06 Workspace User Guide (for Administrators)

Issue	01
Date	2026-01-23

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

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

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

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

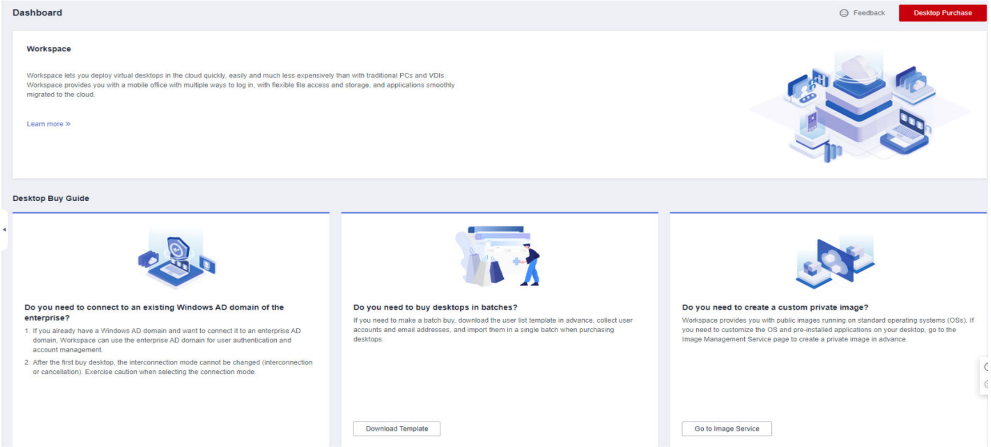
Contents

1 Overview

Service Not Enabled

If you have not purchased a desktop, you can learn about Workspace and *Desktop Purchase Guide* on the **Overview** page, as shown in **Figure 1-1**.

Figure 1-1 Overview



Dashboard

Workspace

Workspace lets you deploy virtual desktops in the cloud quickly, easily and much less expensively than with traditional PCs and VDIs. Workspace provides you with a mobile office with multiple ways to log in, with flexible file access and storage, and applications smoothly migrated to the cloud.

Learn more »

Desktop Buy Guide

Do you need to connect to an existing Windows AD domain of the enterprise?

1. If you already have a Windows AD domain and want to connect it to an enterprise AD domain, Workspace can use the enterprise AD domain for user authentication and account management.
2. After the first buy desktop, the interconnection mode cannot be changed (interconnection or cancellation). Exercise caution when selecting the connection mode.

Do you need to buy desktops in batches?

If you need to make a batch buy, download the user list template in advance, collect user accounts and email addresses, and import them in a single batch when purchasing desktops.

Do you need to create a custom private image?

Workspace provides you with public images running on standard operating systems (OSs). If you need to customize the OS and pre-installed applications on your desktop, go to the Image Management Service page to create a private image in advance.

Service Enabled

After purchasing a desktop, you can check the data trends, alarm notifications, and desktop monitoring information on the **Overview** page.

- In the **Data trends** area, you can view the desktop usage, desktop usage trend, and user usage. For details, see **Figure 1-2** and **Table 1-1**.

Figure 1-2 Data trends

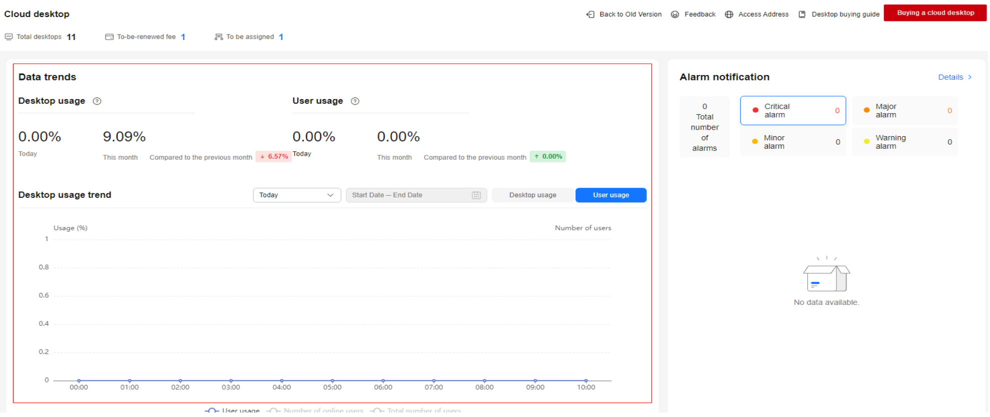
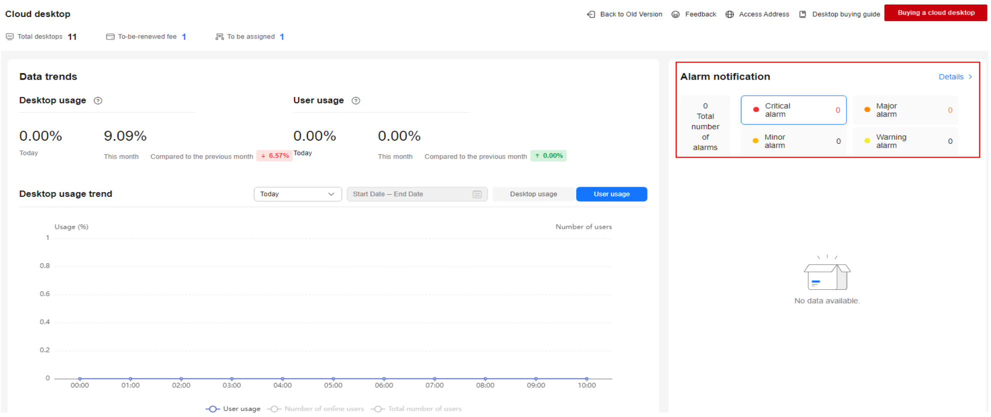


Table 1-1 Status description

Status Type	Description
Desktop Usage	Displays the cloud desktop usage, number of used desktops, and total number of desktops in a specific period. You can check the statistics of today, last 7 days, last 30 days, or a customized period. **NOTE** ● Today: number of used desktops/total number of desktops ● Last 30 days: The daily usage is averaged by month. ● Number of used desktops: including desktops that are in use and desktops that have been used in the specified period ● Number of used desktops: If you query the number of used desktops by hour, the data may be delayed for 0 to 15 minutes. That is, the actual number is the number in the hour before 0 to 15 minutes. If you query by day, the data may be delayed for 0 to 1 hour. That is, the actual number is the number in the day before 0 to 1 hour.
User Usage	Displays the user usage, number of online users, and total number of users in a specific period. You can check the statistics of today, last 7 days, last 30 days, or a customized period. **NOTE** ● Today: number of online users/total number of users ● Last 30 days: The daily usage is averaged by month. ● Number of online users: including users who are using desktops and users who have used desktops in a specified period ● The data is not real-time. If you query the number of online users by hour, the data may be delayed for 0 to 10 minutes. That is, the actual number is the number in the hour before 0 to 10 minutes. If you query by day, the data may be delayed for 0 to 1 hour. That is, the actual number is the number in the day before 0 to 1 hour.

- In the **Alarm notification** area, you can view the total number of alarms and alarm severity of cloud desktops, as shown in **Figure 1-3**. To view the alarm details, you can click **Details** to go to the Cloud Eye console.

Figure 1-3 Alarm notifications



- In the **Desktop Monitoring** area, you can check the running status or login status statistics by desktop or desktop pool, as shown in **Figure 1-4**. For details, see **Table 1-2**.

Figure 1-4 Desktop monitoring

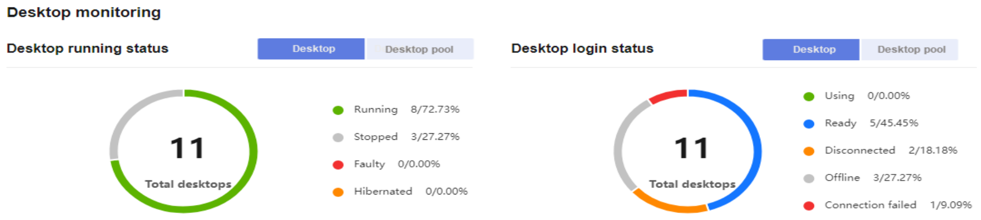


Table 1-2 Status description

Status Type	Status	Description
Cloud desktop running status	Running	The desktop is working properly.
	Stopped	The desktop has been stopped.
	Hibernated	The desktop has been hibernated.
	Faulty	The desktop is faulty.
Cloud desktop connection status	Connected	The desktop is in use.
	Unconnected	The desktop is not in use.

Status Type	Status	Description
	Connection failed	The desktop cannot be connected to temporarily due to abnormal registration status.

- In the **Desktop latency distribution** area, you can view the latency trend within a specified period, as shown in **Figure 1-5**. For details, see **Table 1-3**.

NOTE

1. The cloud desktop latency is the network latency of cloud desktop sessions.
2. Network latency: round-trip time (RTT) between a device and the access gateway. The data of this parameter can be viewed only on the client of 23.12.1.0 or later.
3. You can view the network latency data of any day in the last 30 days.

Figure 1-5 Desktop latency trend

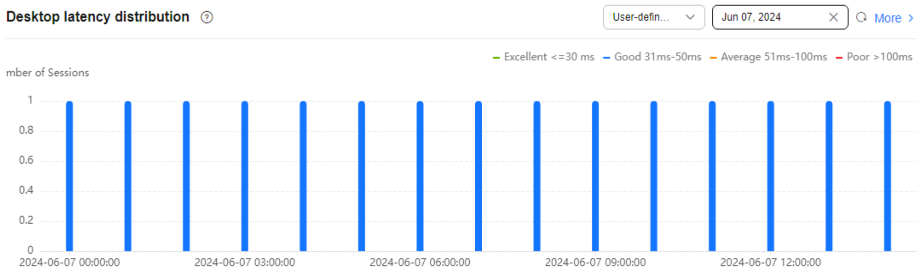


Table 1-3 Latency levels

Level	Latency
Excellent	< 30 ms
Good	31–50 ms
Average	51–100 ms
Poor	> 100 ms

2 Desktops

2.1 Cloud Desktop Statuses

The following status fields are returned by the Workspace API for querying desktop details:

- **status**: power supply status of a desktop
- **task_status**: task status of a desktop, that is, the intermediate status of a desktop when the desktop is processing an operation
- **login_status**: connection status of a desktop

You can view only the following two statuses on the console:

- Running status: consists of **task_status** and **status**. If **task_status** is not empty, its status value is displayed. If **task_status** is empty, the status value of **status** is displayed.
- Connection status: consists of **login_status**. **Table 2-3** describes each status in detail and the status values displayed on the console.

Table 2-1 status list

status	Description
ACTIVE	Running
SHUTOFF	Stopped
HIBERNATED	Hibernated
ERROR	Faulty
STARTING	Starting
STOPPING	Stopping
RESTARTING	Restarting
HIBERNATING	Hibernating
AWAKENING	Waking up

Table 2-2 task_status list

task_status	Description
CreatedSuccess	Created
creating	Creating
Deleting	Deleting
updating	Rebuilding
attaching	Assigning a desktop to a user
DesktopDetaching	Unbinding a user
desktopNetworkChanging	Changing the network
userPrivilegeGroupChanging	Changing the user permission group
migrating	Cold migrating
updatingSids	Updating the SID
rejoiningDomain	Rejoining the domain
restoring	Restoring a desktop
addingVolumes	Adding a disk
deletingVolumes	Deleting a disk
expandingVolumes	Expanding disk capacity
desktopToImage	Creating an image
acrossAzDesktopMigrating	Migrating across AZs

task_status	Description
desktopResizing	Changing specifications
creatingWksSnapshot	Creating a snapshot
restoringWksSnapshot	Restoring a snapshot

Table 2-3 login_status list

login_status	Description	Connection Status Displayed on the Console (New Version)	Connection Status Displayed on the Console (Old Version)
CONNECTED	The user is connecting to a desktop.	Connected	In use
DISCONNECTED	The user has disconnected from a desktop after using it.	Unconnected	Disconnected
REGISTERED	The desktop is ready after being started.		Ready
OFFLINE	The desktop is offline because it is stopped or hibernated.		Offline
UNREGISTER	The desktop cannot be connected to temporarily due to abnormal registration status. If there is an ongoing task, wait until the task is completed and then check the status. If the connection cannot be established for a long time, you can remotely log in to check the issue or restart the desktop.	Connection failed	Connection failed

2.2 Managing Desktops

Scenarios

The administrator can start, stop, restart, and delete desktops, and change desktop names. If a user does not need to use a desktop anymore, the administrator can assign the desktop to another user.

Prerequisites

You have **created** a desktop.

Procedure

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

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

The **Desktops** page is displayed.

Step 3 Perform the operations in **Table 2-4** as required. Some of the following operations can be performed on one desktop or multiple desktops.

- **On one desktop**: In the **Operation** column on the right of the desired desktop, click **Start**, **Stop**, or **More** > **Power Supply** > **Restart**.
- **On multiple desktops**: Select the desired desktops and choose operations above the desktop list, such as **Start**, **Stop**, or **More** > **Power Supply** > **Restart**.

Table 2-4 Operations

Operation Category	Operation	Procedure	Batch Operation
Desktop information	Viewing desktop information	– Select search criteria to view desktop information: 1. In the search box above the desktop list, select search criteria or enter a keyword for search. 2. Search criteria include desktop ID, desktop name, billing mode, running status, connection status, AZ, subnet, IP address, desktop user, assignment status, image ID, maintenance mode, collaboration status, enterprise project, and resource tag. – View desktop information by filtering columns: 1. In the upper right corner of the desktop list, click ⚙ to go to the settings page. 2. In the basic settings area, determine whether to enable **Auto wrapping** and **Fixed position**. 3. On the settings page, view desktop information by desktop name, monitoring metric, specifications/image, running status, connection status, AZ, and IP address. 4. Click **OK**.	Not supported
	Changing a desktop name	1. Click ✎ next to the desired desktop name. 2. Enter the new name and click **OK**. **NOTE** ■ Only uppercase letters, lowercase letters, digits, and hyphens (-) are allowed. ■ Must start with a letter or digit and cannot end with a hyphen (-). ■ 1 to 15 characters are allowed (each digit or letter represents 1 character). ■ Changing the desktop name will restart the desktop.	Not supported

Operation Category	Operation	Procedure	Batch Operation
	Exporting desktop information	1. Click **Export** above the desktop list. 2. In the displayed dialog box, click **Go to Export Center** or **Download** to download the exported desktop information file.	Supported
	Viewing monitoring metrics	1. Click 🖥 in the **Monitoring** column of a desktop to go to the monitoring metric details page of the desktop. 2. You can view the following desktop metrics in the last one hour, last 24 hours, last seven days, last 30 days, or a custom time period. ▪ **User Online Status**: online/offline user count ▪ **CPU Usage (%)**: CPU usage of the desktop ▪ **Memory Usage (%)**: memory usage of the desktop ▪ **Disk I/O Read/Write Speed** (KB/s): speed at which data is read from or written to the desktop disks in a period of time ▪ **Disk Read/Write Speed** (Requests/s): speed at which data is read from or written to the desktop disks and transferred to other devices ▪ **Inbound/Outbound Traffic Rate** (KB/s): rate at which data flows into or out of the desktop in a period of time	Not supported
Power supply operation	Starting a desktop	1. Click **Start** to go to the **Start Desktop** page. 2. If you want to perform this operation, enter **YES** or click **Auto Enter**. 3. Click **OK**.	Supported

Operation Category	Operation	Procedure	Batch Operation
	Stopping a desktop	1. Click **Stop** to go to the **Stop Desktop** page. 2. The execution mode is **Stop** by default. **NOTE** You can determine whether to force stop the desktop. 3. If you want to perform this operation, enter **YES** or click **Auto Enter**. 4. Click **OK**.	Supported
	Restarting a desktop	1. Click **More** > **Power Supply** > **Restart** to go to the **Restart Desktop** page. 2. The execution mode is **Restart** by default. **NOTE** You can determine whether to force restart the desktop. 3. If you want to perform this operation, enter **YES** or click **Auto Enter**. 4. Click **OK**.	Supported
	Hibernating a desktop	1. Click **More** > **Power Supply** > **Hibernate** to go to the **Hibernate Desktop** page. 2. If you want to perform this operation, enter **YES** or click **Auto Enter**. 3. Click **OK**. **NOTE** Currently, only Windows desktops can be hibernated.	Supported
O&M operation	Logging in remotely	1. Click **More** > **O&M** > **Remote Login**. 2. In the displayed dialog box, click **OK** to go to the remote login page. 3. Click **Send CtrlAltDel** in the upper right corner and enter the username and password to remotely log in to the desktop. **NOTE** Before using this function on a new desktop for the first time, ensure that the desktop has been logged in to from the client.	Not supported

Operation Category	Operation	Procedure	Batch Operation
	Rejoining a domain	1. Click **More** > **O&M** > **Rejoin Domain** to go to the **Rejoin Domain** page. 2. Click **OK**. **NOTE** ■ This operation can be performed only on desktops that are running. ■ This operation can be performed only on Windows desktops. ■ This operation can be performed only in the AD scenario.	Not supported
	Updating the Security Identifier (SID)	1. Click **More** > **O&M** > **Update SID** to go to the **Update SID** page. 2. Click **OK**. **NOTE** This operation can be performed only in the AD scenario.	Supported
	Enabling the maintenance mode	1. Click **More** > **O&M** > **Enable Maintenance Mode** to go to the **Enable Maintenance Mode** page. 2. If you want to perform this operation, enter **YES** or click **Auto Enter**. 3. Click **OK**. **NOTE** ■ In the maintenance mode, all operations, such as user access, self-service maintenance, startup, shutdown, and restart, are not allowed. ■ Desktops that are being connected to and have been connected to will not be affected.	Supported
	Disabling the maintenance mode	1. Click **More** > **O&M** > **Disable Maintenance Mode** to go to the **Disable Maintenance Mode** page. 2. If you want to perform this operation, enter **YES** or click **Auto Enter**. 3. Click **OK**. **NOTE** This operation can be performed only on desktops in the maintenance mode.	Supported

Operation Category	Operation	Procedure	Batch Operation
	Executing commands	1. Click **More** > **O&M** > **Execute Command** to go to the **Execute Command** page. 2. Click **Enter Command** to configure the execution. a. **Execution Environment**: Select **Windows Script**, **Windows PowerShell**, or **Linux Shell**. b. Set the command execution timeout interval. The value ranges from 1 to 600 minutes. c. Enter the commands. 1. If you want to perform this operation, enter **YES** or click **Auto Enter**. 2. Confirm the execution. **NOTE** ▪ When executing commands in batches, you cannot select desktops running Windows and Linux at the same time. ▪ This operation can be performed only on desktops that are running.	Supported
	Executing a script	1. Click **More** > **O&M** > **Execute Script** to go to the **Execute Script** page. 2. For details, see "Executing a script" in **12.1 Script Management**.	Supported
	Viewing script records	1. Click **More** > **O&M** > **Script Record**. 2. On the **Desktop Script Records** tab page, view the script records.	Not supported
	Sending a notification	1. Click **More** > **O&M** > **Send Notification** to go to the **Send Notification** page. 2. Enter the notification message. 3. Confirm the notification sending. **NOTE** ▪ This operation can be performed only on desktops that are running. ▪ This operation can be performed only on Windows desktops.	Supported

Operation Category	Operation	Procedure	Batch Operation
User management	Changing user permissions	1. Click **More** > **Users** > **Change User Permission** to go to the **Change User Permission** page. 2. Select a permission group as required: a. **Administrator permission group**: Users in this group have system administrator permissions, that is, full permissions on a computer. They can perform all management tasks, including managing all users, on the computer. b. **User permission group**: Users in this group have basic operation permissions on a computer, for example, running applications, but cannot modify the OS settings or data of other users. 3. Click **OK**. **NOTE** After changing the user permission, you need to restart or log out of the desktop for the change to take effect.	Supported
	Unbinding a user	For details, see **2.3.3 Unbinding Users**.	Supported
	Assigning a desktop to a user	For details, see **2.3.2 Assigning Desktops**.	Supported
	Enabling collaboration	For details, see **2.3.1.2 Enabling Collaboration**.	Supported
	Disabling collaboration	For details, see **2.3.1.3 Disabling Collaboration**.	Supported

----End

2.3 Users

2.3.1 Collaborative Desktops

2.3.1.1 Overview

Collaborative desktops of Workspace are ideal for remote desktop sharing between end users. This feature is applicable to collaborative office scenarios, such as content co-creation and real-time material sharing. Faster data sharing translates into higher work efficiency. Collaborative desktops boast the following advantages:

- One-click sharing: You can quickly share a cloud desktop via a link, allowing multiple users to access the same desktop simultaneously.
- Multi-user viewing: Multiple users can simultaneously view cloud desktop content and listen to audio.
- Voice meetings: You can initiate an instant voice meeting where all users accessing the cloud desktop can communicate seamlessly.
- Remote operation control: Users can remotely control the same cloud desktop using keyboards and mouse devices, with active control limited to one user at a time.

2.3.1.2 Enabling Collaboration

Scenarios

After collaboration is enabled, you can quickly initiate collaboration between desktops to improve work efficiency.

Constraints

- To enable or disable collaboration, configure a whitelist by **creating a service ticket**.
- Only yearly/monthly Windows cloud desktops are supported.
- Supported servers: 23.8.1 or later.
- Supported clients: 23.8.1 or later.
- Collaboration is available only in full-screen mode.

Procedure

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

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

The **Desktops** page is displayed.

Step 3 Enable collaboration for desktops:

- To enable collaboration for one desktop, perform **Step 4** to **Step 5**.
- To enable collaboration for desktops in batches, perform **Step 6** to **Step 9**.

Step 4 Click **More** in the **Operation** column of the desired desktop and choose **Users** > **Enable Collaboration**.

Step 5 On the page displayed, select **Enable** for **Collaboration**, select **Specifications**, and click **OK**.

Step 6 Select multiple desktops for which collaboration is to be enabled. Click **More** in the upper left corner and choose **Users** > **Enable Collaboration**.

Step 7 On the page displayed, configure parameters.

- **Billing Mode**: **Yearly/Monthly**
- **Processor**:
  - **CPU**: 6-party collaborative resource-Standard edition
  - **GPU**: 6-party collaborative resource-Advanced edition
- **OS**: **Windows**

  NOTE

  Only desktops with the same billing mode, processor, and OS can change collaborative resources in batches.

Step 8 Click **OK**.

Step 9 On the page displayed, select **Enable** for **Collaboration**, select **Specifications**, and click **OK**.

Step 10 The page for purchasing collaboration is displayed.

Step 11 Check data in **Cloud Service Orders**.

Step 12 After you select a payment method and pay for your order, the purchase has been completed.

----End

2.3.1.3 Disabling Collaboration

Scenarios

Disable the collaboration function of Workspace.

Procedure

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

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

The **Desktops** page is displayed.

Step 3 You can disable collaboration for one desktop or multiple desktops in batches.

- To disable collaboration for one desktop, perform **Step 4** to **Step 5**.
- To disable collaboration for desktops in batches, perform **Step 6** to **Step 8**.

Step 4 Click **More** in the **Operation** column of the desired desktop and choose **Users** > **Disabling Collaboration**.

Step 5 Click **OK**.

Step 6 Select multiple desktops for which collaboration is to be disabled. Click **More** in the upper left corner and choose **Users** > **Disabling Collaboration**.

Step 7 Select a billing mode and click **OK**. The **Disable Collaboration** page is displayed.

Step 8 Click **OK**.

----End

2.3.2 Assigning Desktops

Scenarios

Assign an idle desktop to a user on the console.

Procedure

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

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

The **Desktops** page is displayed.

Step 3 Select a desktop whose status is unassigned.

- Assigning one desktop: Click **More** > **Users** > **Assign Desktop** in the **Operation** column. On the displayed page, perform **Step 4** to **Step 10**.
- Batch assigning desktops: Select the desktops to be assigned in batches and choose **More** > **Users** > **Assign Desktop**. The page for selecting desktops is displayed. Desktops that cannot be assigned will be automatically filtered out. Check desktops that can be assigned, and click **Next: Select User**. On the **Select User and Assignment Mode** page, perform **Step 11** to **Step 19**.

NOTE

Windows and Linux desktops cannot be selected at the same time.

Assigning one desktop to a user

Step 4 On the page displayed, select **Select User** or **Create User** as required. See **Table 2-5**.

If an existing AD domain is used, you need to create a user on the AD server before assigning desktops.

- **Select User**: If a user has been created, you can select the created user for a single-user desktop or select a user or user group for a multi-user desktop, and filter the query result based on the user type, username, user group, and description.
- **Create User**: If no user has been created, you can select **Create User** and configure parameters as instructed in **Table 2-5**.

Table 2-5 Assigning a desktop to a user

User Authorization Mode	Parameter Description	Operation
Select User	You can search for activated users by setting filter criteria.	You can search for a user based on user type and username.
Create User > **By users** for **User Activation** and **Manually** for **User Import**	– The username is used for user authentication during desktop login. Naming rules: ■ A name can contain 1 to 32 characters. ■ A digit-only name is allowed. ■ A name can contain uppercase letters, lowercase letters, digits, periods (.), hyphens (-), and underscores (_), and must start with a lowercase letter or uppercase letter. ■ This field cannot be left blank. – The email address is used to receive desktop provisioning emails and related notifications. Email address verification rules: ■ Enter a valid email address through system verification. ■ The value can contain a maximum of 64 characters. – The mobile number is used to receive desktop provisioning emails and related notifications. Mobile number verification rules: ■ [+][*Country/Region code*][*Mobile number*] ■ For a mobile number of your country/region, you can omit [+][*Country/Region code*] and directly enter the mobile number. ■ A mobile number can contain spaces, slashes (/), and hyphens (-).	1. Configure **User Info**, **Description**, and **Account Expiration**. 2. Select the required enterprise project from the **Enterprise Project** drop-down list. 3. Select the desired domain name. 4. Click **Add User**. **NOTE** Enter an email address or a mobile number, or both.

User Authorization Mode	Parameter Description	Operation
Create User > **By administrators** for **User Activation** and **Manually** for **User Import**	– The username is used for user authentication during desktop login. Naming rules: ■ A name can contain 1 to 32 characters. ■ A digit-only name is allowed. ■ A name can contain uppercase letters, lowercase letters, digits, periods (.), hyphens (-), and underscores (_), and must start with a lowercase letter or uppercase letter. ■ This field cannot be left blank. – The initial password is used to authenticate the first login to a desktop. Keep the initial password secure. ■ The password contains 8 to 32 characters. ■ The value can contain uppercase letters, lowercase letters, digits, and special characters !@$%^-_=+[{}]:,./? ■ The password cannot be the username or the reverse username. **NOTE** If your tenant connects to an AD domain, **By administrators** is unavailable by default.	

User Authorization Mode	Parameter Description	Operation
Create User > **By administrators** for **User Activation** and **Batch** for **User Import**	Upload the user information recorded in the table and create users in batches.	1. Click **Download Template** on the right of **Import user information** to download the user list template. 2. Enter the No., username, password (only for **By administrators**), domain (AD domain where the user is located. If this parameter is not set, the primary domain is used by default), email, mobile number, expiration time, and description in the table. 3. Click **Upload** to upload the user list that has been filled in as required. 4. Click **OK**. **NOTE** The size of the file (only .xlsx and .xls are allowed) to be uploaded cannot exceed 1 MB. A maximum of 200 records can be uploaded at a time.
Create User > **By users** for **User Activation** and **Batch** for **User Import**	Upload the user information recorded in the table and create users in batches.	

Step 5 Click **Next**. The desktop configuration page is displayed.

NOTE

If the original image does not exist or has been deleted, select a public or private image. If there are resource changes, you will be charged the configuration fee and image fee.

Step 6 Select a naming rule from **Desktop Naming Rule**, or select **Do not use** to use the default naming rule.

To create a naming rule, click **Create Desktop Naming Rule**. After the creation is complete, click **OK**. For details, see **8.3.1 Desktop Naming Rules**.

Step 7 Select user permissions and set the desktop name. The original desktop name is retained by default. You can also enter a new name.

NOTE

- A desktop name can be set only when **Desktop Naming Rules** is set to **Do not use naming rules**.
- A desktop name cannot be set for multi-user desktop assignment. The desktop name remains unchanged.

Step 8 Click **OK**.

Step 9 If you want to perform this operation, enter **YES** or click **Auto Enter**.

Step 10 Click **OK**.

NOTE

Desktop assignment will clear the existing disk data and the data cannot be restored.

Assigning desktops to users in batches

NOTE

- A maximum of 100 desktops can be assigned at a time.
- Only desktops in the running or stopped status can be assigned in batches.
- Do not perform operations on the desktops during the assignment. You are advised to set the desktops to the maintenance mode to prevent exceptions caused by power supply or other operations performed by users during the assignment.
- A desktop can be assigned to multiple users, but only one user can use the desktop at a time.
- The images of the desktops to be assigned in batches must run the same OS, such as Windows or Linux.

Step 11 Select **User** or **User Group** for **Select User**.

Step 12 In the user list, you can select target users or user groups by username, user group, description, or enterprise project, and set the permission group.

Step 13 Set the assignment dimension.

- By user or user group: You can specify each user or user group and *N* ($0 < N \leq$ Number of selected desktops) desktops will be automatically assigned. Ensure that each user or user group is assigned at least one desktop and then consider the number of desktops assigned to each user. Prioritize users or user groups without desktops and sort them by username or user group name in ascending order. Desktops will be matched with users or user groups until all desktops are assigned.
- By desktop: Multiple users can log in to a desktop. Each desktop is automatically assigned to *N* ($0 < N \leq 100$) users. Desktops are sorted by the number of existing users and then by creation time. The earlier a desktop is created, the higher the priority is. Then, users are sorted by username. Ensure that the use of each desktop has been authorized first, and then consider the number of users authorized to use each desktop.

Step 14 Set the number of desktops to be assigned or the number of users to whom desktops are to be assigned.

- When the assignment dimension is by user or user group, set the number of desktops automatically assigned to each user or user group. The value cannot exceed the total number of selected desktops.

  For example, eight desktops (D1 to D8) are assigned to five users or user groups (U1 to U5, among which U1, U2, and U3 do not have desktops). If two desktops are assigned to each user or user group, users or user groups without desktops have a higher priority. In this case, assign the desktops in the following sequence: D1 to U1, D2 to U2, D3 to U3, D4 to U4, D5 to U5, D6 to U1, D7 to U2, and D8 to U3.

- When the assignment dimension is by desktop, set the number of users or user groups automatically assigned with desktops. The value cannot exceed the total number of selected users.

  For example, five desktops (D1 to D5) are assigned to eight users (U1 to U8) and each desktop is assigned to two users. In this case, each desktop (D1 to D5) is assigned to one user, and then another round of assignment will start from D1 until all users are assigned at least one desktop.

Step 15 Select a naming rule from **Desktop Naming Rule**, or select **Do not use** to use the default naming rule.

To create a naming rule, click **Create Desktop Naming Rule**. After the creation is complete, click **OK**. For details, see **8.3.1 Desktop Naming Rules**.

Step 16 Click **Preview** to view the desktop assignment information.

Step 17 If the information is correct, confirm the assignment.

Step 18 If you want to perform this operation, enter **YES** or click **Auto Enter**.

Step 19 Click **OK**.

----End

2.3.3 Unbinding Users

Scenarios

Unbind users from desktops on the console.

Procedure

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

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

The **Desktops** page is displayed.

Step 3 Perform the unbinding operation as required.

- Unbinding a single user
  - Unbinding a single-user desktop:

      i. Locate the row of the desired single-user desktop, click **More** in the **Operation** column, and choose **User Management** > **Unbind User**. The page for unbinding users is displayed.
      ii. Click **OK**. The confirmation dialog box is displayed.
      iii. If you want to perform this operation, enter **YES** or click **Auto Enter**.
      iv. Click **OK**.
   - Unbinding a multi-user desktop:
      i. Locate the row of the desired multi-user desktop, click **More** in the **Operation** column, and choose **User Management** > **Unbind User**. The page for unbinding users is displayed.
      ii. Select the users or user groups to be unbound and click **OK**.
      iii. In the displayed dialog box, enter **YES** or click **Auto Enter** to proceed with the operation.
      iv. Click **OK**.
- Batch unbinding:
   - Unbinding single-user desktops:
      i. Select the single-user desktops to be unbound and choose **More** > **User Management** > **Unbind User** above the list.
      ii. On the page displayed, select the desktops to be unbound and click **OK**.
      iii. In the displayed dialog box, enter **YES** or click **Auto Enter** to proceed with the operation.
      iv. Click **OK**.
   - Unbinding multi-user desktops:
      i. Select the multi-user desktops to be unbound and choose **More** > **User Management** > **Unbind User** above the list.
      ii. On the page displayed, select the multi-user desktops to be unbound and click **OK**.
      iii. In the displayed dialog box, enter **YES** or click **Auto Enter** to proceed with the operation.
      iv. Click **OK**.

NOTE

- Batch unbinding will unbind all users assigned with desktops.
- Once unbound, a single-user desktop will be stopped immediately. The client's desktop list will be refreshed, and the user will be unable to view or connect to the desktop.
- Once unbound, a multi-user desktop will not be stopped. If a multi-user desktop has been stopped, it will be started before being unbound.
- If a desktop is bound to another user, desktop data and snapshots will be cleared only when the desktop is a single-user desktop. The data of each user is separated and secure.
- If you click **Cancel**, the desktop will not be assigned. See **2.3.2 Assigning Desktops** to assign this desktop if needed. If a desktop is not assigned to any users, the data is retained on the desktop. For security purposes, you should assign unbound desktops as soon as possible.
- See **2.3.2 Assigning Desktops** to reassign a desktop.

----End

2.4 Networking

2.4.1 Desktop Network Settings

Scenarios

When the network of a user changes, the administrator can perform related settings for the user to quickly switch the desktop network.

Prerequisites

For desktop network settings, **submit a service ticket**.

Notes

- Switching the network will change the subnet, IP address, and MAC address of the cloud desktop, resulting in network disconnection.
- During the network switchover, do not perform operations on the Elastic IP (EIP) of the cloud desktop.
- After the network is switched, reconfigure network-related services and application software (such as NAT and DNS).
- Switching the network will switch the private IP address. If the desktop bound to an EIP cannot be bound to another EIP after the network settings are changed, perform the binding manually.
- After the network is switched, if the IP address of the desktop cannot be obtained, restart the desktop.
- When changing the desktop security group, check whether the security group in use has allowed the inbound and outbound rules required by the desktop access service. If not, desktop access will be affected.

  For details about the rule requirements, see
- To switch the network of a stopped desktop, start the desktop first. After the network is switched, shut down the desktop.

Procedure

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

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

Step 3 Switch the desktop network.

- For one desktop:
  1. Choose **More** > **Network Settings** > **Desktop Network Settings** in the **Operation** column of the desired desktop.
  2. Configure the desktop network.
     - VPC: Click ⌄ to select the VPC to be switched. To create a VPC, see **Creating a VPC and Subnet**. If a newly created VPC is used, choose **Tenant Configuration** > **Basic Settings**. In the **Network**

Configuration area, click **Edit VPC and Subnet** of **VPC** to add the VPC.

- Subnet: Click ∨ to select the subnet to be switched. To create a subnet, see **Creating a VPC and Subnet**. If a newly created subnet is used, choose **Tenant Configuration** > **Basic Settings**. In the **Network Configuration** area, click **Edit VPC and Subnet** of **VPC** to add the subnet.
- Private IP address: Select a private IP address assignment mode.
  - **Automatically-assigned IP**
  - **Manually-assigned IP**
  - **Existing ENI**
- Security group: Click ∨ to select the security group to be switched. To create a security group, see **Creating a Security Group**.

c. If you are clear about the impact of the desktop network switchover, enter **YES** or click **Auto Enter** for confirmation.

d. Click **OK**.

- For multiple desktops:

  a. In the desktop list, select the desired desktops, and choose **More** > **Network Settings** > **Desktop Network Settings** above the list. The **Desktop Network Settings** page is displayed.

  b. Configure the desktop network.

  - VPC: Click ∨ to select the VPC to be switched. To create a VPC, see **Creating a VPC and Subnet**. If a newly created VPC is used, choose **Tenant Configuration** > **Basic Settings**. In the **Network Configuration** area, click **Edit VPC and Subnet** of **VPC** to add the VPC.
  - Subnet: Click ∨ to select the subnet to be switched. To create a subnet, see **Creating a VPC and Subnet**. If a newly created subnet is used, choose **Tenant Configuration** > **Basic Settings**. In the **Network Configuration** area, click **Edit VPC and Subnet** of **VPC** to add the subnet.
  - Private IP address: Only **Automatically-assigned IP** is supported.
  - Security group: Select **Retain the original security group** or **Use the new security group**. To create a security group, see **Creating a Security Group**.

  c. If you are clear about the impact of the desktop network switchover, enter **YES** or click **Auto Enter** for confirmation.

  d. Click **OK**.

----End

2.5 Images

2.5.1 Converting a Desktop to an Image

2.5.1.1 Converting a Windows Desktop to an Image

Scenarios

If users have the same requirements on desktop configuration and application usage, you can purchase a desktop generated using a Windows OS image on the Workspace console, log in to the desktop, configure the desktop, install software, and convert the desktop to an image. Then, use the image to purchase desktops in batches and assign them to target users. This feature reduces personnel configuration costs and is a turnkey solution.

📖 NOTE

On the desktop to be converted to an image, files (including applications installed in this directory) in the user directory (**C:\Users\***Username of the current desktop*) of the current desktop cannot be added to the image. The configuration and applications of the desktop purchased using this image are inconsistent with those of the desktop to be converted to an image. Use the configuration and applications of the actual desktop that has been converted to an image.

Prerequisites

- A desktop generated using a Windows OS image is available.
- The desktop has been started and is in the **Running** status.
- You have logged in to the desktop at least once.

Procedure

Step 1 Log in to the console.

📖 NOTE

Select the region and project of the desktop to be converted to an image.

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

Step 3 Locate the row that contains the desktop to be converted to an image, and choose **More** > **Image Management** > **Create Image** in the **Operation** column. The image creation page is displayed.

Step 4 Configure image parameters as required, as shown in **Table 2-6**.

Table 2-6 Parameters

Parameter	Description	Example
Name	Image name. Configure this parameter as required. The value can contain only digits, letters, spaces, hyphens (-), underscores (_), and periods (.), and cannot start or end with a space.	temp_image-Windows private image
Description	Remarks about an image. Add remarks on the image usage.	-
Enterprise Project	You can use an enterprise project to centrally manage your cloud resources and members by project. You can select a value as required.	-
Encapsulate	Determine whether to encapsulate the image as required. ● **Yes**: Clears the user information of the desktop to be converted to an image, such as Security Identifier (SID). ● **No**: Retains the user information of the desktop to be converted to an image, such as Security Identifier (SID).	Yes
Agreement	Read *Statement of Commitment to Image Creation* and *Image Management Service Disclaimer*, and select **I have read and agree to *Statement of Commitment to Image Creation* and *Image Disclaimer***.	Selected

Step 5 If you want to perform this operation, enter **YES** or click **Auto Enter**.

Step 6 Click **OK**.

NOTE

- Do not perform any operations on the desktop during image creation.
- During image creation, all files in the desktop directory (**C:\Users\***current username*) will be deleted, and applications installed in this directory will be unavailable.
- If the response file (**c:\windows\system32\untitled.xml**) on which historical image encapsulation depends does not exist, contact the administrator.
- After the image is created, click ☰ on the console and choose **Compute** > **Image Management Service**. The created image is displayed in the **Private Images** list.

----End

2.5.2 Rebuilding a System Disk

Scenarios

If a purchased desktop needs to be initialized or desktop applications and patches need to be updated, you can rebuild or change the system disk.

Impact on the System

If you rebuild the system disk, the data (such as the desktop and favorites) on the system disk will be lost. If the data is needed after rebuilding, ask the user to back up the data in advance. Rebuilding system disks does not affect data disks.

Constraints

When rebuilding the system disk, if the desktop uses a private image, ensure that the private image still exists.

Prerequisites

The system disk can be rebuilt only when the running status of a desktop is running or stopped.

Procedure

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

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

The **Desktops** page is displayed.

Step 3 You can rebuild the system disk of one desktop, or system disks of multiple desktops in batches.

- To rebuild the system disk of one desktop, perform **Step 4** to **Step 6**.
- To batch rebuild the system disks of multiple desktops, perform **Step 7** to **Step 12**.

Step 4 Select the desktops whose system disks are to be rebuilt, and choose **More** > **Image Management** > **Recompose System Disk** in the **Operation** column.

The page for rebuilding system disks is displayed.

Step 5 Configure the system disk to be rebuilt, as shown in **Table 2-7**.

Table 2-7 Basic configuration

Parameter	Description	Example Value
Method	**Reinstall OS**: The original desktop image is used to rebuild the system disk.	Reinstall OS
OS	Select Windows or Linux as required.	Windows
Recomposing Started	Determine when to start rebuilding the system disk after clicking **OK** in **Step 6**. ● **Immediately** ● **In 1 minute** ● **In 5 minutes** ● **In 10 minutes** ● **In 15 minutes**	Immediately
Notification	Determine whether to notify the user of rebuilding the system disk of their desktop. If **Enable** is selected, a notification message is displayed on the desktop after the user logs in.	Disable
Notification Message	After selecting **Enable** for **Notification**, you can customize the content displayed in the pop-up window on the desktop.	-
To confirm the operation	If you want to perform this operation, enter **YES** or click **Auto Enter**.	Auto Enter

Step 6 Click **OK**. The desktop system disk will be rebuilt.

Step 7 On the **Desktops** page, batch select the desktops whose system disks are to be rebuilt, and choose **More** > **Image Management** > **Recompose System Disk** above the list.

Step 8 On the page displayed, if you want to perform this operation, enter **YES** or click **Auto Enter**.

Step 9 Click **OK**.

Step 10 Confirm the target desktops. The administrator can remove undesired desktops.

Step 11 On the page for rebuilding system disks, configure the system disk parameters, as shown in **Table 2-8**.

Table 2-8 Basic configuration

Parameter	Description	Example Value
Method	**Reinstall OS**: The original desktop image is used to rebuild the system disk.	Reinstall OS
Recomposing Started	Determine when to start rebuilding the system disk after clicking **OK** in **Step 6**. ● **Immediately** ● **In 1 minute** ● **In 5 minutes** ● **In 10 minutes** ● **In 15 minutes**	Immediately
To confirm the operation	If you want to perform this operation, enter **YES** or click **Auto Enter**.	Auto Enter

Step 12 Click **OK**.

Step 13 (Optional) Wait until the desktop status becomes **Running**. Contact the user to check and change the disk status of the desktop by referring to **How Do I Do If Data Disks of a Windows Desktop Cannot Be Found After Recomposing the System Disk?**

NOTE

This operation is needed only when you rebuild the system disk of a Windows desktop.

----End

2.6 Adding a Disk

Scenarios

If the data disk capacity of a purchased desktop does not meet requirements, you can add data disks to the desktop.

Prerequisites

You can add data disks only to a running desktop.

Procedure

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

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

The **Desktops** page is displayed.

Step 3 Select the desktop to which a data disk is to be added and choose **More** > **Disks and Snapshots** > **Add Disk**.

The page for adding a disk is displayed.

Step 4 Click **Add** and configure the data disk.

- High I/O disks use serial attached SCSI (SAS) drives to store data. They are suitable for common workloads.
- Ultra-high I/O disks use solid state disk (SSD) drives to store data. They are suitable for mission-critical enterprise services as well as high-throughput workloads demanding low latency.
- General purpose SSD disks use SSD drives to store data. They are suitable for enterprise office applications requiring high throughput and low latency.

NOTE

- The data disk size is 10 to 8200 GB (the value must be an integer multiple of 10).
- Disks cannot be added to hourly-billed Flexus desktops.
- The maximum number of data disks to add is 10 minus the number of existing data disks.

Step 5 Select **I understand the impact of this operation and will perform it** and click **Next**.

Step 6 Confirm the information about the added disk and click **OK**.

----End

2.7 Expanding Disk Capacity

Scenarios

If the data or system disk capacity of a purchased desktop does not meet requirements, you can expand the desktop's disk capacity.

Prerequisites

You can expand the capacity of a system disk or data disk only when the desktop is running or stopped.

Procedure

Step 1 Log in to the console.

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

The **Desktops** page is displayed.

Step 3 Select the desired desktop and choose **More** > **Disks and Snapshots** > **Expand Disk Capacity** in the **Operation** column.

The page for expanding disk capacity is displayed.

Step 4 Select **System Disk** or **Data Disk**.

Step 5 (Optional) If there are multiple data disks, select the data disks for capacity expansion.

Step 6 Set the **Added Capacity (GB)**.

NOTE

- The system disk capacity that can be added is displayed on the page. The total capacity after expansion cannot exceed 1,020 GB.
- The data disk capacity that can be added is displayed on the page. The total capacity after expansion cannot exceed 8,200 GB.
- Disk capacity expansion is not supported for hourly-billed Flexus desktops.

Step 7 Select **I understand the impact of this operation and will perform it** and click **Next**.

Step 8 Confirm the information and click **OK**.

----End

2.8 Deleting a Disk

Scenarios

If users' service volume changes, data disks are redundant, or they want a temporary large-capacity storage space which can be uninstalled and unsubscribe from after using it, you can delete a disk by referring to this section. After a data disk is deleted, the data on the disk is permanently deleted and cannot be restored. You are advised to delete a data disk only when the mapping between disk partitions and data disks can be determined. For example, you can delete data disks when there is only one data disk or data disks can be distinguished by disk capacity.

Prerequisites

- You have confirmed that the data on the user data disk is no longer used.
- The desktop has no running tasks.

Constraints

Only redundant data disks on the pay-per-use desktops can be deleted.

Procedure

Step 1 Log in to the console.

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

The **Desktops** page is displayed.

Step 3 Perform the corresponding operations based on the number of data disks to be deleted.

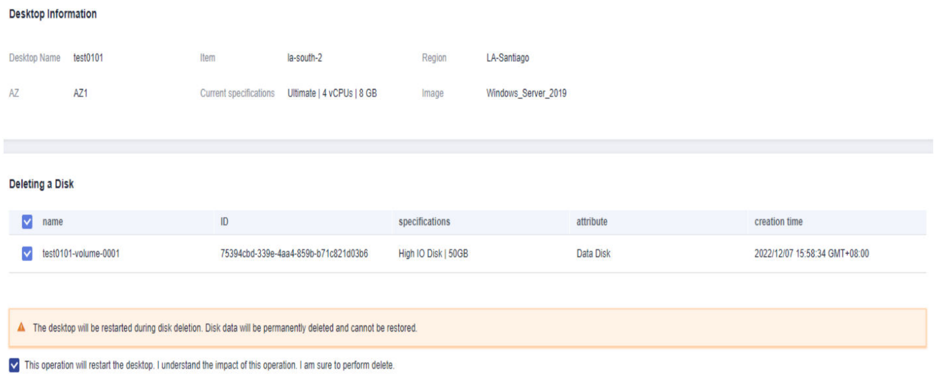
NOTICE

- After a data disk is deleted, the disk data will be permanently deleted and cannot be restored. Exercise caution when performing this operation.
- Disk deletion is not supported for hourly-billed Flexus desktops.

- More than one data disk
  a. Locate the row of the desired desktop, and choose **More** > **Disks and Snapshots** > **Delete Disk**.

     The page for deleting disks is displayed.
  b. Select the data disks to be deleted, as shown in **Figure 2-1**.

Figure 2-1 Selecting the data disks to be deleted



Desktop Information

Desktop Name test0101 Item la-south-2 Region LA-Santiago

AZ AZ1 Current specifications Ultimate | 4 vCPUs | 8 GB Image Windows_Server_2019

Deleting a Disk

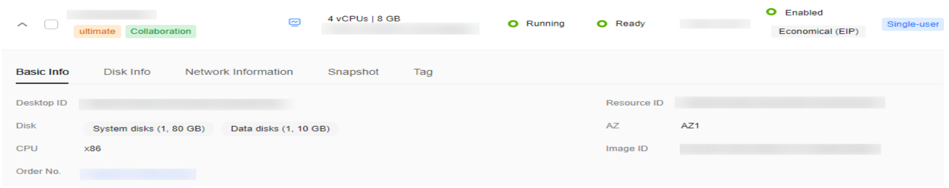
☑ name	ID	specifications	attribute	creation time
☑ test0101-volume-0001	75394cbd-339e-4aa4-859b-b71c821d03b6	High IO Disk | 50GB	Data Disk	2022/12/07 15:58:34 GMT+08:00

⚠ The desktop will be restarted during disk deletion. Disk data will be permanently deleted and cannot be restored.

☑ This operation will restart the desktop. I understand the impact of this operation. I am sure to perform delete.

  c. Confirm the data disks to be deleted, and select **I understand the impact and want to continue.**
  d. Confirm the deletion.
- One data disk
  a. Locate the row that contains the desktop whose data disk is to be deleted, and click ⌄ to expand the desktop information list, as shown in **Figure 2-2**.

Figure 2-2 Desktop details



Desktop ID [redacted] Resource ID [redacted]

Disk System disks (1, 80 GB) Data disks (1, 10 GB) AZ AZ1

CPU x86 Image ID [redacted]

Order No.

  b. Click the **Disk Info** tab page.
  c. Locate the data disk to be deleted and click **Delete** in the **Operation** column.
  d. Confirm the data disk to be deleted, and select **I understand the impact and want to continue.**
  e. Click **OK**.

----End

2.9 Changes and Fees

2.9.1 Changing the Desktop Billing Mode

2.9.1.1 Changing from Pay-per-Use to Yearly/Monthly

Scenarios

You can convert pay-per-use desktops whose validity period can be estimated to yearly/monthly-billed desktops as required.

Constraints

Only a single pay-per-use Windows desktop can be converted to a yearly/monthly-billed desktop.

Procedure

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

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

Step 3 Locate the row of the desired pay-per-use desktop, and choose **More** > **Changes and Expenses** > **Pay-per-Use to Yearly/Monthly** in the **Operation** column.

Step 4 If you want to perform this operation, enter **YES** or click **Auto Enter**.

Step 5 Click **OK**.

Step 6 Confirm the order information and pay the bill.

----End

2.9.1.2 Changing from Yearly/Monthly to Pay-per-Use

Scenario

Administrators can change the billing mode of desktops with an estimated validity period from yearly/monthly to pay-per-use.

NOTE

The change takes effect only after the yearly/monthly subscription expires.

Constraints

- The billing mode can be changed from yearly/monthly to pay-per-use only after you have passed real-name authentication.
- The billing mode can be changed from yearly/monthly to pay-per-use only for desktops whose order status is **Provisioned**. To check the order status, hover

over **Billing** in the upper part of the console and choose **Renewal** from the drop-down list.

Procedure

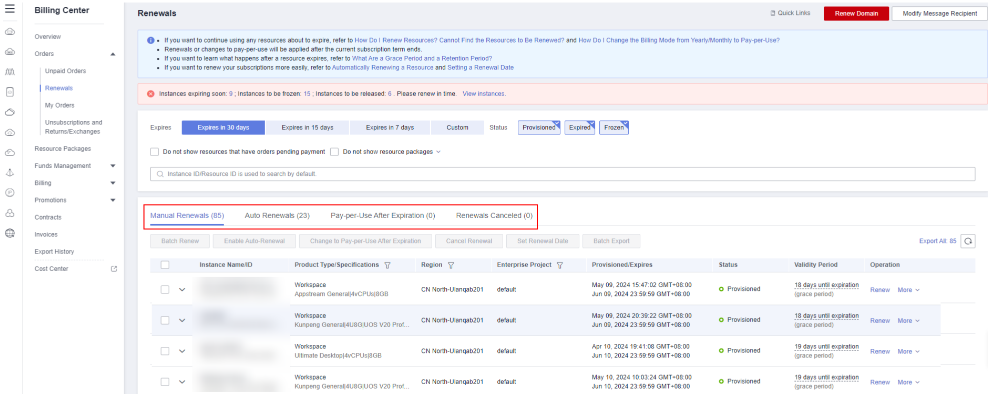
Step 1 Log in to the console.

Step 2 Hover over **Billing** in the upper part of the console and choose **Renewal** from the drop-down list. The **Renewals** page is displayed.

Step 3 Customize search criteria, as shown in **Figure 2-3**.

- Under the **Pay-per-Use After Expiration** tab, you can check the resources that have already been set to change to pay-per-use billing upon expiration.
- Under the **Manual Renewals**, **Auto Renewals**, and **Renewals Canceled** tabs, you can change the resources to pay-per-use billing upon expiration.

Figure 2-3 Renewals



- If you want to continue using any resources about to expire, refer to How Do I Renew Resources? Cannot Find the Resources to Be Renewed? and How Do I Change the Billing Mode from Yearly/Monthly to Pay-per-Use?
- Renewals or changes to pay-per-use will be applied after the current subscription term ends.
- If you want to learn what happens after a resource expires, refer to What Are a Grace Period and a Retention Period?
- If you want to renew your subscriptions more easily, refer to Automatically Renewing a Resource and Setting a Renewal Date

Instances expiring soon: 9 ; Instances to be frozen: 15 ; Instances to be released: 6 . Please renew in time. View instances.

□ Do not show resources that have orders pending payment □ Do not show resource packages

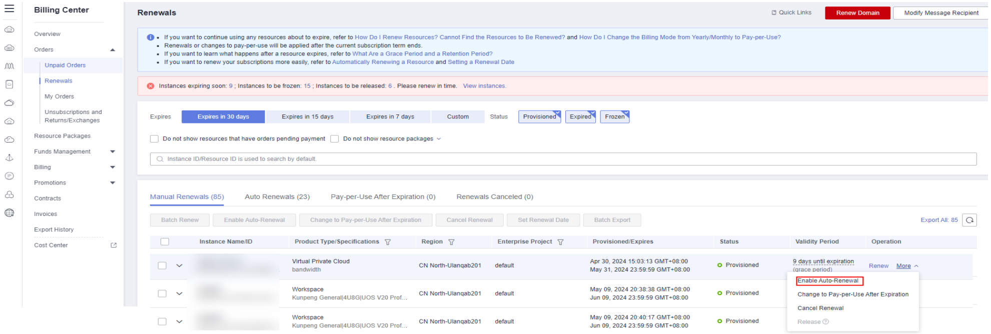
Instance ID/Resource ID is used to search by default.

□	Instance Name/ID	Product Type/Specifications	Region	Enterprise Project	Provisioned/Expires	Status	Validity Period	Operation
□	[redacted]	Workspace Appstream General|4vCPUs|8GB	CN North-Ulanqab201	default	May 09, 2024 15:47:02 GMT+08:00 Jun 09, 2024 23:59:59 GMT+08:00	Provisioned	18 days until expiration (grace period)	Renew More
□	[redacted]	Workspace Kunpeng General|4U8G|UOS V20 Prof...	CN North-Ulanqab201	default	May 09, 2024 20:39:22 GMT+08:00 Jun 09, 2024 23:59:59 GMT+08:00	Provisioned	18 days until expiration (grace period)	Renew More
□	[redacted]	Workspace Ultimate Desktop|4vCPUs|8GB	CN North-Ulanqab201	default	Apr 10, 2024 19:41:08 GMT+08:00 Jun 10, 2024 23:59:59 GMT+08:00	Provisioned	19 days until expiration (grace period)	Renew More
□	[redacted]	Workspace Kunpeng General|4U8G|UOS V20 Prof...	CN North-Ulanqab201	default	May 10, 2024 10:03:24 GMT+08:00 Jun 10, 2024 23:59:59 GMT+08:00	Provisioned	19 days until expiration (grace period)	Renew More

Step 4 Change yearly/monthly desktops to pay-per-use billing upon expiration, as shown in **Figure 2-4**.

- For one desktop: Select the desktop for which you want to change the billing mode, and choose **More** > **Change to Pay-per-Use After Expiration** in the **Operation** column.

Figure 2-4 Changing the billing mode of one desktop to pay-per-use billing



- If you want to continue using any resources about to expire, refer to How Do I Renew Resources? Cannot Find the Resources to Be Renewed? and How Do I Change the Billing Mode from Yearly/Monthly to Pay-per-Use?
- Renewals or changes to pay-per-use will be applied after the current subscription term ends.
- If you want to learn what happens after a resource expires, refer to What Are a Grace Period and a Retention Period?
- If you want to renew your subscriptions more easily, refer to Automatically Renewing a Resource and Setting a Renewal Date

Instances expiring soon: 9 ; Instances to be frozen: 15 ; Instances to be released: 6 . Please renew in time. View instances.

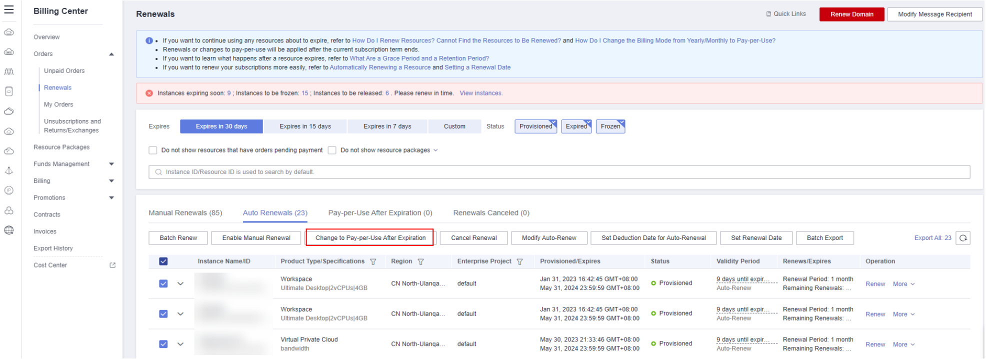
□ Do not show resources that have orders pending payment □ Do not show resource packages

Instance ID/Resource ID is used to search by default.

□	Instance Name/ID	Product Type/Specifications	Region	Enterprise Project	Provisioned/Expires	Status	Validity Period	Operation
□	[redacted]	Virtual Private Cloud bandwidth	CN North-Ulanqab201	default	Apr 30, 2024 15:03:13 GMT+08:00 May 31, 2024 23:59:59 GMT+08:00	Provisioned	9 days until expiration (grace period)	Renew More
□	[redacted]	Workspace Kunpeng General|4U8G|UOS V20 Prof...	CN North-Ulanqab201	default	May 09, 2024 20:38:38 GMT+08:00 Jun 09, 2024 23:59:59 GMT+08:00	Provisioned		
□	[redacted]	Workspace Kunpeng General|4U8G|UOS V20 Prof...	CN North-Ulanqab201	default	May 09, 2024 20:40:17 GMT+08:00 Jun 09, 2024 23:59:59 GMT+08:00	Provisioned		

- For multiple desktops: Select the desktops for which you want to change the billing mode, and click **Change to Pay-per-Use After Expiration** above the resource list, as shown in **Figure 2-5**.

Figure 2-5 Changing the billing mode of multiple desktops to pay-per-use billing



- If you want to continue using any resources about to expire, refer to How Do I Renew Resources? Cannot Find the Resources to Be Renewed? and How Do I Change the Billing Mode from Yearly/Monthly to Pay-per-Use?
- Renewals or changes to pay-per-use will be applied after the current subscription term ends.
- If you want to learn what happens after a resource expires, refer to What Are a Grace Period and a Retention Period?
- If you want to renew your subscriptions more easily, refer to Automatically Renewing a Resource and Setting a Renewal Date

Instances expiring soon: 9 ; Instances to be frozen: 15 ; Instances to be released: 6 . Please renew in time. View instances.

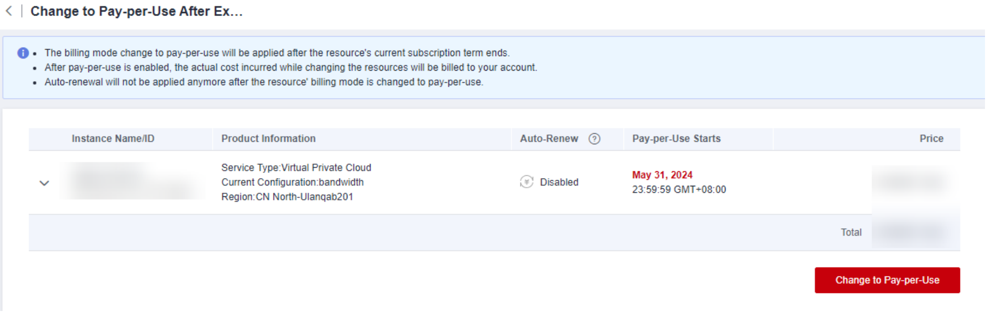
□ Do not show resources that have orders pending payment □ Do not show resource packages

Instance ID/Resource ID is used to search by default.

☑	Instance Name/ID	Product Type/Specifications	Region	Enterprise Project	Provisioned/Expires	Status	Validity Period	Renews/Expires	Operation
☑	[redacted]	Workspace Ultimate Desktop|2vCPUs|4GB	CN North-Ulanqa...	default	Jan 31, 2023 16:42:45 GMT+08:00 May 31, 2024 23:59:59 GMT+08:00	○ Provisioned	9 days until expir... Auto-Renew	Renewal Period: 1 month Remaining Renewals: ...	Renew More
☑	[redacted]	Workspace Ultimate Desktop|2vCPUs|4GB	CN North-Ulanqa...	default	Jan 31, 2023 16:42:45 GMT+08:00 May 31, 2024 23:59:59 GMT+08:00	○ Provisioned	9 days until expir... Auto-Renew	Renewal Period: 1 month Remaining Renewals: ...	Renew More
☑	[redacted]	Virtual Private Cloud bandwidth	CN North-Ulanqa...	default	May 30, 2023 21:33:46 GMT+08:00 May 31, 2024 23:59:59 GMT+08:00	○ Provisioned	9 days until expir... Auto-Renew	Renewal Period: 1 month Remaining Renewals: ...	Renew More

Step 5 Confirm the subscription change details, and click **Change to Pay-per-Use After Expiration**, as shown in **Figure 2-6**.

Figure 2-6 Changing the billing mode to pay-per-use billing upon expiration



- The billing mode change to pay-per-use will be applied after the resource's current subscription term ends.
- After pay-per-use is enabled, the actual cost incurred while changing the resources will be billed to your account.
- Auto-renewal will not be applied anymore after the resource' billing mode is changed to pay-per-use.

Instance Name/ID	Product Information	Auto-Renew	Pay-per-Use Starts	Price
[redacted]	Service Type:Virtual Private Cloud Current Configuration:bandwidth Region:CN North-Ulanqab201	Disabled	May 31, 2024 23:59:59 GMT+08:00	[redacted]
			Total	[redacted]

----End

2.9.2 Renewing a Yearly/Monthly-Billed Desktop

Scenario

You can renew yearly/monthly-billed desktops.

Procedure

Step 1 Log in to the console.

Step 2 In the navigation tree on the left, choose **Desktop Management** > **Desktops**.

The desktop management page is displayed.

Step 3 Select the target yearly/monthly-billed desktop, and click **More** > **Renew** in the upper left corner of the desktop list or in the **Operation** column.

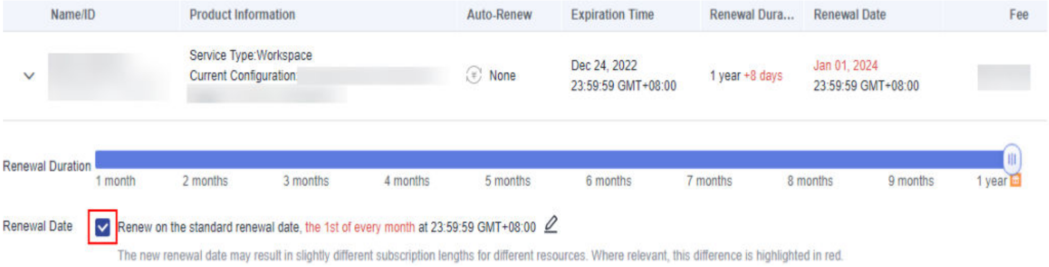
The renewal configuration page is displayed.

Step 4 (Optional) Select **Renew on the standard renewal date**.

NOTE

You can click ✎ to reset a unified renewal date for resources.

Figure 2-7 Setting a unified renewal date



Name/ID	Product Information	Auto-Renew	Expiration Time	Renewal Dura...	Renewal Date	Fee
	Service Type:Workspace Current Configuration:	None	Dec 24, 2022 23:59:59 GMT+08:00	1 year +8 days	Jan 01, 2024 23:59:59 GMT+08:00	

Renewal Duration: 1 month, 2 months, 3 months, 4 months, 5 months, 6 months, 7 months, 8 months, 9 months, 1 year

Renewal Date: ☑ Renew on the standard renewal date, the 1st of every month at 23:59:59 GMT+08:00

The new renewal date may result in slightly different subscription lengths for different resources. Where relevant, this difference is highlighted in red.

Step 5 Click **Pay**.

Step 6 Confirm the order, select a payment method, and pay the bill.

----End

2.9.3 Changing Specifications

Scenarios

If the specifications of a purchased desktop cannot meet service requirements, you can change the specifications, including vCPUs and memory.

Constraints

- When changing desktop specifications, users cannot select vCPU and memory resources that are no longer provided.
- You cannot perform other operations on the desktop when changing the specifications.

Procedure

Step 1 Log in to the console.

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

The **Desktops** page is displayed.

Step 3 Perform operations based on the new billing mode and number of desktops. For details, see **Table 2-9**.

NOTE

- The specifications of **yearly/monthly-billed** desktops cannot be changed in batches.
- When changing specifications in batches, ensure that the selected desktops have the same billing mode, AZ, and specifications.
- Only the power-on and power-off tasks can be performed on the target desktop.
- The desktop performance will be affected if the specifications (CPU or memory) of pay-per-use desktops are decreased. You can change the specifications as required.
- The specifications of Flexus hourly-billed desktops cannot be changed.

Table 2-9 Operations

Billing Mode	Desktop Quantity	Operation
Pay-per-Use	One	In the row of the desktop whose specifications are to be changed, click **More** > **Changes and Expenses** > **Change Specifications** in the **Operation** column.
	More than one	Above the desktop list, click **More** > **Changes and Expenses** > **Change Specifications**.
Yearly/ Monthly	One	In the row of the desktop whose specifications are to be changed, click **More** > **Changes and Expenses** > **Change Specifications** in the **Operation** column.

Step 4 Select **Shut Down to Change Specifications**.

> NOTE
>
> If you have stopped the desktop whose specifications are to be changed before accessing the page for changing specifications, the **Shut Down to Change Specifications** option is unavailable.

Step 5 In the **Select Specifications** area, select the required specifications and click **Next**.

The page for confirming the specification change details is displayed.

Step 6 Confirm the details and click **Confirm**.

- For pay-per-use desktops, after the task is submitted, click **Return to the desktop list**. On the **Desktops** page, the desktop status is **Changing**. You can view the changed desktop specifications in the **Specifications/Image** column.

  > NOTE
  >
  > - Changing specifications does not affect the data on the system disk and data disks of the desktop.
  > - For pay-per-use desktops, pay attention to the fee changes caused by configuration changes (only the CPU and memory fees are included).

- For yearly/monthly-billed desktops, supplement the fees or get the refund on the corresponding page.

  > NOTE
  >
  > Changing specifications does not affect the data on the system disk and data disks of the desktop.

  - If you need to supplement the fees, the payment page is displayed. Select a payment method. Return to the **Desktops** page. The desktop status is **Changing**. You can view the changed desktop specifications in the **Specifications/Image** column.
  - If you need to get the refund (including 0), the task submission page is displayed. In the displayed page, click **Return to the desktop list**. On the **Desktops** page, the desktop status is **Changing**. You can view the changed desktop specifications in the **Specifications/Image** column.

----End

2.9.4 Deleting or Unsubscribing from Desktops

Scenarios

Unsubscribe from desktops on the management console.

Procedure

Step 1 Log in to the console.

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

The **Desktops** page is displayed.

Unsubscribing from pay-per-use desktops

Step 3 Select the pay-per-use desktops to be unsubscribed from, and click **More** > **Changes and Expenses** > **Delete** above the desktop list or in the **Operation** column.

The desktop deletion page is displayed.

Step 4 The default deletion method is **Delete**. You can determine whether to force stop the desktops.

NOTE

1. You can determine whether to delete users at the same time.

2. Deleting a desktop will also delete its system disk. This operation cannot be undone, so exercise caution.

3. Deleting or unsubscribing from a desktop will automatically unbind its EIP, but the EIP billing will continue. You can manually release the EIP by referring to **What Is Elastic IP?**

Step 5 If you want to perform this operation, enter **YES** or click **Auto Enter**, and click **OK**.

Unsubscribing from yearly/monthly desktops

Step 6 Select the yearly/monthly desktops to be unsubscribed from, and click **More** > **Changes and Expenses** > **Unsubscribe** above the desktop list or in the **Operation** column.

The desktop unsubscription page is displayed.

Step 7 On the desktop unsubscription page, confirm the desktop information and click **OK**.

The resource unsubscription page is displayed.

Step 8 On the resource unsubscription page, confirm the unsubscription information, enter the unsubscription reason, and select the checkbox **I've backed up the data or confirmed that the unsubscribed resources are no longer needed. I understand that only resources in the recycle bin can be restored after unsubscription**.

Step 9 Click **Confirm**.

Step 10 If you want to perform this operation, enter **YES** or click **Auto Enter**.

Step 11 Click **OK**.

NOTE

1. Unsubscribing from a desktop will also unsubscribe from its system disk. This operation cannot be undone, so exercise caution.

2. Deleting or unsubscribing from a desktop will automatically unbind its EIP, but the EIP billing will continue. You can manually release the EIP by referring to **What Is Elastic IP?**

3. For details about resource unsubscription, see **Unsubscriptions**.

----End

2.10 Viewing Failed Tasks

Scenarios

You can view the cause of desktop creation failure. The desktops with creation faults rectified are displayed in the desktop management list. Yearly/monthly-billed desktops that fail to be created will be created with the assistance of maintenance personnel.

You can view the causes of failed tasks, including desktop creation, specification change, disk addition, deletion, and capacity expansion, image creation, system disk rebuilding, desktop assignment, desktop network setting, notification sending, snapshot creation and restoration, user permission change, desktop hibernation, and disk QoS modification.

Procedure

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

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

The **Desktops** page is displayed.

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

The page of failed tasks is displayed.

Step 4 You can view the causes of failed tasks, including desktop creation, specification change, disk addition, deletion, and capacity expansion, image creation, system disk rebuilding, desktop assignment, desktop network setting, notification sending, snapshot creation and restoration, user permission change, and desktop hibernation.

----End

2.11 Managing Tags

Scenarios

This section describes how to use tags to search for desktops, and how to add, edit, and delete tags.

Adding/Editing a Tag

Step 1 Log in to the console.

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

The **Desktops** page is displayed.

Adding tags to one desktop

Step 3 Click ⌄ to expand the basic desktop information.

Step 4 Click **Tag**.

Step 5 Click **Add/Edit Tag**.

The page for adding or editing tags is displayed.

Step 6 Enter a tag key and tag value, and click **Add**. See **Table 2-10**.

NOTE

You can add a maximum of 20 tags to a desktop.

Table 2-10 Tag naming rules

Parameter	Rule
Tag Key	● This field cannot be left blank. ● The value can contain up to 36 characters. ● A tag key can contain letters, digits, spaces, and special characters (_.:=+-@), but cannot start or end with a space or start with **_sys_**. ● Each tag key must be unique on the same desktop.
Tag Value	● The value can contain up to 43 characters. ● A tag value can contain letters, digits, spaces, and special characters (_.:/=+-@).

Step 7 Click **OK**.

Batch adding tags to multiple desktops

Step 8 In the desktop list, select the desired desktops.

Step 9 Choose **More** > **O&M Operations** > **Add Tag**. The page for adding tags is displayed.

Step 10 Set the tag key and tag value by referring to **Table 2-10**.

Step 11 Click **OK**.

----End

Searching for a Desktop by Tag

Step 1 Log in to the console.

Step 2 Choose **Desktops** > **Desktops**. The **Desktops** page is displayed.

- Enter a tag key in the search box above the desktop list, and select the tag key and its tag value under **Resource Tag** for search.
- In the search box above the desktop list, select the tag key and its tag value under **Resource Tag** for search.

NOTE

- This query only applies to existing keys and values.
- A maximum of 10 different tags can be combined for search.

----End

Deleting a Tag

Step 1 Log in to the console.

Step 2 Choose **Desktops** > **Desktops**. The **Desktops** page is displayed.

Step 3 Click ⌄ to expand the basic desktop information.

Step 4 Click **Tag**.

Step 5 Click **Delete** in the **Operation** column on the right of the tag.

Step 6 Click **OK**.

NOTE

Deleted tags cannot be recovered.

----End

3 Desktop Pools

3.1 Managing Desktop Pools

Scenarios

The administrator can start, stop, restart, and delete desktops, and change desktop names of a desktop pool. The administrator can also create a group of desktop resources for customers to use them in different time periods to improve work efficiency.

Prerequisites

A desktop pool has been created.

Procedure

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

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

The **Desktop Pools** page is displayed.

Step 3 Perform the operations in **Table 3-1** as required.

Table 3-1 Operations

Operation	Procedure
Viewing desktop pool information	1. Above the desktop list, enter a keyword and press **Enter**. 2. View information such as the desktop pool name, pool type, specifications/images, desktop usage, maintenance mode, and billing mode.
Viewing desktops in a desktop pool	1. In the desktop pool list, click the name of a desktop pool to view its basic information. 2. Filter data based on the property type and view desktop information by desktop ID, desktop name, billing mode, running status, connection status, AZ, subnet, IP address, desktop user, assignment status, image ID, maintenance mode, and enterprise project.
Changing a desktop pool name	1. Click the name of a desktop pool to view its basic information. 2. Click ✎ on the right of the name. 3. Enter the new name and click ✓ . **NOTE** The desktop pool name must be unique and contain 1 to 15 characters in letters, digits, and hyphens (-).
Deleting a desktop pool	For pay-per-use desktops: 1. Choose **More** > **Delete** in the **Operation** column of the desktop pool to be deleted. 2. Click **OK**. **NOTE** Before deleting a desktop pool, disable the automatic creation function and delete the desktops. For yearly/monthly-billed desktop pools: 1. Click the name of the desktop pool to go to the basic information page. Select a desktop and choose **More** > **Unsubscribe** above the list or in the **Operation** column. 2. On the desktop unsubscription page, confirm the desktop information and click **OK**. 3. On the resource unsubscription page, confirm the resource to be unsubscribed from and write the unsubscription reason, select the resource and data statement for desktop unsubscription, and click **Unsubscribe**. For details about resource unsubscription, see **Unsubscriptions**.

