **My Account**.

1.7.2 How Do I Unlock an End User Account?

If an enterprise AD domain is not used and an account is locked due to consecutive incorrect password inputs, you can unlock the account on the console.

NOTE

If an enterprise AD domain is used, you need to unlock the account on the AD server.

Procedure

Step 1 Log in to the console.

Step 2 Click **Users**.

The **Users** page is displayed.

Step 3 Select the user to unlock and choose **More** > **Unlock User**.

The dialog box of unlocking a user is displayed.

Step 4 Click **OK**.

----End

1.7.3 How Do I Do If a User Does Not Receive an Email for Creating a Desktop or Assigning a User?

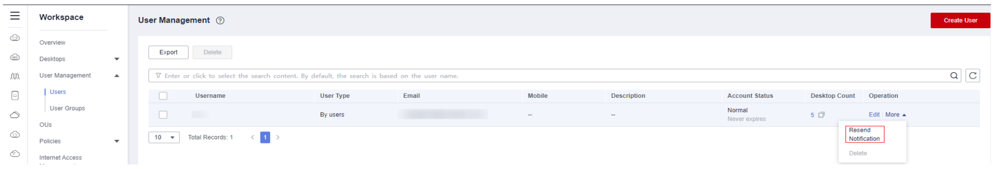
Step 1 Log in to the console.

Step 2 In the navigation pane, choose **Users** > **Users**.

The **Users** page is displayed.

Step 3 Select the target user and choose **More** > **Resend Notification**, as shown in **Figure 1-43**.

Figure 1-43 User management



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

----End

1.7.4 How Do I Do If the Message "Insufficient permissions for the IAM account. Security Administrator permissions required." Is Displayed When I Enable an Agency?

Scenarios

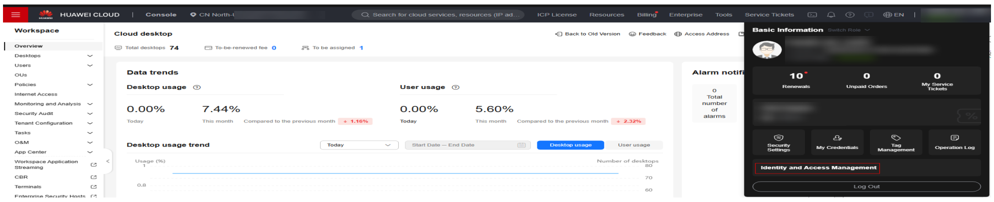
By default, IAM users do not have any permissions. If you use an IAM user for agency authorization, you must have the **Security Administrator** permissions.

Procedure

- Method 1: Contact the Huawei Cloud account for agency authorization. The agency authorization needs to be performed only once. Therefore, if the Huawei Cloud account has been authorized, the IAM user does not need to enable the agency.
- Method 2: Contact the Huawei Cloud account to add the **Security Administrator** permissions to the IAM user. Then, the IAM user can enable the agency.

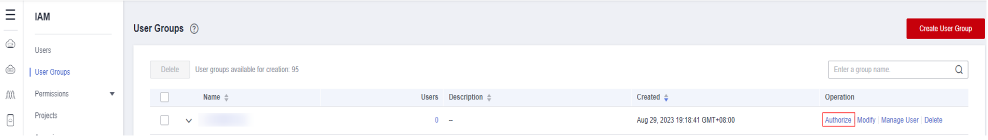
Step 1 Access the IAM page, as shown in **Figure 1-44**.

Figure 1-44 IAM entry



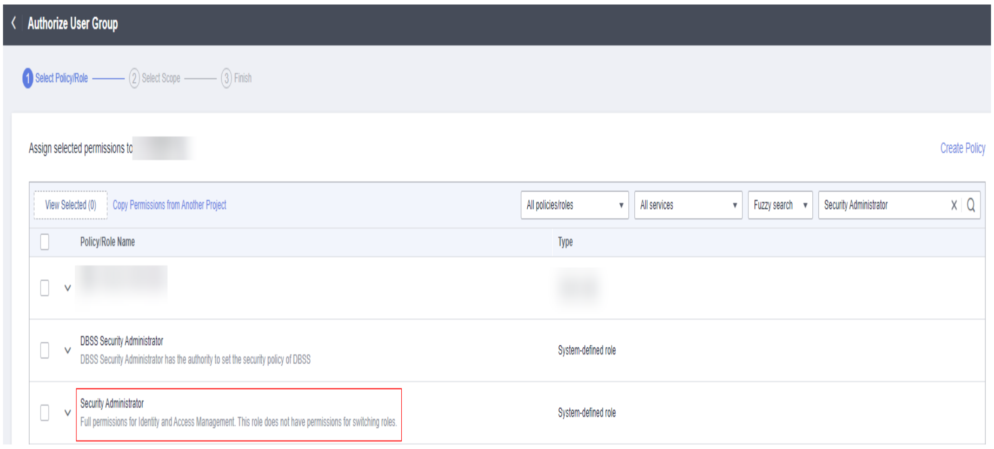
Step 2 Go to the user group page, select a user group to which the user belongs, and click **Authorize**, as shown in **Figure 1-45**.

Figure 1-45 User groups



Step 3 Select the target permissions. Enter **Security Administrator** in the search box. On the displayed page, select **Security Administrator**, and click **Next**, as shown in **Figure 1-46**.

Figure 1-46 Authorization



Authorize User Group

Assign selected permissions to [redacted]

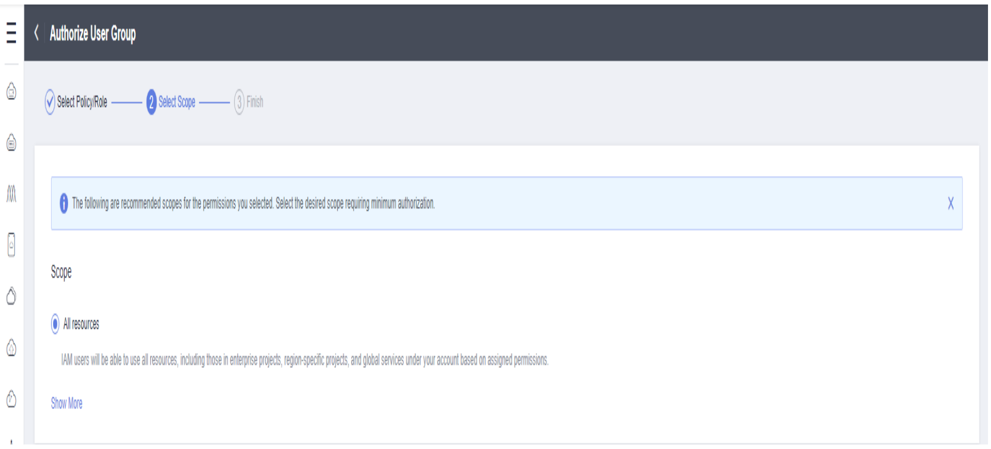
All policies/roles ▾ | All services ▾ | Fuzzy search ▾ | Security Administrator

□	Policy/Role Name	Type
□	[redacted]	[redacted]
□	DBSS Security Administrator DBSS Security Administrator has the authority to set the security policy of DBSS	System-defined role
□	Security Administrator Full permissions for Identity and Access Management. This role does not have permissions for switching roles.	System-defined role

Step 4 Select a region.

Retain the default **All resources** and click **OK**, as shown in **Figure 1-47**.

Figure 1-47 Authorization



Authorize User Group

The following are recommended scopes for the permissions you selected. Select the desired scope requiring minimum authorization.

Scope

● All resources

IAM users will be able to use all resources, including those in enterprise projects, region-specific projects, and global services under your account based on assigned permissions.

----End

1.7.5 How Do I Do If a User Cannot Be Bound to a Client Using the Dynamic Verification Code of the Previously Bound MFA Device?

Scenario

Enable multi-factor authentication (MFA), bind a user to a virtual MFA device, and unbind the virtual MFA device from the user. The user cannot be bound to a client using the dynamic verification code of the previously bound MFA device.

Procedure

Step 1 After the administrator unbinds a virtual MFA device, if the user does not receive an email or SMS message telling the user how to rebind the virtual MFA device, perform the following operations:

Step 2 The operations are as follows:

1. Unbind a user from a virtual MFA device.
2. Rebind the virtual MFA device and use the rebound dynamic verification code to log in from the client.

----End

1.8 Policies

1.8.1 What If a Message Is Displayed Indicating Duplicate Policy Names During Policy Import?

Scenarios

If the policy name in the file to be imported is the same as an existing policy name in the destination region, the system displays a message indicating that the policy name already exists and you need to change the policy name when importing the file.

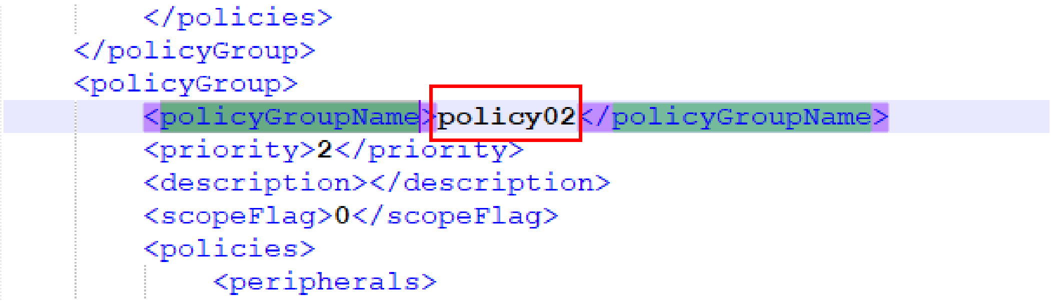
Procedure

Step 1 Use a text editor to open the ***xxx*.xml** file to be imported.

Step 2 Search for **policyGroupName** in the ***xxx*.xml** file and find the duplicate policy name.

Step 3 Change the policy name in **<policyGroupName>*Policy Name*</policyGroupName>**, as shown in **Figure 1-48**.

Figure 1-48 Changing the policy name



```
        </policies>
    </policyGroup>
    <policyGroup>
        <policyGroupName>policy02</policyGroupName>
        <priority>2</priority>
        <description></description>
        <scopeFlag>0</scopeFlag>
        <policies>
            <peripherals>
```

Step 4 Save and close the file.

Step 5 Import the ***xxx*.xml** file again on the console by referring to **Importing a Policy**.

----End

1.8.2 How Do I Disable the Remote Login Port of a Desktop Security Group?

NOTE

- A configured protocol policy cannot take effect when users log in to a desktop remotely. To use the security function of the policy, you are advised to disable the remote login port of the desktop security group.
- This section applies only to Windows cloud desktops.

Step 1 Log in to the console.

Step 2 In the navigation pane, choose **Tenant Configuration** > **Basic Settings**.

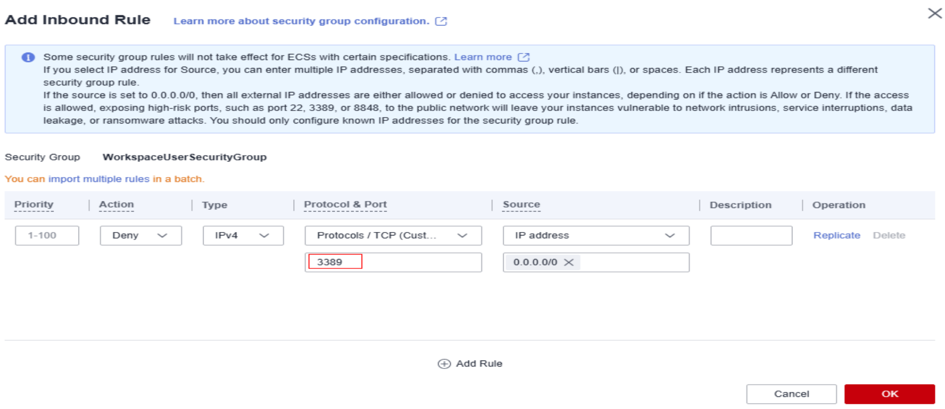
Step 3 In the **Network Configuration** area, click the security group name on the right of **Desktop Security Group** to go to the basic information page of the security group.

Step 4 Click the **Inbound Rules** tab.

Step 5 Click **Add Rule** to go to the **Add Inbound Rule** page.

Step 6 Add a rule to deny access to the remote login port 3389 of the desktop security group, as shown in **Figure 1-49**.

Figure 1-49 Adding a port



Add Inbound Rule Learn more about security group configuration.

Some security group rules will not take effect for ECSs with certain specifications. Learn more
If you select IP address for Source, you can enter multiple IP addresses, separated with commas (,), vertical bars (|), or spaces. Each IP address represents a different security group rule.
If the source is set to 0.0.0.0/0, then all external IP addresses are either allowed or denied to access your instances, depending on if the action is Allow or Deny. If the access is allowed, exposing high-risk ports, such as port 22, 3389, or 8848, to the public network will leave your instances vulnerable to network intrusions, service interruptions, data leakage, or ransomware attacks. You should only configure known IP addresses for the security group rule.

Security Group WorkspaceUserSecurityGroup

You can import multiple rules in a batch.

