06 Workspace User Guide (Administrator)

Issue 01

Date 2023-11-22

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: https://www.huawei.com

Email: support@huawei.com

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to "Vul. Response Process". For details about the policy, see the following website:https://www.huawei.com/en/psirt/vul-response-process For enterprise customers who need to obtain vulnerability information, visit:https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 Dashboard 1

2 Desktop Management 3

2.1 Managing Desktops 3
2.2 Viewing Desktops That Fail to Be Created 7
2.3 Modifying Specifications 7
2.4 Recomposing a System Disk 9
2.5 Adding a Disk 11
2.6 Expanding the Disk Capacity 12
2.7 Deleting a Disk 13
2.8 Managing Tags 14
2.9 Converting a Desktop to an Image 16
2.9.1 Converting a Windows Desktop to an Image 16
2.9.2 Converting a Linux Desktop to an Image 18
2.10 Configuring a Desktop Network 19
2.11 Changing the Desktop Billing Mode (from Pay-per-Use to Yearly/Monthly) 21
2.12 Renewing a Yearly/Monthly-Billed Desktop 21
2.13 Unsubscribing from a Desktop 22

3 Desktop Pool Management 24

3.1 Managing Desktop Pools 24
3.2 Viewing Desktops That Fail to Be Created in the Desktop Pool 27
3.3 Modifying Specifications 28
3.4 Adding a Desktop to a Desktop Pool 29
3.5 Recomposing a System Disk 30
3.6 Adding Disks 33
3.7 Expanding the Disk Capacity 34
3.8 Deleting Disks 35
3.9 Creating an Image 36
3.9.1 Creating a Windows Desktop Image 36
3.9.2 Creating a Linux Desktop Image 38
3.10 Adding Users or User Groups 40
3.11 Removing Users or User Groups 41
3.12 Renewing a Yearly/Monthly-Billed Desktop Pool 41

3.13 Unsubscribing from a Desktop Pool 42
4 Users 44
4.1 Creating a User 44
4.2 Modifying User Information 48
4.3 Resetting a User Password 50
4.4 Unlocking an Account 51
4.5 Resending a Notification Email 51
4.6 Deleting a User 52
4.7 Exporting a User 52
5 User Groups 54
5.1 Creating a User Group 54
5.2 Adding a User to a User Group 55
5.3 Removing a User from a User Group 56
5.4 Modifying a User Group 56
5.5 Deleting a User Group 57
6 Policy Management 59
6.1 Protocol Policy Management 59
6.1.1 Creating a Policy 59
6.1.2 Editing a Policy 64
6.1.3 Configuring Advanced Policy Parameters 67
6.1.4 Exporting a Policy 99
6.1.5 Importing a Policy 100
6.2 Access Policy Management 102
6.2.1 Creating an Access Policy 102
6.2.2 Modifying an Access Policy 104
6.2.3 Deleting an Access Policy 105
7 OU Management 107
8 User Login Records 109
9 Tenant Configuration 110
9.1 Basic Configuration 110
9.1.1 Configuring an AD Domain 110
9.1.2 Configuring AD Domain Certificate Authentication 113
9.1.3 Changing the Domain Administrator Password 114
9.1.4 Modifying Domain Configurations 115
9.1.5 Changing the Internet Access Mode 116
9.1.6 Changing the Service Subnet 118
9.1.7 Changing the Internet Access Port 118
9.1.8 Canceling a Service 119
9.1.9 Reactivating a Service 119
9.1.10 Configuring Multi-Factor Authentication 121

9.1.10.1 Huawei Cloud Virtual MFA 121
9.1.10.2 Enterprise-owned Authentication System 123
9.1.11 Configuring Whether to Block Notification Emails for Desktop Unsubscription or Deletion 126
9.1.12 Multi-VPC Workspace 128
9.2 Authentication Configuration 128
9.2.1 Third-party SSO Authentication 128
10 Internet Access Management 135
10.1 Enabling Small-scale Economical Internet Access (EIP) 135
10.2 Enabling Large-scale Enhanced Internet Access (NAT Gateway+EIP) 138
10.3 Disabling Internet Access 140
11 Scheduled Tasks 142
11.1 Scheduled Shutdown 142
11.2 Scheduled Startup 143
11.3 Scheduled Restart 144
11.4 Scheduled Hibernation 145
11.5 Scheduled System Disk Recomposing 146
12 Application Center 148
12.1 Application Distribution 148
12.1.1 Adding an Application 148
12.1.2 Managing Applications 154
12.1.3 Setting Up a File Server 158
12.2 Application Management 166
13 Private Images 171
13.1 Creating a Windows Private Image 171
13.1.1 Required Software 171
13.1.2 Registering a Private Image Using an ISO File 173
13.1.3 Creating an ECS 177
13.1.4 Configuring an ECS 180
13.1.5 Creating a User Desktop Image 194
14 Permission Management 196
14.1 Workspace Permissions 196
14.2 Creating an IAM User and Granting Permissions 201
14.3 Entrustment Description 202
14.4 Enterprise Projects 203
15 Data Backup and Restoration 205
15.1 Backing Up Desktop Data 205
15.2 Restoring Desktop Data 206
16 Common Function Configuration 207
16.1 Configuring Workspace to Access the Internet 207
16.2 Configuring Workspace to Access the Enterprise Intranet 213