Operation	Procedure
Stopping a desktop pool	1. Locate the row of the desktop pool to be stopped, and click **Stop** in the **Operation** column. 2. If you want to perform this operation, enter **YES** or click **Auto Enter**. **NOTE** You can determine whether to force stop desktops. 3. Click **OK**.
Starting a desktop pool	1. Locate the row of the desktop pool to be started, and click **Start** in the **Operation** column. 2. If you want to perform this operation, enter **YES** or click **Auto Enter**. 3. Click **OK**.
Hibernating a desktop pool	1. Locate the row of the desktop pool to be hibernated, and click **More** > **Hibernate** in the **Operation** column. 2. If you want to perform this operation, enter **YES** or click **Auto Enter**. **NOTE** Currently, only Windows desktops can be hibernated. 3. Click **OK**.
Restarting a desktop pool	1. Locate the row of the desktop pool to be restarted, and click **More** > **Restart** in the **Operation** column. 2. If you want to perform this operation, enter **YES** or click **Auto Enter**. 3. Click **OK**. **NOTE** You can determine whether to force restart desktops.

Operation	Procedure
Creating a snapshot	● Creating a snapshot for one desktop: 1. Click the name of a desktop pool to view its basic information. 2. Select the desktop for which you want to create a snapshot, and click **More** > **Create Snapshot** above the desktop list or in the **Operation** column. 3. On the page displayed, specify **Applied To**. Then enter **System Disk Snapshot Name** or **Data Disk Snapshot Name**, or both, as well as **System Disk Snapshot Description** or **Data Disk Snapshot Description**, or both. 4. Click **OK**. ● Batch creating snapshots for desktops: 1. Click the name of a desktop pool to view its basic information. 2. Select the desired desktops and choose **More** > **Create Snapshot** above the list. 3. On the page displayed, specify **Applied To**. Then enter **System Disk Snapshot Name** or **Data Disk Snapshot Name**, or both, as well as **System Disk Snapshot Description** or **Data Disk Snapshot Description**, or both. 4. Click **OK**. **NOTE** ● Snapshots can be created only for desktops in a static desktop pool. ● A maximum of five system disk snapshots and five data disk snapshots can be saved for each desktop, including those created on the console and those created by end users. ● Rebuilding the system disk, deleting a desktop, deleting a disk, or unbinding a desktop from a user and binding it to another user will automatically delete the snapshots of the desktop.

Operation	Procedure
Restoring a snapshot	1. Click the name of a desktop pool to view its basic information. 2. Click ⌄ on the left of the desired desktop, and click the **Snapshots** tab. 3. Restore a snapshot. – Restoring one snapshot: Click **Restore** in the **Operation** column. On the page displayed, check the box indicating that you understand the impact of this operation (stopping the desktop and restoring the snapshot), and click **OK**. – Batch restoring snapshots: Batch select the desired snapshots and click **Restore** above the snapshot list. On the page displayed, check the box indicating that you understand the impact of this operation (stopping the desktop and restoring the snapshots), and click **OK**. **NOTE** ● Only the snapshots of one data disk and one system disk can be restored for a desktop at a time. ● Snapshot restoration will force stop the desktop. ● A time point will be specified for snapshot restoration. After the restoration, data generated after this time point cannot be retrieved.
Deleting a snapshot	1. Click the name of a desktop pool to view its basic information. 2. Click ⌄ on the left of the desired desktop, and click the **Snapshots** tab. 3. Delete a snapshot. – Deleting one snapshot: Click **Delete** in the **Operation** column. On the page displayed, check the box indicating that you understand the impact of this operation (deleting the snapshot), and click **OK**. – Batch deleting snapshots: Batch select the desired snapshots and click **Delete** above the list. On the page displayed, check the box indicating that you understand the impact of this operation (batch deleting the snapshots), and click **OK**. **NOTE** Rebuilding the system disk, deleting a desktop, or deleting a disk will automatically delete the snapshot of the desktop.

Operation	Procedure
Managing desktop pool scripts	1. In the desktop pool list, choose **More** > **Script** > **Execute Script** in the **Operation** column of the desired desktop pool. For details, see 12.1 Script Management. 2. In the desktop pool list, choose **More** > **Script** > **Execute Command** in the **Operation** column of the desired desktop pool, and click **Enter Command**. On the displayed page, select **Execution Environment**, specify **Command Timeout**, and enter a command. Then click **Execute**. 3. In the desktop pool list, choose **More** > **Script** > **Script Record** in the **Operation** column of the desired desktop pool to check script execution records on the **Scripts** page. For details, see 12.2 Command Records.
Remotely logging in to a desktop in the desktop pool	1. Click the name of a desktop pool to view its basic information. 2. Locate the row that contains the target desktop and choose **More** > **Remote Login** in the **Operation** column. 3. The remote login page is displayed. Enter the account and password to remotely log in to the desktop. **NOTE** – Desktops that are not assigned to users do not support remote login. – Only running desktops support remote login.
Sending a notification	1. Choose **More** > **Send notification** in the **Operation** column of the desktop pool. The **Send notifications** page is displayed. 2. Enter the content of the message to be sent and click **Send**. **NOTE** Notifications can be sent only for desktop pools that are running.
Changing the duration of desktop pool unbinding upon disconnection	1. Click the name of a desktop pool to view its basic information. 2. Click ✎ on the right of **Disconnection and Unbinding**. 3. Change **Retention period** and click **OK**. **NOTE** – This operation can be performed only on dynamic desktop pools. – The value must range from 10 to 43,200. – After a client user disconnects from a desktop, the desktop can be retained for a period of time. After the retention period expires, the desktop is automatically unbound from the user and reset.

Operation	Procedure
Changing the number of desktops automatically created in a desktop pool	1. Click the name of a desktop pool to view its basic information. 2. Click ✎ on the right of **Auto Create**. The **Auto Create** page is displayed. 3. Change the value of *x* as required.
Changing the desktop naming rule of a desktop pool	1. Click the name of a desktop pool to view its basic information. 2. Click ✎ on the right of the desktop naming rule. The **Desktop Naming Rules** window is displayed. 3. Select a naming rule from the drop-down list box and click **OK**. **NOTE** A desktop pool supports only naming rules that do not contain usernames.
Enabling the maintenance mode	1. Select the desired desktop pool and choose **More** > **Enable Maintenance Mode** in the **Operation** column. 2. Check the box of enabling maintenance mode and click **OK**. **NOTE** – In the maintenance mode, all operations, such as user access, self-service maintenance, startup, shutdown, and restart, are not allowed. – Desktops that are being connected to and have been connected to will not be affected.
Disabling the maintenance mode	1. Select the desired desktop pool and choose **More** > **Disable Maintenance Mode** in the **Operation** column. 2. Check the box of disabling maintenance mode and click **OK**.

----End

3.2 Viewing Desktops That Fail to Be Created in the Desktop Pool

Scenario

On the management console, administrators can view the causes of desktop creation failures in the desktop pool.

NOTE

If no desktop fails to be created in the desktop pool, this function is not displayed.

Procedure

Step 1 Log in to the Workspace console.

Step 2 In the navigation pane, choose **Desktop Management** > **Desktop Pool**.

The **Desktop Pool** page is displayed.

Step 3 Click the desktop pool name. The basic information page of the desktop pool is displayed.

Step 4 Click **Failed tasks** on the right of **More** in the **Operation** column.

The **Failed tasks** page is displayed.

Step 5 View the cause of the desktop creation failure.

----End

3.3 Modifying Specifications

Scenario

If the specifications of a purchased desktop pool cannot meet service requirements, you can modify the specifications, including vCPUs and memory.

- The specifications of a **yearly/monthly-billed** desktop cannot be decreased.
- The specifications of a **pay-per-use** desktop can be increased or decreased as required.

Constraints

- When modifying desktop pool specifications, users cannot select vCPU and memory resources that are no longer provided.
- You cannot perform other operations on the desktop pool when modifying the specifications.

Procedure

Step 1 Log in to the Workspace console.

Step 2 In the navigation pane, choose **Desktop Management** > **Desktop Pool**.

The **Desktop Pool** page is displayed.

Step 3 You can access the page for modifying desktop pool specifications in either of the following ways:

Method 1:

Locate the row that contains the desktop pool whose specifications are to be modified, click **More** in the **Operation** column, and select **Change Specification**. The page for modifying specifications is displayed.

Method 2:

On the desktop pool page, click the name of the desktop pool whose specifications are to be modified. The basic information page of the desktop pool is displayed.

Click **Change specifications** on the right of the **Package Specifications** column in the desktop pool information. The page for modifying specifications is displayed.

Step 4 Select **Shut Down to Change Specifications**.

📖 NOTE

If you have stopped the desktop whose specifications are to be modified before accessing the page for modifying specifications, the **Shut Down to Change Specifications** option is unavailable.

Step 5 In the **Select Specifications** area, select the required specifications and click **Next**.

The page for confirming the specification modification details is displayed.

NOTICE

- For yearly-billed/monthly-billed/pay-per-use desktops, pay attention to the fee changes caused by configuration changes (only the CPU and memory fees are included).
- Do not perform other operations on the desktop when modifying specifications.
- Modifying specifications does not affect the data on the system disk and data disks of the ECS.

Step 6 Confirm the modification details and click **Confirm**.

- For pay-per-use desktops, go to the task submission prompt page and click **Return to the desktop list.** On the desktop pool management page, click the name of the desktop pool whose specifications are to be changed. The basic information about the desktop pool is displayed. The desktop pool status is **Changing**. You can view the modified desktop pool specifications in **Package Specifications** on the basic desktop pool information page.

  📖 NOTE

  - Modifying specifications does not affect the data on the system disk and data disks of the desktop.
  - For pay-per-use desktops, pay attention to the fee changes caused by configuration changes (only the CPU and memory fees are included).
- For yearly/monthly-billed desktops, supplement the fees or get the refund on the corresponding page.

  📖 NOTE

  Modifying specifications does not affect the data on the system disk and data disks of the desktop.

  - If you need to supplement the fees, the payment page is displayed. Select a payment method. Click **Return to the desktop list.** The desktop status is **Changing**. You can view the modified desktop specifications in the **Specifications/Image** column.
  - If you need to get the refund (including 0), the task submission page is displayed. Click **Back to Workspace**. On the **Desktop Management**

page, the desktop status is **Changing**. You can view the modified desktop specifications in the **Specifications/Image** column. On the task submission page, click **View order**. The refund order details page is displayed. You can view the order details.

----End

3.4 Adding Users or User Groups

Scenarios

Add users or user groups to desktops in the desktop pool.

Procedure

Step 1 Log in to the console.

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

The **Desktop Pools** page is displayed.

Step 3 You can access the page for adding authorized users or user groups in either of the following ways:

Method 1:

Locate the row that contains the desktop pool to which users or user groups are to be added, click **More** in the **Operation** column, and select **Adding a User or User Group**. The page for adding authorized users or user groups is displayed.

Method 2:

On the desktop pool page, click the name of the desktop pool to which users or user groups are to be added. The basic information page of the desktop pool is displayed.

Choose **User (Group)** > **Authorize** on the right of the desktop pool basic information. The page for adding authorized users or user groups is displayed.

Step 4 You can search for the corresponding user or user group based on the entered user or user group name, or select the required user or user group from the options.

Step 5 Click **OK**.

----End

3.5 Adding Disks

Scenarios

Add data disks to a desktop pool.

Prerequisites

You can add data disks only to a running desktop pool.

Procedure

Step 1 Log in to the console.

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

The **Desktop Pools** page is displayed.

Step 3 You can access the page for adding data disks to a desktop pool in either of the following ways:

Method 1:

Locate the row of the desktop pool to which disks are to be added, and click **More** > **Disk** > **Add Disk** in the **Operation** column. The page for adding disks is displayed.

Method 2:

On the desktop pool page, click the name of the desktop pool to which disks are to be added. The basic information page of the desktop pool is displayed.

Click **Add** on the right of the **Disk Information** column in the desktop pool information. The page for adding disks is displayed.

Step 4 Click **Add a data disk** and configure the data disk.

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

NOTE

- After the desktop is created, you will be billed for the disk until the desktop is deleted.
- After the disk partition is formatted, stop or restart the desktop, or expand the disk capacity.
- The desktop will be restarted during disk addition.
- Only one data disk can be added to a desktop pool at a time.
- The data disk size is 10 to 8200 GB (the value must be an integer multiple of 10).
- The maximum number of added data disks is 10 minus the number of existing data disks.

Step 5 Select **I understand the impact of this operation and are sure to add it**.

Step 6 Click **Next**.

Step 7 Confirm the information about the new disk and click **OK**.

----End

3.6 Expanding the Disk Capacity

Scenario

If the capacity of the system disk or data disk used for purchasing a desktop pool is insufficient, you can expand the disk capacity.

Expand the capacity of a system disk or data disk in a desktop pool.

Prerequisites

You can expand the capacity of a system disk or data disk only when the desktop pool is in the **Running** or **Stopped** status.

Procedure

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

Step 2 In the navigation pane, choose **Desktop Management** > **Desktop Pool**.

The **Desktop Pool** page is displayed.

Step 3 You can access the page for expanding the disk capacity of a desktop pool in either of the following ways:

Method 1:

Locate the row that contains the desktop pool in which disk capacity is to be expanded, click **More** > **Disk** > **Expand Disk** in the **Operation** column. The page for disk capacity expansion is displayed.

Method 2:

On the desktop pool page, click the name of the desktop pool whose disk capacity is to be expanded. The basic information page of the desktop pool is displayed.

Click **Expand** on the right of the **Disk Information** column in the desktop pool information. The page for disk capacity expansion is displayed.

Step 4 Select **System Disk** or **Data Disk** as required.

Step 5 (Optional) If there are multiple data disks, select the data disk to be expanded.

Step 6 Configure the **Add Capacity (GB)**.

NOTE

- The maximum capacity of a system disk is 1020 GB. The capacity of a desktop can only be a multiple of 10. That is, the capacity of a system disk can be expanded only to 1020 GB.
- The maximum capacity of a data disk is 8200 GB.

  The available capacity for expansion depends on on the initial data disk size.

  - If the initial data disk size is less than 1020 GB and the capacity of a desktop can only be a multiple of 10, the maximum data disk capacity is 1020 GB. The excess capacity cannot be used.

    If a data disk needs to be expanded to over 1020 GB, you must change the disk partition style from MBR to GPT (for details, see **Introduction to Data Disk Initialization Scenarios and Partition Styles**). During the change, services will be interrupted and the original data will be cleared. Therefore, back up the data before changing the partition style.
  - If the initial data disk size is greater than 1020 GB and the capacity of a desktop can be expanded only by a multiple of 10, the maximum data disk capacity is 8200 GB.

NOTE

- Only one disk can expand capacity in a desktop pool at a time.
- During disk capacity expansion, the latest expansion snapshot will be deleted. The snapshot generated during the capacity expansion will be automatically deleted seven days later.
- The desktop will be restarted during disk capacity expansion.
- After the capacity of a Linux EVS disk is expanded, the disk will not be partitioned by default. For details about how to partition the disk, see **Extending Partitions and File Systems for Data Disks (Linux)**.

Step 7 Select **I understand the impact of this operation and determine to expand the capacity**.

Step 8 Click **Next**.

Step 9 Confirm the information and click **OK**.

----End

3.7 Deleting Disks

Scenarios

If users' service volume changes, data disks are redundant, or they want temporary large-capacity disks that can be uninstalled and unsubscribe from after using them, you can delete a disk by referring to this section. After a data disk is deleted, the data on the disk is permanently deleted and cannot be restored. You are advised to delete a data disk only when the mapping between disk partitions and data disks can be determined. For example, you can delete data disks when there is only one data disk or data disks can be distinguished by disk capacity.

Prerequisites

- You have confirmed that the data on the user data disk is no longer used.

- The desktop has no running tasks.

Constraints

Unnecessary data disks can be deleted only from Windows desktop pools.

Procedure

Step 1 Log in to the console.

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

The **Desktop Pools** page is displayed.

Step 3 You can access the page for deleting disks of a desktop pool in either of the following ways:

Method 1:

Locate the row of the desktop pool whose disks are to be deleted, and click **More** > **Disk** > **Delete Disk** in the **Operation** column. The page for deleting disks is displayed.

Method 2:

On the desktop pool page, click the name of the desktop pool whose disks are to be deleted. The basic information page of the desktop pool is displayed.

Click **Delete** on the right of the **Disk Information** column in the desktop pool information. The page for deleting disks is displayed.

Step 4 Perform the corresponding operations based on the number of data disks to be deleted.

NOTICE

- The desktop will be restarted during disk deletion. Disk data will be permanently deleted and cannot be restored.
- Only one disk can be deleted from a desktop pool at a time.

Step 5 Select the data disk to be deleted, and select **I understand the impact and want to continue.**

Step 6 Confirm the deletion.

----End

3.8 Images

3.8.1 Creating an Image

3.8.1.1 Creating a Windows Desktop Image

Scenarios

If users have the same requirements on desktop pool configuration and application usage, you can purchase a desktop for a desktop pool generated using a Windows image on the Workspace console, log in to the desktop to configure settings and install software, and convert the desktop to an image. Then, use the image to purchase desktops in batches and assign them to the users. This feature reduces personnel configuration costs and is a turnkey solution.

NOTE

On the desktop to be converted to an image, files (including applications installed in this directory) in the user directory (**C:\Users\***Username of the current desktop*) of the current desktop cannot be added to the image. The configuration and applications of the desktop purchased using this image are inconsistent with those of the desktop to be converted to an image. Use the configuration and applications of the actual desktop that has been converted to an image.

Prerequisites

- A desktop generated using a Windows OS image is available.
- The desktop has been started and is in the **Running** status.
- You have logged in to the desktop in the desktop pool at least once.

  NOTE

  Images can be created only for desktops in a static desktop pool.

Procedure

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

NOTE

Select the region and project of the desktop to be converted to an image.

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

The **Desktop Pools** page is displayed.

Step 3 On the desktop pool page, click the name of the desktop pool in which an image is to be created. The basic information page of the desktop pool is displayed.

Step 4 Locate the row that contains the target desktop, click **More** in the **Operation** column, and select **Create Image**. The page for creating images is displayed.

Step 5 Configure image parameters as required, as shown in **Table 3-2**.

Table 3-2 Parameters

Parameter	Description	Example
Name	Image name. Configure this parameter as required. The value can contain only digits, letters, spaces, hyphens (-), underscores (_), and periods (.), and cannot start or end with a space.	temp_image-Windows private image
Description	Remarks about an image. Add remarks on the image usage.	-
Enterprise Project	You can use an enterprise project to centrally manage your cloud resources and members by project.	-
Agreement	Read *Statement of Commitment to Image Creation* and *Image Management Service Disclaimer*, and select **I have read and agree to *Statement of Commitment to Image Creation* and *Image Disclaimer***.	Selected

Step 6 If you want to perform this operation, enter **YES** or click **Auto Enter**.

Step 7 Click **OK**.

NOTE

- During image creation, the desktop is unavailable and will restart. Do not perform other operations.
- During image creation, all files in the desktop directory (**C:\Users\***current username*) will be deleted, and applications installed in this directory will be unavailable.
- If the response file (**c:\windows\system32\untitled.xml**) on which historical image encapsulation depends does not exist, contact the administrator.
- After the image is created, click ☰ on the console and choose **Service List** > **Compute** > **Image Management Service**. The created image is displayed in the **Private Images** list.

----End

3.8.2 Rebuilding a System Disk

Scenarios

If a purchased desktop pool needs to be restored to the initial template or desktop pool applications and patches need to be updated in batches, the administrator can rebuild or change the system disk.

Impact on the System

If you rebuild the system disk, the data (such as the desktop pool and favorites) on the system disk will be lost. If the data is needed after rebuilding the system disk, ask the user to back up the data in advance. Rebuilding the system disk does not affect data disks.

Constraints

When rebuilding the system disk, if the desktop pool uses a private image, ensure that the private image still exists.

Prerequisites

The system disk can be rebuilt only when the running status of a desktop pool is running or stopped.

Procedure

Step 1 Log in to the console.

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

The **Desktop Pools** page is displayed.

Step 3 You can access the page for rebuilding the system disk of a desktop pool in either of the following ways:

Method 1:

Locate the row that contains the desktop pool whose system disk is to be rebuilt, click **More** in the **Operation** column, and select **rebuild the OS**.

The dialog box of rebuilding a system disk is displayed.

Method 2:

On the desktop pool page, click the name of the desktop pool whose system disk is to be rebuilt. The basic information page of the desktop pool is displayed.

Click **Rebuild the system disk** on the right of the **Image** column in the desktop pool information. The dialog box of rebuilding a system disk is displayed.

Step 4 Configure the system disk to be rebuilt, as shown in Table 3-3.

Table 3-3 Basic configurations

Parameter	Description	Example
Reestablishment Mode	**Reinstall OS**: The original desktop image is used to rebuild the system disk.	Reinstall OS
OS	Select Windows or Linux as required.	Windows

Parameter	Description	Example
Rebuild Method	Determine when to start rebuilding the system disk after clicking **OK** in **Step 5**. ● **Immediately** ● **In 1 minute** ● **In 5 minutes** ● **In 10 minutes** ● **In 15 minutes**	Immediately
Notice Users	Select whether to notify users that the system disks of their desktops need rebuilding. After a user logs in, a notification message is displayed on the desktop.	Not notice
Notification Message	After selecting **Notice**, you can customize the content displayed in the pop-up window on the desktop.	-
To confirm the operation	Enter **YES** or click **Auto Enter**.	YES

Step 5 Click **OK** when rebuilding the system disk of one desktop, and click **OK** when rebuilding the system disks of multiple desktops.

Step 6 (Optional) Wait until the desktop status becomes **Running**. Contact the user to check and change the disk status of the desktop by referring to **How Do I Do If Data Disks of a Windows Desktop Cannot Be Found After Recomposing the System Disk?**

NOTE

This operation is needed only when you rebuild a Windows desktop.

----End

3.9 Changes and Fees

3.9.1 Renewal

Scenario

You can renew yearly/monthly-billed desktops in a desktop pool.

Procedure

Step 1 Log in to the console.

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

The **Desktop Pools** page is displayed.

Step 3 On the desktop pool page, click the name of the yearly/monthly-billed desktop pool. The basic information page of the desktop pool is displayed.

Step 4 Select the yearly/monthly-billed desktop in a desktop pool, and choose **More** > **Renew** above the desktop list or in the **Operation** column.

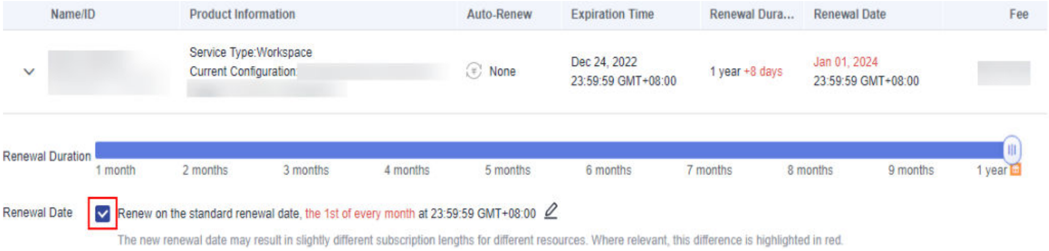
The **Renew** page is displayed.

Step 5 (Optional) Select **Renew on the standard renewal date**.

NOTE

You can click ✎ to reset the unified renewal date for resources.

Figure 3-1 Setting a unified renewal date



	Name/ID	Product Information	Auto-Renew	Expiration Time	Renewal Dura...	Renewal Date	Fee
⌄	[redacted]	Service Type:Workspace Current Configuration: [redacted]	None	Dec 24, 2022 23:59:59 GMT+08:00	1 year +8 days	Jan 01, 2024 23:59:59 GMT+08:00	[redacted]

Renewal Duration: 1 month, 2 months, 3 months, 4 months, 5 months, 6 months, 7 months, 8 months, 9 months, 1 year

Renewal Date ☑ Renew on the standard renewal date, the 1st of every month at 23:59:59 GMT+08:00 ✎

The new renewal date may result in slightly different subscription lengths for different resources. Where relevant, this difference is highlighted in red.

Step 6 Click **Pay**.

Step 7 Confirm the order, select a payment method, and pay the bill.

----End

3.9.2 Unsubscription

Scenarios

Unsubscribe from a desktop pool on the management console.

Procedure

Step 1 Log in to the console.

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

The **Desktop Pools** page is displayed.

Step 3 On the desktop pool page, click the name of the yearly/monthly-billed desktop pool. The basic information page of the desktop pool is displayed.

Step 4 Select the target yearly/monthly-billed desktop in a desktop pool, and choose **More** > **Unsubscribe** in the upper left corner of the desktop list or in the **Operation** column.

The desktop unsubscription page is displayed. Click **OK** to go to the resource unsubscription page.

NOTE

Unsubscribing from a desktop will also unsubscribe from its system disk. This operation cannot be undone, so exercise caution.

Step 5 On the resource unsubscription page, confirm the unsubscription information and provide the unsubscription reason, and check the box indicating that you understand that resources not in the recycle bin will be deleted immediately after unsubscription and cannot be restored, and that you have backed up data or no longer need the data. Then click **Confirm**.

NOTE

- When unsubscribing from a resource in use, confirm the resource information and refund information carefully. Resources cannot be restored after unsubscription. If you want to retain the resources and unsubscribe from only the unused renewal periods, **unsubscribe from the renewal periods**.
- For a non-five-day unconditional full refund (partial refund), handling fees and the amount consumed will be charged. The used cash coupons and discount coupons will not be refunded.

Step 6 Click **Unsubscribe** again.

NOTE

- Ensure that you have backed up or no longer need the data on the resources. After being unsubscribed from, the resources not in the recycle bin will be deleted immediately and their data cannot be restored.
- If you paid your order using a third-party payment platform, the refund will be added to your Huawei Cloud cash account.

----End

3.10 Desktop Pool Scaling Policies

Functions

Efficient utilization of desktop pool resources: time-based reuse and auto scaling

- *N*:*M* desktop solution: *N* users share *M* (a fixed number) desktops. Resources are reused through automatic scheduling.
- Dynamic binding: When a user logs in, an idle desktop will be assigned to them. When disconnecting from the desktop, the user is bound to the desktop within the retention period. The user will be automatically unbound from the desktop after the retention period expires, and the desktop status will be reset. Idle desktops will be bound to users with the retention period, and will be automatically deleted after the retention period expires.
- Reset: After a user is disconnected and unbound from a desktop, the desktop is automatically restored to the initial status to avoid data residue.
- Advantages: The desktop idle rate and purchase frequency are reduced. In particular, this solution is suitable for temporary desktop usage, such as Internet cafes and computer classrooms.

When a user logs in through the client, a desktop in the desktop pool will be automatically assigned to the user. After the user disconnects from the desktop, the desktop can be retained for a period of time. After the retention period expires, the user is automatically unbound from the desktop and the desktop will be reset. This enables automatic desktop scheduling. Users can manage desktops in a pool in a unified manner. Auto scaling improves desktop utilization and reduces costs. Features:

- Dynamic pool: Desktops are randomly assigned and reset after being released. Images can be updated in batches.
- Static pool: Users are fixed and desktops can be manually reset. Images can be updated in batches.
- Auto scaling policies can be flexibly defined to tackle request bursts.
- Desktop specifications in a desktop pool can be adjusted in a unified manner.
- Desktop scaling policies in a desktop pool can be configured in a unified manner.
- Using the same image and security policy, all desktops provide a consistent configuration and user experience.

Scaling Policies

The number of desktops in a desktop pool changes dynamically. You can add multiple end users to a desktop pool and set the minimum number of elastic desktops in a desktop pool. When creating or modifying a desktop pool, you can configure a scaling policy and change the minimum number of elastic desktops. Then desktops will be automatically created or released according to the user connection status and the configured scaling policy.

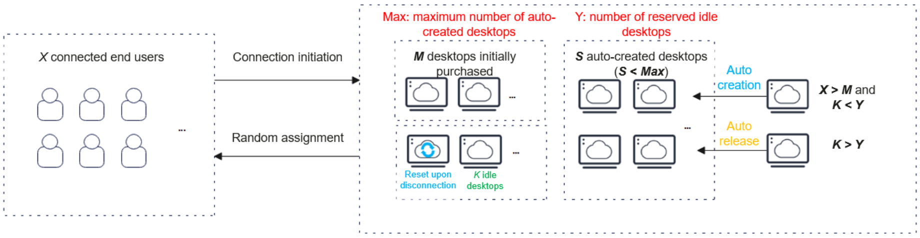
For example, in a three-shift customer service call center, there are 50 customer service representatives in a shift and 50 desktops are purchased. With the scale-out policy, more desktops can be added to ensure that the additional personnel for each shift have desktops to use. When these newly added desktops are no longer needed, they can be released through the scale-in policy.

Yearly/Monthly:

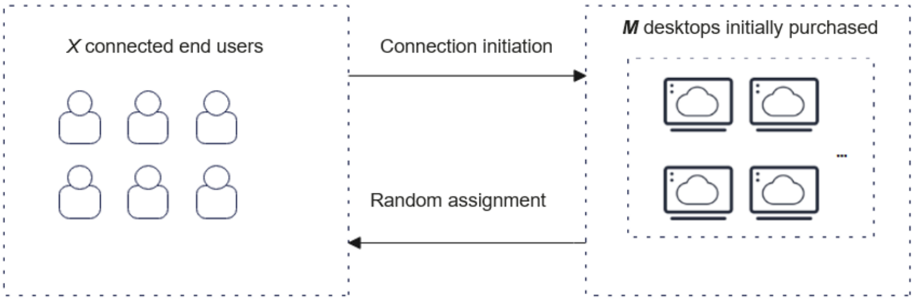
If the billing mode is yearly/monthly, you need to set the initial number of purchased desktops ($M \geq 1$). If you allow automatic desktop creation, set the maximum number of auto-created desktops. You can enable the scale-out policy to meet temporary additional requirements.

Dynamic pool:

- Enabling the scaling policy: Create *M* desktops, reserve *Y* idle desktops, set the maximum number of auto-created desktops to *Max*, and set the idle desktop retention period to *H* minutes. Then, desktops are automatically created according to the connection status of end users.
  - If reserved idle desktops are not used up, the number of desktops ranges from *M* to *M* + *Y*.
  - If reserved idle desktops are used up, new desktops will be automatically created. The number of desktops ranges from *M* to *M* + *Max*. When there are more than *Y* idle desktops, idle desktops can be released using the scale-in policy.

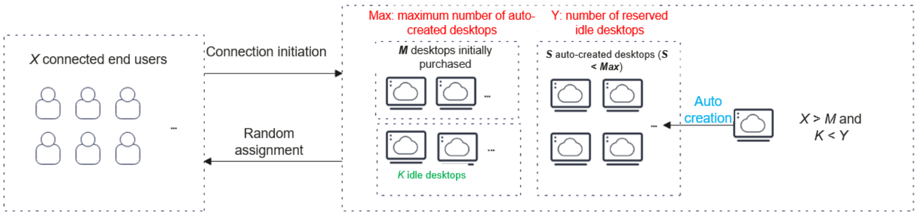


- Disabling the scaling policy:
  - If *M* desktops are created initially and no more desktops are created, the number of desktops is fixed to *M*.
  - If a desktop remains inactive for a period longer than the configured binding retention duration upon disconnection, the desktop will be reset.

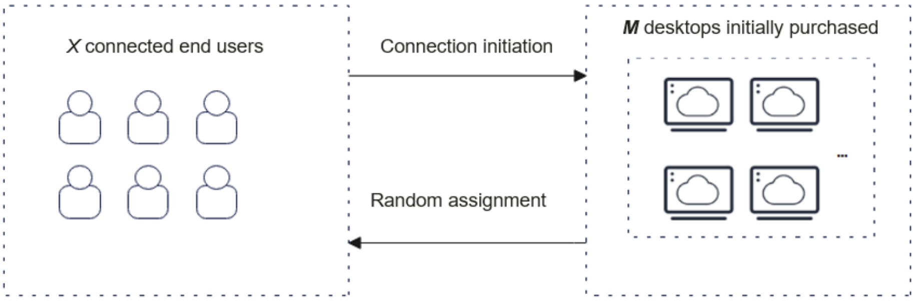


Static pool:

- Enabling the scale-out policy: Create *M* desktops, reserve *Y* idle desktops, and set the maximum number of auto-created desktops to *Max*. Then, desktops are automatically created according to the connection status of end users.
  - If reserved idle desktops are not used up, the number of desktops ranges from *M* to *M* + *Y*.
  - If reserved idle desktops are used up, new desktops will be automatically created. The number of desktops ranges from *M* to *M* + *Max*.


X connected end users
...
Connection initiation
Random assignment
Max: maximum number of auto-created desktops
Y: number of reserved idle desktops
M desktops initially purchased
...
K idle desktops
S auto-created desktops (S < Max)
...
Auto creation
X > M and K < Y

- Disabling the scale-out policy: If *M* desktops are created initially and no more desktops are created, the number of desktops is fixed to *M*.

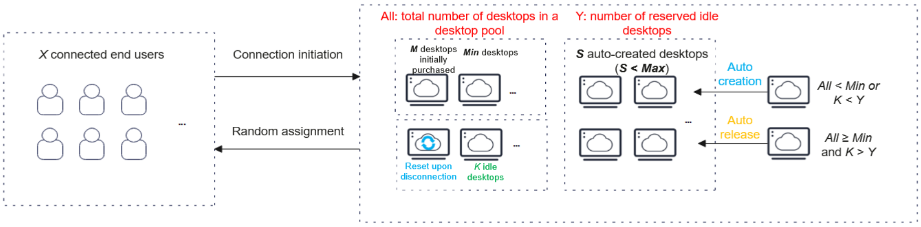


Pay-per-use:

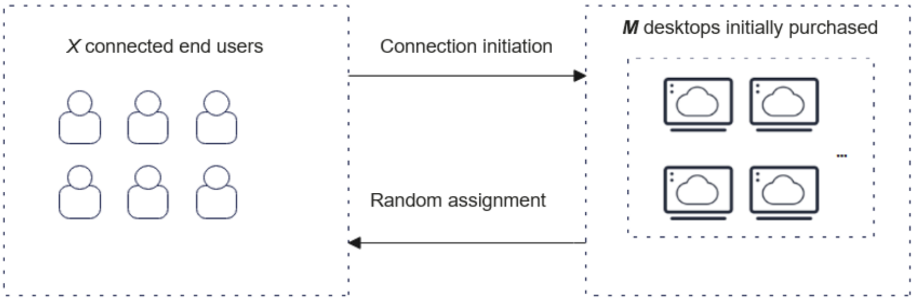
If the billing mode is pay-per-use, you need to set the initial number of purchased desktops ($M \geq 1$). If you allow automatic desktop creation, set the maximum number of auto-created desktops. You can enable the scaling policy to meet temporary requirements.

Dynamic pool:

- Enabling the scaling policy: Create *M* desktops, set the minimum number of desktops to *N*, reserve *Y* idle desktops, set the maximum number of auto-created desktops to *Max*, and set the idle desktop retention period to *H* minutes. Then, desktops are automatically created according to the connection status of end users.
  - If reserved idle desktops are not used up, the number of desktops ranges from *M* to *M* + *N*.
  - If reserved idle desktops are used up, new desktops will be automatically created. The number of desktops ranges from *M* to *M* + *Max*. When there are more than *Y* idle desktops, idle desktops can be released using the scale-in policy.

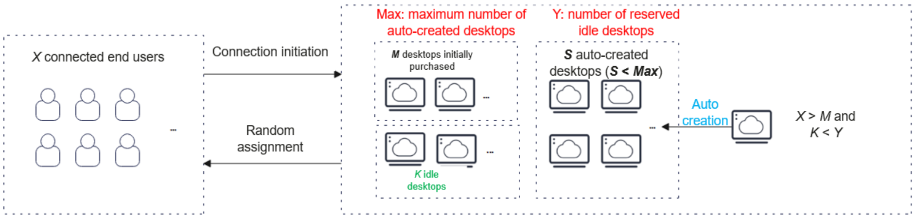

X connected end users
Connection initiation
Random assignment
All: total number of desktops in a desktop pool
Y: number of reserved idle desktops
M desktops initially purchased
Min desktops
Reset upon disconnection
K idle desktops
S auto-created desktops (*S* < *Max*)
Auto creation
Auto release
All < *Min* or *K* < *Y*
All ≥ *Min* and *K* > *Y*

- Disabling the scaling policy:
  - If *M* desktops are created initially and no more desktops are created, the number of desktops is fixed to *M*.
  - If a desktop remains inactive for a period longer than the configured binding retention duration upon disconnection, the desktop will be reset.

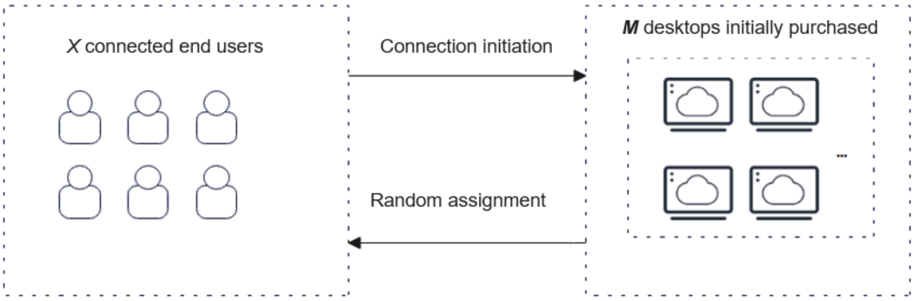


Static pool:

- Enabling the scale-out policy: Create *M* desktops, reserve *Y* idle desktops, and set the maximum number of auto-created desktops to *Max*. Then, desktops are automatically created according to the connection status of end users.
  - If reserved idle desktops are not used up, the number of desktops ranges from *M* to *M* + *Y*.
  - If reserved idle desktops are used up, new desktops will be automatically created. The number of desktops ranges from *M* to *M* + *Max*.


X connected end users
Connection initiation
Random assignment
Max: maximum number of auto-created desktops
Y: number of reserved idle desktops
M desktops initially purchased
K idle desktops
S auto-created desktops (S < Max)
Auto creation
X > M and K < Y

- Disabling the scale-out policy: If *M* desktops are created initially and no more desktops are created, the number of desktops is fixed to *M*.



NOTE

- You can configure the scaling policy for a dynamic pool:
  - You can configure the idle desktop reservation duration. If the reservation duration expires, idle desktops will be automatically deleted.
  - If a user is disconnected from a desktop, the desktop will be automatically unbound from the user and released after the reservation duration upon disconnection expires.
- The minimum number of desktops can be set only for dynamic pay-per-use desktop pools.
- If the scaling policy is not enabled, set the number of initially purchased desktops to a proper value to ensure user experience. If all resources are occupied, users cannot connect to desktops.
- The number of desktops is not fixed. Desktops will be automatically automatically created or released according to the scaling policy and user connection status. As a result, some users may not have desktops available.

Desktop Assignment in a Desktop Pool

Desktops in a desktop pool are not permanently bound to users. You can add multiple users as needed. Desktops will be automatically assigned to users according to their connection status. The following tables show the assignment mechanisms for different billing modes and auto scaling policies:

Table 3-4 Yearly/Monthly billing

Method	Scaling Policy	Pool Type	User Connection Status	Connection Initiation	Idle Desktop Reservation	Unbinding upon Disconnection
Dynamic scaling	Scaling policy enabled	Dynamic pool	Number of connected users ≤ Number of reserved idle desktops	A reserved yearly/monthly desktop is assigned.	Example: The idle desktop reservation duration is set to 20 minutes. Idle desktops can be connected to and used within 20 minutes. Then they will be automatically deleted.	Example: The reservation duration upon disconnection is set to 10 minutes. Desktops can be reconnected to and used within 10 minutes. Then they will be automatically unbound from the users and reset.
			Maximum number of auto-created desktops ≥ Number of connected users > Number of reserved idle desktops	A pay-per-use auto-created desktop is assigned.	Example: The idle desktop reservation duration is set to 20 minutes. Idle desktops can be connected to and used within 20 minutes. Then they will be automatically deleted.	Example: The reservation duration upon disconnection is set to 10 minutes. Desktops can be reconnected to and used within 10 minutes. Then they will be automatically unbound from the users and reset.

Method	Scaling Policy	Pool Type	User Connection Status	Connection Initiation	Idle Desktop Reservation	Unbinding upon Disconnection
			Number of connected users > Maximum number of auto-created desktops	No desktop is assigned, and a message is displayed indicating insufficient desktop pool resources.	N/A	N/A
	Scale-out policy enabled	Static pool	Number of connected users ≤ Number of reserved idle desktops	A reserved yearly/monthly desktop is assigned.	N/A	N/A

Method	Scaling Policy	Pool Type	User Connection Status	Connection Initiation	Idle Desktop Reservation	Unbinding upon Disconnection
			Maximum number of auto-created desktops ≥ Number of connected users > Number of reserved idle desktops	A pay-per-use auto-created desktop is assigned.	N/A	N/A
			Number of connected users > Maximum number of auto-created desktops	No desktop is assigned, and a message is displayed indicating insufficient desktop pool resources.	N/A	N/A

Method	Scaling Policy	Pool Type	User Connection Status	Connection Initiation	Idle Desktop Reservation	Unbinding upon Disconnection
Creation upon access	N/A	Dynamic pool	Number of connected users ≤ Initial purchase quantity	A yearly/monthly desktop is assigned.	Example: The idle desktop reservation duration is set to 20 minutes. Idle desktops can be connected to and used within 20 minutes. Then they will be automatically deleted.	Example: The reservation duration upon disconnection is set to 10 minutes. Desktops can be reconnected to and used within 10 minutes. Then they will be automatically unbound from the users and reset.
			Initial purchase quantity < Number of connected users < Maximum number of auto-created desktops	A pay-per-use auto-created desktop is assigned.	Example: The idle desktop reservation duration is set to 20 minutes. Idle desktops can be connected to and used within 20 minutes. Then they will be automatically deleted.	Example: The reservation duration upon disconnection is set to 10 minutes. Desktops can be reconnected to and used within 10 minutes. Then they will be automatically unbound from the users and reset.

Method	Scaling Policy	Pool Type	User Connection Status	Connection Initiation	Idle Desktop Reservation	Unbinding upon Disconnection
			Number of connected users > Maximum number of auto-created desktops	No desktop is assigned, and a message is displayed indicating insufficient desktop pool resources.	N/A	N/A
		Static pool	Number of connected users ≤ Initial purchase quantity	A yearly/monthly desktop is assigned.	N/A	N/A

Method	Scaling Policy	Pool Type	User Connection Status	Connection Initiation	Idle Desktop Reservation	Unbinding upon Disconnection
			Maximum number of auto-created desktops ≥ Number of connected users > Initial purchase quantity	A pay-per-use auto-created desktop is assigned.	N/A	N/A
			Number of connected users > Maximum number of auto-created desktops	No desktop is assigned, and a message is displayed indicating insufficient desktop pool resources.	N/A	N/A

Table 3-5 Pay-per-use

Method	Scaling Policy	Pool Type	User Connection Status	Connection Initiation	Idle Desktop Reservation	Unbinding upon Disconnection
Dynamic scaling	Scaling policy enabled	Dynamic pool	Number of connected users ≤ Number of reserved idle desktops	A reserved pay-per-use desktop is assigned.	Example: The idle desktop reservation duration is set to 20 minutes. Idle desktops can be connected to and used within 20 minutes. Then they will be automatically deleted.	Example: The reservation duration upon disconnection is set to 10 minutes. Desktops can be reconnected to and used within 10 minutes. Then they will be automatically unbound from the users and reset.
			Minimum number of desktops > Number of connected users > Number of reserved idle desktops	A pay-per-use desktop is assigned.	Example: The idle desktop reservation duration is set to 20 minutes. Idle desktops can be connected to and used within 20 minutes. Then they will be automatically deleted.	Example: The reservation duration upon disconnection is set to 10 minutes. Desktops can be reconnected to and used within 10 minutes. Then they will be automatically unbound from the users and reset.

Method	Scaling Policy	Pool Type	User Connection Status	Connection Initiation	Idle Desktop Reservation	Unbinding upon Disconnection
			Maximum number of auto-created desktops > Number of connected users > Minimum number of desktops	A pay-per-use auto-created desktop is assigned.	Example: The idle desktop reservation duration is set to 20 minutes. Idle desktops can be connected to and used within 20 minutes. Then they will be automatically deleted.	Example: The reservation duration upon disconnection is set to 10 minutes. Desktops can be reconnected to and used within 10 minutes. Then they will be automatically unbound from the users and reset.

Method	Scaling Policy	Pool Type	User Connection Status	Connection Initiation	Idle Desktop Reservation	Unbinding upon Disconnection
			Number of connected users > Maximum number of auto-created desktops	No desktop is assigned, and a message is displayed indicating insufficient desktop pool resources.	N/A	N/A
	Scale-out policy enabled	Static pool	Number of connected users ≤ Number of reserved idle desktops	A reserved pay-per-use desktop is assigned.	N/A	N/A

Method	Scaling Policy	Pool Type	User Connection Status	Connection Initiation	Idle Desktop Reservation	Unbinding upon Disconnection
			Maximum number of auto-created desktops ≥ Number of connected users > Number of reserved idle desktops	A pay-per-use auto-created desktop is assigned.	N/A	N/A
			Number of connected users > Maximum number of auto-created desktops	No desktop is assigned, and a message is displayed indicating insufficient desktop pool resources.	N/A	N/A

Method	Scaling Policy	Pool Type	User Connection Status	Connection Initiation	Idle Desktop Reservation	Unbinding upon Disconnection
Creation upon access	N/A	Dynamic pool	Number of connected users ≤ Initial purchase quantity	A pay-per-use desktop is assigned.	Example: The idle desktop reservation duration is set to 20 minutes. Idle desktops can be connected to and used within 20 minutes. Then they will be automatically deleted.	Example: The reservation duration upon disconnection is set to 10 minutes. Desktops can be reconnected to and used within 10 minutes. Then they will be automatically unbound from the users and reset.
			Initial purchase quantity < Number of connected users < Maximum number of auto-created desktops	A pay-per-use auto-created desktop is assigned.	N/A	N/A

Method	Scaling Policy	Pool Type	User Connection Status	Connection Initiation	Idle Desktop Reservation	Unbinding upon Disconnection
			Number of connected users > Maximum number of auto-created desktops	No desktop is assigned, and a message is displayed indicating insufficient desktop pool resources.	N/A	N/A
		Static pool	Number of connected users ≤ Initial purchase quantity	A pay-per-use desktop is assigned.	N/A	N/A

Method	Scaling Policy	Pool Type	User Connection Status	Connection Initiation	Idle Desktop Reservation	Unbinding upon Disconnection
			Initial purchase quantity < Number of connected users < Maximum number of auto-created desktops	A pay-per-use auto-created desktop is assigned.	N/A	N/A
			Number of connected users > Maximum number of auto-created desktops	No desktop is assigned, and a message is displayed indicating insufficient desktop pool resources.	N/A	N/A

Managing Scaling Policies

You can manage the scaling policies of created desktop pools. If the existing scaling policies are insufficient, you can modify them to meet your needs.

Modifying a scaling policy

Step 1 Log in to the console.

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

The **Desktop Pools** page is displayed.

Step 3 Click the name of a desktop pool to go to its basic information page.

Step 4 Click ✎ next to **Scaling Policy** to go to the **Modify Scaling Policy** page.

Step 5 You can enable or disable the scaling policy and change the method as needed.

Step 6 Click **OK**.

----End

4 Users

4.1 Creating a User

Scenarios

This section describes how to add a user on the console and assign desktops to the user.

NOTE

- When the exiting AD domain is used, before creating a user, you need to create a user on the AD server.
- If you need to create a user in the multi-domain scenario, you need to create another user on the corresponding AD domain server.

Procedure

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

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

The **Users** page is displayed.

Step 3 Click **Create User**.

The **Create User** page is displayed.

Step 4 Enter the user information, as shown in **Table 4-1**.

Table 4-1 Creating a user

Creating a User	Parameter	Operation
User Activation	● **By users** – You need to enter the username, email address, or mobile number. After the user is created, the system sends the user login information (access address, enterprise ID, username, and password) to the email address or mobile number. ● **By administrators** – Enter the username and password. Keep the password secure. **NOTE** 1. If there is no AD, you need to enter the username and password. 2. If there is an AD, you do not need to enter the password. The entered username must be the same as that on the Windows AD server.	Select an activation method as required.

Creating a User	Parameter	Operation
By users > **Manually**	● The username is used for user authentication during desktop login. Naming rules: – A name can contain 1 to 32 characters. – A digit-only name is allowed. – Only letters, digits, and three types of special characters (-_.) are allowed. The value must start with a letter or digit and cannot end with a period (.) or underscore (_). – This field cannot be left blank. ● The email address is used to receive desktop provisioning emails and related notifications. Email address verification rules: – Enter a valid email address through system verification. – The value can contain a maximum of 64 characters. ● The mobile number is used to receive SMS messages about desktop provisioning and related notifications. Mobile number verification rules: – [+][*Country/Region code*][*Mobile number*] – For a mobile number of your country/region, you can omit [+][*Country/Region code*] and directly enter the mobile number. – A mobile number can contain spaces, slashes (/), and hyphens (-).	1. Set **User Activation** to **By users**. 2. Set **User Import** to **Manually**. 3. Set the username, enter the email address, mobile number, and description as required, and set the account expiration time. 4. Select the required enterprise project from the **Enterprise Project** drop-down list. 5. Select the required domain from the drop-down list. 6. Click **Add User**. **NOTE** Enter an email address or a mobile number, or both.

Creating a User	Parameter	Operation
By administrators > **Manually**	● The username is used for user authentication during desktop login. Naming rules: – A name can contain 1 to 32 characters. – A digit-only name is allowed. – Only letters, digits, and three types of special characters (-_.) are allowed. The value must start with a letter or digit and cannot end with a period (.) or underscore (_). – This field cannot be left blank. ● The initial password is authenticated when a user logs in to the desktop. Keep the initial password secure. – The password contains 8 to 32 characters. – The value can contain uppercase letters, lowercase letters, digits, and special characters !@$%^-_=+[{}]:,./? – The password cannot be the username or the reverse username. ● The email address is used to receive desktop provisioning emails and related notifications. Email address verification rules: – Enter a valid email address through system verification. – The value can contain a maximum of 64 characters. ● The mobile number is used to receive SMS messages about desktop provisioning and related notifications. Mobile number verification rules: – [+][*Country/Region code*][*Mobile number*] – For a mobile number of your country/region, you can omit [+][*Country/Region code*] and directly enter the mobile number. – A mobile number can contain spaces, slashes (/), and hyphens (-).	1. Set **User Activation** to **By administrators**. 2. Set **User Import** to **Manually**. 3. Set the username and initial password, enter the mobile number, email address, and description as required, and set the account expiration time. **NOTE** If the Windows AD is interconnected, you do not need to enter the password. 1. Select the required enterprise project from the **Enterprise Project** drop-down list. 2. Select the required domain from the drop-down list. 3. Click **Add User**.

Creating a User	Parameter	Operation
By users > **Batch**	- Upload all user information recorded in the table and create users in batches.	1. Click **Download Template** on the right of **Import user information** to download the user list template. 2. Enter the No., username, password (only for **By administrators**), domain (AD domain where the user is located. If this parameter is not set, the primary domain is used by default), email, mobile number and area code, expiration time, enterprise ID, and description in the table. 3. Click **Upload** to upload the user list that has been filled in. 4. Confirm the creation. **NOTE** The size of the file to be uploaded cannot exceed 1 MB. A maximum of 200 records can be uploaded at a time. Only .xlsx and .xls files are supported.
By administrators > **Batch**	- Upload all user information recorded in the table and create users in batches.	

----End

4.2 Importing a User

Scenarios

Batch import users in the OUs of an AD server to the user management page on the console.

NOTE

- Users in the OUs of an AD server can be batch imported only when the AD server is connected.
- A maximum of 1,000 users under an OU can be imported at a time.

Procedure

Step 1 Log in to the console.

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

The **Users** page is displayed.

Step 3 Click **Importing Users**.

The **Importing Users** dialog box is displayed.

Step 4 Select the OU to be imported from the drop-down list and enter the description.

Step 5 Select the required enterprise project from the **Enterprise Project** drop-down list.

In the user list, you can filter user information by **Username** and **Importable**.

Step 6 Click **OK**.

----End

4.3 Subscribing to Collaboration for a User

Scenarios

After subscribing to collaboration, users can quickly initiate collaboration between desktops, improving communication and collaboration efficiency.

Procedure

Step 1 Log in to the console.

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

The **Users** page is displayed.

Step 3 Select the users for whom you want to subscribe to collaboration and click **Subscribe to Collaboration**.

Step 4 On the page displayed, select the required enterprise project from the **Enterprise Project** drop-down list.

Step 5 Confirm the users and subscription fee, and click **Confirm**. The **Cloud Service Orders** page is displayed.

Step 6 Check the cloud service order and the fee to be paid.

Step 7 After the payment method is selected and the payment is successful, the subscription is complete.

----End

4.4 Modifying User Information

Scenarios

When the exiting AD domain is not used, the administrator can modify user information on the console when the user information is incorrect or changed.

NOTE

If an enterprise has an AD domain, only the email address and mobile number can be modified. User information such as the description, account options, and account expiration cannot be modified.

Prerequisites

A user has been created.

Procedure

Step 1 Log in to the console.

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

The **Users** page is displayed.

Step 3 In the **Operation** column of the user whose information is to be modified, click **Edit**.

The page for modifying user information is displayed.

Step 4 Select **By users** or **By administrators** for **User Activation**.

Step 5 You can modify the email address, mobile number, description, account expiration, and account options.

- **User Info**
  - Email: used to receive emails about desktop provisioning and related notifications
  - Mobile number: used to receive SMS messages about desktop provisioning and related notifications
- **Account Expiration**
  - **Never expires**: The account is permanently valid.
  - **After this date**: If the expiration date is set, the user account expires after this date.
- **Account Options**
  - **Change password upon the next login**: Users need to change the password upon the next desktop login.
  - **Cannot change password**: Only the administrator can reset the user password for desktop login.
  - **Password never expires**: The password is permanently valid.
  - **Account disabled**: Users cannot use disabled accounts for desktop login.

Step 6 Click **OK**.

----End

4.5 Resetting a User Password

Scenarios

If an enterprise AD domain is not used and a user loses or forgets the login password, the administrator can reset the password for the user on the console.

NOTE

- Password resetting is risky. After being reset, the original password cannot be used. Confirm that the operation is necessary.
- If an enterprise AD domain is used, the password needs resetting on the AD server.

Prerequisites

A user has been created.

Procedure

Step 1 Log in to the console.

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

The **Users** page is displayed.

Step 3 Locate the row of the user whose password is to be reset. Click **More** > **Reset Password** in the **Operation** column.

Step 4 Choose email or mobile phone for receive passwords.

NOTE

- If you enter only the email address or mobile number when creating a user, the option you entered will be selected by default on the password resetting page, and the other option will be unavailable by default.
- If you enter both the email address and mobile number when creating a user, **Email** is selected by default and **Mobile Number** is optional on the password resetting page.

Step 5 Confirm the password resetting and click **OK**.

NOTICE

An email address can receive a maximum of five password resetting emails a day. The validity period of the password resetting link in the email is 24 hours. Reset the password in time.

----End

4.6 Unlocking an Account

Scenarios

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

NOTE

- If an enterprise AD domain is used, the administrator needs to unlock the account on the AD server.
- Only locked accounts can be unlocked.

Procedure

Step 1 Log in to the console.

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

The **Users** page is displayed.

Step 3 In the **Operation** column of the user to be unlocked, choose **More** > **Unlock a User**.

The page for unlocking a user is displayed.

Step 4 Click **OK**.

----End

4.7 Resending a Notification Email

Scenarios

If a user already has a desktop and needs to receive a notification email again, the administrator can resend the notification email on the console.

Procedure

Step 1 Log in to the console.

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

The **Users** page is displayed.

Step 3 Locate the row of the desired user. Click **More** in the **Operation** column and select **Resend Notification**.

The page for resending a notification is displayed.

Step 4 Click **OK**.

----End

4.8 Deleting a User

Scenarios

The administrator can delete an account on the console.

NOTE

- In the AD scenario, deleting a user does not delete the user from the AD server.
- Users who have desktops cannot be deleted.

Prerequisites

A user has been created.

Procedure

Step 1 Log in to the console.

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

The **Users** page is displayed.

Step 3 In the **Operation** column of the user to be deleted, choose **More** > **Delete**.

To delete multiple users, select the users to be deleted and click **Delete** in the upper left corner of the page.

The page for deleting users is displayed.

Step 4 If you want to perform this operation, enter **DELETE** or click **Auto Enter**.

Step 5 Click **OK**.

----End

4.9 Exporting a User

Scenarios

Administrators can export users on the management console.

Procedure

Step 1 Log in to the console.

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

The **Users** page is displayed.

Step 3 Select the users to be exported and click **Export** in the upper left corner of the page.

View the exported Excel file on the local PC.

----End

4.10 Managing MFA Devices

Scenario

The administrator enables the Huawei Cloud multi-factor authentication service. After an end user binds a virtual MFA device on the client and logs in to a desktop using a dynamic verification code, a binding record is generated under **Manage MFA Devices** on the console. The record shows the bound username, binding time, and device status.

Prerequisites

- The Huawei Cloud multi-factor authentication service has been enabled. See **8.2.2.1 Huawei Cloud Multi-Factor Authentication Service (Virtual MFA)**.
- After binding a virtual MFA device on the client, an end user can log in to a desktop using the dynamic verification code.

Procedure

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 Click **More** > **Manage MFA Devices** in the **Operation** column.

The **Manage MFA Devices** dialog box is displayed.

Step 4 You can check the bound username, binding time, and device status.

NOTE

- Clicking **Delete** in the **Operation** column of the binding record will delete the bound user information. In this case, the end user needs to bind the virtual MFA device again on the client and log in to the desktop using a dynamic verification code. A new binding record will be generated under **Manage MFA Devices** on the console.
- After the binding record is deleted from the MFA device, the end user needs to bind the virtual MFA device again when logging in.

----End

5 User Groups

5.1 Creating a User Group

Scenarios

Administrators can create user groups on the management console to manage users by group.

NOTICE

When the existing AD domain of an enterprise is used, you can create common user groups and AD user groups. If the enterprise is not connected to the AD domain, only common user groups can be created by default.

Procedure

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

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

The **User Group** page is displayed.

Step 3 Click **Creating a user group** in the upper right corner of the page.

The **Creating a user group** dialog box is displayed.

Step 4 Set **User group name**, **User group type**, and **Description** as required.

- **User group name**: Create a user group to manage desktop users.
  - The value can contain uppercase letters, lowercase letters, digits, hyphens (-), and underscores (_).
  - This field cannot be left blank.
  - The value can contain a maximum of 64 characters.
- **User group type**
  - **AD user group**: user group for interconnecting with the enterprise AD, which applies to the scenario where user permissions are managed using the enterprise AD user group.
  - **Common user group**: the user group management system provided by Workspace, which provides batch user management capabilities and applies to scenarios where interconnection with AD user groups is not required.

Step 5 Click **OK**.

----End

5.2 Adding a User to a User Group

Scenarios

To facilitate user management, the administrator can add users to a user group.

NOTE

- When an AD domain is interconnected with, users cannot be added to AD user groups, and can only be added to user groups.
- You can add users from different domains to the same user group.
- After a user group is authorized to use a desktop pool, if users are added to the user group, the desktop pool is not visible in the desktop list on the terminal of a user who has logged in. It will become visible only when the user logs in again.

Prerequisites

A user group has been created.

Procedure

Step 1 Log in to the console.

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

The **User Groups** page is displayed.

Step 3 Click a user group name in the user group list.

The user group information page is displayed.

Step 4 Click **Add**.

The page for adding a user is displayed.

Step 5 Enter a username in the **Available Users** text box or select the usernames to be added in the **Available** list.

Step 6 Click **OK**.

----End

5.3 Removing a User from a User Group

Scenarios

The administrator can remove a user from a user group on the console.

NOTE

- In a project interconnected with an AD domain, users cannot be removed from an AD user group, and can only be removed from a common user group.
- After a user group is assigned to a desktop or desktop pool, to remove a user from the user group, the user needs to log out and then log in again for the removal to take effect.

Prerequisites

There are users in a user group.

Procedure

Step 1 Log in to the console.

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

The **User Groups** page is displayed.

Step 3 Click a user group name in the user group list.

The user group information page is displayed.

Step 4 On the user group information page, you can choose to remove one or multiple users.

- Removing one user
  a. Click **Remove** in the **Operation** column of the desired user. The page for removing a user is displayed.
  b. If you want to perform this operation, enter **REMOVE** or click **Auto Enter**.
  c. Click **OK**.
- Removing multiple users
  a. Select the users to be removed and click **Remove** above the user list. The page for removing users is displayed.
  b. If you want to perform this operation, enter **REMOVE** or click **Auto Enter**.
  c. Click **OK**.

----End

5.4 Modifying a User Group

Scenarios

To facilitate user group management, the administrator can modify user group information on the console.

NOTE

If the user group type is AD user group, the user group name cannot be changed. Only the description of the user group can be modified.

Prerequisites

A user group has been created.

Procedure

Step 1 Log in to the console.

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

The **User Groups** page is displayed.

Step 3 You can modify user group information in either of the following ways:

- Method 1: Click **Edit** in the **Operation** column on the right of the desired user group. The page for modifying user group information is displayed.

  Modify the user group name and description as required, and click **OK**.
- Method 2: Click a user group name in the user group list. The user group information page is displayed.

  You can modify the user group name and description as required.
  - **User Group Name**

    Click ✎ on the right of the user group name to change the user group name. Then click ✓.
  - **Description**

    Click ✎ to modify the description. Then click ✓.

----End

5.5 Deleting a User Group

Scenarios

The administrator can delete a specified user group on the management console.

Prerequisites

A user group has been created.

Procedure

Step 1 Log in to the console.

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

The **User Groups** page is displayed.

Step 3 On the **User Groups** page, you can choose to delete one or multiple user groups.

- Deleting one user group
  - Method 1:
    1. Click **Delete** in the **Operation** column of the desired user group. The page for deleting a user group is displayed.
    2. If you want to perform this operation, enter **DELETE** or click **Auto Enter**.
    3. Click **OK**.
  - Method 2:
    1. Click the name of the user group to be deleted. The user group information page is displayed.
    2. Click **Delete** in the upper right corner of the user group information page.
    3. In the displayed dialog box, click **OK**.
- Deleting multiple user groups

  a. Select the user groups to be deleted in batches and click **Delete** above the user group list. The page for deleting user groups is displayed.

  b. If you want to perform this operation, enter **DELETE** or click **Auto Enter**.

  c. Click **OK**.

----End

6 Policy Management

By configuring policies, end user desktops can implement different capabilities, such as the permission control on data transmission and peripheral access.

Policies are classified into common policies that meet common office requirements and advanced policies that are customized for special scenarios.

6.1 Protocol Policy Management

6.1.1 Creating a Policy

6.1.1.1 Creating a General Policy

Scenarios

General policies can meet routine office requirements. You can deliver general policies on the console, such as USB port redirection, file redirection, and printer redirection policies, to manage end users' access to cloud desktops, data security, peripheral compatibility, and performance.

Prerequisites

You have purchased a desktop.

Procedure

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

Step 2 Choose **Policies** > **Protocol Policies**. The **Protocol Policies** page is displayed.

Step 3 Click **Create Policy**.

Step 4 Enter the policy name and description.

NOTE

- The policy name can contain up to 55 characters in digits, letters, and underscores (_).
- The description can contain up to 255 characters.

Step 5 Select a creation mode as required.

- **Create without template**: Create a policy using the default blank template.
- **Create with template**: Create a policy using an existing policy template, whose configuration items will be used by default.

  NOTE

  You can select an existing policy template or add a custom template.

  The system provides four policy templates to help you quickly configure desktop policies in four different scenarios.

  - In security scenarios, Huawei Delivery Protocol (HDP) prevents data in a desktop from being transferred to or even stored on personal storage devices and ensures that data is stored only in an on-premises data center.
  - In gaming scenarios, cursor follow-up and image display are optimized to ensure smoothness even in poor bandwidth conditions.
  - In graphics processing scenarios, the display frame rate can be adjusted to improve the display quality and the cursor follow-up mode can be adjusted to narrow the gap between the cursor and the image and reduce the visual difference.
  - In video editing scenarios, video acceleration is used to optimize video playback quality. The cursor closely follows user operations, improving user experience.
- **Use existing policy**: If a policy group has been created, you can import a policy from the existing policy group. The configuration items of the selected policy will be used by default.

Step 6 Click **Next: Configure Policy**. The **General Policy Configuration** page is displayed.

Step 7 On the displayed page, configure application policies for the VM as required.

NOTE

General policies are simplified from advanced policies and can meet routine office requirements. By default, policy parameters that meet routine office requirements are enabled.

- ● indicates that the policy is enabled.
- ○ indicates that the policy is disabled.

For details about configuring a general policy, see **Table 6-1**.

Table 6-1 Policy management

Type	Parameter	Description
USB Port Redirection	Graphics devices (such as scanners)	Supports USB peripherals on Workspace. Users can use devices in VMs through USB port redirection.
	Video devices (such as cameras)	

Type	Parameter	Description
	Printers	
	Storage devices (such as USB flash drives)	
	Smart card devices (such as Ukeys)	
File Redirection	Fixed driver	● **Read-only**: Files in drivers and storage devices can only be pre-viewed. ● **Read/Write**: Files in drivers and storage devices can be modified. Supports drivers on Workspace. Users can use drivers in VMs through file redirection.
	Removable driver	
	CD/DVD-ROM driver	
	Network driver	
Clipboard Redirection	Bidirectional	After this function is enabled, end users can copy data on cloud desktops and paste the data on local desktops, or copy data on local desktops and paste the data on cloud desktops.
	Server to client	After this function is enabled, end users can only copy data on cloud desktops and paste the data on local desktops.
	Client to server	After this function is enabled, end users can only copy data on local desktops and paste the data on cloud desktops. **NOTE** Files can be copied only from a Windows client to a server, and file redirection and the corresponding driver must be enabled.
Printer Redirection	-	Users can use printers connected to TCs.
Rendering Acceleration **NOTE** This option only applies to video editing.	Visual quality first	The visual quality is excellent and the bandwidth usage is high (25 Mbit/s). The parameter details cannot be edited by default.
	Smoothness first	The visual quality and bandwidth usage are balanced (20 Mbit/s). The parameter details cannot be edited by default.

Type	Parameter	Description
	Level 1 **NOTE** The **HDP Plus** parameter can be customized for adaptation.	The bandwidth (kbit/s) ranges from 256 to 25,000. **NOTE** This parameter specifies the limit of the display stream data. Increasing the value of this parameter improves user experience but consumes more network bandwidth. If the network bandwidth is insufficient, increasing the value of this parameter will compromise smoothness. In this case, you are advised to use the default value.
		Display Frame Rate (FPS): 1–60 **NOTE** This parameter specifies the display frame rate when no video is played. Increasing the value improves display smoothness but consumes more bandwidth resources. If the network bandwidth is insufficient, increasing the value of this parameter will compromise smoothness. In this case, you are advised to use the default value.
		Video Frame Rate (FPS): 1–60 **NOTE** This parameter specifies the frame rate of video display. Increasing the value improves display smoothness but consumes more bandwidth resources. If the network bandwidth is insufficient, increasing the value of this parameter will compromise smoothness. In this case, you are advised to use the default value.
		Lossy Compression Recognition Threshold: 0–255 **NOTE** This parameter is used to adjust static image quality. A smaller value indicates higher quality but higher bandwidth usage and lower smoothness.
		Lossy Compression Quality: 20–100 **NOTE** This parameter is used to adjust static natural image quality. A larger value indicates higher quality but higher bandwidth usage and lower smoothness.

Step 8 Click **Next: Select Target Object**.

Step 9 Select an object type as required and then select an object.

Step 10 Click **Next: Finish**.

The policy has been created and will take effect upon the next login to the desktop.

----End

6.1.1.2 Creating an Advanced Policy

Scenarios

General policies can meet daily office requirements. You can customize advanced policies for special scenarios.

Prerequisites

You have purchased a desktop.

Procedure

Step 1 Log in to the console.

Step 2 Choose **Policies** > **Protocol Policies**. The **Protocol Policies** page is displayed.

Step 3 Click **Create Policy**.

Step 4 Enter the policy name and description.

NOTE

- The policy name can contain up to 55 characters in digits, letters, and underscores (_).
- The description can contain up to 255 characters.

Step 5 Select a creation mode as required.

- **Create without template**: Create a policy using the default blank template.
- **Create with template**: Create a policy using an existing policy template, whose configuration items will be used by default.

  NOTE

  You can select an existing policy template or add a custom template.

  The system provides four policy templates to help you quickly configure desktop policies in four different scenarios.

  - In security scenarios, Huawei Delivery Protocol (HDP) prevents data in a desktop from being transferred to or even stored on personal storage devices and ensures that data is stored only in an on-premises data center.
  - In gaming scenarios, cursor follow-up and image display are optimized to ensure smoothness even in poor bandwidth conditions.
  - In graphics processing scenarios, the display frame rate can be adjusted to improve the display quality and the cursor follow-up mode can be adjusted to narrow the gap between the cursor and the image and reduce the visual difference.
  - In video editing scenarios, video acceleration is used to optimize video playback quality. The cursor closely follows user operations, improving user experience.
- **Use existing policy**: If a policy group has been created, you can import a policy from the existing policy group. The configuration items of the selected policy will be used by default.

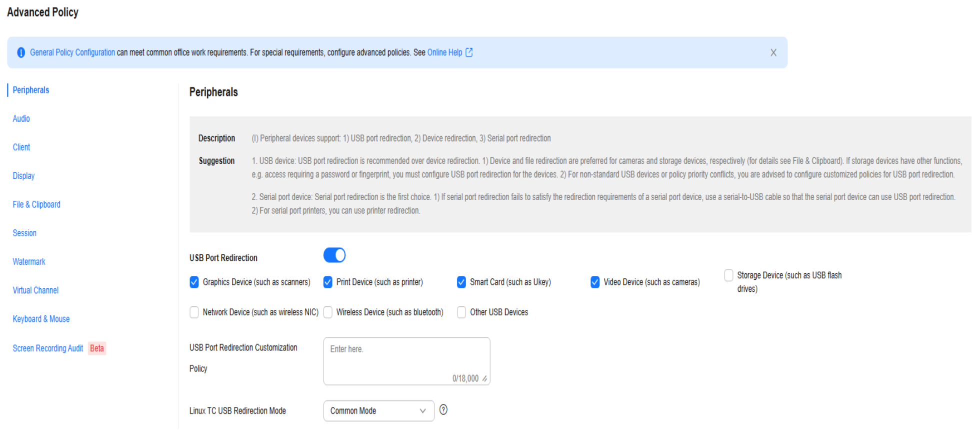
Step 6 Click **Next: Configure Policy**. The **General Policy Configuration** page is displayed.

Step 7 On the **General Policy Configuration** page, click **Advanced Policies** to go to the **Advanced Policies** page.

Step 8 Configure an advanced policy, as shown in **Figure 6-1**.

For details about how to configure an advanced policy, see **Table 6-2**.

Figure 6-1 Configuring an advanced policy



Advanced Policy

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

Peripherals

Description (I) Peripheral devices support: 1) USB port redirection, 2) Device redirection, 3) Serial port redirection

Suggestion 1. USB device: USB port redirection is recommended over device redirection. 1) Device and file redirection are preferred for cameras and storage devices, respectively (for details see File & Clipboard). If storage devices have other functions, e.g. access requiring a password or fingerprint, you must configure USB port redirection for the devices. 2) For non-standard USB devices or policy priority conflicts, you are advised to configure customized policies for USB port redirection.

2. Serial port device: Serial port redirection is the first choice. 1) If serial port redirection fails to satisfy the redirection requirements of a serial port device, use a serial-to-USB cable so that the serial port device can use USB port redirection. 2) For serial port printers, you can use printer redirection.

USB Port Redirection ●

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

□ Network Device (such as wireless NIC) □ Wireless Device (such as bluetooth) □ Other USB Devices

USB Port Redirection Customization Policy: Enter here. 0/18,000

Linux TC USB Redirection Mode: Common Mode

Table 6-2 Advanced policy list

Policy Name	Description
Peripherals	You can configure policies for the redirection of USB ports, devices, printers, and cameras.
Audio	You can configure policies for the redirection of audio, audio playback, and audio recording.
Clients	You can configure policies for automatic reconnection interval, waiting time before automatic monitor shutdown after screen locking, screenshot prevention, and IP address access control.
Display	You can configure policies for the display level, display frame rate, and video frame rate.
Files and Clipboards	You can configure policies for file redirection and clipboard redirection.
Sessions	You can configure policies for automatic screen locking, self-service maintenance, and disconnection after screen locking.
Watermarking	You can configure policies for watermark content, display settings, and display mode.

Policy Name	Description
General Audio/Video Bypass	You can configure policies for general audio/video bypass.
Virtual Channels	You can configure policies for virtual channel control.
Keyboards and Mouse Devices	You can configure policies related to computer mouse devices, such as feedback and simulation mode.

Step 9 Configure required policies and click **Next: Select Target Object**.

Step 10 Select an object type as required and then select an object.

Step 11 Click **Next: Finish**. The policy has been created and will take effect upon the next login to the desktop.

----End

NOTE

- indicates that the policy is enabled.
- indicates that the policy is disabled.

Peripherals

Configure peripheral application policies, as shown in **Table 6-3**.