Priority	Action	Type	Protocol & Port	Source	Description	Operation
1-100	Deny	IPv4	Protocols / TCP (Cust... 3389	IP address 0.0.0.0/0		Replicate Delete

Step 7 Click **OK**.

----End

1.9 End Users and Login

1.9.1 What If Desktop Login by an End User Fails?

Scenarios

If an end user contacts you to resolve the issue of desktop login failure, perform the following procedure.

Procedure

Step 1 Check whether the desktop is running properly.

1. Go to the **Huawei Cloud website**. Log in to the console as an administrator.
2. Click 📍 in the upper left corner of the console and select a region and a project.
3. Click ☰ and choose **Business Applications** > **Workspace** in the service list. On the Workspace console, choose **Desktops**.
4. Check the running status of the desktop and ensure that the status is **Running**.

Step 2 Choose **More** > **Remote Login** of the target desktop and check whether you can remotely log in to the desktop on the console.

- If the login is successful, go to **Step 3**.
- If the login fails, record the resource information and problem occurrence time, and **submit a service ticket** for technical support.

Step 3 Check whether the network is normal.

- If the network is normal, record the resource information and problem occurrence time, and **submit a service ticket** for technical support.
- If the network is abnormal, rectify the network fault and try logging in to the desktop again. If the login still fails, **submit a service ticket** for technical support.

----End

1.10 Backup and Restoration

1.10.1 How Do I Back Up and Restore Desktop Data?

You can use Cloud Backup and Recovery (CBR) to back up and restore cloud desktop data.

For details about the backup, see **Backing Up Desktop Data**. For details about the restoration, see **Restoring Desktop Data**. For details about common backup and restoration issues, see **Backup** and **Restoration**.

1.11 System Configuration and O&M

1.11.1 How Do I Enable or Disable the Emergency Mode for a Desktop?

Scenarios

To enable or disable the emergency mode for a desktop, you need to configure a whitelist. **Submit a service ticket** for technical support.

Enabling the emergency mode

After a whitelist is configured, if the cloud desktop server disconnects from the AD server or the connection request times out, and other auxiliary authentication modes are disabled, the emergency mode will be automatically enabled. Some cloud desktop functions will be disabled, as shown in **Table 1-5**.

Table 1-5 Constraints

Role	Disabled Function
Desktop user	Changing the password
	Reporting issues
	Reporting logs
	Desktop menu – Hibernation
	Desktop menu – Shutdown
	Desktop menu – Force shutdown
	Desktop menu – Restart
	Desktop menu – Force restart
	Desktop menu – Self-maintenance
Tenant administrator	Buying a desktop
	Rebuilding system disks
	Rejoining a desktop to a domain
	Creating an AD user
	Assigning desktops
	Creating an AD user group
	Managing OUs
	Modifying domain configurations

Disabling the emergency mode

When the network between the desktop and the AD server recovers, the emergency mode is automatically disabled. Then the functions listed in **Table 1-5** will become available.

1.11.2 How Do I Enable IPv6 on Workspace?

Scenarios

Enable IPv6 on Workspace.

Prerequisites

A VPC has been created.

Procedure

Step 1 Log in to the console.

Step 2 Click ☰. Choose **Networking** > **Virtual Private Cloud**. The VPC console is displayed.

Step 3 In the navigation pane, choose **Virtual Private Cloud** > **Subnets**.

Enabling IPv6 on an existing subnet

Step 4 Click a subnet name. The basic information page of the subnet is displayed.

Step 5 Click **Enable** on the right of **IPv6 CIDR Block**. In the page displayed, click **OK**.

NOTE

After IPv6 is enabled on a subnet, desktops in the subnet do not support IPv6. To enable IPv6 on these desktops, choose **Desktops** > **Desktops** in the navigation pane. In the **Operation** column of the desired desktop, click **More** > **Network Settings** > **Desktop Network Settings**, and select a subnet with IPv6 enabled. For details, see **Desktop Network Settings**.

Creating a subnet

Step 6 On the **Subnets** page, click **Create Subnet**. For details, see **Creating a Subnet for an Existing VPC**.

NOTE

- Select **Enable** for **IPv6 CIDR Block**. An IPv6 CIDR block will be automatically assigned to the subnet. Currently, the IPv6 CIDR block cannot be customized. This function cannot be disabled once it is enabled.
- Desktops in a subnet with IPv6 enabled will support IPv6.

----End

1.11.3 How Do I Enable RDP on a Windows Cloud Desktop?

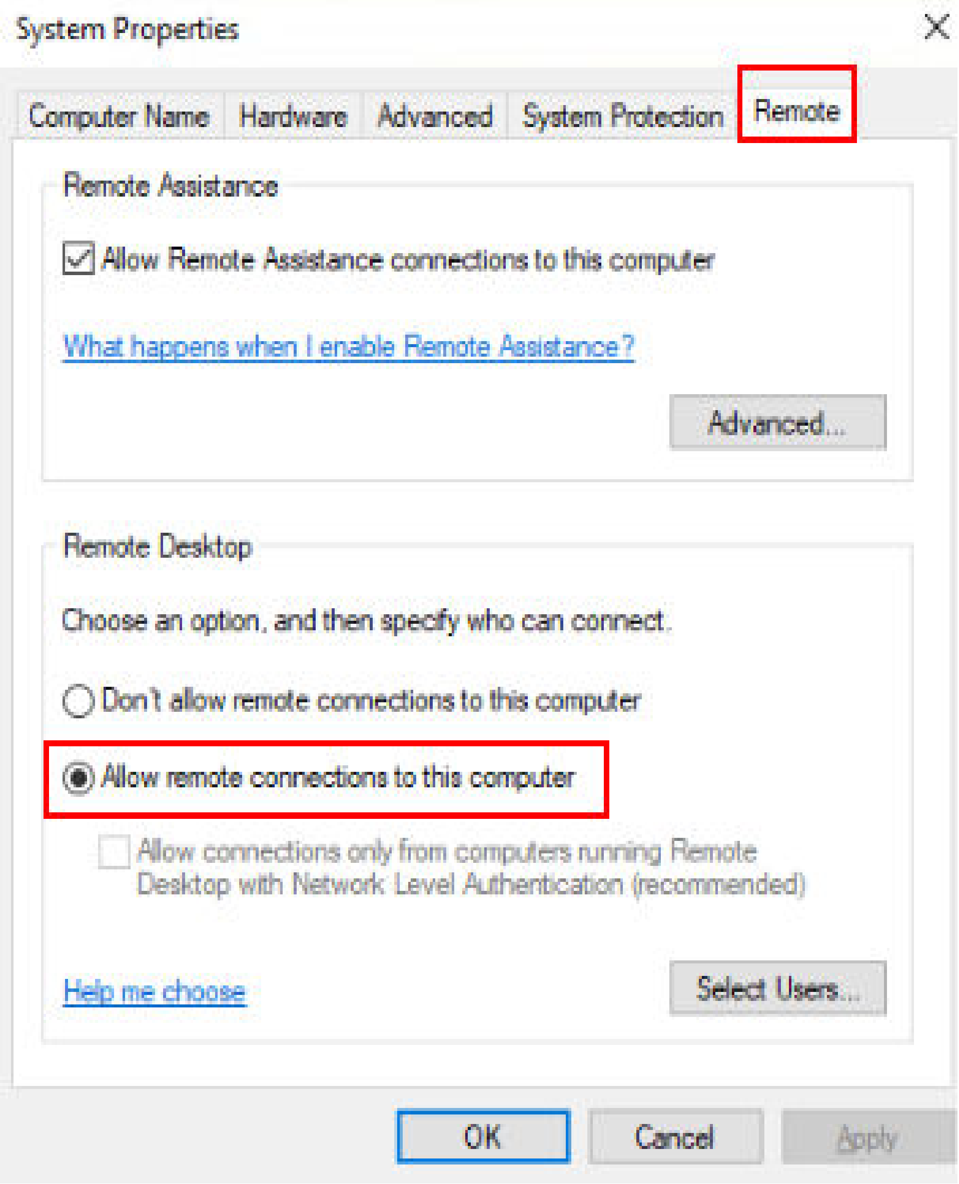
Enabling remote connections to a desktop

Step 1 Log in to a cloud desktop using the client.

Step 2 On the desktop, press **Win** + **R** and enter **sysdm.cpl**. The **System Properties** window is displayed.

Step 3 In the **System Properties** window, choose the **Remote** tab and select **Allow remote connections to this computer**, as shown in **Figure 1-50**.

Figure 1-50 System properties



System Properties

Remote Assistance

☑ Allow Remote Assistance connections to this computer

What happens when I enable Remote Assistance?

Remote Desktop

Choose an option, and then specify who can connect.

○ Don't allow remote connections to this computer

● Allow remote connections to this computer

□ Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)

Help me choose

Step 4 Click **OK**.

Enabling Internet access for the desktop

Step 5 Enable Internet access for the desktop by referring to **Enabling Economical Internet Access (EIP)**.

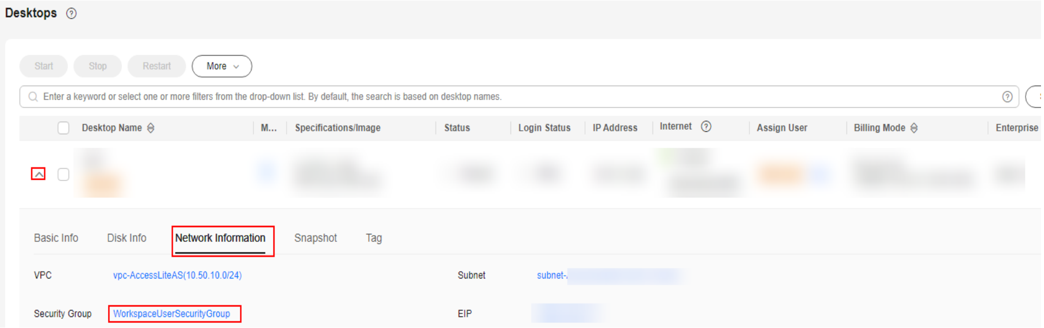
Binding port 3389 to the desktop

Step 6 **Log in to the console**.

Step 7 In the navigation pane, choose **Desktops** > **Desktops**.

Step 8 In the desktop list, click ^ on the left of the desired desktop. Choose **Network Information** and click the security group name, as shown in **Figure 1-51**.

Figure 1-51 Security groups



Enter a keyword or select one or more filters from the drop-down list. By default, the search is based on desktop names.

VPC vpc-AccessLiteAS(10.50.10.0/24)

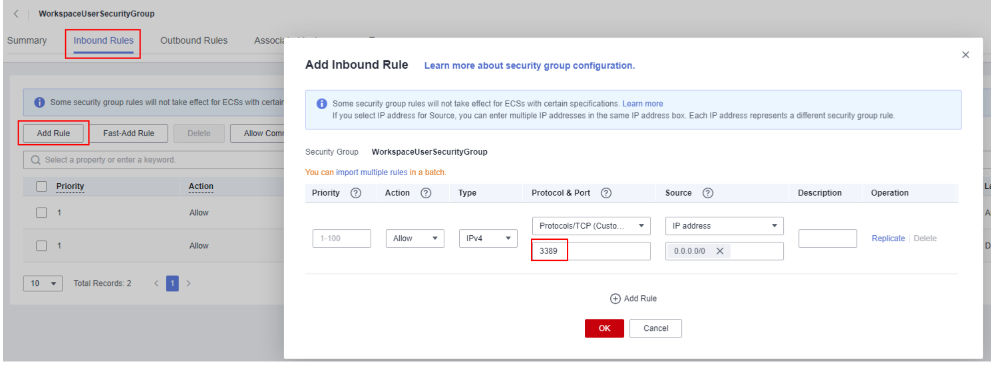
Subnet subnet-

Security Group WorkspaceUserSecurityGroup

EIP

Step 9 In the inbound rule configuration area, enter **3389** in the **Protocol & Port** column, as shown in **Figure 1-52**.

Figure 1-52 Adding port 3389



Some security group rules will not take effect for ECSs with certain specifications. Learn more

If you select IP address for Source, you can enter multiple IP addresses in the same IP address box. Each IP address represents a different security group rule.

Security Group WorkspaceUserSecurityGroup

You can import multiple rules in a batch.

Priority: 1-100; Action: Allow; Type: IPv4; Protocol & Port: Protocols/TCP (Custo... 3389; Source: IP address 0.0.0.0/0

----End

1.11.4 How Do I Collect Workspace Logs?

Scenarios

This section describes how to collect logs of the Workspace client and server (HDA).