16.3 Configuring Network Connection Between Workspace and Windows AD.....215

17 Subscribing to an Event.....219

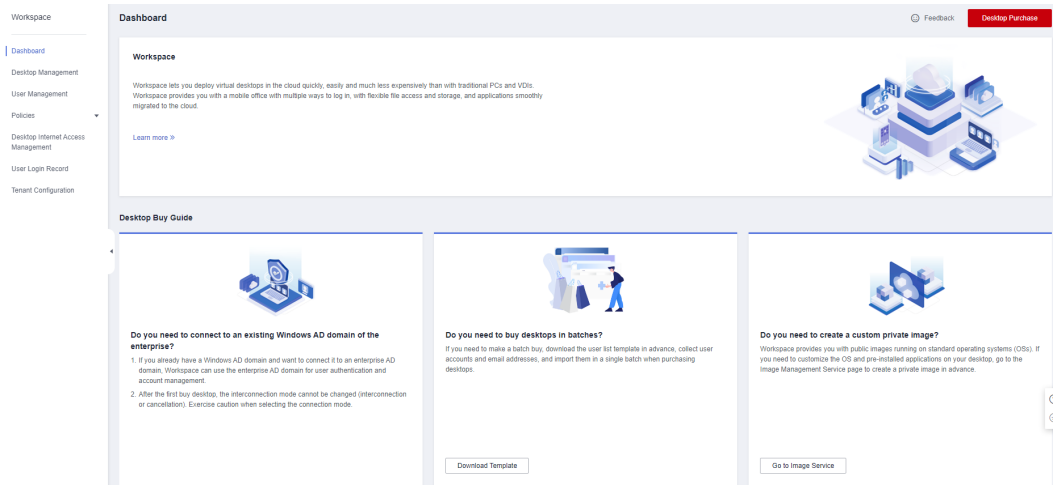
A Change History.....222

1 Dashboard

Having Not Purchased a Desktop

If you have not purchased a desktop, you can learn about Workspace and *Desktop Purchase Guide* on the **Dashboard** page.

Figure 1-1 Dashboard



Having Purchased a Desktop

After purchasing a desktop, you can view the monitoring status of the desktop, such as the running status, login status, and online user count, on the **Dashboard** page, as shown in **Figure 1-2**. For details, see **Table 1 Status description**.

Figure 1-2 Status monitoring

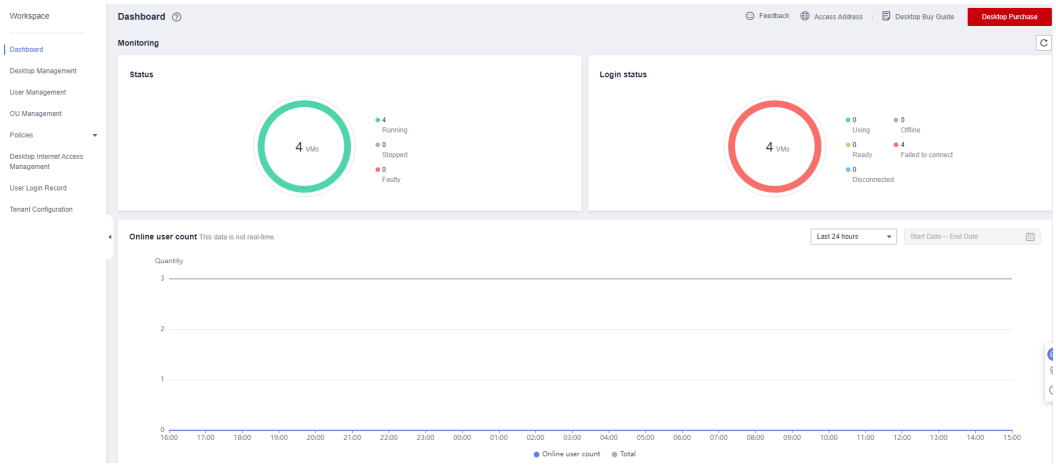


Table 1-1 Status description

Status Type	Status	Description
Login status	Using	Indicates that a user has logged in to the desktop and is using the desktop.
	Disconnected	Indicates that the user has logged out of the desktop and is disconnected.
	Ready	Indicates that the desktop has been registered with and connected to the infrastructure server and is waiting for the user to log in.
	Offline	Indicates that the desktop is stopped.
	Failed to connect	Indicates that the desktop is in an abnormal network or the infrastructure server has not been registered for a long time.
Status	Running	Indicates that the desktop is working.
	Stopped	Indicates that the desktop is stopped.
	Faulty	Indicates that the desktop is faulty.
Online user count	Online user statistics	Displays the number of online users in a specific time range. You can view the number of online users in the last 1 hour, last 24 hours, last 7 days, last 30 days, or a custom time interval. **NOTE** 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 last day before 0 to 1 hour.

2 Desktop Management

2.1 Managing Desktops
2.2 Viewing Desktops That Fail to Be Created
2.3 Modifying Specifications
2.4 Recomposing a System Disk
2.5 Adding a Disk
2.6 Expanding the Disk Capacity
2.7 Deleting a Disk
2.8 Managing Tags
2.9 Converting a Desktop to an Image
2.10 Configuring a Desktop Network
2.11 Changing the Desktop Billing Mode (from Pay-per-Use to Yearly/Monthly)
2.12 Renewing a Yearly/Monthly-Billed Desktop
2.13 Unsubscribing from a Desktop

2.1 Managing Desktops

Scenario

You can start, stop, restart, and delete existing desktops, and change desktop names. If a user stops using a desktop, you can assign the desktop to a new user to save resources.

Prerequisite

You have **created** a desktop.

Procedure

Step 1 Log in to the Workspace console.

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

The desktop management page is displayed.

Step 3 Perform the operations listed in Table 2-1 as required.

Table 2-1 Operations

Operation	Procedure
View desktop information	1. In the upper right corner of the desktop list, select a filter type. 2. Enter a keyword and click  . 3. View the desktop name, usage, specifications, current running status, current desktop login status, IP address, user, billing mode, and ID.
Change a desktop name	1. Click  next to the target desktop name. 2. Enter the new name and click **OK**. **NOTE** Only letters, digits, and hyphens (-) are allowed. The name must start with a letter or digit and cannot end with a hyphen. The name contains a maximum of 15 characters.
Export the desktop list	In the upper right corner of the desktop list, click  to export all desktop lists of the current project. You can view the desktop information, such as desktop creation time, in the downloaded list file.
Delete a desktop	For pay-per-use desktops: 1. Select a desktop and click **More** > **Delete** in the upper left corner of the desktop list or in the **Operation** column. 2. On the page displayed, click **Confirm**. **NOTE** You can select **Delete users at the same time** as required. 3. Click **Yes**. For yearly/monthly-billed desktops: 1. Select a desktop and click **More** > **Unsubscribe** in the upper left corner of the desktop list or in the **Operation** column. 2. On the desktop unsubscription page, confirm the desktop information and click **Yes**. 3. On the resource unsubscribe 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
Stop a desktop	1. Select a desktop and click **Stop** in the upper left corner of the desktop list or in the **Operation** column. 2. On the page displayed, select **Confirm**. **NOTE** You can determine whether to select **Forcibly Stop** as required. 3. Click **Yes**.
Start a desktop	1. Select a desktop and click **Start** in the upper left corner of the desktop list or in the **Operation** column. 2. On the page displayed, select **Confirm**. 3. Click **Yes**.
Hibernate a desktop	1. Select a desktop and choose **More** > **Hibernate** in the upper left corner of the desktop list or in the **Operation** column. 2. On the page displayed, confirm the hibernation. 3. Click **Yes**. **NOTE** Currently, hibernation is only applicable to the Windows OS.
Restart a desktop	1. Select a desktop and click **Restart** in the upper left corner of the desktop list or choose **More** > **Restart** in the **Operation** column. 2. On the page displayed, select **Confirm**. **NOTE** You can determine whether to select **Forcibly Restart** as required. 3. Click **Yes**.
Remotely log in to a desktop	1. Select a desktop and choose **More** > **Log in remotely** in the **Operation** column. 2. In the displayed dialog box, click **OK**. 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 on the client.

