10 Workspace FAQs

Issue	01
Date	2026-04-15



HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2026. All rights reserved.

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

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: https://www.huawei.com

Email: support@huawei.com

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

 Copyright © Huawei Technologies Co., Ltd.

Contents

1 FAQs for Administrators....1
1.1 What Are the Features and Advantages of Workspace?....2
1.2 How Is Workspace Charged?....2
1.3 How Do I Check My Quotas?....3
1.4 How Do I Increase My Quotas?....3
1.5 How Do I Add a Disk?....4
1.6 How Do I Connect the Desktop to a Local Printer?....4
1.7 How Do I Connect the Desktop to a Network Printer?....8
1.8 How Do I Do If the Desktop Fails to Connect to the AD?....10
1.9 Can I Change the User Authentication Mode of the Desktop?....10
1.10 How do I Enable LDAPS on the AD Server?....11
1.11 How do I Export the Root Certificate of an LDAPS-enabled AD server?....17
1.12 What If I Fail to Purchase a Desktop?....17
1.13 How Do I Do If the Functions of Purchasing a Desktop, Creating a User, Creating a Policy, and Enabling the Internet are Unavailable?....18
1.14 Can I Use Private Images to Purchase Desktops?....18
1.15 How Many Private Images Can Be Created on Workspace at Most?....18
1.16 What Are the Network Requirements for Logging In to Desktops?....18
1.17 How Do I Do If My Desktop Cannot Access the Internet?....19
1.18 How Do I Configure Workspace to Access the Internet?....20
1.19 How Do I Configure Workspace to Access the Enterprise Intranet?....20
1.20 How Do I Enable the Internet on Other Cloud Service Pages?....20
1.21 How Do I Copy Files Between a Desktop and a Local Storage Device?....25
1.22 What If I Lost the Administrator Password?....40
1.23 How Does an Administrator Unlock an End User Account?....41
1.24 How Do I Do If an End User Fails to Log In to a Desktop?....41
1.25 How Do I Back Up and Restore a Desktop?....42
1.26 How Do I Do If a Message Is Displayed Indicating Duplicate Policy Names During Policy Import?....42
1.27 How Do I Do If a User Cannot Be Bound to a Client Using the Dynamic Verification Code of the Previously Bound MFA Device?....43
1.28 How Do I Do If the Message "Insufficient permissions for the IAM account. Security Administrator permissions required." Is Displayed When I Enable an Agency?....43
1.29 How Do I Do If a User Does Not Receive an Email for Creating a Desktop or Assigning a User?....45

 Copyright © Huawei Technologies Co., Ltd.

1.30 How Do I Add Resources to or Remove Resources from an Enterprise Project After Purchasing Workspace?..... 45
1.31 Why Can't I Start a Pay-per-Use Cloud Desktop?..... 45
1.32 How Do I Enable IPv6 on Workspace?..... 45
1.33 How Do I Enable RDP on Workspace?..... 46
1.34 How Do I Configure Security Group Rules When Using a Custom Security Group?..... 48
2 FAQs for End Users..... 51
2.1 Desktop Usage Issues..... 51
2.1.1 How Do I Do If the Desktop Freezes?..... 51
2.1.2 How Do I Do If the Disk Space Is Insufficient?..... 52
2.1.3 How Do I Enter the CLI Mode?..... 52
2.1.4 How Do I Do If My Desktop Cannot Connect to the Internet?..... 52
2.1.5 Do Cloud Desktops Support Personalized Settings?..... 54
2.1.6 How Do I Take a Screenshot?..... 54
2.1.7 How Do I Do If the Printer Cannot Be Used?..... 55
2.1.8 What If I Can't Use Network Printers on Workspace?..... 56
2.1.9 How Do I Download the Software?..... 57
2.1.10 How Do I Do If Data Disks of a Windows Desktop Cannot Be Found After Recomposing the System Disk?..... 58
2.1.11 What Do I Do If I Cannot Copy Files Between a Desktop and a Local Storage Device?..... 59
2.1.12 How Do I Do If the Desktop Screen Cannot Be Adapted?..... 64
2.1.13 How Do I Do If I Cannot Receive an Email for Creating a Desktop or Assigning a User?..... 64
2.1.14 How Do I Manually Configure Time Synchronization on a Windows Desktop?..... 65
2.2 Login Issues..... 65
2.2.1 How Do I Do If I Forget the Password?..... 65
2.2.2 What If the Account Is Locked?..... 66
2.2.3 What Devices Can Be Used to Log In to a Desktop?..... 66
2.2.4 What If I Fail to Log in to a Desktop?..... 66
2.2.5 How Do I Do If I Cannot Pass Multi-Factor Authentication?..... 67
2.2.6 How Do I Do If the System Displays a Message Indicating that the Login Fails Due to Policy Restrictions?..... 68
2.3 Terminal Binding Problems..... 69
2.3.1 How Do I Obtain the MAC Address of a Terminal?..... 69
2.4 OS Issues..... 71
2.4.1 Can I Update the Desktop OS?..... 71
2.4.2 What OSs Can Run on Workspace?..... 71
2.4.3 Which Software Cannot Be Uninstalled?..... 71
2.4.4 Which Files Cannot Be Deleted?..... 71
2.4.5 Which Software Cannot Be Upgraded?..... 72
2.4.6 Which Ports Cannot Be Deleted?..... 72
2.4.7 Which Commands Cannot Be Executed?..... 72
2.4.8 How Do I Query the System Information?..... 72
2.4.9 Is There Any Help Document for OSs?..... 72

 Copyright © Huawei Technologies Co., Ltd.

A Change History 73

1 FAQs for Administrators

1.1 What Are the Features and Advantages of Workspace?
1.2 How Is Workspace Charged?
1.3 How Do I Check My Quotas?
1.4 How Do I Increase My Quotas?
1.5 How Do I Add a Disk?
1.6 How Do I Connect the Desktop to a Local Printer?
1.7 How Do I Connect the Desktop to a Network Printer?
1.8 How Do I Do If the Desktop Fails to Connect to the AD?
1.9 Can I Change the User Authentication Mode of the Desktop?
1.10 How do I Enable LDAPS on the AD Server?
1.11 How do I Export the Root Certificate of an LDAPS-enabled AD server?
1.12 What If I Fail to Purchase a Desktop?
1.13 How Do I Do If the Functions of Purchasing a Desktop, Creating a User, Creating a Policy, and Enabling the Internet are Unavailable?
1.14 Can I Use Private Images to Purchase Desktops?
1.15 How Many Private Images Can Be Created on Workspace at Most?
1.16 What Are the Network Requirements for Logging In to Desktops?
1.17 How Do I Do If My Desktop Cannot Access the Internet?
1.18 How Do I Configure Workspace to Access the Internet?
1.19 How Do I Configure Workspace to Access the Enterprise Intranet?
1.20 How Do I Enable the Internet on Other Cloud Service Pages?
1.21 How Do I Copy Files Between a Desktop and a Local Storage Device?
1.22 What If I Lost the Administrator Password?
1.23 How Does an Administrator Unlock an End User Account?

 Copyright © Huawei Technologies Co., Ltd.

1.24 How Do I Do If an End User Fails to Log In to a Desktop?

1.25 How Do I Back Up and Restore a Desktop?

1.26 How Do I Do If a Message Is Displayed Indicating Duplicate Policy Names During Policy Import?

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

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

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

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

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

1.32 How Do I Enable IPv6 on Workspace?

1.33 How Do I Enable RDP on Workspace?

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

1.1 What Are the Features and Advantages of Workspace?

The web-based console allows users to independently create, delete, and flexibly use out-of-the-box desktops.

Workspace has the following features:

- Turnkey: Desktops can be provisioned and deployed quickly and work out of the box whereas deploying conventional private desktops takes several days.
- Easy management: Administrators can manage hundreds of desktops at the same time using the web-based console.
- Elastic scaling: On-demand purchase and elastic scaling are supported.
- Efficient office: Users can access their personal desktops using terminals such as PCs and pads anytime and anywhere without interruption, greatly improving office efficiency.
- Secure office: Encrypted remote access, isolated tenant resources, and network and peripheral security control secure data access.

1.2 How Is Workspace Charged?

Yearly/Monthly: It is a pay-before-use mode.

Pay-per-Use (hourly): You pay for only the resources you actually use. Less than one hour will be calculated as one hour.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- You will be charged for using NAT to access the Internet. For details, see **Billing (Public NAT Gateway)**.
- The administrator 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 **Post Payment** in the Billing Center.

1.3 How Do I Check My Quotas?

NOTE

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

Step 1 Visit the **Huawei Cloud official website**. Log in to the console as the 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

1.4 How Do I Increase My Quotas?

NOTE

You can only increase quotas of the current administrator account.

Step 1 Visit the **Huawei Cloud official website**. Log in to the console as the 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

 Copyright © Huawei Technologies Co., Ltd.

1.5 How Do I Add a Disk?

NOTE

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

Step 1 Visit the **Huawei Cloud official website**. Log in to the console as the 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 **Desktop management** page is displayed.

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

The page for adding a data disk is displayed.

Step 6 Click **Add a data disk** and configure the data disk.

- **High IO Disk**: uses serial attached SCSI (SAS) drives to store data. High I/O disks are suitable for commonly accessed workloads.
- **Ultra high IO Disk**: uses solid state disk (SSD) drives to store data. This disk type is 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 are sure to add it.**.

Step 8 Click **Next**.

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

----End

1.6 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.

 Copyright © Huawei Technologies Co., Ltd.

Step 1 Log in to the console as the 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.

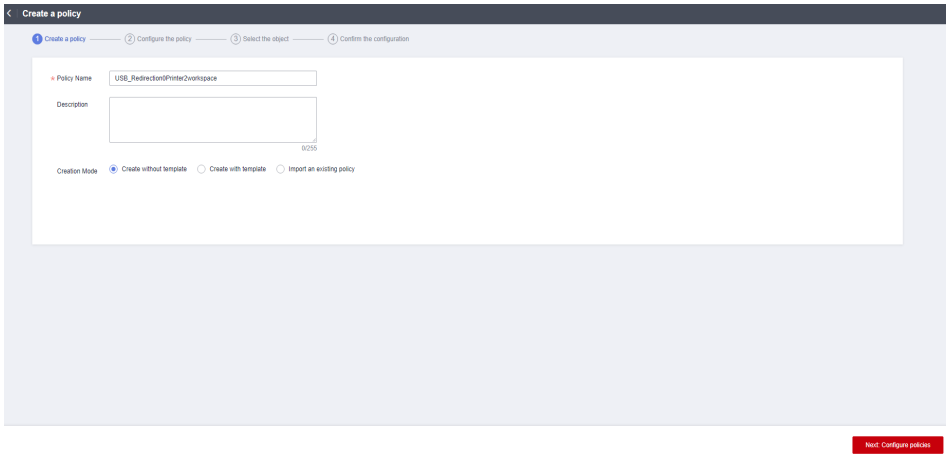
Step 4 Click **Policies**.

The **Policies** page is displayed.

Step 5 Click **Create a policy**.

The page for creating a policy is displayed.

Figure 1-1 Creating a policy



Step 6 Configure the **policy name** and **description**.

NOTE

- The **policy name** must contain digits, letters, and underscores (_), and cannot contain more than 55 characters, for example, **USB_Redirection0Printer2workspace**.
- The policy description contains a maximum of 255 characters. For example, use a local printer using the USB port redirection policy.

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

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

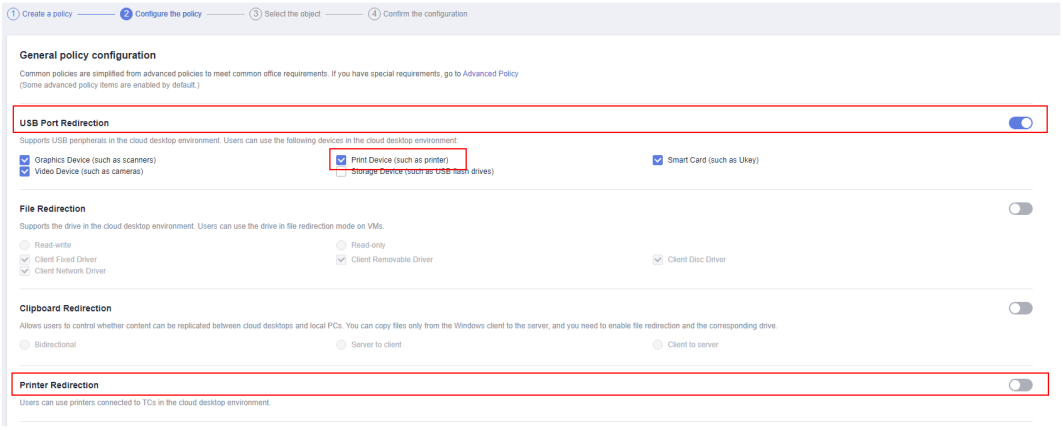
The page for general policy configuration is displayed.

Step 9 Enable **USB Port Redirection** and select **Print Device (such as printer)**, as shown in **Figure 1-2**.

Step 10 Disable **Printer Redirection**, as shown in **Figure 1-2**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-2 Configuring policy parameters

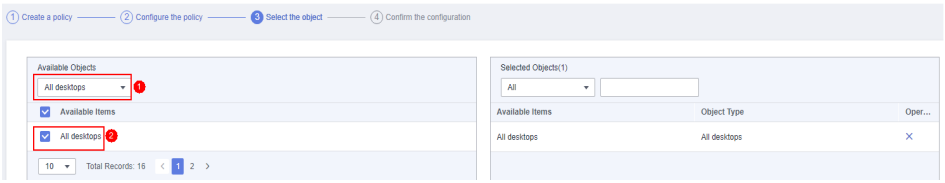


Step 11 Click **Next: Select objects**.

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 1-3 Selecting an object



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 **2.1.7 How Do I Do If the Printer Cannot Be Used?**.

----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 the 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.