Procedure

Obtaining client logs

Method 1:

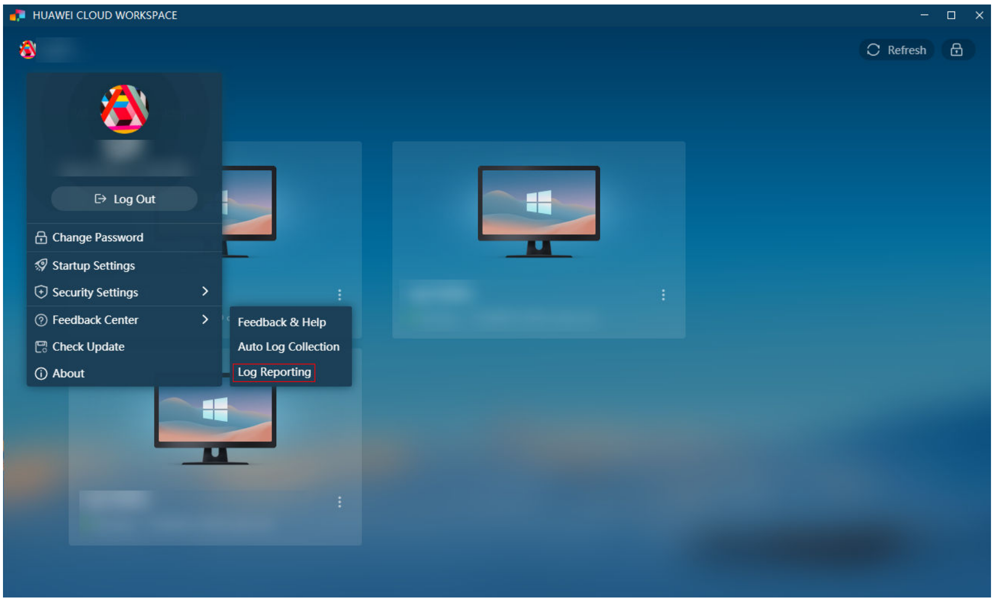
View logs in the following directories:

- Windows: **C:\HdpLog\Workspace**
- UOS: **/opt/apps/com.huawei.HuaweiCloudWorkspace/files/WorkspaceLog**
- Ubuntu: **/var/log/WorkspaceLog/**
- macOS: **~/Library/Logs/Workspace**
- Android: **/sdcard/Hdplog/hdplog/Workspace***

Method 2:

Step 1 Log in to the WI as an administrator, enter the username and password, and click the username in the upper left corner of the client page. Choose **Feedback Center** > **Log Reporting**, as shown in **Figure 1-53**.

Figure 1-53 Log reporting



Step 2 After the logs are reported, technical support personnel can view the logs.

----End

Server (HDA) logs

Step 1 Log in to a cloud desktop using any of the following methods:

- See **Logging In to a Desktop Using an SC**.
- **Log in to the console**, choose **More** > **Remote Login** in the **Operation** column of the desktop whose logs are to be collected, and enter the password to log in to the desktop.
- Log in to the WI as an administrator, enter the username and password, and select the desktop whose logs are to be collected in the desktop list. Click ⋮ in the lower right corner and select **Self-maintenance** to go to the desktop.

Windows cloud desktops

Step 2 Click 🔍 in the lower left corner of the desktop and enter **vdesk** to open Huawei vDesk.

Step 3 On the Huawei vDesk page, choose **Tools** > **Log Collection**. In the **Warning** dialog box, check the **Continue to collect logs** box and click **Yes**.

Step 4 The log is stored in the document directory of the current user and named **HDPLog-*Computer name*.zip**.

----End

1.11.5 How Do I Configure the DNS Address Under Tenant Configuration Within the VPC Subnet?

Scenarios

- Use a shared VPC when creating an account in the AD scenario.
- In the AD scenario, when switching to a shared VPC, you need to configure the DNS address under the tenant configuration within the VPC subnet.

  NOTE

  This configuration is required only in the AD scenario.

Prerequisites

You have obtained the primary or backup DNS IP address in the tenant configuration.

Procedure

Step 1 Log in to the console.

Step 2 Click 📍 in the upper left corner of the console and select a region and a project.

Step 3 Click ☰ and choose **Networking** > **Virtual Private Cloud** under **All Services**. The **Network Console** page is displayed.

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

Step 5 Locate the shared subnet and click the subnet name to go to the basic information page of the subnet.

Step 6 Click ✎ next to the DNS server address to go to the page for modifying a DNS server address.

Step 7 Replace the DNS server address with the DNS address under the tenant configuration, and click **OK**.

----End

1.12 Peripherals

1.12.1 How Do I Connect the Desktop to a Local Printer?

To use the local printer, the administrator needs to configure the **USB Port Redirection** or **Printer Redirection** policy for the desktop. You can select either of them.

Configuring the USB Port Redirection Policy

If the administrator configures the **USB Port Redirection** policy for the desktop, users can use the connected printer to print files using the desktop. However, the connected printer cannot be used for printing using the terminal device.

Step 1 Log in to the console as an administrator.

Step 2 Click 📍 in the upper left corner of the console and select a region and a project.

Step 3 Click ☰ and choose **Business Applications** > **Workspace** in the service list.

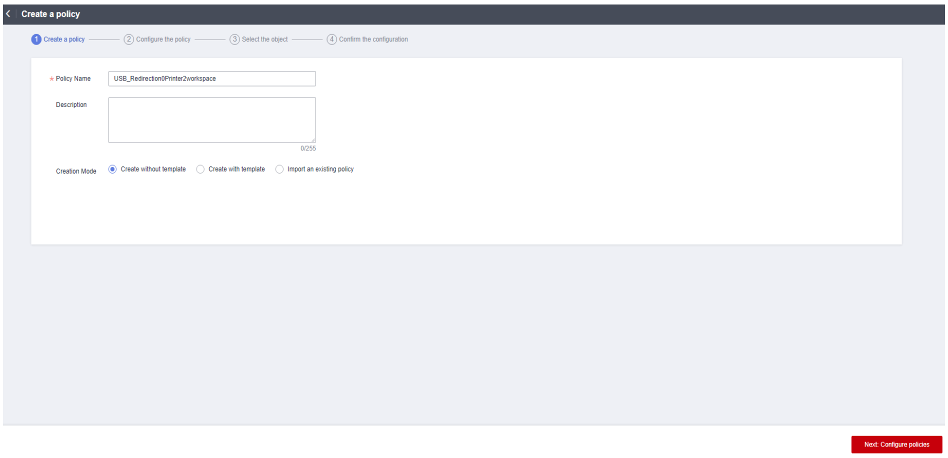
Step 4 Click **Policies**.

The **Policies** page is displayed.

Step 5 Click **Create Policy**.

The page for creating a policy is displayed.

Figure 1-54 Creating a policy



* Policy Name: USB_Redirection0Printer2workspace

Description: 0/255

Creation Mode: ● Create without template ○ Create with template ○ Import an existing policy

Step 6 Set the policy name and enter the description.

NOTE

- The policy name can contain up to 55 characters in digits, letters, and underscores (_), for example, **USB_Redirection0Printer2workspace**.
- The description can contain up to 255 characters, for example, **Use a local printer with the USB port redirection policy**.

Step 7 **Creation Mode**: Select **Create without template**.

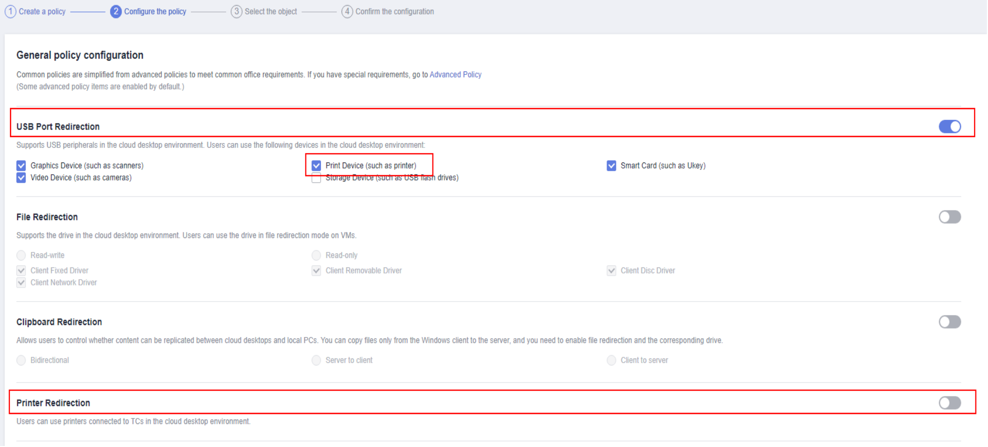
Step 8 Click **Next: Configure policies**.

The page for general policy configuration is displayed.

Step 9 Set **USB Port Redirection** to ● and select **Print Device (such as printer)**, as shown in **Figure 1-55**.

Step 10 Set **Printer Redirection** to ○, as shown in **Figure 1-55**.

Figure 1-55 Configuring policy parameters



General policy configuration

Common policies are simplified from advanced policies to meet common office requirements. If you have special requirements, go to Advanced Policy
(Some advanced policy items are enabled by default.)

USB Port Redirection

Supports USB peripherals in the cloud desktop environment. Users can use the following devices in the cloud desktop environment:

☑ Graphics Device (such as scanners)
☑ Video Device (such as cameras)
☑ Print Device (such as printer)
□ Storage Device (such as USB flash drives)
☑ Smart Card (such as Ukey)

File Redirection

Supports the drive in the cloud desktop environment. Users can use the drive in file redirection mode on VMs.

○ Read-write
○ Read-only
☑ Client Fixed Driver
☑ Client Network Driver
☑ Client Removable Driver
☑ Client Disc Driver

Clipboard Redirection

Allows users to control whether content can be replicated between cloud desktops and local PCs. You can copy files only from the Windows client to the server, and you need to enable file redirection and the corresponding drive.

○ Bidirectional
○ Server to client
○ Client to server

Printer Redirection

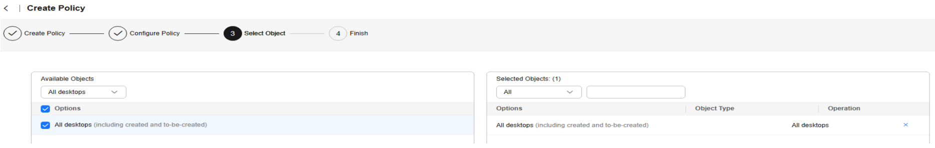
Users can use printers connected to TCs in the cloud desktop environment.

Step 11 Click **Next: Select Object**.

Step 12 Select an object as required.

For example, if you select **All desktops**, the policy applies to all desktops in the current project.

Figure 1-56 Selecting an object



Available Objects

All desktops

☑ Options

☑ All desktops (including created and to-be-created)

Selected Objects: (1)

All

Options	Object Type	Operation
All desktops (including created and to-be-created)	All desktops	×

Step 13 Click **Next: Finish**.

Step 14 The policy has been created. Users can use the printer after logging in to the desktop again.

NOTE

For details about how to set up a printer on the client, see **What If I Can't Use Local Printers on Cloud Desktops?**.

----End

Configuring the Printer Redirection Policy

If the administrator configures the **Printer Redirection** policy for the desktop, users can use the connected printer to print files using both the desktop and the terminal device.

Step 1 Log in to the console as an administrator.

Step 2 Click 📍 in the upper left corner of the console and select a region and a project.

Step 3 Click ☰ and choose **Business Applications** > **Workspace** in the service list.

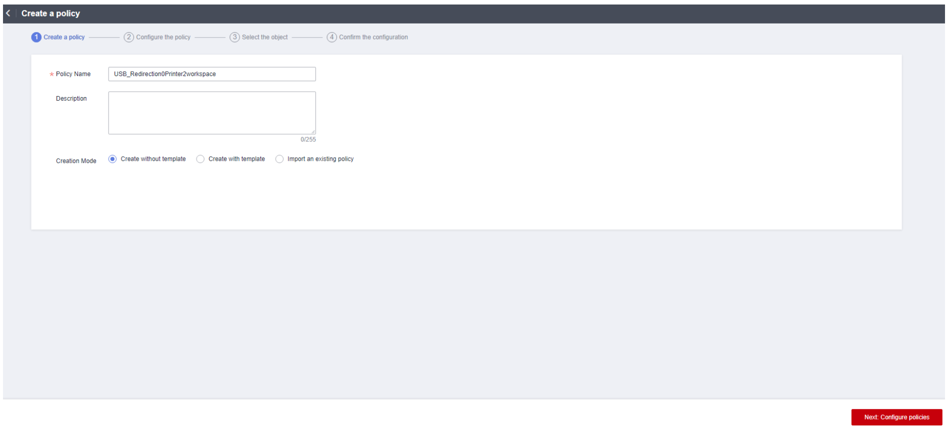
Step 4 Click **Policies**.

The **Policies** page is displayed.

Step 5 Click **Create Policy**.

The page for creating a policy is displayed.

Figure 1-57 Creating a policy



Create a policy

1 Create a policy — 2 Configure the policy — 3 Select the object — 4 Confirm the configuration

* Policy Name: USB_Redirection0Printer2workspace

Description: 0/255

Creation Mode: ● Create without template ○ Create with template ○ Import an existing policy

Next: Configure policies

Step 6 Set the policy name and enter the description.

NOTE

- The policy name can contain up to 55 characters in digits, letters, and underscores (_), for example, **Printer_Device_Redirection0Printer2workspace**.
- The description can contain up to 255 characters, for example, **Use a local printer with the printer redirection policy.**

Step 7 **Creation Mode**: Select **Create without template**.