NOTE

- A peripheral may support:
  - USB port redirection
  - Device redirection
  - Serial port redirection
- USB devices: USB port redirection is recommended over device redirection.
  - Device redirection is recommended for cameras, and file redirection for storage devices (see **Files and Clipboards**). If a storage device has other functions, such as password- or fingerprint-based access, you must configure USB port redirection for the device.
  - For non-standard USB devices or policy priority conflicts, you are advised to customize policies for USB port redirection.
- Serial port devices: Serial port redirection is preferred.
  - If serial port redirection fails to satisfy the redirection requirements of a serial port device, use a serial-to-USB cable so that the serial port device can use USB port redirection.
  - For serial port printers, you can use printer redirection.

Table 6-3 Peripheral policies

Type	Parameter	Description	Example Value
USB Port Redirection	USB port redirection switch	- ●: End users can use USB devices connected to terminals by using USB port redirection. - ○: End users cannot use USB devices connected to terminals by using USB port redirection. - Default value: ●	●
	Graphics devices (such as scanners)	- ☑: End users can use USB graphics devices connected to terminals through USB port redirection. - □: End users cannot use USB graphics devices connected to terminals through USB port redirection. - Default value: ☑	☑
	Printers	- ☑: End users can use USB print devices connected to terminals through USB port redirection. - □: End users cannot use USB print devices connected to terminals through USB port redirection. - Default value: ☑	☑
	Smart card devices (such as Ukeys)	- ☑: End users can use smart card devices on a computer through USB port redirection. - □: End users cannot use smart card devices on a computer through USB port redirection. - Default value: ☑	☑

Type	Parameter	Description	Example Value
	Video devices (such as cameras)	● ☑: End users can use USB video devices connected to terminals through USB port redirection. ● □: End users cannot use USB video devices connected to terminals through USB port redirection. ● Default value: ☑	☑
	Storage devices (such as USB flash drives)	● ☑: End users can use USB storage devices connected to terminals through USB port redirection. ● □: End users cannot use USB storage devices connected to terminals through USB port redirection. ● Default value: □	□
	Network Device (such as wireless NIC)	● ☑: End users can use network devices on a computer through USB port redirection. ● □: End users cannot use network devices on a computer through USB port redirection. ● Default value: □	□
	Wireless Device (such as bluetooth)	● ☑: End users can use wireless devices on a computer through USB port redirection. ● □: End users cannot use wireless devices on a computer through USB port redirection. ● Default value: □	□

Type	Parameter	Description	Example Value
	Other USB Devices	- ☑: End users can use other USB devices (excluding graphics devices, video devices, printers, storage devices, and smart cards) connected to terminals through USB port redirection. - □: End users cannot use other USB devices (excluding graphics devices, video devices, printers, storage devices, and smart cards) connected to terminals through USB port redirection. - Default value: □	□

Type	Parameter	Description	Example Value
	USB Port Redirection Customization Policy	Users can customize USB policies and ADV policies using the customized ID or class policy. Use vertical bars (|) to separate multiple policies and store them in a configuration file as a complete string. The string contains a maximum of 1024 characters and cannot contain spaces or any of the following special characters: "!@#$%^&*()>?. Format examples are as follows: ● Customized ID policy format: **ID:VID:PID:isShare:isCompress** **NOTE** PID fuzzy match format (for peripherals with the same VID): **ID:VID:FFFF:isShare:isCompress** ● Customized class policy format: **CLASS:DeviceClass:DeviceSubClass:DeviceProtocol:InterfaceClass:InterfaceSubClass:InterfaceProtocol:isShare:isCompress** ● USB key policy format: **USBKEY:VID:PID** ● ADV policy format: **ADV:VID:PID:isSelectConfig:isResetInterface:isSelectInterface:isRevert**	ID:147E:2016:1:0|CLASS:08:06:50:08:06:50:1:0|USBKEY:147E:2016|ADV:78e:79f:1:1:1:1

Type	Parameter	Description	Example Value
		NOTE - Priority: Customized ID policies > customized class policies > basic class policies. - PID fuzzy match: This policy is used to forbid or allow the redirection of peripherals with the same VID. - **ADV**: performs advanced debugging on non-standard devices - **VID**: specifies the vendor ID - **PID**: specifies the product ID - **isShare**: specifies whether to allow device redirection If yes, the value is **1**. If no, the value is **0**. - **isCompress**: specifies whether to allow camera compression, which is only available for cameras. If yes, the value is **1**. If no, the value is **0**. - **DeviceClass**: specifies the device descriptor class - **DeviceSubClass**: specifies the device descriptor subclass - **DeviceProtocol**: specifies the device descriptor protocol - **InterfaceClass**: specifies the interface descriptor class - **InterfaceSubClass**: specifies the interface descriptor subclass - **InterfaceProtocol**: specifies the interface descriptor protocol - The USB key is used together with the key lock function of Westone. - **isSelectConfig**: specifies whether to run the command of selecting configuration on the Linux client - **isResetInterface**: specifies whether to run the command of resetting an interface when selecting configuration on the Linux client - **isSelectInterface**: specifies whether to run the command of selecting an interface on the Linux client - **isRevert**: specifies whether to run the command of negating a device ID on the	

Type	Parameter	Description	Example Value
	Linux TC USB Redirection Mode	• This option is available only for setting the USB redirection mode of Linux TCs. • The common mode is recommended for Linux TCs. If a USB device is incompatible with the general mode, you can use the classic mode.	General mode
Printer Redirection	Printer redirection switch	• ●: End users can use printers connected to TCs through printer redirection (a policy of device redirection). • ○: End users cannot use printers connected to TCs on a cloud desktop. • Default value: ● **NOTICE** The printer driver must be installed on both the TC and computer.	●
	Synchronize Client Default Printer	• ☑: The default printer of the client is synchronized. • □: The default printer of the client is not synchronized. • Default value: □	□

Type	Parameter	Description	Example Value
	Universal Printer Driver	- Default - HDP XPSDrv Driver - Universal Printing PCL 5 - Universal Printing PCL 6 - Universal Printing PS If you select **Default**, the **Universal Printing PS** driver is loaded for Linux client printer redirection, and the **HDP XPSDrv Driver** driver is loaded for Windows client printer redirection. **NOTICE** To simplify the printer service, ensure that all users use TCs or SCs running the same OS to log in to cloud desktops. For example, all TCs run Linux.	Default
Session Printer	Session printer switch	- ◉: After the session printer is enabled and a custom policy is configured, a network sharing printer is automatically created in the session. - ○: The session printer is disabled. - Default value: ○	○

Type	Parameter	Description	Example Value
	Session Printer Customization Policy	● Users can customize a session printer policy by configuring *IP address*;*Printer name*;*Printer model*;*Default printer*;*Settings*;*Location*. Configuration items are separated by semicolons (;), and multiple policies are separated by vertical bars (|) and form a string that is saved in the configuration file. The string contains a maximum of 1024 characters and cannot contain any of the following characters: "!@#$%^&*()>?. – *IP address*: IP address of the printer server, for example, **192.168.1.11**. This parameter is mandatory. – *Printer name*: name of the printer, for example, **EPSON TM-T88IV Receipt**. This parameter is mandatory. – *Printer model*: printer driver model, for example, **EPSON TM-T88IV ReceiptSC4**. This parameter is mandatory. – *Default printer*: If the value is **0**, the printer is not a default printer; if the value is **1**, the printer is a default printer. This parameter is mandatory. – *Settings*: If the value is **0**, the printer is a network sharing printer; if the value is **1**, the printer is a network port printer. This parameter is mandatory. – *Location*: indicates the printer location matching. Partial matching and full	192.168.1.11;EPSON TM-T88IV Receipt;EPSON TM-T88IV ReceiptSC4;1;0;IP:192.168.1.12

Type	Parameter	Description	Example Value
		matching of client IP addresses, MAC addresses, and TC host names are supported currently. For example, **IP:192.168.1.12** indicates full match of IP addresses, **IP:192.168** indicates partial match of IP addresses, **MAC:00-ac** indicates partial match of MAC addresses, and **HOSTNAME:workspace-vdesktop** indicates full match of host names. If location matching is not required, set the parameter to **0**.	
Camera Redirection	Camera redirection switch	- ●: End users can use cameras connected to terminals through camera redirection (a policy of device redirection). - ○: End users cannot use cameras connected to terminals through camera redirection. - Default value: ● **NOTE** - The camera driver must be installed on the terminal. - Toggle on the **USB Port Redirection** switch (●) and select **Video Device (such as cameras)**.	●
	Camera Frame Rate (FPS)	The value ranges from 1 to 30.	15
	Camera Max Width (Pixel)	The value ranges from 1 to 9,999.	3000
	Camera Max Height (Pixel)	The value ranges from 1 to 9,999.	3000

Type	Parameter	Description	Example Value
	Camera Data Compression Mode	H.264	H.264
TWAIN Redirection	TWAIN redirection switch	● ◉: End users can use TWAIN devices connected to terminals through TWAIN redirection (a policy of device redirection). ● ○: End users cannot use TWAIN devices connected to terminals through TWAIN redirection. ● Default value: ◉ **NOTE** The TWAIN driver must be installed on the terminal.	◉
	Image Compression Level	Defines the compression level for TWAIN redirection. ● None (no compression) ● Low (highest speed) ● Medium (medium speed) ● Lossless ● Low-loss ● Medium-loss ● High-loss	Medium (medium speed)

Type	Parameter	Description	Example Value
PC/SC Redirection	-	- If you enable this option, you can use smart cards connected to terminals through PC/SC redirection (a policy of device redirection). Disconnecting user sessions when smart cards are being removed is available. - If you disable this option, PC/SC redirection is disabled, but the PC/SC driver is still loaded. If you enable this option again, you do not need to restart the desktop. Disconnecting user sessions when smart cards are being removed is available. - If you disable this option, PC/SC smart card redirection is disabled and the PC/SC driver is not loaded. If you enable this option again, you need to restart the desktop. **NOTE** To configure PC/SC redirection, deselect **Smart Card (such as Ukey)** in the **USB Port Redirection** policy. In addition, you need to customize an ID policy in the format of *ID*:*VID*:*PID*:0:0. To enable PC/SC redirection, you need to install the PC/SC driver on the terminal and desktop.	Disabled
Serial Port Redirection	Serial port redirection switch	- ●: End users can use serial port devices connected to terminals through serial port redirection. - ○: End users cannot use serial port devices connected to terminals through serial port redirection. - Default value: ○ **NOTE** The serial port device driver must be installed on the desktop.	○

Type	Parameter	Description	Example Value
	Auto Connect Client Serial Ports	- ☑: When users log in to cloud desktops, client serial ports are automatically connected to prevent the serial ports from being used by other local programs. You are advised to enable this parameter. - □: When users log in to cloud desktops, client serial ports are not automatically connected. - Default value: □	☑

Type	Parameter	Description	Example Value
Driver Interface Redirection	Customized Drivers	Drivers installed on terminals are simulated to provide interfaces for applications on the computer to call to control and use hardware devices. Currently, only Linux desktops and SKF interfaces of cryptographic algorithm are supported. ● Enter one or more driver file names or full paths of driver files installed on terminals. If multiple ones are entered, separate them with semicolons (;) ● You can enter driver file names or full paths of driver files on different types of terminals. The HDP client dynamically identifies them. ● Full path of a driver file. If the path contains spaces, use double quotation marks ("") to quote the path. ● A driver file name must not contain special characters such as ;*?<>|. ● The string contains a maximum of 1,000 characters. ● This parameter is left empty by default, indicating that the function is disabled. **NOTE** Ensure that hardware devices are supported.	/sdcard/HdpClient/Api/libSKFAPI_arm.so;/sdcard/HdpClient/Api/libSKFAPI_arm64.so;SKFAPI.dll

Audio

Configure audio policies, as shown in **Table 6-4**.

Table 6-4 Audio policies

Type	Parameter	Description	Example Value
Audio Redirection	Audio redirection switch	Applications on user desktops can use audio devices on terminals to record and play audio.	◉
Playback Redirection	Playback redirection switch	This parameter takes effect only after audio redirection is enabled. The playback switch is controlled separately. ● ◉: Playback redirection is enabled so that end users can play audios. ● ○: Playback redirection is disabled so that end users cannot play audios.	◉
	Playback Scenario	● **Lossless**: The voice quality is better, but the bandwidth usage is the highest. ● **Voice call**: The best voice call processing capability can be provided and the bandwidth usage is the lowest, but the music processing capability is average. ● **Music playback**: The best music processing capability can be provided and the bandwidth usage is medium, but the voice call processing capability is average. ● **Automatic identification**: The user's behavior, such as voice call or music playback, can be identified. The accuracy rate exceeds 90%. The system automatically switches to a better algorithm based on user behavior.	Music playback
Recording Redirection	Recording redirection switch	This policy takes effect only after audio redirection is enabled. The recording switch is controlled separately. ● ◉: Recording redirection is enabled so that end users can record audios. ● ○: Recording redirection is disabled so that end users cannot record audios.	◉

Type	Parameter	Description	Example Value
	Recording Scenario	- **Lossless**: The voice quality is better, but the bandwidth usage is the highest. This level is recommended only when the network bandwidth is sufficient and the network is stable and reliable. Generally, this level is not recommended for audio recording. - **Voice call**: The best voice call processing capability can be provided and the bandwidth usage is the lowest, but the music processing capability is average. You are advised to select this level because audio recording is the most common scenario. - **Music recording**: This option is reserved because recording is rarely used for music playback. Therefore, this option is not recommended for audio recording. - **Automatic Identification**: This option is reserved and is equivalent to **Voice call**.	Voice call

Clients

Configure client policies, as shown in **Table 6-5**.

Table 6-5 Client policies

Parameter	Description	Example Value
Auto Reconnection Interval (s)	Specifies the interval at which the client attempts to connect to the server after the client is disconnected abnormally. The value ranges from 0 to 50.	5
Session Persistence Time (s)	Specifies the longest duration allowed for automatic reconnection attempts after the client is disconnected abnormally. The value ranges from 0 to 180.	180

Parameter	Description	Example Value
Auto Monitor Shutdown After Screen Locking	- ◉: After the VM screen is locked, the monitor is automatically shut down if no keyboard or mouse operation is performed on the client after the waiting time. **NOTE** This policy only applies to TCs and does not take effect for nested login. - ◯: After the VM screen is locked, the monitor is not automatically shut down.	◯
Auto Monitor Shutdown In (s)	This parameter is valid only when **Auto Monitor Shutdown After Screen Locking** is enabled. This parameter specifies the waiting time before the local monitor is automatically shut down after the VM screen is locked. The value range is 10–600,000 seconds.	300
Screenshot Prevention Policy	After the policy is enabled, users are prevented from saving and sharing screenshots captured on cloud desktops. - ◉: This policy is enabled. - ◯: This policy is disabled. **NOTE** - Only Windows clients, macOS clients (version 24.6.3 or later), and Linux TCs are supported. After this function is enabled, other terminals cannot access the system. - The screenshot prevention policy relies on the underlying capabilities of the on-premises OS of the terminal user, so the support for this function varies with the client type. - In response to the potential new methods for screen shooting, we will continuously update and optimize the policy, but cannot guarantee comprehensive protection in special cases.	◯

Parameter	Description	Example Value
IP Address Access Control	By default, this parameter is left blank, indicating that all clients can access the desktop. After the IP address of a client is specified, only the specified client can access the desktop. You need to enter a valid IP address and subnet mask for IP address-based access control. The IP address and subnet mask are separated by a vertical bar (|). If there are multiple IP addresses and subnet masks, separate them with semicolons (;), for example, *IP address*|*Mask*;*IP address*|*Mask*;*IP address*|*Mask*.	192.168.0.1|255.255.255.255
Verification of Terminals Added to a Domain	You can configure a policy to control terminal access to desktops. After the policy is enabled, only terminals that are added to the company's domain can access desktops. • ●: verification enabled • ○: verification disabled **NOTE** • This function is supported only when an AD domain is interconnected with. • This function applies only to Windows terminals. You must select Windows after enabling terminal login control. • The terminal device and the desktop project are in the same domain. • Clients of 24.6.2.5001 or later are supported. • Servers of 24.6.2.5001 or later are supported.	○

Parameter	Description	Example Value
Terminal Login Control	You can configure a policy to control terminal access to desktops. - ●: Enable this function to select the terminal types that can access cloud desktops. – ☑: Only the selected terminals are allowed to access desktops. – □: Unselected terminals are not allowed to access desktops. - ○: Disable this function to allow all terminals to access desktops. **NOTE** - Clients of 24.6.2.5001 or later are supported. - Servers of 24.6.2.5001 or later are supported.	○

Display

Configure display policies, as shown in **Table 6-6**.

Table 6-6 Display policies

Type	Parameter	Description	Example Value
Display	Display Policy Level	● **Level 1**: applies to network bandwidth lower than 512 Kbit/s. It can be used only for light-load office scenarios, such as browsing text documents. The display quality of this level is low. ● **Level 2**: applies to network bandwidth lower than 1 Mbit/s. It can be used only for light-load office scenarios, such as browsing text documents and static images. The display quality of this level is better than that of level 1. ● **Level 3**: applies to network bandwidth lower than 4 Mbit/s. It can be used for medium-load office scenarios, such as browsing documents, images, and dynamic web pages. ● **Level 4** (recommended): applies to network bandwidth lower than 20 Mbit/s. It can be used to play standard definition (SD) and high definition (HD) videos. This level ensures the display quality at a proper bandwidth level. ● **Level 5**: applies to network bandwidth higher than 20 Mbit/s. This level delivers good video playback.	Level 4 (recommended)
	Display Frame Rate (FPS)	Indicates the image refresh rate in non-video scenarios. Increasing this value improves image and operation smoothness but consumes more network bandwidth and VM CPU resources. The value ranges from 1 to 60. The recommended value ranges from 15 to 25.	25
	Video Frame Rate (FPS)	Indicates the image refresh rate of video. Increasing this value improves video playback smoothness but consumes more network bandwidth and VM CPU resources. **NOTE** This parameter is unavailable after **Rendering acceleration** is enabled.	-
	Bandwidth (kbit/s)	Limits the peak bandwidth of a user. The value ranges from 256 to 25,000.	20000

Type	Parameter	Description	Example Value
Image Compression Parameters	Min. Capacity for Image Cache (MB)	The minimum capacity for image cache, expressed in MB. Increasing this value reduces bandwidth usage but consumes more client memory resources. If the parameter is set to a value smaller than 50, the cache function is disabled. The value ranges from 0 to 300.	200
	Lossy Compression Recognition Threshold	The threshold for recognizing image complexity. Decreasing this value increases image quality but consumes more network bandwidth resources. The value ranges from 0 to 255.	60
	Lossless compression	Specifies the image compression algorithm. You can select **Basic compression** or **Deep compression**. When you compress the same picture, the compression ratio and CPU usage of basic compression are lower than those of deep compression.	Basic compression
	Deep Compression Level	This parameter takes effect after **Deep compression** is selected. A higher compression level means a higher compression ratio and CPU usage but lower bandwidth usage. **Level 0** indicates a copy operation and no compression is involved. This level consumes the fewest CPU resources but the most bandwidth resources.	Level 0
	Lossy Compression Quality	This parameter is used to set the image quality after lossy compression. Increasing this value improves image quality. The value ranges from 20 to 100.	85
	Color Enhancement for Office Work	This parameter is used for color enhancement in office scenarios. • ●: Color enhancement for office work is enabled. • ○: Color enhancement for office work is disabled.	○

Type	Parameter	Description	Example Value
Video Compression Parameters	Quality/ Bandwidth First	● **Quality First**: If this option is selected, video images are compressed at a fixed quality level. **Average Video Bitrate (Kbit/s)** takes effect only after **Rendering acceleration** is enabled. ● **Bandwidth First**: If this option is selected, video images are compressed at a fixed bitrate. **Average Video Quality**, **Lowest Video Quality**, and **Highest Video Quality** take effect only after **Rendering acceleration** is enabled.	Quality
	Average Video Bitrate (Kbit/s)	Video compression algorithm parameter. In the **Bandwidth First** mode, increasing this value improves video quality. The value ranges from 256 to 100,000.	18,000
	Peak Video Bitrate (Kbit/s)	Video compression algorithm parameter. Increasing this value improves display quality. The value ranges from 256 to 100,000.	18,000
	Average Video Quality	Average quality coefficient of video. In the **Quality First** mode, increasing this value compromises video quality. The value ranges from 5 to 59.	15
	Lowest Video Quality	Lower limit of video quality. In the **Quality First** mode, increasing this value compromises video quality. The value ranges from 5 to 69.	25
	Highest Video Quality	Upper limit of video quality. In the **Quality First** mode, increasing this value compromises video quality. The value ranges from 1 to 59.	7
	GOP Size	Video compression algorithm parameter. Decreasing this value improves video quality but consumes more bandwidth resources. It is recommended that this value be 1 to 2 times the video frame rate. The value ranges from 0 to 65,535.	100
	Encoding Preset	Video compression algorithm parameter. Decreasing this value means faster encoding and better smoothness but lower image quality and higher bandwidth usage.	Preset 1

Type	Parameter	Description	Example Value
Rendering Acceleration	Rendering Acceleration	- ☑: Rendering acceleration is enabled to improve smoothness. - □: Rendering acceleration is disabled.	□
	Video Acceleration Enhancement	- ●: Video acceleration enhancement is enabled. - ○: Video acceleration enhancement is disabled.	●
	Video Optimization	- ●: Video optimization is enabled to improve smoothness. - ○: Video optimization is disabled.	Disabled
	GPU Color Optimization	- ●: GPU color optimization is enabled to improve color reproduction in video/office hybrid scenarios. - ○: GPU color optimization is disabled. **NOTE** This parameter applies only to GPU desktops.	○
	Video Recognition Threshold	Number of frames required when you open or exit a video. It is easier to open or exit a video as the value increases. The value ranges from 0 to 500.	10
	Frame Rate Statistical Length	Number of statistical frames during video detection. It is easier to open a video as the value decreases. The value ranges from 2 to 100.	4
	Image Quality Threshold	It is easier to open a video as the value decreases. The value ranges from 0 to 100.	0
	Refresh Frequency Threshold	It is easier to open a video as the value decreases. The value ranges from 1 to 100.	3

Type	Parameter	Description	Example Value
	Threshold of Exiting Video Area	It is easier to exit a video as the value decreases. The value ranges from 0 to 100.	8
	Min Video Width	It is easier to open a video as the value decreases. The value ranges from 0 to 1,280.	191
	Min Video Height	It is easier to open a video as the value decreases. The value ranges from 0 to 1,280.	191
	Proportion Threshold of Single-Frame Natural Image Block	It is easier to open a video as the value decreases. The value ranges from 0.000001 to 1.	0.3
	Number of Cyclical Natural Images	It is easier to open a video as the value decreases. The value ranges from 0 to 100.	2
	Threshold of the Non-Natural Image Area Percentage	It is harder to exit a video as the value increases. The value ranges from 0.000001 to 1.	0.85
	Number of Non-Natural Images	It is harder to exit a video as the value increases. The value ranges from 0 to 100.	25
Other Parameters	Graphics Card Memory (MB)	Device memory capacity. The value ranges from 0 to 64. This parameter affects the bandwidth in some scenarios. Increasing this value reduces the bandwidth usage.	64

Type	Parameter	Description	Example Value
	Driver Delegation Mode	- ☑: The driver delegation mode is enabled. - ☐: The driver delegation mode is disabled.	☐
	Driver Delegation Latency (*30ms)	The value ranges from 1 to 100.	80
	Video Latency (*30ms)	The value ranges from 1 to 100.	80
	Change Resolution in Computer	- ☑: After the computer resolution change policy is enabled, end users can change the desktop resolution in system settings on cloud desktops. - ☐: After the computer resolution change policy is disabled, end users cannot change the desktop resolution in system settings.	☐
	Application Recognition	Configure display policies for specific applications. (Provided by Huawei engineers) **NOTE** A Windows 10 computer supports up to 4 applications.	-

Files and Clipboards

Configure file & clipboard policies, as shown in **Table 6-7**.

Table 6-7 File & Clipboard policies

Type	Parameter	Description	Example Value
File Redirection	File redirection switch	- **Read-only**: Files in drivers and storage devices can only be pre-viewed. - **Read/write**: Files in drivers and storage devices can be modified. Users can use drivers in file redirection mode on cloud desktops.	Read-only
	Fixed driver	- ☑: Users can use fixed drivers, such as local disks, on cloud desktops in the file redirection mode. - □: Users cannot use fixed drivers, such as local disks, on cloud desktops in the file redirection mode. **NOTE** When file redirection is disabled, this function is disabled.	□
	Removable driver	- ☑: Users can use removable drivers, such as USB flash drives, on cloud desktops in the file redirection mode. - □: Users cannot use removable drivers, such as USB flash drives, on cloud desktops in the file redirection mode. **NOTE** When file redirection is disabled, this function is disabled.	□
	CD/DVD-ROM driver	- ☑: Users can use CD-ROM drivers on cloud desktops in the file redirection mode. - □: Users cannot use CD-ROM drivers on cloud desktops in the file redirection mode.	□

Type	Parameter	Description	Example Value
	Network driver	- ☑: Users can use network drivers on cloud desktops in the file redirection mode. - □: Users cannot use network drivers on cloud desktops in the file redirection mode.	□
	Traffic Control	- ◉: Traffic control is enabled. - ○: Traffic control is disabled.	○
	Good Network Latency Threshold (ms)	Latency threshold of good network. The value ranges from 1 to 1000.	30
	Normal Network Latency Threshold (ms)	Latency threshold of normal network. The value ranges from 1 to 1000.	70
	Poor Network Latency Threshold (ms)	Latency threshold of poor network. The value ranges from 1 to 1000.	100
	Reducing Step (KB)	Step of reducing the transmission speed. The value ranges from 1 to 100.	20
	Slow Increasing Step (KB)	Slow step of increasing the transmission speed. The value ranges from 1 to 100.	10
	Quick Increasing Step (KB)	Quick step of increasing the transmission speed. The value ranges from 1 to 100.	20
	Start Speed (KB/s)	Initial transmission speed. The value ranges from 1 to 10,240.	1024
	Test Block Size (KB)	Block size of speed testing. The value ranges from 64 to 1024.	64
	Test Time Gap (ms)	Gap of testing. The value ranges from 1,000 to 100,000.	10,000

Type	Parameter	Description	Example Value
	Compression	- ●: Compression is enabled. - ○: Compression is disabled.	○
	Compression Threshold (Byte)	The value ranges from 0 to 10,240.	512
	Min Compression Rate	The value ranges from 0 to 1,000.	900
	File Size Supported by Linux	- ●: File size can be set on Linux. - ○: File size cannot be set on Linux.	●
	File Size Threshold for Linux (MB)	The value ranges from 0 to 4,096.	100
	Mobile Client Redirection	- ●: Mobile client redirection is enabled. - ○: Mobile client redirection is disabled.	●
	Linux Root Directory Mounting	- ●: Root directory mounting is enabled on Linux. - ○: Root directory mounting is disabled on Linux.	●
	Linux Root Directory Mounting Path	If root directory mounting is enabled on Linux, you need to configure the mounting path. The value contains a maximum of 256 characters in UTF-8 format.	\var\log
	Linux File System Mounting Path	The value contains a maximum of 256 characters in UTF-8 format.	\media|\Volumes|\swdb\mnt|\home|\storage|\tmp|\run\media

Type	Parameter	Description	Example Value
	Linux Fixed Driver File System Format	The value contains a maximum of 256 characters in UTF-8 format.	-
	Linux Removable Driver File System Format	The value contains a maximum of 256 characters in UTF-8 format.	vfat|ntfs|msdos|fuseblk|sdcardfs|exfat|fuse.fdredir
	Linux CD-ROM Driver File System Format	The value contains a maximum of 256 characters in UTF-8 format.	cd9660|iso9660|udf
	Linux Network Driver File System Format	The value contains a maximum of 256 characters in UTF-8 format.	smbfs|afpfs|cifs
	Path Separator	A single ASCII character	|
	Read/Write Speed (Kbit/s)	This option is disabled when **File Redirection** and **Send File From VM to Client** are disabled. The value **0** indicates that the read/write speed is not limited. Other values indicate the configured read/write speed. The default minimum speed is 32 kbit/s. If the minimum speed is lower than 32 kbit/s, 32 kbit/s is used by default.	0
Send File	Send File from VM to Client	● ◉: Files on a VM can be sent to the client. ● ○: Files on a VM cannot be sent to the client.	○

Type	Parameter	Description	Example Value
Clipboard Redirection	Clipboard Redirection	- **Bidirectional**: End users can copy data on client cloud desktops and paste the data on on-premises desktops, or copy data on on-premises desktops and paste the data on client cloud desktops. - **Server to client**: After this function is enabled, end users can only copy data on client cloud desktops and paste the data on on-premises desktops. - **Client to server**: After this function is enabled, end users can only copy data on on-premises desktops and paste the data on client cloud desktops. **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.	Bidirectional
	Clipboard Rich Text Redirection	- ●: Clipboard rich text redirection is enabled. - ○: Clipboard rich text redirection is disabled. **NOTE** Rich text contains format information, such as font style (bold, italic, etc.), color, hyperlink, image, and table.	●
	Clipboard File Redirection	- ●: Clipboard file redirection is enabled. - ○: Clipboard file redirection is disabled.	●

Sessions

Configure session policies, as shown in **Table 6-8**.

Table 6-8 Session policies

Parameter	Description	Recommended Value
Auto Screen Locking	- : Automatic screen locking is enabled. If the desktop is idle for a period of time after login, screen locking is automatically triggered. - : Automatic screen locking is disabled. **NOTE** For a Windows desktop of HDA 23.8.2 or later, when applications (such as video players and meeting software) on the desktop are set to the in-use status, the desktop is identified as being in use and does not trigger the corresponding automatic policy.	Disabled
Validity Period	Specifies the time when the policy takes effect. The time is the local time of the cloud desktop.	-
Screen Locking In (Minute)	Specifies the waiting time before the desktop screen is automatically locked. The value ranges from 3 to 86,400.	10

Parameter	Description	Recommended Value
Auto Disconnect/Log Out/Restart/ Stop/Hibernate After Auto Screen Locking	After the desktop is hibernated, the applications on the desktop are paused. After the desktop is woken up, the applications can be restored to the status when they were paused. ● **Disconnect**: **Auto Screen Locking** is enabled and **Disconnect** is selected. If automatic screen locking is triggered and no keyboard or mouse device is available on the client and no application on the desktop is set to the in-use status after the waiting time, the VM is automatically disconnected. ● **Log out**: **Auto Screen Locking** is enabled and **Log out** is selected. If automatic screen locking is triggered and no keyboard or mouse device is available on the client and no application on the desktop is set to the in-use status after the waiting time, the VM is automatically logged out of. ● **Restart**: **Auto Screen Locking** is enabled and **Restart** is selected. If automatic screen locking is triggered and no keyboard or mouse device is available on the client and no application on the desktop is set to the in-use status after the waiting time, the VM is automatically restarted. ● **Stop**: **Auto Screen Locking** is enabled and **Stop** is selected. If automatic screen locking is triggered and no keyboard or mouse device is available on the client and no application on the desktop is set to the in-use status after the waiting time, the VM is automatically stopped. ● **Hibernate**: **Auto Screen Locking** is enabled and **Hibernate** is selected. If automatic screen locking is triggered and no keyboard or mouse device is available on the client and no application on the desktop is set to the in-use status after the waiting time, the VM is automatically hibernated. ● **Disabled**: This parameter is disabled.	Disabled
Automatic Disconnection/ Logout/Restart/ Shutdown/ Hibernation After Screen Lock In (Minute)	Specifies the waiting time before a desktop is automatically disconnected, logged out of, restarted, shut down, or hibernated. The value ranges from 1 to 86,400.	1440

Parameter	Description	Recommended Value
Automatic Logout/Restart/ Shutdown/ Hibernation After Disconnection	● **Log out**: If the client is disconnected from a VM for a period longer than the waiting time, the VM is automatically logged out of. ● **Restart**: If the client is disconnected from a VM for a period longer than the waiting time, the VM is automatically restarted. ● **Shut down**: If the client is disconnected from a VM for a period longer than the waiting time, the VM is automatically shut down. ● **Hibernate**: If the client is disconnected from a VM for a period longer than the waiting time, the VM is automatically hibernated. ● **Disabled**: This parameter is disabled. NOTE ● **Automatic Logout/Restart/Shutdown/ Hibernation After Disconnection** is available only when **Disabled** or **Disconnect** is selected for **Automatic Disconnection/Logout/Restart/ Shutdown/Hibernation After Screen Lock**. ● If another logout, restart, or shutdown task is performed on the VM within the waiting time, the automatic logout, restart, shutdown, or hibernation operation will not be triggered.	Disabled
Automatic Logout/Restart/ Shutdown/ Hibernation After Disconnection In (Minute)	Specifies the waiting time before a desktop is automatically logged out of, restarted, shut down, or hibernated after disconnection. The value ranges from 10 to 86,400.	10
Self-help console login preemption	This configuration item is used to determine whether preemption login through the self-help console is allowed when a user desktop has been logged in to. ☑ indicates that preemption login is allowed and □ indicates that preemption login is not allowed. By default, preemption login is enabled. The configuration takes effect only after the cloud desktop is restarted.	☑

Parameter	Description	Recommended Value
Disconnection After Screen Locking	This parameter determines whether to disconnect from a desktop immediately when the desktop is locked. Screen locking may happen when the automatic session locking policy is triggered or the user locks the desktop screen. ☑ indicates that the cloud desktop is disconnected from immediately after the screen is locked. This parameter is not enabled by default. **NOTE** - This operation can be performed only on Windows desktops. - Servers of 24.6.0 or later are supported.	□

Watermarking

Configure watermark policies, as shown in **Table 6-9**.

Table 6-9 Watermark policies

Parameter	Description	Example Value
Watermarking	- ●: After this function is enabled, watermarks are displayed on the screen after users access the cloud desktop. - ○: After this function is disabled, no watermark is displayed on the screen after users access the cloud desktop. **NOTE** Displaying watermarks may compromise video playback on the cloud desktop.	●
Security First	After this function is enabled, if the client version is earlier than the server version, access is rejected.	○

Parameter	Description	Example Value
Custom Content	The content contains only digits, uppercase letters, lowercase letters, and some special characters, and cannot exceed 45 characters. After you customize the content, the desktop screen displays the watermark in the format of *Custom content Login username Time displayed on the desktop*. For example, if the custom content is set to **CopyRight**, the watermark is **CopyRight user 2022-01-08 01:01:01**. **NOTE** ● The following special characters are allowed: ~!@#$%^&*()-_=+|{};:',<.? ● If line breaks or other special characters are used, the custom content may not take effect.	-
User Information	Terminal user information. If the user does not enter the mobile number or email address, the user information is not displayed. ● **Username** ● **Mobile number** ● **Email**	Username
Date-Time Sequence	Sequence in which the date and time are displayed: ● **D (Date)** ● **T (Time)** ● **DT (date-time format)** ● **TD (time-date format)** Example: 2020-01-01 16:40 for DT; 16:40 2020-01-01 for TD	DT (date-time format)

Parameter	Description	Example Value
Display Mode	● **Fixed position**: The watermark is displayed at a fixed position on the screen. ● **Random motion**: The watermark moves randomly on the screen every 2 seconds.	Random motion
Alignment	Watermark alignment. Options: **Left alignment**, **Right alignment**, and **Center alignment**	Left alignment
Quantity	Number of watermarks. This parameter is available when **Display Mode** is set to **Fixed position**. The value ranges from 1 to 17.	1
Repeated Watermarks	Number of repeated watermarks. This parameter is available when **Display Mode** is set to **Fixed position**. The value ranges from 1 to 17.	1
Repetition Interval	Interval of repeated watermarks. This parameter is available when **Display Mode** is set to **Fixed position**. The value ranges from 1 to 17.	10
Tilt	Specifies the tilt of the watermark displayed on the desktop. The value ranges from –90 to 90.	–45
Font Size	Watermark font size. The value ranges from 8 to 100.	30
Color	Watermark color	⬛
Opacity (%)	The value ranges from 0 to 100. **0%** indicates completely transparent, and **100%** indicates completely opaque.	87.5
Preview	You can click to preview the watermark in 16:9 or 4:3.	-

General Audio/Video Bypass

After installing applications and the Huawei Cloud Workspace client on a local terminal running Windows 10, you can configure the audio/video bypass policy to access a cloud desktop from the Huawei Cloud Workspace client and use the applications on the local terminal without installing the applications on the cloud desktop. **Table 6-10** describes the general audio/video bypass policy.

The audio/video bypass function has the following restrictions:

- This parameter is available only when the local terminal runs Windows 10 and the cloud desktop runs Windows.
- Non-cloud desktop applications can be mapped to cloud desktops using the general audio/video bypass policy only when these applications work properly on local terminals.
- Before logging in to a cloud desktop and using an application mapped to the cloud desktop through the audio/video bypass policy, you need to stop the applications that have been started on the local terminal. Otherwise, the application cannot be used on the cloud desktop.
- Before using applications that are mapped to the cloud desktop through the audio/video bypass policy, ensure that the cloud desktop is in full screen mode.
- When an application that is mapped to the cloud desktop through the audio/video bypass policy is used on the cloud desktop, other applications on the cloud desktop cannot be used to interact with the application. For example, you cannot use the screenshot software on the cloud desktop to capture the application GUI.
- The input method used by the application is the terminal-side input method. If you want to switch the input method when using an application that is mapped to the cloud desktop through the audio/video bypass policy on the cloud desktop, you need to switch the input method of the local terminal. For example, an input method is switched by using a keyboard shortcut, or an input method is switched on a local desktop by minimizing a cloud desktop.
- When an application that is mapped to the cloud desktop through the audio/video bypass policy is used on the cloud desktop, if you press **Alt**+**Tab** to switch between windows, the local terminal GUI is displayed.
- If the **Video devices (such as cameras)** policy in **USB Port Redirection** is enabled on the current cloud desktop, the camera on the local terminal cannot be used when you perform video-related operations on the cloud desktop using applications mapped to the cloud desktop through the audio/video bypass policy.
- If you want to copy text between a cloud desktop and an application mapped to the cloud desktop through the audio/video bypass policy, you need to enable the clipboard redirection policy on the cloud desktop. For details about policy configuration, see **How Do I Copy Files Between a Desktop and a Local Storage Device?**
- After a local application is mapped to the cloud desktop through the audio/video bypass policy, you are not advised to use the software package to install the application on the cloud desktop. Otherwise, when you start the

application on a web page, the application installed using the software package on the cloud desktop will be started.

Table 6-10 General audio/video bypass policies

Parameter	Description	Example Value
General Audio/Video Bypass	- ◉: The general audio/video bypass policy is enabled. - ○: The general audio/video bypass policy is disabled. By default, this parameter is disabled.	○

Parameter	Description	Example Value
Software Path	Used to configure the software path and start parameters for the general audio/video bypass policy. Separate multiple paths with semicolons (;). If an installation path contains spaces, use double quotation marks ("") to quote the path. Example: "C:\Users\userName\AppData\Roaming\HuaweiMeeting\HuaweiMeeting\HuaweiMeeting.exe" --bypass; HuaweiMeeting.exe --bypass; Currently, only Huawei Cloud Meeting is supported. **NOTE** ● **C:\Windows\System32\notepad.exe** is the installation path of the corresponding software on the local PC. You can find the shortcut icon of the installed software on the local PC, right-click the shortcut icon, and choose **Properties** from the shortcut menu. On the **Shortcut** tab of the application properties, replace the address with that in **Target**. ● **hello.txt** is the start parameter of the corresponding software on the local PC. You need to configure the start parameters only when the software has start parameters. For example, skip this operation for Huawei Cloud Meeting, which does not have start parameters.	C:\Users\Username\AppData\Roaming\HuaweiMeeting\HuaweiMeeting\HuaweiMeeting.exe

Virtual Channels

The administrator can configure a virtual channel policy so that users can access the cloud desktop through the Huawei Cloud Workspace client and download plug-ins. **Table 6-11** describes virtual channel policies.

Table 6-11 Virtual channel policies

Parameter	Description	Example Value
Virtual Channel Control	- ◉: The virtual channel control policy is enabled. - ○: The virtual channel control policy is disabled. By default, this parameter is disabled.	○
Custom Virtual Channel Registered Name	Contact Huawei technical support to obtain it.	-
Configuration Information	Contact Huawei technical support to obtain it.	-
Third-Party Plug-in Name	Used by clients (Windows clients only) to load third-party plug-ins, for example, LyncVdiPluginLib. Multiple plug-in names can be entered and must be separated by spaces or commas (,).	LyncVdiPluginLib

Keyboards and Mouse Devices

Configure keyboard and mouse device policies, as shown in **Table 6-12**.

Table 6-12 Keyboard and mouse device policies

Parameter	Description	Recommended Value
Computer Mouse Device Feedback	- **Adaptive** - **Force** - **Disabled**	Adaptive

Parameter	Description	Recommended Value
Computer Mouse Device Simulation Mode	If you select **Relative positioning**, the value of **Change the size of text, apps, and the other items on the display settings** cannot be higher than 100% on the user VM. ● **Absolute positioning** ● **Relative positioning**	Absolute positioning
Self-help Console Login Preemption	This configuration item is used to determine whether preemption login through the self-help console is allowed when a user desktop has been logged in to.	☑
Computer External Cursor Feedback	● ☑: Computer external cursor feedback is enabled. ● □: Computer external cursor feedback is disabled.	□

6.1.2 Editing a Policy

Scenarios

This section describes how to edit an existing policy.

Procedure

Step 1 Log in to the console.

Step 2 Choose **Policies** > **Protocol Policies**.

The **Protocol Policies** page is displayed.

Step 3 Perform operations as required.

NOTE

- The default policy is a preset general policy and its priority cannot be changed.
- When you create multiple policies, the default policy has the lowest priority.

- Adjust the policy priority. Click ✎ in the **Priority** column, adjust the priority to a proper level, and click **OK**.

- Click ✎ in the **Policy Name** column to change the policy name.
- Click **View Object** in the **Policy Target Object** column to view a policy's target objects. On the page displayed, you can click **Edit** to modify the target objects.
- To modify a policy's target objects, choose **More** > **Modify Object** in the **Operation** column.
- To modify the description, choose **More** > **Change Description** in the **Operation** column.
- To delete a policy, choose **More** > **Delete** in the **Operation** column.
- To modify a policy, perform **Step 4** to **Step 7**.

Step 4 In the **Operation** column of the desired policy, click **Modify Policy Item**.

The **General Policy Configuration** page is displayed.

Step 5 On the page displayed, enable or disable the corresponding policy, as shown in **Table 6-13**.

- ⬤ indicates that the policy is enabled.
- ○ indicates that the policy is disabled.

Table 6-13 Policy management

Type	Parameter	Description
USB Port Redirection	Graphics devices (such as scanners)	Supports USB peripherals on Workspace. Users can use devices in VMs through USB port redirection.
	Video devices (such as cameras)	
	Printers	
	Storage devices (such as USB flash drives)	
	Smart card devices (such as Ukeys)	
File Redirection	Fixed driver	– **Read-only**: Files in drivers and storage devices can only be pre-viewed. – **Read/Write**: Files in drivers and storage devices can be modified. Supports drivers on Workspace. Users can use drivers in VMs through file redirection.
	Removable driver	
	CD/DVD-ROM driver	
	Network driver	

Type	Parameter	Description
Clipboard Redirection	Bidirectional	After this function is enabled, end users can copy data on cloud desktops and paste the data on local desktops, or copy data on local desktops and paste the data on cloud desktops.
	Server to client	After this function is enabled, end users can only copy data on cloud desktops and paste the data on local desktops.
	Client to server	After this function is enabled, end users can only copy data on local desktops and paste the data on cloud desktops. **NOTE** Files can be copied only from a Windows client to a server, and file redirection and the corresponding driver must be enabled.
Printer Redirection	-	VM end users can use printers connected to devices through printer redirection (a policy of device redirection).
Rendering Acceleration **NOTE** This option only applies to video editing.	Visual quality first	The visual quality is excellent and the bandwidth usage is high (25 Mbit/s). The parameter details cannot be edited by default.
	Smoothness first	The visual quality and bandwidth usage are balanced (20 Mbit/s). The parameter details cannot be edited by default.
	Level 1 **NOTE** The **HDP Plus** parameter can be customized for adaptation.	The bandwidth (kbit/s) ranges from 256 to 25,000. **NOTE** This parameter specifies the limit of the display stream data. Increasing the value of this parameter improves user experience but consumes more network bandwidth. If the network bandwidth is insufficient, increasing the value of this parameter will compromise smoothness. In this case, you are advised to use the default value.

Type	Parameter	Description
		Display Frame Rate (FPS): 1–60 NOTE This parameter specifies the display frame rate when no video is played. Increasing the value improves display smoothness but consumes more bandwidth resources. If the network bandwidth is insufficient, increasing the value of this parameter will compromise smoothness. In this case, you are advised to use the default value.
		Video Frame Rate (FPS): 1–60 NOTE This parameter specifies the frame rate of video display. Increasing the value improves display smoothness but consumes more bandwidth resources. If the network bandwidth is insufficient, increasing the value of this parameter will compromise smoothness. In this case, you are advised to use the default value.
		Lossy Compression Recognition Threshold: 0–255 NOTE This parameter is used to adjust static image quality. A smaller value indicates higher quality but higher bandwidth usage and lower smoothness.
		Lossy Compression Quality: 20–100 NOTE This parameter is used to adjust static natural image quality. A larger value indicates higher quality but higher bandwidth usage and lower smoothness.

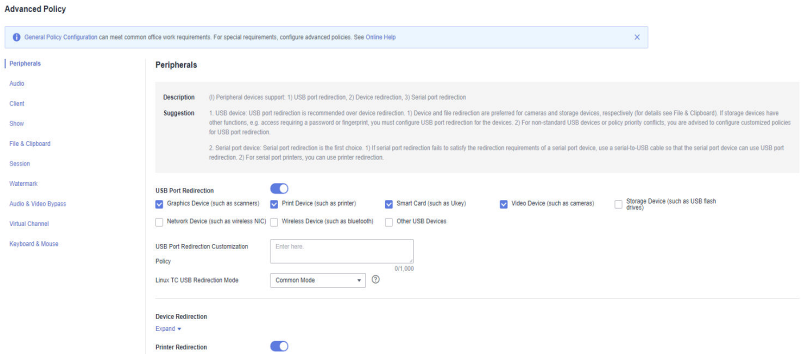
Step 6 Edit an advanced policy.

1. On the **General Policy Configuration** page, click **Advanced Policy**.

   The **Advanced Policy** page is displayed.

2. Configure an advanced policy, as shown in **Figure 6-2**. For details about the advanced policy parameters, see **6.1.1.2 Creating an Advanced Policy**.

Figure 6-2 Configuring an advanced policy



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

Peripherals

Description (I) Peripheral devices support: 1) USB port redirection, 2) Device redirection, 3) Serial port redirection

Suggestion 1. USB device: USB port redirection is recommended over device redirection. 1) Device and file redirection are preferred for cameras and storage devices, respectively (for details see File & Clipboard). If storage devices have other functions, e.g. access requiring a password or fingerprint, you must configure USB port redirection for the devices. 2) For non-standard USB devices or policy priority conflicts, you are advised to configure customized policies for USB port redirection.

2. Serial port device: Serial port redirection is the first choice. 1) If serial port redirection fails to satisfy the redirection requirements of a serial port device, use a serial-to-USB cable so that the serial port device can use USB port redirection. 2) For serial port printers, you can use printer redirection.

USB Port Redirection ●

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

□ Network Device (such as wireless NIC) □ Wireless Device (such as bluetooth) □ Other USB Devices

USB Port Redirection Customization Policy: Enter here. 0/1,000

Linux TC USB Redirection Mode: Common Mode

Device Redirection

Printer Redirection ●

Step 7 Click **OK** to save the configured policy information.

An end user must log in to the desktop again for the new policy to take effect.

----End

6.1.3 Exporting a Policy

Scenario

You can create projects in multiple areas. The policies of each project must be the same. You can export the configured policies of an area and import the policies to the target areas.

Prerequisites

Desktop policies have been configured for a workspace.

Constraints

Only policies customized by the administrator can be exported.

Procedure

Step 1 Log in to the console.

Step 2 Choose **Policies** > **Protocol Policy**.

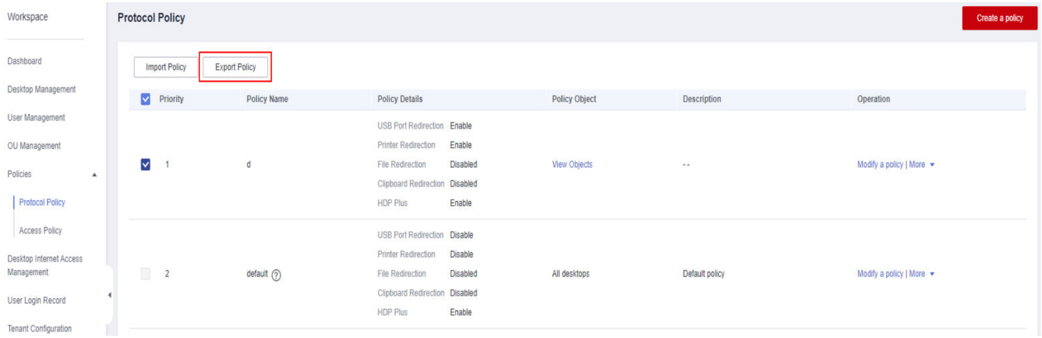
The **Protocol Policy** page is displayed.

Step 3 Select the policies to be exported and click **Export Policy**.

NOTE

- You can select a maximum of 10 policies to export.

Figure 6-3 Exporting a policy



☑ Priority	Policy Name	Policy Details	Policy Object	Description	Operation
☑ 1	d	USB Port Redirection Enable Printer Redirection Enable File Redirection Disabled Clipboard Redirection Disabled HDP Plus Enable	View Objects	--	Modify a policy | More ▾
□ 2	default ⓘ	USB Port Redirection Disable Printer Redirection Disable File Redirection Disabled Clipboard Redirection Disabled HDP Plus Enable	All desktops	Default policy	Modify a policy | More ▾

Step 4 Record the path where the ***xxx*.xml** file is stored.

NOTE

You can customize a path to store the file for easy selection during policy import.

----End

6.1.4 Importing a Policy

Scenario

You can create projects in multiple areas. The policies of each project must be the same. You can export the configured policies of an area and import the policies to the target areas.

Prerequisites

You have obtained the policy file (xxx.xml) exported.

Constraints

- The policy name in the file to be imported should be different from the names of existing policies in the destination.
- The maximum of 10 policies can be included in the file to be imported. It is not advised importing an integration of multiple policy files.
- By default, a maximum of 50 policies can exist in an area. If the number of policies exceeds the quota, the file cannot be imported.

Procedure

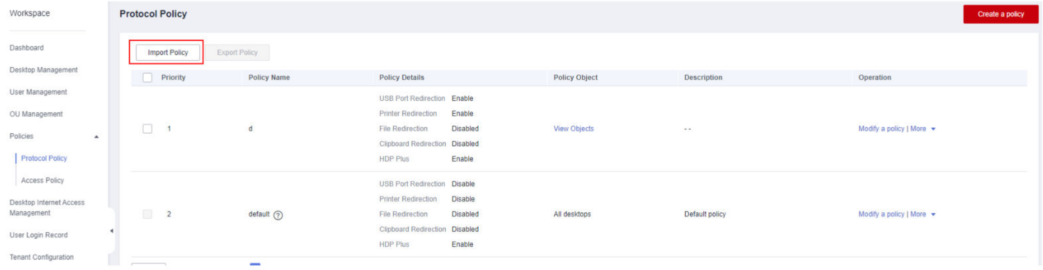
Step 1 Log in to the console.

Step 2 Choose **Policies** > **Protocol Policy**.

The **Protocol Policy** page is displayed.

Step 3 Click **Import Policy**.

Figure 6-4 Importing a policy



Priority	Policy Name	Policy Details	Policy Object	Description	Operation
1	d	USB Port Redirection Enable Printer Redirection Enable File Redirection Disabled Clipboard Redirection Disabled HDP Plus Enable	View Objects	--	Modify a policy | More
2	default	USB Port Redirection Disable Printer Redirection Disable File Redirection Disabled Clipboard Redirection Disabled HDP Plus Enable	All desktops	Default policy	Modify a policy | More

Step 4 Select the obtained policy file (xxx.xml) and click **Open**.

NOTE

- If a message indicating that the quota is insufficient is displayed when you import the xxx.xml file, increase the quota and import the file again. For details about how to increase quota, see **How Do I Increase My Quotas?**
- If a message indicating that the policy name already exists is displayed when you import the xxx.xml file, change the policy name and import the file again. For details about how to change policy name, see **How Do I Do If a Message Is Displayed Indicating Duplicate Policy Names During Policy Import?**

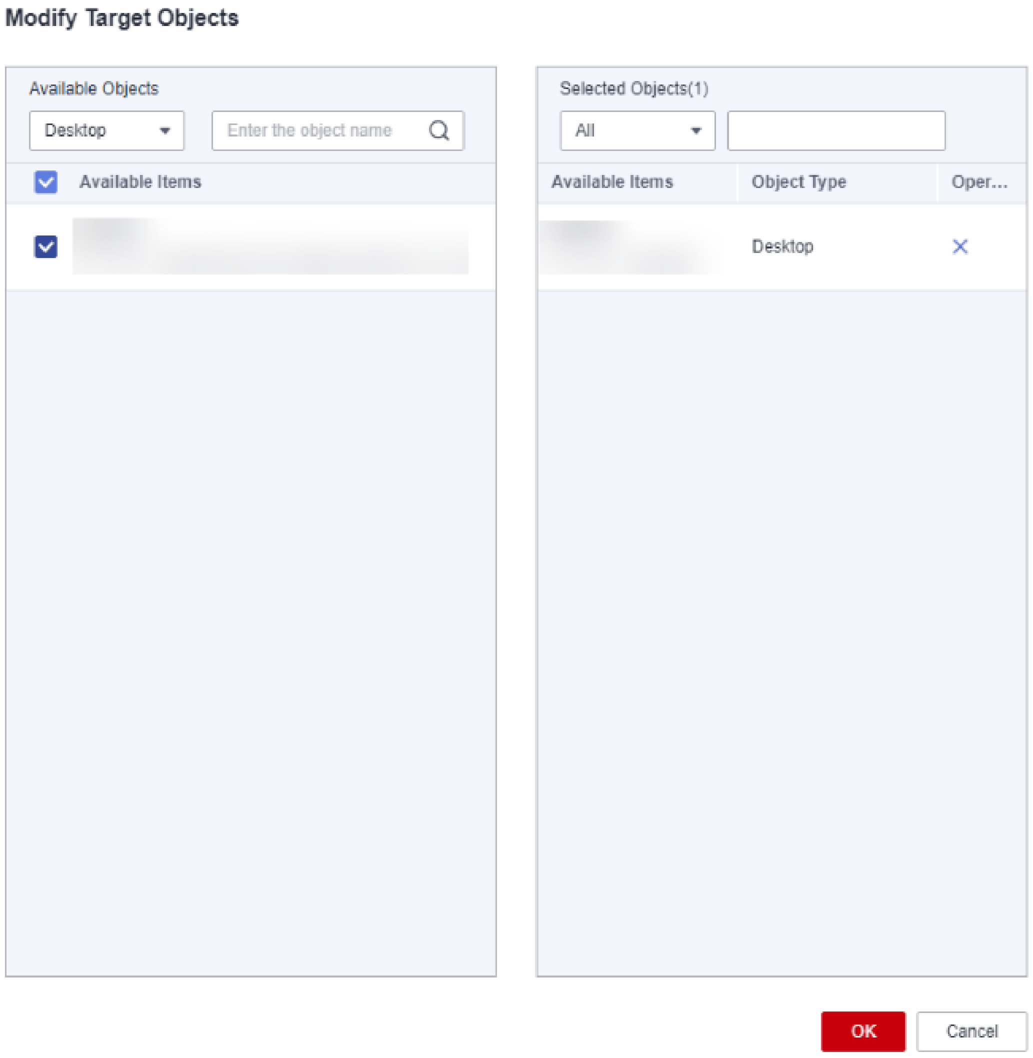
Step 5 Locate the row that contains the imported policy, and click **More** > **Modify Policy Object** in the **Operation** column.

NOTE

The policy file exported does not contain the application object information of policies. You need to reconfigure the information.

Step 6 In the available objects on the left, select the objects to which the policies apply based on the required object type.

Figure 6-5 Selecting objects



Modify Target Objects

Step 7 Click **Next: Finish**.

After the policies are configured for the objects, they take effect after the objects logs in to the desktop next time.

NOTE

The imported policies are prioritized based on the priority of the existing policies (The default policy has the lowest priority.) of the current tenant and their own priority in the imported file. For example, if the priorities of three imported policies are 1, 5, and 7 and the priorities of three existing policies of the current tenant are 1, 2, and 3 (default policy), the priorities of the six policies are 1 (the existing policy whose priority is 1), 2 (the existing policy whose priority is 2), 3 (the policy whose priority is 1 in the imported file), 4 (the policy whose priority is 5 in the imported file), 5 (the policy whose priority is 7 in the imported file), and 6 (the default policy).

----End

6.1.5 Deleting a Policy

Scenarios

You can delete created policies that are no longer needed.

Constraints

The default policy cannot be deleted.

Procedure

Step 1 Log in to the console.

Step 2 Choose **Policies** > **Protocol Policies**.

The **Protocol Policies** page is displayed.

Step 3 Delete policies.

- Deleting one policy: In the **Operation** column of the policy to be deleted, choose **More** > **Delete**. In the dialog box displayed, click **OK**.
- Deleting multiple policies: Check the boxes of the policies to be deleted, click **Delete** above the list, and then click **OK** in the dialog box displayed.

📖 NOTE

A policy in use on the desktop becomes invalid after it is deleted.

----End

6.2 Access Policy Management

6.2.1 Direct Connect Access Management

6.2.1.1 Creating an Access Policy

Scenario

You can create different access policies to restrict users in different positions to access desktops using Internet access address or only using Direct Connect access address.

Prerequisites

- You have purchased desktops for users in the current project.
- The Internet access address and Direct Connect access address have been enabled for the current project.

📖 NOTE

For details about how to configure the network access mode, see **8.1.5 Changing the Internet Access Mode**.

Constraints

- If Internet access address is not enabled, the configured access policy cannot take effect. That is, all users can access the cloud desktop only using Direct Connect access address.
- If Direct Connect access address is not enabled and an access policy is created, the selected users cannot use desktops.

Procedure

Step 1 Log in to the Workspace console.

Step 2 Choose **Policies** > **Access Policy**.

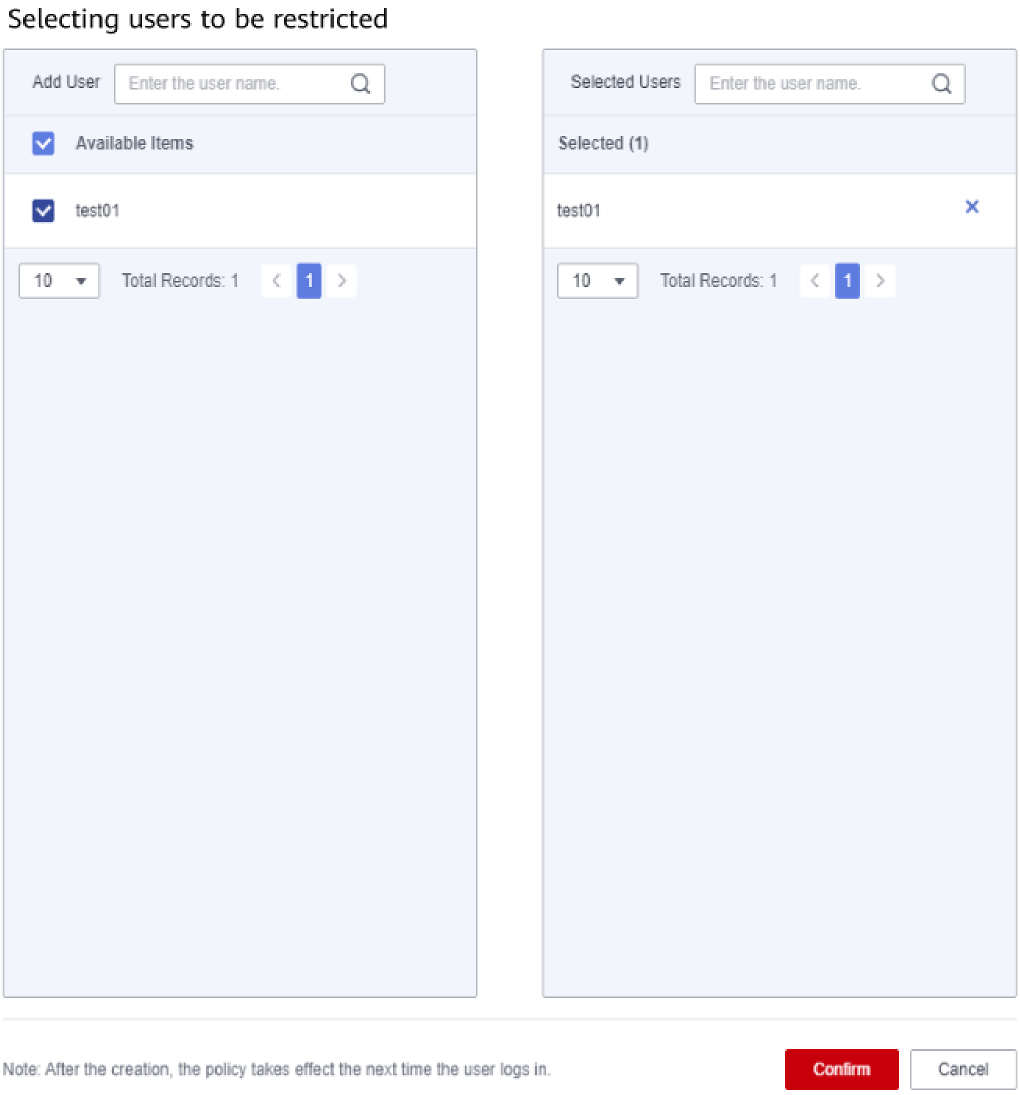
The **Access Policy** page is displayed.

Step 3 Click the button for creating a policy.

The **Adding a Private Line Network Access Policy** page is displayed.

Step 4 Select the users whose network access mode needs to be restricted, as shown in **Figure 6-6**.

Figure 6-6 Selecting users to be restricted



Selecting users to be restricted

Add User	Enter the user name.
☑	Available Items
☑	test01

10 Total Records: 1 1

Selected Users	Enter the user name.
Selected (1)	
test01	×

10 Total Records: 1 1

Note: After the creation, the policy takes effect the next time the user logs in.

NOTE

- In the **Add User** area on the left, enter a username to search for the desired user.
- In the **Selected Users** area on the right, enter a username to check whether the user to be restricted to use only Direct Connect is selected.

Step 5 Click **Confirm**.

NOTE

After the policy is created, it takes effect upon the next login of the user.

----End

6.2.1.2 Modifying an Access Policy

Scenario

When the position of a user changes, you can modify the policy object to adjust the network access mode of the user.

Prerequisites

- You have purchased desktops for users in the current project.
- The Internet access address and Direct Connect access address have been enabled for the current project.

Procedure

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

Step 2 Choose **Policies** > **Access Policy**.

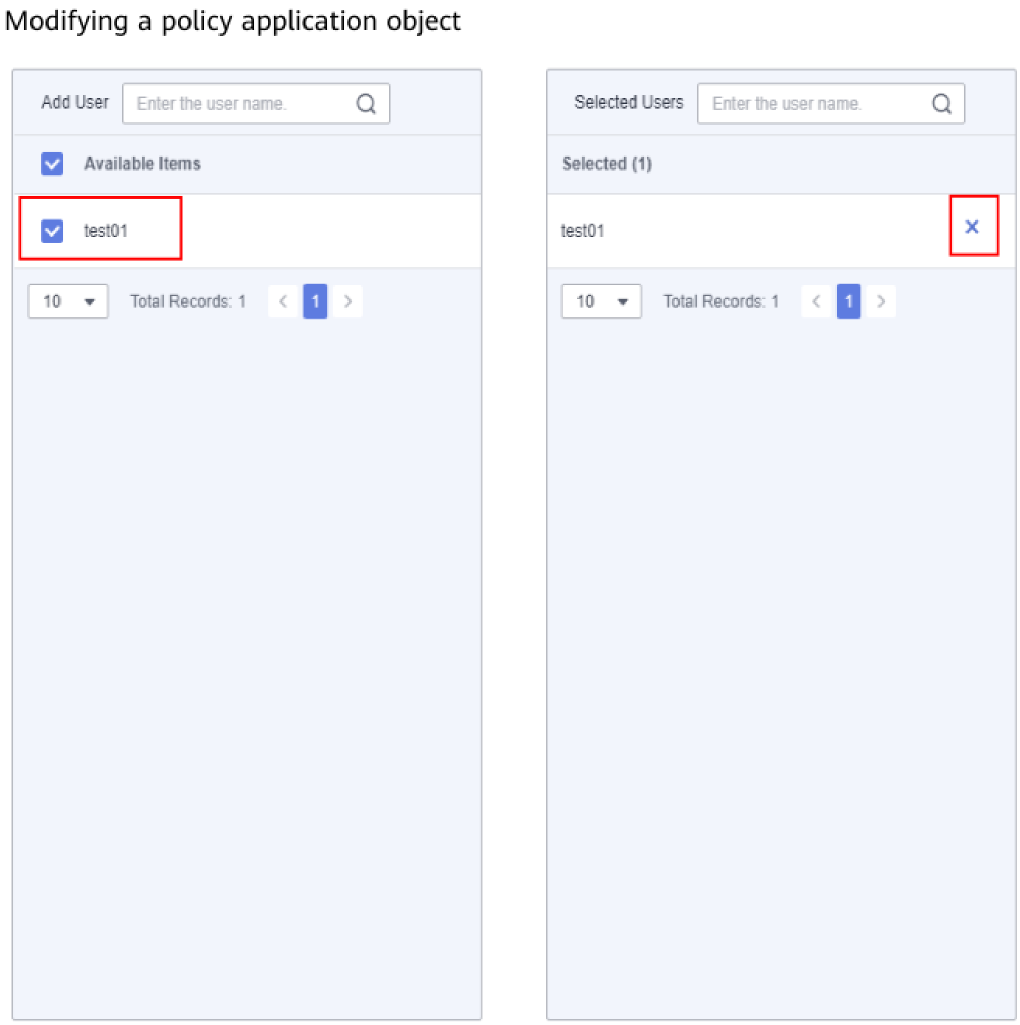
The **Access Policy** page is displayed.

Step 3 Click **Modify Target Objects**.

The **Modifying a Policy Application Object** page is displayed.

Step 4 In the **Available Items** on the left, select users who need to be restricted to access the desktops only using Direct Connect access address. In the **Selected** on the right, click ✕ to delete a user from the restricted user list, as shown in **Figure 6-7**.

Figure 6-7 Modifying a policy object



Step 5 Click **OK**.

NOTE

After the policy is modified, it takes effect upon the next login of the user.

----End

6.2.1.3 Deleting an Access Policy

Scenarios

If users in the current project do not need to use different network access modes, you can delete the configured access policies.

Prerequisite

It has been confirmed that users in the current project do not need to use different network access modes.

Procedure

Step 1 Log in to the management console.

Step 2 Choose **Policies** > **Access Policy**.

The **Access Policy** page is displayed.

Step 3 Click **Delete** in the row of the target policy.

The **Deletion policy** page is displayed.

Step 4 Click **OK**.

----End

6.2.2 Internet Access IP Address Control

Scenarios

You can enable or disable Internet access IP address control to restrict the Internet access of terminals. Enabling such control will prohibit the Internet access of all terminal users. You can set a whitelist of IP addresses for Internet access. Clients using these IP addresses can connect to cloud desktops via the Internet.

NOTE

If you do not set a whitelist after enabling Internet access IP address control, Internet access is prohibited for all terminals.

Prerequisites

Internet access has been enabled for the current project.

Procedure

Step 1 Log in to the console.

Step 2 Choose **Policies** > **Access Policies**.

The **Access Policies** page is displayed.

Step 3 Select the **Internet Access IP Address Control** tab.

Enabling Internet access IP address control

Step 4 Configure Internet access IP address control.

- : enabled. Only the terminals within the added IP address segment can access the Internet.
- : disabled. Terminals in all IP address segments can access the Internet.

Step 5 Select a restriction range.

- You can allow some IP addresses to access the Internet. In this case, only the terminals within the added IP address segment can access the Internet.

  After allowing some IP addresses to access the Internet, click **Add** to go to the **Add Internet IP Address Access Control** page.

Select a method of adding:

a. **Add manually**:

   i. Enter the IP address and subnet mask of the terminal.

   ii. Click **Add** below to add multiple records.

   iii. Click **OK**.

b. **Batch add**:

   i. Click **Download Template** and enter the IP address and subnet mask of the terminal in the template.

   ii. Click **Add** to upload a local template file.

   NOTE

   Upload an Excel file no larger than 1 MB.

   iii. Click **OK**.

- You can prohibit all IP addresses from accessing the Internet. In this case, all terminals cannot access the Internet.

Deleting IP addresses

NOTE

To remove the Internet access restriction on a terminal, delete the IP address of the terminal from the IP address list.

Step 6 Choose **Policies** > **Access Policies**.

The **Access Policies** page is displayed.

Step 7 In the top navigation bar, select the **Internet Access IP Address Control** tab.

Step 8 In the IP address list, delete the desired IP addresses.

- To delete one IP address, click **Delete** in the **Operation** column of the IP address and click **OK**.
- To batch delete IP addresses, select the IP addresses from the IP address list, click **Delete** above the list, and click **OK**.

Disabling Internet access IP address control

Step 9 Toggle off on the right of **Internet Access IP Address Control**. The **Disable Internet IP Address Access Control** dialog box is displayed.

NOTE

Disabling this policy allows all terminals to access cloud desktops using Internet IP addresses.

Step 10 Click **OK**.

----End

6.3 Terminal-Desktop Binding Relationship Management

6.3.1 Enabling or Disabling Terminal-Desktop Binding

Scenario

The administrator can enable or disable the functions of terminal-desktop binding and automatic binding upon desktop login in the current project. After terminal-desktop binding and automatic binding upon desktop login are enabled, you can specify the terminals that can be used to log in to the desktop based on the binding relationship. After terminal-desktop binding is disabled, the recorded binding relationship becomes invalid. That is, any supported terminals can be used to log in to the desktop.

Constraints

This feature is not applicable to Android mobile terminals and Android TCs.

Procedure

Step 1 Log in to the console.

Step 2 In the navigation pane, choose **Policies** > **Terminal and Desktop Binding**.

The terminal-desktop binding list is displayed.

Step 3 Enable or disable the terminal-desktop binding function as required.

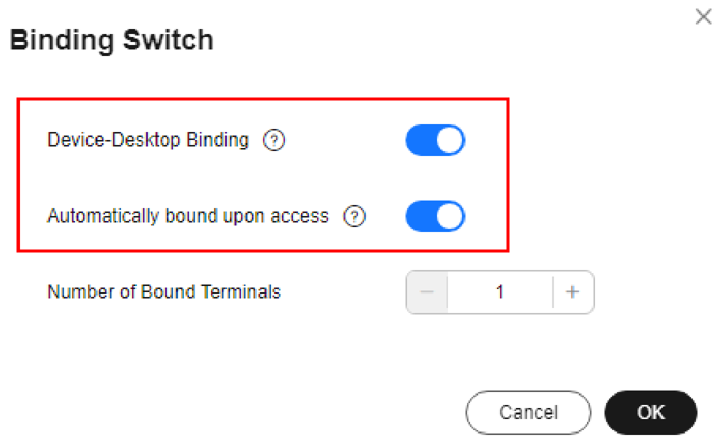
- Enable terminal-desktop binding:
  a. Click **Binding Settings**.
  b. On the displayed dialog box, toggle on the switch of **Device-Desktop Binding**.
  c. Determine whether to toggle on the switch of **Automatically bound upon access** and set **Number of Bound Terminals** (value range: 1–10).

     NOTE

     - **Automatically bound upon access** can be enabled only after **Device-Desktop Binding** is enabled.
     - After **Automatically bound upon access** is enabled, the MAC address is automatically bound when the cloud desktop is accessed from a terminal.

  d. Click **OK**, as shown in Figure 6-8.

Figure 6-8 Enabling terminal-desktop binding



Binding Switch

Device-Desktop Binding: on

Automatically bound upon access: on

Number of Bound Terminals: 1

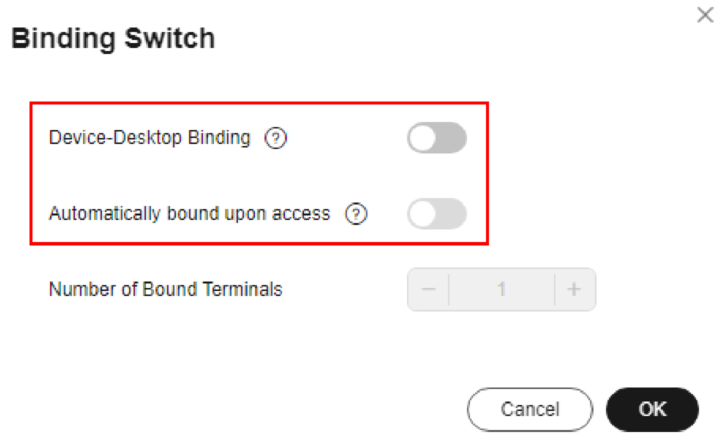
- Disable terminal-desktop binding:
  a. Click **Binding Settings**.
  b. On the displayed dialog box, toggle off the switch of **Device-Desktop Binding**.

  NOTE

  - The switch of **Automatically bound upon access** can be toggled off separately.
  - Toggling off the switch of **Device-Desktop Binding** will disable **Automatically bound upon access**.

  c. Click **OK**, as shown in **Figure 6-9**.

Figure 6-9 Disabling terminal-desktop binding



Binding Switch

Device-Desktop Binding: off

Automatically bound upon access: off

Number of Bound Terminals: 1

----End

6.3.2 Creating a Binding Relationship

Scenarios

To restrict the application scenarios of a desktop, the administrator can bind the MAC address of a terminal to a desktop so that only the bound terminal can be used to log in to the desktop.

Constraints

This feature is not applicable to Android mobile terminals and Android TCs.