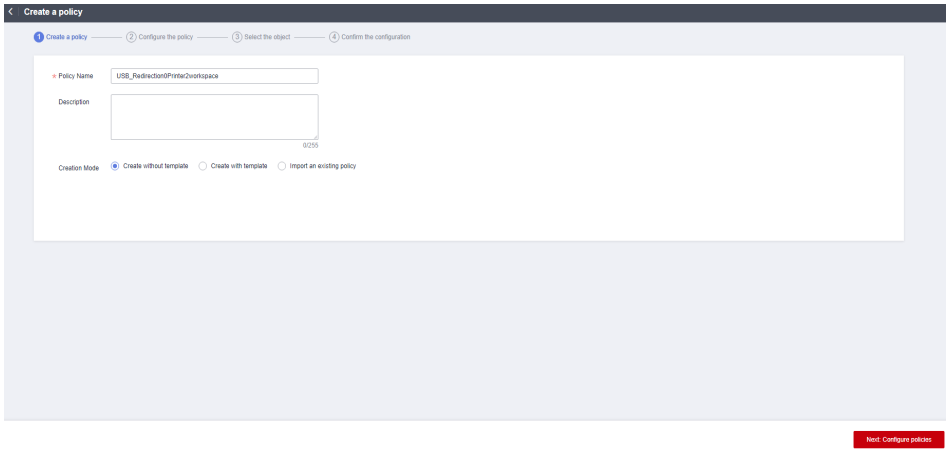
Step 4 Click **Policies**.

The **Policies** page is displayed.

Step 5 Click **Create a policy**.

The page for creating a policy is displayed.

Figure 1-4 Creating a policy



Step 6 Configure the **policy name** and **description**.

NOTE

- The **policy name** must contain digits, letters, and underscores (_), and cannot contain more than 55 characters, for example, **Printer_Device_Redirection0Printer2workspace**.
- The policy description contains a maximum of 255 characters. For example, **Use a local printer with the printer redirection policy.**

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

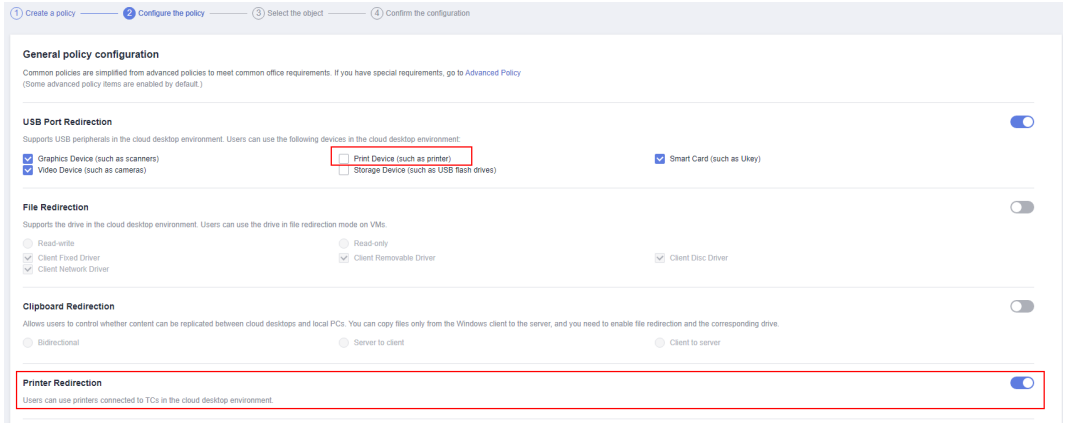
Step 8 Click **Next: Configure policies**.

The page for general policy configuration is displayed.

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

Step 10 Enable **Printer Redirection**, as shown in **Figure 1-5**.

Figure 1-5 Configuring policy parameters



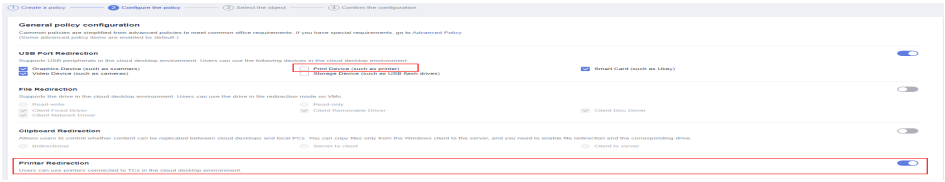
Step 11 Click **Next: Select objects**.

 Copyright © Huawei Technologies Co., Ltd.

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 1-6 Selecting an object



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 **2.1.7 How Do I Do If the Printer Cannot Be Used?**.

----End

1.7 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 the 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**.

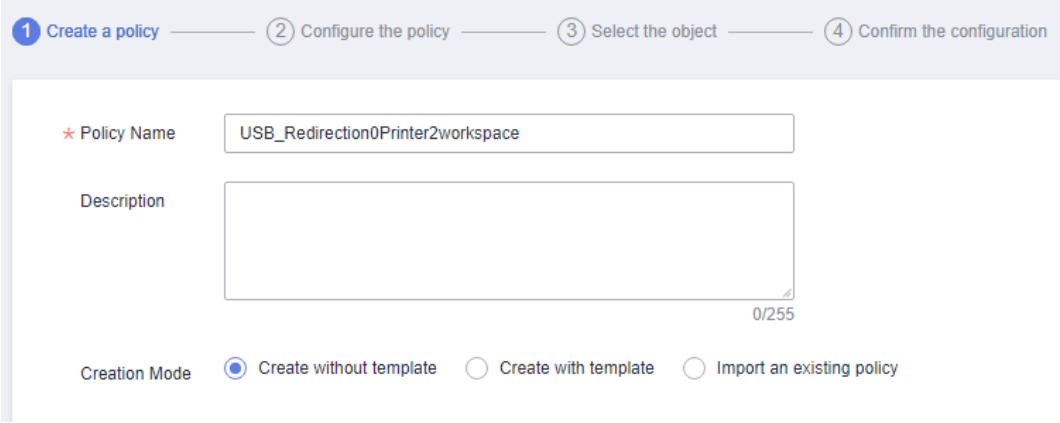
The **Policies** page is displayed.

Step 5 Click **Create a policy**.

The page for creating a policy is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-7 Creating a policy



Step 6 Configure the **policy name** and **description**.

NOTE

- The policy name must contain digits, letters, and underscores (_), and cannot contain more than 55 characters, for example, **Network_Printer_Policy**.
- The policy description contains a maximum of 255 characters, For example, **Use a network printer with the printer redirection policy.**

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

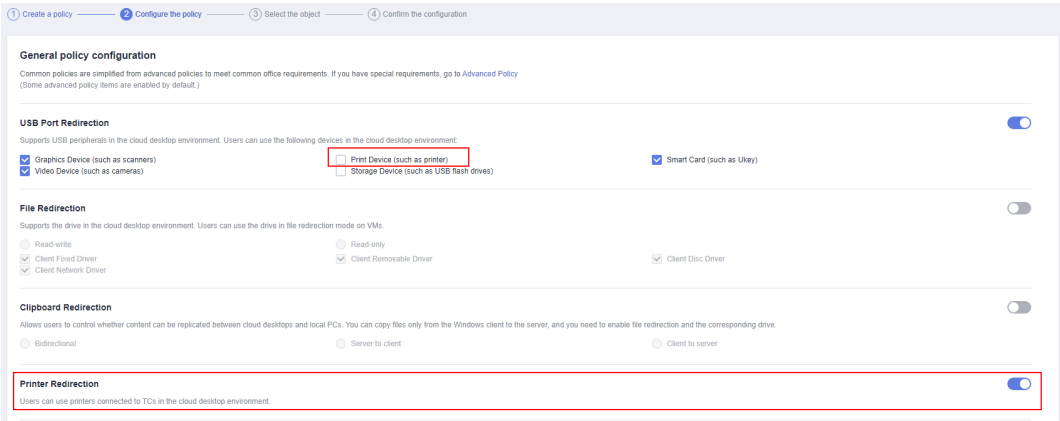
Step 8 Click **Next: Configure policies**.

The page for general policy configuration is displayed.

Step 9 Deselect **Print Device (such as printer)** under **USB Port Redirection**, as shown in **Figure 1-8**.

Step 10 Enable **Printer Redirection**, as shown in **Figure 1-8**.

Figure 1-8 Configuring policy parameters



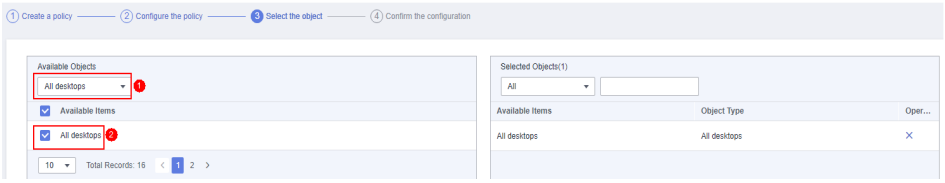
Step 11 Click **Next: Select objects**.

Step 12 Select an object as required.

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

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-9 Selecting an object



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 **2.1.8 What If I Can't Use Network Printers on Workspace?**.

----End

1.8 How Do I Do If the Desktop Fails to Connect to the AD?

Step 1 Check whether the information on the desktop 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 Workspace 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 Workspace and Windows AD.** If the interconnection still fails, go to **Step 4**.

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

----End

1.9 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, purchased a desktop in another project with no desktop and configure the required user

 Copyright © Huawei Technologies Co., Ltd.

authentication mode for the new desktop. Exercise caution when purchasing desktops by referring to the following description.

- If the enterprise does not deploy the Windows AD for user authentication, select **No** when purchasing desktops. That is, the desktop uses the account authentication system of Huawei for user authentication.
- If the enterprise has an existing unified AD for user authentication and the desktop also needs to use this authentication mode, select **Yes** when purchasing the desktop.

NOTE

- For details about how to purchase a desktop, see **Purchasing Desktops in Yearly/Monthly Mode.**
- For details about project-related operations, see **Projects**

1.10 How do I Enable LDAPS on the AD Server?

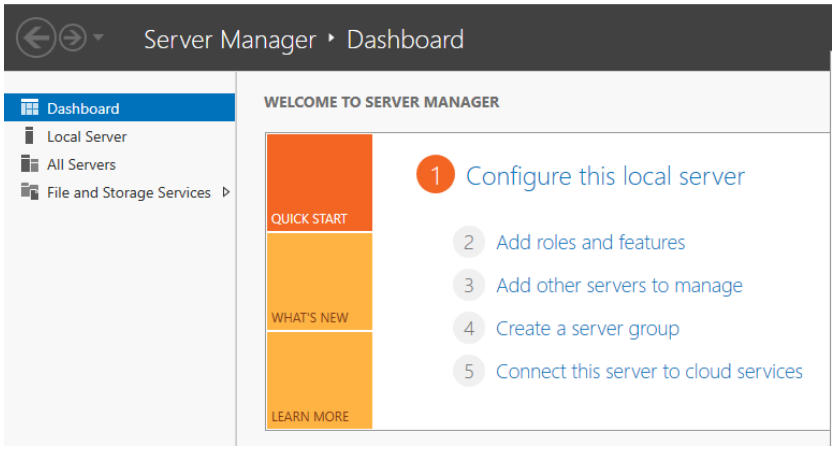
If an enterprise needs to enable LDAPS so that cloud desktops can communicate with AD server applications using LDAPS, perform the following operations:

- 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 1-10**.

Figure 1-10 Server manager



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

 Copyright © Huawei Technologies Co., Ltd.

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**.

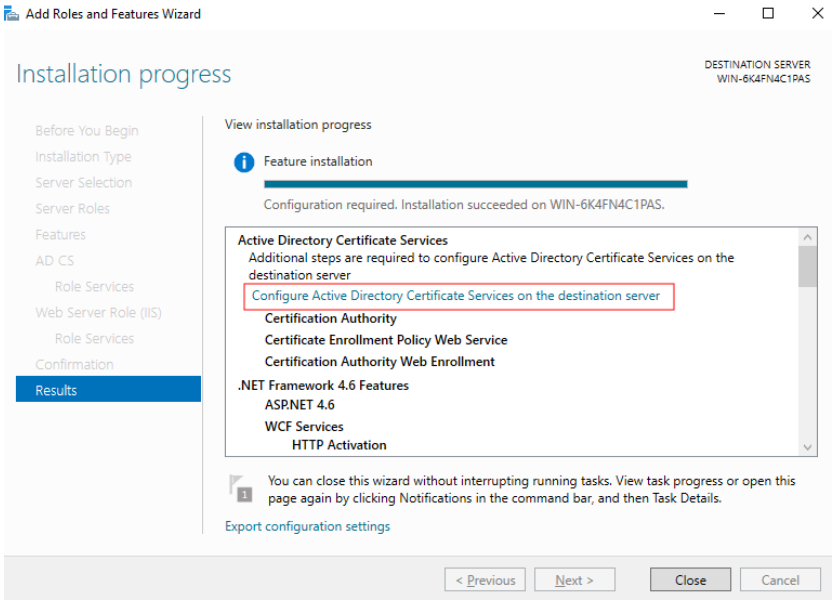
Step 10 Select **Certification Enrollment Policy Web Service** and click **Add Features**.

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 1-11**. The **AD CS Configuration** page is displayed.

Figure 1-11 Configuring the Active Directory certificate service



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.

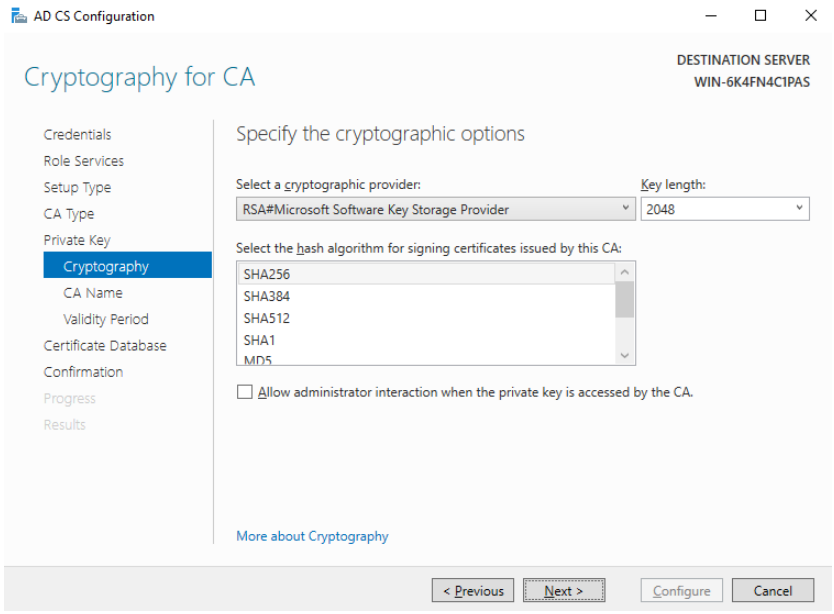
 Copyright © Huawei Technologies Co., Ltd.