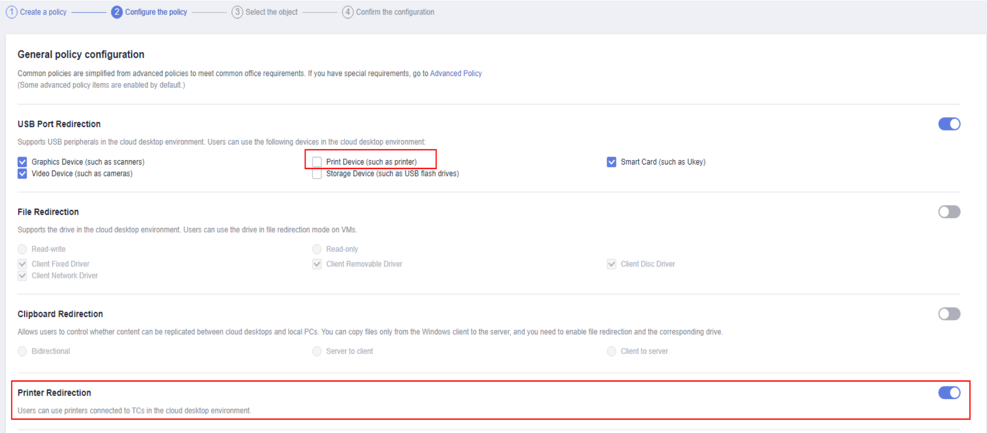
Step 8 Click **Next: Configure policies**.

The page for general policy configuration is displayed.

Step 9 Deselect **Print Device (such as printer)** under **USB Port Redirection**, as shown in **Figure 1-58**.

Step 10 Set **Printer Redirection** to ●, as shown in **Figure 1-58**.

Figure 1-58 Configuring policy parameters



1 Create a policy — 2 Configure the policy — 3 Select the object — 4 Confirm the configuration

General policy configuration

Common policies are simplified from advanced policies to meet common office requirements. If you have special requirements, go to Advanced Policy
(Some advanced policy items are enabled by default.)

USB Port Redirection ●

Supports USB peripherals in the cloud desktop environment. Users can use the following devices in the cloud desktop environment:

☑ Graphics Device (such as scanners)
☑ Video Device (such as cameras)
□ Print Device (such as printer)
□ Storage Device (such as USB flash drives)
☑ Smart Card (such as Ukey)

File Redirection ○

Supports the drive in the cloud desktop environment. Users can use the drive in file redirection mode on VMs.

○ Read-write
○ Read-only
☑ Client Fixed Driver
☑ Client Network Driver
☑ Client Removable Driver
☑ Client Disc Driver

Clipboard Redirection ○

Allows users to control whether content can be replicated between cloud desktops and local PCs. You can copy files only from the Windows client to the server, and you need to enable file redirection and the corresponding drive.

○ Bidirectional ○ Server to client ○ Client to server

Printer Redirection ●

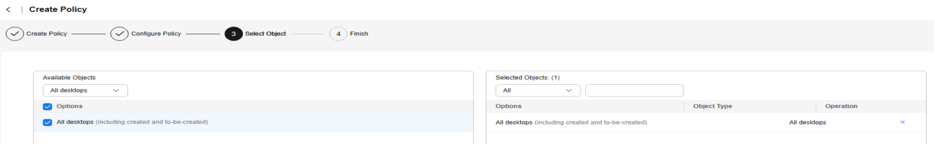
Users can use printers connected to TCs in the cloud desktop environment.

Step 11 Click **Next: Select Object**.

Step 12 Select an object as required.

For example, if you select **All desktops**, the policy applies to all desktops in the current project.

Figure 1-59 Selecting an object



Available Objects: All desktops

☑ Options

☑ All desktops (including created and to-be-created)

Selected Objects: (1) All

Options	Object Type	Operation
All desktops (including created and to-be-created)	All desktops	×

Step 13 Click **Next: Finish**.

Step 14 The policy has been created. Users can use the printer after logging in to the desktop again.

NOTE

For details about how to set up a printer on the client, see **What If I Can't Use Local Printers on Cloud Desktops?**.

----End

1.12.2 How Do I Connect the Desktop to a Network Printer?

Prerequisites

The device that accesses the desktop can communicate with the target printer.

Procedure

The administrator has configured the **Printer Redirection** policy for the user. After logging in to the desktop, the user can use the network printer to print files.

Step 1 Log in to the console as an administrator.

Step 2 Click in the upper left corner of the console and select a region and a project.

Step 3 Click and choose **Business Applications** > **Workspace** in the service list.

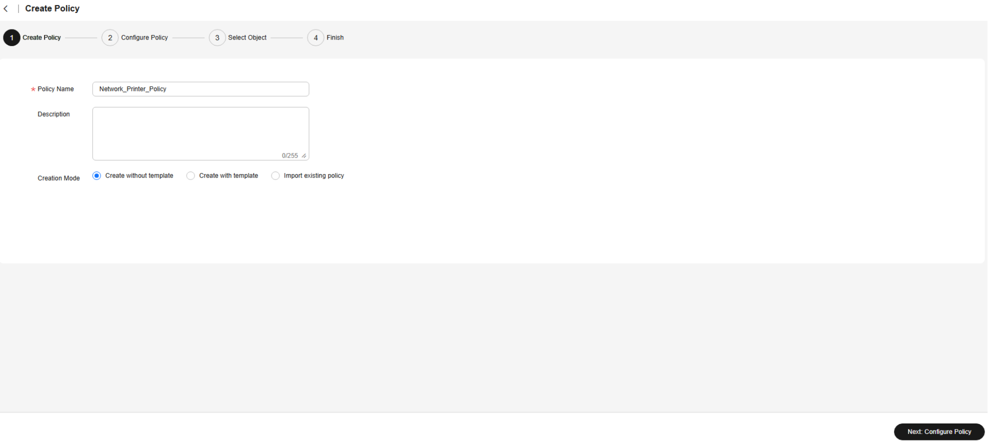
Step 4 Click **Policies**.

The **Policies** page is displayed.

Step 5 Click **Create Policy**.

The page for creating a policy is displayed.

Figure 1-60 Creating a policy



< | **Create Policy**

1 Create Policy —— 2 Configure Policy —— 3 Select Object —— 4 Finish

* Policy Name: Network_Printer_Policy

Description: 0/255

Creation Mode: ● Create without template ○ Create with template ○ Import existing policy

Step 6 Set the policy name and enter the description.

NOTE

- The policy name can contain up to 55 characters in digits, letters, and underscores (_), for example, **Network_Printer_Policy**.
- The description can contain up to 255 characters, for example, **Use a network printer with the printer redirection policy**.

Step 7 **Creation Mode**: Select **Create without template**.

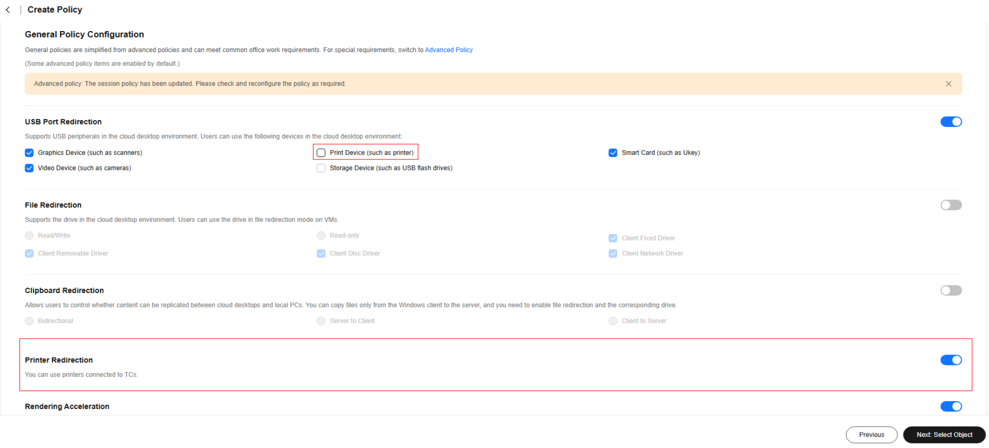
Step 8 Click **Next: Configure policies**.

The page for general policy configuration is displayed.

Step 9 Deselect **Print Device (such as printer)** under **USB Port Redirection**, as shown in **Figure 1-61**.

Step 10 Set **Printer Redirection** to ●, as shown in **Figure 1-61**.

Figure 1-61 Configuring policy parameters



< | **Create Policy**

General Policy Configuration

General policies are simplified from advanced policies and can meet common office work requirements. For special requirements, switch to Advanced Policy

(Some advanced policy items are enabled by default.)

Advanced policy: The session policy has been updated. Please check and reconfigure the policy as required. ×

USB Port Redirection ●

Supports USB peripherals in the cloud desktop environment. Users can use the following devices in the cloud desktop environment:

☑ Graphics Device (such as scanners) □ Print Device (such as printer) ☑ Smart Card (such as Ukey)
☑ Video Device (such as cameras) □ Storage Device (such as USB flash drives)

File Redirection ○

Supports the drive in the cloud desktop environment. Users can use the drive in file redirection mode on VMs.

○ Read/Write ○ Read-only ☑ Client Fixed Driver
☑ Client Removable Driver ☑ Client Disc Driver ☑ Client Network Driver

Clipboard Redirection ○

Allows users to control whether content can be replicated between cloud desktops and local PCs. You can copy files only from the Windows client to the server, and you need to enable file redirection and the corresponding drive.

○ Bidirectional ○ Server to Client ○ Client to Server

Printer Redirection ●

You can use printers connected to TCs.

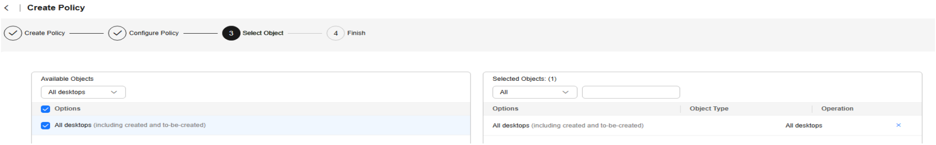
Rendering Acceleration ●

Step 11 Click **Next: Select Object**.

Step 12 Select an object as required.

For example, if you select **All desktops**, the policy applies to all desktops in the current project.

Figure 1-62 Selecting an object



< | **Create Policy**

✓ Create Policy — ✓ Configure Policy — 3 Select Object — 4 Finish

Available Objects

All desktops

☑ Options

☑ All desktops (including created and to-be-created)

Selected Objects: (1)

All

Options	Object Type	Operation
All desktops (including created and to-be-created)	All desktops	×

Step 13 Click **Next: Finish**.

Step 14 The policy has been created. Users can use the network printer after logging in to the desktop again.

NOTE

For details about how to set up the network printer, see **What If I Can't Use Network Printers on Cloud Desktops?**.

----End

1.13 Images

1.13.1 Can I Use Private Images to Purchase Desktops?

Workspace allows administrators to purchase desktops using Windows private images created in either of the following ways:

- You can use the one-click image conversion function to convert a desktop purchased using a Windows image into a private image. For details about the operations and constraints, see **Converting a Desktop to an Image**.
- You can register an official ISO image file obtained from an official channel as a private image in IMS on Huawei Cloud. Then you can create and configure an ECS, and convert the ECS into a private desktop image. For details about the operations and constraints, see **Creating a Windows Private Image**.

1.13.2 How Many Private Images Can Be Created for Workspace?

You can create a maximum of 500 private images for Workspace on IMS, but these images have configuration constraints.

1.13.3 What If a Blue Screen or Black Screen Occurs on a Desktop Provisioned Using an Image?

If the system patch is installed during image creation, the blue screen or black screen may occur on the provisioned desktop. To avoid this, uninstall the current system patch or update the system patch to the latest version when creating the system image.

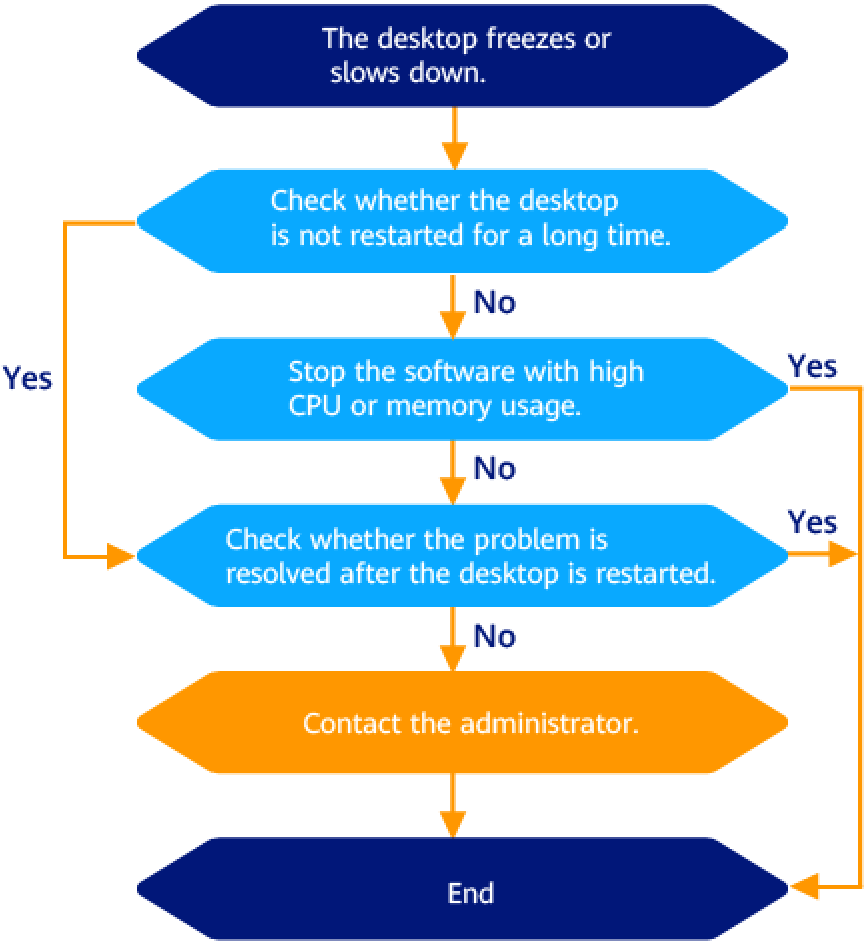
2 FAQs for End Users

2.1 Desktop Usage Issues

2.1.1 How Do I Do If the Desktop Freezes?

If a fault such as desktop freezing or slow response occurs, rectify the fault by performing operations provided in this section.