Operation	Procedure
Unbind a user	1. Select the desktop to be unbound and choose **More** > **Unbind a user** in the **Operation** column. 2. Confirm the desktop and user information and click **OK**. **NOTE** – Enter a new username and email address, change the user permissions and desktop name as required, and click **Confirm** to assign the desktop to a new user. During assigning a desktop to a new user, the system deletes all data of the last user. – If you do not enter user information and click **Cancel**, the desktop is not assigned to any user. For details about how to assign a desktop to a user, see **Assign Users**. If no user is assigned, the data of the last user is retained on the desktop. For security purposes, you should assign the unbound desktop to a user as soon as possible.
Assign desktops	1. Select **Unassigned Users** for **User**, and click **Unassigned Users** or **More** > **Assign Users** in the **Operation** column. 2. Select an image type and a specific image. **NOTE** If the system detects that the image file used by the current desktop does not exist in the system, you need to select another image for the desktop to reinstall the system disk. Pay attention to the fee change as prompted. – Only images running the same OS can be selected. For Windows desktops, only Windows images can be selected. Currently, Windows public images of Workspace are Marketplace images. – For pay-per-use cloud desktops to be changed to MarketPlace images, which means a Windows desktop is changed from a private or public image to a public image, the fees are charged based on the new configuration and image. In other scenarios where images are not changed to Marketplace images, the fees are charged based on the new configuration. – For yearly/monthly-billed cloud desktops, if the image type remains unchanged or a public image is changed to a private image, you can reassign the desktop without paying extra fees. If a private image is changed to a public image, you can reassign the desktop after paying the bill. 3. On the user assignment page, enter a new username and email address, and change the user permissions and desktop name as required. 4. Click **Confirm**. **NOTE** During user assignment, all data of the last user will be deleted.

----End

2.2 Viewing Desktops That Fail to Be Created

Scenario

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.

NOTE

If there is no desktop creation failure, this function is not displayed.

Procedure

Step 1 Log in to the Workspace console.

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

The desktop management page is displayed.

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

The page of desktop creation failure is displayed.

Step 4 View the cause of the desktop creation failure.

----End

2.3 Modifying Specifications

Scenario

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

Constraints

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

Procedure

Step 1 Log in to the Workspace console.

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

The desktop management page is displayed.

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

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 modify the specifications as required.

Table 2-2 Operation description

Billing Mode	Desktop Quantity	Operation
Pay-per-Use	1	In the row containing the desktop whose specifications are to be modified, click **More** > **Change Specifications** in the **Operation** column.
	More than one	In the upper left corner of the desktop list, choose **More** > **Change Specifications** > **Change Specifications**.
Yearly/ Monthly	1	In the row containing the desktop whose specifications are to be modified, click **More** > **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 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.

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

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

  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. Return to the **Desktop Management** page. 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. In the displayed page, click **Return to the desktop list**. On the **Desktop Management** page, the desktop status is **Changing**. You can view the modified desktop specifications in the **Specifications/Image** column.

----End

2.4 Recomposing a System Disk

Scenarios

If a purchased desktop needs to be restored to the initial template or desktop applications and patches need to be updated, you can recompose or change the system disk.

Impact on the System

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

Restrictions

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

Prerequisite

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

Procedure

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

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

The desktop management page is displayed.

Step 3 Select the desktop whose system disk needs to be recomposed and choose **More** > **Rebuild the OS**.

The **Rebuild the OS** page is displayed.

Step 4 Configure information about the system disk to be rebuilt, as listed in **Table 2-3**.

Table 2-3 Basic settings

Parameter	Description	Example Value
Reestablishment Mode	**Reinstall OS**: Use the original desktop image.	Reinstall OS
OS	Select Windows or Linux as required.	Windows
Rebuild Method	Select an implementation method for recomposing the system disk as required. • **Forcible Restart Immediately**: The system disk recomposing starts immediately after you click **Confirm** in **Step 5**. • Restart in 1 minute: The system disk recomposing starts 1 minute after you click **Confirm** in **Step 5**. • Restart in 5 minutes: The system disk recomposing starts 5 minutes after you click **Confirm** in **Step 5**. • Restart in 10 minutes: The system disk recomposing starts 10 minutes after you click **Confirm** in **Step 5**. • Restart in 15 minutes: The system disk recomposing starts 15 minutes after you click **Confirm** in **Step 5**.	Forcible Restart Immediately
Notice Users	Select whether to notify users of recomposing the system disks of their desktops. If they are notified, a notification message is displayed on the desktops after they log in to the desktops.	Not notice
Notification Message	If you choose to notify users, you can customize the content displayed in the pop-up window on their desktops.	-
Enter **rebuild** to confirm the system disk recomposing.	Enter **rebulid** in the text box as prompted.	rebulid

Step 5 Click **Confirm**. The desktop system disk is recomposed using the selected recomposing method.