Prerequisites

- The name of the desktop to which the terminal is to be bound has been obtained on the Workspace console.
- The MAC address of the terminal to be bound has been obtained.

  NOTE

  See **How Do I Obtain the MAC Address of a Terminal?**
- The terminal-desktop binding function has been enabled by referring to **6.3.1 Enabling or Disabling Terminal-Desktop Binding**.

Procedure

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

Step 2 In the navigation pane, choose **Policies** > **Terminal-Desktop Binding**.

The terminal-desktop binding list is displayed.

Step 3 Record the binding relationship.

You can manually enter binding relationships or enter binding relationships in batches based on the number of binding relationships.

- **Add Manually**

  If a small number of desktops need to be bound to terminals, you can manually enter the information.

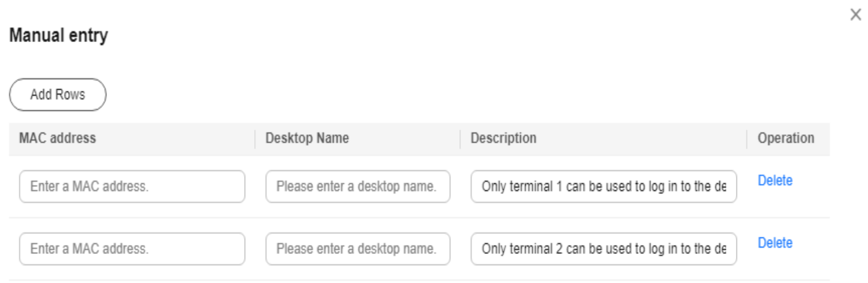
  a. Click **Add Manually**.

  b. On the displayed page, enter the MAC address, desktop name, and description, as shown in **Figure 6-10**.

     NOTE

     - The MAC address format is xx-xx-xx-xx-xx-xx.
     - One MAC address can be bound to multiple desktops.
     - A desktop can be bound to multiple MAC addresses.
     - Information cannot be entered if there are more than 100,000 binding relationships.

Figure 6-10 Entering binding information



Manual entry

MAC address	Desktop Name	Description	Operation
Enter a MAC address.	Please enter a desktop name.	Only terminal 1 can be used to log in to the de	Delete
Enter a MAC address.	Please enter a desktop name.	Only terminal 2 can be used to log in to the de	Delete

c. If multiple terminals need to be bound, click **Add Rows** to add binding information.

d. Click **OK**.

- **Batch Add**

  If a large number of desktops need to be bound to terminals, you can batch enter the information.

  a. Click **Batch Add**.

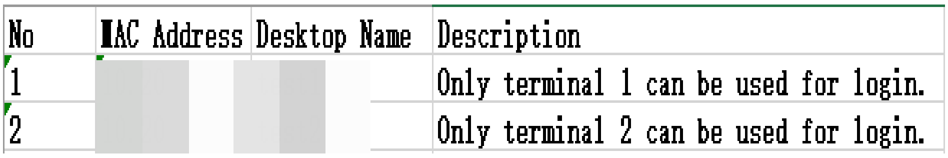
  b. On the displayed page, click **Download Template**.

  c. Open the downloaded template and enter the serial number, MAC address, desktop name, and description, as shown in **Figure 6-11**.

  NOTE

  - The MAC address format is xx-xx-xx-xx-xx-xx.
  - One MAC address can be bound to multiple desktops.
  - A desktop can be bound to multiple MAC addresses.
  - The maximum size of a file to be uploaded at a time is 1 MB, and only the .xlsx format is supported.
  - Information cannot be entered if there are more than 100,000 binding relationships. Information of up to 1,000 binding relationships can be entered at a time.

Figure 6-11 Batch entering binding information



No	IAC Address	Desktop Name	Description
1	[redacted]	[redacted]	Only terminal 1 can be used for login.
2	[redacted]	[redacted]	Only terminal 2 can be used for login.

d. Save and close the template file containing the binding information.

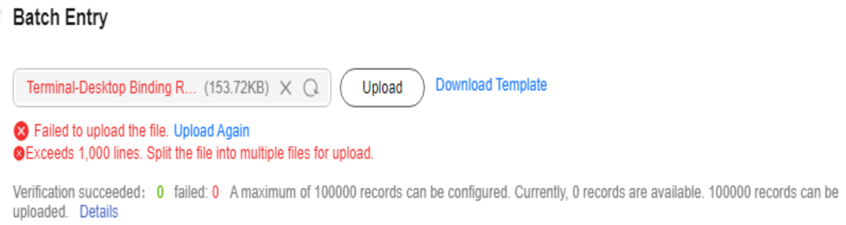
e. On the page of batch entering information, click **Upload**.

f. Select the file in which the binding information has been filled in **Step 3.d** and click **Open**.

The system verifies the correctness of the imported information and compares the information with that of the existing binding relationships.

- If a message indicating successful upload is displayed, the binding relationships in the file have been uploaded to the system. After clicking **Close**, you can view the uploaded binding relationships on the **Terminal-Desktop Binding** page.

- If a message indicating failed upload is displayed, the binding relationships in the file were not uploaded to the system. You can click **Details** to check the exception cause, modify the uploaded file according to the exception cause, and upload the file again by referring to **Step 3.d** to **Step 3.f**. If some binding relationships pass the verification, you can click **OK** to upload the verified binding relationships to the system. If you click **Cancel**, the batch upload is canceled.



Batch Entry

Terminal-Desktop Binding R... (153.72KB)

Failed to upload the file. Upload Again

Exceeds 1,000 lines. Split the file into multiple files for upload.

Verification succeeded: 0 failed: 0 A maximum of 100000 records can be configured. Currently, 0 records are available. 100000 records can be uploaded. Details

NOTE

If the format of the imported information is correct and the information does not conflict with the existing binding relationships, but a message indicating upload failure still appears, click **Re-upload** to try again. If the upload still fails, **submit a service ticket** for technical support.

----End

6.3.3 Modifying a Binding Relationship

Scenario

If the binding relationship between a terminal and a desktop is incorrect or needs to be modified, the administrator can edit the existing binding relationship.

Prerequisites

The desktop name or the MAC address of the terminal whose binding relationship is to be modified has been obtained.

Procedure

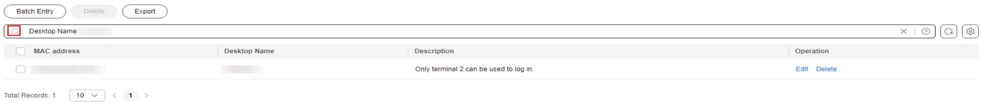
Step 1 **Log in to the console**.

Step 2 In the navigation pane, choose **Policies** > **Terminal and Desktop Binding**.

The terminal-desktop binding list is displayed.

Step 3 Find the binding relationship to be modified.

- Enter the MAC address or desktop name in the search box and click 🔍 to select the binding relationships to be modified.



MAC address	Desktop Name	Description	Operation
[redacted]	[redacted]	Only terminal 2 can be used to log in.	Edit Delete

- You can find the desired binding relationships in the binding relationship list.

Step 4 Click **Edit** in the **Operation** column of the desired binding relationship.

Step 5 Modify the MAC address, desktop name, and description as required, and click **OK**.

----End

6.3.4 Deleting a Binding Relationship

Scenario

If the terminals that can be used to log in to a desktop are no longer restricted, you can delete the existing binding relationships.

Prerequisites

The desktop names or the MAC addresses of the terminals whose binding relationship are to be deleted have been obtained.

Procedure

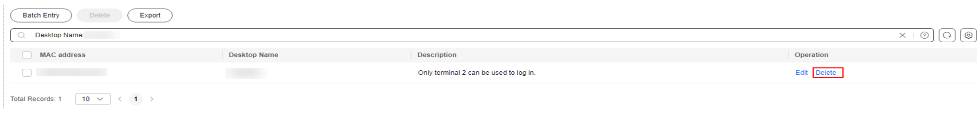
Step 1 Log in to the console.

Step 2 In the navigation pane, choose **Policies** > **Terminal and Desktop Binding**.

The terminal-desktop binding list is displayed.

Step 3 Find the binding relationship to be deleted.

- Enter the MAC address or desktop name in the search box and click 🔍 to select the binding relationships to be deleted.



MAC address	Desktop Name	Description	Operation
[redacted]	[redacted]	Only terminal 2 can be used to log in.	Edit Delete

- You can find the desired binding relationships in the binding relationship list.

Step 4 Select a deletion method based on the number of binding relationships to be deleted.

- **Deleting a single binding relationship**

  You can delete a single binding relationship.

  a. Click **Delete** in the **Operation** column of the desired binding relationship.

  b. On the page displayed, click **OK**.

- **Batch deleting binding relationships**

  If you need to delete a large number of binding relationships, you can delete them in batches.

  a. Select the desired binding relationships and click **Delete** above the relationship list. The deletion confirmation page is displayed.

  b. To confirm the deletion, enter **DELETE**, click **Auto Enter**, and click **OK**.

----End

6.3.5 Exporting a Binding Relationship List

Scenario

The administrator can export the recorded binding relationships to the local PC.

Prerequisites

Binding relationships have been recorded.

Procedure

Step 1 Log in to the console.

Step 2 In the navigation pane, choose **Policies** > **Terminal and Desktop Binding**.

The terminal-desktop binding list is displayed.

Step 3 Click **Export** to export the existing binding relationship list.

----End

7 OU Management

Scenarios

An organization unit (OU) is a container that organizes objects into logical management groups to manage resources in the containers. An OU contains one or more objects, such as users, computers, printers, applications, file sharing, and other sub-OUs.

Prerequisites

- A Windows AD domain has been configured.
- Before creating an OU, you need to create OUs on the AD server.

Procedure

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

Step 2 Click **OU Management**.

The **OU Management** page is displayed.

Step 3 Click **Create OU**.

The **Create OU** dialog box is displayed.

Step 4 Enter the OU name.

NOTE

- In *OU1*/*OU2*/*OU3*..., **/** separates layers of OUs. Enter an OU name that exists in the domain.
- OU naming rule: Only letters, digits, spaces, and special characters (-_/$!@*?.) are allowed. The OU name cannot contain slashes (/) but multiple layers of OU can be separated using slashes (/). A maximum of five layers of OUs are supported. Spaces are not allowed before and after slashes (/). For example, the format of a layer-3 OU is **ab/cd/ef**.

Step 5 Select a domain name and enter the description.

Step 6 Click **OK**. The OU is created.

----End

Associated Operation

If the name of an OU on the AD server is changed or an OU has been deleted, you can modify or delete the OU in the **OU Management** list.

8 Tenant Configuration

8.1 Basic Configuration

8.1.1 Configuring an AD Domain

Scenario

This section describes how to configure the networks of the AD domain and domain user on the console. If the created desktop needs to connect to the Windows AD domain, refer to this section when purchasing a desktop for the first time.

NOTE

- After you purchase a desktop for the first time, your selection (connecting to the AD domain or canceling the connection to the AD domain) cannot be changed. Exercise caution when performing this operation.
- Multiple subprojects in the same region can interconnect with the same Windows AD server.

Prerequisites

If an AD domain needs to be configured, enable related ports on the AD server by referring to **Configuring Network Connection Between Workspace and Windows AD** (If multiple subprojects interconnect with the same AD server, connect the network of these subprojects to the network of Windows AD by referring to **17.3 Configuring Network Connection Between Cloud Desktops and Windows AD**.) and prepare the following data:

- Domain
- Domain Administrator Account

- Domain Administrator Password
- Active Domain Controller Name
- Active Domain Controller IP Address
- Active DNS Server IP Address
- (Optional) Backup Domain Controller Name
- (Optional) Backup Domain Controller IP Address
- (Optional) Backup DNS Server IP Address

Procedure

(Optional) Setting an enterprise ID

Step 1 Log in to the console.

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

The **Basic Settings** page is displayed.

Step 3 Set the enterprise ID.

NOTE

- **Enterprise ID** is the unique identifier of your tenant environment. End users need to enter the enterprise ID when logging in to the system.

  You are advised to use identifiable fields such as the enterprise name pinyin as the enterprise ID. The enterprise ID can be changed.
- The enterprise ID contains a maximum of 32 characters and can only include digits and letters.

Configuring the AD domain

Step 4 Configure the connection to Windows AD.

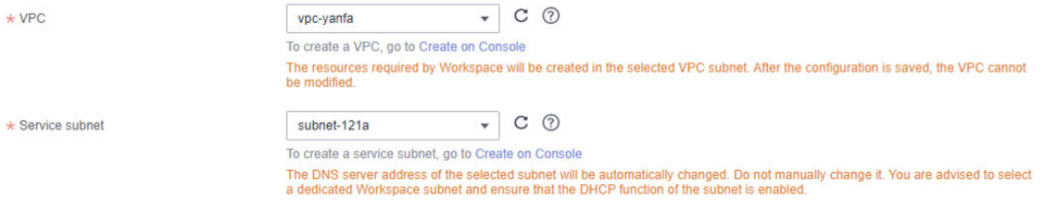
- **Domain Name**: Windows AD domain name
- **Domain Administrator Account**: administrator name for logging in to the Windows AD server
- **Domain Administrator Password**: administrator password for login
- **Active Domain Controller Name**: It can be the host name of the AD service or the combination of the host name of the AD service and the domain name.
  - The host name of the AD service: Log in to the AD server using the corresponding IP address, choose **Control Panel** > **System and Security** > **System** to obtain the computer name as the host name, replace the letters of the host name with uppercase letters, and use the host name as the active domain controller name. For example, if the host name is **Fa-2016Ad-01**, the active domain controller name is **FA-2016AD-01**.
  - The combination of the host name of the AD service and the domain name: Log in to the AD server using the corresponding IP address, choose **Control Panel** > **System and Security** > **System**, obtain the computer name as the host name, add the domain name to the host name, and use the combined name as the active domain controller name. For example, if the host name is **Fa-2016Ad-01** and the domain name is **vdesk.cloud.com**, the active domain controller name is **Fa-2016Ad-01.vdesk.cloud.com** or **FA-2016AD-01.vdesk.cloud.com**.

- **IP Address of Active Domain Controller**: service plane IP address of the Windows AD server
- **Active DNS IP Address**: service plane IP address of the DNS server
- **Delete Computer Objects on AD**
  - **Yes**: When a desktop is deleted, the computer object in the AD domain is also deleted.
  - **No**: When a desktop is deleted, the computer object in the AD domain is not deleted.
- **(Optional) Advanced Settings**
  - **Backup Domain Controller Name**
  - **Backup Domain Controller IP Address**
  - **Backup DNS IP Address**

Network settings

Step 5 Configure **VPC** and **Service Subnet**, as shown in **Figure 8-1**.

Figure 8-1 VPC and service subnet



* VPC: vpc-yanfa

To create a VPC, go to Create on Console

The resources required by Workspace will be created in the selected VPC subnet. After the configuration is saved, the VPC cannot be modified.

* Service subnet: subnet-121a

To create a service subnet, go to Create on Console

The DNS server address of the selected subnet will be automatically changed. Do not manually change it. You are advised to select a dedicated Workspace subnet and ensure that the DHCP function of the subnet is enabled.

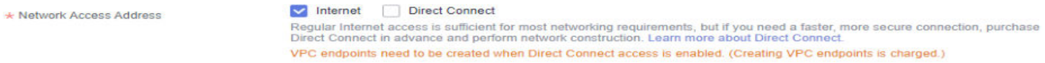
- To configure an existing VPC, select an existing VPC and service subnet.
- To configure a new VPC, click **Create on Console**, and create a VPC and service subnet. For details, see **Creating a VPC**.

NOTE

- The resources required by Workspace will be created in the selected VPC subnet. After the desktop is purchased for the first time, the VPC cannot be modified.
- A VPC is an isolated, configurable, and manageable virtual network environment for cloud desktops, facilitating internal network management and configuration. Your cloud desktops will be created in the selected VPC subnet for your access to the resources and applications on the enterprise intranet.
- Each desktop has a network interface card (NIC) of a service subnet. The service subnet is used to interconnect desktops and cloud hosts or enterprise intranets for easy access of applications and resources on cloud hosts or enterprise intranets.
- The DNS server address of the selected subnet will be automatically changed. Do not manually change it. You are advised to select a dedicated Workspace subnet and ensure that the DHCP function is enabled for the subnet.

Step 6 Select a network access mode, as shown in **Figure 8-2**. By default, **Internet** is selected. You can select multiple options.

Figure 8-2 Network access mode



* Network Access Address: ☑ Internet □ Direct Connect

Regular Internet access is sufficient for most networking requirements, but if you need a faster, more secure connection, purchase Direct Connect in advance and perform network construction. Learn more about Direct Connect.

VPC endpoints need to be created when Direct Connect access is enabled. (Creating VPC endpoints is charged.)

NOTE

- If you have high requirements on network quality and security, you can purchase Direct Connect and perform network construction in advance. For details, see the **Direct Connect Documentation**.
- To enable **Direct Connect**, you need to create an endpoint service client which is charged. If you disable Direct Connect, the endpoint service client will be deleted.
- The Direct Connect access mode provides the load balancing capability. You do not need to add a third-party load balancing device in front of the access address.
- If you want to upgrade the client online through Direct Connect, you need to configure an endpoint (free) for accessing OBS intranet address. For details, see **Configuring a VPC Endpoint for Accessing OBS Using the OBS Private Address**. For details about the endpoint service of the corresponding site, submit a service ticket.

Step 7 Click **Save Configuration** to start deploying cloud desktops.

Cloud desktops are successfully deployed, that is, Workspace has been enabled. You can **purchase a desktop**.

If the service fails to be enabled, perform operations as prompted.

----End

Follow-up Operations

To improve network security, you can enable LDAPS so that cloud desktops can communicate with AD server applications through LDAPS. For details, see **8.1.2 Configuring AD Domain Certificate Authentication**.

8.1.2 Configuring AD Domain Certificate Authentication

Scenarios

When AD domain authentication is used, you can enable LDAPS so that cloud desktops can communicate with AD server applications through LDAPS, improving network security.

Prerequisites

- You have obtained the password of the AD domain administrator.
- LDAPS has been enabled on the AD server, and the CA root certificate file has been exported from the AD server.

  NOTE

  - The CA root certificate file must be in the PEM format.
  - For details about how to enable LDAPS, see **Enabling LDAPS for an AD Server**. For details about how to export the root certificate of the LDAPS-enabled AD server, see **Exporting the Root Certificate of the LDAPS-enabled AD Server**.

Procedure

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

Step 2 Click **Tenant Configuration**.

The **Tenant Configuration** page is displayed.

Step 3 Click **Modify domain configuration**.

Step 4 Enter the domain administrator password.

Step 5 Expand **Advanced Settings** and enable **Using LDAPS**.

Step 6 In the **Key certificate** area, click **Certificate Upload** and select the certificate file in **Prerequisites**.

NOTE

Only certificate files in the PEM format can be imported.

Step 7 Click **OK**.

----End

8.1.3 Changing the Domain Administrator Password

Scenario

In a scenario where the exiting AD domain is used, to ensure system security, the domain administrator password needs to be changed periodically. You are advised to change the password every three months. You can change the password on the Workspace console.

NOTE

If the enterprise uses an existing AD domain, the period for changing the domain administrator password depends on the preset password policy. Change the domain administrator password on the AD server first, and then perform the following operations.

Prerequisites

An AD domain has been configured.

Procedure

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

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

The **Basic Settings** page is displayed.

Step 3 Click **Change Password**

The **Change Password** dialog box is displayed.

Step 4 Set the password.

- Enter a new password.
- Confirm the password.

NOTE

- A password must be a string of 8 to 64 characters.
- A password must contain at least two types of the following characters: letters, digits, and special characters (`~!@#$%^&*()-_=+\|[{}];:'",<.>/? or space).
- A password should be different from the username or the username spelled backwards.
- The password must start with a letter.

Step 5 Click **OK**.

----End

8.1.4 Modifying Domain Configurations

Scenario

On the Workspace console, you can modify domain configurations on the **Tenant Configuration** page as required.

Prerequisites

An AD domain has been configured.

Procedure

Step 1 Log in to the console.

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

The **Basic Settings** page is displayed.

Step 3 Click **Modify Domain Configuration**.

The window for modifying domain configuration is displayed.

Step 4 Modify the domain configurations.

- **Domain Administrator Account**: administrator name for logging in to the Windows AD server
- **Domain Administrator Password**: administrator password for login
- **Active Domain Controller Name**: It can be the host name of the AD service or the combination of the host name of the AD service and the domain name.
  - The host name of the AD service: Log in to the AD server using the corresponding IP address, choose **Control Panel** > **System and Security** > **System** to obtain the computer name as the host name, replace the letters of the host name with uppercase letters, and use the host name as the active domain controller name. For example, if the host name is **Fa-2016Ad-01**, the active domain controller name is **FA-2016AD-01**.
  - The combination of the host name of the AD service and the domain name: Log in to the AD server using the corresponding IP address, choose **Control Panel** > **System and Security** > **System**, obtain the computer name as the host name, add the domain name to the host name, and use the combined name as the active domain controller name. For

example, if the host name is **Fa-2016Ad-01** and the domain name is **vdesk.cloud.com**, the active domain controller name is **Fa-2016Ad-01.vdesk.cloud.com** or **FA-2016AD-01.vdesk.cloud.com**.

- **IP Address of Active Domain Controller**: service plane IP address of the Windows AD server
- **Active DNS IP Address**: service plane IP address of the DNS server
- **Delete Computer Objects on AD**
  - **Yes**: When a desktop is deleted, the computer object in the AD domain is also deleted.
  - **No**: When a desktop is deleted, the computer object in the AD domain is not deleted.
- **Advanced Settings**
  - **Backup Domain Controller Name**
  - **Backup Domain Controller IP Address**
  - **Backup DNS IP Address**
  - **Using LDAPS**: disabled by default
    - ○: disabled
    - ●: enabled
    - **Key Certificate**: Click **Certificate Upload**.

Step 5 Click **OK**.

The domain configuration has been modified.

----End

8.1.5 Changing the Internet Access Mode

Scenarios

On the Workspace console, you can change your Internet access mode.

Procedure

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

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

The **Basic Settings** page is displayed.

Step 3 Click **Disable** or **Enable** on the right of **Internet Access Address** or **Direct Connect Access Address**. Wait for about one minute for the change to take effect. For details, see **Table 8-1**.

NOTE

Workspace supports Internet access and Direct Connect access at the same time. At least one access mode must be enabled.

Table 8-1 Modifying the network access mode

Operation	Procedure
Disable Internet access	If **Direct Connect Access** and **Internet Access** are enabled, you can disable Internet access. 1. In the **Network Configuration** area, click **Disable** next to **Internet Access Address**. 2. In the confirmation dialog box, click **OK**.
Enable Internet access	After the Internet access address is disabled, you can enable Internet access again. After the function is enabled again, the IP address changes. You need to notify the desktop user to use the new IP address to access the desktop. 1. In the **Network Configuration** area, click **Enable** next to **Internet Access Address**. 2. In the confirmation dialog box, click **OK**.
Disable Direct Connect access	If **Direct Connect Access Address** and **Internet Access Address** are enabled, you can disable Direct Connect access. 1. In the **Network Configuration** area, click **Disable** next to **Direct Connect Access Address**. 2. In the confirmation dialog box, click **OK**.

Operation	Procedure
Enable Direct Connect access	Tenants who have enabled Direct Connect can configure Direct Connect access for cloud desktops. 1. In the **Network Configuration** area, click **Enable** next to **Direct Connect Access Address**. 2. In the displayed dialog box, configure **Direct Connect network segment**. NOTE – Check whether the service subnet of the cloud desktop and the subnet of the Direct Connect are in the same range. If yes, you do not need to configure the Direct Connect network segment. If no, you need to configure the Direct Connect CIDR block in the **Direct Connect network segment** area. You can view the service subnet of the cloud desktop and the subnet network segment of the Direct Connect on the VPC page. – A maximum of five network segments can be configured. Use semicolons (;) to separate multiple network segments. – The network segment is as follows: 192.168.11.0/24;172.10.240.0/20 3. In the **Enabling Direct Connect Access Addresses** dialog box, select **I have confirmed that I've confirmed that a VPC endpoint needs to be created to enable Direct Connect access. (Do not modify the VPC endpoint after creation. Otherwise, Direct Connect access will be affected. VPC endpoint creation is a charged service.)**. 4. In the confirmation dialog box, click **OK**. 5. (Optional) Modify the Direct Connect network segment. If the Direct Connect network segment is incorrect, click **Modify** on the right of **Direct Connect network segment** in the network configuration area. In the displayed dialog box, modify the network segment as required. If you want to perform this operation, enter **YES** or click **Auto Enter**, and click **OK**.

----End

8.1.6 Changing the Service Subnet

Scenario

On the Workspace console, you can change the service subnet based on your plan.

Procedure

Step 1 Log in to the console.

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

The **Basic Settings** page is displayed.

Step 3 Click **Modify Subnet**.

The service subnet list page is displayed.

Step 4 Select a desired service subnet based on your planned subnet information.

Step 5 Click **OK**.

----End

8.1.7 Canceling a Service

Scenarios

If you do not need to use the Workspace service of the current project (no subprojects) or a subproject anymore, you can delete the existing user desktops and application servers of Application Streaming. Then perform the following steps to cancel the Workspace service.

NOTE

- Resources (such as desktops and disks) of the tenant should be released before the service is canceled. If Internet access is enabled, billing of the EIP, NAT, and bandwidth that are not released will continue. Release them if they are no longer needed.

Procedure

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

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

The **Basic Settings** page is displayed.

Step 3 Click **Cancel Service** at the bottom of the page.

A dialog box for canceling the service is displayed.

Step 4 Click **OK**.

Step 5 Click **OK**.

----End

8.1.8 Reactivating a Service

Scenario

After you enable a service, if no desktop exists in the current project (no subprojects) or a subproject for more than 14 days, the system automatically locks the service. If a service is locked, you can purchase desktops and create users only after reactivating the service of the project or subproject.

Prerequisites

The service of the current project (no subprojects) or subproject has been locked.

Procedure

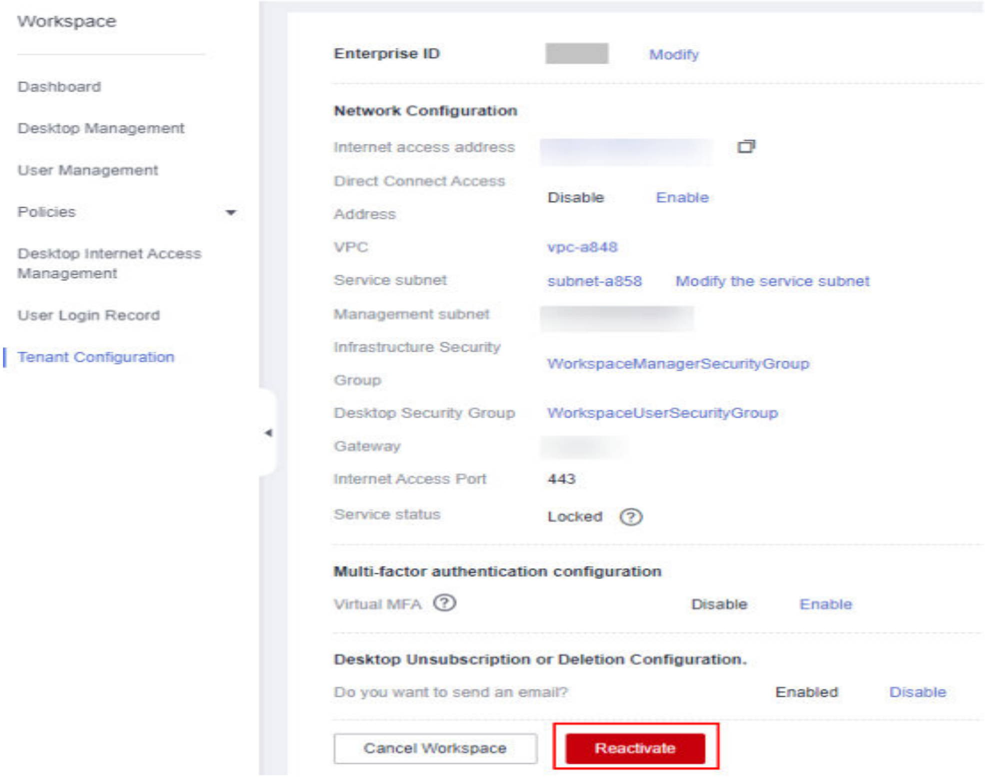
Step 1 Log in to the console.

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

The **Basic Settings** page is displayed.

Step 3 At the bottom of the page, click **Reactivate**, as shown in **Figure 8-3**.

Figure 8-3 Reactivating the service



Enterprise ID [redacted] Modify

Network Configuration

Internet access address [redacted]

Direct Connect Access Address Disable Enable

VPC vpc-a848

Service subnet subnet-a858 Modify the service subnet

Management subnet [redacted]

Infrastructure Security Group WorkspaceManagerSecurityGroup

Desktop Security Group WorkspaceUserSecurityGroup

Gateway [redacted]

Internet Access Port 443

Service status Locked

Multi-factor authentication configuration

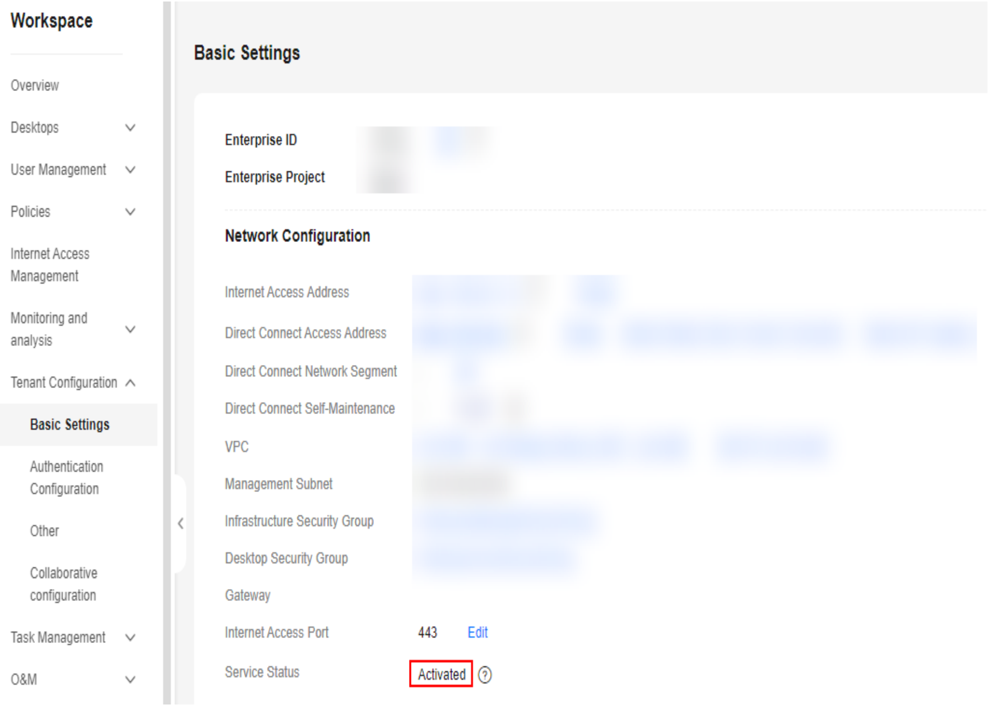
Virtual MFA Disable Enable

Desktop Unsubscription or Deletion Configuration.

Do you want to send an email? Enabled Disable

Wait until **Service Status** changes to **Activated**, as shown in **Figure 8-4**. Then, you can purchase desktops or create users.

Figure 8-4 Service activated



Basic Settings

Enterprise ID [redacted]

Enterprise Project [redacted]

Network Configuration

Internet Access Address [redacted]

Direct Connect Access Address [redacted]

Direct Connect Network Segment [redacted]

Direct Connect Self-Maintenance [redacted]

VPC [redacted]

Management Subnet [redacted]

Infrastructure Security Group [redacted]

Desktop Security Group [redacted]

Gateway

Internet Access Port 443

Service Status Activated

----End

8.1.9 Configuring Whether to Block Notification Emails for Desktop Unsubscription or Deletion

Scenarios

When you unsubscribe from or delete a desktop, you can determine whether to send a notification email to the user. The notification email informs the user of the desktop unsubscription or deletion.

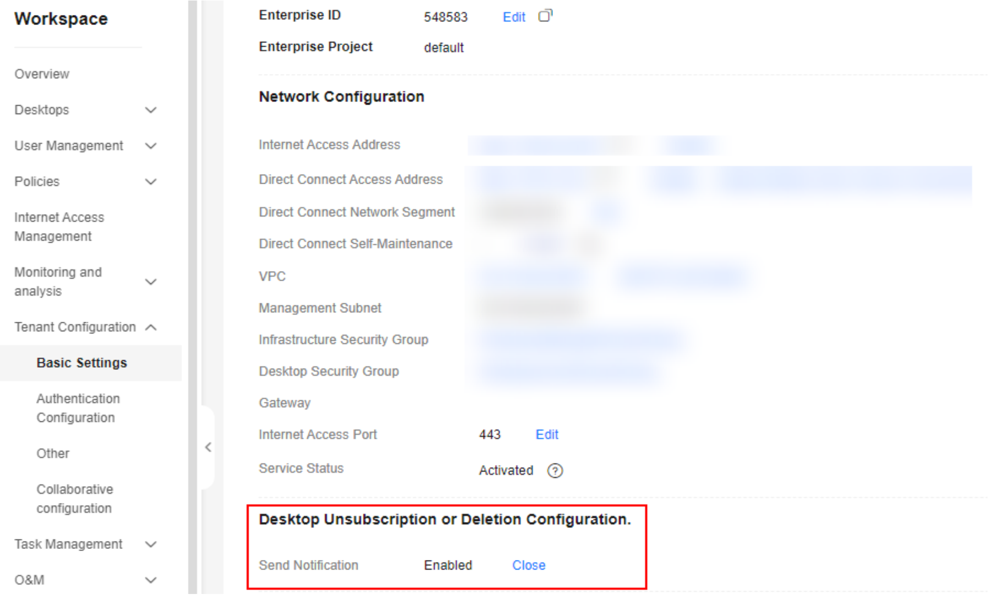
Procedure

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

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

The **Basic Settings** page is displayed.

Step 3 In the **Desktop Unsubscription/Deletion** area on the **Tenant Configuration** page, perform operations as required.



Enterprise ID 548583 Edit

Enterprise Project default

Network Configuration

Internet Access Address

Direct Connect Access Address

Direct Connect Network Segment

Direct Connect Self-Maintenance

VPC

Management Subnet

Infrastructure Security Group

Desktop Security Group

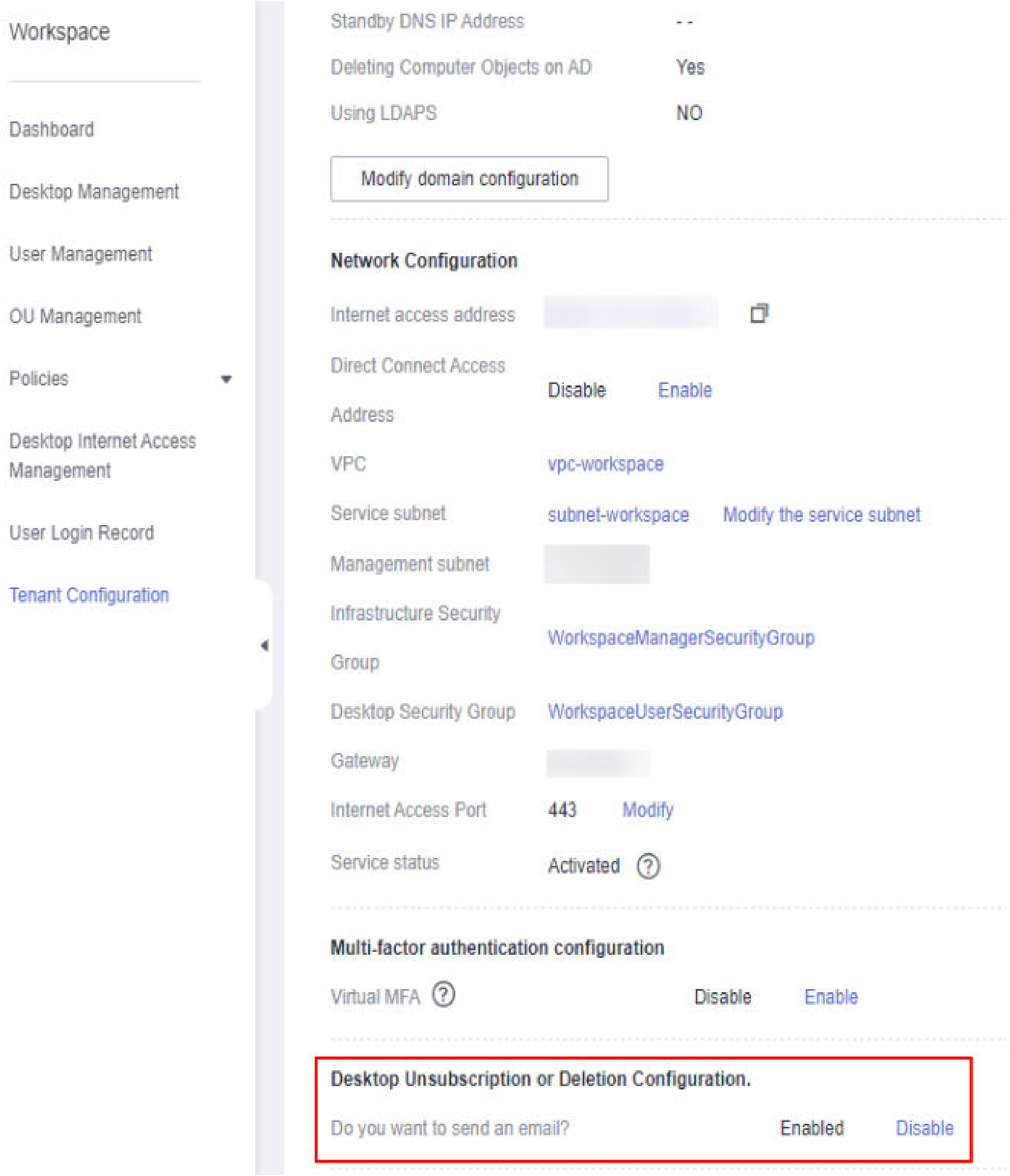
Gateway

Internet Access Port 443 Edit

Service Status Activated

Desktop Unsubscription or Deletion Configuration.

Send Notification Enabled Close



Standby DNS IP Address: - -

Deleting Computer Objects on AD: Yes

Using LDAPS: NO

Modify domain configuration

Network Configuration

Internet access address: [redacted]

Direct Connect Access Address: Disable Enable

VPC: vpc-workspace

Service subnet: subnet-workspace Modify the service subnet

Management subnet: [redacted]

Infrastructure Security Group: WorkspaceManagerSecurityGroup

Desktop Security Group: WorkspaceUserSecurityGroup

Gateway: [redacted]

Internet Access Port: 443 Modify

Service status: Activated

Multi-factor authentication configuration

Virtual MFA: Disable Enable

Desktop Unsubscription or Deletion Configuration.

Do you want to send an email? Enabled Disable

- Email sending is enabled by default, indicating that notification emails of desktop unsubscription or deletion are sent to users.
- If you do not want users to receive such emails, click **Disable**.

----End

8.1.10 VPC Sharing for Workspace

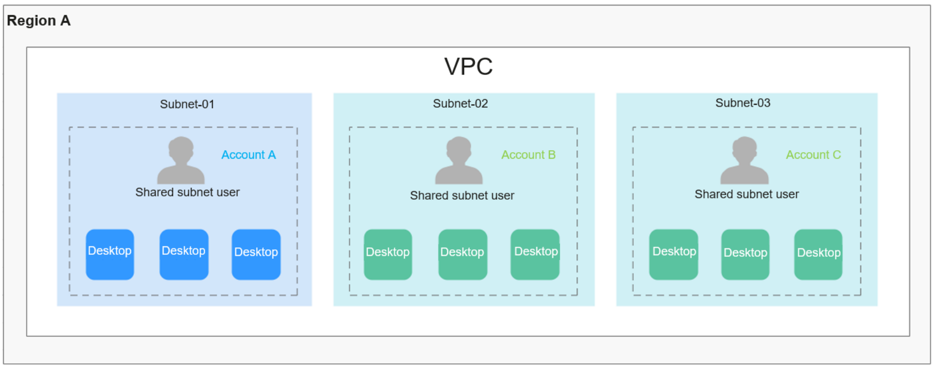
Scenario

When you purchase a cloud desktop or cloud desktop pool, VPC sharing allows you to use the VPCs and subnets shared by other accounts and manage network resources in a unified manner. This feature improves resource management efficiency and reduces O&M costs.

For example, to simplify network resource management, you can use one account to manage IT network resources, such as VPCs and subnets, of other accounts. Suppose you have three accounts (A, B, and C):

- Account A: the IT management account and the resource owner. You can use it to create a VPC and share subnets in it with other accounts.
- Account B: a service account that uses resources. In this example, you can use it to create cloud desktops in **Subnet-02** shared by account A.
- Account C: a service account that uses resources. In this example, you can use it to create cloud desktops in **Subnet-03** shared by account A.

Figure 8-5 Service planning



This section describes how to purchase a cloud desktop in a shared VPC. For details about VPC subnet sharing, see in the *Virtual Private Cloud User Guide*.

Constraints

- For details about the constraints on VPC sharing, see in the *Virtual Private Cloud User Guide*.
- When using VPC sharing with Direct Connect access enabled, you need to create a dedicated load balancer as the Direct Connect access address.
- If you need to create a new shared VPC, see .

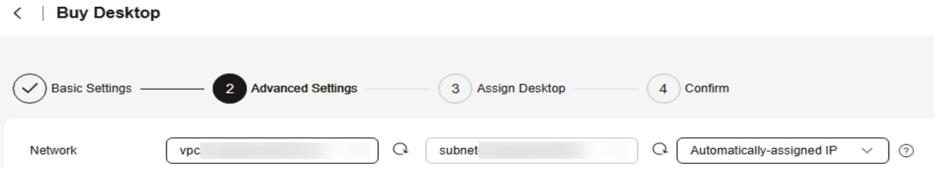
Procedure

Step 1 Log in to the console.

Step 2 Configure parameters required for purchasing a cloud desktop.

When configuring **Network**, select the VPC and subnet shared by account A.

Figure 8-6 Configuring network parameters



Network: vpc | subnet | Automatically-assigned IP

For details about other configurations, see section "Purchasing a Desktop" in the *Workspace Getting Started*.

NOTE

If you no longer need to access resources that are shared with you, you can at any time.

----End

8.1.11 Enabling NAT Mapping for Direct Connect

8.1.11.1 Address Mapping

Scenarios

If an enterprise network is configured with a firewall, cloud desktops cannot be accessed via the enterprise network, or via the Direct Connect access address or Internet access address provided by Workspace. In this case, cloud desktops can be accessed through NAT mapping.

Prerequisites

The Direct Connect access address has been enabled.

Procedure

Step 1 Prepare an ECS that can access the Internet access address and Direct Connect access address of the project and use the ECS as the mapping server.

Tenant configuration

Step 2 **Log in to the console**.

Step 3 In the navigation pane, choose **Tenant Configuration** > **Basic Settings**.

The **Basic Settings** page is displayed.

Step 4 Click **NAT Mapping Settings** on the right of **Direct Connect Access Address**. The **NAT Mapping Settings** page is displayed.

Step 5 Determine whether to enable NAT mapping.

- ○: not enabled
- ●: enabled

Step 6 After NAT mapping is enabled, select the **IP Address Mapping** tab and click **Add**. The page for adding IP address mapping is displayed.

Step 7 Enter the required domain name, domain name + port, IP address, and IP address + port in the address box.

NOTE

Ensure that the entered address is accessible for the mapping server in **1**.

Step 8 Determine whether to associate enterprise projects and tags.

- ●: Associate enterprise projects and tags and perform **Step 9** to **Step 10**.

- : Do not associate enterprise projects and tags. Perform **Step 11** to **Step 12**.

Step 9 Select the required enterprise project from the **Associated Enterprise Project** drop-down list, or click **Add** below, and select the required tag key and value.

NOTE

After enabling the function of associating with enterprise projects and tags, if you do not select an enterprise project, you must associate with at least one tag.

Step 10 Click **OK**.

Step 11 Select the **IP Address Mapping** tab and click **Add**. The page for adding IP address mapping is displayed. Toggle off **Associate with Enterprise Project and Tag**.

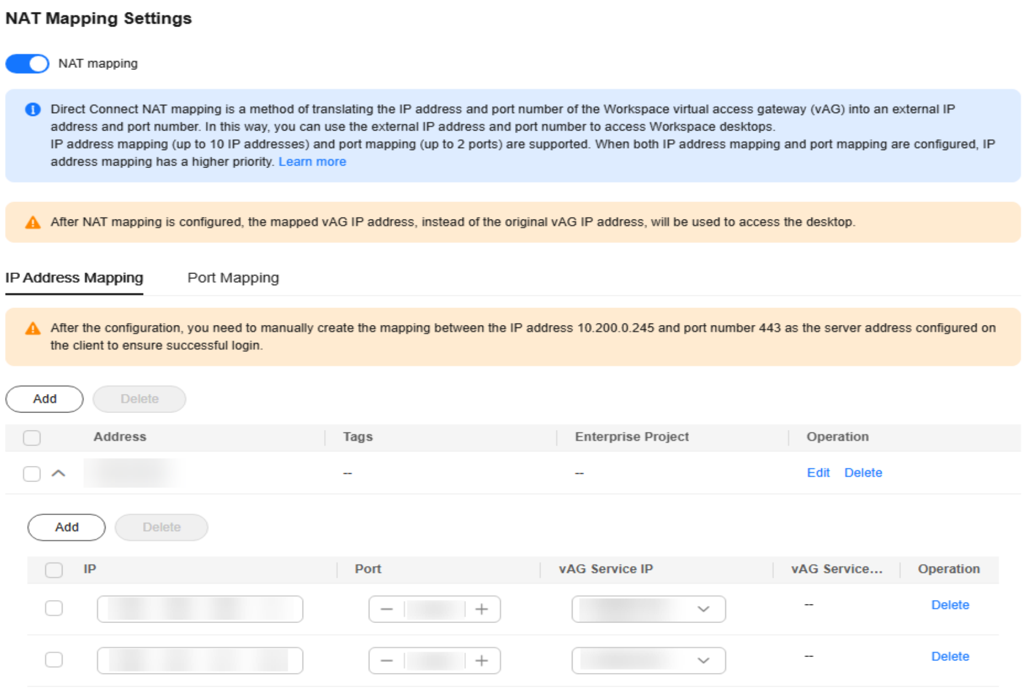
Step 12 Click **OK**.

NOTE

You can add a maximum of 10 addresses.

Step 13 Click ⌄ on the left of the added address to expand the address details and configure the address, as shown in **Figure 8-7**.

Figure 8-7 NAT mapping settings



NAT Mapping Settings

NAT mapping

Direct Connect NAT mapping is a method of translating the IP address and port number of the Workspace virtual access gateway (vAG) into an external IP address and port number. In this way, you can use the external IP address and port number to access Workspace desktops.
IP address mapping (up to 10 IP addresses) and port mapping (up to 2 ports) are supported. When both IP address mapping and port mapping are configured, IP address mapping has a higher priority. Learn more

After NAT mapping is configured, the mapped vAG IP address, instead of the original vAG IP address, will be used to access the desktop.

IP Address Mapping | Port Mapping

After the configuration, you need to manually create the mapping between the IP address 10.200.0.245 and port number 443 as the server address configured on the client to ensure successful login.

□	Address	Tags	Enterprise Project	Operation
□ ^		--	--	Edit Delete

□	IP	Port	vAG Service IP	vAG Service...	Operation
□		− +	⌄	--	Delete
□		− +	⌄	--	Delete

- **IP**: Enter the IP address of the mapping server in **1**.
- **Port**: Enter a port number ranging from 1 to 65535.
- **vAG Service IP**: Select one as required.

NOTE

- If there are multiple vAG service IP addresses, you need to add multiple data records. Click **Add** to add a row of data.
- To delete unnecessary data, click **Delete** in the **Operation** column.
- After NAT mapping is enabled, when you delete all data records at a time or the only data record, the button of confirming the deletion is unavailable and a message is displayed, indicating that no mapping rule is available.

Step 14 Check the box **After NAT mapping is configured, the mapped vAG IP address, instead of the original vAG IP address, will be used to access the desktop.** and click **OK**.

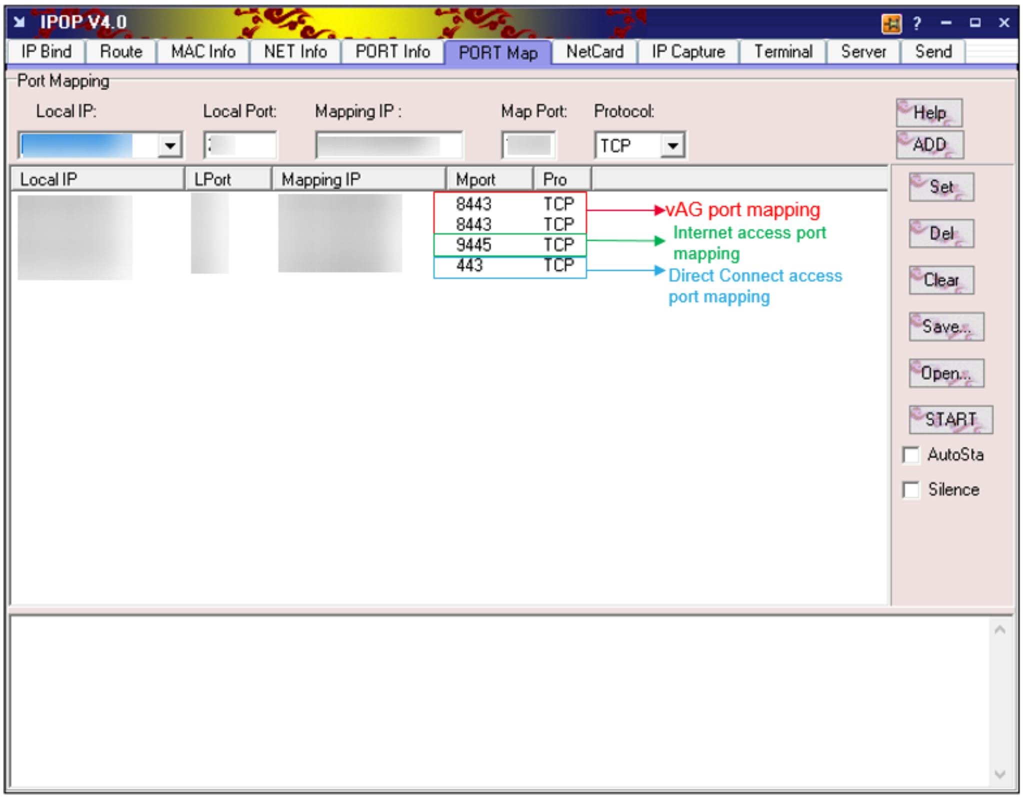
Mapping server configuration

Step 15 Log in to the mapping server created in 1.

Step 16 Open the mapping tool on the mapping server. IPOP is used as an example.

Step 17 In the IPOP window, select the **Port Mapping** tab to configure port mapping, vAG mapping, Internet access mapping, or Direct Connect access mapping.

Figure 8-8 Configuring port mapping



Local IP: [redacted] Local Port: [redacted] Mapping IP : [redacted] Map Port: [redacted] Protocol: TCP

Local IP	LPort	Mapping IP	Mport	Pro
[redacted]	[redacted]	[redacted]	8443	TCP
			8443	TCP
			9445	TCP
			443	TCP

vAG port mapping

Internet access port mapping

Direct Connect access port mapping

Configure vAG port mapping, as shown in Figure 8-8.

1. Select the **Port Mapping** tab to configure port mapping.
2. **Local IP**: local IP address of the mapping server
3. **Local Port**: port configured in NAT mapping under tenant configuration

4. **Mapping IP**: **vAG IP address configured in NAT mapping under tenant configuration**
5. **Map Port**: The default vAG port is 8443.
6. **Protocol**: The default value is TCP.
7. Click **Add**.

   NOTE

   - If there are multiple vAG service IP addresses, you need to add multiple data records. Click **Add** to add a row of data.
   - To delete unnecessary data, click **Delete** in the **Operation** column.

Configure address mapping, as shown in **Figure 8-8**.

1. Select the **Port Mapping** tab to configure port mapping.
2. **Local IP**: local IP address of the mapping server
3. **Local Port**: **port configured in NAT mapping under tenant configuration**
4. **Mapping IP**: Internet access address or Direct Connect access address (check it in **Tenant Configuration** on the console)
5. **Map Port**:
   a. Port configured for the Internet IP address: 9445 for Huawei Cloud central sites and 443 for edge sites
   b. Port configured for the Direct Connect IP address: 443 for Huawei Cloud central sites and 9443 for edge sites
6. **Protocol**: The default value is TCP.
7. Click **Add**.

Step 18 After the configuration is complete, click **START** in IPOP.

NOTE

The access address configured during client login is the address mapped to the Internet access address or Direct Connect access address. (If the corresponding port is available, add the port.)

Example: https://100.*xx*.*xx*.*xx*:1000

----End

8.1.11.2 Port Mapping

Scenarios

If an enterprise network is configured with a firewall, cloud desktops cannot be accessed via the enterprise network, or via the Direct Connect access address or Internet access address provided by Workspace. In this case, cloud desktops can be accessed through NAT mapping.

Prerequisites

- Enable **Direct Connect Access Address** before enabling **Direct Connect access port**.
- Enable **Internet Access Address** before enabling **Internet access port**.

Procedure

Step 1 Prepare an ECS that can access the Internet access address and Direct Connect access address of the project and use the ECS as the mapping server.

Tenant configuration

Step 2 Log in to the console.

Step 3 In the navigation pane, choose **Tenant Configuration** > **Basic Settings**.

The **Basic Settings** page is displayed.

Step 4 Click **NAT Mapping Settings** on the right of **Direct Connect Access Address**. The **NAT Mapping Settings** page is displayed.

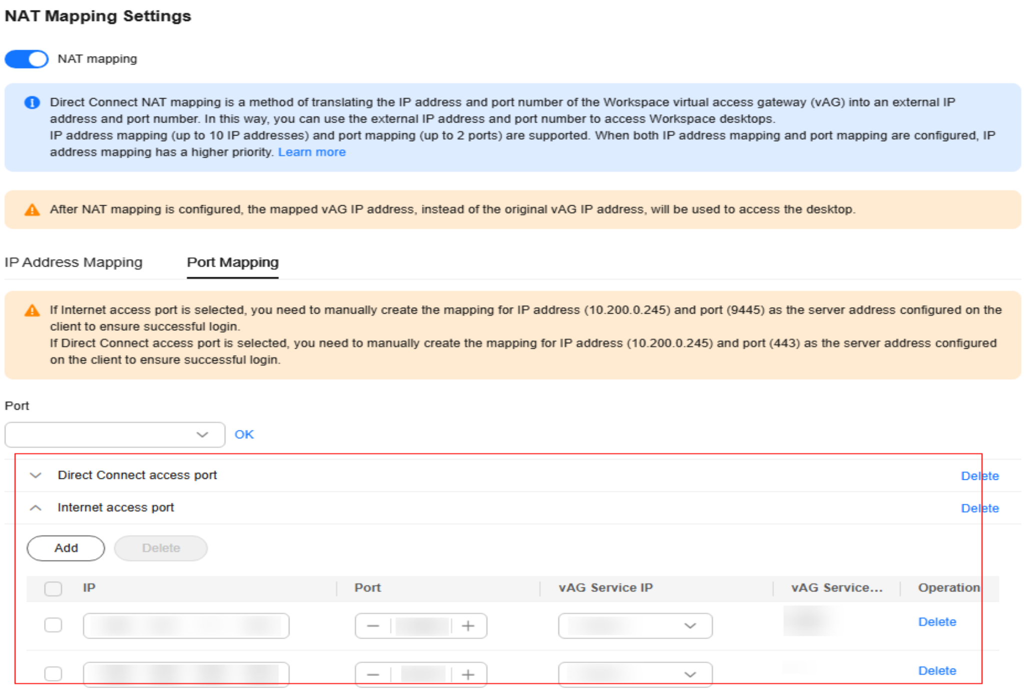
Step 5 Determine whether to enable NAT mapping.

- ○: not enabled
- ●: enabled

Step 6 After enabling NAT mapping, select the **Port Mapping** tab, select **Internet access port** or **Direct Connect access port** from the **Port** drop-down list, and click **OK**.

Step 7 Click ⌄ on the left of the added Internet access port or Direct Connect access port to expand the port details. Configure the port as shown in **Figure 8-9**.

Figure 8-9 NAT mapping settings



NAT Mapping Settings

NAT mapping

Direct Connect NAT mapping is a method of translating the IP address and port number of the Workspace virtual access gateway (vAG) into an external IP address and port number. In this way, you can use the external IP address and port number to access Workspace desktops.
IP address mapping (up to 10 IP addresses) and port mapping (up to 2 ports) are supported. When both IP address mapping and port mapping are configured, IP address mapping has a higher priority. Learn more

After NAT mapping is configured, the mapped vAG IP address, instead of the original vAG IP address, will be used to access the desktop.

If Internet access port is selected, you need to manually create the mapping for IP address (10.200.0.245) and port (9445) as the server address configured on the client to ensure successful login.
If Direct Connect access port is selected, you need to manually create the mapping for IP address (10.200.0.245) and port (443) as the server address configured on the client to ensure successful login.

Port

□	IP	Port	vAG Service IP	vAG Service...	Operation
□					Delete
□					Delete

- **IP**: Enter the IP address of the mapping server in **1**.
- **Port**: Enter a port number ranging from 1 to 65535.
- **vAG Service IP**: Select one as required.

NOTE

- If there are multiple vAG service IP addresses, you need to add multiple data records. Click **Add** to add a row of data.
- To delete unnecessary data, click **Delete** in the **Operation** column.
- After NAT mapping is enabled, when you delete all data records at a time or the only data record, the button of confirming the deletion is unavailable and a message is displayed, indicating that no mapping rule is available.

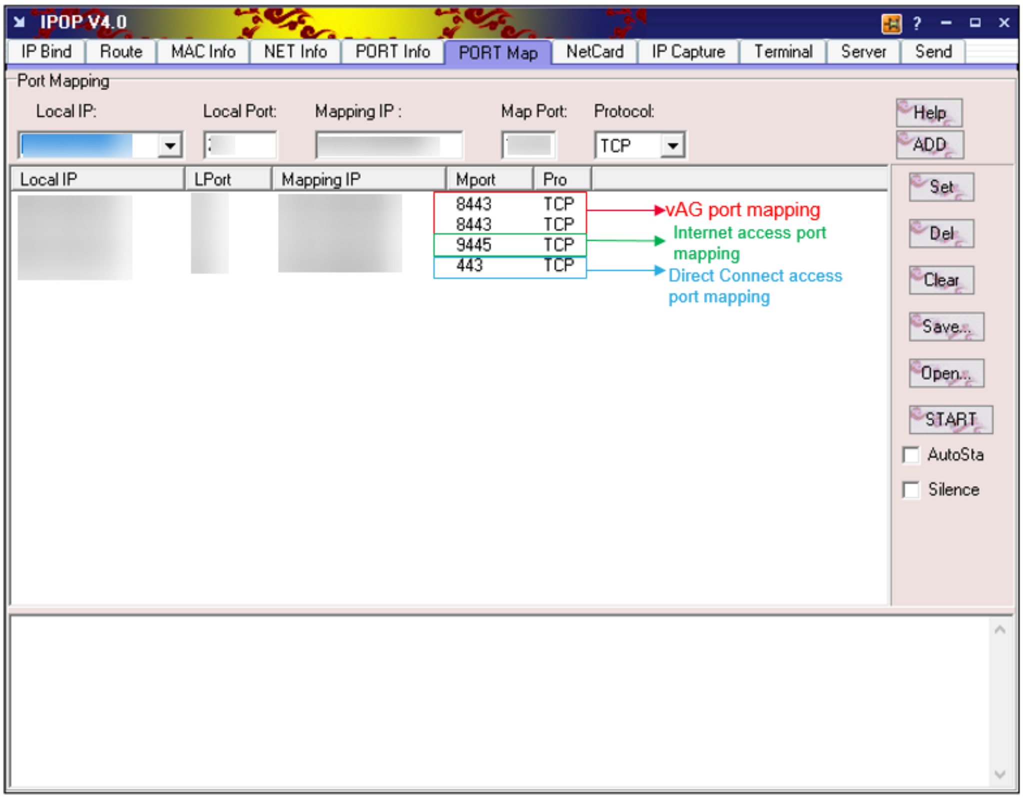
Step 8 Check the box **After NAT mapping is configured, the mapped vAG IP address, instead of the original vAG IP address, will be used to access the desktop.** and click **OK**.

Mapping server configuration

Step 9 Log in to the mapping server created in 1 and open the mapping tool on the mapping server. IPOP is used as an example.

Step 10 Configure vAG mapping, Internet access mapping, or Direct Connect access mapping using IPOP on the mapped server.

Figure 8-10 Configuring port mapping



Protocol: TCP

Local IP	LPort	Mapping IP	Mport	Pro
			8443	TCP
			8443	TCP
			9445	TCP
			443	TCP

vAG port mapping
Internet access port mapping
Direct Connect access port mapping

Configure vAG port mapping, as shown in **Figure 8-10**.

1. Select the **Port Mapping** tab to configure port mapping.
2. **Local IP**: The local IP address is used by default.
3. **Local Port**: **port configured in NAT mapping under tenant configuration**

4. **Mapping IP**: vAG IP address configured in NAT mapping under tenant configuration
5. **Map Port**: The default vAG port is 8443.
6. **Protocol**: The default value is TCP.
7. Click **Add**.

Configure address mapping, as shown in **Figure 8-10**.

1. Select the **Port Mapping** tab to configure port mapping.
2. **Local IP**: local IP address of the mapping server
3. **Local Port**: port configured in NAT mapping under tenant configuration
4. **Mapping IP**: Internet access address or Direct Connect access address (check it in **Tenant Configuration** on the console)
5. **Map Port**:
   a. Port configured for the Internet IP address: 9445 for Huawei Cloud central sites and 443 for edge sites
   b. Port configured for the Direct Connect IP address: 443 for Huawei Cloud central sites and 9443 for edge sites
6. **Protocol**: The default value is TCP.
7. Click **Add**.

Step 11 After the configuration is complete, click **START** in IPOP.

NOTE

The access address configured during client login is the address mapped to the Internet access address or Direct Connect access address. (If the corresponding port is available, add the port.)

Example: https://100.*xx.xx.xx*:1000

----End

8.1.12 Configuring User Log Collection

Scenario

The administrator can enable Workspace log collection for better O&M of Workspace desktops. After the function is enabled, Workspace logs are collected. If user log collection is not needed, the administrator can disable Workspace log collection.

Procedure

Step 1 Log in to the console.

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

The **Basic Settings** page is displayed.

Step 3 In the **User Log Collection** area, perform operations as required.

- By default, **Authorization** is disabled. If you click **Enable**, Workspace logs will be collected.

- If you do not need to authorize log collection, click **Close**. After **Authorization** is disabled, log collection will be unavailable.

----End

8.1.13 Upgrading Client and VM Components and Rotating Authentication Credentials

Scenario

To continuously optimize user experience on Workspace desktops, the administrator can enable **Upgrading Client and VM Components and Rotating Authentication Credentials** on the **Basic Settings** page. After this function is enabled, the administrator can upgrade client and desktop components based on version features and rotate machine-machine authentication credentials of a desktop.

Procedure

Step 1 Log in to the console.

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

The **Basic Settings** page is displayed.

Step 3 In the **Upgrading Client and VM Components and Rotating Authentication Credentials** area, perform operations as required.

- **Authorization** defaults to **Disabled**. If you click **Enable**, the client and desktop components will be upgraded based on the version features, and machine-machine authentication credentials of a desktop will be rotated based on desktop users' requirements.
- If authorization is not needed, click **Close**. After the function is disabled, the function of upgrading client and VM components and rotating authentication credentials is unavailable.

----End

8.1.14 Access Address Priority

Scenarios

The administrator has enabled both Direct Connect and Internet access. The Internet access address and Direct Connect access address are in primary/standby mode. If one access method malfunctions, you can easily switch to the other access method.

Prerequisites

- Internet access has been enabled.
- Direct Connect access has been enabled.

Constraints

- After the access address priority is set, the access address configuration of the terminal user will be force updated upon their first login.
- Ensure smooth networking between the terminal and the access address.
- To configure an associated domain (proxy address), ensure smooth networking between the terminal and the domain (proxy address), and the mapping between the domain (proxy address) and the desktop access address should be configured.
- Access policies and protocol policies will not vary with access addresses.

Procedure

Step 1 Log in to the console.

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

The **Basic Settings** page is displayed.

Step 3 Click **Settings** under **Access Address Priority** to go to the **Access Address Priority** dialog box:

- ○: Disable access address priority.
- ●: Enable access address priority.

Step 4 After enabling access address priority, in the **Priority** drop-down list, click ⌄ to select **Direct Connect access address** or **Internet access address**. Then determine whether to enter the associated domain name or proxy address.

NOTE

- A smaller value indicates a higher priority.
- If **Direct Connect access address** is selected for **Priority 1**, **Internet access address** is selected for **Priority 2** by default, indicating that the Direct Connect access address is prioritized. If the Direct Connect access address malfunctions, you can switch to the Internet access address as prompted.
- If **Internet access address** is selected for **Priority 1**, **Direct Connect access address** is selected for **Priority 2** by default, indicating that the Internet access address is prioritized. If the Internet access address malfunctions, you can switch to the Direct Connect access address as prompted.

Step 5 Click **OK**.

----End

8.1.15 Other

8.1.15.1 User Name Prefixes

Scenarios

You can configure the username prefix for a Linux desktop in **Tenant Configuration**.

Procedure

Step 1 Log in to the console.

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

The **Basic Settings** page is displayed.

Step 3 In the **Other** area on the **Basic Settings** page, determine whether to enable username prefix.

- Enabled: The username prefix takes effect only for Linux desktops and digit-only usernames.

  Click **Enable** and enter a prefix in letters. Click **OK**.

  After the username prefix is enabled, you can click **Modify** next to **Prefix** to modify the prefix. Then click **OK**.
- Disabled: No username prefix is used.

  Click **Disable** and then click **OK**.

----End

8.1.15.2 Screen Capture on the Login Page

Scenarios

You can configure whether to allow screen capture after login from an Android client on the **Tenant Configuration** page.

Procedure

Step 1 Log in to the console.

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

The **Basic Settings** page is displayed.

Step 3 In the **Other** area on the **Basic Settings** page, determine whether to enable **Screen Capture on Login Page**.

- Enabled: Screen capture is allowed after login from an Android client.

  Click **Enable**. In the displayed dialog box, click **OK**.
- Disabled: Screen capture is not allowed after login from an Android client.

  Click **Disable**. In the displayed dialog box, click **OK**.

NOTE

Only Android clients of 24.6.4 and later versions support this function.

----End

8.1.15.3 Allowing Users to Change Passwords on the Client

Scenarios

You can determine whether users can change their passwords on the client.

Procedure

Step 1 Log in to the console.

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

The **Basic Settings** page is displayed.

Step 3 In the **Other** area on the **Basic Settings** page, determine whether to enable **Password Change by Users on Client**.

- **Enabled**: By default, this function is enabled. Users are allowed to change their passwords on the client.
- **Disabled**: **Change Password** is not available on the client.

----End

8.2 Authentication Configuration

8.2.1 Third-party SSO Authentication

Scenarios

Workspace supports multiple third-party authentication sources, including individual social authentication, enterprise social authentication, and enterprise authentication sources, providing simpler and more convenient login modes and better user experience for enterprise users. As an administrator, you can add, modify, and delete authentication providers.

NOTICE

Currently, switchover between OAuth2.0, LDAP, and two-factor authentication (TFA) is unavailable, and they cannot be enabled at the same time.

Data

Table 8-2 lists the configuration data required for this operation.

Table 8-2 Required data

Protocol	Parameter	Description	Example Value
OAuth 2.0 **View Type** > **Visual**	APP ID	Application (client) ID obtained when an application is created on the third-party authentication source platform. Azure: Obtain the value of **Application (client) ID** in the name of the application created on the Azure platform. DINGTALK: Obtain the value of **Appkey** in the name of the application created on the DINGTALK platform. Obtain the configuration as required. For details, submit a service ticket.	ed2a****0feb

Protocol	Parameter	Description	Example Value
	APP Secret	**client_secret** obtained when an application is created on the third-party authentication source platform. Azure: Obtain the value of **Client Credentials** in the name of the application created on the Azure platform. Click **Add a certificate or secret**. On the displayed **Client Secrets** page, click **New client secret** to create. DINGTALK: Obtain the value of **APP Secret** in the name of the application created on the DINGTALK platform. Obtain the configuration as required. For details, **submit a service ticket**.	VdS8****lpoA
	Authentication Success Check Field	Azure configurations: "displayName" or "userPrincipalName" DINGTALK: nick **NOTE** The user created on the Azure platform must be the same as the Workspace user. Otherwise, the verification fails.	displayName

Protocol	Parameter	Description	Example Value
	Validation Field Separator Configuration	Truncation rules: 1. Scanning starts from back to front, and splitting is performed at the position where the separator field appears for the first time. The front part is used. 2. The default separator is @. 3. The separator can only be a letter, digit, or any of the special characters in parentheses (.-_ $#@>).	Example: test#EXT#&te@teleperformance.com The separators are **@** and **#EXT#**. **test** is returned after splitting.
	Azure Tenant ID	Directory (tenant) ID of the login tenant. Azure: Obtain the value of **Directory (tenant) ID** in the name of the application created on the Azure platform. Obtain the configuration as required. For details, **submit a service ticket**. **NOTE** This parameter is mandatory when the third-party source is set to **AZURE**.	feff****eed9
OAuth 2.0 **View Type** > **JSON**	JSON file configuration	**Submit a service ticket** for technical support.	-

Protocol	Parameter	Description	Example Value
LDAP	Server Address	IP address of the authentication server. Set this parameter to the IP address used for setting up the LDAP server.	10.134.151.140
	Port	Port used by the authentication server to communicate with Workspace. Set this parameter to the port used for setting up the LDAP server.	636 or 389
	Base DN	LDAP root directory. Set this parameter to the root directory collected from the LDAP server.	DC=huawei,DC=com
	Administrator DN	DN of the administrator of the LDAP authentication server. Set this parameter to the administrator account created when setting up the LDAP server.	CN=manager,DC=huawei,DC=com

Protocol	Parameter	Description	Example Value
	Administrator Password	Password of the administrator of the LDAP authentication server. Set this parameter to the password of the administrator created when setting up the LDAP server. **NOTE** Password for accessing the LDAP server.	-
	User Query Base	Directory where the user is located upon LDAP creation. Set this parameter to the name of the directory used for creating a user.	cn=users
	SSL/TLS Certificate Verification	● Enable: LDAPS is used to set up an LDAP server. ● Disable: LDAP is used to set up an LDAP server.	Enable
	Certificate Upload	After SSL/TLS certificate verification is enabled, you need to upload a certificate. Set this parameter to the certificate used when a user sets up an LDAP server and enables LDAPS.	-

Procedure

(Optional) Configuring the Auth URL whitelist

NOTE

Enable OAuth 2.0. To configure a third-party authentication source, configure a whitelist on the third-party authentication platform first.

Step 1 Log in to the console.

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

The **Basic Settings** page is displayed.

Step 3 In the **Network Configuration** area, obtain the IP addresses of Internet access and Direct Connect.

NOTE

If the network configuration mode of the tenant is set to either Internet access or Direct Connect, select desired configuration.

Step 4 Click **Redirect URls** in the name of the application created on the Azure platform, and add the IP addresses of Internet access and Direct Connect obtained in **3** to the whitelist.

----End

Configuring third-party SSO authentication

NOTE

After third-party SSO is enabled, the username created on the interconnected platform must be the same as the Workspace username. Otherwise, the verification fails.

Step 1 Log in to the console.

Step 2 In the navigation pane, choose **Tenant Configuration** > **Authentication Configuration** > **Primary Authentication**, and click **Modify**.

Step 3 Select **Third-party SSO authentication** for **Primary Authentication Type**.

- If **Protocol** is **OAuth 2.0**, perform **Step 4**.
- If **Protocol** is **LDAP**, perform **Step 5**.

Step 4 Set **View Type** to **Visual** and configure OAuth 2.0 parameters according to **Table 8-2**.

Step 5 Configure LDAP parameters according to **Table 8-2**.

Step 6 Click **Save**.

----End

8.2.2 Configuring Multi-Factor Authentication

8.2.2.1 Huawei Cloud Multi-Factor Authentication Service (Virtual MFA)

Scenarios

After the administrator enables virtual multi-factor authentication (MFA), Huawei Cloud virtual MFA is used by default. When an end user uses the account and password to log in to a desktop from Huawei Cloud Workspace client, the end user must pass the MFA using a dynamic verification code.

Prerequisites

You have purchased desktops.

Constraints

The emergency mode is disabled.

NOTE

The emergency mode is disabled by default.

If the emergency mode is enabled, multi-factor authentication cannot be used. Enter the **service ticket** information, obtain the emergency mode status of the current tenant, and disable the emergency mode as required.