Figure 2-1 Troubleshooting process


The desktop freezes or slows down.
Check whether the desktop is not restarted for a long time.
Yes
No
Stop the software with high CPU or memory usage.
Yes
No
Check whether the problem is resolved after the desktop is restarted.
Yes
No
Contact the administrator.
End

2.1.2 How Do I Do If the Disk Space Is Insufficient?

Workspace allows you to add disks and expand disk capacity. You can contact the administrator to expand disk capacity.

2.1.3 How Do I Enter the CLI Mode?

In addition to the graphical user interface (GUI), the CLI mode is another man-machine interaction mode provided by the OS. You can use the CLI mode to quickly, automatically, and intelligently manage the system and process services in batches.

You can enter the CLI mode by performing the following operations.

Windows

- Right-click ⊞ on the taskbar, choose **Run**, enter **cmd**, and click **OK** to enter the CLI mode.

2.1.4 What If My Desktop Cannot Connect to the Internet?

Step 1 Disable the proxy.

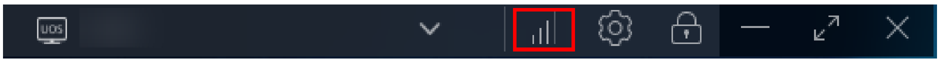
Windows desktops:

1. Log in to the desktop.
2. Click ⊞ in the lower left corner of the desktop and choose ⚙. The Windows settings page is displayed.
3. Click **Network & internet**. The network status page is displayed.
4. In the navigation pane, click **Proxy**. The proxy configuration page is displayed.
5. Disable the proxy.
   - If the connection to the Internet is successful, no further action is required.
   - If the connection to the Internet fails, go to **Step 2**.

Step 2 Check the network status.

1. Move the cursor to the upper edge of the desktop. A floating window is displayed, as shown in **Figure 2-2**.

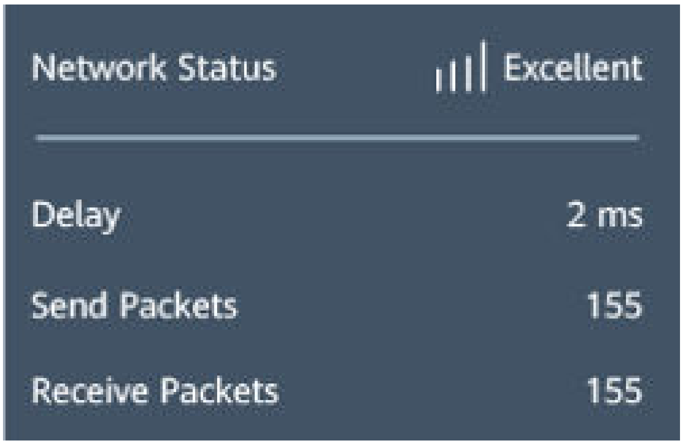
Figure 2-2 Floating window



2. Click 📶 in the floating window.

   The **Network Status** dialog box is displayed.
3. Check the latency, as shown in **Figure 2-3**.

Figure 2-3 Network status



Network Status Excellent

Delay 2 ms

Send Packets 155

Receive Packets 155

The latency is described as follows:

- 1 to 30 ms, indicating that the network speed is extremely high and there is almost no delay.
- 30 to 50 ms, indicating that the network speed is good and there is no obvious delay.

   - 50 to 100 ms, indicating that the network speed is normal and there is a slight delay.
   - 100 to 200 ms, indicating that the network speed is low and disconnection occurs occasionally.
   - If the value is greater than 200 ms, the network speed is extremely low, and the network is frequently disconnected or cannot be accessed.

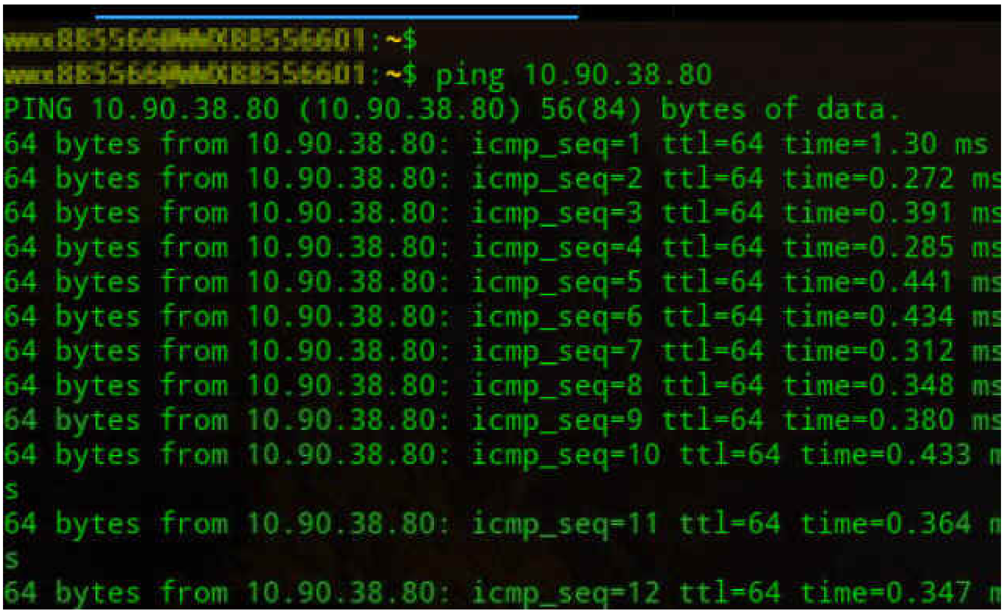
4. In any blank area on the desktop, enter the CLI mode.
5. Run the following command to check the network status:

   ping + ***Address for the desktop to access the Internet***

   NOTE

   Obtain the address for the desktop to access the Internet from the desktop enabling notification email sent by the system.

   Information similar to the following is displayed:



```
[redacted]:~$
[redacted]:~$ ping 10.90.38.80
PING 10.90.38.80 (10.90.38.80) 56(84) bytes of data.
64 bytes from 10.90.38.80: icmp_seq=1 ttl=64 time=1.30 ms
64 bytes from 10.90.38.80: icmp_seq=2 ttl=64 time=0.272 ms
64 bytes from 10.90.38.80: icmp_seq=3 ttl=64 time=0.391 ms
64 bytes from 10.90.38.80: icmp_seq=4 ttl=64 time=0.285 ms
64 bytes from 10.90.38.80: icmp_seq=5 ttl=64 time=0.441 ms
64 bytes from 10.90.38.80: icmp_seq=6 ttl=64 time=0.434 ms
64 bytes from 10.90.38.80: icmp_seq=7 ttl=64 time=0.312 ms
64 bytes from 10.90.38.80: icmp_seq=8 ttl=64 time=0.348 ms
64 bytes from 10.90.38.80: icmp_seq=9 ttl=64 time=0.380 ms
64 bytes from 10.90.38.80: icmp_seq=10 ttl=64 time=0.433 m
s
64 bytes from 10.90.38.80: icmp_seq=11 ttl=64 time=0.364 m
s
64 bytes from 10.90.38.80: icmp_seq=12 ttl=64 time=0.347 m
```

Step 3 Determine the network segment where the network connection is abnormal based on the results in **Step 2.3** and **Step 2.5**, record the exception, and contact the administrator.

- If the network latency in **Step 2.3** and **Step 2.5** is too high, the public network is abnormal.
- If the network latency in **Step 2.3** is too high but the network latency in **Step 2.5** is low, the internal network of the desktop is abnormal.

----End

2.1.5 Do Cloud Desktops Support Personalized Settings?

For Windows desktops, you can click ⊞ and choose **Settings** > **Personalization** to set the parameters.

2.1.6 How Do I Take a Screenshot?

Windows

You can use the following shortcut keys to take a screenshot.

Table 2-1 Shortcut keys for taking a screenshot

Shortcut Key	Description
Alt + **PrintScreen**	Screenshot of the window where the cursor is located.
Ctrl + **PrintScreen**	Screenshot with a delay of 5 seconds.
PrintScreen	Full-screen screenshot.

2.1.7 What If I Can't Use Local Printers on Cloud Desktops?

Step 1 Contact the administrator to check whether the **USB Port Redirection** or **Printer Redirection** policy has been configured for the user desktop by referring to **How Do I Connect the Desktop to a Local Printer?**.

- If a policy has been configured, go to **Step 2**.
- If no policy is configured, the administrator needs to configure the **USB Port Redirection** or **Printer Redirection** policy for the user desktop by referring to **How Do I Connect the Desktop to a Local Printer?**, and then go to **Step 2**.

Step 2 Log in to the desktop again.

1. Click ⌄ on the top of the desktop to expand the floating toolbar, click ✕, and close the desktop window.
2. Enter the password again on the client and access the corresponding desktop.

Step 3 Check whether the local printer is visible.

Windows desktops:

1. Click ⊞ in the lower left corner of the desktop and choose ⚙. The Windows settings page is displayed.
2. Click **Devices**.
3. In the navigation pane on the left, click **Printers & scanners**.
4. In the **Printers & scanners** list, check whether a local printer (displayed as the local printer name *xxx* or *xxx* (from HDP redirection)) exists.
   - If yes, go to **Step 5**.
   - If no, go to **Step 4**.

Step 4 Add a printer.

Windows desktops:

1. On the printer and scanner list page, click **Add device**.
2. Click **The printer that I want isn't listed. Add manually.** The page for adding a printer is displayed.
3. Select **Add a printer using an IP address or hostname** or **Add a local printer or network printer with manual settings**, and click **Next**.

4. Add the printer as prompted.

   NOTE

   When installing the printer driver, select **Install from disk** and select the driver file of the corresponding printer.

   You can obtain the driver file as follows:

   - If the desktop can access the Internet, you can use a browser to obtain the driver file based on the local printer model.
   - If the desktop cannot access the Internet, find the driver file of the printer on the local terminal, contact the administrator to configure policies for the desktop by referring to **Copying Files from an External Storage Device to the Desktop**, and copy the driver file to the desktop by referring to **What If I Can't Copy Files Between a Desktop and a Local Storage Device?**.

Step 5 Check whether the local printer can be used.

Windows desktops:

1. In the **Printers & scanners** list, click the local printer (displayed as local printer name *xxx* or *xxx*(from HDP redirection)). The local printer management page is displayed.
2. Click **Print test page**.
   - If the information can be printed, the local printer is available. Open the file to be printed and select a local printer to print the file.
   - If the printing fails, contact the administrator to **submit a service ticket** for technical support.

----End

2.1.8 What If I Can't Use Network Printers on Cloud Desktops?

Step 1 Contact the administrator to check whether the **Printer Redirection** policy has been configured for the user desktop by referring to **How Do I Connect the Desktop to a Network Printer?**.

- If a policy has been configured, go to **Step 2**.
- If no policy is configured, contact the administrator to complete the configuration by referring to **How Do I Connect the Desktop to a Network Printer?**, and then go to **Step 2**.

Step 2 Log in to the desktop again.

1. Click ⌄ on the top of the desktop to expand the floating toolbar, click ✕, and close the desktop window.
2. Enter the password again on the client and access the corresponding desktop.

Step 3 Check whether the network printer is visible.

Windows desktops:

1. Click ⊞ in the lower left corner of the desktop and choose ⚙. The Windows settings page is displayed.
2. Click **Devices**.

3. In the navigation pane on the left, click **Printers & scanners**.
4. In the **Printers & scanners** list, check whether the target printer (the target printer model) exists.
   - If yes, go to **Step 5**.
   - If no, go to **Step 4**.

Step 4 Add a printer.

Windows desktops:

1. On the printer and scanner list page, click **Add device**.
2. Click **The printer that I want isn't listed. Add manually.** The page for adding a printer is displayed.
3. Select **Add a local printer or network printer with manual settings** and click **Next**.
4. Add the printer as prompted.

   NOTE

   When installing the printer driver, select **Install from disk** and select the driver file of the corresponding printer.