Step 6 (Optional) Wait until the desktop status changes to **Running**. Contact the user to view and change the disk status of the desktop by referring to **What If the Data Disk of a Windows Desktop Disappears After Recomposing the System Disk?**

NOTE

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

----End

2.5 Adding a Disk

Scenarios

This section describes how to add a data disk to a desktop.

Prerequisite

You can add data disks only to a running desktop.

Procedure

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

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

The desktop management page is displayed.

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

The page for adding a data disk 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.
- 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).
- 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**. The data disk has been added.

----End

2.6 Expanding the Disk Capacity

Scenario

If the capacity of the system disk or data disk used for purchasing a desktop is insufficient, you need to expand its capacity.

This section describes how to expand the capacity of a system disk or data disk for a desktop.

Prerequisite

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 Workspace console**.

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

The desktop management page is displayed.

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

Step 7 Read the operation impact statement and select the statement checkbox.

Step 8 Click **Next**.

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

----End

2.7 Deleting a Disk

Scenario

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.

Constraint

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

Procedure

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

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

The desktop management page is displayed.

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

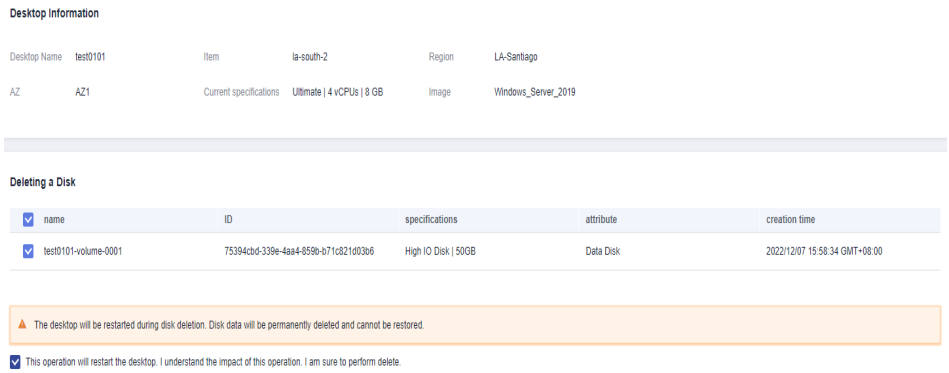
NOTICE

After a data disk is deleted, the disk data will be permanently deleted and cannot be restored. Exercise caution when performing this operation.

- More than one data disk
  a. Locate the row that contains the target desktop, and choose **More** > **Disk** > **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



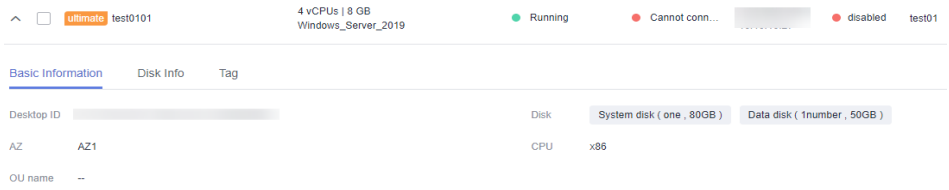
c. Confirm the data disks to be deleted, and select **I understand the impact and want to continue.**

d. Click **Confirm Delete**.

- 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



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

2.8 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 Workspace console.

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

The desktop management page is displayed.

Step 3 Click to expand the basic desktop information.

Step 4 Click **Tag**.

Step 5 Click **Adding or editing tags**.

The dialog box for adding or editing tags is displayed.

Step 6 Enter a tag key and tag value, and click **Add**. Table 1 describes the tag naming rules.

NOTE

You can add a maximum of 10 tags to a desktop.

Table 2-4 Tag naming rules

Parameter	Rule
Tag key	• This field cannot be left blank. • The value can contain up to 36 characters. • The value cannot start or end with a space and cannot contain the following characters: =*<>\,|/. • Each tag key must be unique on the same desktop.
Tag value	• The value can contain up to 43 characters. • The value cannot start or end with a space and cannot contain the following characters: =*<>\,|/.

Step 7 Click **Yes**.

The tag has been added.

----End

Searching for a Desktop by Tag

Step 1 Log in to the Workspace console.

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

The desktop management page is displayed.

Step 3 In the upper right corner of the desktop management page, click **Search for an instance by tags**.

Expand the window of search by tag.

Step 4 Enter an existing tag key and tag value.

Step 5 Click **Search**.

NOTE

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

----End

2.9 Converting a Desktop to an Image

2.9.1 Converting a Windows Desktop to an Image

Scenario

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 into 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 Workspace console**.

NOTE

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

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

Step 3 In the row that contains the desktop to be converted into an image, click **More** > **Create Image**.

Step 4 Configure image parameters as required, as shown in **Table 2-5**.

Table 2-5 Description

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 Click **Yes**.

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 **Service List** > **Compute** > **Image Management Service**. The created image is displayed in the **Private Images** list.

----End

2.9.2 Converting a Linux Desktop to an Image

Scenario

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 into 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.

Prerequisites

- A desktop generated using a Linux OS image is available.
- The desktop has been started and is in the **Running** status.

Procedure

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

NOTE

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

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

Step 3 In the row that contains the desktop to be converted to an image, click **More** > **Create Image**.

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

Table 2-6 Description

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-uos 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.	-
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 Click **Yes**.

NOTE

- During image creation, the desktop is unavailable and will restart. Do not perform other operations.
- After an image is created, the allocated user and user directory are deleted.
- 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

2.10 Configuring a Desktop Network

Scenario

When the network of a user changes, you can switch the desktop network settings so that the user can quickly switch the desktop network.

Prerequisites

To use the desktop network setting function, fill in the service ticket information to obtain technical support. For details, see Submitting 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 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.
- If the network of a stopped desktop is switched, the desktop will be started first, the network is switched, and then the desktop is shut down.

Procedure

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

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

Step 3 Locate the row that contains the desktop whose VPC is to be switched and choose **More** > **Network settings** > **Desktop network settings**.

Step 4 Configure desktop network settings.

- 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 Configuration** and click **Edit VPC** under **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 Configuration** and click **Edit Subnet** under **VPC** to add the subnet.
- Private IP address: Select a private IP address assignment mode as required.
  - Automatically assign an IP address.
  - Manually assign an IP address.
  - Use an existing elastic network interface.
- Security group: Click to select the security group to be switched. To create a security group, see **Creating a Security Group**.