Procedure

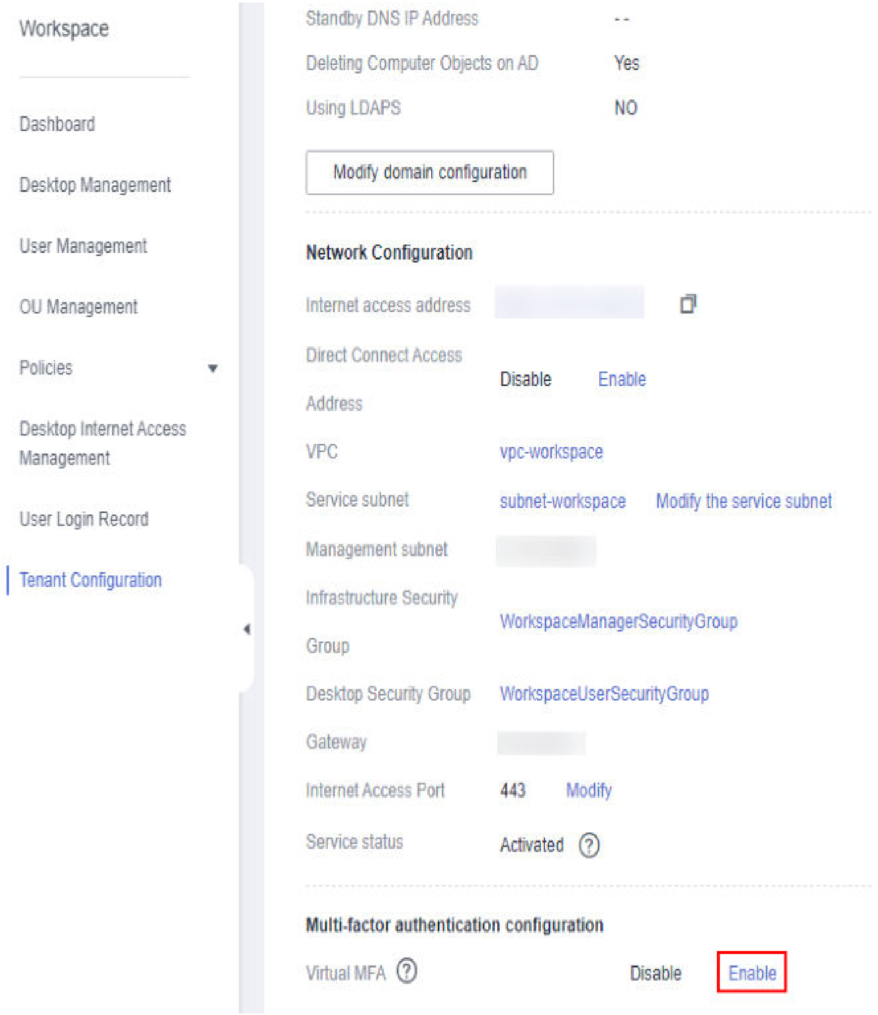
Enabling the Huawei Cloud Multi-factor Authentication Service

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

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

The **Authentication Configuration** page is displayed.

Step 3 Click the **Auxiliary Authentication** tab. Under **Multi-Factor Authentication Configuration**, click **Enable**.



Standby DNS IP Address --

Deleting Computer Objects on AD Yes

Using LDAPS NO

Network Configuration

Internet access address [redacted]

Direct Connect Access Address Disable

VPC vpc-workspace

Service subnet subnet-workspace

Management subnet [redacted]

Infrastructure Security Group WorkspaceManagerSecurityGroup

Desktop Security Group WorkspaceUserSecurityGroup

Gateway [redacted]

Internet Access Port 443

Service status Activated

Multi-factor authentication configuration

Virtual MFA Disable

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

- **Multi-Factor Authentication**: Set it to **Huawei Cloud MFA service**.
- **MFA Type**: The default value is **Virtual MFA**.
- **Access Method**:
  - Internet access user
  - Direct Connect access user

Step 5 Select target objects as required. The target objects can be users, user groups, or all users.

NOTE

By default, **All users** is selected. You can choose specific users or user groups as target objects. Once selected, the default **All users** object can be removed so that only the specified objects take effect.

Step 6 Click **OK**.

NOTE

After the administrator enables virtual MFA, end users need to use the virtual MFA device in a cloud application on a smart device (such as a mobile phone) or other TOTP-supported devices to obtain a dynamic verification code when logging in to the desktop from the Workspace client. (For the first login, the virtual MFA device must be bound to the smart device.) Then end users need to enter the dynamic verification code on the login page of the Workspace client. For details about the operations of end users for different device types, see **Logging In to a Desktop Using an SC**, **Logging In to a Desktop Using a TC**, or **Logging In to a Desktop Using a Mobile Terminal**.

----End

Managing the configuration of auxiliary authentication

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

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

The **Authentication Configuration** page is displayed.

Step 3 Click the **Auxiliary Authentication** tab.

Step 4 Perform the operations in **Table 8-3** as required.

Table 8-3 Operations for auxiliary authentication configuration

Operation	Procedure	Description
Adding target objects	1. Click **Select** on the right of the target object. The **Select Target Object** page is displayed. 2. Select target objects as required. The target objects can be users, user groups, or all users. 3. Click **OK**.	The administrator can add target objects to enable multi-factor authentication for individual users or users in a user group.

Operation	Procedure	Description
Removing a target object	● Single removal 1. Locate the target object and click **Remove** in the **Operation** column. The **Remove Target Object** dialog box is displayed. 2. If you want to perform this operation, enter **DELETE** or click **Auto Enter** for confirmation. ● Batch removal Select users or user groups to be removed from the target object list. 1. Click **Remove** above the list. The **Remove Target Object** dialog box is displayed. 2. If you want to perform this operation, enter **DELETE** or click **Auto Enter** for confirmation. 3. Click **OK**. **NOTE** Removing a target object will disable auxiliary authentication for its users and user groups.	The administrator can remove users who do not need to be connected for multi-factor authentication.
Modifying the configuration of auxiliary authentication	1. Click **Modify** on the right of the Huawei Cloud MFA service 2. Modify the following configurations as required: – **Multi-Factor Authentication**: You can change the authentication server to **Enterprise's authentication system** if needed. For details, see **8.2.2.2 Enterprise's Authentication System**. – **Access Method**: Select **Internet access user** or **Direct Connect access user** as required. **NOTE** You must select either of the access methods. – **Target Object**: You can add or remove target objects. 3. Click **Save Configuration**.	The administrator can modify the auxiliary authentication configuration as required.

----End

8.2.2.2 Enterprise's Authentication System

Scenarios

The administrator can configure the interconnection with an enterprise's authentication system so that end users can use the system to perform the second authentication when logging in to desktops from Huawei Cloud Workspace client using accounts and passwords.

Prerequisites

- You have purchased desktops.
- The network between the customer's data center (where the enterprise authentication server is) and the VPC has been configured by referring to Direct Connect - **Getting Started** or Virtual Private Network **Administrator Guide**.

  NOTE

  A random port has been enabled on the cloud desktop to connect to the third-party service plane. If the cloud desktop is also interconnected with the Windows AD, ensure that the Windows AD port does not conflict with the port of the authentication server.
- The following information about the enterprise authentication server has been obtained:
  - (Optional) Domain name of the authentication server
  - Authentication server IP address
  - Access key (AK) of the authentication server
  - Secret access key (SK) of the authentication server
  - SSL/TLS certificate file in PEM or CER format of the authentication server

Constraints

The emergency mode is disabled.

NOTE

The emergency mode is disabled by default.

If the emergency mode is enabled, multi-factor authentication cannot be used. Enter the **service ticket** information, obtain the emergency mode status of the current tenant, and disable the emergency mode as required.

Procedure

Enabling interconnection with the enterprise's authentication system

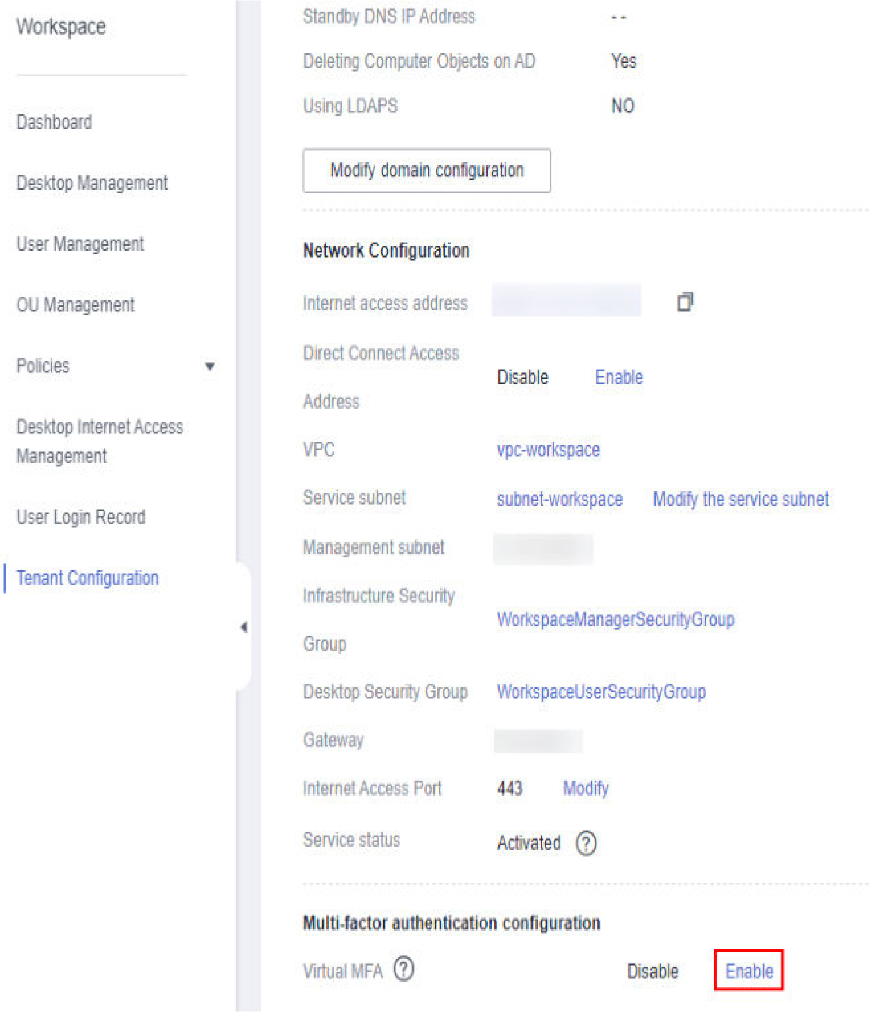
Step 1 **Log in to the console**.

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

The **Authentication Configuration** page is displayed.

Step 3 Click the **Auxiliary Authentication** tab. Under **Multi-Factor Authentication Configuration**, click **Enable**.

Figure 8-11 Enabling virtual MFA



Standby DNS IP Address --
Deleting Computer Objects on AD Yes
Using LDAPS NO

Network Configuration

Internet access address
Direct Connect Access Address Disable Enable
VPC vpc-workspace
Service subnet subnet-workspace
Management subnet
Infrastructure Security Group WorkspaceManagerSecurityGroup
Desktop Security Group WorkspaceUserSecurityGroup
Gateway
Internet Access Port 443
Service status Activated

Multi-factor authentication configuration

Virtual MFA Disable Enable

Step 4 In the dialog box displayed, click **OK**. The page for modifying the MFA configuration is displayed.

Step 5 Configure parameters by referring to **Table 8-4**.

Table 8-4 Parameters for interconnecting with an enterprise's authentication system

Parameter	Description	Example Value
Authentication Server	Select **Enterprise's authentication system**.	Enterprise's authentication system
Server address	Enter the IP address of the enterprise authentication server prepared in **Prerequisites**. If **Access mode** is set to **Internet**, enter the domain name of the enterprise authentication server.	192.168.0.0

Parameter	Description	Example Value
APP ID	Enter the AK of the enterprise authentication server prepared in **Prerequisites**. The AK can contain a maximum of 24 characters.	-
APP Secret	Enter the SK of the enterprise authentication server prepared in **Prerequisites**. The SK can contain a maximum of 128 characters.	-
SSL/TLS Certificate	1. Click **Upload Certificate** and select the SSL/TLS certificate of the enterprise authentication server prepared in **Prerequisites**. 2. Click **Open**.	-
Access Method	Set this parameter based on the network condition of the user's authentication server. ● If only the public network is accessible, select **Internet access user**. ● If only the private network is accessible, select **Direct Connect access user**.	Internet access user
Target Object	Set **Target Object** to **All users**, **Users**, or **User groups**. NOTE By default, **All users** is selected. You can choose specific users or user groups as target objects. Once selected, the default **All users** object can be removed so that only the specified objects take effect.	-

Step 6 Click **OK**.

NOTE

When the enterprise's authentication system is used for authentication, end users do not need to bind devices. For details, see **Logging In to a Desktop Using an SC**, **Logging In to a Desktop Using a TC**, or **Logging In to a Desktop Using a Mobile Terminal**.

----End

Managing the configuration of auxiliary authentication

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

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

The **Authentication Configuration** page is displayed.

Step 3 Click the **Auxiliary Authentication** tab.

Step 4 Perform the operations in **Table 8-5** as required.

Table 8-5 Operations for auxiliary authentication configuration

Operation	Procedure	Description
Adding target objects	1. Click **Select** on the right of the target object. The **Select Target Object** page is displayed. 2. Select target objects as required. The target objects can be users, user groups, or all users. 3. Click **OK**.	The administrator can add target objects to enable multi-factor authentication for individual users or users in a user group.
Removing target objects	● Single removal 1. Locate the target object and click **Remove** in the **Operation** column. The **Remove Target Object** dialog box is displayed. 2. If you want to perform this operation, enter **DELETE** or click **Auto Enter** for confirmation. ● Batch removal Select users or user groups to be removed from the target object list. 1. Click **Remove** above the list. The **Remove Target Object** dialog box is displayed. 2. If you want to perform this operation, enter **DELETE** or click **Auto Enter** for confirmation. 3. Click **OK**. **NOTE** Removing a target object will disable auxiliary authentication for its users and user groups.	The administrator can remove users who do not need to be connected for multi-factor authentication.

Operation	Procedure	Description
Modifying the configuration of auxiliary authentication	1. Click **Modify** on the right of the Huawei Cloud MFA service 2. Modify the following configurations as required: – **Multi-Factor Authentication**: You can change the authentication server to Huawei Cloud multi-factor authentication if needed. For details, see **8.2.2.1 Huawei Cloud Multi-Factor Authentication Service (Virtual MFA)**. – **Access Method**: Select **Internet access user** or **Direct Connect access user** as required. **NOTE** You must select either of the access methods. – **Target Object**: You can add or remove target objects. 3. Click **Save Configuration**.	The administrator can modify the auxiliary authentication configuration as required.

----End

8.2.2.3 Disabling MFA

Scenario

The administrator can disable virtual MFA under **Multi-Factor Authentication Configuration**. After MFA is disabled, users can directly use their accounts and passwords to log in to desktops with no need for the second time of virtual MFA.

Procedure

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

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

The **Authentication Configuration** page is displayed.

Step 3 Click the **Auxiliary Authentication** tab. Under **Multi-Factor Authentication Configuration**, click **Disable**.

Step 4 Click **OK**.

NOTE

After virtual MFA is disabled, all bound virtual MFA devices will be deleted. Delete the MFA devices from the list on the mobile device. To enable virtual MFA again, bind the virtual MFA device.

----End

8.3 Other

8.3.1 Desktop Naming Rules

Scenarios

Create a desktop naming rule in **Other**.

Procedure

Step 1 Log in to the console.

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

The **Other** page is displayed.

Creating a desktop naming rule

Step 3 Under the **Desktop Naming Rules** tab, click **Create Desktop Naming Rule** in the upper right corner. The **Create Desktop Naming Rule** page is displayed.

Step 4 See **Table 8-6** to create a desktop naming rule.

Table 8-6 Desktop naming rules

Parameter	Description	Example Value
Naming Rule Name	A desktop naming rule can contain 1 to 30 characters in only letters, digits, and underscores (_), and must start with a letter or underscore (_).	-

Parameter	Description	Example Value
Username	- **Included**: A naming rule contains the name prefix and username and is not applicable to desktop pools. - **Not included**: A naming rule contains only the name prefix and applies to all scenarios.	-
Name Prefix	A name prefix can contain 1 to 14 characters in only letters, digits, and hyphens (-), and must start with a letter or digit.	Username included: A + *Username* + B + 1 Username not included: A + 1
Number of Digits	The value range is 1 to 5.	-
Start Value	The start value is related to the number of digits. If **Number of Digits** is **1**, the start value ranges from 1 to 9. If **Number of Digits** is **2**, the start value ranges from 1 to 99. If **Number of Digits** is **5**, the start value ranges from 1 to 99999. That is, the maximum **Number of Digits** of the start value is the value of **Number of Digits**.	-

Parameter	Description	Example Value
Increment for One Username	● **Yes**: The value of **Number of Digits** increases in ascending order based on the sequence in which desktops are assigned to a single user. ● **No**: The value of **Number of Digits** increases in ascending order based on the assignment sequence of all desktops. **NOTE** If **Username** is set to **Not included**, **Increment for One Username** is not available.	For example, let's assume that **Number of Digits** is **3** and **Start Value** is **1**; and the second and eighth desktops are assigned to User A. When this parameter is set to **Yes**, the desktop names are **UserA001** and **UserA002**. When this parameter is set to **No**, the desktop names are **UserA002** and **UserA008**.

Step 5 Click **OK**.

Modifying a desktop naming rule

Step 6 Under the **Desktop Naming Rules** tab, click **Edit** in the **Operation** column of the desired naming rule. The **Modify Desktop Naming Rule** page is displayed.

Step 7 Modify the desktop naming rule.

- **Naming Rule Name**
- **Username**
- **Name Prefix**
- **Number of Digits**
- **Start Value**
- **Increment for One Username**

Step 8 Click **OK**.

Deleting a desktop naming rule

Step 9 Under the **Desktop Naming Rules** tab, click **Delete** in the **Operation** column of the desired naming rule. The **Delete Desktop Naming Rule** page is displayed.

Step 10 Click **OK**.

Setting a naming rule to a default one

Step 11 Under the **Desktop Naming Rules** tab, click **Set as Default** in the **Operation** column of the desired naming rule. The **Default** icon will be displayed on the right of the naming rule.

----End

9 Internet Access Management

9.1 Enabling Economical Internet Access (EIP)

Scenarios

The administrator can select economical Internet access (EIP) for cloud desktops. After Internet access is enabled, cloud desktops can access the Internet.

Prerequisites

You have purchased a cloud desktop.

Procedure

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

Step 2 In the navigation pane, choose **Internet Access Management**.

The **Internet Access** page is displayed.

Step 3 Click the button of enabling Internet access in the upper right corner of the page.

The page of enabling Internet access is displayed.

Step 4 Configure Internet access.

- **Type**
  - **Economical (EIP)**: Desktops access the Internet through **Elastic IP (EIP)**. Each desktop is bound to an EIP. This mode is applicable when there are a small number of desktops.

NOTE

Enabling economical Internet access will create the following networking resources:

An **EIP** provides independent public IP addresses and bandwidth for Internet access.

- **Billing Mode**: Select a billing mode as required.
  - **Yearly/Monthly**, as shown in **Table 9-1**.
  - **Pay-per-use**, as shown in **Table 9-2**.

Table 9-1 Yearly/Monthly

Parameter	Description	Example Value
Billing Mode	Select **Yearly/Monthly**.	Yearly/Monthly
Bandwidth (Mbit/s)	The value ranges from 1 to 280 and can be customized.	-
Enterprise Project	You can use an enterprise project to centrally manage your cloud resources and members by project. Select one as required.	-
Required Duration	Set the required duration. **NOTE** You can determine whether to select **Auto renewal**.	-

Parameter	Description	Example Value
Select Desktop	Select Desktop: ● Search with the desktop name or desktop user for the desktop for which Internet access is to be enabled. ● Select the desired desktop name in the list. – Enabling Internet access for one desktop: Select the desired desktop in the desktop list and confirm it. – Batch enabling Internet access for desktops: Select the desired desktops in the desktop list and confirm them.	-

Table 9-2 Pay-per-use

Parameter	Description	Example Value
Billing Mode	Select **Pay-per-use**.	Pay-per-use

Parameter	Description	Example Value
Public Network Bandwidth	Select a bandwidth billing mode as needed. ● **By bandwidth**: You need to specify a bandwidth limit and pay for the amount of time you use the bandwidth. This is applicable to high or stable traffic. The bandwidth ranges from 1 to 280 Mbit/s. ● **By traffic**: You need to specify a bandwidth limit and pay for the total traffic you generate. This is applicable to light or sharply fluctuating traffic. The bandwidth ranges from 1 to 260 Mbit/s.	-
Bandwidth	The value ranges from 1 to 280 Mbit/s and can be customized.	-
Enterprise Project	You can use an enterprise project to centrally manage your cloud resources and members by project. Select one as required.	-

Parameter	Description	Example Value
Select Desktop	Select Desktop: ● Search with the desktop name or desktop user for the desktop for which Internet access is to be enabled. ● Select the desired desktop name in the list. – Enabling Internet access for one desktop: Select the desired desktop in the desktop list and confirm it. – Batch enabling Internet access for desktops: Select the desired desktops in the desktop list and confirm them.	-

- If you set **Billing Mode** to **Yearly/Monthly**, perform **Step 6** to **Step 8**.
- If you set **Billing Mode** to **Pay-per-use**, perform **Step 9**.

Step 5 Click **OK**.

Step 6 Confirm the configuration and click **OK**. The payment page is displayed.

Step 7 Check the cloud service order and the fee to be paid.

Step 8 After selecting the payment method and paying, click **Confirm**.

Step 9 Confirm the configuration and click **OK**.

----End

9.2 Enabling Enhanced Internet Access (NAT Gateway +EIP)

Scenarios

You can configure a **NAT gateway** and an **EIP** for each subnet as required. After they are enabled, all desktops in the subnet can access the Internet.

Prerequisites

You have purchased a cloud desktop.

Procedure

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

Step 2 In the navigation pane, choose **Internet Access Management**.

The **Internet Access** page is displayed.

Step 3 Click the button of enabling Internet access in the upper right corner of the page.

The page of enabling Internet access is displayed.

Step 4 Configure Internet access, as shown in **Table 9-3**.

NOTE

Enabling enhanced Internet access will create the following networking resources:

1. A public **NAT gateway** can be used to easily construct the network address translations for VPC.

2. An **EIP** provides independent public IP addresses and bandwidth for Internet access.

Table 9-3 Parameters

Parameter	Description	Example Value
Type	Each subnet must be configured with a **NAT gateway** and an **EIP**. After they are enabled, all desktops in the subnet can access the Internet.	Enhanced (NAT Gateway +EIP)
Billing Mode	Pay-per-use	-
Network	Select a VPC and a subnet.	-

Parameter	Description	Example Value
NAT Gateway Name	To allow cloud servers to access the Internet and save IP address resources, a high-performance **NAT gateway** is required. The gateway name can contain only letters, digits, underscores (_), and hyphens (-). **NOTE** The new gateway can be used only after the VPC subnet route is configured. **Learn how to configure**.	-
NAT Gateway Specifications	● The NAT gateway specifications refer to the maximum number of supported SNAT connections. **Learn more**. ● There are four types of specifications: **Small**, **Medium**, **Large**, and **Extra-large**.	-
EIP Name	An **EIP** provides independent public IP addresses and bandwidth for Internet access.	-

Parameter	Description	Example Value
Public Network Bandwidth	Select a bandwidth billing mode as needed. ● **By bandwidth**: You need to specify a bandwidth limit and pay for the amount of time you use the bandwidth. This is applicable to high or stable traffic. The bandwidth ranges from 1 to 280 Mbit/s. ● **By traffic**: You need to specify a bandwidth limit and pay for the total traffic you generate. This is applicable to light or sharply fluctuating traffic. The bandwidth ranges from 1 to 260 Mbit/s.	-
Enterprise Project	You can use an enterprise project to centrally manage your cloud resources and members by project. Select one as required.	-

Step 5 Click **OK**.

----End

9.3 Disabling Internet Access

Scenarios

Cancel the Internet access permission of desktops.

Prerequisites

Economical or enhanced Internet access has been enabled for a desktop.

Procedure

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

Step 2 In the navigation pane, choose **Internet Access Management**.

The **Internet Access** page is displayed.

Step 3 Select an Internet type to be disabled.

- If you select **Economical**, perform **Step 4**.
- If you select **Enhanced**, perform **Step 5** to **Step 6**.

Step 4 Select a desktop in the desktop list.

- Disabling Internet access for one desktop:
  a. Click **Disable Internet** in the **Operation** column of the desired desktop. The **Disable Internet** page is displayed.
  b. Select a method for **Disable By**.
     i. Unbinding only the EIP. After that, the desktop can be bound again.
     ii. Unbinding and deleting the EIP. After confirmation, you will be redirected to the EIP management page. Select the EIP to unbind and delete it.
  c. Click **OK**.
- Batch disabling Internet access for desktops:
  a. Batch select the desired desktops and click **Disable Internet** above the list. The **Disable Internet** page is displayed.
  b. Select a method for **Disable By**.
     i. Unbinding only the EIP. After that, the desktop can be bound again.
     ii. Unbinding and deleting the EIP. After confirmation, you will be redirected to the EIP management page. Select the EIP to unbind and delete it.
  c. Click **OK**.

Step 5 Click **Disable Internet** in the **Operation** column of the desktop list.

The **Disable Internet** page is displayed.

Step 6 Check the configuration of disabling Internet access.

NOTE

1. To disable Internet access, you need only to delete the SNAT rule. Related resources will not be deleted.

2. Delete resources that are no longer needed to avoid unexpected costs.

- Deleting an SNAT rule:
  a. Click **Delete >>**. In the SNAT rule list, locate the SNAT rule to delete, and click **Delete** in the **Operation** column.
  b. If you want to perform this operation, enter **DELETE** or click **Auto Enter**.
  c. Click **OK**.
- (Optional) Deleting an EIP:
  a. Click **Delete >>**. On the EIP page, choose **More** > **Release** in the **Operation** column.
  b. In the displayed dialog box, click **OK**.

- (Optional) Deleting a NAT gateway:
  a. Click **Delete >>**. In the NAT gateway list, locate the NAT gateway to delete, and click **Delete** in the **Operation** column.
  b. If you want to perform this operation, enter **DELETE** or click **Auto Enter**.
  c. Click **OK**.

  📖 NOTE

  Delete resources that are no longer needed to avoid unexpected costs.

----End

10 Monitoring and Analysis

10.1 Alarms

10.1.1 Creating an Alarm Rule

Scenarios

Cloud Eye lets you create alarm rules for Workspace and set notifications. This allows users to get real-time notifications and take immediate action when an alarm is triggered.

Prerequisites

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

Billing

You will not be charged for the basic alarm function. Alarm notifications sent by SMN will generate additional costs. For details, see **Billing**.

Procedure

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

Step 2 In **All Services**, choose **Cloud Eye** under **Management & Governance**.

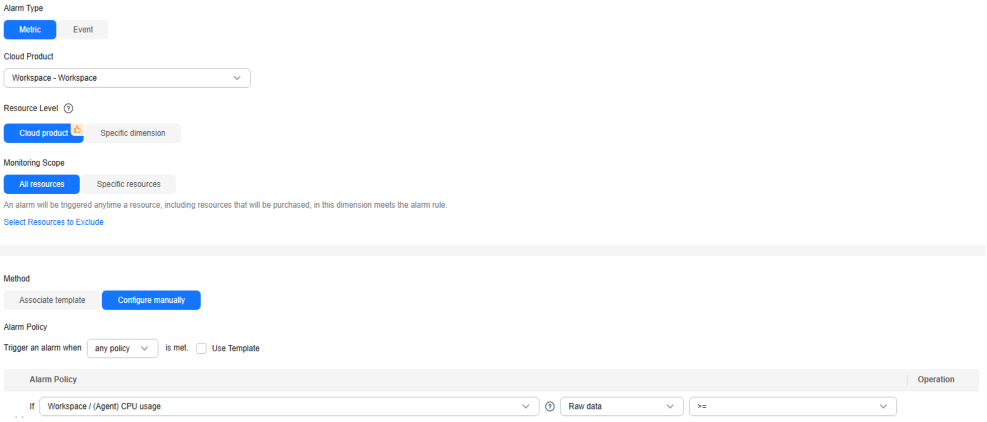
Step 3 In the navigation pane, choose **Alarm Management** > **Alarm Rules**.

Step 4 Click **Create Alarm Rule** in the upper right corner.

Step 5 Configure alarm rule parameters.

- If you select **Metric** for **Alarm Type**, you can create alarm rules by referring to **18.2 Monitoring Metrics Reported by Workspace to Cloud Eye** or **18.3 Cloud Eye OS Monitoring Metrics Supported by Workspace (with Agent Installed)**, as shown in **Figure 10-1**.

  Figure 10-1 Workspace metric alarm configuration

  Alarm Type

  Metric | Event

  Cloud Product

  Workspace - Workspace

  Resource Level

  Cloud product | Specific dimension

  Monitoring Scope

  All resources | Specific resources

  An alarm will be triggered anytime a resource, including resources that will be purchased, in this dimension meets the alarm rule.

  Select Resources to Exclude

  Method

  Associate template | Configure manually

  Alarm Policy

  Trigger an alarm when any policy is met. □ Use Template

Alarm Policy	Operation
If Workspace / (Agent) CPU usage ⓘ Raw data >=	

  Key parameters are described below. For details, see **Creating an Alarm Rule and Notifications**.

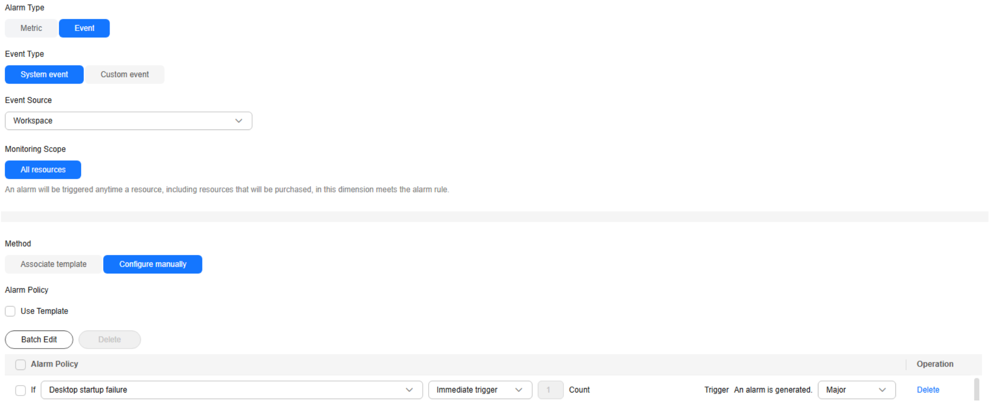
  - **Alarm Type**: The type of the alarm that the alarm rule applies to. You can select **Metric** or **Event**.
  - **Cloud Product**: When selecting **Metric** for **Alarm Type**, set this parameter to **Workspace - Workspace**.
  - **Resource Level**: This parameter is available only when you select **Metric** for **Alarm Type**. Two options are available: **Cloud product** (recommended) and **Specific dimension**.
  - **Monitoring Scope**: Select **All resources** or **Specific resources** that the alarm rule will apply to.
  - **Method**: Select **Associate template** and select a template from the drop-down list, or select **Configure manually**.

    NOTE

    After an associated template is modified, the policies contained in this alarm rule to be created will be modified accordingly.

- If you select **Event** for **Alarm Type**, you can create alarm rules by referring to **18.4 Cloud Eye Events Supported by Workspace**, as shown in **Figure 10-2**.

Figure 10-2 Workspace event alarm configuration



Alarm Type: Metric | **Event**

Event Type: **System event** | Custom event

Event Source: Workspace

Monitoring Scope: **All resources**

An alarm will be triggered anytime a resource, including resources that will be purchased, in this dimension meets the alarm rule.

Method: Associate template | **Configure manually**

Alarm Policy

□ Use Template

Batch Edit | Delete

□ Alarm Policy	Operation
□ If Desktop startup failure · Immediate trigger · 1 Count · Trigger An alarm is generated. Major	Delete

Key parameters are described below. For details, see **Creating an Alarm Rule and Notifications**.

- **Event Type**: You can select **System event** or **Custom event**.
- **Event Source**: Select **Workspace** from the drop-down list.
- **Method**: Select **Associate template** or **Configure manually**.
- **Alarm Policy**: Specifies the policy for triggering an alarm.

Step 6 Configure the alarm notification parameters.

Step 7 Click **Create**.

NOTE

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

----End

10.1.2 Viewing Alarm Records

When a monitoring metric reaches the threshold specified in an alarm rule or an event (such as desktop access or startup failure) occurs, you can view monitoring details in alarm records. By default, you can view alarm records of the past seven days. You can select a time range to view alarm records of the past 30 days. When an alarm is generated, you can **view alarm details**.

NOTE

On the **Alarm Records** page, set **Resource Type** to **Workspace** to view Workspace alarms.

10.2 User Connection Records

Scenarios

You can view user connection records to keep yourself informed of the desktop running status and user connection status. This facilitates troubleshooting and system maintenance.

Procedure

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

Step 2 In the navigation pane, choose **Monitoring and Analysis** > **User Connection Records**.

The **User Connection Records** page is displayed.

Step 3 View user connection records.

- Connection statistics

  You can view the connection statistics in the last seven days, last 30 days, or a custom time period. You can select search criteria (username and total usage duration in hours) to view user connection records. Specifically, you can view usernames, number of connection times (including successful and failed ones), and total usage duration.

- Connection records

  You can view the connection records in the last seven days, last 30 days, or a custom time period. You can select search criteria, including **Desktop Name**, **Connected User**, **Terminal OS Type**, and **Average Latency**, to view connection records in a specific period. Specifically, you can view **Desktop Name**, **Connected User**, **Terminal IP Address**, **Terminal OS Type**, **Desktop IP Address**, **Connection Started**, **Average Latency**, **Session Monitoring**, **Connection Details**, **Terminal MAC Address**, **Terminal Name**, **AccessClient Version**, **AccessAgent Version**, **Connection Established**, and **Reconnection (Yes/No)**.

  NOTE

  > Some connection record information is hidden by default. To view such information, click ⚙. On the displayed page, select the connection record information to be displayed and click **OK**.

  Session monitoring

  a. Click under **Session Monitoring** to go to the **Session Monitoring** page.

  b. You can view the following monitoring metrics in the last one hour, last 24 hours, last seven days, last 30 days, or a custom time period.

     Latency monitoring: round-trip time (RTT) between a terminal and the access gateway. This metric is available only for clients of 23.12.1.0 or later.

     Network jitter: time difference between the maximum network latency and the minimum network latency when using cloud desktops

     Packet loss rate: rate of data packets that fail to be transmitted from the sender to the receiver during the network communication of Workspace. Possible causes are network congestion, hardware device faults, and software errors.

     Traffic monitoring: statistics on the incoming and outgoing network traffic of the measured object per second

NOTE

- Under the **Connection Statistics** tab, click **Export** to export connection statistics.
- Under the **Connection Records** tab, click **Export** to export connection records.

----End

10.3 Desktop Usage Records

Scenarios

You can view desktop usage records to keep yourself informed of the running statuses of cloud desktops. This facilitates troubleshooting and system maintenance.

Procedure

Step 1 Log in to the console.

Step 2 In the navigation pane, choose **Monitoring and Analysis** > **Desktop Usage Records**.

The **Desktop Usage Records** page is displayed.

Step 3 On the **Desktop Usage Records** page, you can check information such as **Desktop Name**, **Usage Duration**, **Idle For**, and **Operation**.

Step 4 Click **View Connection Record** in the **Operation** column of the desired desktop.

The **User Connection Records** page is displayed.

Step 5 You can view the connection records in the last seven days, last 30 days, or a custom time period. You can select search criteria, including **Desktop Name**, **Connected User**, **Terminal OS Type**, and **Average Latency**, to view connection records in a specific period. Specifically, you can view **Desktop Name**, **Connected User**, **Terminal IP Address**, **Terminal OS Type**, **Desktop IP Address**, **Connection Started**, **Average Latency**, **Session Monitoring**, and **Connection Failure Cause**.

NOTE

Under the **Desktop Usage Records** tab, click **Export** to export desktop usage records.

Setting notifications

Step 6 Click **Set Notification** next to **Desktop Usage Records**. The authorization description is displayed upon the first setting.

NOTE

Workspace requests for the permission to access the following cloud service resources:

- SMN permissions

  To send notifications, Workspace needs the permission to access SMN.

After the permission granting is approved, an agency named **workspace_admin_trust** will be created on IAM. Do not delete or modify **workspace_admin_trust** when performing a scheduled task or using a desktop pool.

Step 7 Set notifications.

- **Send Notification**: indicates that the function is enabled.
- **Sent When**: A notification is sent when the desktop has been inactive for *x* days.
- **Notification Frequency**: A notification is sent once every *x* days.
- **Recipient**: Select one from the drop-down list box.

NOTE

You can select a topic. If there is no desired topic, click **Create Topic** (see **Creating a Topic**). After creating a topic, click **Add Subscription** in the **Operation** column of the desired topic (see **Adding a Subscription**) to configure the notification.

Step 8 Click **OK**.

----End

11 Tasks

11.1 Scheduled Tasks

11.1.1 Scheduled Shutdown

Scenarios

This section describes how to stop a cloud desktop or a desktop pool periodically.

Impact on the System

Stopping a desktop may result in the loss of unsaved personal application data.

Prerequisites

This operation can be performed only on desktops that are running.

Procedure

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

Step 2 In the navigation pane, choose **Tasks** > **Scheduled Tasks**.

The **Scheduled Tasks** page is displayed.

Step 3 Click **Create Scheduled Task** in the upper right corner of the page.

The **Create Scheduled Task** page is displayed.

Step 4 Configure a scheduled task.

- **Task Type**: Select **Shutdown**.

  NOTE

  After configuring a scheduled shutdown task, the desktop will not be stopped when it is still connected, even if the scheduled time arrives. Instead, the task is automatically postponed to the next scheduled time. If you choose to force execute the shutdown task, the desktop will be force stopped when the scheduled time arrives.

- **Task Name**: This parameter is user-defined.
- **Execution Interval**: You can select one of the following intervals:
  - **Specified time**: The time is accurate to seconds.
  - **By day**: You can specify **Time**, **Executed Once Per**, and **Expires At**.
  - **By week**: You can specify **Weekday**, **Time**, and **Expires At**.
  - **By month**: You can specify **Month**, **Day**, **Time**, and **Expires At**.
- **Time Zone**: The local time zone is selected by default.
- **Description**: This parameter is optional and user-defined.

Step 5 Determine whether to notify users.

- **Yes**: Set **Earlier Than Scheduled Task** to a value ranging from 1 to 10,080 minutes. Enter the notification, which can only be text in 1 to 400 characters.
- **No**: Perform **Step 6**.

  NOTE

  Notification messages are available only for Windows.

Step 6 Click **Next: Select Object**.

The page for selecting target objects is displayed.

Step 7 Select target objects as required. The objects include all desktops, desktop, desktop pool, and desktop tag.

NOTE

You can search for desktops in batches by entering multiple filter criteria. Use commas (,) to separate multiple values, for example, Desktop1,Desktop2,Desktop3.

Step 8 Click **Create Now**.

----End

11.1.2 Scheduled Startup

Scenarios

This section describes how to start a cloud desktop or a desktop pool periodically.

Impact on the System

This operation has no adverse impact on the system.

Prerequisites

This operation can be performed only on desktops that have been stopped.

Procedure

Step 1 Log in to the console.

Step 2 In the navigation pane, choose **Tasks** > **Scheduled Tasks**.

The **Scheduled Tasks** page is displayed.

Step 3 Click **Create Scheduled Task** in the upper right corner of the page.

The **Create Scheduled Task** page is displayed.

Step 4 Configure a scheduled task.

- **Task Type**: Select **Startup**.
- **Task Name**: This parameter is user-defined.
- **Execution Interval**: You can select one of the following intervals:
  - **Specified time**: The time is accurate to seconds.
  - **By day**: You can specify **Time**, **Executed Once Per**, and **Expires At**.
  - **By week**: You can specify **Weekday**, **Time**, and **Expires At**.
  - **By month**: You can specify **Month**, **Day**, **Time**, and **Expires At**.
- **Time Zone**: The local time zone is selected by default.
- **Description**: This parameter is optional and user-defined.

Step 5 Click **Next: Select Object**.

The page for selecting target objects is displayed.

Step 6 Select target objects as required. The objects include all desktops, desktop, desktop pool, and desktop tag.

NOTE

You can search for desktops in batches by entering multiple filter criteria. Use commas (,) to separate multiple values, for example, Desktop1,Desktop2,Desktop3.

Step 7 Click **Create Now**.

----End

11.1.3 Scheduled Restart

Scenarios

This section describes how to restart a cloud desktop or a desktop pool periodically.

Impact on the System

Restarting a desktop may result in the loss of unsaved personal application data.

Prerequisites

This operation can be performed only on desktops that are running.

Procedure

Step 1 Log in to the console.

Step 2 In the navigation pane, choose **Tasks** > **Scheduled Tasks**.

The **Scheduled Tasks** page is displayed.

Step 3 Click **Create Scheduled Task** in the upper right corner of the page.

The **Create Scheduled Task** page is displayed.

Step 4 Configure a scheduled task.

- **Task Type**: Select **Restart**.

  NOTE

  After configuring a scheduled restart task, the desktop will not be restarted when it is still connected, even if the scheduled time arrives. Instead, the task is automatically postponed to the next scheduled time. If you choose to force execute the restart task, the desktop will be force restarted when the scheduled time arrives.

- **Task Name**: This parameter is user-defined.
- **Execution Interval**: You can select one of the following intervals:
  - **Specified time**: The time is accurate to seconds.
  - **By day**: You can specify **Time**, **Executed Once Per**, and **Expires At**.
  - **By week**: You can specify **Weekday**, **Time**, and **Expires At**.
  - **By month**: You can specify **Month**, **Day**, **Time**, and **Expires At**.
- **Time Zone**: The local time zone is selected by default.
- **Description**: This parameter is optional and user-defined.

Step 5 Determine whether to notify users.

- **Yes**: Set **Earlier Than Scheduled Task** to a value ranging from 1 to 10,080 minutes. Enter the notification, which can only be text in 1 to 400 characters.
- **No**: Perform **Step 6**.

  NOTE

  Notification messages are available only for Windows.

Step 6 Click **Next: Select Object**.

The page for selecting target objects is displayed.

Step 7 Select target objects as required. The objects include all desktops, desktop, desktop pool, and desktop tag.

NOTE

You can search for desktops in batches by entering multiple filter criteria. Use commas (,) to separate multiple values, for example, Desktop1,Desktop2,Desktop3.

Step 8 Click **Create Now**.

----End

11.1.4 Scheduled Hibernation

Scenarios

This section describes how to hibernate a cloud desktop or a desktop pool periodically.

Impact on the System

This operation has no adverse impact on the system.

Prerequisites

This operation can be performed only on desktops that are running.

Procedure

Step 1 Log in to the console.

Step 2 In the navigation pane, choose **Tasks** > **Scheduled Tasks**.

The **Scheduled Tasks** page is displayed.

Step 3 Click **Create Scheduled Task** in the upper right corner of the page.

The **Create Scheduled Task** page is displayed.

Step 4 Configure a scheduled task.

- **Task Type**: Select **Hibernation**.

  NOTE

  1. Scheduled hibernation can be performed only on Windows desktops.
  2. After configuring a scheduled hibernation task, the desktop will not be hibernated when it is still connected, even if the scheduled time arrives. Instead, the task is automatically postponed to the next scheduled time. If you choose to force execute the hibernation task, the desktop will be force hibernated when the scheduled time arrives.

- **Task Name**: This parameter is user-defined.
- **Execution Interval**: You can select one of the following intervals:
  - **Specified time**: The time is accurate to seconds.
  - **By day**: You can specify **Time**, **Executed Once Per**, and **Expires At**.
  - **By week**: You can specify **Weekday**, **Time**, and **Expires At**.
  - **By month**: You can specify **Month**, **Day**, **Time**, and **Expires At**.
- **Time Zone**: The local time zone is selected by default.
- **Description**: This parameter is optional and user-defined.

Step 5 Determine whether to notify users.

- **Yes**: Set **Earlier Than Scheduled Task** to a value ranging from 1 to 10,080 minutes. Enter the notification, which can only be text in 1 to 400 characters.
- **No**: Perform **Step 6**.

NOTE

Notification messages are available only for Windows.

Step 6 Click **Next: Select Object**.

The page for selecting target objects is displayed.

Step 7 Select target objects as required. The objects include all desktops, desktop, desktop pool, and desktop tag.

NOTE

You can search for desktops in batches by entering multiple filter criteria. Use commas (,) to separate multiple values, for example, Desktop1,Desktop2,Desktop3.

Step 8 Click **Create Now**.

----End

11.1.5 Scheduled Snapshot Creation

Scenarios

This section describes how to create a snapshot for a desktop periodically.

Procedure

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

Step 2 In the navigation pane, choose **Tasks** > **Scheduled Tasks**.

The **Scheduled Tasks** page is displayed.

Step 3 Click **Create Scheduled Task** in the upper right corner of the page.

The **Create Scheduled Task** page is displayed.

Step 4 Configure a scheduled task.

- **Task Type**: Select **Snapshot creation**.

  NOTE

  - The snapshot feature of Huawei Cloud Workspace is currently in open beta test (OBT) and is free of charge. This feature will be charged in the future.
  - A maximum of 10 snapshot creation records can be saved for each desktop, including those created on the console and those created by end users.
  - Rebuilding the system disk, deleting a desktop, or deleting a disk will automatically delete the snapshots of the desktop.
- **Task Name**: This parameter is user-defined.
- **Snapshots Apply To**
  - **System disks and data disks**: A snapshot is created for both the system disk and data disks.
  - **System disks only**: A snapshot is created only for the system disk.
  - **Data disks only**: A snapshot is created only for the data disks.
- **Execution Interval**: You can select one of the following intervals:

  - **Specified time**: The time is accurate to seconds.
  - **By day**: You can specify **Time**, **Executed Once Per**, and **Expires At**.
  - **By week**: You can specify **Weekday**, **Time**, and **Expires At**.
  - **By month**: You can specify **Month**, **Day**, **Time**, and **Expires At**.
- **Time Zone**: The local time zone is selected by default.
- **Description**: This parameter is optional and user-defined.

Step 5 Determine whether to notify users.

- **Yes**: Set **Earlier Than Scheduled Task** to a value ranging from 1 to 10,080 minutes. Enter the notification, which can only be text in 1 to 400 characters.
- **No**: Perform **Step 6**.

  NOTE

  Notification messages are available only for Windows.

Step 6 Click **Next: Select Object**.

The page for selecting target objects is displayed.

Step 7 Select target objects as required. The objects include all desktops, desktop, desktop pool, and desktop tag.

NOTE

You can search for desktops in batches by entering multiple filter criteria. Use commas (,) to separate multiple values, for example, Desktop1,Desktop2,Desktop3.

Step 8 Click **Create Now**.

----End

11.1.6 Scheduled System Disk Rebuilding

Scenarios

This section describes how to rebuild a system disk periodically for a cloud desktop or a desktop pool. For details about the impact and restrictions of system disk rebuilding on the system, see **2.5.2 Rebuilding a System Disk** or **3.8.2 Rebuilding a System Disk**.

Procedure

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

Step 2 In the navigation pane, choose **Tasks** > **Scheduled Tasks**.

The **Scheduled Tasks** page is displayed.

Step 3 Click **Create Scheduled Task** in the upper right corner of the page.

The **Create Scheduled Task** page is displayed.

Step 4 Configure a scheduled task.

- **Task Type**: Select **System disk recomposing**.

- **Task Name**: This parameter is user-defined.
- **Rebuilding Method**: The default value is **Reinstall OS**.
- **Execution Interval**: You can select one of the following intervals:
  - **Specified time**: The time is accurate to seconds.
  - **By day**: You can specify **Time**, **Executed Once Per**, and **Expires At**.
  - **By week**: You can specify **Weekday**, **Time**, and **Expires At**.
  - **By month**: You can specify **Month**, **Day**, **Time**, and **Expires At**.
- **Time Zone**: The local time zone is selected by default.
- **Description**: This parameter is optional and user-defined.
- **Confirm System Disk Reinstallation**: Enter **Reinstall System Disk**.

Step 5 Determine whether to notify users.

- **Yes**: Set **Earlier Than Scheduled Task** to a value ranging from 1 to 10,080 minutes. Enter the notification, which can only be text in 1 to 400 characters.
- **No**: Perform **Step 6**.

  NOTE

  Notification messages are available only for Windows.

Step 6 Click **Next: Select Object**.

The page for selecting target objects is displayed.

NOTE

For the first time when you click **Next: Select Objects**, the authorization description will be displayed.

Cloud service administrator permissions: Workspace supports scheduled system disk rebuilding and auto scaling. Therefore, the tenant administrator permissions are required.

After the permission is granted (only once), an agency named **workspace_admin_trust** will be created in IAM. Do not delete or modify the agency when performing a scheduled task or using a desktop pool. For details, see **15.4 Entrustment Description**.

Step 7 Select target objects as required. The objects include all desktops, desktop, desktop pool, and desktop tag.

NOTE

You can search for desktops in batches by entering multiple filter criteria. Use commas (,) to separate multiple values, for example, Desktop1,Desktop2,Desktop3.

Step 8 Click **Create Now**.

----End

11.1.7 Scheduled Remote Script Execution

Scenarios

This section describes how to remotely run commands based on the created scripts to perform operations on cloud desktops. For details about the scripts to be executed, see **12.1 Script Management**.

Procedure

Step 1 Log in to the console.

Step 2 In the navigation pane, choose **Tasks** > **Scheduled Tasks**.

The **Scheduled Tasks** page is displayed.

Step 3 Click **Create Scheduled Task** in the upper right corner of the page.

The **Create Scheduled Task** page is displayed.

Step 4 Configure a scheduled task.

- **Task Type**: Select **Remote script**.
- **Task Name**: This parameter is user-defined.
- **Execution Interval**: You can select one of the following intervals:
  - **Specified time**: The time is accurate to seconds.
  - **By day**: You can specify **Time**, **Executed Once Per**, and **Expires At**.
  - **By week**: You can specify **Weekday**, **Time**, and **Expires At**.
  - **By month**: You can specify **Month**, **Day**, **Time**, and **Expires At**.
- **Time Zone**: The local time zone is selected by default.
- **Description**: This parameter is optional and user-defined.
- **Add Script**: Click **Add Script**. In the window displayed, select the desired scripts and click **OK**.

Step 5 Specify **Timeout**. The value ranges from 1 to 600 minutes.

Step 6 Determine whether to notify users.

- **Yes**: Set **Earlier Than Scheduled Task** to a value ranging from 1 to 10,080 minutes. Enter the notification, which can only be text in 1 to 400 characters.
- **No**: Perform **Step 7**.

NOTE

Notification messages are available only for Windows.

Step 7 Select **I've checked. No problem.** and click **Next: Select Object**.

The page for selecting target objects is displayed.

Step 8 Select target objects as required. The objects include all desktops, desktop, desktop pool, and desktop tag.

NOTE

You can search for desktops in batches by entering multiple filter criteria. Use commas (,) to separate multiple values, for example, Desktop1,Desktop2,Desktop3.

Step 9 Click **Create Now**.

----End

11.2 Scheduled Task Management

Scenarios

This section describes how to add, delete, or modify a scheduled task on the console.

Prerequisites

A scheduled task has been created.

Procedure

Enabling or disabling a scheduled task

Step 1 Log in to the console.

Step 2 In the navigation pane, choose **Tasks** > **Scheduled Tasks**.

The **Scheduled Tasks** page is displayed.

Step 3 In the task list, toggle on or off the switch in the **Enabled or Not** column of the desired scheduled task.

NOTE

- ● indicates that the scheduled task has been enabled.
- ○ indicates that the scheduled task has been disabled.

Checking the execution log of a scheduled task

Step 4 Click **Log Details** in the **Execution Log** column of the desired scheduled task.

Step 5 On the **Execution Log Details** page displayed, you can check the **Execution Time**, **Task Type**, **Execution Interval**, **Task Execution Status**, and **Successes/Failures** of the scheduled task.

NOTE

Click **Export** to export execution log details.

Modifying a scheduled task

Step 6 Click **Modify** in the **Operation** column of the desired scheduled task.

Step 7 You can modify parameters such as **Task Name**, **Execution Interval**, **Time Zone**, **Time**, **Description (Optional)**, **Add Script**, and **Timeout**.

NOTE

You can click **Add Script** to add or deselect scripts.

Step 8 Select **I've checked. No problem.** and go to the next step: configuring execution.

Step 9 On the page displayed, you can modify the **Execution Policy** and **Gray Rule** parameters.

NOTE

You can click **Batch Set** to determine whether the script is executed in the first batch.

Step 10 If you want to perform this operation, enter **YES** or click **Auto Enter**.

Step 11 Click **OK**.

Modifying the execution objects of a scheduled task

Step 12 Choose **More** > **Modify Object** in the **Operation** column of the desired scheduled task.

Step 13 Modify the objects as required and click **OK**.

Copying a scheduled task

Step 14 Choose **More** > **Copy** in the **Operation** column of the desired scheduled task.

Step 15 Specify **Task Name** and **Description** and click **OK**.

Deleting a scheduled task

Step 16 You can delete one scheduled task or batch delete multiple scheduled tasks.

- To delete one scheduled task, perform **Step 17** to **Step 18**.
- To batch delete multiple scheduled tasks, perform **Step 19** to **Step 21**.

Step 17 Choose **More** > **Delete** in the **Operation** column of the desired scheduled task. The page for deleting a scheduled task is displayed.

Step 18 Click **OK**.

Step 19 Select the scheduled tasks to be deleted and click **Delete** above the list.

Step 20 If you want to perform this operation, enter **YES** or click **Auto Enter**.

Step 21 Click **OK**.

----End

11.3 Export Center

Scenario

The administrator can export the desktop list, user list, and user login records of a cloud desktop. After the export is successful, the administrator can download or delete the record files in **Export Center**.

Procedure

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

Step 2 In the navigation pane, choose **Tasks** > **Export Center**.

The **Export Center** page is displayed.

Step 3 On the page displayed, you can view the file name, status, download status, generation time, and operation.

Step 4 In the **Operation** column of a file, you can click **Download** or **Delete** to download or delete the record file.

----End

11.4 Snapshots

Scenario

You can view and delete desktop snapshots on the console. If data of a cloud disk is lost or abnormal, you can use a snapshot to restore the desktop data to a specific time point to ensure service continuity.

Procedure

Snapshot settings

Step 1 Log in to the console.

Step 2 In the navigation pane, choose **Tasks** > **Snapshots**.

The **Snapshots** page is displayed.

Step 3 Click **Snapshot Settings**. The **Snapshot Settings** page is displayed.

Create snapshots on client: End users can create desktop snapshots on the client.

- : The function is enabled.
- : The function is disabled.

NOTE

- The Huawei Cloud Workspace snapshot service is in the open beta test (OBT) and is not charged. In the future, the service will be charged.
- You can save a maximum of five system disk snapshots and five data disk snapshots for each desktop, including those created on the console and those created by end users.
- Rebuilding the system disk, deleting a desktop, deleting a disk, or unbinding a desktop from a user and binding it to another user will automatically delete the snapshots of the desktop.

Step 4 Click **OK**.

Viewing a snapshot

Step 5 On the **Snapshots** page, you can view desktop snapshots by **Snapshot Name/ID**, **Desktop Name/ID**, **Disk Type**, **Snapshot Status**, and **Creation Mode**.

Restoring a snapshot

Step 6 You can restore one snapshot or batch restore multiple snapshots.

- To restore one snapshot, perform **Step 7** to **Step 8**.
- To batch restore multiple snapshots, perform **Step 9** to **Step 10**.

Step 7 Click **Restore** in the **Operation** column of the desired snapshot.

Step 8 On the page displayed, select **I understand the impact of this operation. Shut down the VM and restore the snapshot.** and click **OK**.

NOTE

- The desktop will be forcibly shut down during snapshot restoration.
- A time point will be specified for snapshot restoration. After the restoration, data generated after this time point cannot be retrieved.

Step 9 Batch select the desired snapshots and click **Restore** above the snapshot list.

Step 10 On the page displayed, select **I understand the impact of this operation. Shut down the VM and restore the snapshot.** and click **OK**.

NOTE

Only the snapshots of one data disk and one system disk can be restored for a desktop at a time.

Deleting a snapshot

Step 11 You can delete one snapshot or batch delete snapshots.

- To delete one snapshot, perform **Step 12** to **Step 13**.
- To batch delete snapshots, perform **Step 14** to **Step 15**.

Step 12 Click **Delete** in the **Operation** column of the desired snapshot.

Step 13 On the page displayed, select **I understand the impact of the operation and confirm to delete the snapshot.** and click **OK**.

Step 14 Batch select the desired snapshots and click **Delete** above the snapshot list.

Step 15 On the page displayed, select **I understand the impact of the operation and confirm to delete the snapshot.** and click **OK**.

----End

12 O&M

12.1 Script Management

Scenarios

On the console, the administrator can remotely run commands based on the created scripts to perform operations on cloud desktops.

NOTE

By default, PowerShell script execution is prohibited on Windows desktops. You need to run commands to enable PowerShell script execution.

Procedure: Press **Win** + **S** on the cloud desktop and enter **Windows PowerShell** in the search box. Right-click **Windows PowerShell** in the search result, and choose **Run as administrator** from the shortcut menu. On the displayed CLI page, enter **Set-ExecutionPolicy RemoteSigned**, press **Enter**, and select **y**.

Prerequisites

You have obtained the script.

Constraints

The API for batch command execution has the following requirements on components:

WKSAppCenterAgent 1.2.16 or later

HW.SysAgent 24.8.30.19029 or later

Procedure

Creating a script

Step 1 Log in to the console.

Step 2 In the navigation pane, choose **O&M** > **Script Management**.

The **Script Management** page is displayed.

Step 3 Click **Create Script** in the upper right corner to go to the **Create Script** page.

Step 4 Configure the script.

- **Script Name**: name of the script to be created. The script name must be unique and cannot be empty.
- **Execution Environment**: Select **Windows Script**, **Windows PowerShell**, or **Linux Shell**.
- **Description**: Enter the description.
- **Script Content**: Enter the script content.

Step 5 Click **OK**.

Executing a script

Step 6 Select the script to be executed in the script list.

Step 7 Click **Execute Script** above the list. The **Execute Script** page is displayed.

- To execute more scripts, click **Add Script**. In the displayed **Add Script** dialog box, select the scripts to execute and click **OK**.
- If the selected script does not need to be executed, click **Deselect** in the **Operation** column on the **Execute Script** page.

Step 8 Select **I've checked. No problem.** and click **Next: Select Target Object**.

Step 9 In the **Available Objects** area, search for the desktop or desktop pool name, select the name, and click **Select Execution Configuration**.

Step 10 Select an execution policy, as shown in Table 12-1.

Table 12-1 Execution policies

Policy Execution Mode	Parameter Description	Operation
Delivery to all	By default, the script is executed for all selected desktops or desktop pools.	1. Set **Execution Policy** to **Delivery to all**. 2. Set the script execution timeout, which ranges from 1 to 600 minutes.

Policy Execution Mode	Parameter Description	Operation
Gray delivery	**Specified**: whether the desktop or desktop pool for which the script is to be executed belongs to the first batch of objects.	1. If **Execution Policy** is set to **Gray delivery**, set **Gray Rule** to **Specified**. 2. Toggle on the **First-Batch Execution (Yes/No)** switch and select a desktop. **NOTE** First-batch execution is allowed only for running desktops whose login status is **Disconnected**, **In use**, or **Ready**. 3. Set the script execution timeout, which ranges from 1 to 600 minutes. 4. Enter the threshold for stopping executing the next batch if the number of desktops with script execution failure in the first batch is greater than or equal to *x*.

Policy Execution Mode	Parameter Description	Operation
	Random: The desktop or desktop pool for which the script is to be executed is randomly selected. **NOTE** The gray delivery policy divides desktops into the gray batch and non-gray batch. If the number of desktops with script execution failure in the first batch is greater than or equal to *x*, scripts will not be executed for desktops in the non-gray batch. If the threshold *x* is not reached, scripts will be executed for desktops in the non-gray batch.	1. If **Execution Policy** is set to **Gray delivery**, set **Gray Rule** to **Random**. 2. Set the script execution timeout, which ranges from 1 to 600 minutes. 3. Enter the threshold (*x*) for the number of desktops that are randomly selected for script execution in the first batch. 4. Enter the threshold for stopping executing the next batch if the number of desktops with script execution failure in the first batch is greater than or equal to *x*.

Step 11 If you want to perform this operation, enter **YES** or click **Auto Enter**. Click **Execute**.

NOTE

You can choose **Script Management** > **Desktop Script Records** or **Desktop Pool Script Records** to view the script execution result.

Editing a script

Step 12 Click **Edit** in the **Operation** column of the desired script. The **Edit Script** page is displayed.

Step 13 You can edit the script name, description, and script content.

Step 14 Click **OK**.

Copying a script

Step 15 Click **Copy** in the **Operation** column of the desired script. The **Copy Script** page is displayed.

Step 16 You can edit the copied script name, execution environment, description, and script content.

Step 17 Click **OK**.

Deleting a script

Step 18 Click **Delete** in the **Operation** column of the desired script. The **Delete Script** page is displayed.

Step 19 Click **OK**.

----End

Desktop or desktop pool script records

Step 1 Under the **Desktop Script Records** tab, you can use filters, such as **Desktop ID**, **Script ID**, **Task ID**, **Execution Status**, **First-Batch Execution (Yes/No)**, and **Started**, to check data of the desktop, such as **Desktop Name/ID**, **Script Name/ID**, **Task ID**, **Execution Status**, **First-Batch Execution (Yes/No)**, **Response**, **Execution History**, **Started**, and **Ended**.

NOTE

- In the **Script Name/ID** column, click a script name to check **History Script Details**.
- In the **Execution Status** column, click **Retry** and click **OK** to execute the script again.
- In the **Response** column, click **View** to check the response of the desktop to the script execution. You can click **Download** to download the response.
- In the **Execution History** column, click **View** to view **Execution Status**, **First-Batch Execution (Yes/No)**, **Response**, **Started**, and **Ended** of the script. Click **Retry** to execute the script again. Click **View** in the **Response** column to view the response, or click **Download** to download the response.

Step 2 Under the **Desktop Pool Script Records** tab, you can use filters, such as **Desktop Pool ID**, **Script ID**, **Task ID**, **Execution Status**, and **Started**, to check data of the desktop pool, such as **Desktop Pool Name/ID**, **Script Name/ID**, **Task ID**, **Execution Status**, **Execution Details**, **Started**, and **Ended**.

NOTE

- In the **Script Name/ID** column, click a script name to check **History Script Details**.
- In the **Execution Status** column, click **Retry** and click **OK** to execute the script again.
- In the **Execution Details** column, click **View** to check data of the desktop pool, such as **Desktop Name/ID**, **Script Name/ID**, **Task ID**, **Execution Status**, **First-Batch Execution (Yes/No)**, **Response**, **Execution History**, **Started**, and **Ended**.
  - In the **Response** column, click **View** to check the response of the desktop to the script execution. You can click **Download** to download the response.
  - In the **Execution History** column, click **View** to view **Execution Status**, **First-Batch Execution (Yes/No)**, **Response**, **Started**, and **Ended** of the script. Click **Retry** to execute the script again. Click **View** in the **Response** column to view the response, or click **Download** to download the response.

----End

12.2 Command Records

Scenario

The administrator can check the remote script execution records of desktops or desktop pools on the Workspace console.

Prerequisites

The script has been remotely executed on a desktop or desktop pool.

Procedure

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

Step 2 In the navigation pane, choose **O&M** > **Command Records**.

The **Command Records** page is displayed.

Step 3 Under the **Desktops** tab, you can use filters, such as **Desktop ID**, **Task ID**, **Execution Status**, and **Started**, to check data of the desktop, such as **Desktop Name/ID**, **Command Details**, **Task ID**, **Execution Status**, **Response**, **Started**, and **Ended**.

Step 4 Under the **Desktop Pools** tab, you can use filters, such as **Desktop Pool ID**, **Execution Status**, and **Started**, to check data of the desktop pool, such as **Desktop Pool Name/ID**, **Command Details**, **Execution Status**, **Execution Details**, **Started**, and **Ended**.

----End

13 Application Center

13.1 Application Distribution

13.1.1 Adding an Application

Scenarios

Administrators can upload enterprise applications or third-party applications and manage and allocate applications through App Center in a unified manner.

NOTE

- This operation can be performed only on Windows desktops.
- Before using App Center, you need to contact O&M personnel to check whether the basic components of your desktops have been upgraded to a version that supports App Center.

Prerequisites

The application to be installed has been obtained and verified as expected.

Installation Restrictions

- Automatic installation
  - Automatic installation is to install applications with the system permission. Applications that can be installed only by user roles, such as WPS, cannot adopt automatic installation.
  - The actual installation result will not be verified.
- Installation through the App Center client
  - Installation by users with common user group permissions is not supported.

– The installation result of the application whose advanced configuration items are not correctly set is not verified.

Procedure

Step 1 Log in to the console.

Step 2 In the navigation pane on the left, choose **App Center** > **App Distribution**.

The **App Center** page is displayed.

Step 3 Click **Add App** in the upper right corner.

The **Add App** page is displayed.

Step 4 Configure an application, as shown in **Table 13-1** and **Table 13-2**.

Table 13-1 Basic parameters

Parameter	Description	Restriction	Example Value
App Name	User-defined cloud application name: If you enter *xxx*.exe or *xxx*, the execution process of *xxx*.exe will be stopped during automatic installation.	● The application name can contain visible characters or spaces but cannot contain only spaces. ● The value contains 1 to 128 characters.	HelloAppCenter
Version	ID of an application version.	● The value can contain a maximum of 128 characters.	-
Description	Description of an application, which helps identify the application.	● The value contains a maximum of 2048 characters.	Office software
App Icon	Icon of an application, which helps identify the application. If you do not upload an application icon, the default icon is used.	● Currently, only .png images are supported, and the maximum size is 64 KB.	-

Parameter	Description	Restriction	Example Value
App Category	Category of an application.	Currently, the following application categories are supported: ● System ● Work ● Security ● Browser ● Media ● Design ● Programming ● Input Method ● Other	-
OS	OS of the application.	● Option: Windows	Windows
App Source	Location of the application. If you choose to upload a file, the file is stored in OBS. If you select a link, the application is downloaded from the link.	Application source: ● File Upload ● Link	File Upload

Parameter	Description	Restriction	Example Value
File Upload	Application file to be uploaded. After uploading the application, select **I have read and agree to Non-infringement Commitment and Disclaimer**.	● Supported application file types: – .exe – .msi – .rar – .zip – .7z ● The size of the application package to be uploaded cannot exceed 5 GB. **NOTE** ● When you upload a file for the first time, an OBS bucket named **app-center-*xx*** is created to store the file. ● Only App Center 1.0.3 and later versions support compressed packages.	-

Parameter	Description	Restriction	Example Value
Link	Link for downloading an application. Currently, only HTTP or HTTPS links are supported. Note: The path in the address must end with the file name extension, for example, https://*xxx.xxx.xxx/xxx/xxx*.exe. Select **I have read and agree to Non-infringement Commitment and Disclaimer**.	● The link must be a valid one that can be accessed by the desktop.	-
Installation Mode	Mode of installing an application.	The options are as follows: ● Silent installation ● GUI ● Distributing Installation Package	-

Parameter	Description	Restriction	Example Value
Installation Parameter	Parameters needed for application installation. If this parameter is not specified, the default installation parameter is used. ● Default parameter of the .exe installation package: **/S** ● Fixed parameter of the .msi installation package: **/qb REBOOT=SUPPRESS** **NOTE** Note: For details about how to obtain the parameters of the .exe installation package, see the instruction. The parameters of the .msi installation package are built-in and do not need to be entered.	● The value contains a maximum of 2048 characters. ● If Internet access is required during application installation, ensure that the desktop where the application is installed has the permission for accessing the Internet.	/S

NOTE

How do I obtain silent installation parameters?

Among the applications that support silent installation, some applications need silent installation parameters to perform silent installation. Obtain silent installation parameters from the application developer or third parties, for example, from the official help document of the application support center, or third-party support websites. Take 7-Zip as an example. You can query the silent installation parameters of 7-Zip from the third-party silent installation knowledge base **Silent Install HQ**.

7-Zip 22.00 (32-bit) Silent Install (EXE)

1. Visit https://www.7-zip.org/download.html.

2. Click the **Download** link for 32-bit x86.exe.

3. Download the file to a folder created in **C:\Downloads**.

4. Open an elevated command prompt by right-clicking **Command Prompt** and selecting **Run as Administrator**.

5. Go to **C:\Downloads folder**.

6. Run **7z2200.exe /S**.

7. Press **Enter**.

Table 13-2 Advanced settings

Parameter	Description	Restriction	Example Value
Registered Name	Registration item **DisplayName** in the registry after the application is installed.	-	Value: App Center See **Figure 13-1**.
Registered Version	Registration item **DisplayVersion** in the registry after the application is installed.	-	Value: 0.0.8.0 See **Figure 13-1**.
Executable Program Name	File name of the application program executed when the application is started.	-	-

NOTE

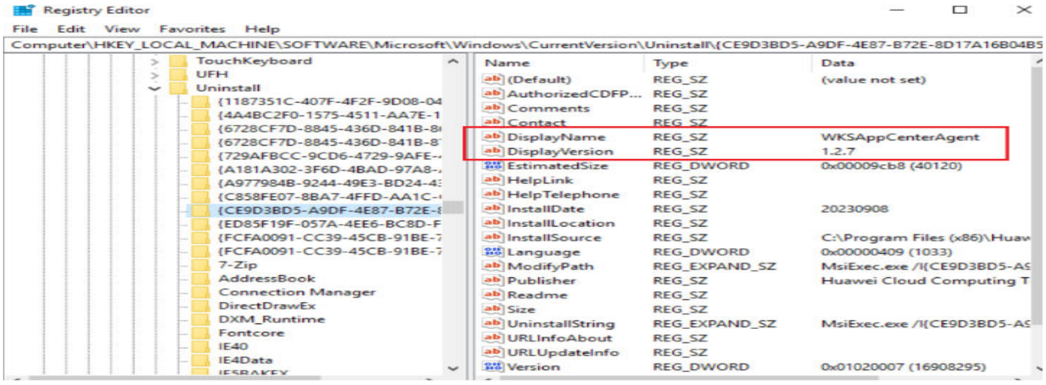
About advanced settings:

This configuration item applies to the App Center client.

To collect information after the application is installed, you need to correctly set the advanced configuration item. Otherwise, the application cannot be opened or uninstalled.

If the installation location and uninstallation parameters of an application are not correctly registered in the OS, the application cannot be opened or uninstalled.

Figure 13-1 Example of App Center


Registry Editor
File
Edit
View
Favorites
Help
TouchKeyboard
UFH
Uninstall
{1187351C-407F-4F2F-9D08-04
{4A4BC2F0-1575-4511-AA7E-1
{6728CF7D-8845-436D-841B-8
{6728CF7D-8845-436D-841B-8
{729AFBCC-9CD6-4729-9AFE-
{A181A302-3F6D-4BAD-97A8-
{A977984B-9244-49E3-BD24-4
{C858FE07-8BA7-4FFD-AA1C-
{CE9D3BD5-A9DF-4E87-B72E-
{ED85F19F-057A-4EE6-BC8D-F
{FCFA0091-CC39-45CB-91BE-7
{FCFA0091-CC39-45CB-91BE-7
7-Zip
AddressBook
Connection Manager
DirectDrawEx
DXM_Runtime
Fontcore
IE40
IE4Data
IE5BAKEX

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{CE9D3BD5-A9DF-4E87-B72E-8D17A16B04B5

Name	Type	Data
(Default)	REG_SZ	(value not set)
AuthorizedCDFP...	REG_SZ	
Comments	REG_SZ	
Contact	REG_SZ	
DisplayName	REG_SZ	WKSAppCenterAgent
DisplayVersion	REG_SZ	1.2.7
EstimatedSize	REG_DWORD	0x00009cb8 (40120)
HelpLink	REG_SZ	
HelpTelephone	REG_SZ	
InstallDate	REG_SZ	20230908
InstallLocation	REG_SZ	
InstallSource	REG_SZ	C:\Program Files (x86)\Huaw
Language	REG_DWORD	0x00000409 (1033)
ModifyPath	REG_EXPAND_SZ	MsiExec.exe /I{CE9D3BD5-A9
Publisher	REG_SZ	Huawei Cloud Computing T
Readme	REG_SZ	
Size	REG_SZ	
UninstallString	REG_EXPAND_SZ	MsiExec.exe /I{CE9D3BD5-A9
URLInfoAbout	REG_SZ	
URLUpdateInfo	REG_SZ	
Version	REG_DWORD	0x01020007 (16908295)

Step 5 Select **I have read and agree to Non-infringement Commitment and Disclaimer**. Click **Confirm**.

----End

13.1.2 Managing Applications

Scenario

Administrators can upload enterprise applications or third-party applications and manage and allocate applications through App Center in a unified manner.

Prerequisites

The administrator has uploaded an application and installed the application for the user in the App Center.

Procedure

Step 1 Log in to the Workspace console.

Step 2 In the navigation pane on the left, choose **App Center** > **App Distribution**.

The **App Center** page is displayed.

Step 3 Perform the operations listed in **Table 13-3** as required.

Table 13-3 Operations

Operation	Procedure
Setting permissions	1. On the right of the **App Center** page, click **Set Permission**. The page for setting permissions is displayed. 2. Users can select either of the following types: ● **All**: applicable to all users ● **Some users**: applicable to some users 3. Click **OK**.
Automatic installation	1. On the right of the **App Center** page, click **Auto Install**. The automatic installation page is displayed. 2. You can select either of the following user types: ● **All**: applicable to all users ● **Some users**: applicable to some users 3. Click **OK**. 4. You can view the installation records. **NOTE** Currently, AD user groups are not supported.
More > **Edit** **More** > **Delete** **More** > **Set Visibility**	1. In the App Center list, choose **More** > **Edit** or **Delete**. The page for modifying or deleting an application is displayed. 2. You can modify parameters of an added application or delete an application. 3. In the App Center list, choose **More** > **Set Visibility**. The **Set Visibility** page is displayed. 4. Set the visibility as required.