   You can obtain the driver file as follows:

   - If the desktop can access the Internet, you can use a browser to obtain the driver file based on the target printer model.
   - If the desktop cannot access the Internet, find the driver file of the printer on the local terminal, contact the administrator to configure policies for the desktop by referring to **Copying Files from an External Storage Device to the Desktop**, and copy the driver file to the desktop by referring to **What If I Can't Copy Files Between a Desktop and a Local Storage Device?**.

Step 5 Check whether the target printer is available.

Windows desktops:

1. In the **Printers & scanners** list, click the target printer and choose **Management**. The device management page of the local printer is displayed.
2. Click **Print test page**.
   - If the page can be printed, the network printer is available. Open the file to be printed and select a printer to print the file.
   - If the printing fails, contact the administrator to **submit a service ticket** for technical support.

----End

2.1.9 How Do I Download Software?

Prerequisites

The desktop has connected to the enterprise intranet or Internet.

Windows

- If you can access the enterprise intranet, log in to the desktop, obtain the software from the application center, and install the software.

- If you can access the Internet, log in to the desktop and obtain the application from the official channel.

2.1.10 How Do I Do If Data Disks of a Windows Desktop Cannot Be Found After Recomposing the System Disk?

Scenario

The SAN policy of some Windows OSs is not OnlineAll. As a result, data disks cannot be found after you recompose the system disk. You need to change the disk status from offline to online so that the data disks can be properly displayed on the desktop.

Procedure

Checking the disk status

Step 1 Log in to the desktop whose system disk has been recomposed.

Step 2 Press **Win+R** and enter **cmd** to run **cmd.exe**.

Step 3 Run the following command to access DiskPart:

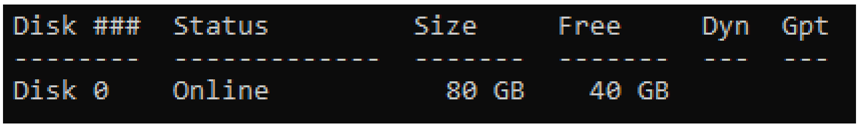
diskpart

Step 4 Run the following command to check the disk status on the desktop:

list disk

Figure 2-4 shows the command output.

Figure 2-4 Disk status



```
Disk ###  Status         Size     Free     Dyn  Gpt
--------  -------------  -------  -------  ---  ---
Disk 0    Online           80 GB    40 GB
```

- If any disk is in the **Offline** status, go to **Step 5**.
- If no disk is in the **Offline** state, run the **exit** command to exit DiskPart and close **cmd.exe**.

Changing the disk status

Step 5 Run the following command to select the disk in the offline status:

select disk *1*

The information about the selected disk is displayed. Disk *1* is now the selected disk.

Change the disk number based on the actual offline disk. For example, if disk 1 is offline in **Figure 2-4**, the actual command is **select disk 1**.

Step 6 Run the following command to change the offline disk status to online:

online disk

A message is displayed, indicating that the modification is successful. DiskPart successfully brings the selected disk online.

Step 7 Run the **exit** command to exit DiskPart and close **cmd.exe**.

----End

2.1.11 What If I Can't Copy Files Between a Desktop and a Local Storage Device?

If the office environment has strict requirements on file transmission, it is normal that files can be transferred only in one direction or cannot be transferred. Contact the administrator to confirm the office environment policy.

If the office environment has no special requirements on file transmission and files cannot be copied between desktops and local storage devices, contact the administrator to check whether the corresponding policy has been enabled for the desktop. For details about the policy, see **How Do I Copy Files Between a Desktop and a Local Storage Device?**. After the administrator enables the policy for the corresponding desktop, files can be copied between the desktop and the local storage device. Operations on desktops vary with the enabled policy. Contact the administrator to confirm the enabled policy and perform operations by referring to **Table 2-2**.

Table 2-2 Policy operation list

Enabled Policy	Data Flow	User Guide
Enable the **Clipboard Redirection** policy and select **Server to client**.	Desktop → Terminal	**NOTE** ● Rich text copy and file copy are supported only when both the client (TC/SC) and desktop run Windows. A maximum of 500 files can be copied at a time. ● If the OS of a client (TC/SC or mobile client) or desktop is not Windows, only text can be copied. 1. Log in to the desktop. 2. Select the content to copy based on the OS types of the terminal and desktop. Example: **You can copy text from desktops to external devices** 3. Click ∨ on the top of the desktop to expand the floating toolbar, and click — to minimize the Workspace client. 4. Open the text editing page and paste the copied content to the terminal. Example: **You can copy text from desktops to external devices**

Enabled Policy	Data Flow	User Guide
Enable the **Clipboard Redirection** policy and select **Client to server**.	Desktop ← Terminal	**NOTE** - Rich text copy and file copy are supported only when both the client (TC/SC) and desktop run Windows. A maximum of 500 files can be copied at a time. - If the OS of a client (TC/SC or mobile client) or desktop is not Windows, only text can be copied. 1. Log in to the desktop. 2. Click ⌄ on the top of the desktop to expand the floating toolbar, and click − to minimize the Workspace client. 3. Select the content to copy based on the OS types of the terminal and desktop. Example: **You can copy text from external devices to desktops** 4. Click the Workspace client. The desktop is displayed. 5. Open the text editing page and paste the copied content to the desktop. Example: **You can copy text from external devices to desktops**
Enable the **Clipboard Redirection** policy and select **Bidirectional**.	Desktop → Terminal	**NOTE** - Rich text copy and file copy are supported only when both the client (TC/SC) and desktop run Windows. A maximum of 500 files can be copied at a time. - If the OS of a client (TC/SC or mobile client) or desktop is not Windows, only text can be copied. 1. Log in to the desktop. 2. Select the content to copy based on the OS types of the terminal and desktop. Example: **You can copy text from desktops to external devices** 3. Click ⌄ on the top of the desktop to expand the floating toolbar, and click − to minimize the Workspace client. 4. Open the text editing page and paste the copied content to the terminal. Example: **You can copy text from desktops to external devices**

Enabled Policy	Data Flow	User Guide
	Desktop ← Terminal	**NOTE** ● Rich text copy and file copy are supported only when both the client (TC/SC) and desktop run Windows. A maximum of 500 files can be copied at a time. ● If the OS of a client (TC/SC or mobile client) or desktop is not Windows, only text can be copied. 1. Log in to the desktop. 2. Click ∨ on the top of the desktop to expand the floating toolbar, and click — to minimize the Workspace client. 3. Select the content to copy based on the OS types of the terminal and desktop. Example: **You can copy text from external devices to desktops** 4. Click the Workspace client. The desktop is displayed. 5. Open the text editing page and paste the copied content to the desktop. Example: **You can copy text from external devices to desktops**
Enable the **Send File In Virtual Machine to Client** policy.	Desktop ← Terminal	**NOTE** You can copy files from an external storage device to the desktop by sending files only when both the client (TC/SC) and the desktop run Windows. 1. Log in to the desktop. 2. Click ∨ on the top of the desktop to expand the floating toolbar, and click — to minimize the Workspace client. 3. Select the file to be copied from the terminal device. Example: **copy2workspace.txt** 4. Right-click, choose **Send to**, and select a desktop disk.

Enabled Policy	Data Flow	User Guide
Enable the **File Redirection** policy and set it to **Read-only**.	Desktop ← Terminal	**Windows desktops:** 1. Log in to the desktop. 2. In the lower left corner of the desktop, click 📁. In the navigation pane on the left, click 🖥. The computer list page is displayed. 3. In **Network locations**, double-click 🖧 to access the terminal device disk other than the local disk of the desktop. 4. Find the file to be copied in the target path and copy it. Example: **copy2workspace.txt** 5. Return to the computer list page. Under **Devices and drives**, go to the local disk of the desktop. 6. Select a path and paste the copied file.
Enable the **File Redirection** policy and set it to **Read/ Write**.	Desktop → Terminal	**Windows desktops:** 1. Log in to the desktop. 2. In the lower left corner of the desktop, click 📁. In the navigation pane on the left, click 🖥. The computer list page is displayed. 3. Under **Devices and drives**, go to the local disk of the desktop. 4. Find the file to be copied in the target path and copy it. Example: **workspace2C.txt** 5. Return to the computer list page. In **Network locations**, double-click 🖧 to access the terminal device disk other than the local disk of the desktop. 6. Select a path and paste the copied file.

Enabled Policy	Data Flow	User Guide
	Desktop ← Terminal	**Windows desktops:** 1. Log in to the desktop. 2. In the lower left corner of the desktop, click 📁. In the navigation pane on the left, click 🖥. The computer list page is displayed. 3. In **Network locations**, double-click 🖧 to access the terminal device disk other than the local disk of the desktop. 4. Find the file to be copied in the target path and copy it. Example: **copy2workspace.txt** 5. Return to the computer list page. Under **Devices and drives**, go to the local disk of the desktop. 6. Select a path and paste the copied file.
Enable the **USB Port Redirection** policy and select **Storage Device (such as USB flash drives)**.	Desktop → Terminal	**Windows desktops:** 1. Log in to the desktop. 2. In the lower left corner of the desktop, click 📁. In the navigation pane on the left, click 🖥. The computer list page is displayed. 3. Under **Devices and drives**, go to the local disk of the desktop. 4. Find the file to be copied in the target path and copy it. Example: **workspace2C.txt** 5. Return to the computer list page. In **Network locations**, double-click 🖧 to access the external USB device storage disk of the terminal device. 6. Select a path and paste the copied file.

Enabled Policy	Data Flow	User Guide
	Desktop ← Terminal	**Windows desktops:** 1. Log in to the desktop. 2. In the lower left corner of the desktop, click 📁. In the navigation pane on the left, click 🖥. The computer list page is displayed. 3. In **Network locations**, double-click 🖧 to access the external USB device storage disk of the terminal device. 4. Find the file to be copied in the target path and copy it. Example: **copy2workspace.txt** 5. Return to the computer list page. Under **Devices and drives**, go to the local disk of the desktop. 6. Select a path and paste the copied file.

2.1.12 How Do I Do If the Desktop Screen Cannot Be Adapted?

By default, the desktop screen automatically adapts to the display device. If automatic adaptation is not enabled, you can manually configure the parameters based on the terminal device in use.

- TC
  a. Expand the client floating box on the top of the desktop and click — to minimize the desktop.
  b. Choose **Start** > **Control Center**, and then double-click **Display**.
  c. Adjust the DVI resolution.
- PC
  a. Expand the client floating box on the top of the desktop and click — to minimize the desktop.
  b. Right-click in a blank area on the desktop of the local PC and choose **Display settings** from the shortcut menu.
  c. Adjust the resolution.

2.1.13 How Do I Do If I Cannot Receive an Email for Creating a Desktop or Assigning a User?

Contact the administrator to configure **Resend Notification** on the user management page.

2.1.14 How Do I Manually Configure Time Synchronization on a Windows Desktop?

If the system time of a Windows user desktop is different from the standard time and has not been automatically synchronized for a long time, perform the following steps to manually synchronize the time:

Step 1 Right-click ⊞ in the lower left corner of the desktop and choose **Run** from the shortcut menu.

Step 2 Enter **cmd** and press **Enter** to open the command-line interface (CLI).

Step 3 Run the following command to synchronize the desktop time:

```
w32tm /resync /rediscover
```

If the command is executed successfully, the time synchronization is successful.

Step 4 The system time is the same as the standard time.

----End

2.1.15 What If the Hop Count of a Cloud Desktop Is Abnormal?

Scenarios

After the network of a cloud desktop is reset, the hop count is restored to the default value, which may cause Internet access failure.

Procedure

Step 1 Press **Win** + **R** on the desktop. In the **Run** dialog box, enter **cmd** and press **Enter** to open the CLI.

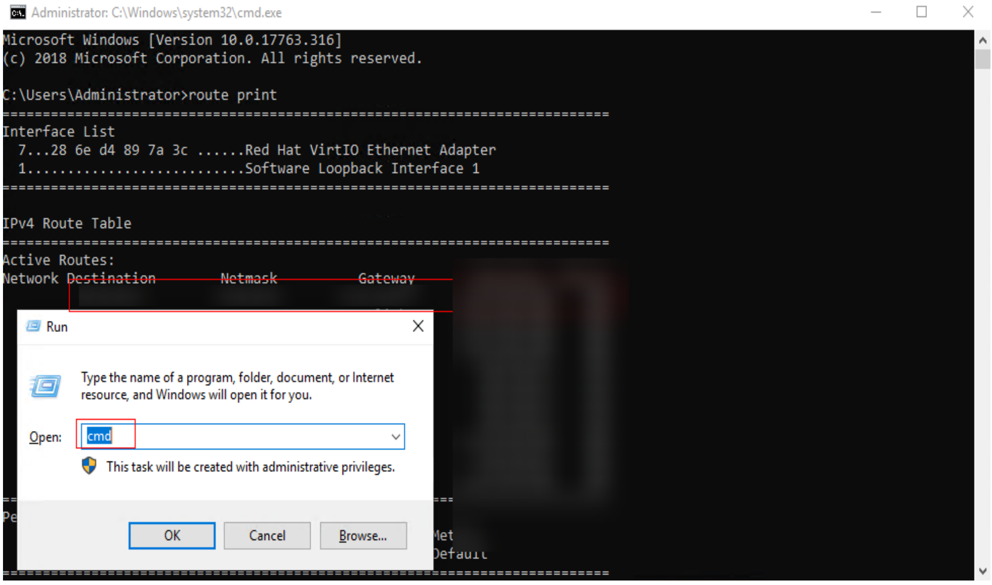
Step 2 Enter **route print** and press **Enter** to view the result.