Step 5 Confirm the desktop network configuration.

----End

2.11 Changing the Desktop Billing Mode (from Pay-per-Use to Yearly/Monthly)

Scenario

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

Constraint

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

Procedure

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

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

Step 3 Locate the row that contains the target pay-per-use desktop, and click **More** > **Change the billing mode from Pay-per-Use to Yearly/Monthly desktop** in the **Operation** column.

Step 4 Confirm the information about the target desktop and select **Confirm**.

Step 5 Click **Yes**.

Step 6 Confirm the order information and pay the bill.

----End

2.12 Renewing a Yearly/Monthly-Billed Desktop

Scenario

You can renew yearly/monthly-billed desktops.

Procedure

Step 1 **Log in to the Workspace 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.

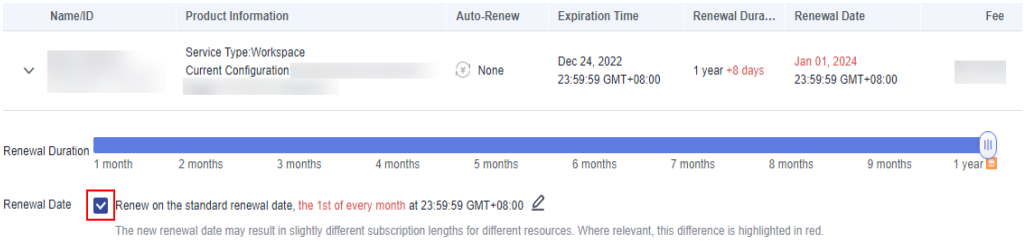
The renewal configuration page is displayed.

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

NOTE

You can click to reset the unified expiration date for resources.

Figure 2-3 Setting a unified expiration date



Step 5 Click **Pay**.

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

----End

2.13 Unsubscribing from a Desktop

Scenario

Unsubscribe from a desktop on the management console.

Procedure

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

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

The desktop management page is displayed.

Step 3 To unsubscribe from a pay-per-use desktop, go to **4**.

To unsubscribe from a yearly/monthly desktop, go to **6**.

Step 4 Select the pay-per-use desktops to be unsubscribed from, and click **More** > **Delete** in the upper left corner of the desktop list or in the **Operation** column.

The dialog box for confirming deletion is displayed.

Step 5 In the displayed dialog box, select **Confirm**and click **Yes**.

NOTE

1. You can determine whether to select **Delete users at the same time**.

2. Once a desktop is deleted, system disks are deleted together. This operation cannot be undone. Exercise caution when performing this operation.

3. After a desktop is deleted or unsubscribed from, the elastic IP (EIP) address of the desktop is automatically unbound. After the EIP is unbound, it is retained and continues to be billed.

To release an EIP, go to the **EIP management** page and manually release it.

Step 6 Select the yearly/monthly desktop to be unsubscribed from, and click **More** > **Unsubscribe** in the upper left corner of the desktop list or in the **Operation** column.

The dialog box for confirming unsubscription is displayed.

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

The resource unsubscription page is displayed.

Step 8 On the resource unsubscription page, confirm the resource to be unsubscribed from and write the unsubscription reason, select **After being unsubscribed from, the resources not in the recycle bin will be deleted immediately and cannot be restored. I've backed up data or no longer need the data.**, and click **Confirm**.

Step 9 Click **Unsubscribe** again.

NOTE

1. Once a desktop is deleted, system disks are deleted together. This operation cannot be undone. Exercise caution when performing this operation.

2. After a desktop is deleted or unsubscribed from, the elastic IP (EIP) address of the desktop is automatically unbound. After the EIP is unbound, it is retained and continues to be billed.

To release an EIP, go to the **EIP management** page and manually release it.

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

----End

3 Desktop Pool Management

3.1 Managing Desktop Pools
3.2 Viewing Desktops That Fail to Be Created in the Desktop Pool
3.3 Modifying Specifications
3.4 Adding a Desktop to a Desktop Pool
3.5 Recomposing a System Disk
3.6 Adding Disks
3.7 Expanding the Disk Capacity
3.8 Deleting Disks
3.9 Creating an Image
3.10 Adding Users or User Groups
3.11 Removing Users or User Groups
3.12 Renewing a Yearly/Monthly-Billed Desktop Pool
3.13 Unsubscribing from a Desktop Pool

3.1 Managing Desktop Pools

Scenario

You can start, stop, restart, and delete existing desktop pools, and change desktop names. You can create a group of desktop resources 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 Workspace console.

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

The **Desktop Pool** page is displayed.

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

Table 3-1 Operations

Operation	Procedure
Viewing desktop pool information	1. In the upper part of the desktop list, enter a keyword and click  . 2. View information such as the desktop pool name, pool type, specifications/images, desktop usage, and billing mode.
Changing the desktop pool name	1. Click the desktop pool name. The basic information page of the desktop pool is displayed. 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. Only letters, digits, and hyphens (-) are allowed.
Deleting a desktop pool	For pay-per-use desktops: 1. Choose **More** > **Delete** in the **Operation** column of the desktop pool to be deleted. **NOTE** Before deleting a desktop pool, disable the automatic creation function and delete the desktop. 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** in the upper left corner of the desktop list or in the **Operation** column. 2. On the desktop unsubscription page, confirm the desktop information and click **Yes**. 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
Shutting down a desktop pool	1. Locate the row that contains the desktop pool to be stopped, and click **Stop** in the **Operation** column. 2. On the page displayed, confirm the shutdown. **NOTE** You can determine whether to select **Forcible execution** as required.
Starting a desktop pool	1. Locate the row that contains the desktop pool to be started, and click **Start** in the **Operation** column. 2. On the page displayed, confirm the startup.
Hibernating a desktop pool	1. Locate the row that contains the desktop pool to be hibernated, and choose **More** > **Hibernate** in the **Operation** column. 2. On the page displayed, confirm the hibernation. **NOTE** – Currently, hibernation is only applicable to the Windows OS. – You can determine whether to select **Forcible execution** as required.
Restarting a desktop pool	1. Locate the row that contains the desktop pool to be restarted, and choose **More** > **Restart** in the **Operation** column. 2. On the page displayed, confirm the restart. 3. Click **Yes**. **NOTE** You can determine whether to select **Forcible execution** as required.
Remotely logging in to a desktop in the desktop pool	1. Click the desktop pool name. The basic information page of the desktop pool is displayed. 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.
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 **OK**. **NOTE** Notifications can be sent only for running desktop pools.