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 1-12**.

Figure 1-12 Cryptography settings



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.

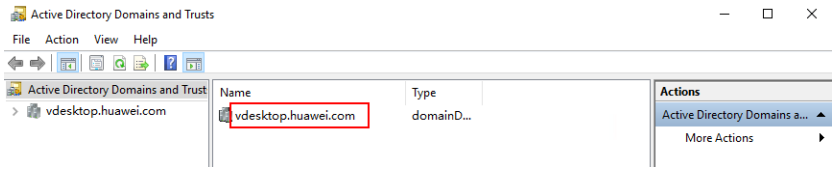
Step 2 On **Connection**, click **Connect**.

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 1-13**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-13 Domain name



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 configurations and click **Finish**.

Step 16 Log in to the standby AD server.

 Copyright © Huawei Technologies Co., Ltd.

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**.

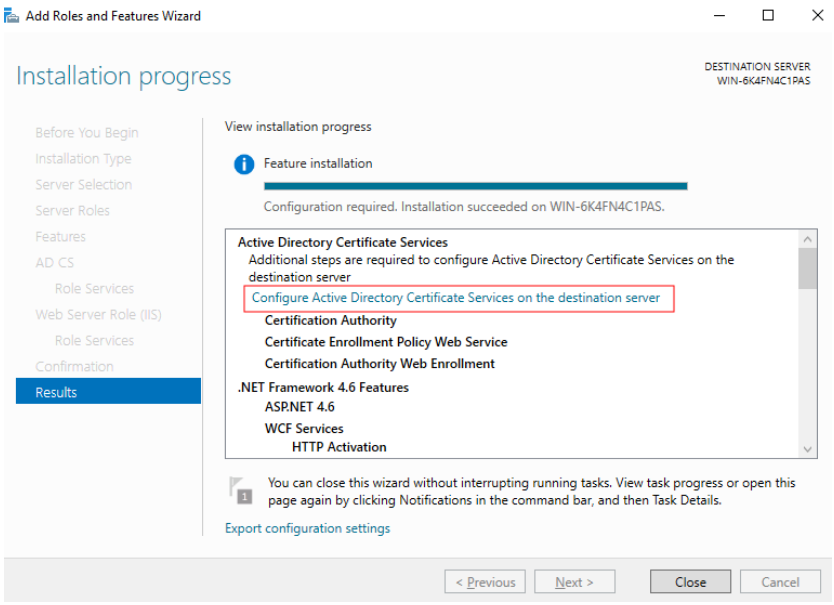
Step 27 Select **Certification Enrollment Policy Web Service** and click **Add Features**.

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 1-14**. The **AD CS Configuration** page is displayed.

Figure 1-14 Configuring the Active Directory certificate service



 Copyright © Huawei Technologies Co., Ltd.

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

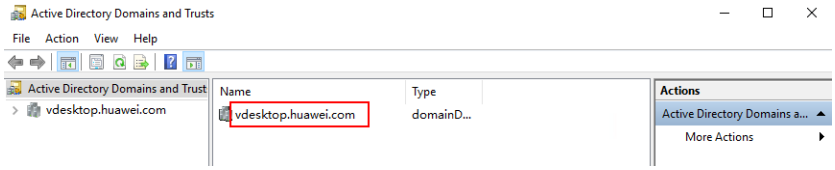
Step 1 On the desktop of the standby AD server, click  and enter **Ldp** to start Ldp.

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 1-15**.

Figure 1-15 Domain name



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

Step 5 Select **SSL**.

Step 6 Click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

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

----End

1.11 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

1.12 What If I Fail to Purchase a Desktop?

If you fail to purchase a desktop, submit a service ticketsubmit a service ticket to obtain technical support.

 Copyright © Huawei Technologies Co., Ltd.

1.13 How Do I Do If the Functions of Purchasing a Desktop, Creating a User, Creating a Policy, and Enabling the Internet are Unavailable?

After the administrator enables the service, the system automatically locks the service if no desktop exists in the current project (without sub-projects) or sub-projects for more than 14 days. As a result, the functions of **Desktop Purchase**, **Create User**, **Create a Policy**, and **Enable the Internet** are unavailable. Administrators can click **Reactivate** on the **Tenant Configuration** page to activate the service. After the service is reactivated, the preceding functions are available.

1.14 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 restrictions, 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, create and configure an ECS, and convert the ECS to a private desktop image. For details, see **Creating a Windows Private Image**.

1.15 How Many Private Images Can Be Created on Workspace at Most?

You can create a maximum of 500 private images on Workspace, but they are restricted by the IMS configuration.

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

Table 1-1 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.

 Copyright © Huawei Technologies Co., Ltd.

Table 1-1 Network QoS requirements

Level	Network QoS Requirement	User Experience
Excellent	• Packet loss rate ≤ 0.01% • Round-trip latency ≤ 30 ms • Network jitter ≤ 10 ms	Smooth office work, smooth audio and video playback. Operations on peripherals such as USB storage devices are smooth.
Good	• Packet loss rate ≤ 0.1% • Round-trip latency ≤ 50 ms • Network jitter ≤ 10 ms	Smooth office work; occasional frame freezing during audio/video playback; slow peripheral identification; slow operations on storage devices such as data copy of USB flash drives
Acceptable	• Packet loss rate ≤ 0.3% • Round-trip latency ≤ 100 ms • Network jitter ≤ 40 ms	Basic office services are available, frame freezing occurs during audio/video playback, and the system identifies and responds slowly to peripherals.

1.17 How Do I Do If My Desktop Cannot Access the Internet?

Checking whether Internet access has been enabled

Step 1 Log in to the console as the administrator.

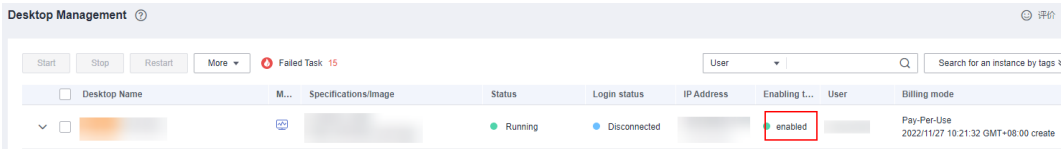
Step 2 Click in the upper left corner and select the desired region and project.

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

The **Dashboard** page is displayed.

Step 4 In the navigation pane, click **Desktop Management**.

Figure 1-16 Desktop network status



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

- If **enabled** is displayed in the **Enabling the Internet** column, go to **Step 5**.

 Copyright © Huawei Technologies Co., Ltd.

- If **disabled** is displayed, try to access the Internet by referring to **Configuring Workspace to Access the Internet**. 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 **Fault Locating**.

- If the network configuration is correct, go to **Step 6**.
- If the network configuration is incorrect, modify the configuration by referring to **Fault Locating** and try again. If the fault persists, go to **Step 6**.

Submitting a service ticket

Step 6 Submit a service ticket for technical support.

----End

1.18 How Do I Configure Workspace to Access the Internet?

If a desktop needs to access the Internet, see **Configuring Workspace to Access the Internet**.

1.19 How Do I Configure Workspace to Access the Enterprise Intranet?

If a desktop needs to access the enterprise intranet, see **Configuring Workspace to Access the Enterprise Intranet**.

1.20 How Do I Enable the Internet on Other Cloud Service Pages?

Scenario

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 so that the cloud desktop can access the Internet. You can use the quick entry on Workspace to purchase NAT and EIP services to enable the Internet. For details, see **Configuring Workspace to Access the Internet**.

 Copyright © Huawei Technologies Co., Ltd.

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, a self-registered Huawei account has 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 user 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 **Creating a User and Granting NAT Gateway Permissions** and .

Procedure (Not Interconnecting to Windows AD)

Creating an EIP

Step 1 Log in to the console as the administrator.

Step 2 Click in the upper left corner and select the region and project where the desktop to access the public network is located.

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

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

Step 5 Set the parameters by referring to the parameter description in section **Assigning an EIP**.

NOTE

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

Step 6 Click **Next**.

Step 7 Confirm the configurations 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 Set the parameters by referring to the parameter description in section **Create a Public NAT Gateway**.

NOTE

Select the VPC and subnet to which the desktop that needs to access the Internet belongs.

Step 11 Click **Next**.

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

 Copyright © Huawei Technologies Co., Ltd.

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.

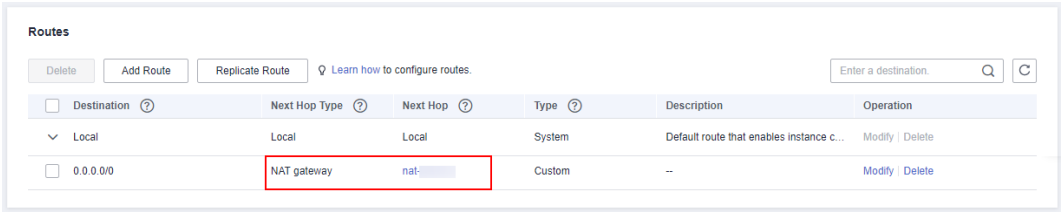
Step 17 In the **Networking Components** area on the right of the page, click the *number next to* ***Route Tables*** to go to the route table list page of the VPC.

Step 18 Click *the name of the target route table*. The basic information list is displayed.

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 1-17**.

Figure 1-17 Route to the NAT gateway



- If the route shown in **Figure 1-17** exists, go to **Step 20**.
- If the route shown in **Figure 1-17** 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 Set the parameters based on the parameter description in section **Add 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** state, the rule is added successfully.

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

 Copyright © Huawei Technologies Co., Ltd.

Step 25 Use the user account and password to log in to the desktop through the client to check whether the desktop can access the external network.

----End

Procedure (Interconnecting to Windows AD)

Creating an EIP

Step 1 Log in to the console as the administrator.

Step 2 Click in the upper left corner and select the region and project where the desktop to access the public network is located.

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

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

Step 5 Set the parameters by referring to the parameter description in section **Assigning an EIP**.

NOTE

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

Step 6 Click **Next**.

Step 7 Confirm the configurations 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**. The **Buy Public NAT Gateway** page is displayed.

Step 10 Set the parameters by referring to the parameter description in section **Create a Public NAT Gateway**.

NOTE

Select the VPC and subnet to which the desktop that needs to access the Internet belongs.

Step 11 Click **Next**.

Step 12 Confirm the configurations 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.

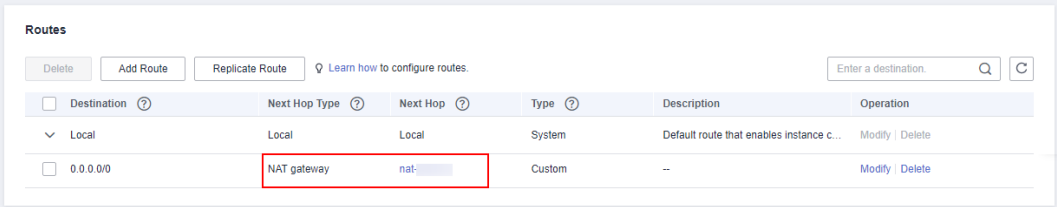
 Copyright © Huawei Technologies Co., Ltd.

Step 18 Click *the name of the target route table*. The basic information list is displayed.

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 1-17**.

Figure 1-18 Route to the NAT gateway



- If the route shown in **Figure 1-17** exists, go to **Step 20**.
- If the route shown in **Figure 1-17** 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 Set the parameters based on the parameter description in section **Add 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** state, the rule is added successfully.

Configuring DNS forwarding

Step 25 Log in to the DNS server as the 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.

 Copyright © Huawei Technologies Co., Ltd.

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

The default DNS server IP address of the desktop region can be obtained from the **private DNS server addresses provided by Huawei Cloud**.

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

Step 35 Use the user account and password to log in to the desktop through the client to check whether the desktop can access the external network.

----End

1.21 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

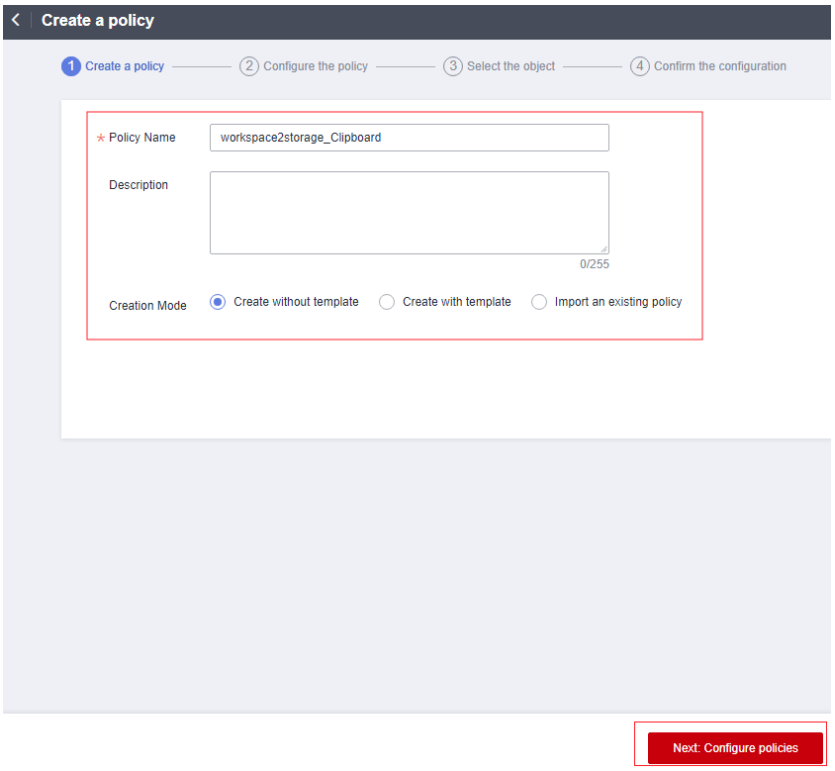
If Workspace desktops are used in offices and there are strict requirements for input data on office desktops, you can configure the clipboard policies for the desktops.

1. Log in to the console as the administrator.
2. Click in the upper left corner and select the desired region and project.
3. Click and choose **Business Applications** > **Workspace** in the service list.
   The **Dashboard** page is displayed.
4. In the navigation tree on the left, choose **Policies** > **Protocol**.
5. Click **Create a policy** in the upper right corner.
6. Configure the policy name, description, and creation mode, and click **Next: Configure policies**.
   - The policy name must contain digits, letters, and underscores (_), and cannot contain more than 55 characters, for example, **workspace2storage_Clipboard**.