Operation	Procedure
Batch automatic installation	1. Select one or more applications on the **App Center** page. 2. Click **Batch Auto Install** on the **App Center** page. The automatic installation page is displayed. 3. You can select either of the following user types: ● **All**: applicable to all users ● **Some users**: applicable to some users 4. Click **OK**. **NOTE** Currently, AD user groups are not supported.
Batch deletion	1. Select one or more applications on the **App Center** page. 2. Click **Batch Delete** in the upper left corner of the **App Center** page. The batch deletion page is displayed. 3. Click **OK**.
Batch setting permissions	1. Select one or more applications on the **App Center** page. 2. Click **Batch Set Permission** on the **App Center** page. The page of batch setting permissions is displayed. 3. You can select either of the following authorization types: ● **All**: applicable to all users ● **Some users**: applicable to some users 4. Click **OK**.
Batch setting visibility	1. Select one or more applications on the **App Center** page. 2. Click **Batch Set Visibility** on the **App Center** page. The page of batch setting visibility is displayed. 3. Select visibility. 4. Click **OK**.
Viewing installation records	On the **App Center** page, click **View Installation Record** to view the application installation result.

Operation	Procedure
Viewing installation records > Automatic reinstallation	Automatic reinstallation of one application 1. Click **View Installation Record** on the **App Center** page. 2. On the **View Installation Record** page, click **Auto Reinstall** in the **Operation** column of the application that needs to be automatically reinstalled. Batch automatic reinstallation of applications 1. Click **View Installation Record** on the **App Center** page. 2. Select the applications that need to be automatically reinstalled. 3. On the **View Installation Record** page, click **Batch Auto Reinstall**. 4. Click **OK**.
Viewing installation records > Deleting applications	Automatic deletion of one application 1. Click **View Installation Record** on the **App Center** page. 2. On the **View Installation Record** page, click **Delete** in the **Operation** column of the application installation record to be deleted. Batch automatic deletion of applications 1. Click **View Installation Record** on the **App Center** page. 2. Select the application installation records to be deleted. 3. On the **View Installation Record** page, click **Batch Delete**. 4. Click **OK**.

NOTE

Currently, the App Center supports only the execution of application installation commands and displays the execution results in installation records. The App Center does not support the detection of the actual application status after installation. Before automatic installation, you are advised to log in to an available desktop to check whether the installation result meets the expectation.

----End

13.1.3 Setting Up a File Server

Scenario

Set up a file server.

Prerequisites

- A Windows Server ECS is available. For details, see **Purchasing an ECS**.
- The VPC of the ECS must be the same as that of the Workspace tenant. If different VPCs are used, you need to configure a VPC peering connection and ensure that the IP address segments do not conflict.

Procedure

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

Step 2 In the navigation pane on the left, click ☰ and choose **Elastic Cloud Server**.

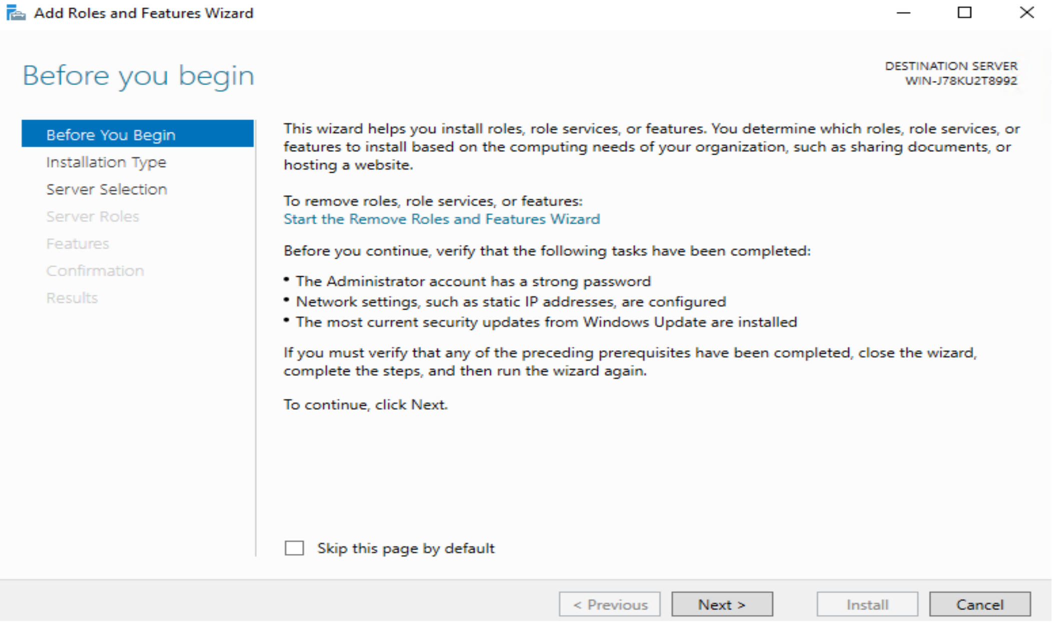
Step 3 Locate the row that contains the target ECS, click **Remote Login** in the **Operation** column, and enter the username and password created during ECS purchase.

Installing the IIS management console

Step 4 Click ⊞ in the lower left corner of the ECS and choose **Server Manager**. The **Server Manager** page is displayed.

Step 5 On the **Server Manager** page, click **Add role and features**. The **Add Roles and Features Wizard** dialog box is displayed, as shown in **Figure 13-2**.

Figure 13-2 Installation wizard



This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

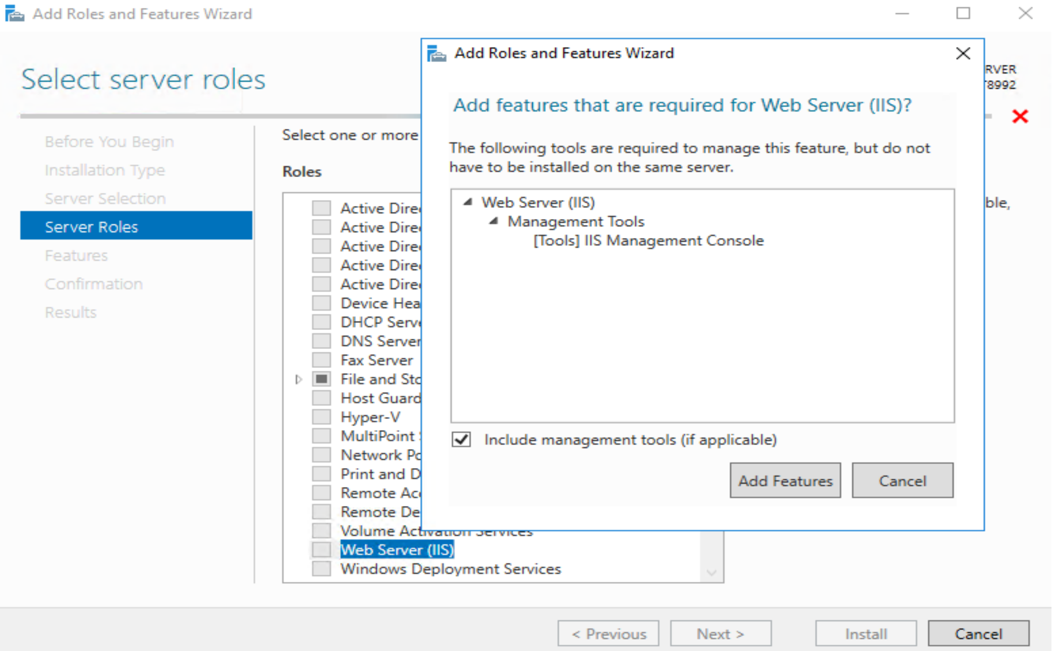
If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default

Step 6 Click **Next** as prompted. On the **Server Roles** page, select **Web Server (IIS)**. In the displayed **Add features that are required for Web Server (IIS)** dialog box, click **Add Features**, as shown in **Figure 13-3**.

Figure 13-3 Configuring a server role



Add Roles and Features Wizard

Select server roles

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results

Select one or more

Roles

- □ Active Dire
- □ Active Dire
- □ Active Dire
- □ Active Dire
- □ Active Dire
- □ Device Hea
- □ DHCP Serv
- □ DNS Server
- □ Fax Server
- ▪ File and Sto
- □ Host Guard
- □ Hyper-V
- □ MultiPoint
- □ Network Po
- □ Print and D
- □ Remote Ac
- □ Remote De
- □ Volume Activation Services
- □ Web Server (IIS)
- □ Windows Deployment Services

Add Roles and Features Wizard

Add features that are required for Web Server (IIS)?

The following tools are required to manage this feature, but do not have to be installed on the same server.

- Web Server (IIS)
  - Management Tools
    - [Tools] IIS Management Console

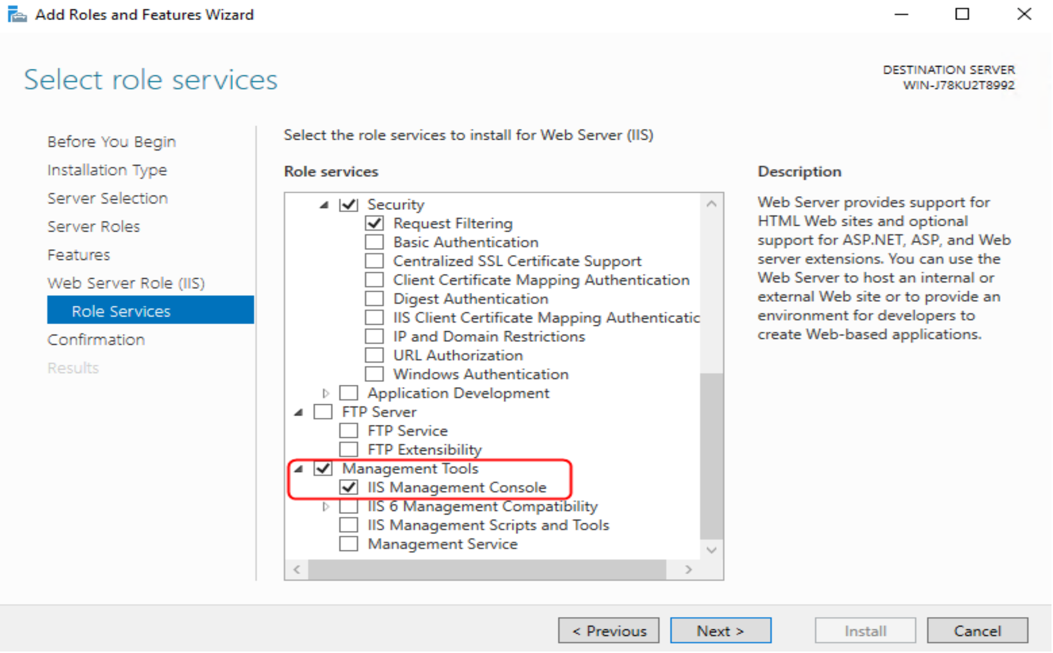
☑ Include management tools (if applicable)

Add Features | Cancel

< Previous | Next > | Install | Cancel

Step 7 Click **Next**. On the **Role Services** page, ensure that **IIS Management Console** under **Management Tools** has been selected, as shown in **Figure 13-4**.

Figure 13-4 IIS management console



Add Roles and Features Wizard

Select role services

DESTINATION SERVER
WIN-J78KU2T8992

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results

Select the role services to install for Web Server (IIS)

Role services

- ☑ Security
  - ☑ Request Filtering
  - □ Basic Authentication
  - □ Centralized SSL Certificate Support
  - □ Client Certificate Mapping Authentication
  - □ Digest Authentication
  - □ IIS Client Certificate Mapping Authenticatic
  - □ IP and Domain Restrictions
  - □ URL Authorization
  - □ Windows Authentication
- □ Application Development
- □ FTP Server
  - □ FTP Service
  - □ FTP Extensibility
- ☑ Management Tools
  - ☑ IIS Management Console
  - □ IIS 6 Management Compatibility
  - □ IIS Management Scripts and Tools
  - □ Management Service

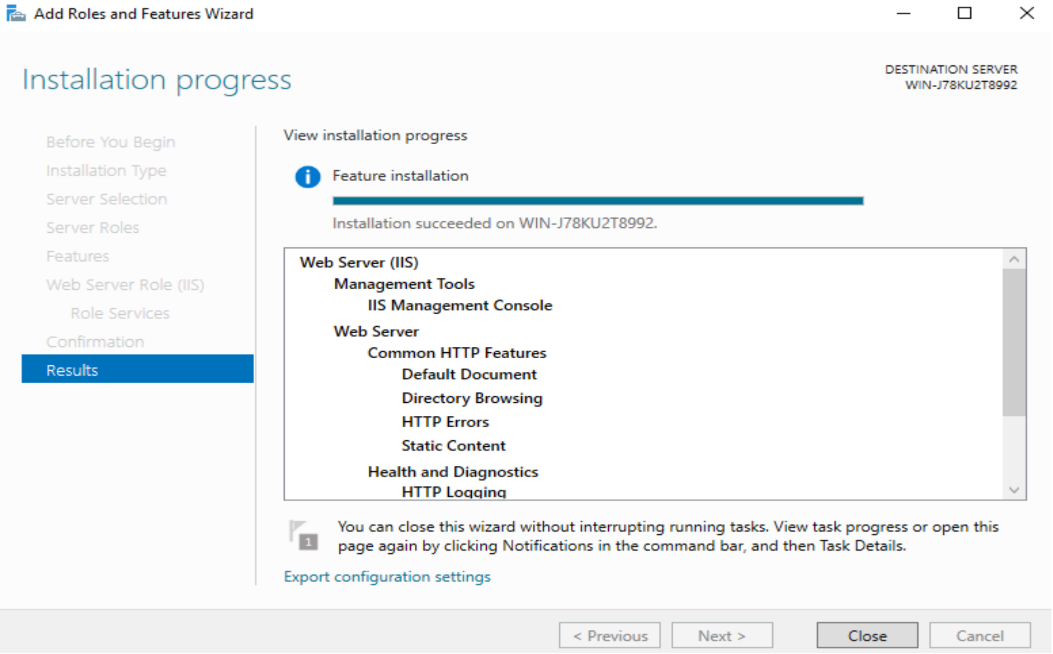
Description

Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.

< Previous | Next > | Install | Cancel

Step 8 Click **Next** to switch to the confirmation page. Confirm the information and click **Install**. Wait for the installation result. If the information shown in **Figure 13-5** is displayed, the installation is successful.

Figure 13-5 Example installation result



Add Roles and Features Wizard

Installation progress

DESTINATION SERVER
WIN-J78KU2T8992

View installation progress

Feature installation

Installation succeeded on WIN-J78KU2T8992.

Web Server (IIS)
Management Tools
IIS Management Console
Web Server
Common HTTP Features
Default Document
Directory Browsing
HTTP Errors
Static Content
Health and Diagnostics
HTTP Logging

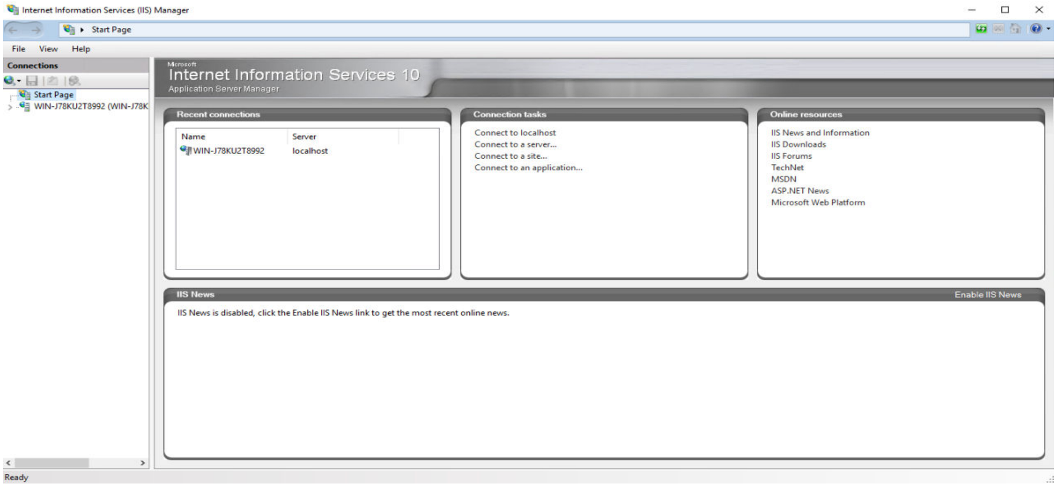
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

Configuring the IIS console (Configuring applications)

Step 9 Click ⊞ in the lower left corner of the ECS and choose **Administrative Tools** > **Internet Information Service (IIS) Manager**. The **Internet Information Service (IIS) Manager** page is displayed, as shown in **Figure 13-6**.

Figure 13-6 IIS Manager



Internet Information Services (IIS) Manager

Start Page
File View Help
Connections
Start Page
WIN-J78KU2T8992 (WIN-J78K
Microsoft
Internet Information Services 10
Application Server Manager

Recent connections

Name	Server
WIN-J78KU2T8992	localhost

Connection tasks

Connect to localhost
Connect to a server...
Connect to a site...
Connect to an application...

Online resources

IIS News and Information
IIS Downloads
IIS Forums
TechNet
MSDN
ASP.NET News
Microsoft Web Platform

IIS News

Enable IIS News

IIS News is disabled, click the Enable IIS News link to get the most recent online news.

Ready

Step 10 On the **Internet Information Services (IIS) Manager** page, expand the *server name* and **Sites**, right-click **Default Web Site** and select **Remove** from the shortcut menu.

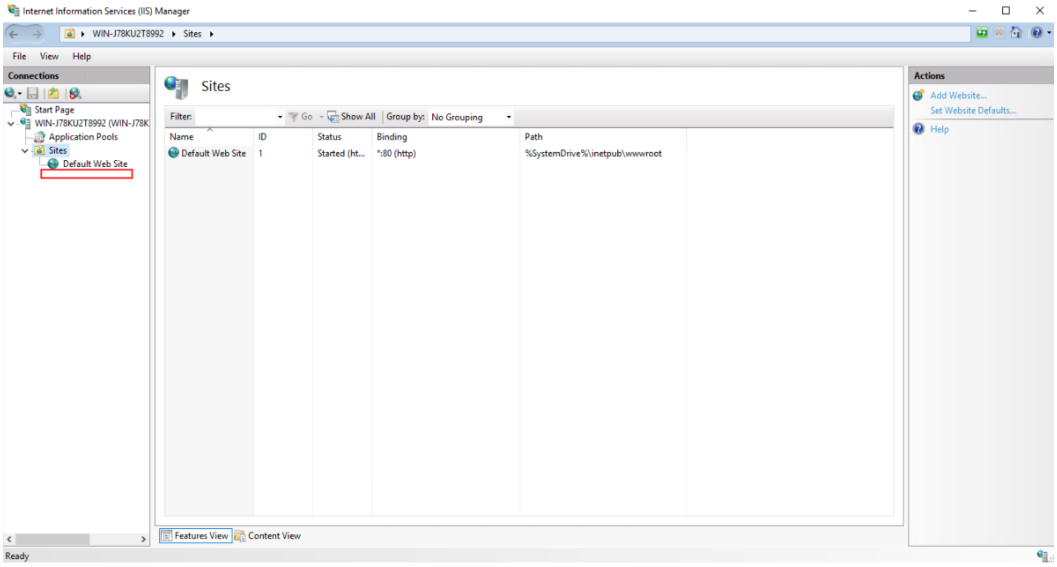
Step 11 Right-click **Sites** and choose **Add Website** from the shortcut menu to configure website information.

- **Site Name**: This parameter is user-defined.

- **Physical path**: path for storing the local application installation package.
- **Type**: Select **http**.
- **IP address**: Select the ECS IP address from the drop-down list box.
- **Port**: Configure this parameter as required.
- **Host name**: This parameter is left blank by default.

Step 12 After the configuration is complete, click **OK**. The website has been added, as shown in **Figure 13-7**.

Figure 13-7 Adding a website

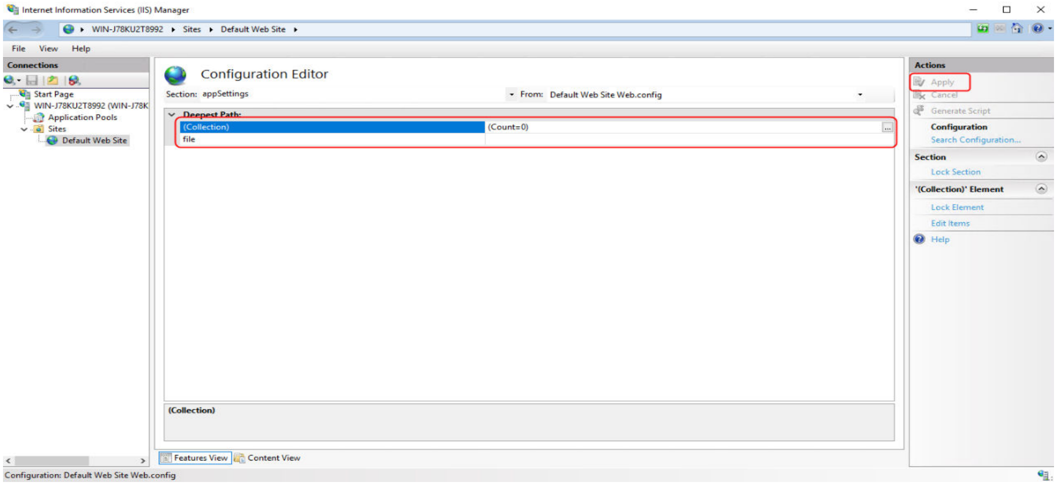

Internet Information Services (IIS) Manager
WIN-J78KU2T8992 ▸ Sites ▸
File View Help
Connections
Start Page
WIN-J78KU2T8992 (WIN-J78K
Application Pools
Sites
Default Web Site
Sites
Filter: Go Show All Group by: No Grouping
Actions
Add Website...
Set Website Defaults...
Help
Features View Content View
Ready

Name	ID	Status	Binding	Path
Default Web Site	1	Started (ht...	*:80 (http)	%SystemDrive%\inetpub\wwwroot

Step 13 Click the website added in **12**. On the home page of the website, double-click **Configuration Editor**.

Step 14 On the **Configuration Editor** page, click ▾ on the right of **Section:**. Choose **system.webServer** > **directoryBrowse**, change the value of **enabled** from **False** to **True**, and click **Apply**, as shown in **Figure 13-8**.

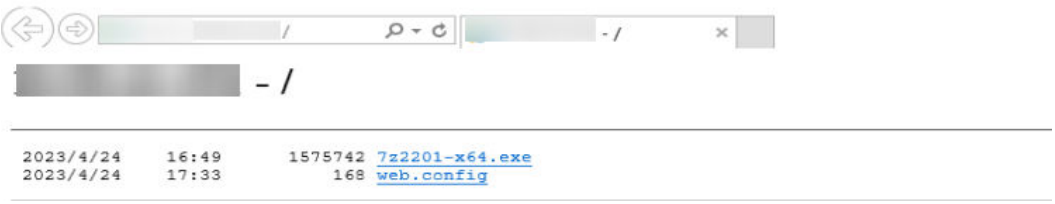
Figure 13-8 Configuration editor



Verifying (applications)

Step 15 On the ECS, click to open Internet Explorer. In the address box, enter the server address (the type and IP address configured in **11**, for example, http://192.168.1.1) to open the application, as shown in **Figure 13-9**.

Figure 13-9 Opening an application



- /

```
2023/4/24    16:49      1575742 7z2201-x64.exe
2023/4/24    17:33          168 web.config
```

Adding an application

Step 16 Log in to the Workspace console.

Step 17 In the navigation pane, choose **App Center**.

The **App Center** page is displayed.

Step 18 Click **Add App** in the upper right corner.

The **Add App** page is displayed.

Step 19 On the displayed page, configure application parameters by referring to **Table 13-1**. Set **App Source** to **Link**. The link address is the server address obtained in **11**.

NOTE

The link address must end with the file name extension. The format is https://*Absolute path of the .exe file*, for example, https://*xxx*/7z2201-x64.exe.

Step 20 Click **OK**.

----End

(Optional) IP and domain restrictions

NOTE

- The administrator can configure the IP and domain restrictions to restrict the IP addresses allowed to access the client.
- The file server has been set up by referring to **1** to **8**.

Step 1 .

Step 2 In the navigation pane on the left, click ☰ and choose **Elastic Cloud Server**.

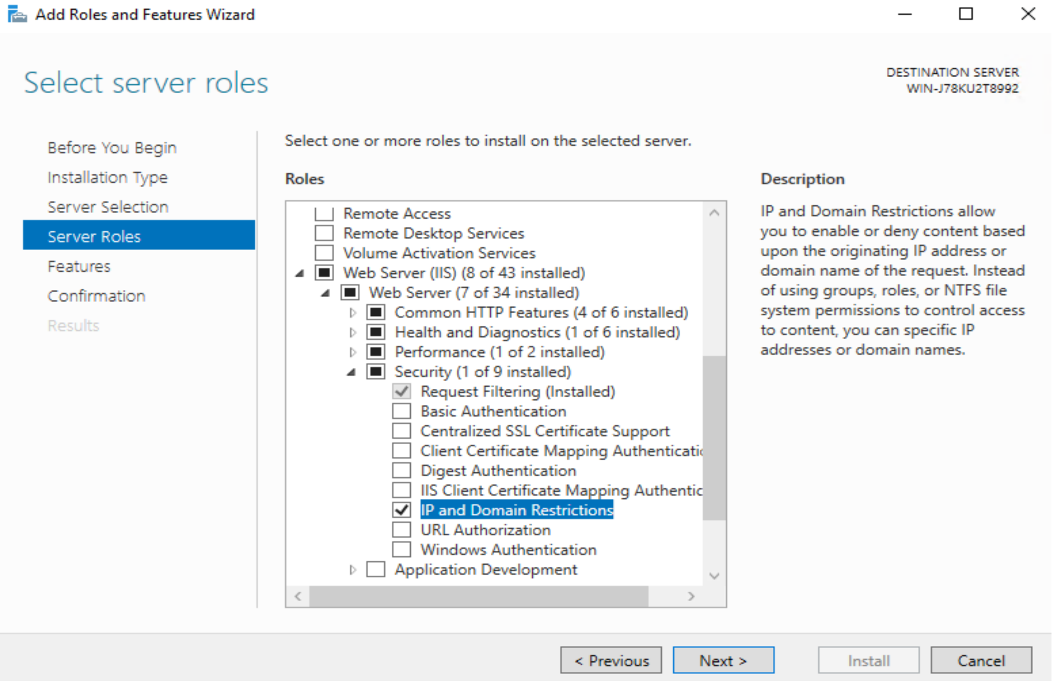
Step 3 Locate the row that contains the target ECS, click **Remote Login** in the **Operation** column, and enter the username and password created during ECS purchase.

Step 4 Click ⊞ in the lower left corner of the ECS and choose **Server Manager**. The **Server Manager** page is displayed.

Step 5 On the **Server Manager** page, click **Add role and features**. The **Add Roles and Features Wizard** dialog box is displayed. Click **Next** as prompted.

Step 6 On the **Server Roles** page, select **Web Server (IIS)**, choose **Web Server** > **Security**, and select **IP and Domain Restrictions**, as shown in **Figure 13-10**.

Figure 13-10 Adding a server role



Select server roles

DESTINATION SERVER
WIN-J78KU2T8992

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

Roles

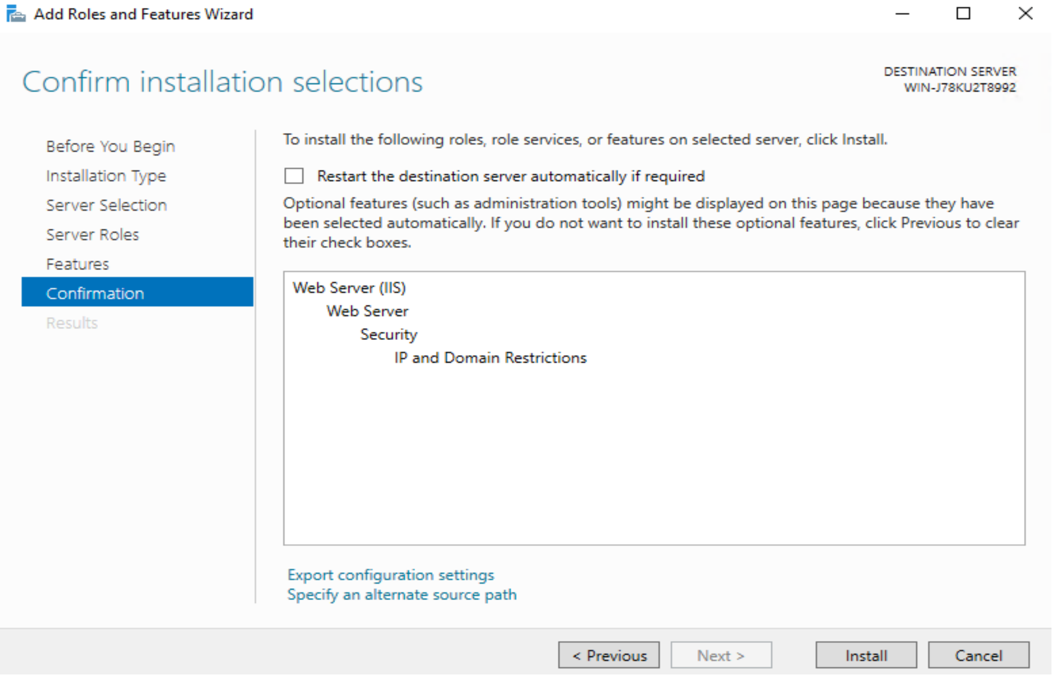
- □ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- ■ Web Server (IIS) (8 of 43 installed)
  - ■ Web Server (7 of 34 installed)
    - ■ Common HTTP Features (4 of 6 installed)
    - ■ Health and Diagnostics (1 of 6 installed)
    - ■ Performance (1 of 2 installed)
    - ■ Security (1 of 9 installed)
      - ☑ Request Filtering (Installed)
      - □ Basic Authentication
      - □ Centralized SSL Certificate Support
      - □ Client Certificate Mapping Authenticati
      - □ Digest Authentication
      - □ IIS Client Certificate Mapping Authentic
      - ☑ IP and Domain Restrictions
      - □ URL Authorization
      - □ Windows Authentication
    - □ Application Development

Description

IP and Domain Restrictions allow you to enable or deny content based upon the originating IP address or domain name of the request. Instead of using groups, roles, or NTFS file system permissions to control access to content, you can specific IP addresses or domain names.

Step 7 Click **Next** as prompted. On the confirmation page, ensure that **IP and Domain Restrictions** is selected under **Web Server (IIS)**, as shown in **Figure 13-11**.

Figure 13-11 Confirmation page



Confirm installation selections

DESTINATION SERVER
WIN-J78KU2T8992

To install the following roles, role services, or features on selected server, click Install.

□ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

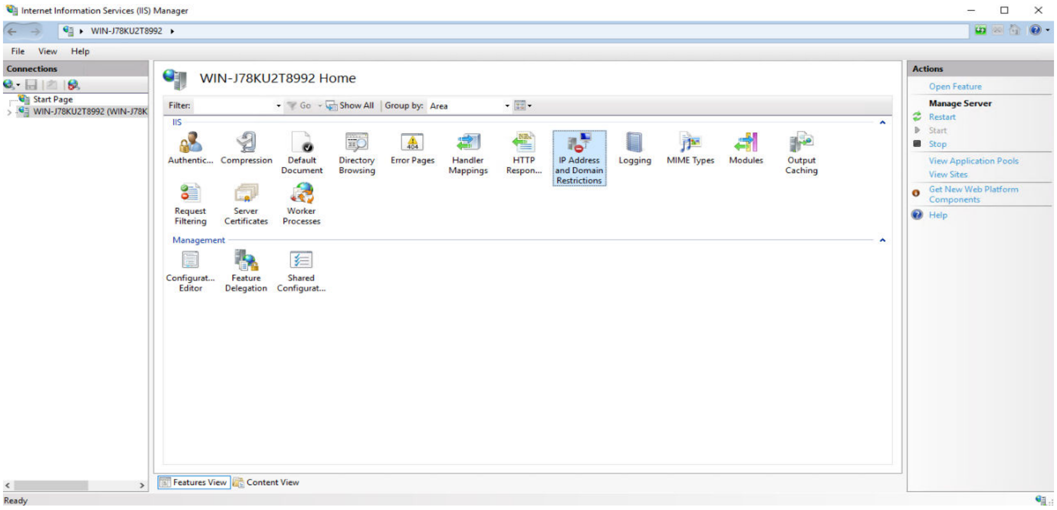
Web Server (IIS)
  Web Server
    Security
      IP and Domain Restrictions

Export configuration settings
Specify an alternate source path

Step 8 Click **Install**.

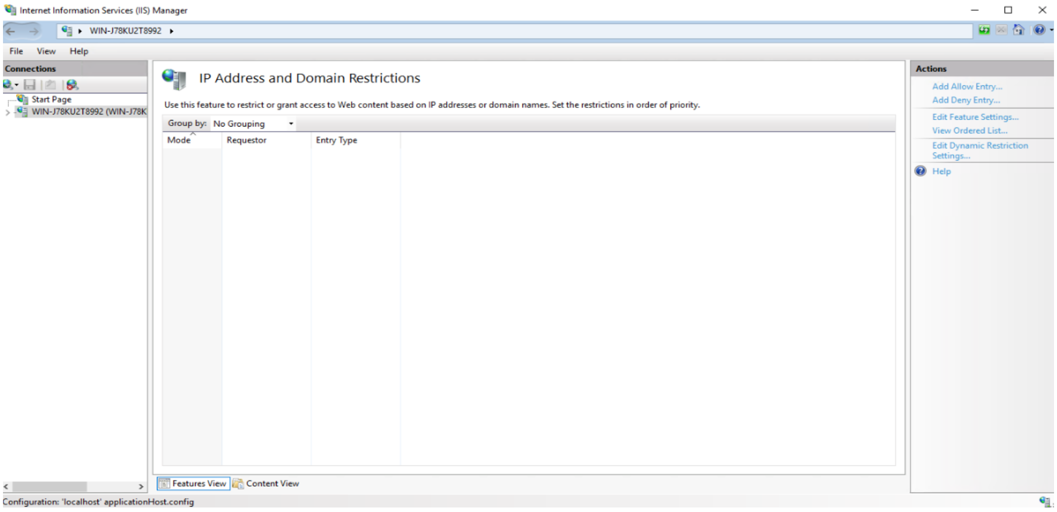
Step 9 Click ⊞ in the lower left corner of the ECS and choose **Administrative Tools** > **Internet Information Service (IIS) Manager**. The **Internet Information Service (IIS) Manager** page is displayed. Click the *host name*, as shown in **Figure 13-12**.

Figure 13-12 Host name home page



Step 10 Double-click **IP Address and Domain Restrictions** on the host name page. The **IP Address and Domain Restrictions** page is displayed, as shown in **Figure 13-13**.

Figure 13-13 IP address and domain restrictions

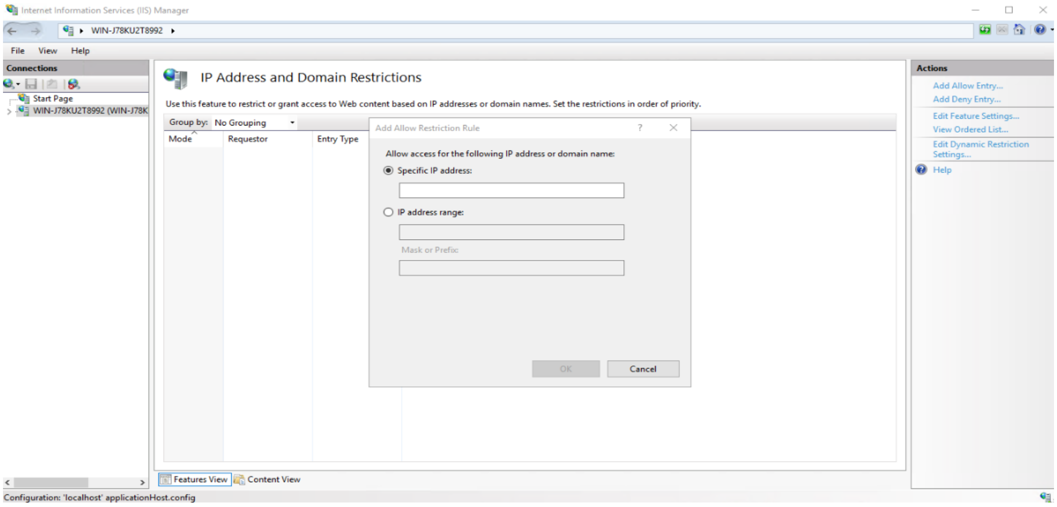


Use this feature to restrict or grant access to Web content based on IP addresses or domain names. Set the restrictions in order of priority.

Configuration: 'localhost' applicationHost.config

Step 11 In the upper right corner of the **IP Address and Domain Restrictions** page, click **Add Allow Restriction Rule** in the **Operation** column. The **Add Allow Restriction Rule** dialog box is displayed, as shown in **Figure 13-14**.

Figure 13-14 Adding allow restriction rules



IP Address and Domain Restrictions

Use this feature to restrict or grant access to Web content based on IP addresses or domain names. Set the restrictions in order of priority.

Add Allow Restriction Rule

Allow access for the following IP address or domain name:

● Specific IP address:

○ IP address range:

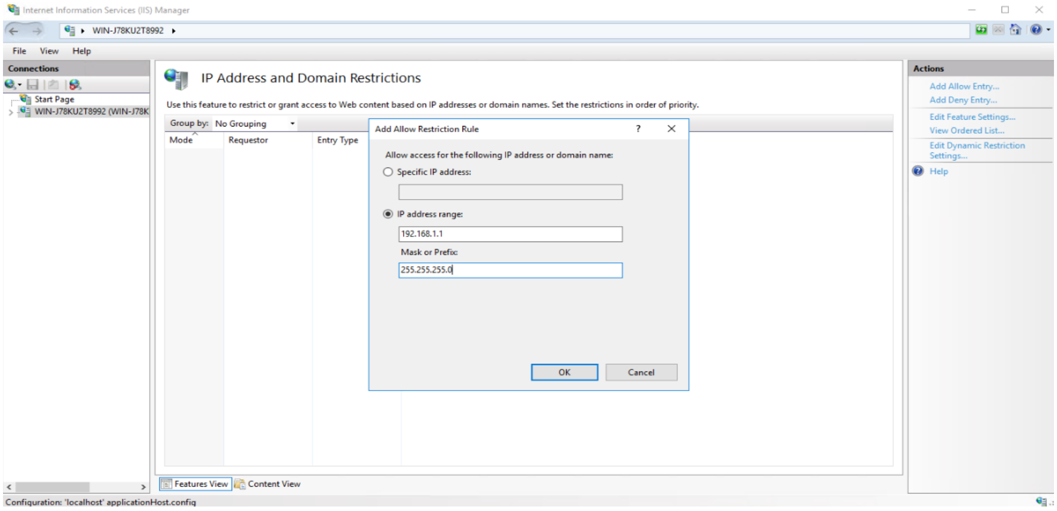
Mask or Prefix:

Configuration: 'localhost' applicationHost.config

Step 12 In the **Add Allow Restriction Rule** dialog box, select and configure **IP address range**, as shown in **Figure 13-15**.

- **IP address range**: IP address segment, for example, 192.168.1.1.
- **Mask or Prefix**: Set this parameter to the subnet mask, for example, 255.255.255.0.

Figure 13-15 Configuring restriction rules



IP Address and Domain Restrictions

Use this feature to restrict or grant access to Web content based on IP addresses or domain names. Set the restrictions in order of priority.

Add Allow Restriction Rule

Allow access for the following IP address or domain name:

○ Specific IP address:

● IP address range:

192.168.1.1

Mask or Prefix:

255.255.255.0

Configuration: 'localhost' applicationHost.config

NOTE

It is recommended that the IP address range be the same as the network segment of the subnet in **Workspace** > **Tenant Configuration**. If not, the cloud desktop may fail to access the file server.

Step 13 Click **OK**.

----End

13.2 Application Management

13.2.1 Obtaining Product Information

Scenarios

This section describes how to obtain product information (including the publisher name, product name, and process name) when creating a product information rule.

Procedure

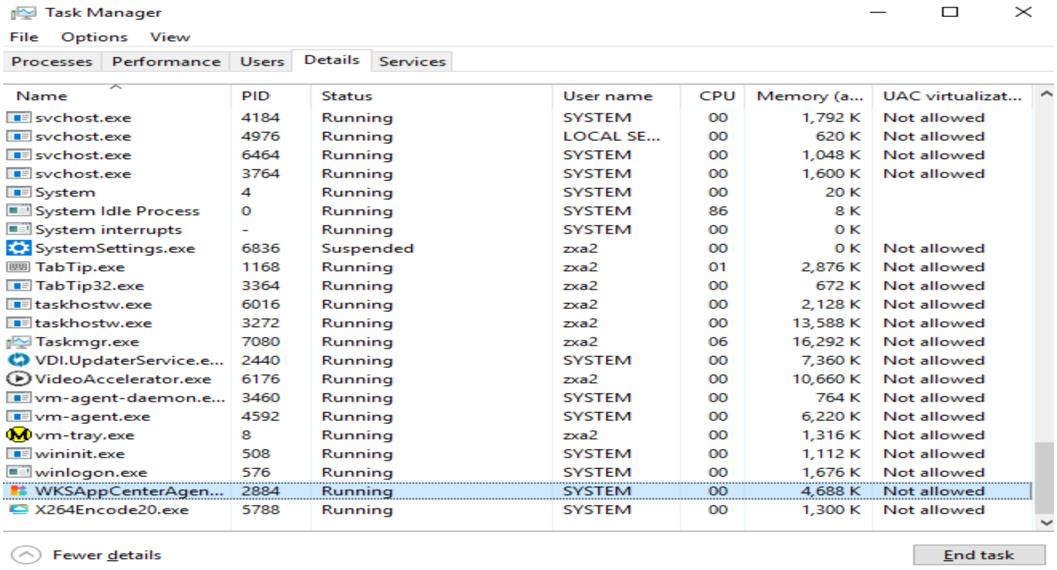
Obtaining the process name

Step 1 The administrator runs the application to be managed on the application server.

Step 2 Right-click ⊞, choose **Run**, run **taskmgr**, and press **Enter** to open the task manager.

Step 3 In the **Task Manager** window, click the **Details** tab and find the name of the application process to be managed, as shown in **Figure 13-16**.

Figure 13-16 Process name



Name	PID	Status	User name	CPU	Memory (a...	UAC virtualizat...
svchost.exe	4184	Running	SYSTEM	00	1,792 K	Not allowed
svchost.exe	4976	Running	LOCAL SE...	00	620 K	Not allowed
svchost.exe	6464	Running	SYSTEM	00	1,048 K	Not allowed
svchost.exe	3764	Running	SYSTEM	00	1,600 K	Not allowed
System	4	Running	SYSTEM	00	20 K	
System Idle Process	0	Running	SYSTEM	86	8 K	
System interrupts	-	Running	SYSTEM	00	0 K	
SystemSettings.exe	6836	Suspended	zxa2	00	0 K	Not allowed
TabTip.exe	1168	Running	zxa2	01	2,876 K	Not allowed
TabTip32.exe	3364	Running	zxa2	00	672 K	Not allowed
taskhostw.exe	6016	Running	zxa2	00	2,128 K	Not allowed
taskhostw.exe	3272	Running	zxa2	00	13,588 K	Not allowed
Taskmgr.exe	7080	Running	zxa2	06	16,292 K	Not allowed
VDI.UpdaterService.e...	2440	Running	SYSTEM	00	7,360 K	Not allowed
VideoAccelerator.exe	6176	Running	zxa2	00	10,660 K	Not allowed
vm-agent-daemon.e...	3460	Running	SYSTEM	00	764 K	Not allowed
vm-agent.exe	4592	Running	SYSTEM	00	6,220 K	Not allowed
vm-tray.exe	8	Running	zxa2	00	1,316 K	Not allowed
wininit.exe	508	Running	SYSTEM	00	1,112 K	Not allowed
winlogon.exe	576	Running	SYSTEM	00	1,676 K	Not allowed
WKSAppCenterAgen...	2884	Running	SYSTEM	00	4,688 K	Not allowed
X264Encode20.exe	5788	Running	SYSTEM	00	1,300 K	Not allowed

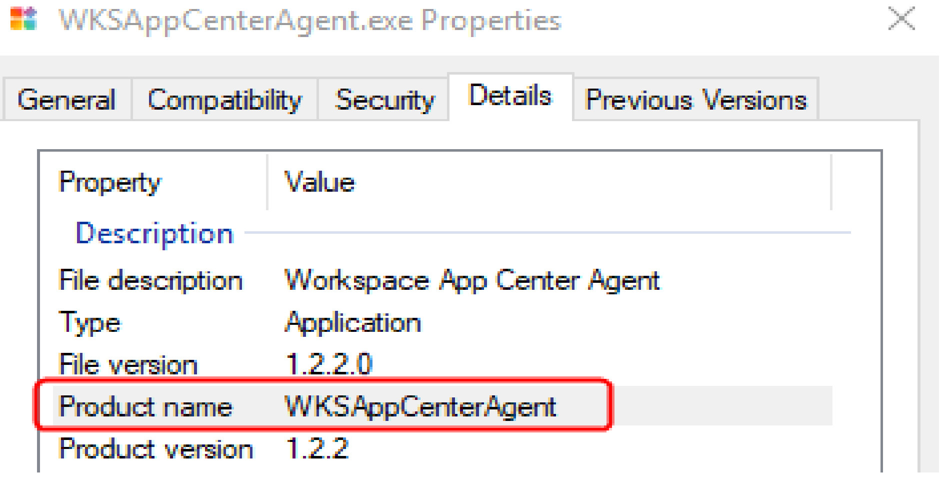
Obtaining the product name

Step 4 The administrator accesses the installation location of the application to be managed on the application server.

Step 5 Right-click the program, for example, *xxx.exe*. Choose **Properties** from the shortcut menu. The ***Application*** **Properties** page is displayed.

Step 6 Click the **Details** tab to view the product name, as shown in **Figure 13-17**.

Figure 13-17 Product name



WKSAppCenterAgent.exe Properties

Property	Value
Description	
File description	Workspace App Center Agent
Type	Application
File version	1.2.2.0
Product name	WKSAppCenterAgent
Product version	1.2.2

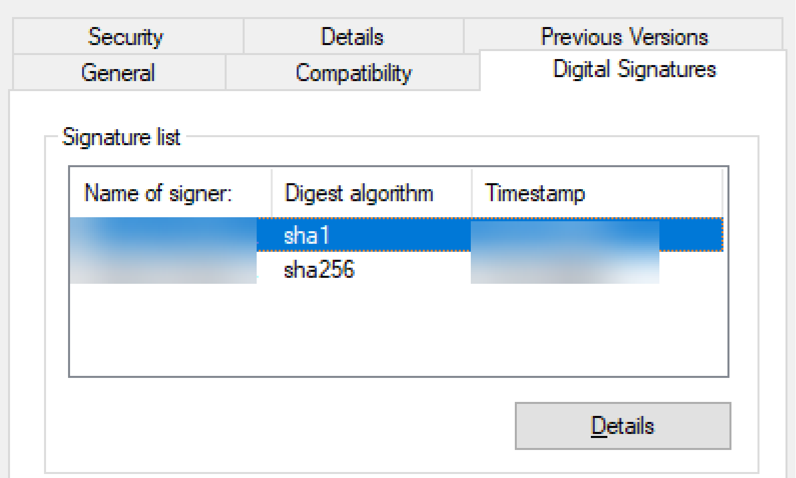
Obtaining the publisher name

Step 7 The administrator accesses the installation location of the application to be managed on the application server.

Step 8 Right-click the program, for example, *xxx.exe*. Choose **Properties** from the shortcut menu. The ***Application* Properties** page is displayed.

Step 9 Click **Digital Signatures**, select a signature from the signature list, and click **Details**, as shown in **Figure 13-18**.

Figure 13-18 Digital signature

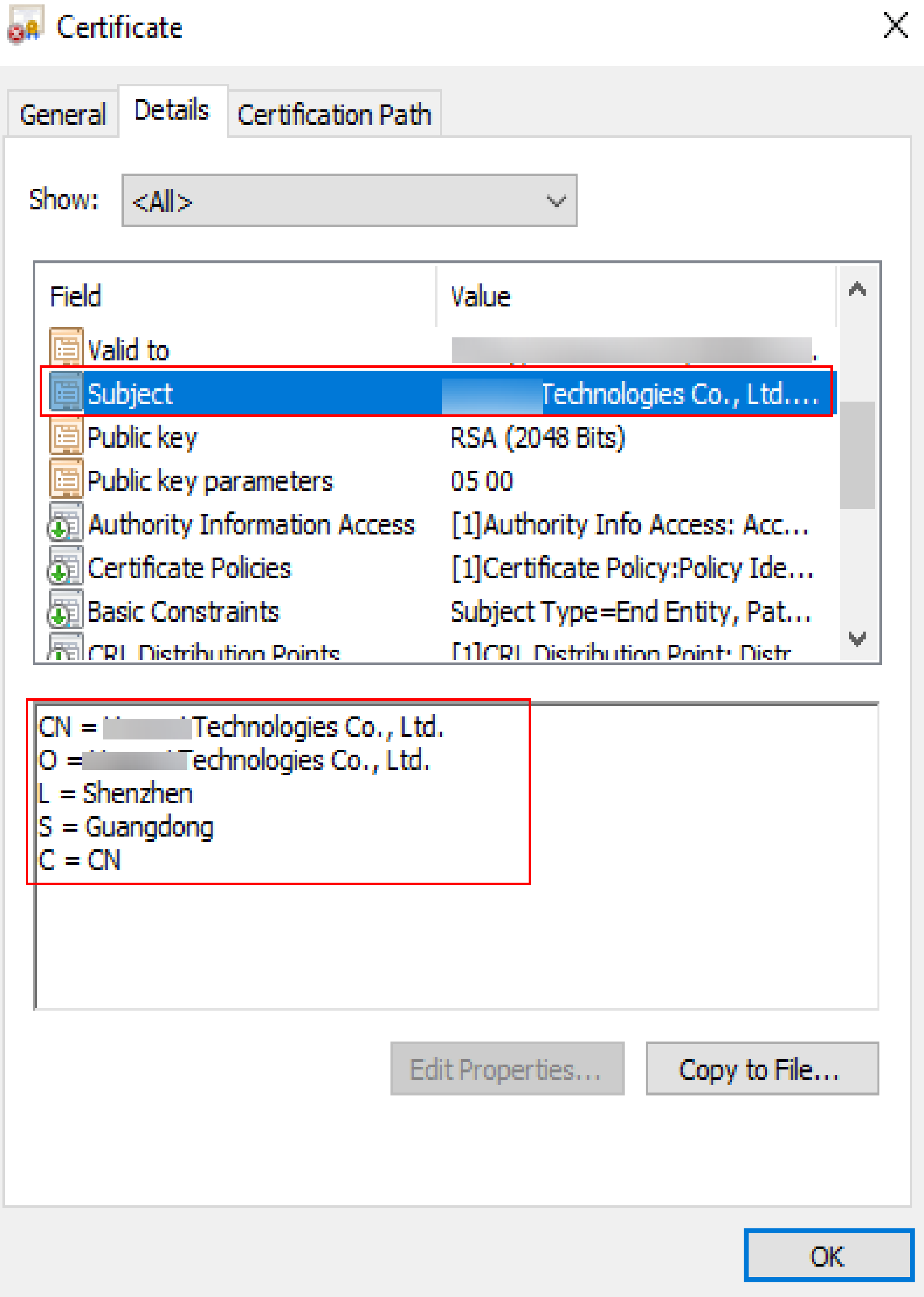


Name of signer:	Digest algorithm	Timestamp
	sha1	
	sha256	

Step 10 On the displayed page of digital signature details, click **View Certificate** to go to the **Certificate** page.

Step 11 On the **Certificate** page, click **Details**. On the displayed page, the value of the field **Subject** is the publisher name, as shown in **Figure 13-19**.

Figure 13-19 Subject information



Certificate

General | Details | Certification Path

Show: <All>

Field	Value
Valid to	[redacted]
Subject	[redacted] Technologies Co., Ltd....
Public key	RSA (2048 Bits)
Public key parameters	05 00
Authority Information Access	[1]Authority Info Access: Acc...
Certificate Policies	[1]Certificate Policy:Policy Ide...
Basic Constraints	Subject Type=End Entity, Pat...
CRL Distribution Points	[1]CRL Distribution Point: Distr

CN = [redacted] Technologies Co., Ltd.
O = [redacted] Technologies Co., Ltd.
L = Shenzhen
S = Guangdong
C = CN

----End

13.2.2 Application Rule Management

Scenarios

You can create application rules on the Workspace console for rule-based application management.

Procedure

Step 1 Log in to the console.

Step 2 In the navigation pane, choose **App Center** > **App Management**.

The **App Management** page is displayed.

Creating a path rule

Step 3 On the **App Rule Library** page, click **Create Path Rule** to go to the **Create Path Rule** page.

- **Rule Name**: The name can contain 1 to 64 characters (spaces included), but cannot be space-only.
- **Rule Description**: Enter 0 to 128 characters (spaces included) but do not enter only spaces.
- **Rule Path**: Enter a complete application installation directory, for example, C \App Center\App Management\Browser.

Step 4 Click **OK**.

Creating a product information rule

Step 5 On the **App Rule Library** page, click **Create Product Information Rule** to go to the **Create Product Information Rule** page.

- **Rule Name**: The name can contain 1 to 64 characters (spaces included), but cannot be space-only.
- **Rule Description**: Enter 0 to 128 characters (spaces included) but do not enter only spaces.
- **Identified By** (For details about how to obtain product information, see 13.2.1 Obtaining Product Information.)
  - **Process name**: name of an application process
  - **Product name**: name of a service product
  - **Publisher name**: name of an application publisher

NOTE

***** indicates full match. If all identification conditions are *****, the rule cannot be created.

Step 6 Click **OK**.

Editing a path rule

Step 7 Click **Edit** in the **Operation** column of the desired path rule to go to the **Modify Path Rule** page.

Step 8 You can modify the rule name, rule description, and rule path.

Step 9 Click **OK**.

Editing a product information rule

Step 10 Click **Edit** in the **Operation** column of the desired product information rule to go to the **Modify Product Information Rule** page.

Step 11 You can modify the rule name, rule description, and identification conditions.

Step 12 Click **OK**.

Deleting a rule

Step 13 Select the **App Rule Library** tab.

Step 14 Delete created rules as required.

- Deletion of a single application rule:
  a. Click **Delete** in the **Operation** column of the desired application rule to go to the **Delete Application Rule** page.
  b. Enter **DELETE** or click **Auto Enter** to quickly enter the value. Click **OK**.
- Batch deletion:
  a. Select the application rules to delete in batches and click **Batch Delete** to go to the **Delete Application Rule** page.
  b. Enter **DELETE** or click **Auto Enter** to quickly enter the value. Click **OK**.

----End

13.2.3 Application Management Configuration

Scenarios

You can configure tenant application management rules on the Workspace console to manage applications in a unified manner.

NOTE

- Before using application management, you need to contact O&M personnel to check whether the basic components of your desktops have been upgraded to a version that supports application management.
- HDA version: Only 25.1.0 and later versions are supported.
- This operation can be performed only on Windows desktops.

Procedure

Adding an application rule

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

Step 2 In the navigation pane, choose **App Center** > **App Management**.

The **App Management** page is displayed.

Step 3 On the top navigation bar, click **App Management**.

Step 4 Click **Add App Rule** to go to the **Add App Rule** page.

Step 5 Search for and select the application rule to be added by rule name, and click **OK**.

----End

Delete an application rule

Step 1 On the top navigation bar, click **App Management**.

Step 2 Delete added application rules as required.

- Deletion of a single application rule:
  a. Click **Delete** in the **Operation** column of the desired application rule to go to the **Delete Application Rule** page.
  b. Enter **DELETE** or click **Auto Enter** to quickly enter the value. Click **OK**.
- Batch deletion:
  a. Select the application rules to delete in batches and click **Batch Delete** to go to the **Delete Application Rule** page.
  b. Enter **DELETE** or click **Auto Enter** to quickly enter the value. Click **OK**.

----End

Modifying application management configuration

Step 1 Click **Modify Configuration** on the right of the **App Management** tab to go to the page for modifying application management configuration.

- **App Management**: After enabling this function, you can determine whether to enable periodic monitoring.
  - : application management disabled
  - : application management enabled

  NOTE

  Blacklist policy rules:
  1. When a desktop user opens a blacklisted application, the application is forbidden to run.
  2. The policy cannot take effect on running processes.
  3. The policy takes effect in five to ten minutes.
  4. Periodic monitoring and force application killing are supported only for HDA 25.1.0 or later.
- **App Management Mode**: **Do not run apps in the list**
- **Periodic Monitoring**: This parameter is available only after **App Management** is enabled. You can determine whether to enable this parameter (disabled by default).
  - : periodic monitoring disabled
  - : periodic monitoring enabled
  - **Monitoring Period (min)**: This parameter is available only after you enable **App Management** and **Periodic Monitoring**. The monitoring period ranges from 5 minutes (default) to 60 minutes.
  - **Force Application Killing**: This parameter is available only after you enable **App Management** and **Periodic Monitoring**. You can determine whether to enable this parameter (enabled by default).
    - : disabled
    - : enabled

----End

13.2.4 Monitoring Events of Application Management

- An application may start earlier than the application management agent, or bypass monitoring when the application management agent is killed. To minimize the impact, you can configure an alarm rule and view alarm records on Cloud Eye to get real-time notifications of monitoring events. For details, see **10.1 Alarms**.
- **Table 13-4** describes the monitoring events of application management.

Table 13-4 Monitoring events

Event Source	Dimension (Mandatory for Specified Resources)	Event ID	Event Name	Event Severity	Event Description	Handling Suggestion	Event Impact
Workspace	-	agentAbnormal	Abnormal agent process	Major	The agent process has been killed or reset.	The agent process can be automatically restarted after being killed.	Functions such as application management and upgrade will be affected.
Workspace	-	appRestrictFailed	Bypassing controlled applications	Major	The application management agent is continuously killed.	Check whether a script is used to continuously kill the application management agent.	Application management failed.

📖 NOTE

For alarm policy configuration, the events **Bypassing controlled applications** and **Abnormal agent process** are available only for HDA 25.1.0 or later.

14 Private Images

14.1 Creating a Windows Private Image

14.1.1 Required Software

Table 14-1 lists the software packages required for creating a Windows private image.

NOTE

Check the integrity of downloaded installation packages during Windows image creation, that is, check whether the packages are tampered with or lost during download. For details, see .

Table 14-1 Required software packages

Name	Description	How to Obtain
Workspace_HDP_WindowsDesktop_Installer_x.x.x.iso	Windows image creation tool	Contact technical support engineers.

Name	Description	How to Obtain
ISO file	● Windows 10 64-bit (Chinese and English) ● Windows Server 2016 Standard 64-bit (Chinese and English) ● Windows Server 2019 Standard 64-bit (Chinese and English)	Obtain ISO files from Microsoft or other legal channels. **NOTICE** The ISO file must be an official pure image obtained from an official channel. Do not use non-official images or customized private images. These images have many unknown modifications of the OS and can lead to failed template creation or incompatibility with HDP.
AnyBurn	CD/DVD-ROM drive creation tool	Contact technical support engineers.
VirtIO driver package	VirtIO driver	**Click here** to download the required driver package (**virtio-win.iso** of the latest version is recommended) from the VirtIO official website.
Applications	Prepare application software as required, such as office and real-time communication software.	Prepared by users
7z1900-x64.exe	7-Zip compression software, which is used to compress or decompress software packages	Contact technical support engineers.
VC_redist.x64.exe	Visual Studio 2017 runtime library, which is used to install the basic library for running desktop applications	Contact technical support engineers.
VC_redist.x86.exe		

Name	Description	How to Obtain
CloudbaseInitSetup_*xxx*.msi	An ECS initialization tool used to configure usernames, passwords, and the **hostname** and **hosts** files of ECSs to be created using images	Contact technical support engineers.
Peripheral driver	Prepare the peripheral drivers as required.	Prepared by users
HW.SysAgent.Installer_64.msi HW.SysPrep.Installer_64.msi	Used for desktop provisioning and HDA upgrade. Double-click to install.	Contact technical support engineers.
WKSAppCenterAgent.msi WKSAppCenter.msi	Needs to be installed when Workspace uses the application center. Double-click to install.	Contact technical support engineers.

14.1.2 Registering a Private Image Using an ISO File

Scenarios

This section describes how to create a Windows private image.

Prerequisites

- You have obtained the username and password for logging in to the console.
- You have prepared the OS ISO file. For details, see **Table 14-1**.

  NOTE

  The name of the ISO image file can contain only letters, digits, hyphens (-), and underscores (_). If the name does not meet the requirements, change it.

Procedure

Integrating the VirtIO driver into an ISO File using AnyBurn

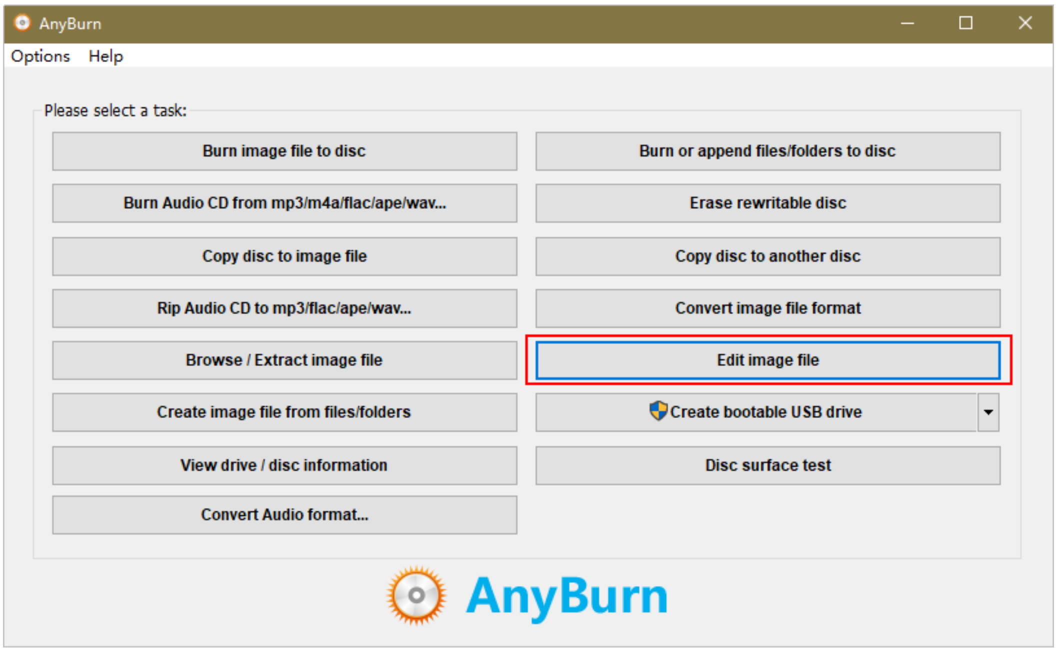
Step 1 Install AnyBurn on the local PC.

Step 2 Download the VirtIO driver package and decompress it to your local PC.

Step 3 Use AnyBurn to open the ISO file.

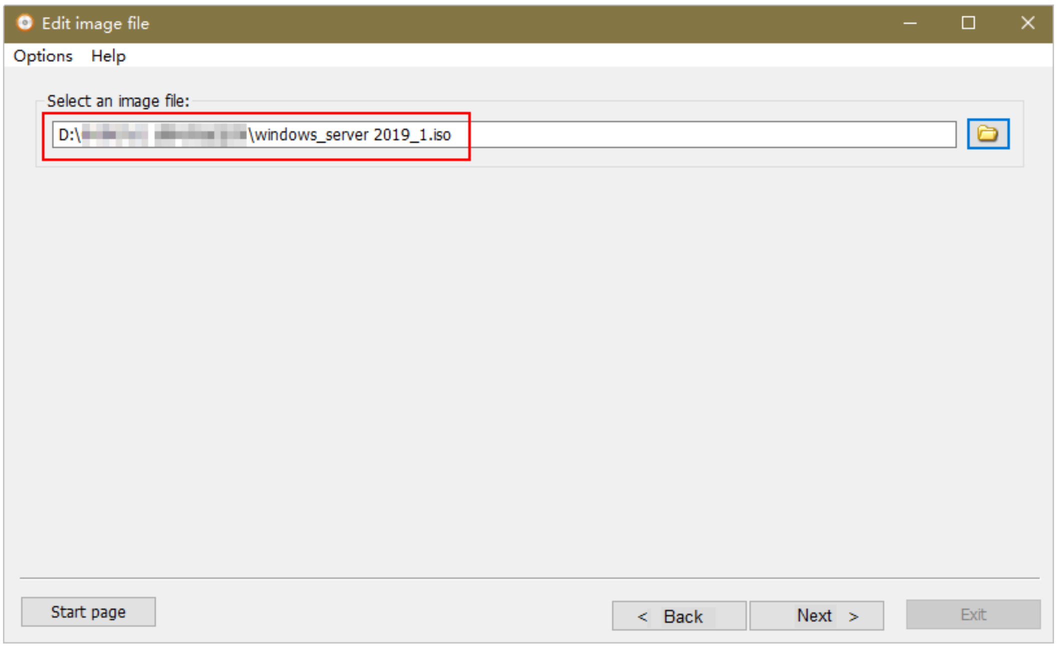
Open the AnyBurn software and select **Edit Image File**, as shown in **Figure 14-1**.

Figure 14-1 Editing an image file


AnyBurn
Options Help
Please select a task:
Burn image file to disc
Burn or append files/folders to disc
Burn Audio CD from mp3/m4a/flac/ape/wav...
Erase rewritable disc
Copy disc to image file
Copy disc to another disc
Rip Audio CD to mp3/flac/ape/wav...
Convert image file format
Browse / Extract image file
Edit image file
Create image file from files/folders
Create bootable USB drive
View drive / disc information
Disc surface test
Convert Audio format...
AnyBurn

Select the ISO file and click **Next**, as shown in **Figure 14-2**.

Figure 14-2 Selecting the ISO file



Select an image file:

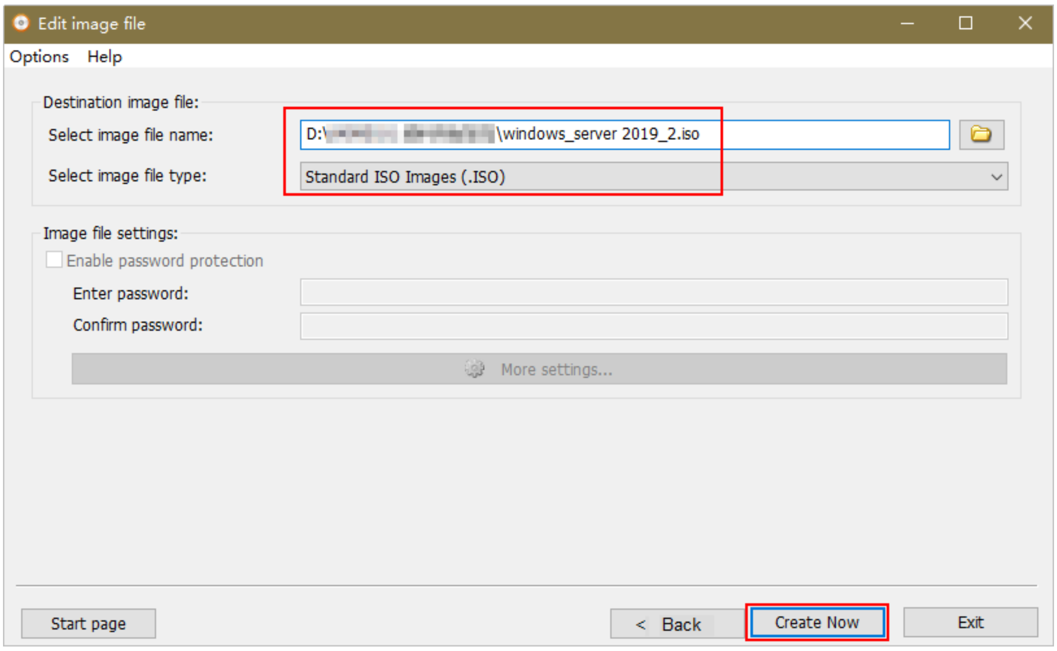
D:\[redacted]\windows_server 2019_1.iso

Step 4 Edit the ISO file to integrate the VirtIO driver.

1. Decompress the **virtio-win.iso** file downloaded in 2.
2. Click **Add** to add all the decompressed files to the parent node of the ISO file, and click **Next**.
3. Specify the path for saving the file and the ISO file name, select the ISO format, and click **Create Now**.

After the ISO file is generated, view the ISO file integrated with the VirtIO driver, as shown in **Figure 14-3**.

Figure 14-3 Viewing the ISO file integrated with the VirtIO driver



Destination image file:

Select image file name: D:\[redacted]\windows_server 2019_2.iso

Select image file type: Standard ISO Images (.ISO)

Image file settings:

☐ Enable password protection

Enter password:

Confirm password:

More settings...

Registering a private image

Step 5 Log in to the Huawei Cloud management console.

Step 6 Upload an image file.

You are advised to use OBS Browser+ to upload external image files to an OBS bucket. For details, see **OBS Browser+ Best Practices**.

For details about how to download, install, and log in to OBS Browser+, see section "Tools Guide" > "OBS Browser+" in **OBS User Guide**.

NOTE

- If no OBS bucket is available, create one by referring to section "Getting Started" in **OBS User Guide**.
- The bucket file and the image to be registered must belong to the same region.
- Only unencrypted external image files or those encrypted using SSE-KMS can be uploaded to the OBS bucket.
- The storage class of the OBS bucket must be **Standard**.

Step 7 Click **Service List**. Under **Compute**, click **Image Management Service**.

The IMS console is displayed.

Step 8 Click **Create Image** in the upper right corner of the page.

Step 9 In the **Image Type and Source** area, select **Import Image** for **Type** and **ISO image** for **Image Type**.

Step 10 In the image file list, select the bucket in **Step 6** and then the image file.

Step 11 In the **Image Information** area, configure basic information about the image according to **Table 14-2**. Retain the default values for the parameters that are not listed below.

Table 14-2 Image parameters

Parameter	Parameters
Architecture	Select **x86**.
Boot Mode	Select **BIOS**.
OS	Configure this parameter based on the OS version, for example, Windows Server 2016 Standard 64bit.
System Disk (GiB)	Configure this parameter based on the OS requirements, for example, 40 GiB.
Name	Enter the image name, for example, **Windows***XXX*-**Template_ISO**.
Enterprise Project	Select the enterprise project to which the resource belongs, for example, **default**.

Step 12 Click **Create Now**.

Step 13 Confirm the image parameters, select **I have read and agree to the Image Disclaimer**, and click **Submit**.

Step 14 Return to the private image list to view the image status.

When the image status becomes **Normal**, the image has been created.

----End

14.1.3 Creating an ECS

Scenarios

This section describes how to create an ECS for subsequent ECS configuration and image creation.

Prerequisites

- You have obtained the username and password for logging in to the console.
- You have registered a private image using an ISO file. See **14.1.2 Registering a Private Image Using an ISO File**.

Procedure

Creating an ECS

Step 1 Log in to the console.

Step 2 Click **Service List**. Under **Compute**, click **Image Management Service**.

The IMS console is displayed.

Step 3 Click **Apply for Server** in the **Operation** column of the private image created in **14.1.2 Registering a Private Image Using an ISO File**.

Step 4 On the displayed page, configure the parameters in **Table 14-3** and retain the default values for other parameters.

Table 14-3 Cloud server parameters

Parameter	Description	Example Value
Specifications	Select the planned ECS flavor, for example, **s6.xlarge.2**.	s6.xlarge.2
VPC	Select the planned VPC.	fa_vpc
Subnet	Select the planned subnet.	subnet-fa
ECS Name	The value can be customized.	WKS-desktop_temp
Enterprise Project	Select an enterprise project.	default

Step 5 Click **OK**.

After the request is successful, the created ECS is displayed in the ECS list on the ECS console.

Configuring a security group policy

Step 6 In the **Service List**, choose **Networking** > **Virtual Private Cloud**.

Step 7 In the navigation pane on the left, choose **Access Control** > **Security Groups**.

Step 8 In the upper right corner of the **Security Groups** page, click **Create Security Group**.

The page for creating a security group is displayed.

Step 9 Configure the parameters of a security group, as shown in **Table 14-4**.

Table 14-4 Security group configuration

Parameter	Description	Example Value
Name	The value can be customized.	-

Parameter	Description	Example Value
Enterprise Project	Use the enterprise project selected in **Step 4**. **NOTE** This parameter is mandatory when the enterprise project function is enabled.	default
Template	● **General-purpose web server**: allows all inbound ICMP traffic and inbound traffic on ports **22**, **80**, **443**, and **3389**. This template type applies to cloud servers for remote login, public network ping, and website services. ● **All ports open**: The security group that you create using this template includes default rules that allow inbound traffic on all ports. Note that allowing inbound traffic on all ports poses security risks. ● **Customization**: Users can configure this parameter as required.	-

Step 10 Locate the row that contains the security group created in **Step 9**, and click **Configure Rule**. On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, set **Protocol & Port**, as shown in **Table 14-5**.

Table 14-5 Security group rules

Protocol & Port	Type	Source IP
Choose **Protocols** > **All**.	IPv4	Select **IP Address**, and enter **0.0.0.0/0**.

Step 11 Locate the row that contains the security group created in **Step 9**, and click **Manage Instance**.

Step 12 On the **Associated Instances** page, click **Add** on the **Servers** tab.

Step 13 Select **ECS**, select the ECS created in **Step 4**, and click **OK**.

----End

14.1.4 Configuring an ECS

Scenarios

This section describes how to install application software, configure patch update, and install system patches on an ECS.

Prerequisites

- You have obtained the username and password for logging in to the ECS.
- You have **created an ECS**.
- You have obtained the files listed in **14.1.1 Required Software** and decompressed **Workspace_HDP_WindowsDesktop_Installer_*x.x.x*.iso** to obtain the folder **Workspace_HDP_WindowsDesktop_Installer_*x.x.x***.