Operation	Procedure
Changing the duration of desktop pool unbinding upon disconnection	1. Click the desktop pool name. The basic information page of the desktop pool is displayed. 2. Click on the right of **Disconnection retention duration**. The page of unbinding upon disconnection is displayed. 3. Change the disconnection retention duration as required and click **Confirm**. **NOTE** The value must range from 10 to 43,200.
Changing the number of desktops automatically created in a desktop pool	1. Click the desktop pool name. The basic information page of the desktop pool is displayed. 2. Click next to **A maximum of *x* desktops can be created during access.**. The **Auto Create** page is displayed. 3. Modify the number of *x* as required.

----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 a Desktop to a Desktop Pool

Scenario

If desktops need to be added to a purchased desktop pool, the administrator can purchase more desktops in the desktop pool.

NOTE

The billing mode of the newly purchased desktop is the same as that of the desktop pool.

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 name of the desktop pool to which you want to add a desktop. The basic information page of the desktop pool is displayed.

Step 4 Click on the right of **Number of Desktops**. The **Buy More** page is displayed.

Step 5 Select the number of desktops to be purchased as required and click **OK**. The desktop pool configuration page is displayed.

Step 6 Select **I have read and agree to the Image Disclaimer.**

Step 7 Click **Buy Now**.

----End

3.5 Recomposing a System Disk

Scenario

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 recompose or change the system disk.

Impact on the System

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

Constraints

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

Prerequisites

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

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 recomposing 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 recomposed, click **More** in the **Operation** column, and select **rebuild the OS**.

The dialog box of recomposing 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 recomposed. 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 recomposing a system disk is displayed.

Step 4 Configure the system disk to be recomposed, as shown in **Table 3-2**.

Table 3-2 Basic configurations

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

Parameter	Description	Example
Rebuild Method	Select a mode for recomposing the system disk as required. • **Forcible Restart Immediately**: After you click **OK** in **Step 5**, the system disk recomposing starts. • **Restart in 1 minute**: The system disk recomposing starts 1 minute after you click **OK** in **Step 5**. • **Restart in 5 minutes**: The system disk recomposing starts 5 minutes after you click **OK** in **Step 5**. • **Restart in 10 minutes**: The system disk recomposing starts 10 minutes after you click **OK** in **Step 5**. • **Restart in 15 minutes**: The system disk recomposing starts 15 minutes after you click **OK** in **Step 5**.	Forcible Restart Immediately
Notice Users	Select whether to notify users that the system disks of their desktops need recomposing. 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.	-
Enter **rebuild** to confirm the system disk recomposing.	Enter **rebuild** in the text box as prompted.	rebuild

Step 5 Click **OK**. The system recomposes the desktop system disk using the selected method.

Step 6 (Optional) Wait until the desktop status changes to **Running**. Contact the user to view and change the disk status of the desktop by referring to

NOTE

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

----End

3.6 Adding Disks

Scenario

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 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 adding data disks to a desktop pool in either of the following ways:

Method 1:

Locate the row that contains the desktop pool to which disks are to be added, 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 whose 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**. The data disk has been added.

----End

3.7 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 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 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). 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 .

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

3.8 Deleting Disks

Scenario

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 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 deleting disks of a desktop pool in either of the following ways:

Method 1:

Locate the row that contains the desktop pool whose disks are to be deleted, 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.**

Confirm the deletion.

----End

3.9 Creating an Image

3.9.1 Creating a Windows Desktop Image

Scenario

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 Workspace console.

NOTE

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

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

The **Desktop Pool** 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.

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 4 Configure image parameters as required, as shown in **Table 3-3**.

Table 3-3 Description

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

Parameter	Description	Example
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 5 Click **Yes**.

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

3.9.2 Creating a Linux Desktop Image

Scenario

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 Linux 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.

Prerequisites

- A desktop generated using a Linux OS image is available.
- The desktop has been started and is in the **Running** status.

NOTE

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

Procedure

Step 1 Log in to the Workspace console.

NOTE

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

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

The **Desktop Pool** 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.

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 4 Configure image parameters as required, as shown in Table 3-4.

Table 3-4 Description

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-uos 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 5 Click **Yes**.

NOTE

- During image creation, the desktop is unavailable and will restart. Do not perform other operations.
- After an image is created, the allocated user and user directory are deleted.
- 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

3.10 Adding Users or User Groups

Scenario

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

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 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.

----End

3.11 Removing Users or User Groups

Scenario

Administrators can remove specified users or user groups from a desktop pool on the console.

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

Click **User (Group)** on the right of the desktop pool basic information. The **User (Group)** page is displayed.

Step 4 Select the user or user group to be removed.

- Removing a single user or user group:

  Locate the user or user group to be removed, and click **Remove** in the **Operation** column.

  Click **OK**.

- Removing users or user groups in batches

  Select the users or user groups to be removed in batches.

  Click **Remove** in the upper left corner of the page. The dialog box for removing users or user groups in batches is displayed.

  Confirm the batch removal and click **Yes**.

----End

3.12 Renewing a Yearly/Monthly-Billed Desktop Pool

Scenario

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

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 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** in the upper left corner of the desktop list or in the **Operation** column.

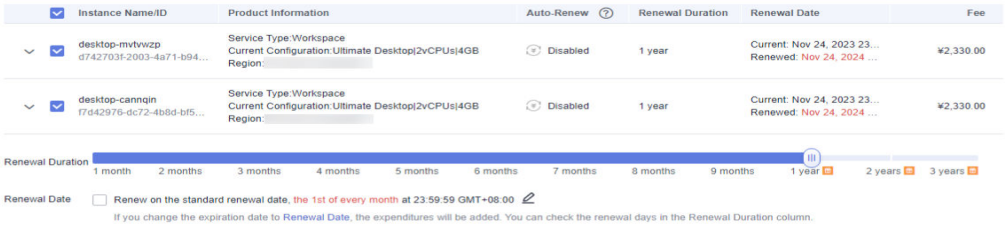
The **Renew desktop** window is displayed. Click **Yes** to go to the page for desktop renewal.