 Copyright © Huawei Technologies Co., Ltd.

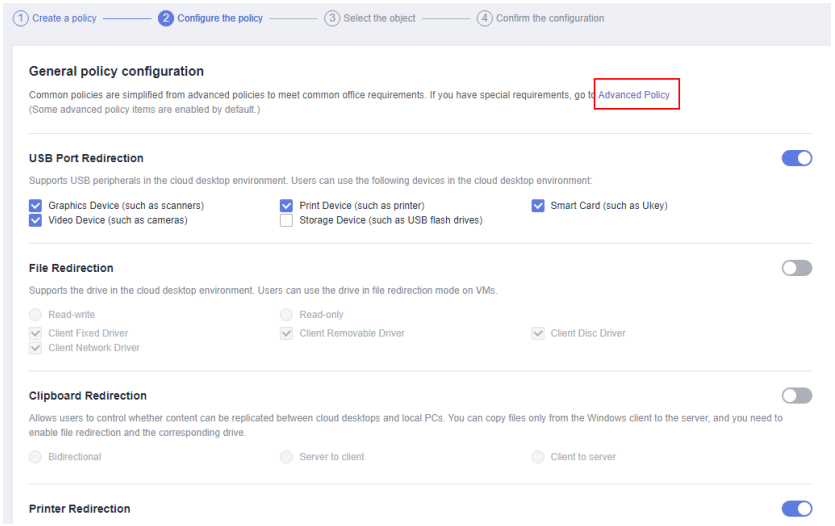
- The policy description contains a maximum of 255 characters, for example, **Clipboard redirection is used to copy files from a Workspace desktop to an external device**.
- Retain the default creation mode.

Figure 1-19 Creating a policy



7. Click **Advanced Policy**.

Figure 1-20 Advanced policy entry



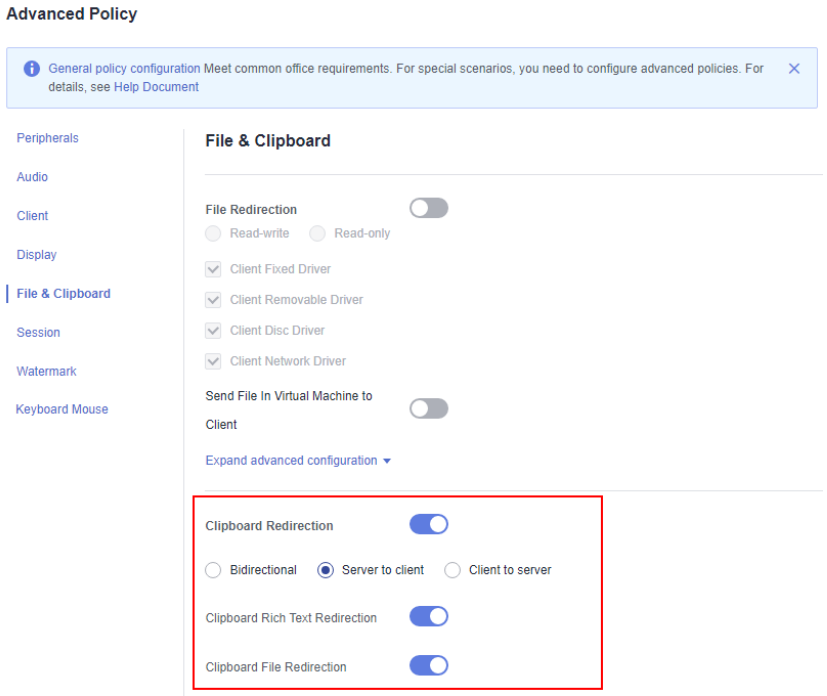
8. On the **Advanced Policy** page, click **File & Clipboard**.
9. Enable the **Clipboard Redirection** policy and select **Server to client**, as shown in **Figure 1-21**.

 Copyright © Huawei Technologies Co., Ltd.

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.

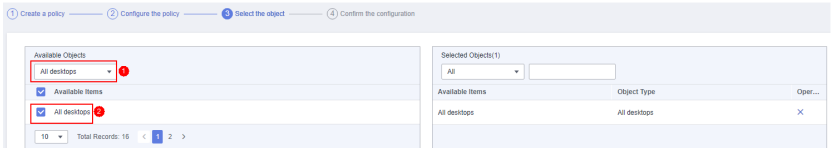
Figure 1-21 Configuring the clipboard redirection policy from the server to the client



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 1-22 Selecting an object



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**

 Copyright © Huawei Technologies Co., Ltd.

a. Log in to the console as the administrator.

b. Click in the upper left corner and select the desired region and project.

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

The **Dashboard** page is displayed.

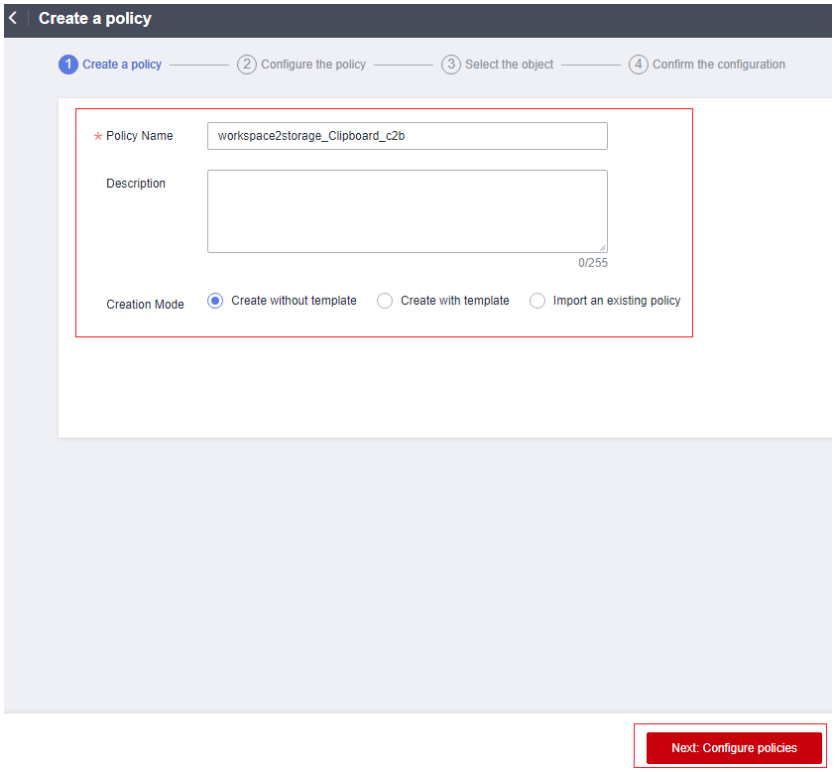
d. In the navigation tree on the left, choose **Policies** > **Protocol**.

e. Click **Create a policy** in the upper right corner.

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

- The policy name must contain digits, letters, and underscores (_), and cannot contain more than 55 characters, for example, **workspace2storage_Clipboard_c2b**.
- The policy description contains a maximum of 255 characters, for example, **Clipboard redirection is used to copy files from an external device to a desktop**.
- Retain the default creation mode.

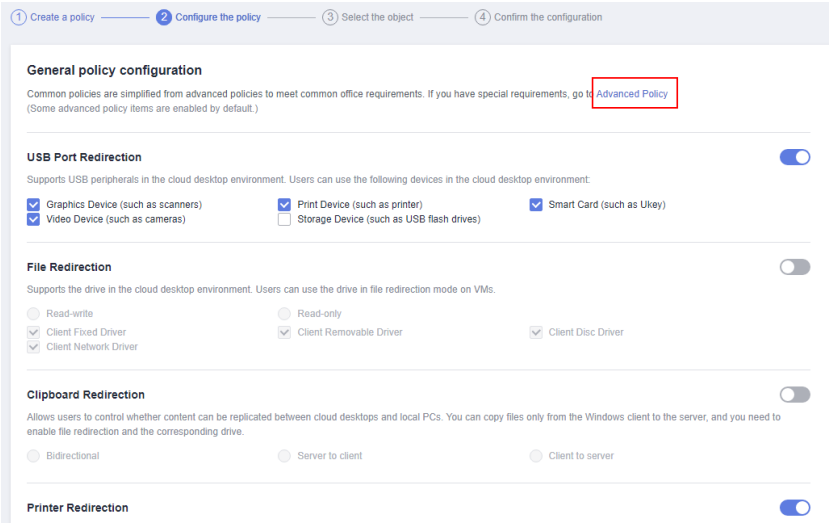
Figure 1-23 Creating a policy



g. Click **Advanced Policy**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-24 Advanced policy entry



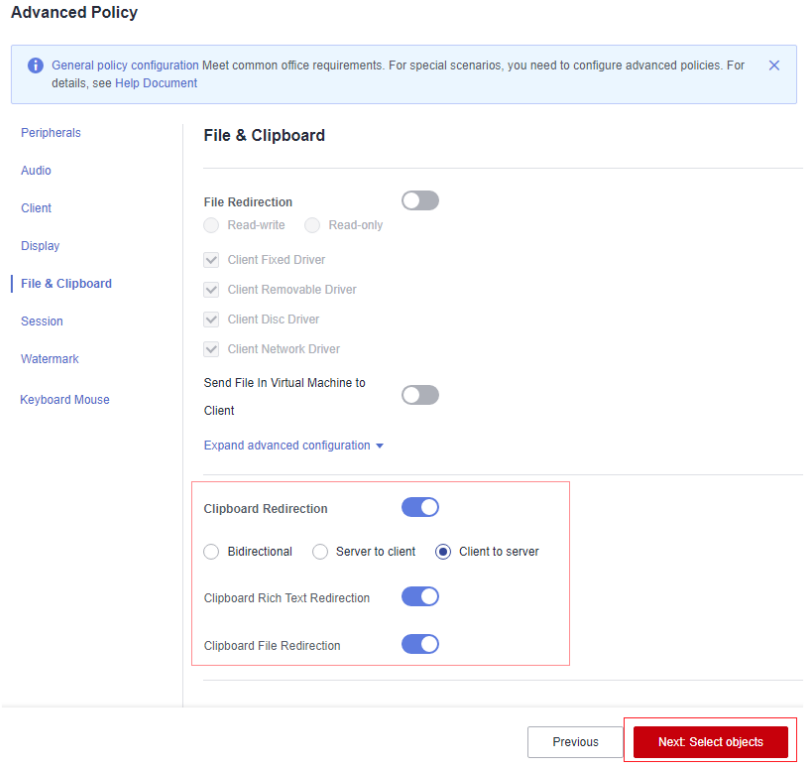
h. On the **Advanced Policy** page, click **File & Clipboard**.

i. Enable the **Clipboard Redirection** policy and select **Client to server**, as shown in **Figure 1-25**.

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 1-25 Configuring the clipboard redirection policy from the client to the server



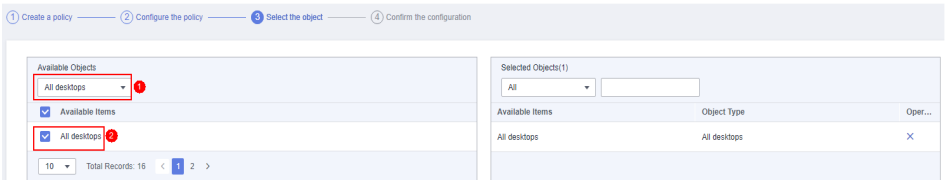
 Copyright © Huawei Technologies Co., Ltd.

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 1-26 Selecting an object



l. Click **Next: Finish**.

- **Sending files from VMs to clients**

a. Log in to the console as the administrator.

b. Click in the upper left corner and select the desired region and project.

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

The **Dashboard** page is displayed.

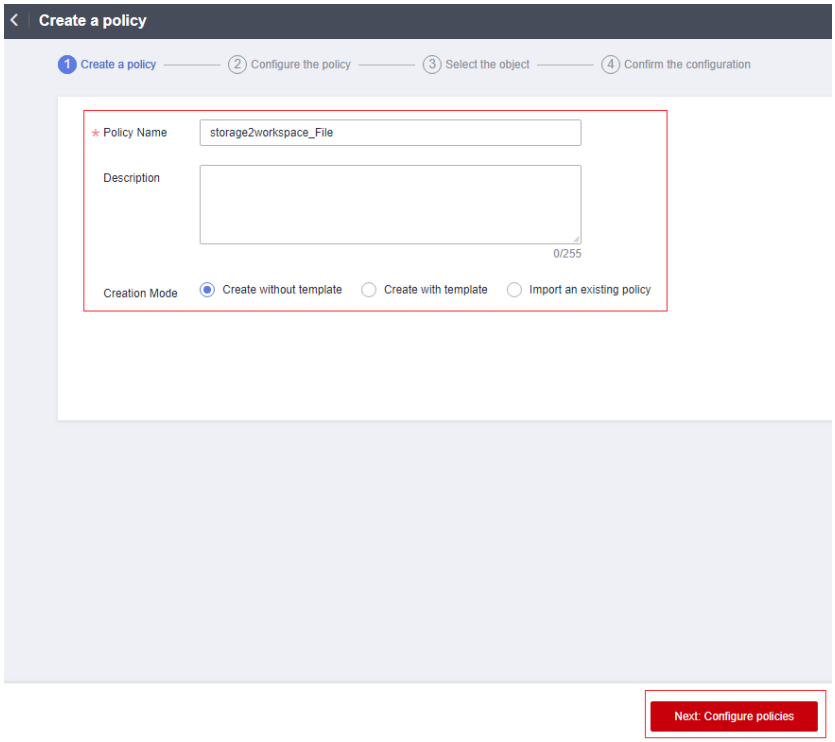
d. In the navigation tree on the left, choose **Policies** > **Protocol**.

e. Click **Create a policy** in the upper right corner.