NOTE

The service NIC is the subnet NIC in the VPC created by the user.

- Normal routing

  Example: There are two routes. The hop count of the service subnet is 4. A value smaller than 5 indicates that the service NIC has a high priority and the routing is normal.



```
Microsoft Windows [Version 10.0.17763.316]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>route print
===========================================================================
Interface List
  7...28 6e d4 89 7a 3c ......Red Hat VirtIO Ethernet Adapter
  1.........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway
```

[redacted]

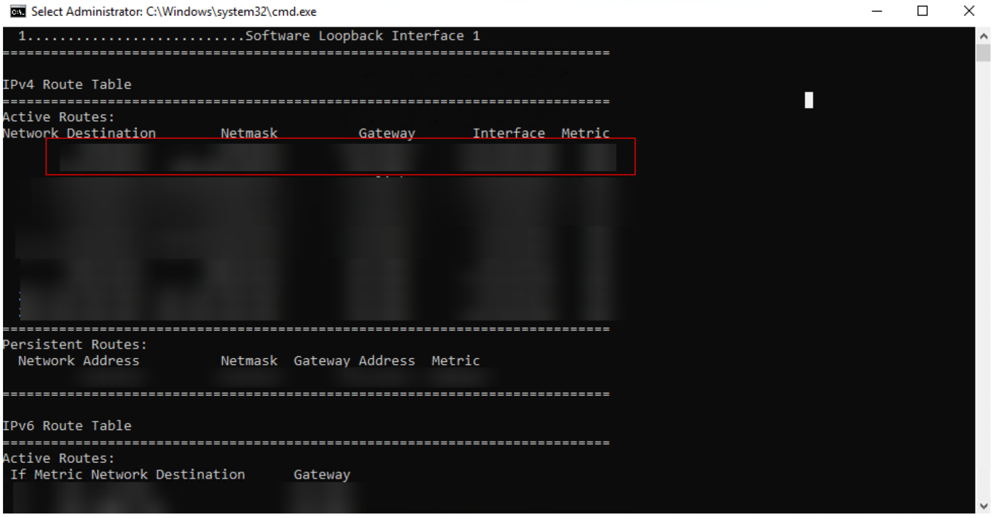
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: cmd

This task will be created with administrative privileges.

- Abnormal routing

  Example: There are two routes. The hop count of the service subnet is 7. A value greater than 5 indicates that the service NIC has a low priority and the routing is abnormal.



```
  1.........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
```

[redacted]

```
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
```

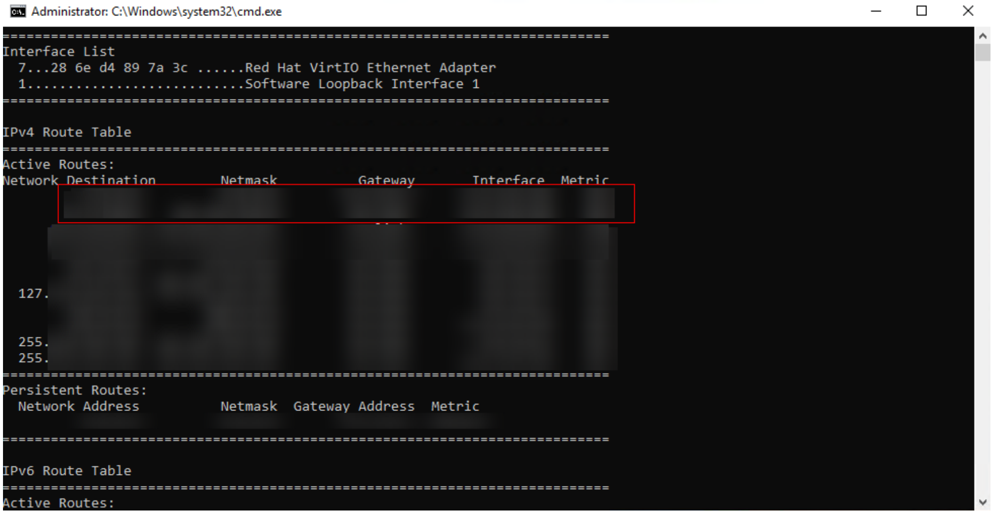
[redacted]

```
===========================================================================

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
```

[redacted]

- Abnormal routing

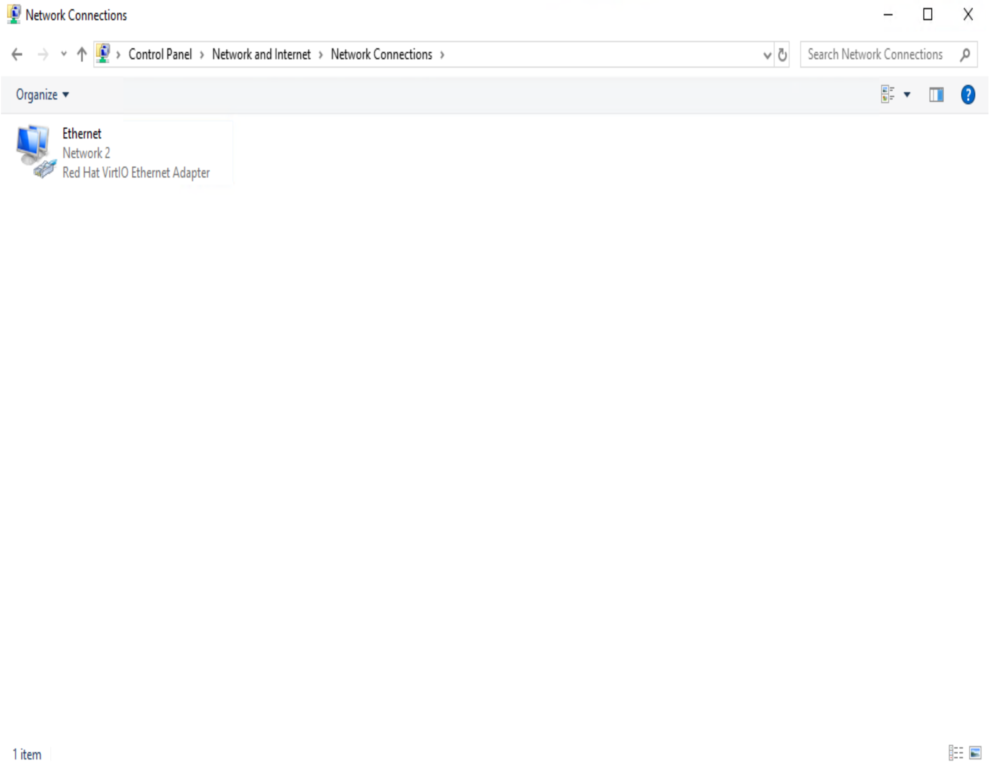
  Example: There are two routes. The hop count of the service subnet is 5, indicating that the service NIC is the same as the NIC of the management CIDR block. As a result, network requests cannot distinguish the NICs and the routing is abnormal.



Administrator: C:\Windows\system32\cmd.exe

```
===========================================================================
Interface List
  7...28 6e d4 89 7a 3c ......Red Hat VirtIO Ethernet Adapter
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
[redacted]

  127.[redacted]


  255.
  255.
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric

===========================================================================

IPv6 Route Table
===========================================================================
Active Routes:
```

Step 3 Press **Win** + **R** on the desktop. In the **Run** dialog box, enter **ncpa.cpl** and press **Enter** to go to the **Network Connections** page.



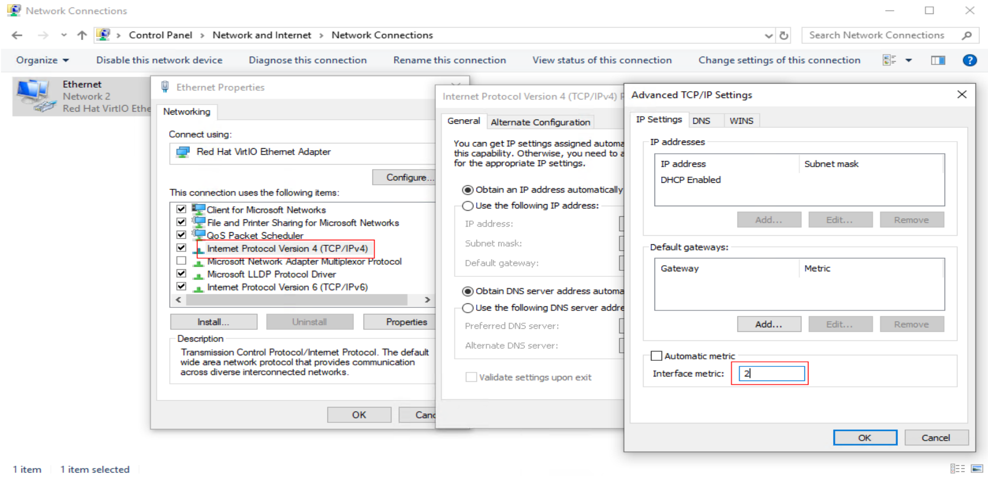
Network Connections
Control Panel › Network and Internet › Network Connections ›
Search Network Connections
Organize ▾
Ethernet
Network 2
Red Hat VirtIO Ethernet Adapter
1 item

📖 NOTE

Depending on the desktop system version, you may find multiple NICs or only one NIC.

Step 4 Double-click the service NIC. In the displayed dialog box, click **Properties**. On the **Networking** tab, double-click **Internet Protocol Version 4 (TCP/IPv4)** to go to the **Internet Protocol Version 4 (TCP/IPv4) Properties** page.

Step 5 Click **Advanced**. On the **IP Settings** tab, deselect **Automatic metric** and set **Interface metric** of the service NIC to a value less than that of the management CIDR block. For example, if the hop count of the management CIDR block is 5, the value of **Interface metric** of the service NIC must be less than 5.


Network Connections
Control Panel > Network and Internet > Network Connections
Search Network Connections
Organize
Disable this network device
Diagnose this connection
Rename this connection
View status of this connection
Change settings of this connection
Ethernet
Network 2
Red Hat VirtIO Ethe
Ethernet Properties
Networking
Connect using:
Red Hat VirtIO Ethernet Adapter
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
Internet Protocol Version 4 (TCP/IPv4)
Microsoft Network Adapter Multiplexor Protocol
Microsoft LLDP Protocol Driver
Internet Protocol Version 6 (TCP/IPv6)
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
OK
Canc
Internet Protocol Version 4 (TCP/IPv4) P
General
Alternate Configuration
You can get IP settings assigned automa this capability. Otherwise, you need to a for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automa
Use the following DNS server addre
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced TCP/IP Settings
IP Settings
DNS
WINS
IP addresses
IP address
Subnet mask
DHCP Enabled
Add...
Edit...
Remove
Default gateways:
Gateway
Metric
Add...
Edit...
Remove
Automatic metric
Interface metric:
2
OK
Cancel
1 item
1 item selected

Step 6 Click **OK**.

----End

2.2 Login Issues

2.2.1 What If I Forget the Password?

- If you lose or forget the login password, contact the administrator.
  - For desktops connected to the AD server, the administrator resets the password for the user on the AD server and notifies the user of the new password.
  - For desktops that are not connected to the AD server, the system sends the address for resetting the password to the reserved email address after the administrator processes the password.

  NOTICE

  The validity period of the password resetting link in the email is 24 hours.

- If you lose or forget the login password, you can perform the following operations to reset the password:
  a. Click **Forgot Password** on the login page. The **Password Reset Request** page is displayed.
  b. On the displayed page, enter the username, user email address, and enterprise ID, and click **OK**.

     NOTE

     If the system displays a message indicating that the account is an AD domain account, contact the administrator.
  c. After receiving the email, click the link for resetting the password in the email. On the password resetting page, reset the password as prompted and click **OK**.

NOTICE

The validity period of the password resetting link in the email is 24 hours.

2.2.2 What If the Account Is Locked?

If your account is locked because you enter incorrect passwords or dynamic verification codes for five consecutive times, contact the administrator for technical support and enter the correct password to log in again.

2.2.3 Which Devices Can Be Used for Desktop Login?

You can log in to a desktop using a **thin client (TC)**, **soft client (SC)**, or **mobile terminal**.

2.2.4 What If Desktop Login Failed?

You can rectify the fault based on the displayed information. The possible causes and corresponding handling procedures are listed for reference, as shown in **Table 2-3**. If the login still fails, contact the administrator.

Table 2-3 Example

Login Failure Prompt	Possible Cause	Handling Method
6005: Your VM is not ready. Please try again later or restart the TC.	An internal copy error occurs on the client.	● Method 1: Try to log in to the desktop again. ● Method 2: Restart the TC and log in again.
6008: Your VM is not ready. Try again later.	The client program is running abnormally because of incorrect memory allocation.	● Method 1: Try to log in to the desktop again. ● Method 2: Restart the TC and log in again.
6008: Your client version is not supported. Update the client version.	The client version does not match the server version.	Update the client version.