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

NOTE

You can click to reset the unified expiration date for resources.

Figure 3-1 Setting a unified expiration date



Step 6 Click **Pay**.

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

----End

3.13 Unsubscribing from a Desktop Pool

Scenario

Unsubscribe from a desktop pool on the management console.

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 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 **Unsubscribe desktop** window is displayed. Click **Yes** to go to the page for unsubscribing from resources.

NOTE

Once a desktop is deleted, system disks are deleted together. This operation cannot be undone. Exercise caution when performing this operation.

Step 5 On the page for unsubscribing from resources, confirm the unsubscription information and provide the unsubscription reason, and select **After being unsubscribed from, the resources not in the recycle bin will be deleted immediately and cannot be restored. I've backed up data or no longer need the data.** 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, .
- 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

4 Users

4.1 Creating a User
4.2 Modifying User Information
4.3 Resetting a User Password
4.4 Unlocking an Account
4.5 Resending a Notification Email
4.6 Deleting a User
4.7 Exporting a User

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.

Procedure

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

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

The **User** page is displayed.

Step 3 Click **Create User**.

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

Step 4 Enter the user information, as shown in the following table.

Creating a User	Parameter	Operation
Activation method	• **User Activation** – 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. • **Manager Activation** – Enter the username and password. Keep the password secure. **NOTE** If your tenant connects to the enterprise AD, the **Manager Activation** method is unavailable by default.	Select an activation method as required.

Creating a User	Parameter	Operation
User Activation > **Manual Input**	• **User name** is used for user authentication during desktop login. Naming rules: – The name can contain 1 to 20 characters. – A name containing only digits is allowed. – The 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. • **Email** is used to receive desktop provisioning emails and related notifications. Rules for verifying an email address: – Enter a valid email address through system verification. – The value can contain a maximum of 64 characters. – This field cannot be left blank. • **Phone** is used to receive desktop subscription emails and related notifications. Mobile number verification rule: – [+][*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. – The mobile number can contain spaces, slashes (/), and hyphens (-).	1. Set **Activation method** to **User Activation**. 2. Select **Manual Input**. 3. Set the username, email address, and mobile number, enter the description as required, and set the account expiration time. 4. Click **Add user**. **NOTE** Enter the email address or mobile number, or both.

Creating a User	Parameter	Operation
Manager Activation > **Manual Input**	• **User name** is used for user authentication during desktop login. Naming rules: – The name can contain 1 to 20 characters. – A name containing only digits is allowed. – The 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 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. • **Email** is used to receive desktop provisioning emails and related notifications. Rules for verifying an email address: – Enter a valid email address through system verification. – The value can contain a maximum of 64 characters. – This field cannot be left blank. • **Phone** is used to receive desktop subscription emails and related notifications. Mobile number verification rule: – [+][*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.	1. Set **Activation method** to **Manager Activation**. 2. Select **Manual Input**. 3. Set the username and initial password, enter the mobile number, email address, and description as required, and set the account expiration time. 4. Click **Add user**. **NOTE** Enter the email address or mobile number, or both.

Creating a User	Parameter	Operation
	– The mobile number can contain spaces, slashes (/), and hyphens (-).	
User Activation > **Batch import**	• Upload the users recorded in the table and create them in batches.	1. Click **Download Template** on the right of **Import user information** to download the user list template. 2. Enter the serial number, username, email address, mobile number, expiration time, and description in the table as required. 3. Click **Upload** to upload the user list that has been filled in as required. 4. Click **Confirm 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.
Manager Activation > **Batch import**	• Upload the users recorded in the table and create them in batches.	

----End

4.2 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 user information (email address and mobile number) can be modified. User information (description, account options, and account expiration information) cannot be modified.

Prerequisites

A user has been created.

Procedure

Step 1 Log in to the management console.

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

The **User** page is displayed.

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

The **Update User** dialog box is displayed.

Step 4 Select **User Activation** or **Manager Activation** for **Activation method**.

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

- **Information Supplement**
  - **Email**

    Used to receive desktop provisioning emails and related notifications.
  - **Phone**

    Used to receive desktop provisioning messages and related notifications.
- **Account expired**
  - **Never expires**

    The validity period of an account is not limited.
  - **After this time**

    After the expiration date is set, the user account expires after this date.
- **Account Options**
  - The user needs to change the password upon the next login.

    After the administrator sets a password, the user needs to change the password upon the next login to the desktop.
  - **Cannot change password**

    Only the administrator can reset user passwords. Users cannot change desktop login passwords.
  - **Password never expires**

    The validity period of a password is not limited.
  - **Account has been disabled**

    Users cannot use disabled accounts to log in to desktops.

Step 6 Click **Confirm update**.

----End

4.3 Resetting a User Password

Scenarios

When the exiting AD domain is not used, if 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 the exiting AD domain is used, you need to reset the password on the AD server.

Prerequisites

A user has been created.

Procedure

Step 1 Log in to the management console.

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

The **User** page is displayed.

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

Step 4 Choose **Email** or **Phone** as the method for sending 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 reset 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 **Phone** is optional on the password reset page.

Step 5 Select **Confirm reset password**.

Step 6 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

4.4 Unlocking an Account

Scenarios

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

Procedure

Step 1 Log in to the management console.

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

The **User** page is displayed.

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

The **Unlock a User** dialog box is displayed.

Step 4 Click **OK**.

----End

4.5 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 management console.

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

The **User** page is displayed.

Step 3 Locate the row that contains the target user. Click **More** in the **Operation** column and select **Resend Notification**.

The **Resend Notification** window is displayed.

Step 4 Click **OK**.

----End

4.6 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.
- You cannot delete a user if the user has desktops.

Prerequisites

A user has been created.

Procedure

Step 1 Log in to the management console.

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

The **User** page is displayed.

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

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

The dialog box for user information deletion is displayed.

Step 4 Click **OK**.