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

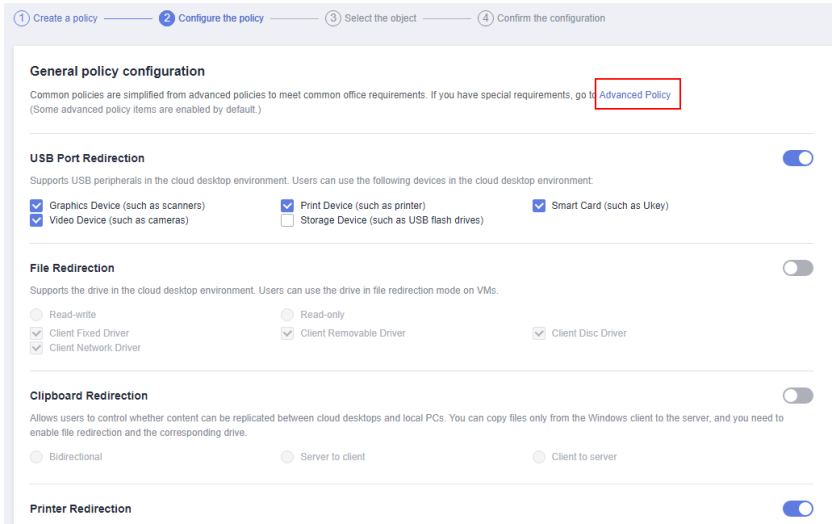
- The policy name must contain digits, letters, and underscores (_), and cannot contain more than 55 characters, for example, **storage2workspace_File**.
- The policy description contains a maximum of 255 characters, for example, **Copying files from an external device to a desktop**.
- Retain the default creation mode.

Figure 1-27 Creating a policy



g. Click **Advanced Policy**.

Figure 1-28 Advanced policy entry



h. On the **Advanced Policy** page, click **File & Clipboard**.

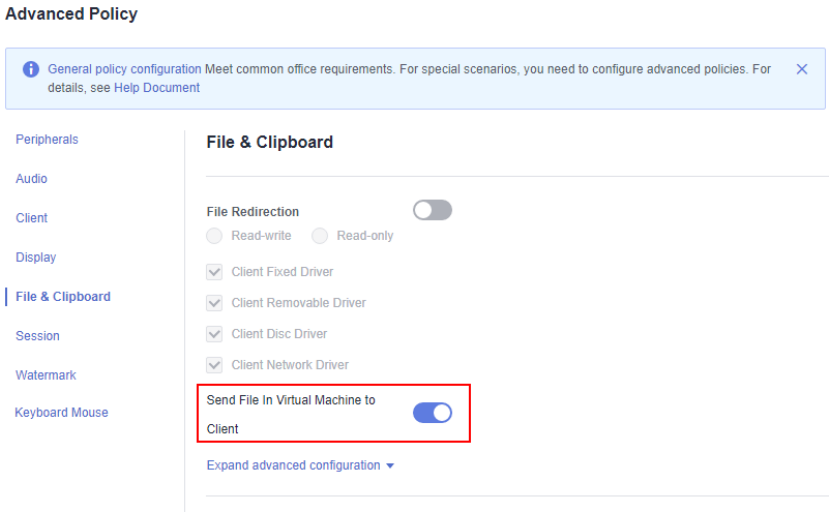
i. Enable **Send File In Virtual Machine to Client** as shown in **Figure 1-29**.

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.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-29 Configuring the policy

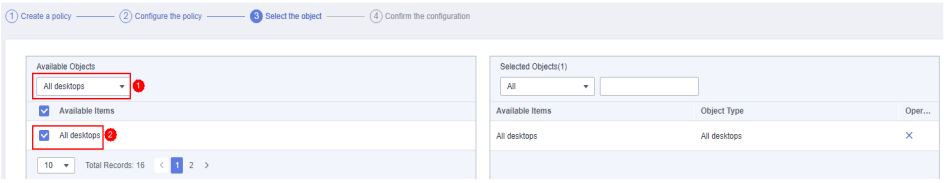


j. Click **Next: Select objects**.

k. Select an object as required.

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

Figure 1-30 Selecting an object



l. Click **Next: Finish**.

- **File redirection**

a. Log in to the console as the administrator.

b. Click  in the upper left corner and select the desired region and project.

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

The **Dashboard** page is displayed.

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

e. Click **Create a policy** in the upper right corner.

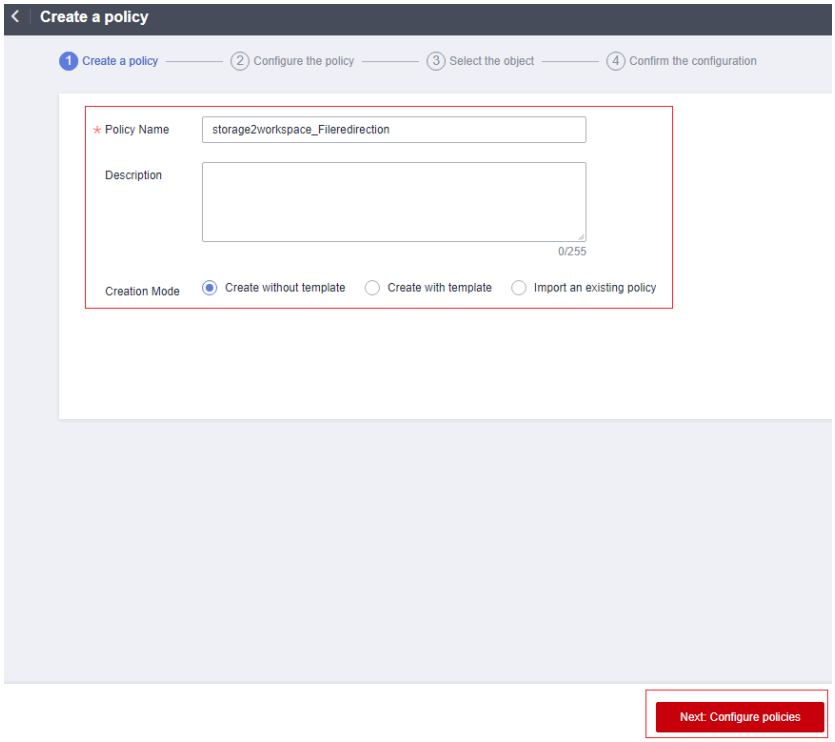
f. Configure the policy name, description, and creation mode, and click **Next: Configure policies**.

- The policy name must contain digits, letters, and underscores (_), and cannot contain more than 55 characters, for example, **storage2workspace_Fileredirection**.
- The policy description contains a maximum of 255 characters, for example, **Copying files from an external device to a desktop**.

 Copyright © Huawei Technologies Co., Ltd.

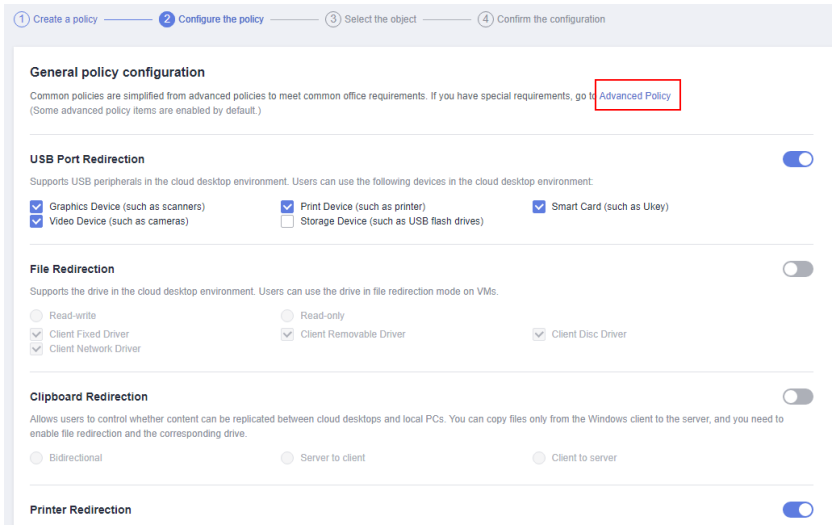
- Retain the default creation mode.

Figure 1-31 Creating a policy



g. Click **Advanced Policy**.

Figure 1-32 Advanced policy entry



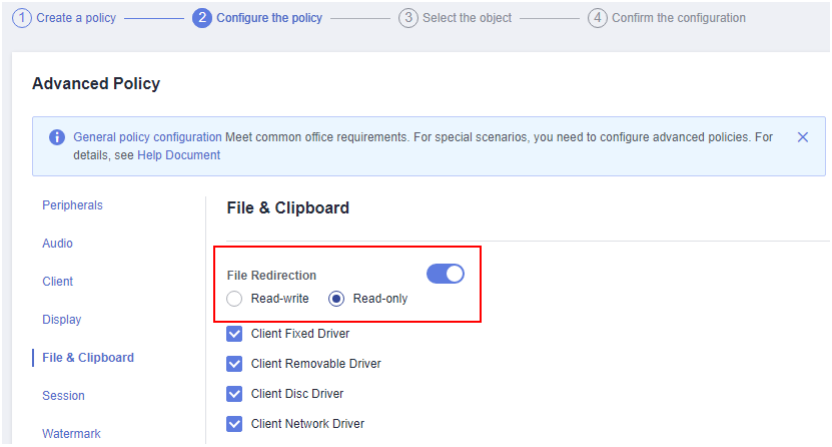
h. On the **Advanced Policy** page, click **File & Clipboard**.

i. Enable the **File Redirection** policy and set it to **Read-only**, as shown in **Figure 1-33**.

NOTE

You do not need to configure other advanced policy parameters under **File & Clipboard**. If you have strict requirements on the traffic and file size, configure them by referring to the parameter description in **Configuring Advanced Policy Parameters**. If you use a Linux terminal, expand **Advanced Policy** and ensure that **Linux Root Directory Mount Switch** is set to . If you use an Android terminal, expand **Advanced Policy** and ensure that **Mobile Client Redirection** is set to .

Figure 1-33 Configuring the policy

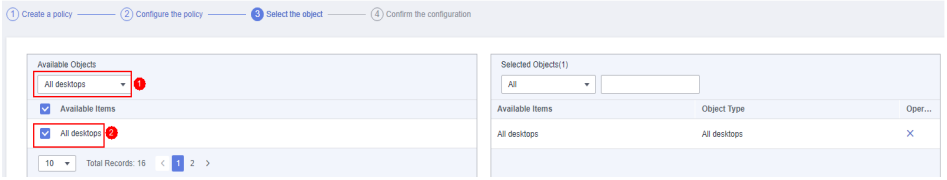


j. Click **Next: Select objects**.

k. Select an object as required.

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

Figure 1-34 Selecting an object



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 the administrator.

 Copyright © Huawei Technologies Co., Ltd.

b. Click in the upper left corner and select the desired region and project.

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

The **Dashboard** page is displayed.

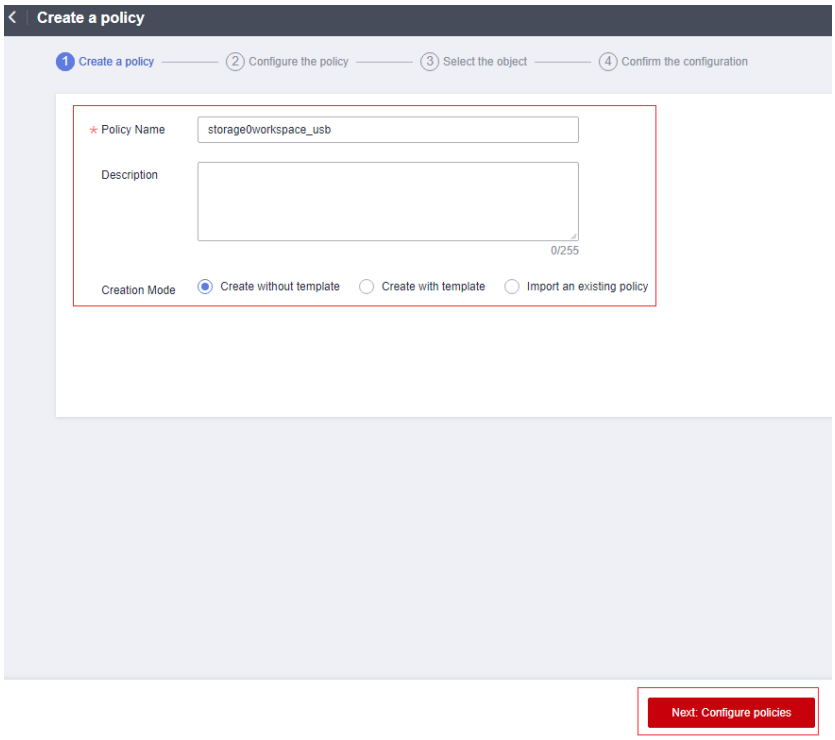
d. In the navigation tree on the left, choose **Policies** > **Protocol**.

e. Click **Create a policy** in the upper right corner.

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

- The policy name must contain digits, letters, and underscores (_), and cannot contain more than 55 characters, for example, **storage0workspace_usb**.
- The policy description contains a maximum of 255 characters, for example, **USB port redirection is used to copy files between external devices and desktops**.
- Retain the default creation mode.

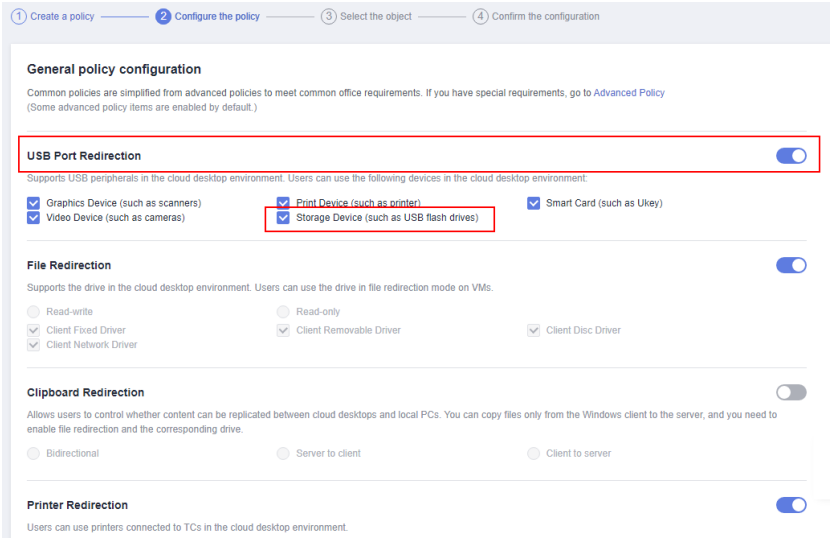
Figure 1-35 Creating a policy



g. Select **Storage Device (such as USB flash drives)** in **USB Port Redirection**, as shown in **Figure 1-36**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-36 Configuring the policy

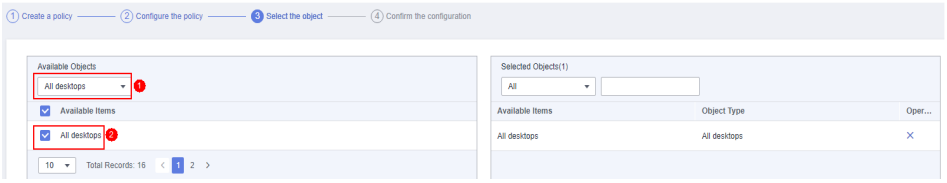


h. Click **Next: Select objects**.

i. Select an object as required.