Procedure

NOTE

- The operations vary depending on the OS. Follow the instructions on the GUI.
- In Windows, the user directory is the system disk by default, for example, C:\Users\Username. To ensure successful login to the desktop created using an image, do not change the storage location of the user directory.

Installing a Windows OS and the VirtIO driver

Step 1 Log in to the console.

Step 2 Choose **Compute** > **Elastic Cloud Server** under **All Services**.

Step 3 Locate the row that contains the ECS created in **14.1.3 Creating an ECS**, and click **Remote Login** to log in to the Windows VM.

Step 4 For details, see **Installing a Windows OS and VirtIO Drivers**.

Activating the Administrator account for the VM

NOTE

Skip this operation if Windows Server 2016 or Windows Server 2019 is used.

Step 5 In the VM, right-click ⊞ in the lower left corner and choose **Run** from the shortcut menu.

Step 6 In the **Run** dialog box, enter **compmgmt.msc** and press **Enter**.

The **Computer Management** page is displayed.

Step 7 In the navigation pane on the left, choose **Computer Management (Local)** > **System Tools** > **Local Users and Groups**, and select **Users**.

Step 8 In the right pane, right-click **Administrator** and choose **Properties**.

The **Administrator Properties** window is displayed.

Step 9 On the **General** tab page, deselect **Account is disabled**, and click **OK**.

The **Administrator** account has been activated, and its default password is empty.

Step 10 Right-click **Administrator** and choose **Set Password**.

NOTICE

- Set a password for the **Administrator** account and ensure that the password is not empty. Otherwise, the task execution will fail.
- Password requirements:
  - Contains at least one uppercase letter (A–Z), one lowercase letter (a–z), one digit (0–9), and one special character (~!@#$%^&*()-_=+\|{};:'",<.>/? or space).
  - Contains 8 to 32 characters.
  - Cannot be the same as the recent three passwords.
  - Cannot contain the username or the username in reversed order.

Step 11 Click **Proceed**. The **Set Password for Administrator** dialog box is displayed.

Step 12 Set a password for the **Administrator** account, confirm the password, and click **OK**.

The password has been set.

Step 13 Click **OK**.

Step 14 Right-click ⊞ in the lower left corner and choose **Shut down or sign out** > **Sign out** from the shortcut menu to log out of the OS and log in to the ECS again using the **Administrator** account.

Step 15 On the **Choose privacy settings for your device** window, click **Accept**.

Manage Your Server page not displayed upon login

Step 16 On the ECS, right-click ⊞ in the lower left corner and choose **Run** from the shortcut menu.

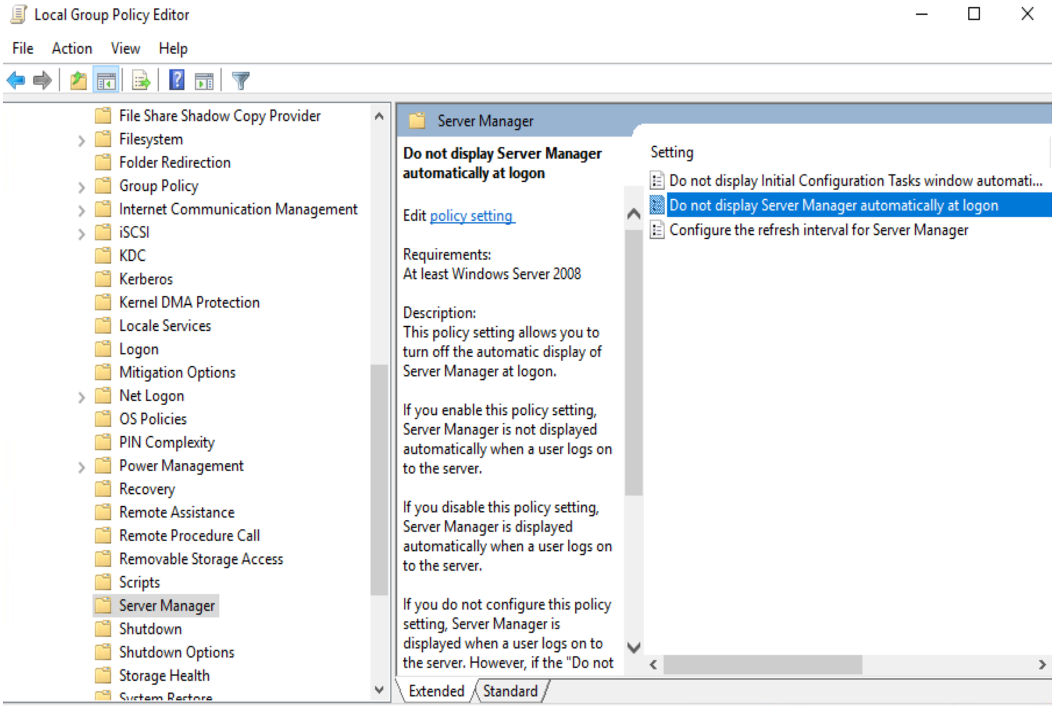
The **Run** dialog box is displayed.

Step 17 Enter **gpedit.msc** in the **Open** text box and press **Enter**.

The **Local Group Policy Editor** window is displayed.

Step 18 In the navigation pane, choose **Computer Configuration** > **Policy** > **Administrative Templates** > **System** > **Server Manager**, as shown in **Figure 14-4**.

Figure 14-4 Manage Your Server page not displayed upon login



Do not display Server Manager automatically at logon

Edit policy setting

Requirements:
At least Windows Server 2008

Description:
This policy setting allows you to turn off the automatic display of Server Manager at logon.

If you enable this policy setting, Server Manager is not displayed automatically when a user logs on to the server.

If you disable this policy setting, Server Manager is displayed automatically when a user logs on to the server.

If you do not configure this policy setting, Server Manager is displayed when a user logs on to the server. However, if the "Do not

Step 19 In the right pane, double-click **Do not display Server Manager automatically at logon**.

The **Do not display Server Manager automatically at logon** dialog box is displayed.

Step 20 Select **Enabled**.

Step 21 Click **OK**.

----End

Disabling hybrid sleep

Step 1 On the ECS, right-click ⊞ in the lower left corner and choose **Run** from the shortcut menu.

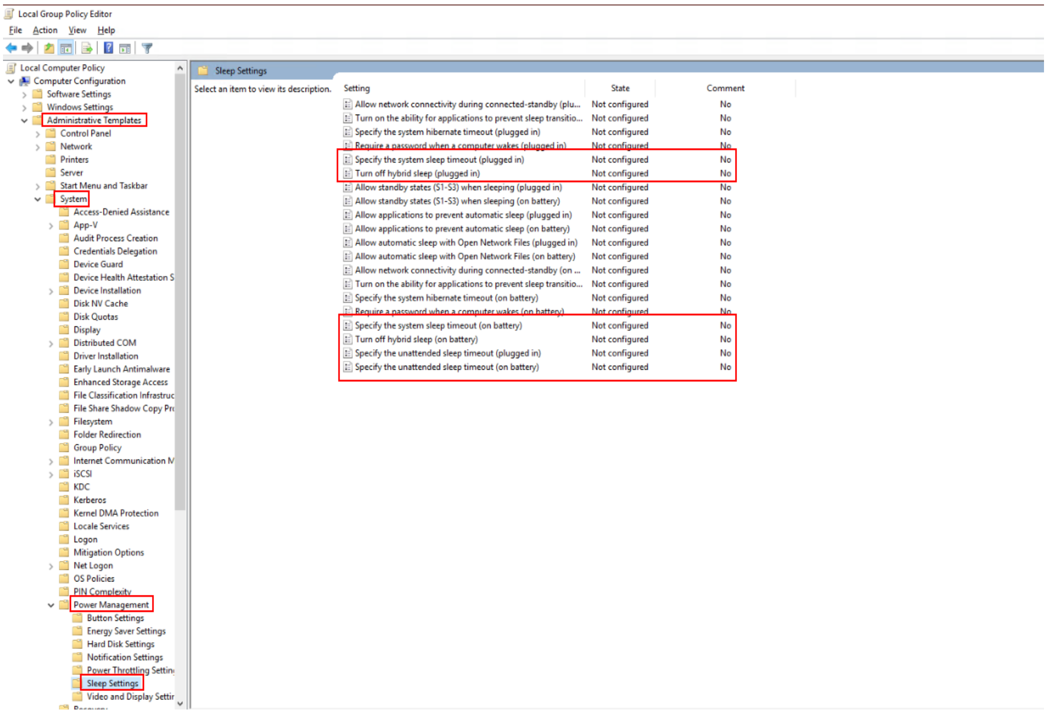
The **Run** dialog box is displayed.

Step 2 Enter **gpedit.msc** in the **Open** text box and press **Enter**.

The **Local Group Policy Editor** window is displayed.

Step 3 In the navigation pane, choose **Computer Configuration** > **Administrative Templates** > **System** > **Power Management** > **Sleep Settings**. Enable **Specify the system sleep timeout (plugged in)**, **Turn off hybrid sleep (plugged in)**, **Specify the system sleep timeout (on battery)**, **Turn off hybrid sleep (on battery)**, **Specify the unattended sleep timeout (plugged in)**, and **Specify the unattended sleep timeout (on battery)**, as shown in Figure 14-5.

Figure 14-5 Sleep settings

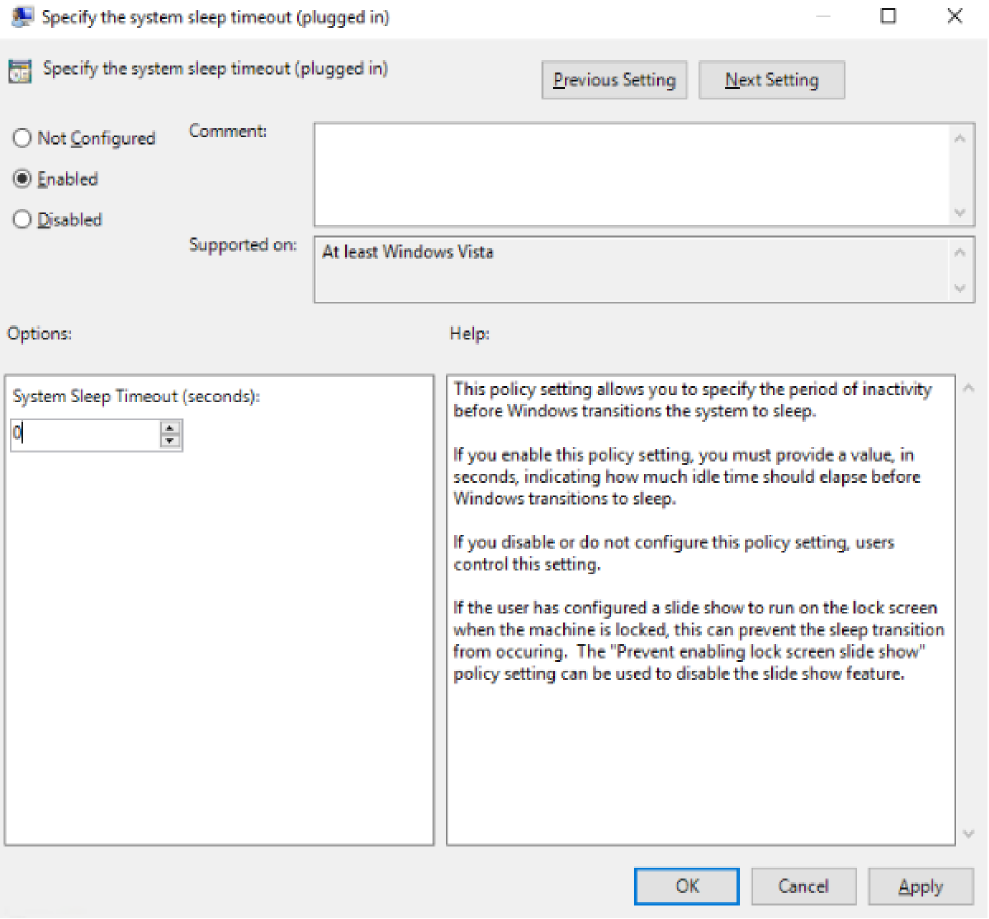


Select an item to view its description.

Setting	State	Comment
Allow network connectivity during connected-standby (plu...	Not configured	No
Turn on the ability for applications to prevent sleep transitio...	Not configured	No
Specify the system hibernate timeout (plugged in)	Not configured	No
Require a password when a computer wakes (plugged in)	Not configured	No
Specify the system sleep timeout (plugged in)	Not configured	No
Turn off hybrid sleep (plugged in)	Not configured	No
Allow standby states (S1-S3) when sleeping (plugged in)	Not configured	No
Allow standby states (S1-S3) when sleeping (on battery)	Not configured	No
Allow applications to prevent automatic sleep (plugged in)	Not configured	No
Allow applications to prevent automatic sleep (on battery)	Not configured	No
Allow automatic sleep with Open Network Files (plugged in)	Not configured	No
Allow automatic sleep with Open Network Files (on battery)	Not configured	No
Allow network connectivity during connected-standby (on ...	Not configured	No
Turn on the ability for applications to prevent sleep transitio...	Not configured	No
Specify the system hibernate timeout (on battery)	Not configured	No
Require a password when a computer wakes (on battery)	Not configured	No
Specify the system sleep timeout (on battery)	Not configured	No
Turn off hybrid sleep (on battery)	Not configured	No
Specify the unattended sleep timeout (plugged in)	Not configured	No
Specify the unattended sleep timeout (on battery)	Not configured	No

Step 4 Double-click **Specify the system sleep timeout (plugged in)**. In the displayed dialog box, select **Enabled** and set **System Sleep Timeout (seconds)** to **0**.

Figure 14-6 Specifying the system sleep timeout (plugged in)



Specify the system sleep timeout (plugged in)

Specify the system sleep timeout (plugged in)

Previous Setting | Next Setting

○ Not Configured

● Enabled

○ Disabled

Comment:

Supported on: At least Windows Vista

Options:

Help:

System Sleep Timeout (seconds): 0

This policy setting allows you to specify the period of inactivity before Windows transitions the system to sleep.

If you enable this policy setting, you must provide a value, in seconds, indicating how much idle time should elapse before Windows transitions to sleep.

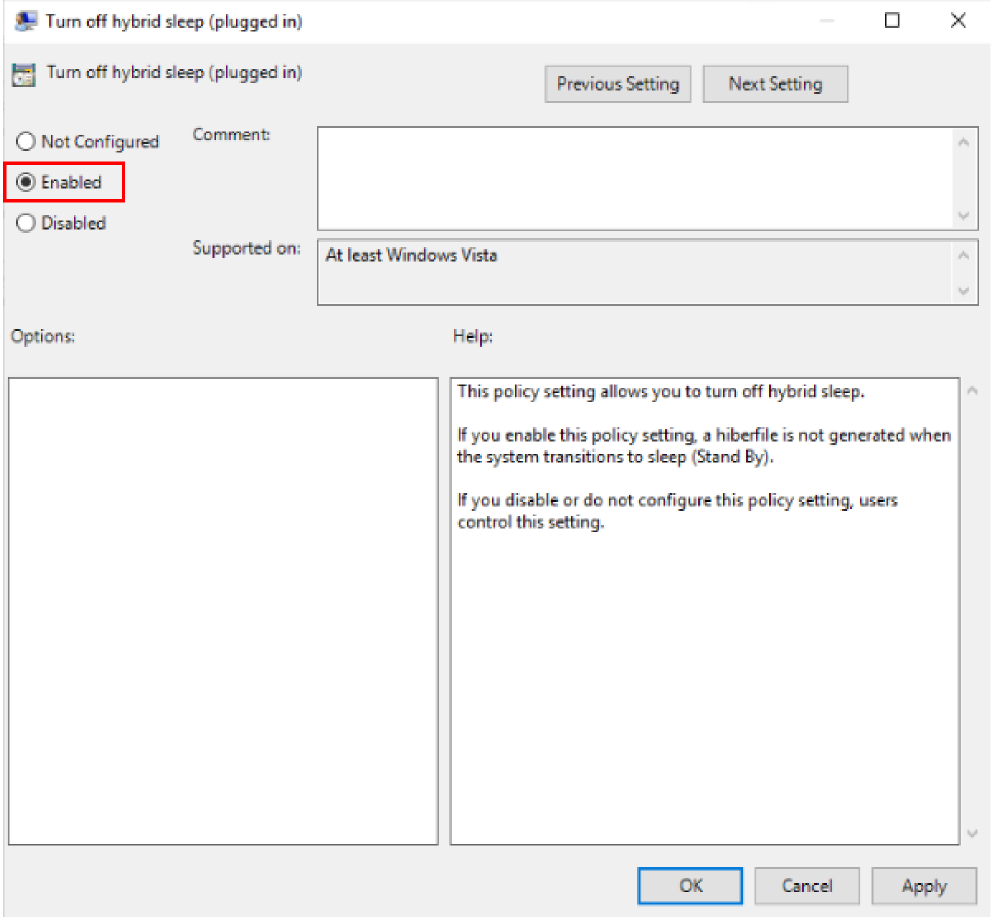
If you disable or do not configure this policy setting, users control this setting.

If the user has configured a slide show to run on the lock screen when the machine is locked, this can prevent the sleep transition from occuring. The "Prevent enabling lock screen slide show" policy setting can be used to disable the slide show feature.

Step 5 Click **OK**.

Step 6 Double-click **Turn off hybrid sleep (plugged in)**. In the displayed dialog box, select **Enabled**.

Figure 14-7 Turning off hybrid sleep (plugged in)



○ Not Configured
● Enabled
○ Disabled

Supported on: At least Windows Vista

This policy setting allows you to turn off hybrid sleep.

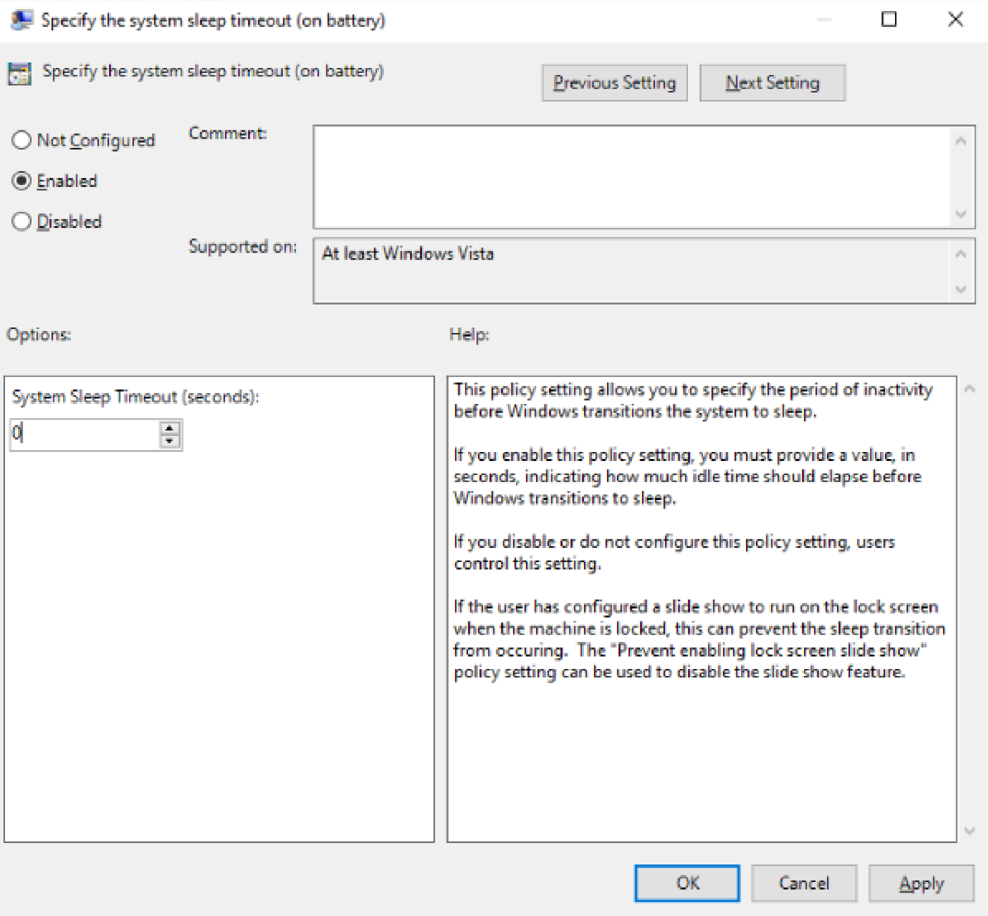
If you enable this policy setting, a hiberfile is not generated when the system transitions to sleep (Stand By).

If you disable or do not configure this policy setting, users control this setting.

Step 7 Click **OK**.

Step 8 Double-click **Specify the system sleep timeout (on battery)**. In the displayed dialog box, select **Enabled** and set **System Sleep Timeout (seconds)** to **0**.

Figure 14-8 Specifying the system sleep timeout (on battery)



Specify the system sleep timeout (on battery)

Specify the system sleep timeout (on battery)

○ Not Configured

● Enabled

○ Disabled

Comment:

Supported on: At least Windows Vista

Options:

System Sleep Timeout (seconds): 0

Help:

This policy setting allows you to specify the period of inactivity before Windows transitions the system to sleep.

If you enable this policy setting, you must provide a value, in seconds, indicating how much idle time should elapse before Windows transitions to sleep.

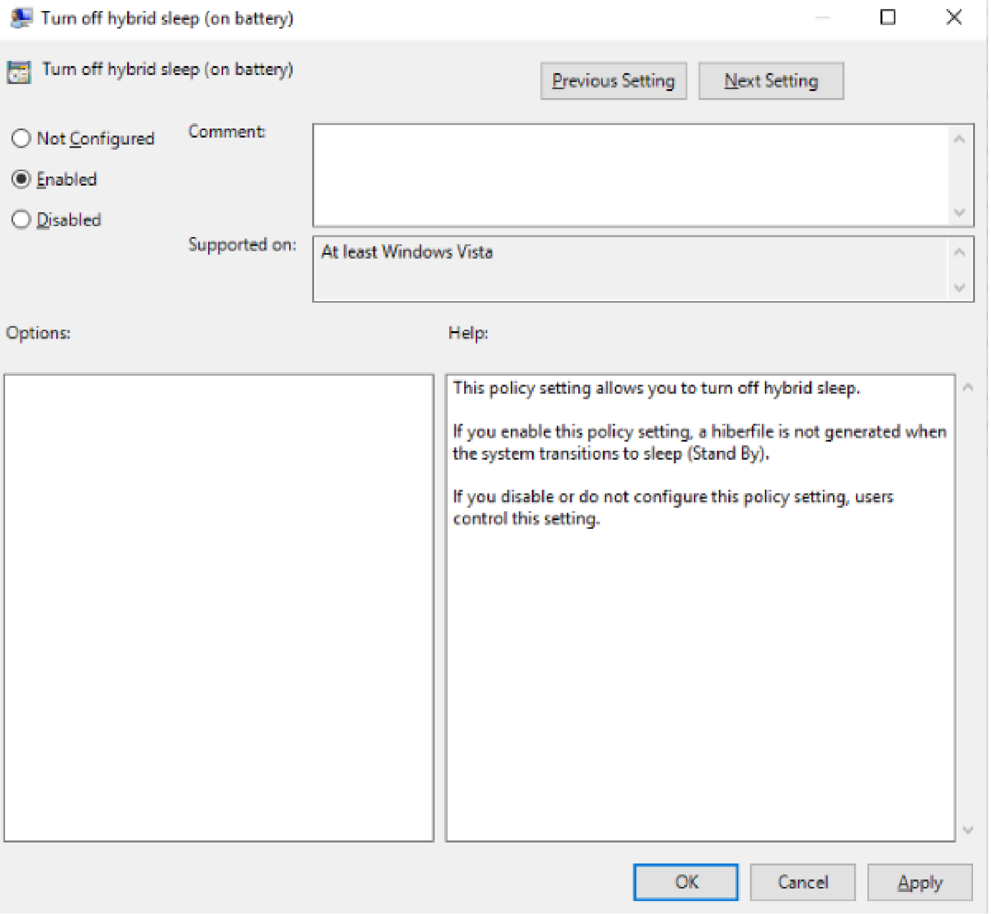
If you disable or do not configure this policy setting, users control this setting.

If the user has configured a slide show to run on the lock screen when the machine is locked, this can prevent the sleep transition from occuring. The "Prevent enabling lock screen slide show" policy setting can be used to disable the slide show feature.

Step 9 Click **OK**.

Step 10 Double-click **Turn off hybrid sleep (on battery)**. In the displayed dialog box, select **Enabled**.

Figure 14-9 Turning off hybrid sleep (on battery)



○ Not Configured

● Enabled

○ Disabled

Supported on: At least Windows Vista

This policy setting allows you to turn off hybrid sleep.

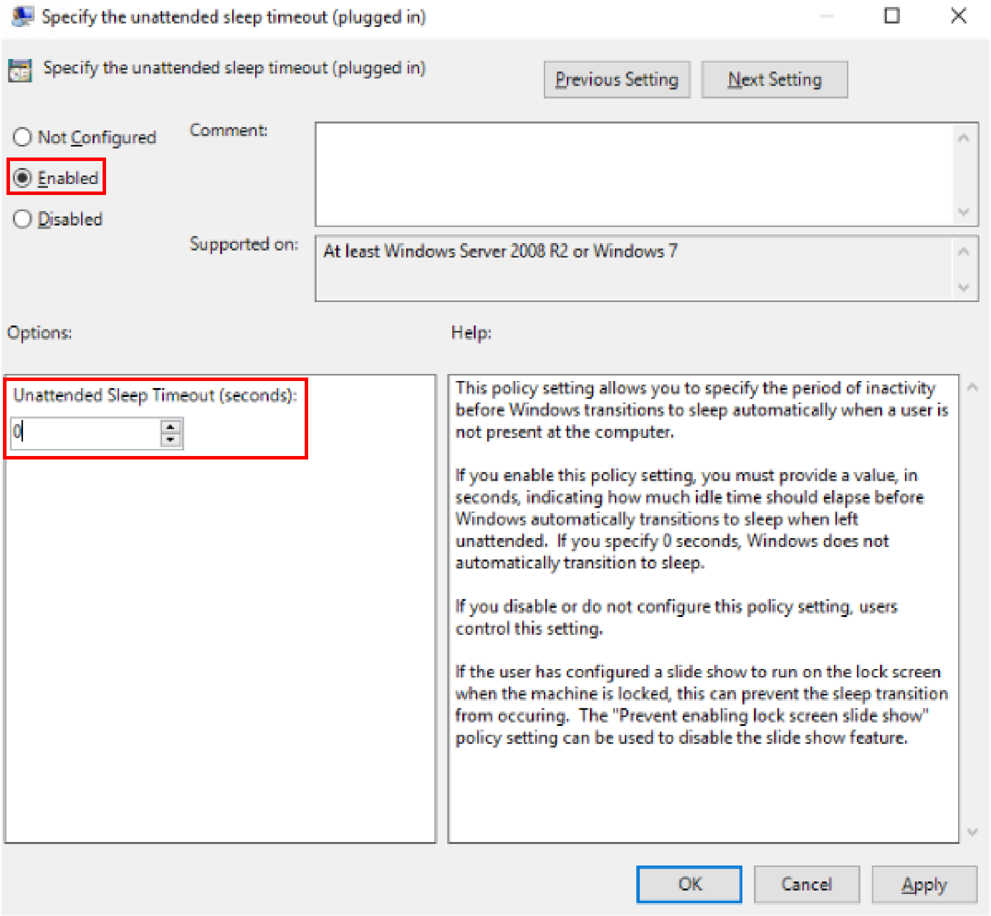
If you enable this policy setting, a hiberfile is not generated when the system transitions to sleep (Stand By).

If you disable or do not configure this policy setting, users control this setting.

Step 11 Click **OK**.

Step 12 Double-click **Specify the unattended sleep timeout (plugged in)**. In the displayed dialog box, select **Enabled** and set **Unattended Sleep Timeout (seconds)** to **0**.

Figure 14-10 Specifying the unattended sleep timeout (plugged in)



Specify the unattended sleep timeout (plugged in)

○ Not Configured
● Enabled
○ Disabled

Supported on: At least Windows Server 2008 R2 or Windows 7

Unattended Sleep Timeout (seconds): 0

This policy setting allows you to specify the period of inactivity before Windows transitions to sleep automatically when a user is not present at the computer.

If you enable this policy setting, you must provide a value, in seconds, indicating how much idle time should elapse before Windows automatically transitions to sleep when left unattended. If you specify 0 seconds, Windows does not automatically transition to sleep.

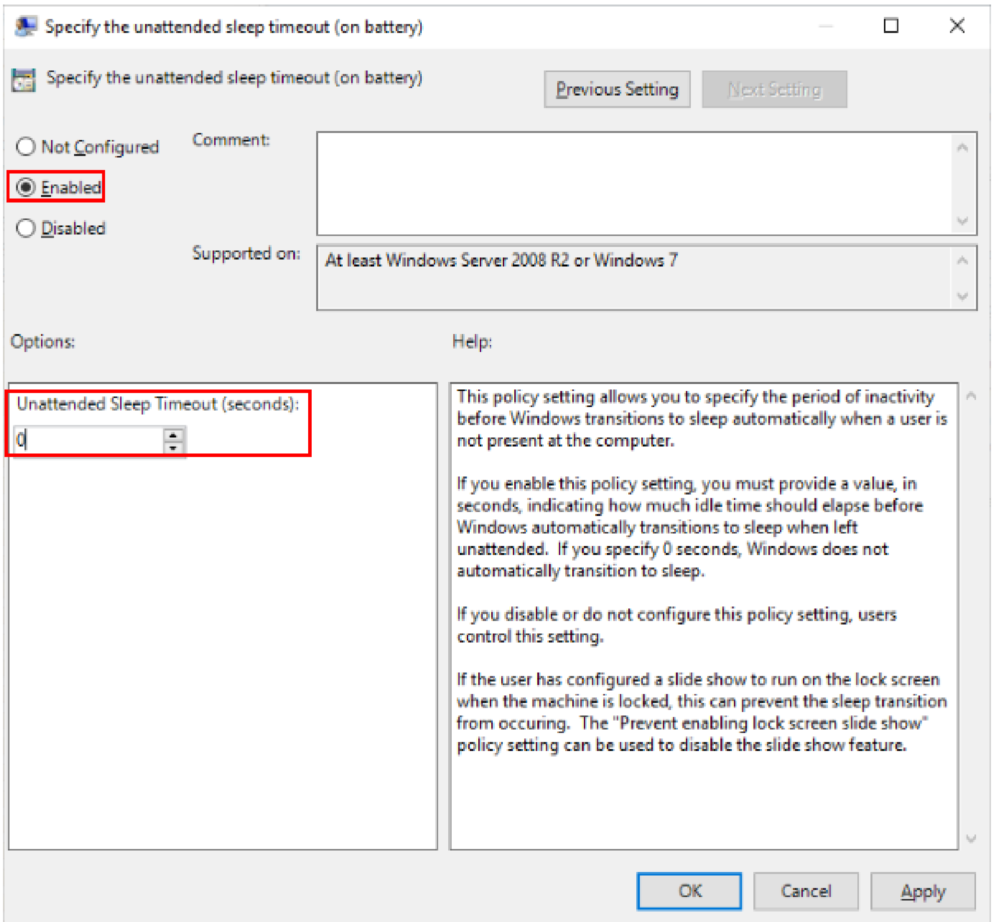
If you disable or do not configure this policy setting, users control this setting.

If the user has configured a slide show to run on the lock screen when the machine is locked, this can prevent the sleep transition from occuring. The "Prevent enabling lock screen slide show" policy setting can be used to disable the slide show feature.

Step 13 Click **OK**.

Step 14 Double-click **Specify the unattended sleep timeout (on battery)**. In the displayed dialog box, select **Enabled** and set **Unattended Sleep Timeout (seconds)** to **0**.

Figure 14-11 Specifying the unattended sleep timeout (on battery)



Specify the unattended sleep timeout (on battery)

Specify the unattended sleep timeout (on battery)

○ Not Configured

● Enabled

○ Disabled

Comment:

Supported on: At least Windows Server 2008 R2 or Windows 7

Options:

Help:

Unattended Sleep Timeout (seconds): 0

This policy setting allows you to specify the period of inactivity before Windows transitions to sleep automatically when a user is not present at the computer.

If you enable this policy setting, you must provide a value, in seconds, indicating how much idle time should elapse before Windows automatically transitions to sleep when left unattended. If you specify 0 seconds, Windows does not automatically transition to sleep.

If you disable or do not configure this policy setting, users control this setting.

If the user has configured a slide show to run on the lock screen when the machine is locked, this can prevent the sleep transition from occuring. The "Prevent enabling lock screen slide show" policy setting can be used to disable the slide show feature.

Step 15 Click **OK**.

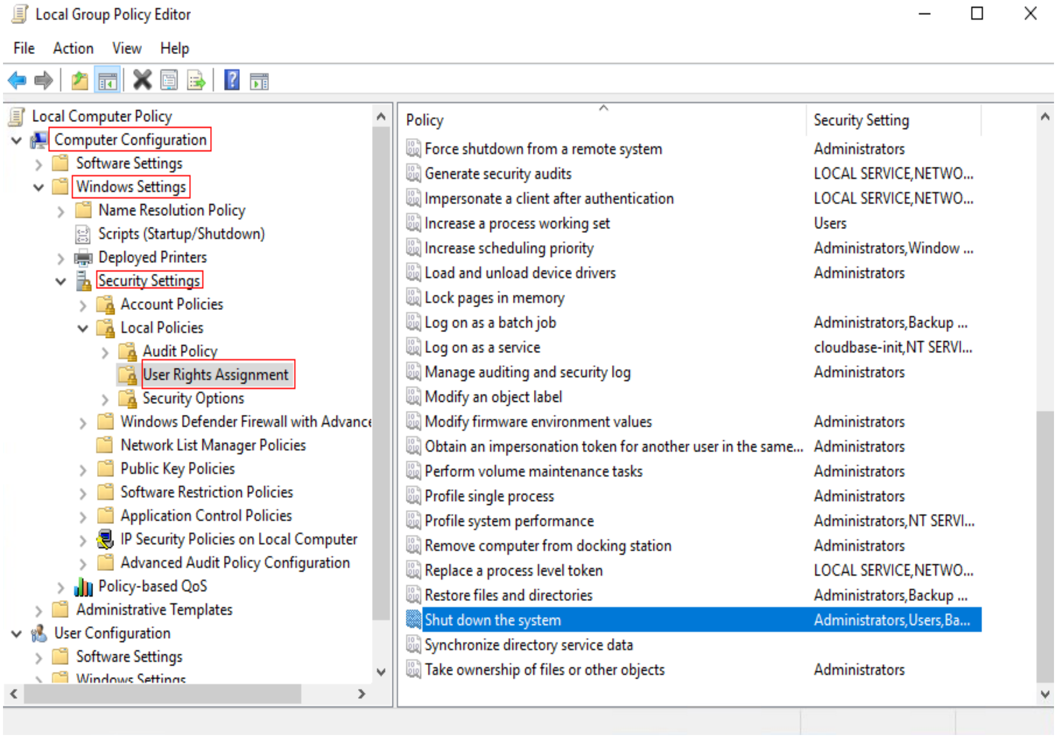
Enabling the group policy that allows the standard user group to shut down Windows

NOTE

Perform this operation for Windows Server 2016 and Windows Server 2019.

Step 16 In the **Local Group Policy Editor** navigation pane, choose **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies** > **User Rights Assignment**, as shown in **Figure 14-12**.

Figure 14-12 User rights assignment



Policy	Security Setting
Force shutdown from a remote system	Administrators
Generate security audits	LOCAL SERVICE,NETWO...
Impersonate a client after authentication	LOCAL SERVICE,NETWO...
Increase a process working set	Users
Increase scheduling priority	Administrators,Window ...
Load and unload device drivers	Administrators
Lock pages in memory	
Log on as a batch job	Administrators,Backup ...
Log on as a service	cloudbase-init,NT SERVI...
Manage auditing and security log	Administrators
Modify an object label	
Modify firmware environment values	Administrators
Obtain an impersonation token for another user in the same...	Administrators
Perform volume maintenance tasks	Administrators
Profile single process	Administrators
Profile system performance	Administrators,NT SERVI...
Remove computer from docking station	Administrators
Replace a process level token	LOCAL SERVICE,NETWO...
Restore files and directories	Administrators,Backup ...
Shut down the system	Administrators,Users,Ba...
Synchronize directory service data	
Take ownership of files or other objects	Administrators

Step 17 In the right pane, double-click **Shut down the system**.

The **Shut down the system properties** dialog box is displayed.

Step 18 Click **Add User or Group**. The **Select Users or Groups** dialog box is displayed.

Step 19 Click **Object Types**, select **Groups**, and click **OK**.

Step 20 In the **Enter the object names to select** area, enter **Users** to query and add the **Users** group to the policy.

Step 21 Click **OK**.

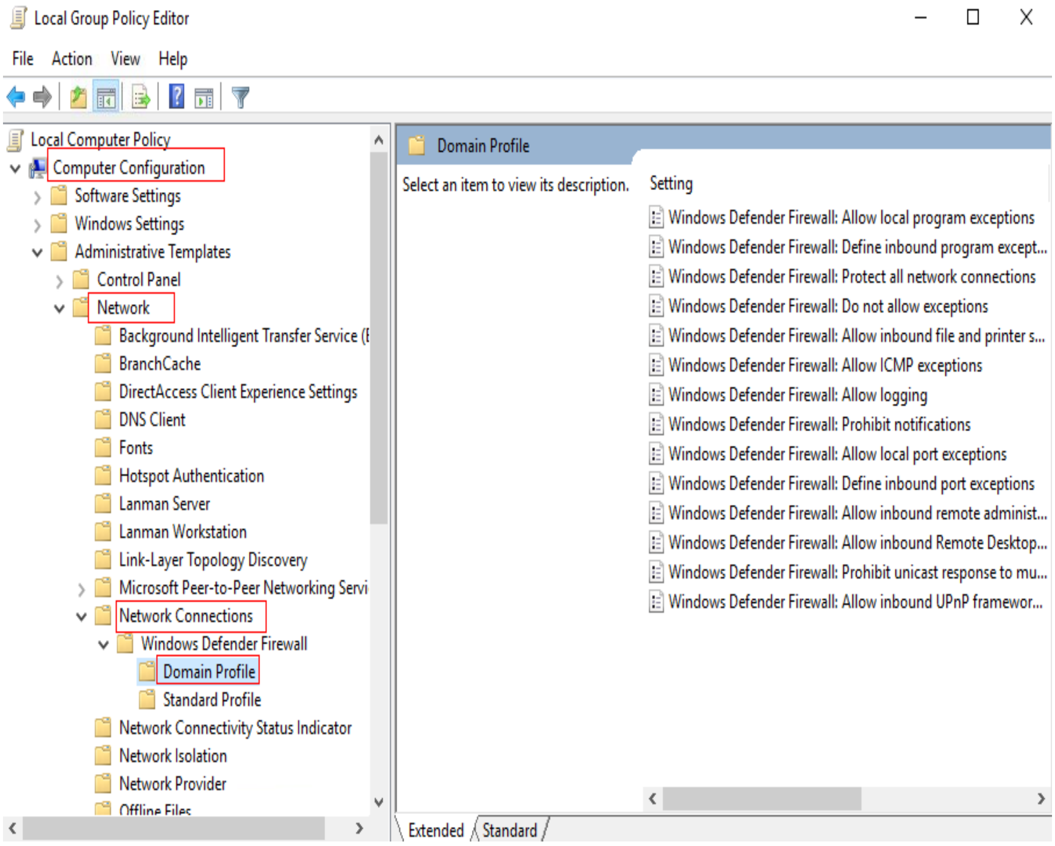
Step 22 Click **OK**.

Disabling the firewall

Step 23 In the navigation pane of the **Local Group Policy Editor**, choose **Computer Configuration** > **Administrative Templates** > **Network** > **Network Connections** > **Windows Firewall** > **Domain Profile**.

The **Domain Profile** page is displayed, as shown in **Figure 14-13**.

Figure 14-13 Domain profiles



Select an item to view its description.

Windows Defender Firewall: Allow local program exceptions
Windows Defender Firewall: Define inbound program except...
Windows Defender Firewall: Protect all network connections
Windows Defender Firewall: Do not allow exceptions
Windows Defender Firewall: Allow inbound file and printer s...
Windows Defender Firewall: Allow ICMP exceptions
Windows Defender Firewall: Allow logging
Windows Defender Firewall: Prohibit notifications
Windows Defender Firewall: Allow local port exceptions
Windows Defender Firewall: Define inbound port exceptions
Windows Defender Firewall: Allow inbound remote administ...
Windows Defender Firewall: Allow inbound Remote Desktop...
Windows Defender Firewall: Prohibit unicast response to mu...
Windows Defender Firewall: Allow inbound UPnP framewor...

Step 24 In the right pane, double-click **Windows Firewall: Protect all network connections**.

The **Windows Firewall: Protect all network connections** dialog box is displayed.

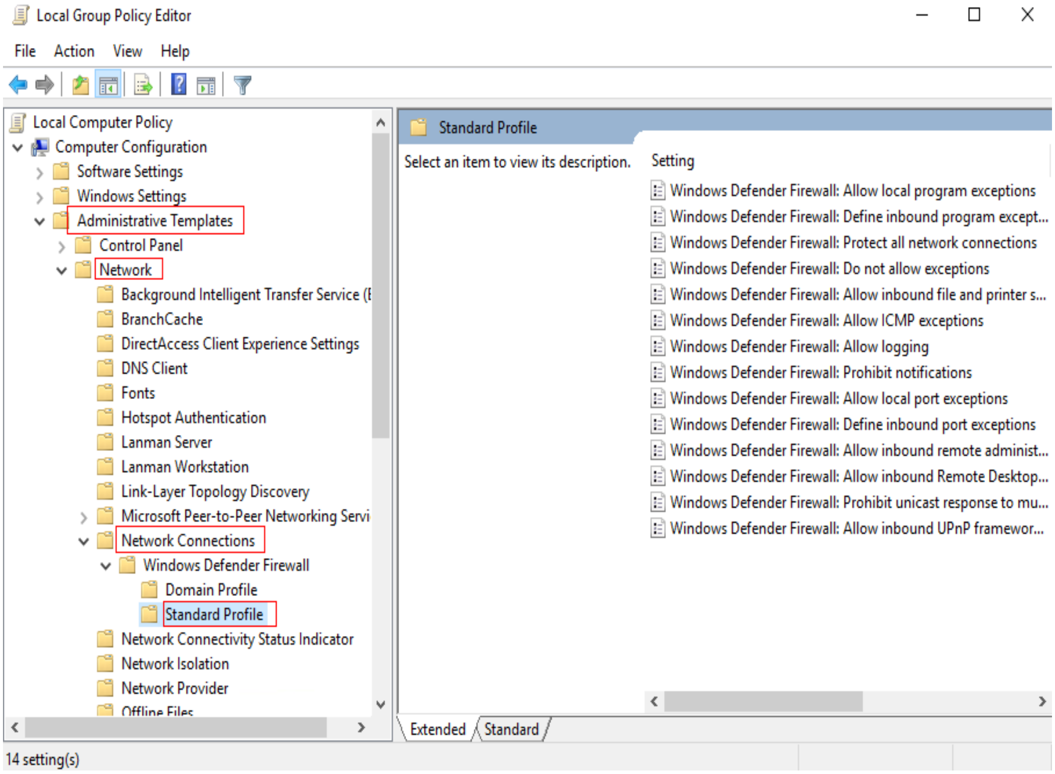
Step 25 Select **Disabled**.

Step 26 Click **OK**.

Step 27 In the navigation pane, choose **Standard Profile**.

The **Standard Profile** page is displayed, as shown in **Figure 14-14**.

Figure 14-14 Standard profiles



- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates
      - Control Panel
      - Network
        - Background Intelligent Transfer Service (I
        - BranchCache
        - DirectAccess Client Experience Settings
        - DNS Client
        - Fonts
        - Hotspot Authentication
        - Lanman Server
        - Lanman Workstation
        - Link-Layer Topology Discovery
        - Microsoft Peer-to-Peer Networking Servi
        - Network Connections
          - Windows Defender Firewall
            - Domain Profile
            - Standard Profile
        - Network Connectivity Status Indicator
        - Network Isolation
        - Network Provider
        - Offline Files

Standard Profile

Select an item to view its description.

Setting

- Windows Defender Firewall: Allow local program exceptions
- Windows Defender Firewall: Define inbound program except...
- Windows Defender Firewall: Protect all network connections
- Windows Defender Firewall: Do not allow exceptions
- Windows Defender Firewall: Allow inbound file and printer s...
- Windows Defender Firewall: Allow ICMP exceptions
- Windows Defender Firewall: Allow logging
- Windows Defender Firewall: Prohibit notifications
- Windows Defender Firewall: Allow local port exceptions
- Windows Defender Firewall: Define inbound port exceptions
- Windows Defender Firewall: Allow inbound remote administ...
- Windows Defender Firewall: Allow inbound Remote Desktop...
- Windows Defender Firewall: Prohibit unicast response to mu...
- Windows Defender Firewall: Allow inbound UPnP framewor...

14 setting(s)

Step 28 In the right pane, double-click **Windows Firewall: Protect all network connections**.

The **Windows Firewall: Protect all network connections** dialog box is displayed.

Step 29 Select **Disabled**.

Step 30 Click **OK**.

Step 31 Close the **Local Group Policy Editor** window.

Step 32 On the ECS, right-click in the lower left corner and choose **Run** from the shortcut menu.

The **Run** dialog box is displayed.

Step 33 Enter **services.msc** in the **Open** text box and press **Enter**.

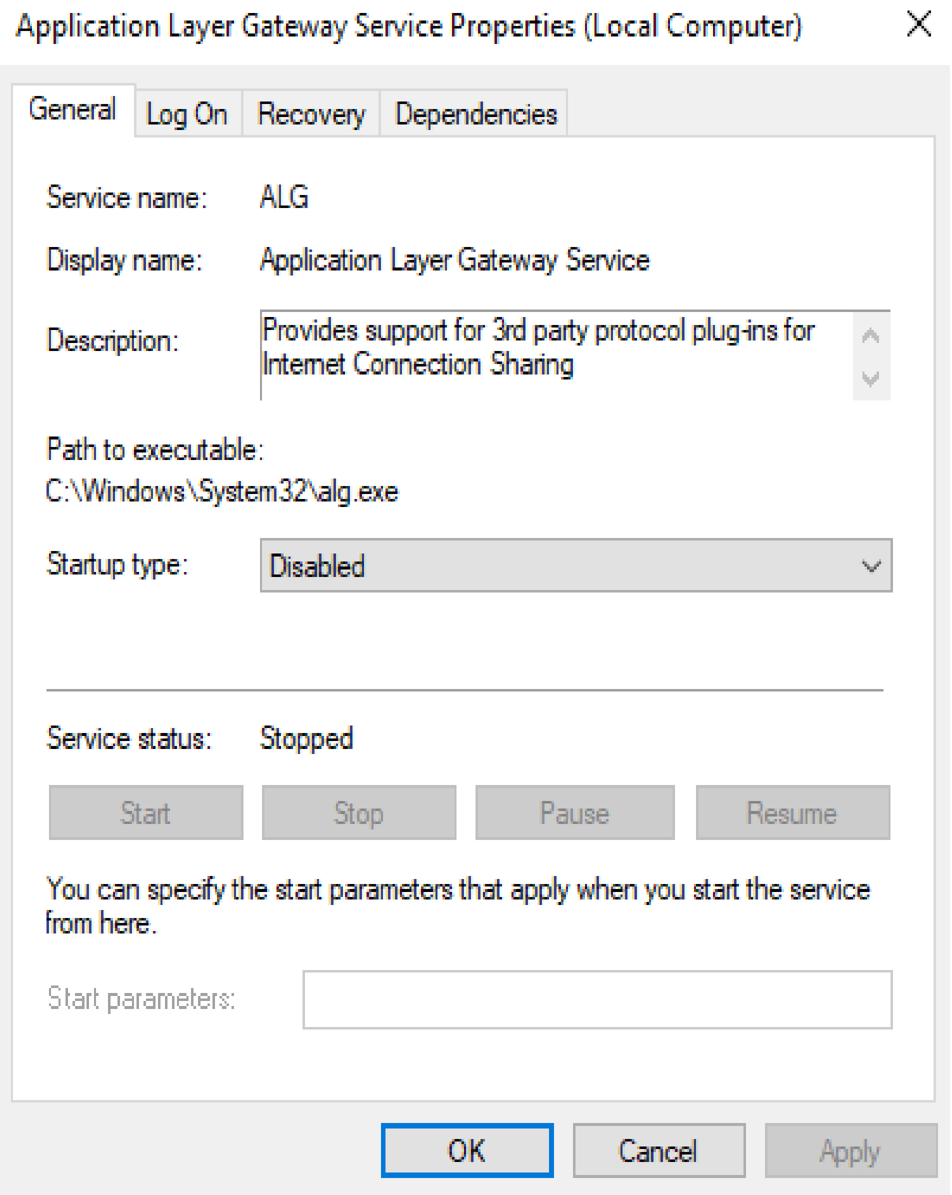
The **Services** window is displayed.

Step 34 In the right pane, double-click **Application Layer Gateway Service**.

The **Application Layer Gateway Service Properties (Local Computer)** page is displayed.

Step 35 On the **General** tab, set **Startup Type** to **Disabled**, as shown in **Figure 14-15**.

Figure 14-15 Configuring the startup type



Application Layer Gateway Service Properties (Local Computer)

Service name: ALG

Display name: Application Layer Gateway Service

Description: Provides support for 3rd party protocol plug-ins for Internet Connection Sharing

Path to executable:
C:\Windows\System32\alg.exe

Startup type: Disabled

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Step 36 Click **OK**.

Step 37 Set the **Startup Type** of **Internet Connection Sharing (ICS)** and **Windows Firewall** to **Disabled** by referring to **Step 34** to **Step 36**.

NOTE

You do not need to configure **Windows Defender Firewall** for Windows Server 2019.

Step 38 Close the **Services** window.

Disabling Windows update

Step 39 On the ECS, right-click ⊞ in the lower left corner and choose **Run** from the shortcut menu.

The **Run** dialog box is displayed.

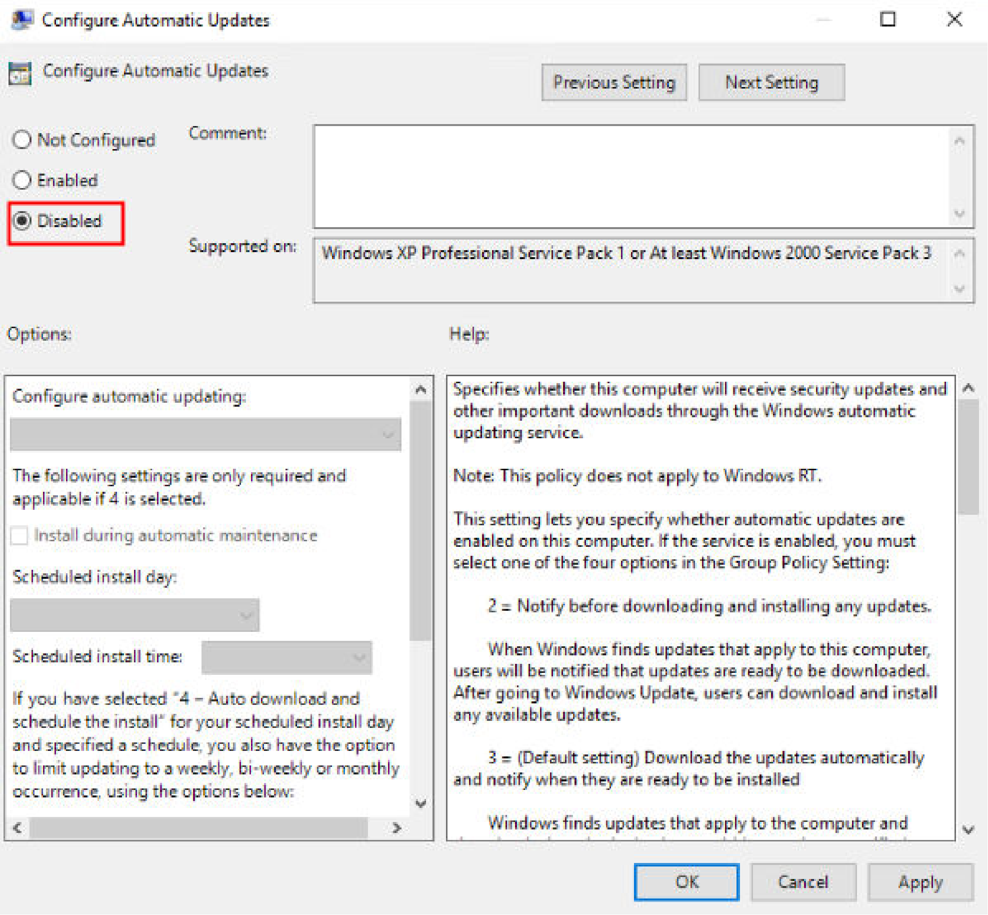
Step 40 Enter **gpedit.msc** in the **Open** text box and press **Enter**.

The **Local Group Policy Editor** window is displayed.

Step 41 Choose **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Windows Update**, and double-click **Configure Automatic Updates**. The **Configure Automatic Updates** dialog box is displayed.

Step 42 Select **Disabled** and click **OK**, as shown in **Figure 14-16**.

Figure 14-16 Configuring automatic updates



Configure Automatic Updates

Configure Automatic Updates

○ Not Configured

○ Enabled

● Disabled

Comment:

Supported on: Windows XP Professional Service Pack 1 or At least Windows 2000 Service Pack 3

Options:

Configure automatic updating:

The following settings are only required and applicable if 4 is selected.

□ Install during automatic maintenance

Scheduled install day:

Scheduled install time:

If you have selected "4 – Auto download and schedule the install" for your scheduled install day and specified a schedule, you also have the option to limit updating to a weekly, bi-weekly or monthly occurrence, using the options below:

Help:

Specifies whether this computer will receive security updates and other important downloads through the Windows automatic updating service.

Note: This policy does not apply to Windows RT.

This setting lets you specify whether automatic updates are enabled on this computer. If the service is enabled, you must select one of the four options in the Group Policy Setting:

2 = Notify before downloading and installing any updates.

When Windows finds updates that apply to this computer, users will be notified that updates are ready to be downloaded. After going to Windows Update, users can download and install any available updates.

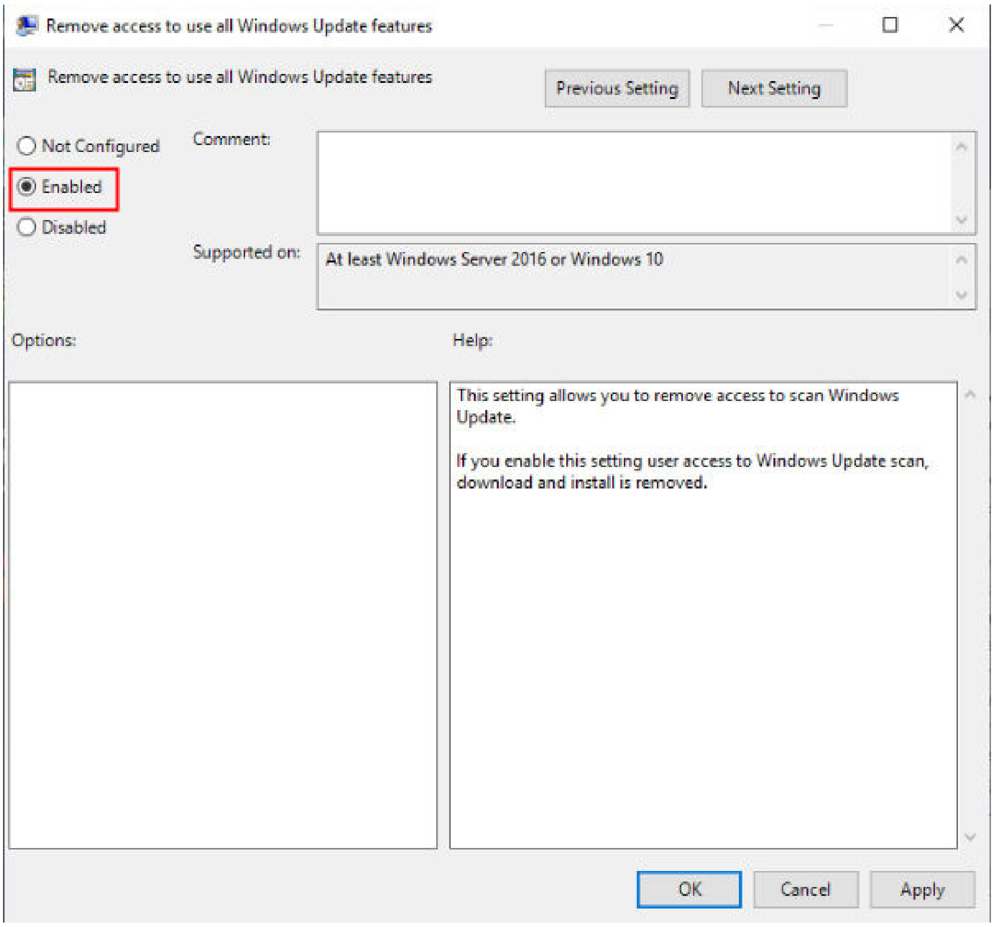
3 = (Default setting) Download the updates automatically and notify when they are ready to be installed

Windows finds updates that apply to the computer and

Step 43 In the **Local Group Policy Editor** window, choose **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Windows Update**, and double-click **Remove access to all Windows Update features**. The **Remove access to all Windows Update features** dialog box is displayed.

Step 44 Select **Enabled** and click **OK**, as shown in **Figure 14-17**.

Figure 14-17 Removing access to all Windows Update features



Remove access to use all Windows Update features

Remove access to use all Windows Update features

○ Not Configured

● Enabled

○ Disabled

Comment:

Supported on: At least Windows Server 2016 or Windows 10

Options:

Help:

This setting allows you to remove access to scan Windows Update.

If you enable this setting user access to Windows Update scan, download and install is removed.

Creating a temporary local user admin

NOTICE

- After Cloudbase-Init is installed, it will randomize the password of the **Administrator** account if application software that takes effect only after a restart is installed. To prevent login failure after randomization, create a temporary account and reset the password of **Administrator**.
- If your login using the default password of **Administrator** fails after the restart, log in as the **admin** user and reset the password of **Administrator**. Then log in as the **Administrator** user again.

Step 45 On the ECS, click 🔍 in the lower left corner, enter **compmgmt.msc**, and press **Enter**.

The **Computer Management** window is displayed.

Step 46 In the navigation pane, choose **Local Users and Groups** > **Users**.

Step 47 Right-click and choose **New User** from the shortcut menu.

Step 48 In the **New User** dialog box, enter the username and password, confirm the password, and click **Create**.

Step 49 In the navigation pane, choose **Local Users and Groups** > **Groups**.

Step 50 Right-click **Administrators** and choose **Add to Group** from the shortcut menu.

NOTE

If you need to add administrators to other groups, select an option as required.

Step 51 In the **Administrators Properties** dialog box, click **Add** to add the user to the group.

Step 52 Click **OK** and close the **Administrators Properties** dialog box.

Step 53 Close the **Server Manager** window.

Configuring a private DNS

You can configure a private DNS server address for OBS so that Windows ECSs on Huawei Cloud can directly access OBS through the private network.

Step 54 On the ECS, right-click 🔍 in the lower left corner, enter **cmd**, and press **Enter**.

Step 55 Run the **ipconfig /all** command to check whether the DNS server is at the private DNS address in the region where the ECS resides.

NOTE

Huawei Cloud provides different private DNS server addresses for different regions. For details, see **What Are the Private DNS Server Addresses Provided by Huawei Cloud?**

Step 56 Change the DNS server address of the VPC subnet.

Locate the VPC where the ECS resides and change the DNS server address of the VPC subnet to the private DNS address. In this manner, ECSs in the VPC can use the private DNS for resolution and thereby you can access OBS on Huawei Cloud intranet. For details, see **Modifying a Subnet**.

NOTE

The private DNS server address must be selected based on the region where the ECS is. For details, see **What Are Huawei Cloud Private DNS Server Addresses?**

Enabling applications to access the microphone of the OS

Step 57 Choose **Start** > **Settings**. The OS setting page is displayed.

Step 58 Click **Privacy**. The privacy setting page is displayed.

Step 59 In the list on the left, click **Microphone**. The page for setting microphone permissions is displayed.

Step 60 Set **Microphone access** to **On**.

Obtaining required installation packages

Step 61 Upload the packages obtained in **14.1.1 Required Software**, except the OS ISO file, to the OBS bucket used in **14.1.2 Registering a Private Image Using an ISO File**.

NOTE

Set the object permission to **public-read**.

Step 62 Record the link of each package in the OBS bucket.

NOTE

On OBS Browser+, right-click the package, choose **Share** from the shortcut menu, and click **Copy Link** to obtain the download link of the package. You need to download the package within the sharing validity period.

Step 63 In the root directory of drive C on the ECS, create a folder, for example, **software**, for storing the package to be installed.

Step 64 Open the browser on the ECS, copy the package link recorded in **Step 62** to the address box, and press **Enter** to download the package.

NOTE

- If Internet Explorer does not allow file download by default, enable file download in the displayed security settings dialog box.
- Switch the input mode of the ECS to English.
- Download the required packages in sequence.

Step 65 Copy the obtained packages to **C:\software**.

Installing the 7-Zip

Step 66 Go to **C:\software** to find and decompress the 7-Zip installation package.

Installing the Visual Studio 2017 runtime library

Step 67 Go to **C:\software** to find the **vc_redist.x64.exe** and **vc_redist.x86.exe** packages, and double-click to install the Visual Studio 2017 runtime library.

Step 68 Restart the ECS.

(Optional) Deleting the Microsoft language package

Step 69 Search for **Windows PowerShell** in the **Start** menu and click **Run as administrator**. The Windows PowerShell running page is displayed.

Step 70 Run the following command to delete the Microsoft language package:

```
Get-Appxpackage -allusers *Microsoft.LanguageExperiencePackzh-CN* |
remove-appxpackage
```

NOTE

- To ensure that users can purchase Workspace desktops, you need to delete the Microsoft language package when creating a Windows 10 image.
- If there are multiple users, you need to log in to the system using each user account to delete the language package.

(Optional) Installing the OS patch

Step 71 Go to **C:\software** where the package is stored and install the OS patch.

NOTE

OS patches are updated by Microsoft on an irregular basis. Pay attention to Microsoft announcements and update the OS in a timely manner.

(Optional) Installing applications

Step 72 Go to **C:\software** where the package is stored and install the application.

NOTICE

Some security software (antivirus software, safeguards, and firewalls) may conflict with the Microsoft encapsulation tool. As a result, desktop creation may fail, and the blue screen of death (BSOD) or black screen may occur on the created desktop. Therefore, install security software only after desktops are provisioned.

(Optional) Installing peripheral drivers

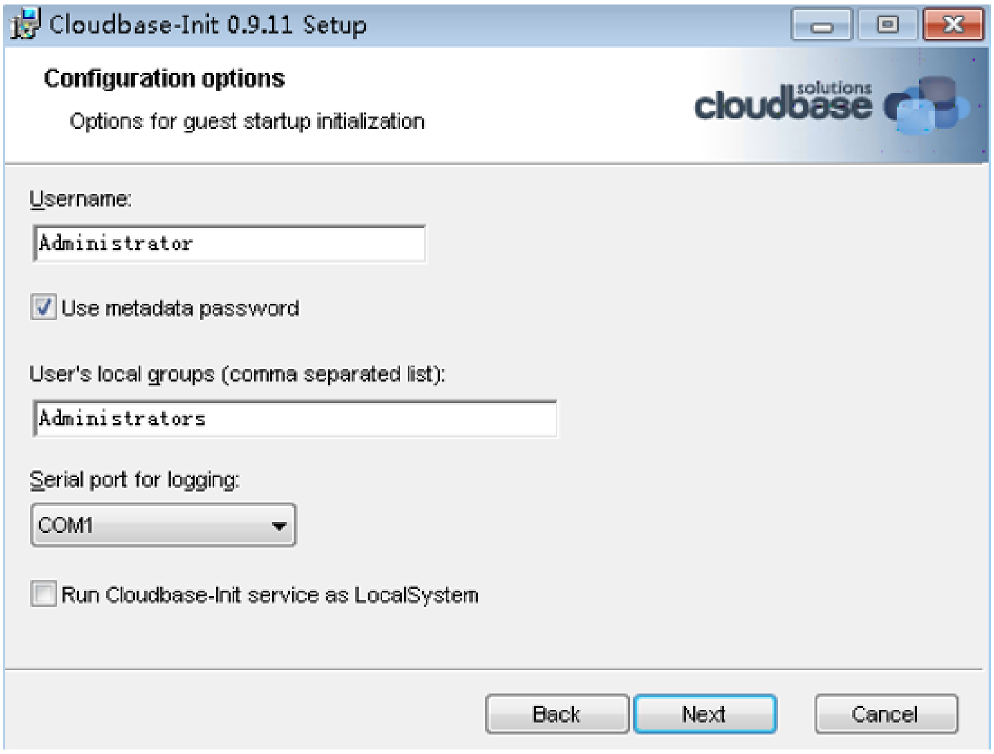
Step 73 Go to **C:\software** where the package is stored and install the peripheral driver.

Installing the Cloudbase-Init software

Step 74 Go to **C:\software** where the package is stored, open the Cloudbase-Init installation package, and install Cloudbase-Init as prompted.

Step 75 On the **Configuration options** page, configure parameters by referring to **Figure 14-18**.

Figure 14-18 Configuration options



Cloudbase-Init 0.9.11 Setup

Configuration options

Options for guest startup initialization

Username: Administrator

☑ Use metadata password

User's local groups (comma separated list): Administrators

Serial port for logging: COM1

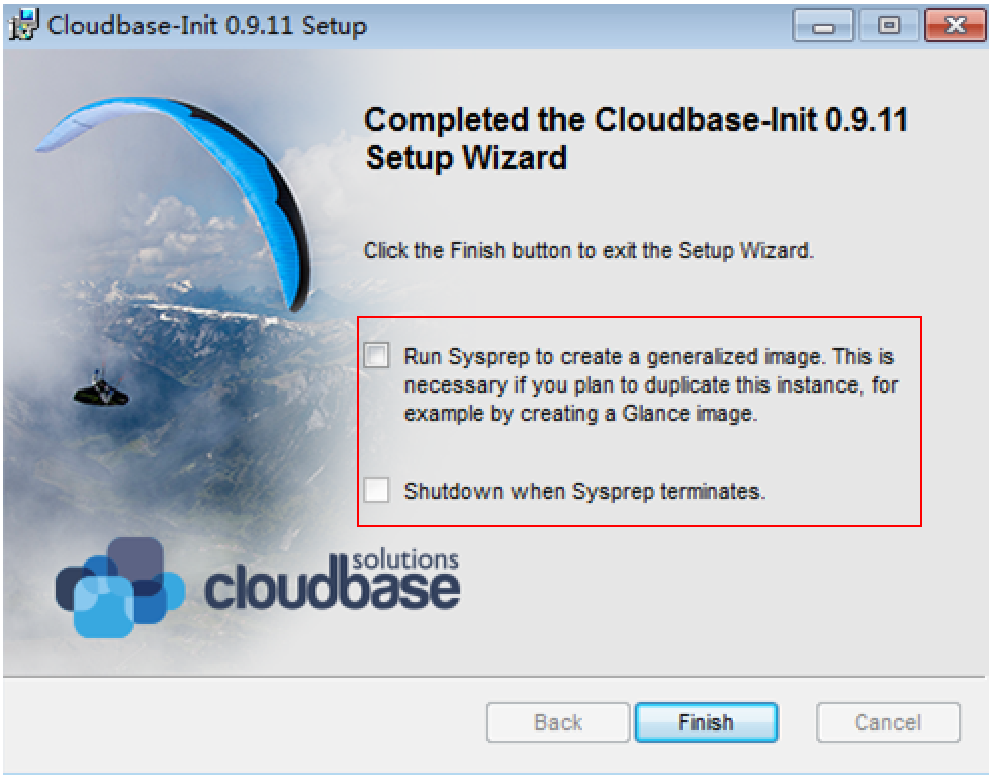
☐ Run Cloudbase-Init service as LocalSystem

NOTE

The version number in the figure is for reference only. Use the actual version number.

Step 76 After the configuration is complete, deselect the options shown in **Figure 14-19**.

Figure 14-19 Finish



Cloudbase-Init 0.9.11 Setup

Completed the Cloudbase-Init 0.9.11 Setup Wizard

Click the Finish button to exit the Setup Wizard.

□ Run Sysprep to create a generalized image. This is necessary if you plan to duplicate this instance, for example by creating a Glance image.

□ Shutdown when Sysprep terminates.

Step 77 Click **Finish**.

Configuring Cloudbase-Init

Step 78 Edit the configuration file **C:\Program Files\Cloudbase Solutions\Cloudbase-Init\conf\cloudbase-init.conf** in the Cloudbase-Init installation path.

1. Add the **netbios_host_name_compatibility=false** configuration item to the last line of the configuration file so that the host name of the Windows OS can contain a maximum of 63 characters.

   NOTE

   NetBIOS supports up to 15 characters due to the constraint of Windows OS.

2. Add the configuration item **metadata_services=cloudbaseinit.metadata.services.httpservice.HttpService** to enable the agent to access the OpenStack data source.

3. Add the following configuration item to disable Cloudbase-Init restart:

```
plugins=cloudbaseinit.plugins.windows.extendvolumes.ExtendVolumesPlugin,cloudbaseinit.plugins.windows.createuser.CreateUserPlugin,cloudbaseinit.plugins.common.sshpublickeys.SetUserSSHPublicKeysPlugin,cloudbaseinit.plugins.common.setuserpassword.SetUserPasswordPlugin,cloudbaseinit.plugins.common.localscripts.LocalScriptsPlugin,cloudbaseinit.plugins.common.userdata.UserDataPlugin
```

Step 79 In **C:\Program Files\Cloudbase Solutions\Cloudbase-Init\conf\cloudbase-init-unattend.conf**, check whether **cloudbaseinit.plugins.common.sethostname.SetHostNamePlugin,** exists.

- If yes, delete it and perform subsequent operations.
- If no, perform subsequent operations.
- Add **cloudbaseinit.plugins.common.userdata.UserDataPlugin** at the end of **plugins=**. Add a comma (,) in front of the added configuration item.

Step 80 If you use a Windows ECS to create an image, change the SAN policy of the ECS to **OnlineAll**. Otherwise, when you use the image to create ECSs, the disks may be offline.

Windows has three types of SAN policies: **OnlineAll**, **OfflineShared**, and **OfflineInternal**.

Table 14-6 SAN policies of Windows

Type	Description
OnlineAll	All newly found disks are online.
OfflineShared	All newly found disks on sharable buses, such as iSCSI and FC, are left offline by default, while disks on non-sharable buses are online.
OfflineInternal	All newly found disks are left offline.

1. Execute **cmd.exe** and run the following command to query the current SAN policy of the ECS using DiskPart:

   diskpart
2. Run the following command to view the SAN policy of the ECS:

   san
   - If the SAN policy is **OnlineAll**, run the **exit** command to exit DiskPart and close **cmd.exe**.
   - If no, go to 80.3.
3. Run the following command to change the SAN policy to **OnlineAll**:

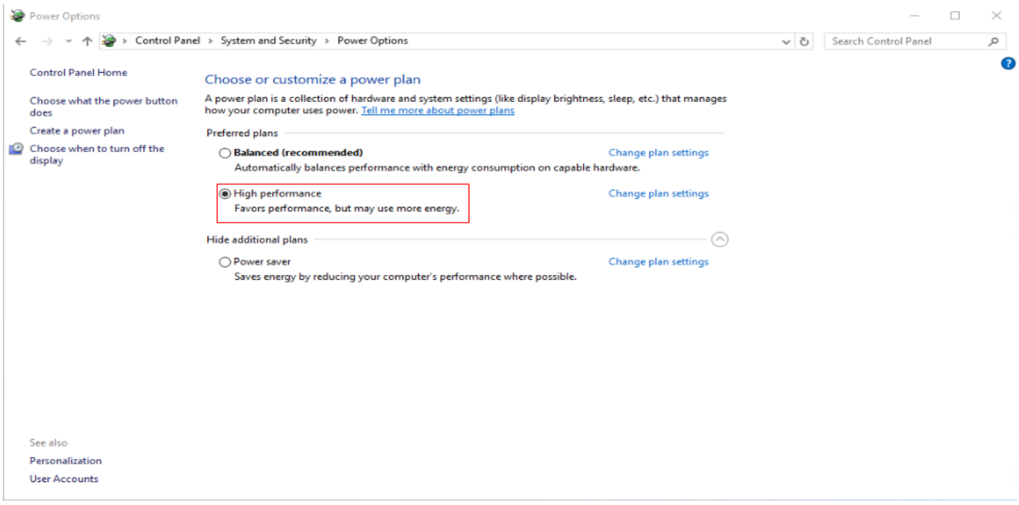
   san policy=onlineall
4. Run the **exit** command to exit DiskPart and close **cmd.exe**.

Changing the power settings to high performance/ultimate performance

NOTE

You need to modify the power settings of all Windows desktops.

Step 81 Choose **Control Panel** > **System and Security** > **Power Options**, and select **High performance** for **Preferred plans**, or **Ultimate Performance** after showing additional plans.



Power Options

Control Panel > System and Security > Power Options

Search Control Panel

Control Panel Home

Choose what the power button does

Create a power plan

Choose when to turn off the display

Choose or customize a power plan

A power plan is a collection of hardware and system settings (like display brightness, sleep, etc.) that manages how your computer uses power. Tell me more about power plans

Preferred plans

○ **Balanced (recommended)** Change plan settings

Automatically balances performance with energy consumption on capable hardware.

● High performance Change plan settings

Favors performance, but may use more energy.