Login Failure Prompt	Possible Cause	Handling Method
6010: Your VM is not ready. Try again later or contact the administrator.	The configuration on the client is not synchronized with that on the server.	● Method 1: Try to log in to the desktop again. ● Method 2: Restart the client and log in again. ● Method 3: Restart the computer and log in again.
6050: Network errors exist. Try again later.	The network connection between the client and the server is abnormal.	● Method 1: Check whether the network connection between the client and the server is normal. ● Method 2: Restart the computer and log in again.
00030216: The desktop time is not synchronized. Try restarting the desktop or contacting the administrator.	The desktop time is not synchronized with the server time on the managemen t side.	● Method 1: 1. Open the self-help console and log in to the cloud desktop. 2. On the cloud desktop, press **Win** + **R**, enter **cmd**, and press **Enter**. In the displayed command window, run the following command to synchronize the cloud desktop time: w32tm /resync /rediscover 3. Return to the VM list and log in to the cloud desktop again. ● Method 2: Restart the computer and log in again.

2.2.5 What If I Can't Pass Multi-Factor Authentication?

You can rectify the fault based on the following scenarios. If the fault persists, contact the administrator to submit a service ticket.

Login Timeout

Possible causes

When you log in to a desktop from a client, you enter the username and password to go to the multi-factor authentication page. However, you do not bind a virtual MFA device for a long time or do not submit a dynamic verification code for the second authentication.

Solution

Return to the login page, log in again, bind a virtual MFA device, and submit a dynamic verification code for the second authentication.

Abnormal Verification Code

Possible causes

- The verification code is incorrect.
- The verification code is not the virtual MFA verification code of your account.
- If the time difference between your mobile phone and the virtual MFA device is greater than 30 seconds, the MFA verification code generated on your mobile phone will fail the verification.

Solution

- Enter the correct verification code.
- Contact the administrator to delete the MFA device. Then you log in to the desktop again and bind the virtual MFA device again to obtain the verification code.
- Ensure that the time on your mobile phone is the same as the time on the virtual MFA device, and try again. (You do not need to consider the time zone on your mobile phone, because the MFA authentication will be based on UTC time.)

Locked Account

Possible causes

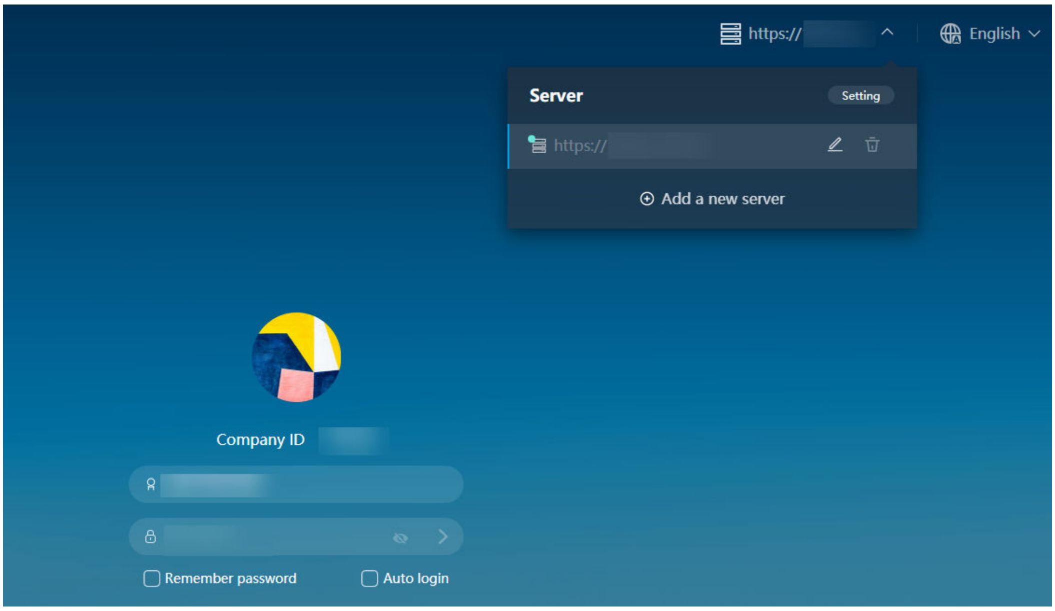
If you enter an incorrect verification code five consecutive times, the account will be locked.

Solution

Contact the administrator to unlock the account and enter the correct verification code.

2.2.6 What If a Message Is Displayed Indicating Login Failure Due to Policy Restrictions?

Step 1 Click the server address in the upper right corner of the login page to expand the server list.



Step 2 Change the IP address of the current login server or add a new IP address.

Changing the IP address of the current login server

1. Locate the row that contains the current login address, click ✎, and change the access address to the Direct Connect access address.

   NOTE

   You can contact the administrator to obtain the Direct Connect access address on the **Tenant Configuration** page of the Workspace console.

2. Click **OK**.

Adding a new server address

1. Click **Add a new server** and enter the Direct Connect access address and enterprise ID.

   NOTE

   You can contact the administrator to obtain the Direct Connect access address and enterprise ID on the **Tenant Configuration** page of the Workspace console.

2. Click **Confirm**.

Step 3 Log in again.

- If the login is successful, no further action is required.
- If the login still fails, contact the administrator.

----End

2.3 Terminal Binding Problems

2.3.1 How Do I Obtain the MAC Address of a Terminal?

Scenario

The administrator specifies a terminal device for logging in to the corresponding cloud desktop. The administrator needs to obtain the MAC address of the terminal device and binds them on the management console. You can perform the following operations to obtain the MAC address of a device based on the device type:

TC

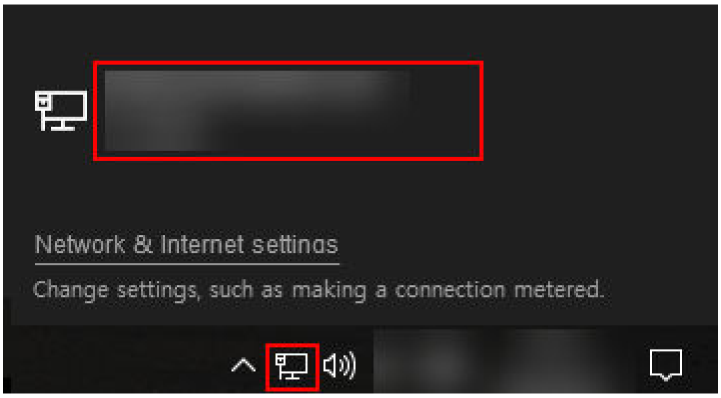
Workspace supports login from multiple types of TCs. The operations vary depending on the TC model. The following is only an example.

1. Power on the TC.
2. Choose **Start** > **Control Center**.
3. Double-click **Network**.
4. On the displayed page, click **Property**. The NIC information page is displayed.
5. Record the MAC address.

PCs

- **Windows PCs**

  a. In the lower right corner of the local PC, click 🖳 and select the connected network, as shown in the following figure. The Ethernet settings page is displayed.

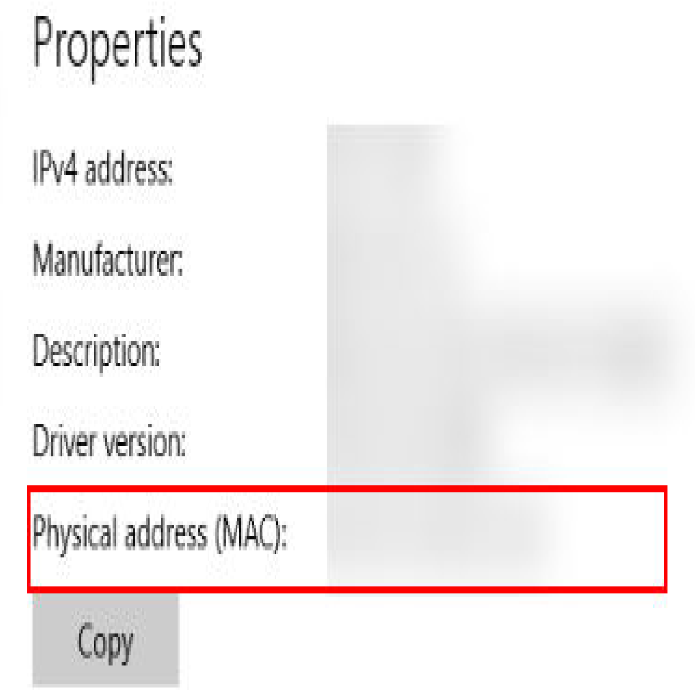
  

  Change settings, such as making a connection metered.

  b. Click the connected network under Ethernet. The network information page is displayed.

  c. The **Physical address (MAC)** in the **Properties** area is the required MAC address, as shown in **Figure 2-5**.

Figure 2-5 MAC address of the Windows PC



Properties

IPv4 address: [redacted]

Manufacturer: [redacted]

Description: [redacted]

Driver version: [redacted]

Physical address (MAC): [redacted]

d. Record the MAC address.

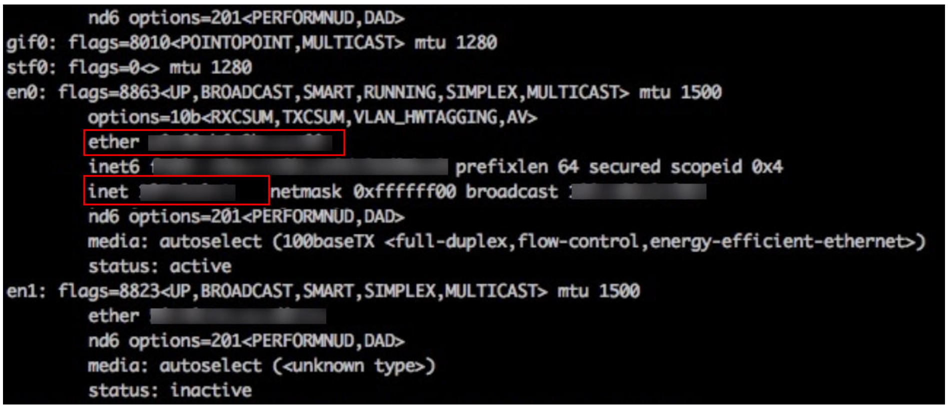
- **macOS PCs**

a. Open the terminal on the local PC.

b. Enter the **ifconfig** command.

c. In the command output, the ether information corresponding to the network adapter whose name contains **inet** is the required MAC address.

Figure 2-6 MAC address of the macOS PC



```
        nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=10b<RXCSUM,TXCSUM,VLAN_HWTAGGING,AV>
        ether [redacted]
        inet6 [redacted] prefixlen 64 secured scopeid 0x4
        inet [redacted] netmask 0xffffff00 broadcast [redacted]
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect (100baseTX <full-duplex,flow-control,energy-efficient-ethernet>)
        status: active
en1: flags=8823<UP,BROADCAST,SMART,SIMPLEX,MULTICAST> mtu 1500
        ether [redacted]
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect (<unknown type>)
        status: inactive
```

d. Record the MAC address.

2.4 OS Issues

2.4.1 Can I Update the Desktop OS?

You cannot update the OS, but you can install patches on the OS.

NOTE

After obtaining the OS patch package, run the patch installation file on the desktop to install the patch and restart the desktop for the patch to take effect.

2.4.2 Which OSs Are Supported by Cloud Desktops?

Cloud desktops of Workspace support the following OSs and will support more in the future:

- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- UOS V20 1050/1060
- Kylin V10 SP1

2.4.3 Which Software Cannot Be Uninstalled?

Windows

Do not uninstall the following software:

- **Access Agent**
- **Microsoft .NET Framework *x* Client Profile**
- **Microsoft .NET Framework *x* Extended**
- **Microsoft Visual C++ *xxx* Redistributable - *xxx***

2.4.4 Which Files Cannot Be Deleted?

Do not delete files or folders in **C:\Program Files\Huawei**.

2.4.5 Which Software Cannot Be Upgraded?

Do not upgrade the OS kernel. Otherwise, the system may run slowly or abnormally.

2.4.6 Which Ports Cannot Be Deleted?

Do not delete the following ports. Otherwise, the system may malfunction.

- 28511
- 28512
- 28521

- 28522
- 8502-8509
- 6781
- 6791
- 6969
- 6970

2.4.7 Which Commands Cannot Be Executed?

Windows

Do not execute the script or command, for example, **route DELETE ***, to modify route data.

2.4.8 How Do I Query the System Information?

Windows

1. Right-click **This PC** and choose **Properties** from the shortcut menu.
2. In the **System** window, view the system information.

2.4.9 Is There Any Help Document for OSs?

Obtain documentation for Windows from the official website.

2.5 Client Issues

2.5.1 What If the Workspace Client Installation Failed?

You can install the Huawei Cloud Workspace client only on devices running the following OSs:

- Windows 10 or later
- macOS 10.14 to 13.6
- Android 6.0 or later

If the client installation still fails, **submit a service ticket** for technical support.