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

Figure 1-37 Selecting an object



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 the administrator.

b. Click in the upper left corner and select the desired region and project.

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

The **Dashboard** page is displayed.

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

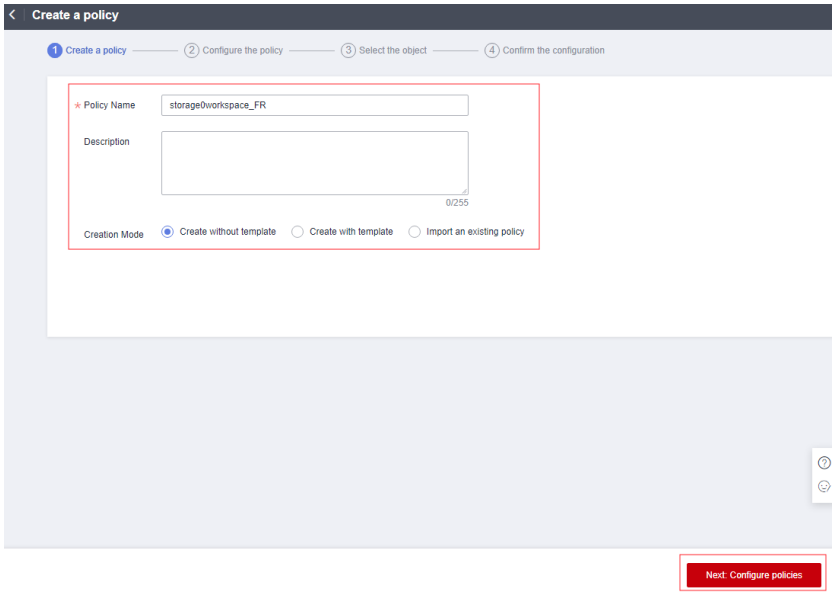
e. Click **Create a policy** in the upper right corner.

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

- The policy name must contain digits, letters, and underscores (_), and cannot contain more than 55 characters, for example, **storage0workspace_FR**.

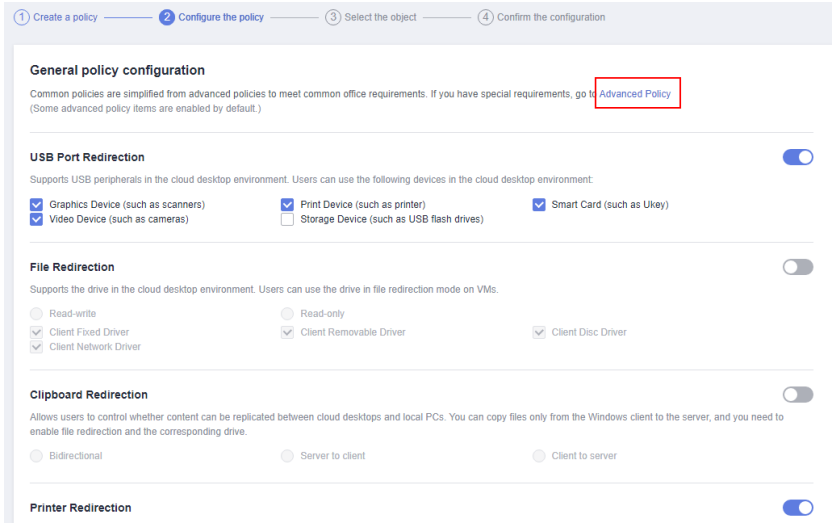
- The policy description contains a maximum of 255 characters, for example, **File redirection for copying files between external devices and desktops**.
- Retain the default creation mode.

Figure 1-38 Creating a policy



g. Click **Advanced Policy**.

Figure 1-39 Advanced policy entry



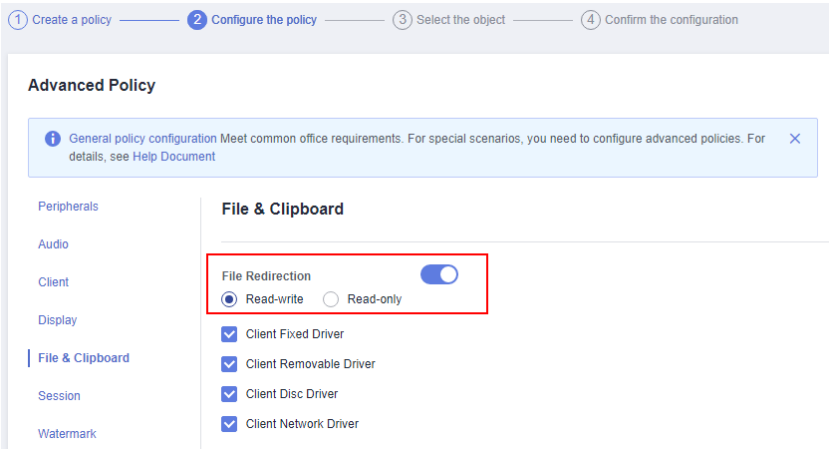
h. On the **Advanced Policy** page, click **File & Clipboard**.

i. Enable the **File Redirection** policy and set it to **Read-write**, as shown in **Figure 1-40**.

NOTE

You do not need to configure other advanced policy parameters under **File & Clipboard**. If you have strict requirements on the traffic and file size, configure them by referring to the parameter description in **Configuring Advanced Policy Parameters**. If you use a Linux terminal, expand **Advanced Policy** and ensure that **Linux Root Directory Mount Switch** is set to . If you use an Android terminal, expand **Advanced Policy** and ensure that **Mobile Client Redirection** is set to .

Figure 1-40 Configuring the policy

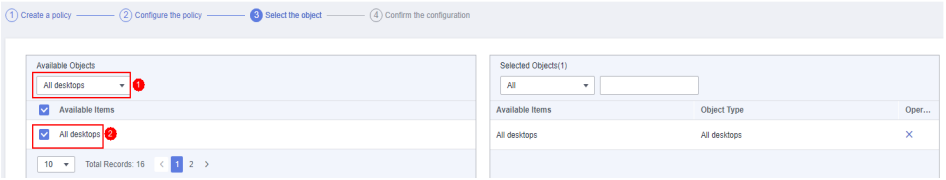


j. Click **Next: Select objects**.

k. Select an object as required.

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

Figure 1-41 Selecting an object



l. Click **Next: Finish**.

- **Clipboard redirection**

  Clipboard redirection supports file copy between storage devices and desktops.

  a. Log in to the console as the administrator.

  b. Click in the upper left corner and select the desired region and project.

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

  The **Dashboard** page is displayed.

 Copyright © Huawei Technologies Co., Ltd.

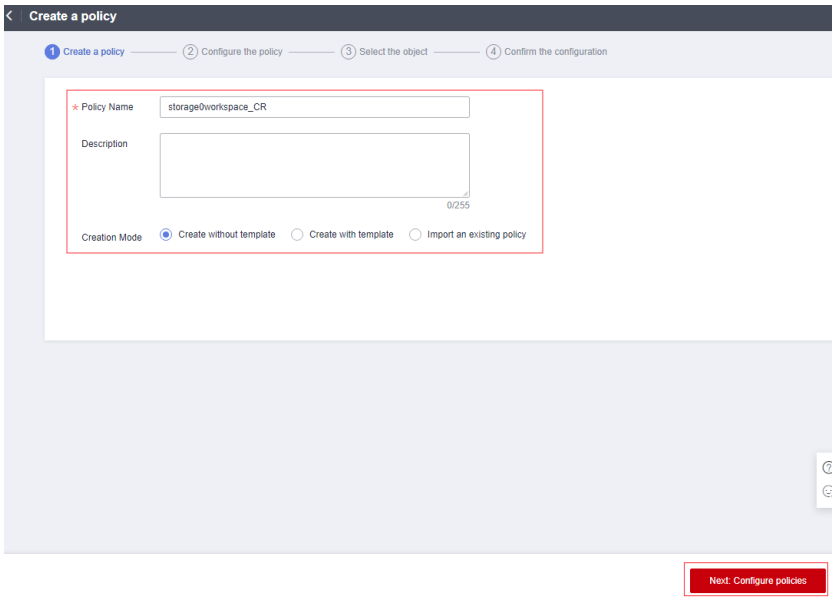
d. In the navigation tree on the left, choose **Policies** > **Protocol**.

e. Click **Create a policy** in the upper right corner.

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

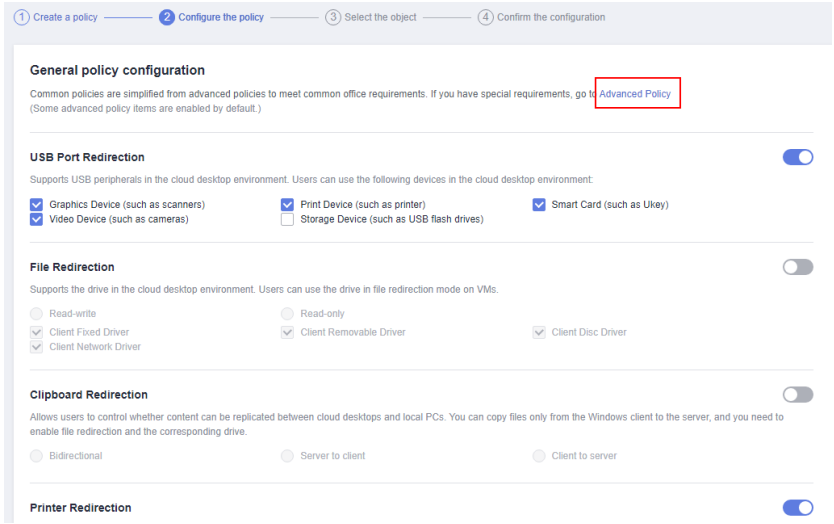
- The policy name must contain digits, letters, and underscores (_), and cannot contain more than 55 characters, for example, **storage0workspace_CR**.
- The policy description contains a maximum of 255 characters, for example, **Clipboard redirection is used to copy files between external devices and desktops**.
- Retain the default creation mode.

Figure 1-42 Creating a policy



g. Click **Advanced Policy**.

Figure 1-43 Advanced policy entry



 Copyright © Huawei Technologies Co., Ltd.

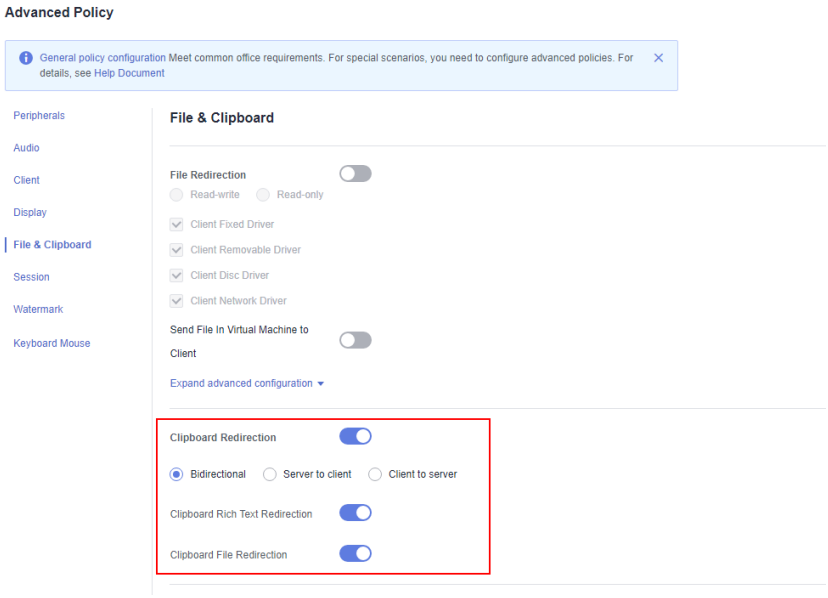
h. On the **Advanced Policy** page, click **File & Clipboard**.

i. Enable the **Clipboard Redirection** policy and select **Bidirectional**, as shown in **Figure 1-44**.

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 1-44 Configuring the policy

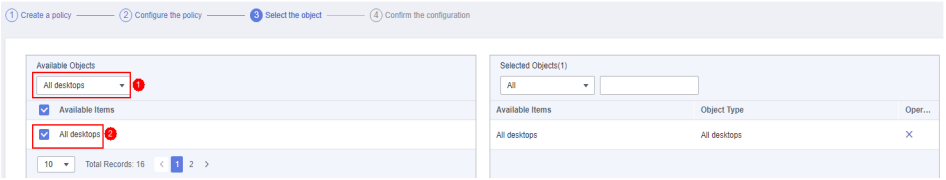


j. Click **Next: Select objects**.

k. Select an object as required.

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

Figure 1-45 Selecting an object



l. Click **Next: Finish**.

1.22 What If I Lost the Administrator Password?

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

1.23 How Does an Administrator Unlock an End User Account?

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

NOTE

If an enterprise has an AD domain, you need to unlock the AD domain on the AD server.

Procedure

Step 1 Log in to the console.

Step 2 Click **User Management**.

The **User Management** page is displayed.

Step 3 Select the user to be unlocked and choose **More** > **Unlock a User**.

The dialog box of unlocking a user is displayed.

Step 4 Click **OK**.

----End

1.24 How Do I Do If an End User Fails to Log In to a Desktop?

Scenario

If an end user fails to log in to a desktop, contact the administrator. The administrator can perform the following steps to rectify the fault.

Procedure

Step 1 Check whether the desktop is running properly.

1. Open the **Huawei Cloud website**. Log in to the management console as an administrator.
2. Click  in the upper left corner of the console and select a region and a project.
3. Click . In the service list, choose **Enterprise Application** > **Workspace** > **Desktop Management**.
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.

 Copyright © Huawei Technologies Co., Ltd.

- 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 to obtain 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 to obtain technical support.
- If the network is abnormal, rectify the network fault and log in to the desktop again. If the login fails, submit a service ticket to obtain technical support.