Hide additional plans

○ Power saver Change plan settings

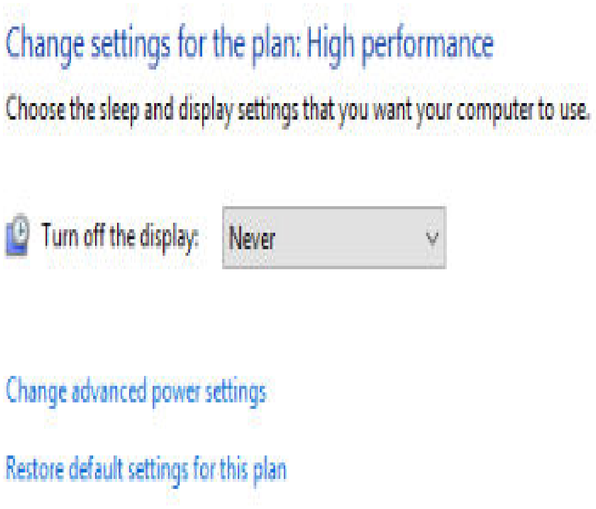
Saves energy by reducing your computer's performance where possible.

See also

Personalization

User Accounts

Step 82 Click **Change plan settings** on the right of **High performance** or **Ultimate Performance**. On the page displayed, select **Never** for **Turn off the display:**



Change settings for the plan: High performance

Choose the sleep and display settings that you want your computer to use.

Turn off the display: Never

Change advanced power settings

Restore default settings for this plan

Installing SysAgent and SysPrep

Step 83 Double-click **HW.SysAgent.Installer_64.msi** and **HW.SysPrep.Installer_64.msi** in **C:\software**.

Installing AppCenterAgent and AppCenter

Step 84 Double-click **WKSAppCenterAgent.msi** and **WKSAppCenter.msi** in **C:\software**.

----End

Deleting a system recovery partition

NOTE

This operation is required for Windows 10 or Windows 11 images.

Step 1 Right-click **Start** and choose **Disk Management** from the shortcut menu. Check whether the system disk (generally drive C) has a recovery partition. Go to the next step only when there is a recovery partition.

Step 2 Press **Win** + **R**, enter **cmd**, and enter

diskpart.

The **diskpart** window is displayed.

Step 3 Run the following commands in sequence to delete the system recovery partition:

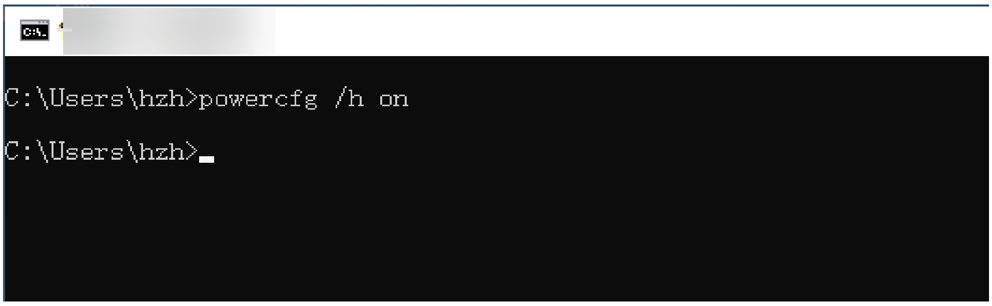
1. Print the disk list and select the system disk.
   ```
   list disk
   # The number 0 indicates that the selected disk 0 is the system disk. Select a disk as required.
   select disk 0
   ```
2. Print the disk partition list and select the recovery partition to be deleted.
   ```
   list partition
   # In this example, 3 indicates the number of the recovery partition. Select a value as required.
   select partition 3
   ```
3. Delete the recovery partition.
   ```
   delete partition override
   ```

Enabling hibernation

Step 4 On the ECS, right-click ⊞ in the lower left corner and choose **Run** from the shortcut menu.

The **Run** dialog box is displayed.

Run the **powercfg -h on** command to enable hibernation.



```
C:\Users\hzh>powercfg /h on

C:\Users\hzh>_
```

NOTE

Configure this parameter only for Windows Server 2016 and 2019.

(Optional) Backing up an image

NOTE

After an image is encapsulated, if the ECS is stopped and restarted, the image is decapsulated and cannot be used. In this case, you need to configure and encapsulate the ECS again. If necessary, you can back up the ECS before encapsulation.

Step 5 In the ECS list, locate the configured ECS and choose **More** > **Stop** to stop it.

Step 6 After the ECS is stopped, choose **More** > **Manage Image/Backup** > **Create Image** to create an ECS backup.

Step 7 After the ECS backup is created, restart and encapsulate the ECS.

Encapsulating the image

- To create an encapsulated image, perform **Step 8** to **Step 11**.
- To create an image that is not encapsulated, perform **Step 8** to **Step 10**, and **Step 12**.

NOTE

1. If images are not encapsulated, problems may occur on some applications, such as Windows Server Update Services (WSUS).
2. In Windows 8 or Windows Server 2012, you may encounter problems where push notifications do not work.
3. Images that are not encapsulated can be provisioned more rapidly.
4. The encapsulation command can be executed only by a user granted the administrator permissions.

Step 8 On the ECS, find the Windows image creation tool in **C:\software** and decompress it to obtain the **Workspace_HDP_WindowsDesktop**_*XXX* folder.

Step 9 Right-click 🔍 in the lower left corner, enter **cmd**, and press **Enter**.

Step 10 Switch to the directory containing the template tool:

cd C:\software\Workspace_HDP_WindowsDesktop_Installer_*x.x.x*

Step 11 In the displayed CLI, run the following command to encapsulate the image:

run_silent.bat --passive --environment_type 2 --nocheck --noshutdown

NOTE

During image encapsulation, the ECS automatically restarts. Do not exit or stop the ECS. After the ECS is restarted, enter the ECS password to proceed with image encapsulation.

Step 12 (Optional) In the displayed CLI, run the following command to create an image not encapsulated:

run_silent.bat --passive --environment_type 2 --nocheck --noshutdown --nosysprep

Deleting the temporary admin user

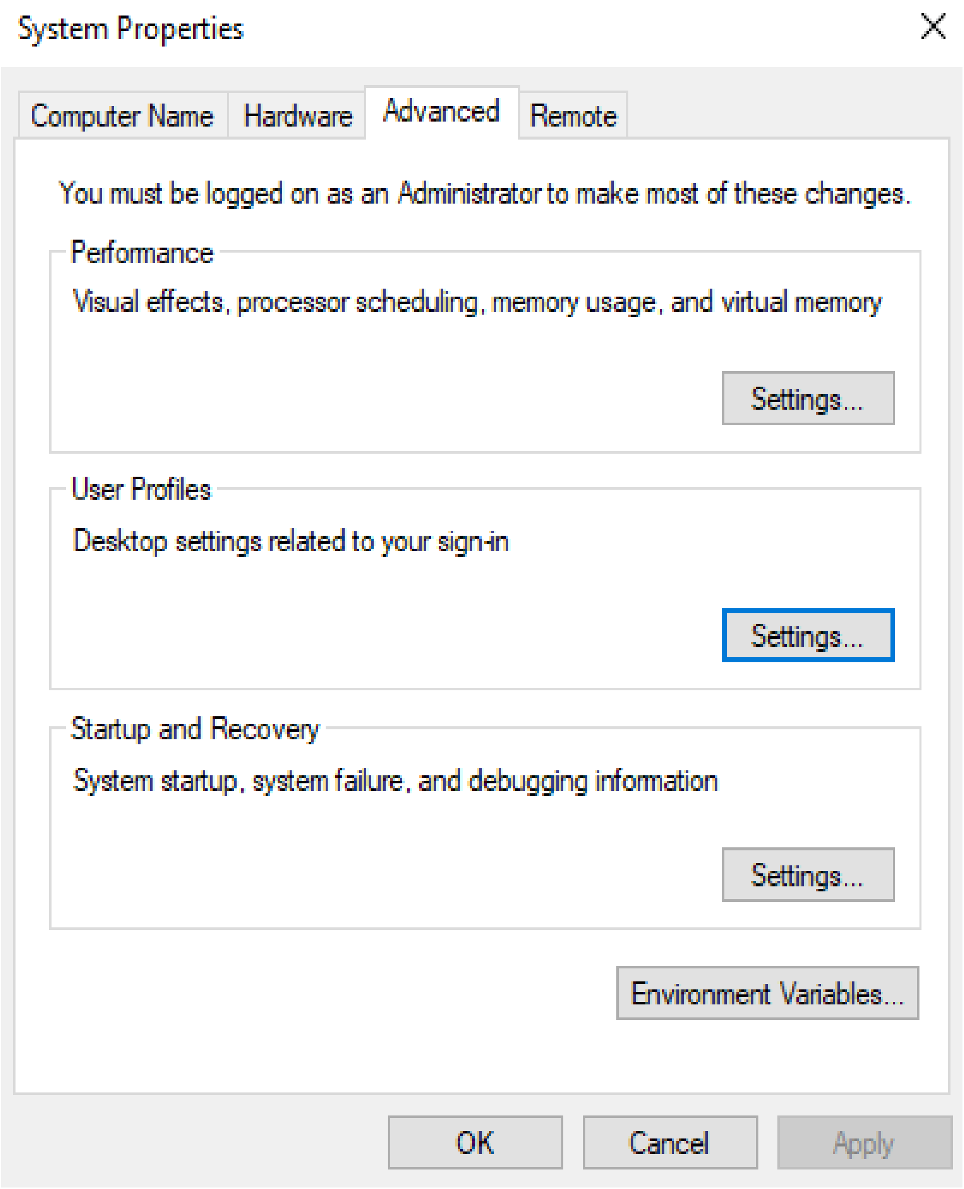
Step 13 On the ECS, right-click ⊞ in the lower left corner and choose **Run** from the shortcut menu.

The **Run** dialog box is displayed.

Step 14 Enter **sysdm.cpl** in the **Open** text box and press **Enter**.

The **System Properties** window is displayed.

Step 15 On the **Advanced** tab, click **Settings** under **User Profiles**.



You must be logged on as an Administrator to make most of these changes.

Visual effects, processor scheduling, memory usage, and virtual memory

Desktop settings related to your sign-in

System startup, system failure, and debugging information

Step 16 On the **User Profiles** page, select the profiles of the user to be deleted and click **Delete**.

Step 17 Click **OK**.

Step 18 Close the **System Properties** window.

Step 19 Click **Start** > **Run**.

The **Run** dialog box is displayed.

Step 20 Enter **compmgmt.msc** in the **Open** text box and press **Enter**.

The **Computer Management** window is displayed.

Step 21 In the navigation pane on the left, choose **System Tools** > **Local Users and Groups** > **Users**.

Step 22 In the right pane, right-click the username to be deleted and choose **Delete**.

Step 23 Click **Yes**.

Step 24 Click **OK**.

Step 25 Close the **Computer Management** window.

Stopping the ECS

Step 26 On the ECS list page of the console, locate the row that contains the ECS created in **14.1.3 Creating an ECS**, and choose **More** > **Stop** to stop the ECS.

----End

14.1.5 Creating a User Desktop Image

Scenarios

This section describes how to create a user desktop image.

Prerequisites

- You have obtained the username and password for logging in to the console.
- You have obtained the password of the OS administrator **Administrator**.

Procedure

Step 1 Log in to the ECS console.

Step 2 In the service list, choose **Elastic Cloud Server**.

Step 3 Locate the row of the desired ECS, and choose **More** > **Manage Image/Backup** > **Create Image**.

Step 4 On the page for creating a private image, configure parameters as prompted.

- **Type**: Select **Create Image**.
- **Image Type**: Select **System disk image**.
- **Source**: cloud server. Select the cloud server that has been stopped in **14.1.4 Configuring an ECS**.
- **Name**: Configure this parameter based on the actual OS, for example, **Workspace_Image_01**.
- **Enterprise Project**: Select the enterprise project to which the resource belongs, for example, **default**.

Step 5 Confirm the image parameters, select **I have read and agree to the Image Disclaimer**, and click **Submit**.

It takes about 10 to 15 minutes to create an image. The created image is displayed in the list under **Cloud Server Console** > **Image Management Service** > **Private Image**.

----End

15 Permission Management

15.1 Workspace Permissions

Related Concepts

IAM can be used free of charge on Huawei Cloud. You pay only for the resources in your account. For details about IAM, see **IAM Service Overview**.

Account

An account registered upon your first use of Huawei Cloud. You can use this account to pay the bill, access all Huawei Cloud resources and services under the account, and to reset user passwords and grant user permissions. You can use your account to receive and pay all bills generated by your IAM users' use of resources.

You cannot modify or delete your account in IAM, but you can do so in **My Account**.

IAM user

You can use your account to create IAM users and assign permissions for specific resources. Each IAM user has their own identity credentials (password or access keys) and uses cloud resources based on the assigned permissions. IAM users cannot make payments themselves. You can use your account to pay their bills.

User group

You can use user groups to assign permissions to IAM users. IAM users must be added to a user group to obtain the permissions required for accessing specified resources or cloud services under the account. If you add a user to multiple user groups, the user inherits the permissions that are assigned to all the groups.

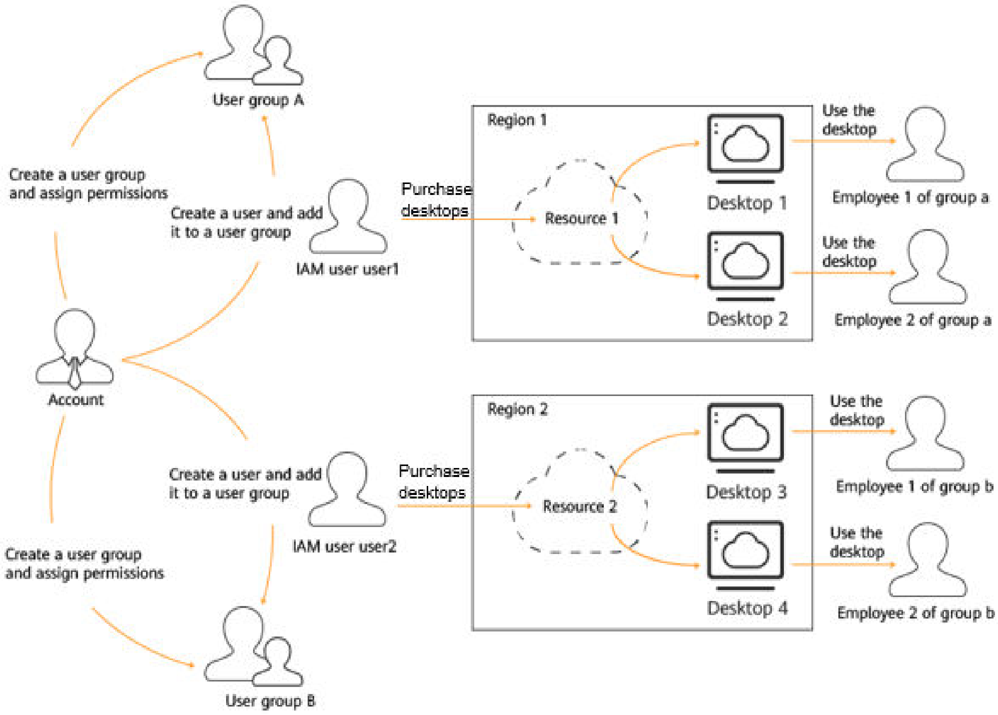
The default user group **admin** has all the permissions for using all of the cloud resources. Users in this group can perform operations on all resources, including but not limited to creating user groups and users, assigning permissions, and managing resources.

Examples

For example, you want to isolate permissions of employees in groups a and b. That is, employees in group a use Workspace resources in region 1, and employees in group b use Workspace resources in region 2.

1. You can create user groups A and B and grant permissions to them. That is, assign the administrator permissions of Workspace in region 1 to user group A, and assign the administrator permissions of Workspace in region 2 to user group B.
2. Create two IAM users **user1** and **user2**, and add **user1** to user group A and **user2** to user group B. IAM user **user1** has the administrator permissions of Workspace in region 1, and IAM user **user2** has the administrator permissions of Workspace in region 2.
3. The administrator of group a can use the account of **user1** to log in to Huawei Cloud and go to the Workspace console of the project in region 1 to purchase desktops for the employees of group a and manage the desktops of the project in region 1. The administrator of group b can use the account of **user2** to log in to Huawei Cloud and go to the Workspace console of the project in region 2 to purchase desktops for the employees of group b and manage the desktops of the project in region 2. **Figure 15-1** shows the operation process. For details about how to create an IAM user, see **Creating an IAM User and Assigning Permissions**.

Figure 15-1 Operation process



Workspace Administrator Permissions

You can grant users permissions by using roles and policies. Workspace grants administrator permissions to IAM users by using roles.

By default, new IAM users do not have permissions assigned. You need to add a user to one or more groups, and grant Workspace administrator permissions to these groups. Users inherit permissions from their groups. After authorization, IAM users can perform operations on Workspace resources in the corresponding projects.

Table 15-1 lists all system-defined permissions of Workspace. The **Dependency** column indicates roles on which a Workspace permission depends to take effect. Workspace roles are dependent on the roles of other services because Huawei Cloud services interact with each other. Therefore, when assigning Workspace permissions to a user group, do not deselect other dependent permissions. Otherwise, Workspace permissions do not take effect.

Table 15-1 Workspace permissions

System-defined Permission	Description	Details
Workspace FullAccess	All permissions on Workspace	All permissions on Workspace
Workspace DesktopsManager	Desktop administrator permissions on Workspace	Creating, deleting, and performing operations on a desktop or desktop pool; desktop-related operations, including Internet access, scheduled tasks, App Center, and image management
Workspace UserManager	User administrator permissions on Workspace	User management operations, such as creating users, deleting users, and resetting passwords
Workspace SecurityManager	Security administrator permissions on Workspace	All security-related operations, such as policy management and checking user connection records
Workspace TenantManager	Tenant administrator permissions on Workspace	All tenant configuration functions
Workspace ReadOnlyAccess	Read-only permissions on Workspace	Read-only permissions on Workspace

Table 15-2 lists the permissions to be added for the following operations.

NOTE

For details about the permissions required for Workspace, see **Assigning Permissions to an IAM User** or **Creating a Custom Policy**.

Table 15-2 Additional permissions

Operation	Dependent System-defined Role, Policy, or Custom Policy	Description
BSS-related permissions: Perform yearly/monthly operations, such as purchasing and changing desktops, and switching from pay-per-use to yearly/monthly billing.	The policy must contain the following action permissions: bss:discount:view bss:order:update bss:order:view bss:order:pay bss:renewal:view	Select either the system-defined role or the custom policy.
IAM-related permissions: Perform scheduled tasks, perform operations on desktop pools, and create and query agencies.	**Permissions required for creating and querying agencies:** The policy must contain the following action permissions: iam:roles:getRole iam:roles:listRoles iam:agencies:getAgency iam:agencies:listAgencies iam:agencies:createAgency iam:permissions:listRolesForAgencyOnProject iam:permissions:grantRoleToAgencyOnProject **Permissions required for querying agencies:** The policy must contain the following action permissions: iam:agencies:getAgency iam:agencies:listAgencies iam:permissions:listRolesForAgencyOnProject	When creating an agency, select either the system-defined role Security Administrator or the custom policy. When querying agencies, select either the system-defined policy IAM ReadOnlyAccess or the custom policy.

Operation	Dependent System-defined Role, Policy, or Custom Policy	Description
TMS-related permissions: Query predefined tags during desktop creation.	The policy must contain the following action permissions: tms:predefineTags:list	Select either the system-defined policy or the custom policy.
VPCEP-related permissions: Enable or disable Direct Connect access (required for fine-grained authentication of enterprise projects).	System-defined role: VPCEndpoint Administrator	VPCEP does not support fine-grained authentication of enterprise projects.
VPC-related permissions: Perform desktop-related operations and enable economical Internet access (required for fine-grained authentication of enterprise projects).	IAM project-level permissions System-defined policy: VPC ReadOnlyAccess System-defined role: VPC Administrator	You must have the VPC permission of the enterprise project where the VPC used for enabling Workspace is.
IMS-related permissions: Create an image (required for fine-grained authentication of enterprise projects).	The policy must contain the following action permissions: ims:images:get ims:images:share	IMS does not support fine-grained authentication of enterprise projects.

Once granted permissions on the IAM console, users can perform the following actions (starting, shutting down, and restarting a desktop) only using northbound interfaces (NBIs). They are still not allowed to perform these operations on the Workspace console.

NOTE

Permissions must be granted on actions of startup, shutdown, and restart on the Workspace console:

Permission: performing operations on a desktop

API: **POST/v2/{project_id}/desktops/action**

Action: **workspace:desktops:operate**

Table 15-3 NBI-based permissions

Permission	API	Action
Starting a desktop	POST /v2/{project_id}/desktops/start	workspace:desktops:start

Permission	API	Action
Shutting down a desktop	POST /v2/{project_id}/desktops/stop	workspace:desktops:stop
Restarting a desktop	POST /v2/{project_id}/desktops/reboot	workspace:desktops:reboot

15.2 Creating an IAM User and Granting Permissions to Use Workspace

Scenarios

This section describes how to use **IAM** to implement fine-grained permissions control for your Workspace resources. With IAM, you can:

- Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has their own security credentials, providing access to Workspace cloud desktops.
- Grant only the permissions required for users to perform a specific task.

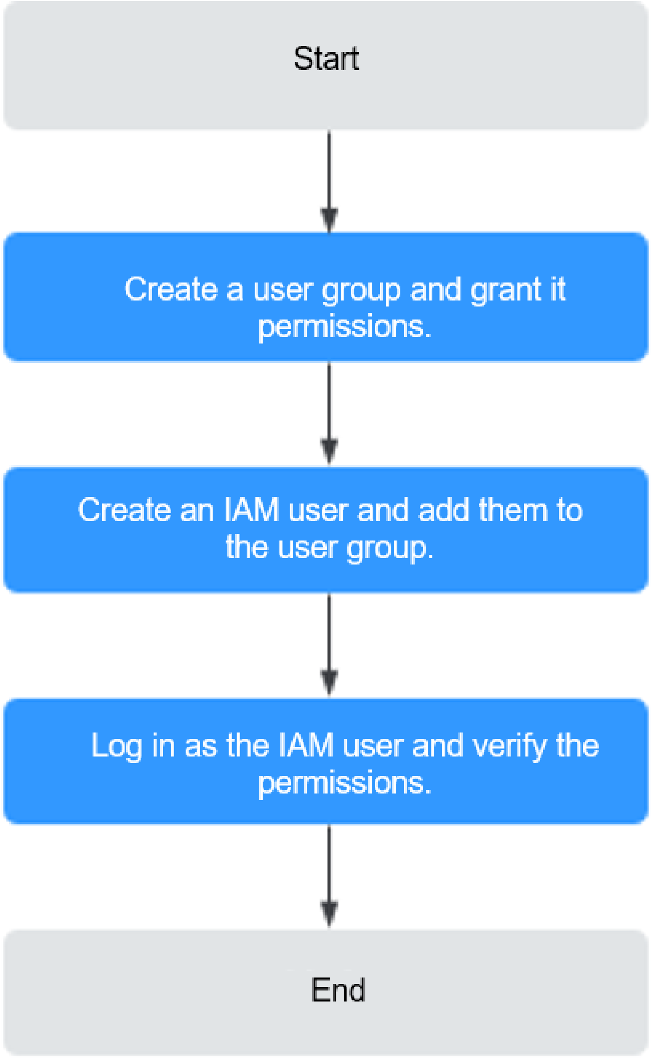
If your Huawei account does not need individual IAM users, you may skip this section.

This section takes the **Workspace ReadOnlyAccess** permission as an example to describe how to grant an IAM user permissions.

Prerequisites

Learn about the permissions supported by Workspace and choose permissions as required. For the system-defined permissions of other services, see **System-defined Permissions**.

Example Process


Start
Create a user group and grant it permissions.
Create an IAM user and add them to the user group.
Log in as the IAM user and verify the permissions.
End

1. **Create a user group and grant it permissions**.

   Create a user group on the IAM console and grant it the **Workspace ReadOnlyAccess** permission.

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

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

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

   Log in to the console as the IAM user, switch to a region where the permission takes effect, and verify the permission (assume that the user has only the **Workspace ReadOnlyAccess** permission).

   – Choose **Service List** > **Workspace**. On the **Desktops** page, perform operations other than query, such as starting, stopping, restarting, creating, modifying, and deleting a desktop.

     Take starting or stopping a desktop as an example. If a message indicating insufficient permissions is displayed, the **Workspace ReadOnlyAccess** permission has taken effect.

   – Choose any other service in the **Service List**, such as **Virtual Private Cloud**. If a message indicating insufficient permissions to access the service is displayed, the **Workspace ReadOnlyAccess** permission has taken effect.

15.3 Workspace Custom Policies

Scenarios

Custom policies can be created to supplement the system-defined permissions of Workspace.

To create a custom policy, choose either visual editor or JSON.

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Create a JSON policy or edit an existing one.

For details about how to create custom policies, see **Creating a Custom Policy**. This section describes examples of common Workspace custom policies.

Example custom policies

- Example 1: Assigning the permissions for desktop startup and shutdown to users.

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "workspace:*:get*",
            "workspace:*:list*",
            "workspace:*:export*",
            "ims:images:get",
            "ims:images:list",
            "ims:quotas:get",
            "nat:natGateways:list",
            "nat:snatRules:list",
            "vpc:bandwidths:list",
            "vpc:networks:get",
            "vpc:ports:get",
            "vpc:publicIps:get",
            "vpc:publicIps:list",
            "vpc:quotas:list",
            "vpc:securityGroupRules:get",
            "vpc:securityGroups:get",
            "vpc:subnets:get",
            "vpc:vpcs:get",
            "vpc:vpcs:list",
            "vpcep:endpoints:get",
            "dss:pools:list",
            "workspace:desktops:operate"
         ]
      }
   ]
}
```

NOTE

workspace:desktops:operate indicates desktop operations (startup, shutdown, restart, and hibernation). Other permissions are read-only and dependent permissions.

15.4 Entrustment Description

Workspace works closely with multiple cloud service resources, such as compute, networking, and images. When you create a scheduled task for recomposing a system disk, create a desktop pool, or send a notification about idle desktops, Workspace automatically requests permissions to access the cloud resources in the region. See the permissions displayed on the page.

After the permission granting is approved, an agency named **workspace_admin_trust** will be created on IAM. To ensure normal service usage, do not delete or modify the **workspace_admin_trust** agency when performing scheduled tasks or using the desktop pool.

workspace_admin_trust agency description:

The **workspace_admin_trust** agency has the permissions as Tenant Administrator. Tenant Administrator has the permissions on all cloud services except IAM and can call the cloud services on which Workspace depends. The delegation takes effect only in the current region.

To use Workspace in multiple regions, you need to request cloud resource permissions in each region. To view the delegation records of each region, go to the IAM console, choose **Agencies**, and click **workspace_admin_trust**.

NOTE

Workspace may malfunction if the Tenant Administrator role is not assigned. Therefore, do not delete or modify the **workspace_admin_trust** agency when using Workspace.

The **workspace_admin_trust** agency may need to be delegated again in the following scenarios:

- The permissions required by Workspace may change with the version. For example, if a new component requires new permissions, Workspace will update the expected permission list. In this case, you need to delegate the **workspace_admin_trust** agency again.
- If you manually change the permissions of the **workspace_admin_trust** agency, and the new permissions of this agency are different from those expected by Workspace, a message is displayed asking you to grant the permissions. If you grant the new permissions, the previous permissions may become invalid.

15.5 Enterprise Projects

Creating an enterprise project

Step 1 Log in to the console.

Step 2 Click **Enterprise** > **Project Management** in the upper right corner.

Step 3 On the **Enterprise Project Management** console, click **Create Enterprise Project**.

NOTE

Enterprise is available on the console only if the enterprise project has been enabled, or the account is the primary account. To enable this function, contact customer service.

Assigning permissions

You can add a user group to an enterprise project and configure a policy to associate the enterprise project with the user group. You can add users to a user group to control projects that users can access and the resources on which users can perform operations. The procedure is as follows:

Step 4 On the **Enterprise Management** console, click the name of an enterprise project to go to the enterprise project details page.

Step 5 On the **Permissions** tab, click **Authorize User Group** to go to the **User Groups** page on the IAM console. Associate the enterprise project with a user group and assign permissions to the group. For details, see **Creating a User Group and Assigning Permissions**.

----End

Associating resources with enterprise projects

To use an enterprise project to manage cloud resources, associate resources with the enterprise project.

- Selecting an enterprise project when subscribing to Workspace

  On the page for subscribing to Workspace, select an enterprise project from the **Enterprise Project** drop-down list.
- Adding resources
  - On the **Enterprise Project Management** page, you can add existing cloud desktops to an enterprise project. For details, see **Resource Management Overview**.
  - **default** indicates the default enterprise project. Resources that are not allocated to any enterprise projects under your account are listed in the default enterprise project.

For details, see **Enterprise Management User Guide**.

16 Data Backup and Restoration

16.1 Backing Up Desktop Data

Scenarios

Workspace uses Cloud Backup and Recovery (CBR) to back up desktop data. CBR protects your workloads by ensuring the security and consistency of your data.

Prerequisites

- Workspace has been subscribed to.
- The administrator has the permission on CBR.

  NOTE

  - By default, a Huawei account has the operation permissions on all Huawei Cloud services.
  - To use CBR, the IAM account created under the Huawei account must be added to the **admin** user group or a user group with CBR operation permissions. Go to the IAM page to check whether the user belongs to the **admin** user group. If not, **grant the IAM account the permission on CBR**.

Procedure

Step 1 For details, see **Creating a Cloud Server Backup** in the *Cloud Backup and Recovery Getting Started*.

NOTE

- A cloud desktop can be backed up only when its status is **Available** or **In-use**. If you have performed operations such as expanding, attaching, detaching, or deleting a desktop, refresh the page first to ensure that the operation is complete and then determine whether to back up the desktop.
- If you delete files on the desktop during the backup, the backup of deleted files may fail. Therefore, to ensure data integrity, you are advised to delete the target data after the current backup is complete and then perform a backup again.

----End

16.2 Restoring Desktop Data

Scenarios

If a cloud desktop malfunctions, you can select a desktop backup in the vault to restore the cloud desktop to the state at a given backup point in time, ensuring normal running of user workloads.

Prerequisites

You have **backed up desktop data**.

Procedure

NOTICE

The historical data at the backup point in time will overwrite the current desktop data. The restoration cannot be undone.

Step 1 **Restore data from a cloud server backup**.

----End

17 Common Function Configuration

17.1 Configuring Cloud Desktops to Access the Internet

Scenarios

After you purchase a cloud desktop, the cloud desktop is in the VPC subnet by default and cannot access the Internet. You need to configure the NAT gateway to share an EIP so that users can access the Internet from the cloud desktop after accessing the cloud desktop. If the cloud desktop has multiple service subnets, the Internet function must be enabled for each service subnet. When a user logs in to a cloud desktop in a subnet for which the Internet is not enabled, the user cannot access the Internet from the desktop.

NOTE

This section describes how to enable Internet access through the pages provided by Workspace for purchasing NAT gateways and EIPs. You can also access the NAT or EIP page to purchase the service to enable the Internet by referring to **How Do I Enable the Internet on Other Cloud Service Pages?**

Prerequisites

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

NOTE

- By default, a Huawei account has the operation permissions on all Huawei Cloud services.
- 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. Go to the IAM page to check whether the user belongs to the **admin** user group. If not, 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 **Creating a User and Granting EIP Permissions**.

Procedure

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

Step 2 Check whether the Internet access address is enabled.

NOTE

After a desktop is purchased, the Internet access address is enabled by default.

1. In the navigation pane on the left, choose **Tenant Configuration** > **Basic Settings**.
2. Check the status of **Internet access address**.
   - If the IP address is displayed, the Internet access address is enabled. Go to **Step 3**.
   - If **Disable** is displayed, the Internet access address is disabled. Click **Enable** and go to **Step 3**.

   NOTE

   After the Internet access address is disabled, you can enable Internet access address again. After the function is enabled again, the IP address changes. You need to notify the desktop user to use the new IP address to access the desktop.

Step 3 Check whether the desktop can access the Internet.

1. In the navigation pane on the left, choose **Desktops** > **Desktops**.
2. On the **Desktops** page, check the **Internet** column of the desired desktop.
   - If the value is **Disabled**, end users cannot access the Internet through cloud desktops. See **9 Internet Access Management** to enable Internet access.
   - If the value is **Enabled**, end users can access the Internet through cloud desktops. In this case, skip subsequent operations.

   NOTE

   - If the current tenant VPC has multiple service subnets and cloud desktops in each service subnet need to access the Internet, enable Internet access for each service subnet by referring to **9 Internet Access Management**.
   - If multiple NAT gateways are created in the same VPC, ensure that the default route in the route table points to all NAT gateways. **Check whether the default route in the route table points to all NAT gateways**. If no, configure this.

Step 4 (Optional) Configure DNS forwarding.

If a Windows AD server is connected, you need to configure DNS domain name resolution on the Windows AD server. For details, see **Step 4.1** to **Step 4.10**. If no Windows AD is connected, skip the following operations.

1. Log in to the DNS server as the administrator.
2. On the taskbar in the lower left corner, click ⊞.
3. Click on the right of the **Start** menu.
4. The **Server Manager** window is displayed.
5. In the navigation pane on the left, click **DNS**.
6. In the **SERVERS** area, right-click a *Server name* and choose **DNS Manager** from the shortcut menu.
7. The **DNS Manager** dialog box is displayed.
8. Expand **DNS**. Right-click the computer name, and choose **Properties** from the shortcut menu.
9. On the **Advanced** tab page, deselect **Disable recursion (also disable forwarders)** and click **Apply**.
10. 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 **What Are Huawei Cloud Private DNS Server Addresses?**

Step 5 Notify end users to use the Internet access address to access cloud desktops.

----End

Follow-up Operations

When a user does not need to access the Internet, see **9.3 Disabling Internet Access** to disable Internet access.

17.2 Configuring Cloud Desktops to Access the Enterprise Intranet

Scenarios

After you purchase a cloud desktop, the cloud desktop is in the VPC subnet by default and cannot access the enterprise intranet. You need to configure Direct Connect or VPN so that users can access the enterprise intranet from the cloud desktop after accessing it.

Prerequisites

You have used Direct Connect to connect the enterprise intranet to the VPC where the cloud desktop resides by referring to **Direct Connect Getting Started**. Alternatively, you have connected the on-premises data center to the VPC where the cloud desktop resides by referring to **VPN Administrator Guide**, for example, **Interconnection with an AR Router of Huawei (Active-Active Connections)**.

Constraints

If a firewall is used, ensure that ports 8443 and 443 in the outbound direction of the firewall are enabled.

Procedure

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

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

Step 3 In the **Network Configuration** area, click **Enable** next to **Direct Connect Access Address**.

Step 4 (Optional) In the displayed dialog box, configure **Direct Connect CIDR Block**.

- Using Direct Connect:
  - Check whether the service subnet of the cloud desktop and the subnet of Direct Connect are in the same range.

    If yes, you do not need to configure the Direct Connect CIDR block.

    If no, you need to configure the Direct Connect CIDR block. You can view the service subnet of the cloud desktop and the subnet CIDR block of Direct Connect on the VPC page.
  - You can configure a maximum of five CIDR blocks. Use semicolons (;) to separate them.
  - An example of CIDR block:

    192.168.11.0/24;172.10.240.0/20
- Using a VPN connection:

  Enter the CIDR block of the on-premises data center to be connected, for example, 10.119.156.0/24. This CIDR block cannot conflict with that of the VPC where the cloud desktop is located.

Step 5 In the **Enabling Direct Connect Access Addresses** dialog box, select **I have confirmed, VPC endpoints need to be created when Direct Connect access is enabled. (Creating VPC endpoints is charged.)**.

Step 6 Click **OK**.

Step 7 Notify end users to use the Direct Connect access address to access cloud desktops.

----End

17.3 Configuring Network Connection Between Cloud Desktops and Windows AD

Scenarios

When the Windows AD is deployed on the enterprise intranet or in the same VPC as the cloud desktop, if the cloud desktop uses the Windows AD for authentication, you need to configure the network connection between the cloud desktop and the Windows AD.

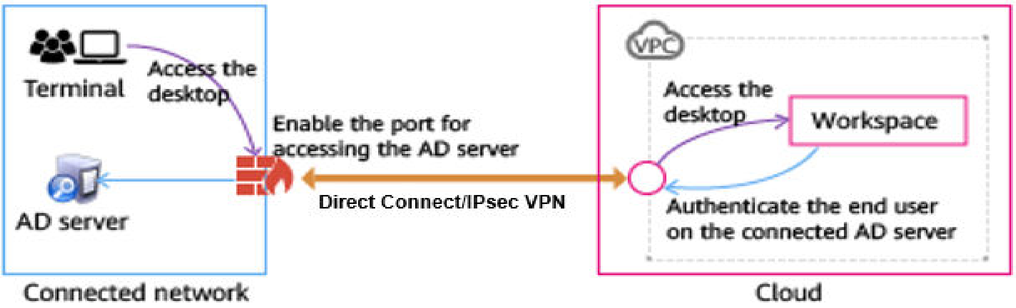
Prerequisites

You have obtained the domain administrator account and password.

Procedure

Scenario 1: Deploying the Windows AD in the customer's data center intranet

Figure 17-1 Deploying the Windows AD in the customer's data center intranet



Step 1 Use Direct Connect or IPsec VPN to connect the customer data center to the VPC. For details, see **Direct Connect Getting Started** or **VPN Administrator Guide**.

Step 2 If a firewall is deployed between the Windows AD and the cloud desktop, enable the following ports on the firewall for successful connection, as shown in **Table 17-1**.

Table 17-1 Port list

Role	Port	Agreement	Description
AD	135	TCP	Port for the Remote Procedure Call (RPC) protocol (LDAP, DFS, and DFSR)
	137	UDP	Port for NetBIOS name resolution (network login service)
	138	UDP	Port for the NetBIOS data gram service (DFS and network login service)
	139	TCP	Port for the NetBIOS-SSN service (network basic input/output)
	445	TCP	Port for the NetBIOS-SSN service (network basic input/output)
	445	UDP	Port for the NetBIOS-SSN service (network basic input/output)

Role	Port	Agreement	Description
	49152-65535	TCP	RPC dynamic port (This port is not hardened and opened on AD. If it is hardened on AD, ports 50152 to 51151 need to be enabled.)
	49152-65535	UDP	RPC dynamic port (This port is not hardened and opened on AD. If it is hardened on AD, ports 50152 to 51151 need to be enabled.)
	88	TCP	Kerberos key distribution center service
	88	UDP	Kerberos key distribution center service
	123	UDP	NTP service
	389	UDP	LDAP server
	389	TCP	LDAP server
	464	TCP	Kerberos authentication protocol
	464	UDP	Kerberos authentication protocol
	500	UDP	isakmp
	593	TCP	RPC over HTTP
	636	TCP	LDAP SSL
DNS	53	TCP	DNS server
	53	UDP	DNS server

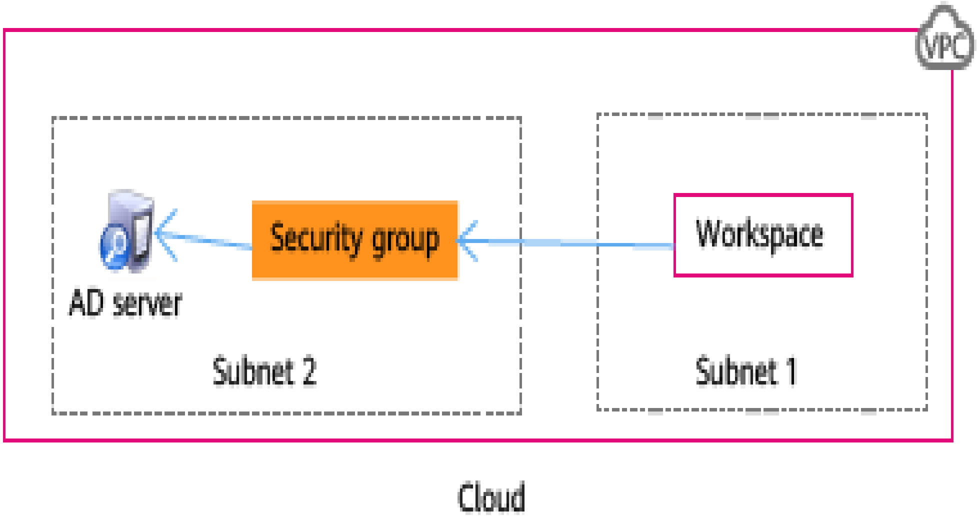
Step 3 After the configuration is complete, check whether the networks and ports are working properly by referring to **Verification Methods**.

----End

Scenario 2: Deploying the Windows AD in another subnet of the VPC where the cloud desktop is located

In this scenario, you need to add security group rules for the Windows AD and open some ports of the Windows AD to the cloud desktop so that the cloud desktop can connect to the Windows AD.

Figure 17-2 Deploying the Windows AD in another subnet of the VPC where the cloud desktop is located



Step 1 Create a security group in the VPC. For details, see **Creating a Security Group**.

Step 2 Add an inbound rule. For details, see **Adding a Security Group Rule**.

Step 3 After the security group is created, apply the security group to the Windows AD management server so that the cloud desktop can communicate with the Windows AD.

NOTE

To minimize the number of open ports and protocols, you can add multiple inbound rules to a security group and enable only the ports and protocols listed in **Table 17-1**.

Step 4 After the configuration is complete, check whether the networks and ports are working properly by referring to **Verification Methods**.

----End

Verification Methods

Step 1 Check the firewall or security group settings of the AD server and ensure that ports in **Table 17-1** are enabled.

NOTE

For details about the port requirements of the Windows AD server, see **Active Directory and Active Directory Domain Services Port Requirements**.

Step 2 Use the ECS service to create a Windows OS instance in the VPC where the user desktop is located and add the instance to an existing domain.

NOTE

For details about ECS configurations and operations, see **ECS User Guide**. Use the RDP client tool (such as **mstsc**) or VNC to log in to the Windows instance.

Step 3 Use an RDP client tool (such as **mstsc**), or VNC to log in to the Windows instance.

1. Download **ADTest.zip** to the Windows instance and decompress it.
2. Press **Shift** and right-click the blank area of the folder where **ADTest.exe** is located, and choose **Open command windows here** from the shortcut menu.
3. In the displayed CLI, run the following command to check the connectivity of the Windows AD management server:

   ADTest.exe -file ADTest.cfg -ip *IP address of the Windows AD* **-domain** *Domain name of the Windows AD* **-user** *Domain administrator account*

   In this example, run the following command:

   ADTest.exe -file ADTest.cfg -ip ***192.168.161.78*** **-domain** ***abc.com*** **-user** ***vdsadmin***
4. Enter the password of user **vdsadmin**.
5. Check whether all the returned test results are **SUCCEEDED**. If **FAILED** is displayed, check the AD management server configurations or firewall ports as prompted.

----End

18 Monitoring

18.1 Workspace O&M Monitoring Metrics

Functions

Table 18-1 describes the O&M monitoring metrics of Workspace.

Table 18-1 O&M monitoring metrics of Workspace

Metric ID	Metrics Name	Description	Dimension	Example Value (By Dimension)	Statistical Type (Calculation Method of the Return Value Queried by the / metric Interface)	Statistical Period	Max Query Time Range	Max Data Retention Duration	Metric Usage
desktopUsage	Desktop usage	Proportion of the number of used desktops to the total number of desktops. Unit: percentage (%)	Project	No need to transfer value separately	Average value	1 hour or 1 day	30 days	180 days	Metric query supported
dailyUserOnlineRate	Daily user usage	User usage within a specified period. Unit: percentage (%)	Project	No need to transfer value separately	Average value	1 day	30 days	180 days	Metric query supported

Metric ID	Metrics Name	Description	Dimension	Example Value (By Dimension)	Statistical Type (Calculation Method of the Return Value Queried by the / metric Interface)	Statistical Period	Max Query Time Range	Max Data Retention Duration	Metric Usage
desktopUseNumber	Number of used desktops	Number of desktops used in a specified period. Statistics of each desktop are collected only once. Unit: per desktop	Project	No need to transfer value separately	Latest value	1 hour or 1 day	30 days	180 days	Metric query supported
desktop_num_per_project	Total number of desktops	Total number of desktops in a project. Unit: per desktop	Project	No need to transfer value separately	Latest value	1 hour or 1 day	30 days	180 days	Metric query supported

Metric ID	Metrics Name	Description	Dimension	Example Value (By Dimension)	Statistical Type (Calculation Method of the Return Value Queried by the / metric Interface)	Statistical Period	Max Query Time Range	Max Data Retention Duration	Metric Usage
excellent_network_rtt_num	Number of sessions with excellent network performance	Number of sessions whose network latency is within 30 ms. Unit: per session	Project	No need to transfer value separately	Latest value	1 hour	30 days	180 days	Metric trend query supported
good_network_rtt_num	Number of sessions with good network performance	Number of sessions whose network latency is between 31 to 50 ms. Unit: per session	Project	No need to transfer value separately	Latest value	1 hour	30 days	180 days	Metric trend query supported

Metric ID	Metrics Name	Description	Dimension	Example Value (By Dimension)	Statistical Type (Calculation Method of the Return Value Queried by the / metric Interface)	Statistical Period	Max Query Time Range	Max Data Retention Duration	Metric Usage
average_network_rtt_num	Number of sessions with average network performance	Number of sessions whose network latency is between 51 to 100 ms. Unit: per session	Project	No need to transfer value separately	Latest value	1 hour	30 days	180 days	Metric trend query supported
poor_network_rtt_num	Number of sessions with poor network performance	Number of sessions whose network latency is higher than 100 ms. Unit: per session	Project	No need to transfer value separately	Latest value	1 hour	30 days	180 days	Metric trend query supported

Metric ID	Metrics Name	Description	Dimension	Example Value (By Dimension)	Statistical Type (Calculation Method of the Return Value Queried by the / metric Interface)	Statistical Period	Max Query Time Range	Max Data Retention Duration	Metric Usage
up_bandwidth	Uplink traffic	Traffic sent when using cloud desktops. Unit: byte	Login session	dim.0=transaction_id,TID-15171242896-1ca01b00014641e	Session-level metrics do not have statistics. Only the trend can be viewed.	1 minute	7 days	7 days	Metric trend query supported
down_bandwidth	Downlink traffic	Traffic received when using cloud desktops. Unit: byte	Login session	dim.0=transaction_id,TID-15171242896-1ca01b00014641e	Session-level metrics do not have statistics. Only the trend can be viewed.	1 minute	7 days	7 days	Metric trend query supported

Metric ID	Metrics Name	Description	Dimension	Example Value (By Dimension)	Statistical Type (Calculation Method of the Return Value Queried by the / metric Interface)	Statistical Period	Max Query Time Range	Max Data Retention Duration	Metric Usage
network_rtt	Network latency	Data transmission latency when using cloud desktops. Unit: ms	Login session	dim.0=transaction_id,TID-15171242896-1ca01b00014641e	Session-level metrics do not have statistics. Only the trend can be viewed.	1 minute	7 days	7 days	Metric trend query supported
network_jitter	Network jitter	Time difference between the maximum network latency and the minimum network latency when using cloud desktops. Unit: ms	Login session	dim.0=transaction_id,TID-15171242896-1ca01b00014641e	Session-level metrics do not have statistics. Only the trend can be viewed.	1 minute	7 days	7 days	Metric trend query supported

Metric ID	Metrics Name	Description	Dimension	Example Value (By Dimension)	Statistical Type (Calculation Method of the Return Value Queried by the / metric Interface)	Statistical Period	Max Query Time Range	Max Data Retention Duration	Metric Usage
network_loss	Network packet loss rate	Ratio of the number of lost packets to the number of sent packets during the network test. Unit: percentage (%)	Login session	dim.0=transaction_id,TID-15171242896-1ca01b00014641e	Session-level metrics do not have statistics. Only the trend can be viewed.	1 minute	7 days	7 days	Metric trend query supported

18.2 Monitoring Metrics Reported by Workspace to Cloud Eye

Functions

This section describes the monitoring metrics reported by Workspace to Cloud Eye and defines the namespace for the metrics. You can use Cloud Eye to query metrics and alarms generated by Workspace.

Namespaces

SYS.Workspace

Supported Metrics

The supported metrics vary with desktop OSs. See **Table 18-2**. (√: supported; x: unsupported)

Table 18-2 Workspace monitoring metrics

Metric	Windows	Linux
CPU Usage	√	√
Memory Usage	√	x
Disk Usage	√	x
Disk Read Bandwidth	√	√
Disk Write Bandwidth	√	√
Disk Read IOPS	√	√
Disk Write IOPS	√	√
Inband Incoming Rate	√	x
Inband Outgoing Rate	√	x
Outband Incoming Rate	√	√
Outband Outgoing Rate	√	√

Table 18-3 describes these metrics.

Table 18-3 Monitoring metrics supported by Workspace

Metric ID	Metrics Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Interval (Raw Data)
cpu_util	CPU Usage	This metric is used to show the CPU usage of a desktop. Formula: CPU usage of a desktop/ Number of vCPUs in the desktop	0-100	%	N/A	Cloud desktop	5 min

Metric ID	Metrics Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Interval (Raw Data)
mem_util	Memory Usage	This metric is used to show the memory usage of a desktop. Formula: Used memory of a desktop/Total memory of the desktop	0-100	%	N/A	Cloud desktop	5 min
disk_util_inband	Disk Usage	This metric is used to show the disk usage of a desktop. Formula: Used disk capacity of a desktop/Total disk capacity of the desktop	0-100	%	N/A	Cloud desktop	5 min
disk_read_bytes_rate	Disk Read Bandwidth	This metric is used to show the data volume read from a desktop per second. Formula: Total number of bytes read from a desktop disk/ Monitoring interval byte_out = (rd_bytes - last_rd_bytes)/ Time difference	≥ 0	Byte/s	1024(IEC)	Cloud desktop	5 min

Metric ID	Metrics Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Interval (Raw Data)
disk_write_bytes_rate	Disk Write Bandwidth	This metric is used to show the data volume written to a desktop per second. Formula: Total number of bytes written to a desktop disk/ Monitoring interval	≥ 0	Byte/s	1024(IEC)	Cloud desktop	5 min
disk_read_requests_rate	Disk Read IOPS	This metric is used to show the number of read requests sent to a desktop per second. Formula: Total number of read requests sent to a desktop/ Monitoring interval req_out = (rd_req - last_rd_req)/ Time difference	≥ 0	Request/s	N/A	Cloud desktop	5 min

Metric ID	Metrics Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Interval (Raw Data)
disk_write_requests_rate	Disk Write IOPS	This metric is used to show the number of write requests sent to a desktop per second. Formula: Total number of write requests sent to a desktop/ Monitoring interval req_in = (wr_req - last_wr_req)/ Time difference	≥ 0	Request/s	N/A	Cloud desktop	5 min
network_incoming_bytes_rate_inband	Inband Incoming Rate	This metric is used to show the number of incoming bytes on a desktop per second. Formula: Total number of inband incoming bytes on a desktop/ Monitoring interval	≥ 0	Byte/s	1024(IEC)	Cloud desktop	5 min

Metric ID	Metrics Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Interval (Raw Data)
network_outgoing_bytes_rate_inband	Inband Outgoing Rate	This metric is used to show the number of outgoing bytes on a desktop per second. Formula: Total number of inband outgoing bytes on a desktop/ Monitoring interval	≥ 0	Byte/s	1024(IEC)	Cloud desktop	5 min
network_incoming_bytes_aggregate_rate	Outband Incoming Rate	This metric is used to show the number of incoming bytes on a desktop per second on the hypervisor. Formula: Total number of outband incoming bytes on a desktop/ Monitoring interval	≥ 0	Byte/s	1024(IEC)	Cloud desktop	5 min
network_outgoing_bytes_aggregate_rate	Outband Outgoing Rate	This metric is used to show the number of outgoing bytes on a desktop per second on the hypervisor. Formula: Total number of outband outgoing bytes on a desktop/ Monitoring interval	≥ 0	Byte/s	1024(IEC)	Cloud desktop	5 min

Dimensions

Key	Value
instance_id	Desktop ID

18.3 Cloud Eye OS Monitoring Metrics Supported by Workspace (with Agent Installed)

Functions

You can install the Agent plug-in on a desktop to provide system-level, proactive, and fine-grained monitoring of servers. This section describes the OS monitoring metrics reported by Workspace to Cloud Eye.

GPU monitoring metrics are supported.

OS monitoring supports metrics about CPU, CPU load, memory, disk, disk I/O, file system, NIC, TCP, and GPU.

After installing the Agent, you can view OS monitoring metrics of ECSs running different OSs. Monitoring data is collected every one minute.

- **OS monitoring metrics: CPU**

Table 18-4 CPU monitoring metrics

Metric	Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Period (Raw Data)
cpu_usage	(Agent) CPU Usage	CPU usage of the monitored object. ● Linux: Check metric value changes in file **/proc/stat** in a collection period. Run the **top** command to check the **%Cpu(s)** value. ● Windows: Obtain the metric value using the Windows API **GetSystemTimes**.	0-100	%	N/A	Cloud desktop	1 minute

- **OS monitoring metrics: Memory**

Table 18-5 Memory monitoring metrics

Metric	Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Period (Raw Data)
mem_usedPercent	(Agent) Memory Usage	Memory usage of the monitored object. ● Linux: Obtain the metric value from the **/proc/meminfo** file: (**MemTotal** - **MemAvailable**)/**MemTotal** – If **MemAvailable** is displayed in **/proc/meminfo**, **MemUsedPercent** = (**MemTotal** - **MemAvailable**)/**MemTotal** – If **MemAvailable** is not displayed in **/proc/meminfo**, **MemUsedPercent** = (**MemTotal** – **MemFree** – **Buffers** – **Cached**)/**MemTotal** ● Windows: The calculation formula is as follows: Used memory size/	0-100	%	N/A	Cloud desktop	1 minute

Metric	Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Period (Raw Data)
		Total memory size x 100%.					

- **OS monitoring metrics: NIC**

Table 18-6 NIC monitoring metrics

Metric	Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Period (Raw Data)
net_bitRecv	(Agent) Outbound Bandwidth	Number of bits sent by this NIC per second. ● Linux: Check metric value changes in file **/proc/net/dev** in a collection period. ● Windows: Use the MibIfRow object in the WMI to obtain network metric data.	≥ 0	bit/s	1024(IEC)	Cloud desktop	1 minute

Metric	Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Period (Raw Data)
net_bitSent	(Agent) Inbound Bandwidth	Number of bits received by this NIC per second. ● Linux: Check metric value changes in file **/proc/net/dev** in a collection period. ● Windows: Use the MibIfRow object in the WMI to obtain network metric data.	≥ 0	bit/s	1024(IEC)	Cloud desktop	1 minute
net_packetRecv	(Agent) NIC Packet Receive Rate	Number of packets received by this NIC per second. ● Linux: Check metric value changes in file **/proc/net/dev** in a collection period. ● Windows: Use the MibIfRow object in the WMI to obtain network metric data.	≥ 0	Counts/s	N/A	Cloud desktop	1 minute

Metric	Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Period (Raw Data)
net_packetSent	(Agent) NIC Packet Send Rate	Number of packets sent by this NIC per second. ● Linux: Check metric value changes in file **/proc/net/dev** in a collection period. ● Windows: Use the MibIfRow object in the WMI to obtain network metric data.	≥ 0	Counts/s	N/A	Cloud desktop	1 minute

- **OS monitoring metric: Disk**

Table 18-7 Disk monitoring metrics

Metric	Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Period (Raw Data)
disk_free	(Agent) Available Disk Space	Available disk space on the monitored object. ● Linux: Run the **df -h** command to check the value in the **Avail** column. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~). ● Windows: Obtain the metric value using the WMI API **GetDiskFreeSpaceExW**. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).	≥0	GB	N/A	Cloud desktop	1 minute

Metric	Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Period (Raw Data)
disk_usedPercent	(Agent) Disk Usage	Percentage of total disk space that is used, which is calculated as follows: **Disk Usage** = **Used Disk Space**/**Disk Storage Capacity**. ● Linux: Obtain the metric value using the following formula: **Disk Usage** = **Used Disk Space**/ **Disk Capacity**. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~). ● Windows: Obtain the metric value using the WMI API **GetDiskFreeSpaceExW**. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only	0-100	%	N/A	Cloud desktop	1 minute

Metric	Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Period (Raw Data)
		digits, letters, hyphens (-), periods (.), and swung dashes (~).					

- **OS monitoring metric: File system**

Table 18-8 File system monitoring metrics

Metric	Name	Description	Value Range	Unit	Metric	Monitored Object (Dimension)	Monitoring Period (Raw Data)
disk_inodesUsedPercent	(Agent) Percentage of Total inode Used	Percentage of used inodes on the disk of the monitored object. Linux: Run the **df -i** command to check the value in the **IUse%** column. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).	0-100	%	N/A	Cloud desktop	1 minute

- **OS monitoring metric: Disk I/O**

Table 18-9 Disk I/O monitoring metrics

Metric	Name	Description	Value Range	Unit	Metric	Monitored Object (Dimension)	Monitoring Period (Raw Data)
disk_ioUtils	(Agent) Disk I/O Usage	Disk I/O usage of the monitored object. ● Linux: The disk I/O usage is calculated based on the data changes in the thirteenth column of the corresponding device in file **/proc/diskstats** in a collection period. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~). ● Windows does not support this metric.	0-100	%	N/A	Cloud desktop	1 minute

- **OS monitoring metric: GPU**

Table 18-10 GPU monitoring metrics

Metric	Name	Description	Value Range	Unit	Metric	Monitored Object (Dimension)	Monitoring Period (Raw Data)
gpu_aggregate_correctable	Aggregate Correctable ECC Errors	Aggregate correctable ECC errors on the GPU. ● Linux: Obtain the metric value using the **libnvidia-ml.so.1** library file of the GPU. ● Windows: Obtain the metric value using the **nvml.dll** library of the GPU.	≥ 0	count	N/A	Cloud desktop	1 minute
gpu_aggregate_uncorrectable	Aggregate Uncorrectable ECC Errors	Aggregate uncorrectable ECC errors on the GPU. ● Linux: Obtain the metric value using the **libnvidia-ml.so.1** library file of the GPU. ● Windows: Obtain the metric value using the **nvml.dll** library of the GPU.	≥ 0	count	N/A	Cloud desktop	1 minute

Metric	Name	Description	Value Range	Unit	Metric	Monitored Object (Dimension)	Monitoring Period (Raw Data)
gpu_performance_state	(Agent) Performance Status	GPU performance of the monitored object. Unit: none - Linux: Obtain the metric value using the **libnvidia-ml.so.1** library file of the GPU. - Windows: Obtain the metric value using the **nvml.dll** library of the GPU.	P0-P15, P32 - **P0**: indicates the maximum performance status	N/A	N/A	Cloud desktop	1 minute

Metric	Name	Description	Value Range	Unit	Metric	Monitored Object (Dimension)	Monitoring Period (Raw Data)
			- **P15**: indicates the minimum performance status - **P32**: i				

Metric	Name	Description	Value Range	Unit	Metric	Monitored Object (Dimension)	Monitoring Period (Raw Data)
			ndicates the unknown performance status				

Metric	Name	Description	Value Range	Unit	Metric	Monitored Object (Dimension)	Monitoring Period (Raw Data)
gpu_retired_page_double_bit	Retired Page Double Bit Errors	Number of retired page double-bit errors, which indicates the number of double-bit pages blocked by the GPU ● Linux: Obtain the metric value using the **libnvidia-ml.so.1** library file of the GPU. ● Windows: Obtain the metric value using the **nvml.dll** library of the GPU.	≥ 0	count	N/A	Cloud desktop	1 minute
gpu_retired_page_single_bit	Retired Page Single Bit Errors	Number of retired page single-bit errors, which indicates the number of single-bit pages blocked by the GPU. Unit: count ● Linux: Obtain the metric value using the **libnvidia-ml.so.1** library file of the GPU. ● Windows: Obtain the metric value using the **nvml.dll** library of the GPU.	≥ 0	count	N/A	Cloud desktop	1 minute

Metric	Name	Description	Value Range	Unit	Metric	Monitored Object (Dimension)	Monitoring Period (Raw Data)
gpu_status	GPU Health Status	Overall measurement of the GPU health. Unit: none ● Linux: Obtain the metric value using the **libnvidia-ml.so.1** library file of the GPU. ● Windows: Obtain the metric value using the **nvml.dll** library of the GPU.	● **0**: healthy ● **1**: subhealthy ● **2**: faulty	N/A	N/A	Cloud desktop	1 minute

Metric	Name	Description	Value Range	Unit	Metric	Monitored Object (Dimension)	Monitoring Period (Raw Data)
gpu_usage_decoder	Decoding Usage	Decoding capability usage of the GPU. ● Linux: Obtain the metric value using the **libnvidia-ml.so.1** library file of the GPU. ● Windows: Obtain the metric value using the **nvml.dll** library of the GPU.	0-100	%	N/A	Cloud desktop	1 minute
gpu_usage_encoder	Encoding Usage	Encoding capability usage of the GPU. ● Linux: Obtain the metric value using the **libnvidia-ml.so.1** library file of the GPU. ● Windows: Obtain the metric value using the **nvml.dll** library of the GPU.	0-100	%	N/A	Cloud desktop	1 minute

Metric	Name	Description	Value Range	Unit	Metric	Monitored Object (Dimension)	Monitoring Period (Raw Data)
gpu_usage_gpu	(Agent) GPU Usage	GPU usage of the monitored object. ● Linux: Obtain the metric value using the **libnvidia-ml.so.1** library file of the GPU. ● Windows: Obtain the metric value using the **nvml.dll** library of the GPU.	0-100	%	N/A	Cloud desktop	1 minute
gpu_usage_mem	(Agent) GPU Memory Usage	GPU memory usage of the monitored object. Unit: % ● Linux: Obtain the metric value using the **libnvidia-ml.so.1** library file of the GPU. ● Windows: Obtain the metric value using the **nvml.dll** library of the GPU.	0-100	%	N/A	Cloud desktop	1 minute

Metric	Name	Description	Value Range	Unit	Metric	Monitored Object (Dimension)	Monitoring Period (Raw Data)
gpu_volatile_correctable	Volatile Correctable ECC Errors	Number of correctable ECC errors since the GPU is reset. The value is reset to **0** each time the GPU is reset. ● Linux: Obtain the metric value using the **libnvidia-ml.so.1** library file of the GPU. ● Windows: Obtain the metric value using the **nvml.dll** library of the GPU.	≥ 0	count	N/A	Cloud desktop	1 minute
gpu_volatile_uncorrectable	Volatile Uncorrectable ECC Errors	Number of uncorrectable ECC errors since the GPU is reset. The value is reset to **0** each time the GPU is reset. ● Linux: Obtain the metric value using the **libnvidia-ml.so.1** library file of the GPU. ● Windows: Obtain the metric value using the **nvml.dll** library of the GPU.	≥ 0	count	N/A	Cloud desktop	1 minute

- **OS monitoring metric: CPU load**

Table 18-11 CPU load monitoring metrics

Metric	Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Period (Raw Data)
load_average1	(Agent) 1-Minute Load Average	CPU load averaged from the last one minute. Linux: Obtain the metric value from the number of logic CPUs in **load1/** in file **/proc/loadavg**. You can run the **top** command to check the value of **load1**.	≥ 0	N/A	N/A	Cloud desktop	1 minute
load_average5	(Agent) 5-Minute Load Average	CPU load averaged from the last five minutes. Linux: Obtain the metric value from the number of logic CPUs in **load5/** in file **/proc/loadavg**. You can run the **top** command to check the value of **load5**.	≥ 0	N/A	N/A	Cloud desktop	1 minute
load_average15	(Agent) 15-Minute Load Average	CPU load averaged from the last 15 minutes. Linux: Obtain the metric value from the number of logic CPUs in **load15/** in file **/proc/loadavg**. You can run the **top** command to check the value of **load15**.	≥ 0	N/A	N/A	Cloud desktop	1 minute

- **OS monitoring metric: TCP**

Table 18-12 TCP monitoring metrics

Metric	Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Period (Raw Data)
net_tcp_total	(Agent) TCP TOTAL	Total number of TCP connections in all statuses. ● Linux: Obtain TCP connections in all statuses from the **/proc/net/tcp** file, and then collect the number of connections in each status. ● Windows: Obtain the metric value using the Windows API **GetTcpTable2**.	≥ 0	Count	N/A	Cloud desktop	1 minute
net_tcp_established	(Agent) TCP ESTABLISHED	Number of TCP connections in the **ESTABLISHED** status. ● Linux: Obtain TCP connections in all statuses from the **/proc/net/tcp** file, and then collect the number of connections in each status. ● Windows: Obtain the metric value using the Windows API **GetTcpTable2**.	≥ 0	Count	N/A	Cloud desktop	1 minute

18.4 Cloud Eye Events Supported by Workspace

Functions

The Cloud Eye event monitoring supported by Workspace provides event data reporting, query, and alarm reporting. When there are specified events, you will receive alarm notifications from Cloud Eye.

Namespaces

SYS.Workspace

Monitored Events

Table 18-13 Events monitored by Workspace

Event Name	Event ID	Event Severity	Event Description	Handling Suggestion	Impact
Abnormal desktop heartbeat	desktopStatusAbnormal	Major	The network is disconnected or the key is lost.	1. Restart the desktop. 2. Check whether the desktop time is the current time. If not, change the desktop time to the current time. 3. Check whether special security software or network connection software is installed on the desktop. If yes, uninstall the software and restart the system. Alternatively, uninstall the software, reinstall the AccessAgent, and restart the system.	The desktop cannot be accessed.

Event Name	Event ID	Event Severity	Event Description	Handling Suggestion	Impact
Failure of assigning desktops in a desktop pool	desktopPoolAssignFailed	Major	This fault is caused by policies.	1. Adjust the desktop pool policy to ensure that there are idle desktops in the desktop pool or desktops can be automatically created. 2. If Linux desktops cannot be assigned to users with digit-only usernames, enable the username prefix function.	New desktops cannot be assigned.
Desktop access failure	desktopAccessFailed	Major	This fault is caused by VM shutdown and restart, access gateway exceptions, or network faults.	1. If you shut down or restart a VM, wait for a period of time and try again when the desktop status is normal. 2. Check the network environment and reconnect to the network when the network is normal.	The desktop cannot be accessed.

Event Name	Event ID	Event Severity	Event Description	Handling Suggestion	Impact
Desktop startup failure	desktopStartFailed	Major	Underlying resources are insufficient.	Wait for a while and try again.	The desktop cannot be accessed.
Failure of automatic desktop pool capacity expansion	desktopPoolExpandFailed	Major	The instance quota or underlying resources are insufficient.	1. If the quota is insufficient, request a higher quota (such as the number of desktops, CPUs, memory, and VPCs). 2. If underlying resources are insufficient, make purchases in the next capacity expansion period. 3. If automatic desktop capacity expansion is not required, disable the function of automatic desktop pool capacity expansion.	Desktop capacity cannot be expanded.

Event Name	Event ID	Event Severity	Event Description	Handling Suggestion	Impact
Failure of migrating a desktop running on a dedicated host	desktopMigrateFailed	Major	The host malfunctions.	1. Replace the faulty host with a normal one. 2. Contact technical support to rectify the host fault.	No dedicated host is available for desktop scheduling.
Login failure	userLoginFailed	Major	The client network is disconnected, or the enterprise ID, username, or password is invalid.	1. Check the network environment and reconnect to the network when the network is normal. 2. Check whether the enterprise ID, username, and password are valid.	The desktop or applications cannot be used.
Bypassing controlled applications	appRestrictFailed	Major	The application control agent is continuously killed.	Check whether a script is used to continuously kill the application control agent.	Application control failed.
Abnormal agent process	agentAbnormal	Major	The agent process has been killed or reset.	The agent process can be automatically restarted after being killed.	Functions such as application control and upgrade will be affected.

19 Subscribing to an Event

Scenarios

Configure SMN to obtain desktop status information in a timely manner, such as desktop creation, creation failure, startup, startup failure, shutdown, shutdown failure, and deletion failure, and report the information to Cloud Trace Service (CTS) to improve the desktop access speed and operation accuracy.

NOTE

Event notifications may cause message queue blocking or failure of calling CTS, so users cannot solely depend on event notifications. Instead, they need to periodically call APIs to update data. For any questions, **submit a service ticket** for technical support.

Procedure

Configuring a subscription event

Step 1 Enable CTS.

NOTE

Enabling CTS will automatically create a system tracker for your use.

Step 2 Create an SMN topic.

Step 3 Add a subscription.

Step 4 Configure key event notifications.

NOTE

Configure parameters for key event notifications as follows.

- **Notification Name**: This parameter is user-defined, for example, keyOperate_Workspace.
- **Operation**: Select **Custom**. In the operation list, set **Select Service** to **Workspace**, **Select Resource** to **workspace**, and **Select Operation** to **createDesktops**, **stopDesktops**, **startDesktops**, or **deleteDesktops**.
- **User**: Not specified.
- **Send Notification**: **Yes**
- **Topic**: Select the topic created in 2.

Verifying the subscription event

NOTE

- Events (including desktop creation, startup, and shutdown; failure of creating, starting, stopping, or deleting a desktop) are automatically reported to CTS. You will receive a message based on the protocol configured in 3. For example, if you select email, you will receive a notification email.
- You can also view all traces on the CTS console.

Step 5 Log in to the console.

Step 6 Click **Service List** and choose **Management & Governance** > **Cloud Trace Service**.

Step 7 Choose **Trace List**. On the **Trace List** page, set **Trace Source** to **Workspace**, **Resource Type** to **Workspace**, and **Filter By** to **Trace Name**.

NOTE

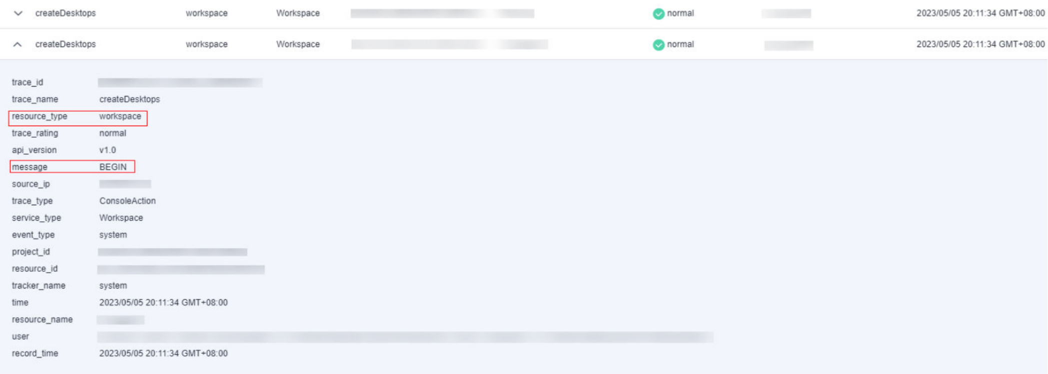
Traces are classified into the following types:

- **createDesktops**: creates a desktop
- **stopDesktops**: stops a desktop
- **startDesktops**: starts a desktop
- **deleteDesktops**: deletes a desktop

Step 8 Click **Query**.

Step 9 Take desktop purchase as an example. View the desktop purchase trace and start the purchase, as shown in **Figure 19-1**.

Figure 19-1 Starting the purchase

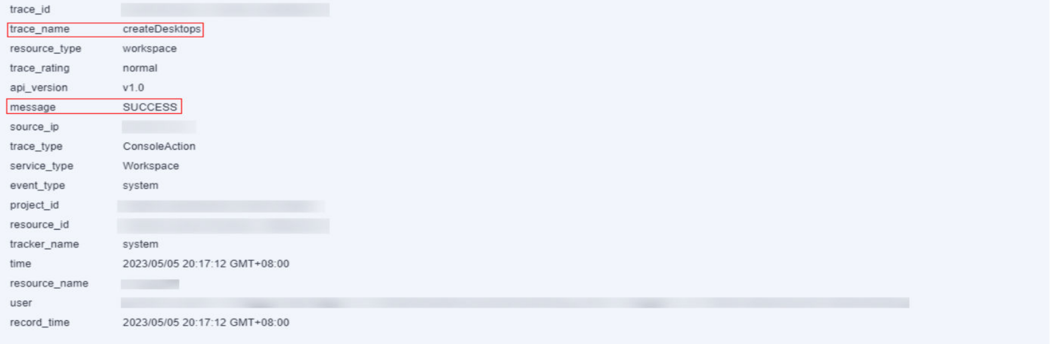


createDesktops	workspace	Workspace	[redacted]	normal	[redacted]	2023/05/05 20:11:34 GMT+08:00
createDesktops	workspace	Workspace	[redacted]	normal	[redacted]	2023/05/05 20:11:34 GMT+08:00

trace_id	[redacted]
trace_name	createDesktops
resource_type	workspace
trace_rating	normal
api_version	v1.0
message	BEGIN
source_ip	[redacted]
trace_type	ConsoleAction
service_type	Workspace
event_type	system
project_id	[redacted]
resource_id	[redacted]
tracker_name	system
time	2023/05/05 20:11:34 GMT+08:00
resource_name	[redacted]
user	[redacted]
record_time	2023/05/05 20:11:34 GMT+08:00

View the desktop purchase trace to complete the purchase, as shown in **Figure 19-2**.

Figure 19-2 Completing the purchase



trace_id	[redacted]
trace_name	createDesktops
resource_type	workspace
trace_rating	normal
api_version	v1.0
message	SUCCESS
source_ip	[redacted]
trace_type	ConsoleAction
service_type	Workspace
event_type	system
project_id	[redacted]
resource_id	[redacted]
tracker_name	system
time	2023/05/05 20:17:12 GMT+08:00
resource_name	[redacted]
user	[redacted]
record_time	2023/05/05 20:17:12 GMT+08:00

NOTE

- When desktop purchase or deletion fails, a failure trace is reported. In the trace details, the value of **Message** is **FAILED**.
- If the desktop is stopped, the **BEGIN** message is not reported by CTS. Only the message indicating that the desktop has been stopped will be reported.
- Three minutes after the desktop is started, if the login status of the desktop is not **Ready** on the desktop management page, a timeout trace is reported. In the trace details, the value of **Message** is **TIMEOUT**.
- Three minutes after the desktop is stopped, if the login status of the desktop is not **Stopped** on the desktop management page, a timeout trace is reported. In the trace details, the value of **Message** is **TIMEOUT**.

----End