----End

1.25 How Do I Back Up and Restore a Desktop?

CBR backs up data of Workspace desktops, and restores backup data to desktops.

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 problems, see **Backup** and **Restoration**.

1.26 How Do I Do If a Message Is Displayed Indicating Duplicate Policy Names During Policy Import?

Scenario

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 1-46**.

Figure 1-46 Changing the policy name

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

 Copyright © Huawei Technologies Co., Ltd.

Step 4 Save and close the file.

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

----End

1.27 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

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

Scenario

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

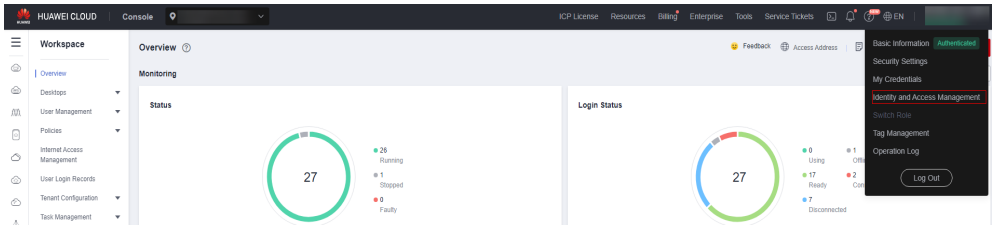
- Method 1: Contact the Huawei Cloud account for agency authorization. The agency authorization needs to be performed only once. Therefore, if the Huawei Cloud account has been authorized, the IAM user does not need to enable the agency.

 Copyright © Huawei Technologies Co., Ltd.

- 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.

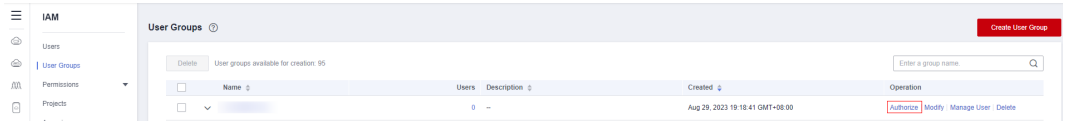
Step 1 Access the IAM page, as shown in **Figure 1-47**.

Figure 1-47 IAM entry



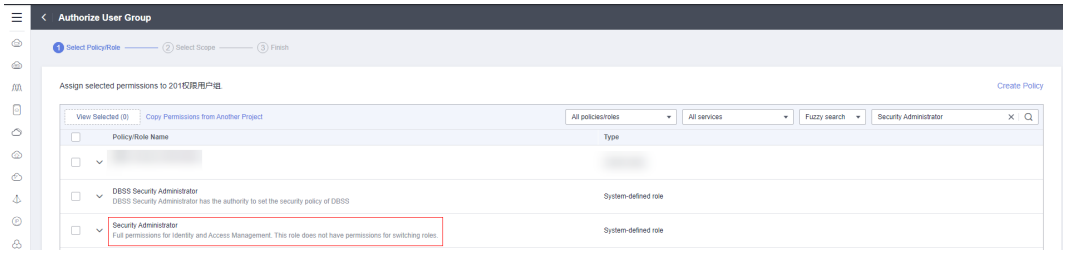
Step 2 Go to the user group page, select a user group to which the user belongs, and click **Authorize**, as shown in **Figure 1-48**.

Figure 1-48 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 1-49**.

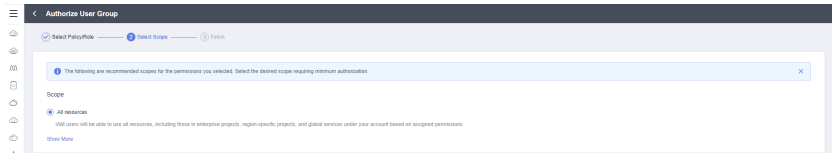
Figure 1-49 Authorization



Step 4 Select a region.

Retain the default **All resources** and click **OK**, as shown in **Figure 1-50**.

Figure 1-50 Authorization



----End

 Copyright © Huawei Technologies Co., Ltd.

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

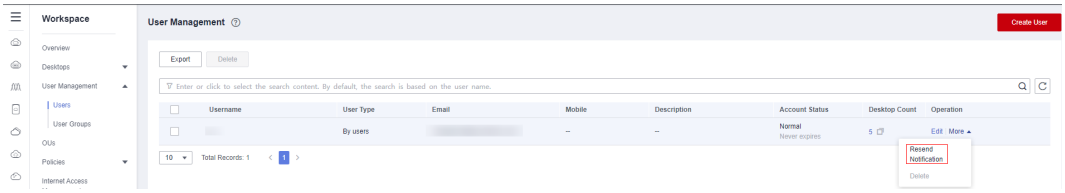
Step 1 Log in to the console.

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

The **User Management** page is displayed.

Step 3 Select the target user and choose **More** > **Resend Notification**, as shown in **Figure 1-51**.

Figure 1-51 User Management



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

----End

1.30 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**.

1.31 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.

1.32 How Do I Enable IPv6 on Workspace?

Scenario

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 .

Creating a subnet

Step 6 On the **Subnets** page, click **Create Subnet**. For details, see **Creating a Subnet for the 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 on which IPv6 is enabled will support IPv6.

----End

1.33 How Do I Enable RDP on Workspace?

Enabling remote connections to a desktop

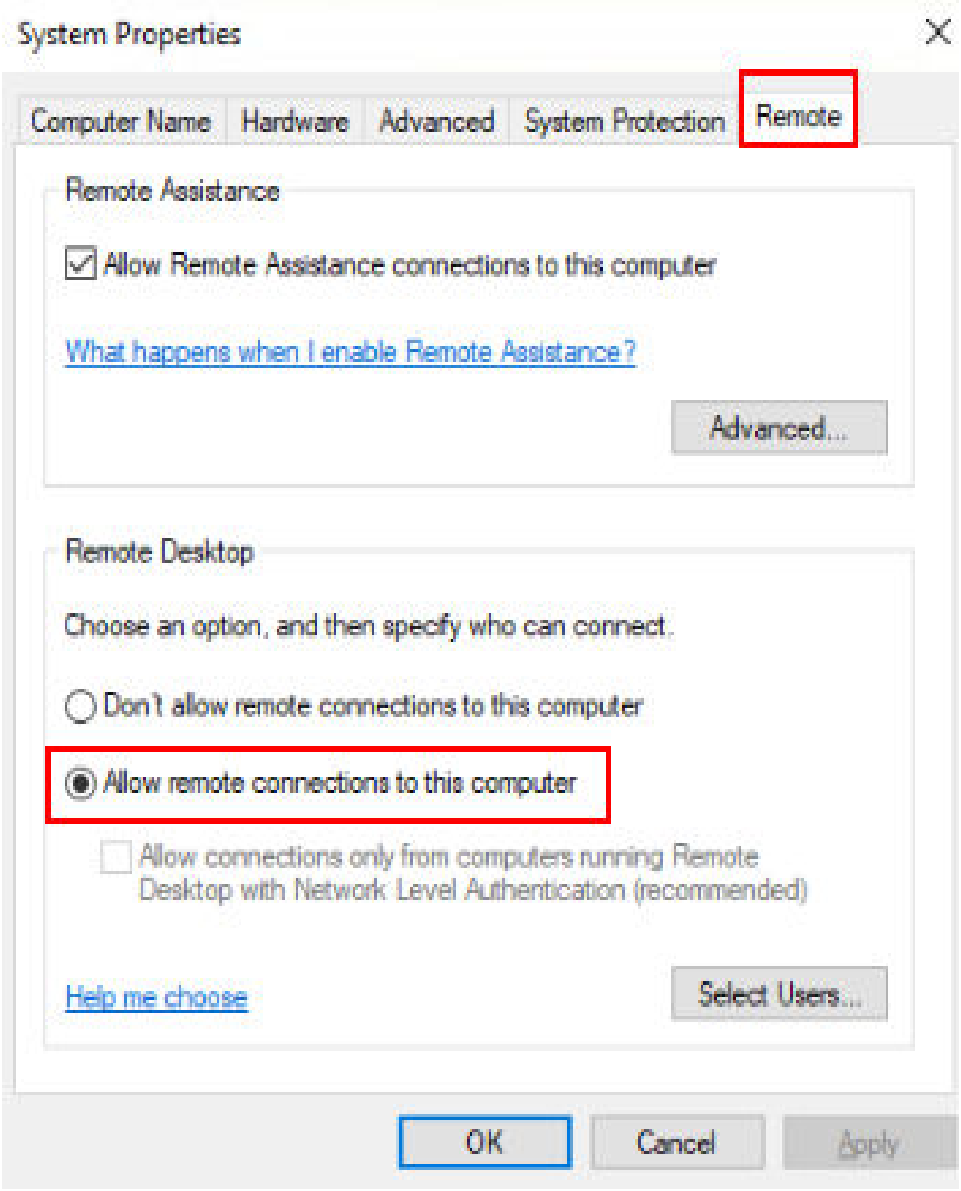
Step 1 Log in to the cloud desktop using the client.

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 1-52**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-52 System properties



Step 4 Click **OK**.

Enabling Internet access for the desktop

Step 5 Refer to .

Binding port 3389 to the desktop

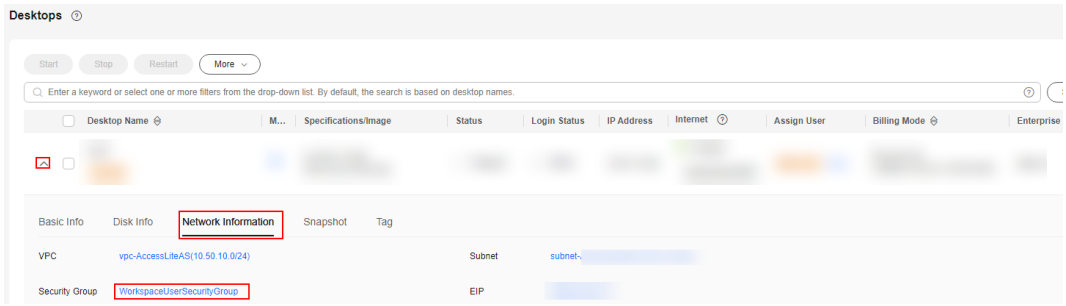
Step 6 **Log in to the console**.

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 1-53**.

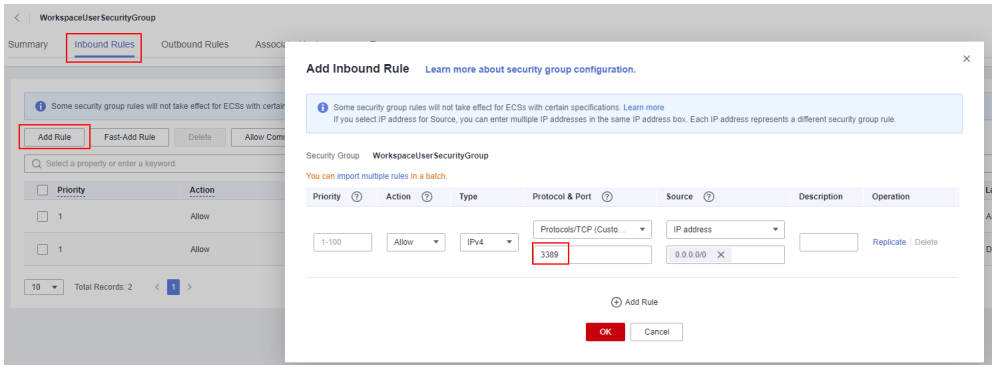
 Copyright © Huawei Technologies Co., Ltd.

Figure 1-53 Security groups



Step 9 In the inbound rule configuration area, enter **3389** in the **Protocol & Port** column, as shown in **Figure 1-54**.

Figure 1-54 Adding port 3389



----End

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

Scenario

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

AD connected

NOTE

- At least the IP addresses whose destination addresses are AD/DNS and ports of AD/DNS must be allowed in the outbound rules of the security group. Check details about the port list in .
- If Workspace needs to access other service systems, configure security group rules as needed.

Direct Connect access

 Copyright © Huawei Technologies Co., Ltd.

Step 1 **Log in to the Workspace 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 1-2** exist under the **Inbound Rules** tab.

Table 1-2 Ports

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

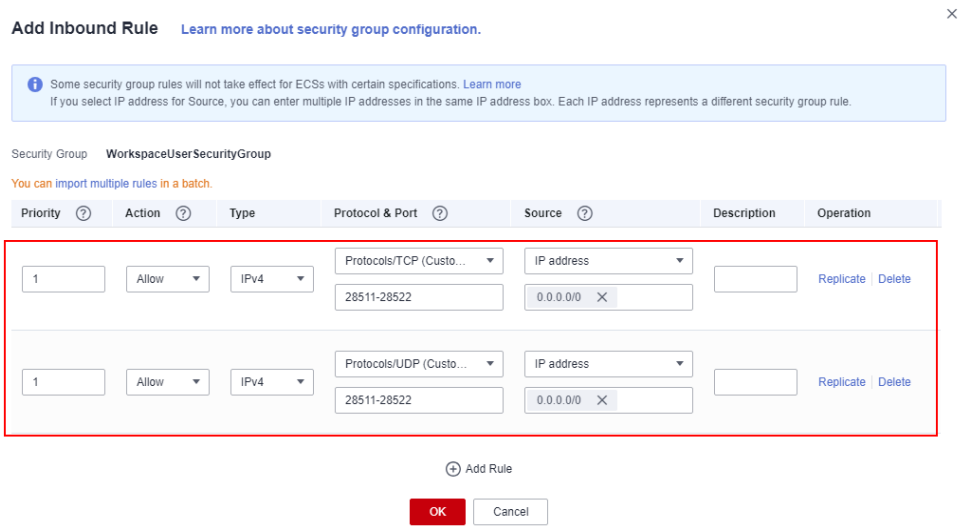
- If yes, the security group has allowed the inbound rules required for desktop access. You do not need to add the rules again.
- If no, perform **Step 9** to **Step 11**.

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.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-55 Adding an inbound rule



Step 11 Click **OK**.

----End

2 FAQs for End Users

2.1 Desktop Usage Issues
2.2 Login Issues
2.3 Terminal Binding Problems
2.4 OS Issues

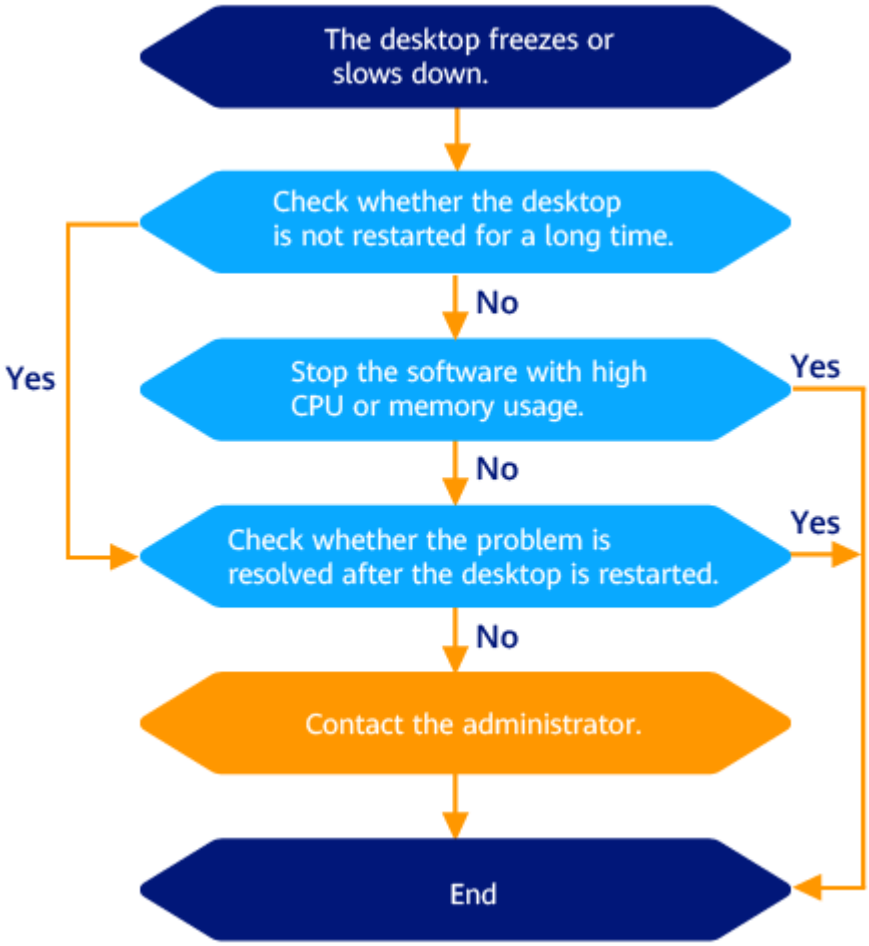
2.1 Desktop Usage Issues

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.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-1 Troubleshooting process



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.

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

2.1.4 How Do I Do If My Desktop Cannot Connect to the Internet?

Step 1 Disable the proxy.

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**.

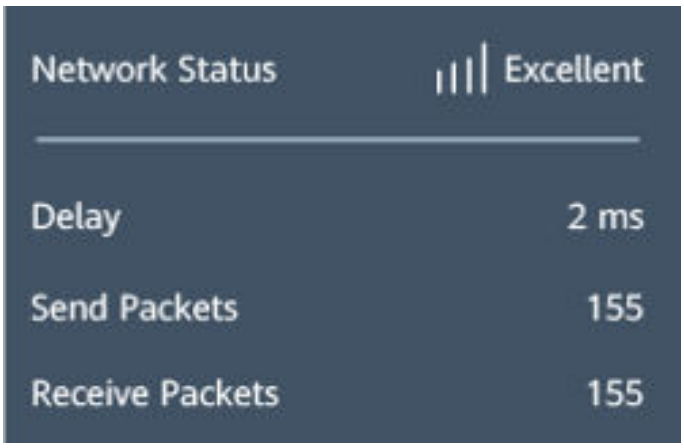
   Figure 2-2 Floating window

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

   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.

 Copyright © Huawei Technologies Co., Ltd.

- If the value is greater than 200 ms, the network speed is extremely low, and the network is frequently disconnected or cannot be accessed.

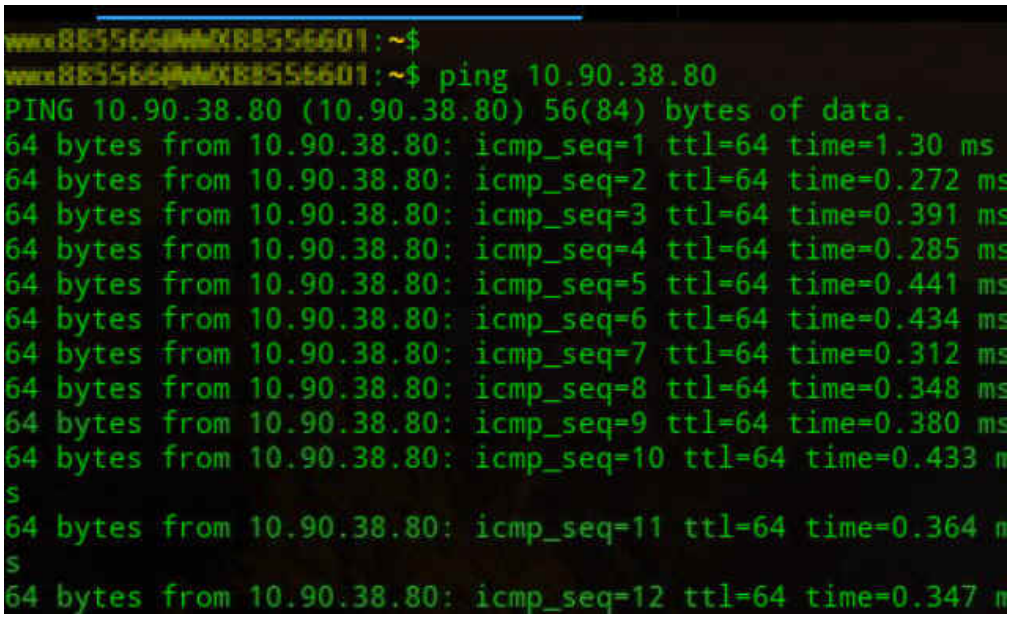
4. In any blank area on the desktop, enter the CLI mode.
5. Run the following command to check the network status:

   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:



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?

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

 Copyright © Huawei Technologies Co., Ltd.

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 How Do I Do If the Printer Cannot Be Used?

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 **1.6 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 **1.6 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.

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 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.

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.

 Copyright © Huawei Technologies Co., Ltd.

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 **2.1.11 What Do I Do If I Cannot Copy Files Between a Desktop and a Local Storage Device?**.

Step 5 Check whether the local printer can be used.

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 can be used. 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 Workspace?

Step 1 Contact the administrator to check whether the **Printer Redirection** policy has been configured for the user desktop by referring to **1.7 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 **1.7 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 available.

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**.

 Copyright © Huawei Technologies Co., Ltd.

- If no, go to **Step 4**.

Step 4 Add a printer.

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 device, 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 **2.1.11 What Do I Do If I Cannot Copy Files Between a Desktop and a Local Storage Device?**.

Step 5 Check whether the target printer is available.

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 the 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.

 Copyright © Huawei Technologies Co., Ltd.

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.

 Copyright © Huawei Technologies Co., Ltd.

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

----End

2.1.11 What Do I Do If I Cannot 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 **1.21 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 based on the OS type of the terminal and desktop. For 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 desktop client. 4. Open the text editing page and paste the copied content in the terminal device. For example, **You can copy text from desktops to external devices**.

 Copyright © Huawei Technologies Co., Ltd.

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 desktop client. 3. Select the content based on the OS type of the terminal and desktop. For 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 in the desktop. For 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 based on the OS type of the terminal and desktop. For 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 desktop client. 4. Open the text editing page and paste the copied content in the terminal device. For example, **You can copy text from desktops to external devices**.

 Copyright © Huawei Technologies Co., Ltd.

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 desktop client. 3. Select the content based on the OS type of the terminal and desktop. For 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 in the desktop. For 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 desktop 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.

 Copyright © Huawei Technologies Co., Ltd.

Enabled Policy	Data Flow	User Guide
Enable the **File Redirection** policy and set it to **Read-only**.	Desktop ← Terminal	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	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.

 Copyright © Huawei Technologies Co., Ltd.

Enabled Policy	Data Flow	User Guide
	Desktop ← Terminal	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	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.

 Copyright © Huawei Technologies Co., Ltd.

Enabled Policy	Data Flow	User Guide
	Desktop ← Terminal	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.

 Copyright © Huawei Technologies Co., Ltd.

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

2.2 Login Issues

2.2.1 How Do I Do 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.

 Copyright © Huawei Technologies Co., Ltd.

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 What Devices Can Be Used to Log In to a Desktop?

You can **use a TC**, **an SC**, or **a mobile terminal** to log in to a desktop.

2.2.4 What If I Fail to Log in to a Desktop?

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.

 Copyright © Huawei Technologies Co., Ltd.

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.

2.2.5 How Do I Do If I Cannot 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.

 Copyright © Huawei Technologies Co., Ltd.

- 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.)

Account Locked

Possible causes

If you enter incorrect verification codes for five consecutive times, the account will be locked.

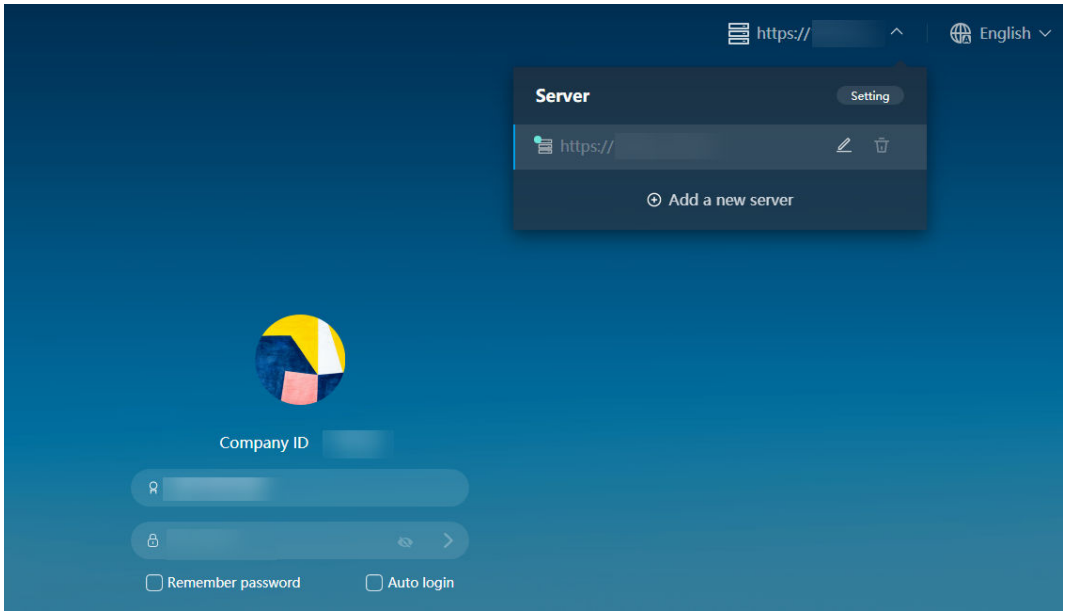
Solution

Contact the administrator to unlock the account and enter the correct verification code.

2.2.6 How Do I Do If the System Displays a Message Indicating that the Login Fails Due to Policy Restrictions?

Step 1 Click the server address 

in the upper right corner on 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.

 Copyright © Huawei Technologies Co., Ltd.

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

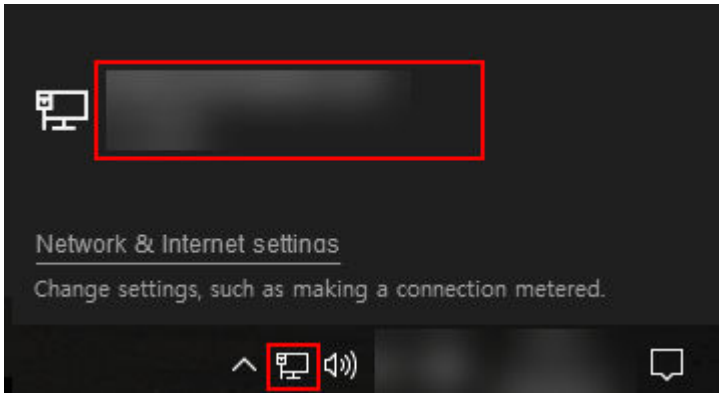
Workspace supports login from multiple types of TCs. The operations vary depending on the TC model. The following is only an example.

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.



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

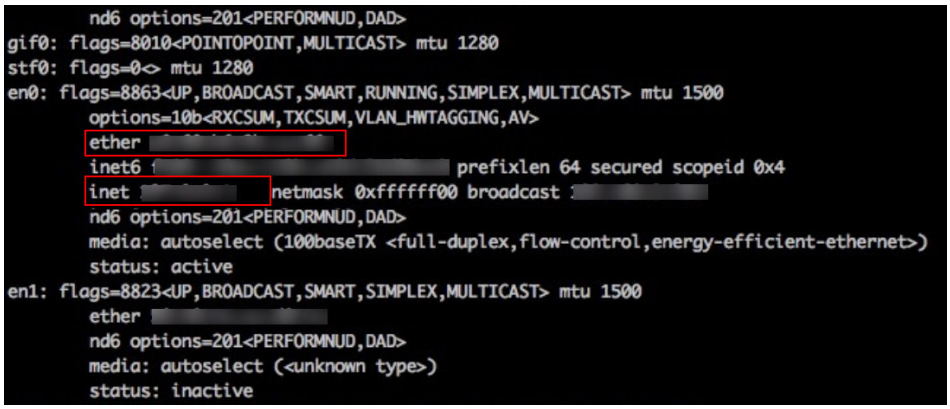


d. Record the MAC address.

- **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



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 What OSs Can Run on Workspace?

Workspace supports the following OSs. More OSs will be supported in the future.

- Windows Server 2016
- Windows Server 2019 LTSC

2.4.3 Which Software Cannot Be Uninstalled?

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**.

 Copyright © Huawei Technologies Co., Ltd.

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

2.4.7 Which Commands Cannot Be Executed?

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?

Procedure

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.

 Copyright © Huawei Technologies Co., Ltd.

A Change History

Release Date	Description
2023-11-09	This issue is the first official release.

 Copyright © Huawei Technologies Co., Ltd.