----End

4.7 Exporting a User

Scenarios

Administrators can export users on the management console.

Procedure

Step 1 Log in to the management console.

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

The **User** 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

5 User Groups

5.1 Creating a User Group
5.2 Adding a User to a User Group
5.3 Removing a User from a User Group
5.4 Modifying a User Group
5.5 Deleting a User Group

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, you can add users to a user group.

NOTE

In a project that interconnects with an AD domain, users cannot be added to AD user groups, and can only be added to common user groups.

Prerequisites

A user group has been created.

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 a user group name in the user group list.

The user group information page is displayed.

Step 4 Click **Add**.

The **Adding a user** dialog box is displayed.

Step 5 Enter a username in the **Optional Users** text box or select the username to be added in the **Options** 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 management 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.

Prerequisites

A user group has been created and contains users.

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 a user group name in the user group list.

The user group information page is displayed.

Step 4 On the user group information page, choose **remove** or **Batch Remover**.

- **remove**

  For a single user, click **remove** in the **Operation** column of the row that contains the username.

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

- **Batch Remover**

  Select the users to be removed in batches and click **Remove** in the upper left corner of the user list.

  In the displayed dialog box, select **confirm Batch Remover** and click **Yes**.

----End

5.4 Modifying a User Group

Scenarios

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

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

The **User Group** 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 user group whose information is to be modified. The **Edit User Group** page 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 of a user group as required.
  - **User group name**

    Click  of the target user group, change the user group name as required, and click  .
  - **Description**

    Click  , modify the description as required, and click  .

----End

5.5 Deleting a User Group

Scenarios

Administrators can delete a specified user group on the management console.

Prerequisites

A user group has been created.

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 On the **User Group** page, you can choose **remove** or **Batch Remove**.

- **remove**
  - Method 1: Select a user group and click **Delete** in the **Operation** column of the user group.

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

- Method 2: Click the name of the user group to be deleted. The user group information page is displayed.

  Click **Delete** in the upper right corner of the user group information page.

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

- **Batch Remove**

  Select the user groups to be deleted in batches and click **Delete** in the upper left corner of the user list.

  In the displayed dialog box, select **confirm Batch Remove** and click **Yes**.

----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

6.2 Access Policy Management

6.1 Protocol Policy Management

6.1.1 Creating a Policy

Scenario

You can plan and customize application policies of the following types to create an efficient policy management solution for different scenarios.

- General
- Peripheral
- Audio
- Client
- Display
- File & Clipboard
- Session
- Watermark
- Keyboard & Mouse

Prerequisites

You have purchased a desktop.

Procedure

Step 1 Log in to the Workspace console.

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

The **Protocol Policy** page is displayed.

Step 3 Click **Create Policy**.

The **Create Policy** page is displayed.

Step 4 Configure the policy name and description.

NOTE

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

  The administrator can select an existing policy template or create a template by adding a user-defined 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.
- **Import an existing policy**: If a policy group has been created, you can import a policy from an existing policy group. The configuration items of the selected policy will be used by default.

Step 6 Click **Next: Configure policies**.

The **General policy configuration** page is displayed.

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

NOTE

General policies the simplified version of advanced policies and can meet common office automation (OA) requirements. By default, policy parameters that meet common OA requirements are enabled.

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

For details about configuring a general policy, see **Table 1 Policy management**.

Table 6-1 Policy management

Type	Parameter	Policy
USB Port Redirection	Graphics Device (such as scanners)	Supports USB peripherals on Workspace. Users can use devices in VMs through USB port redirection.
	Video Device (such as cameras)	
	Print Device (such as printer)	
	Storage Device (such as USB flash drives)	
	Smart Card (such as Ukey)	
File Redirection	Client 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.
	Client Removable Driver	
	Client Disc Driver	
	Client 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.

Type	Parameter	Policy
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 scenarios.	Image Quality	The display quality is excellent and the bandwidth usage is high. The bandwidth is 25 Mbit/s. The parameter details cannot be edited by default.
	Smoothness	The display quality and bandwidth usage are balanced. The bandwidth is 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 decrease the 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 decrease the 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 decrease the smoothness. In this case, you are advised to use the default value.

Type	Parameter	Policy
		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 Configure an advanced policy.

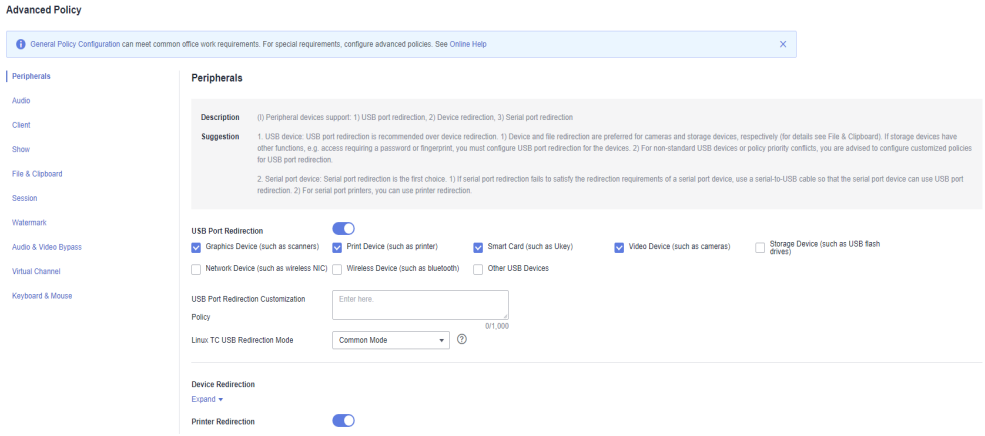
The general policies can meet general office work requirements. Configure an advanced policy for special requirements.

1. On the general policy configuration page, click **Advanced Policy**.

   The **Advanced Policy** page is displayed.

2. Configure an advanced policy as required, as shown in **Figure 6-1**. For details about the advanced policy parameters, see **6.1.3 Configuring Advanced Policy Parameters**.

Figure 6-1 Configuring an advanced policy



Step 9 Click **Next: Select objects**.

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

6.1.2 Editing a Policy

Scenario

This section describes how to edit an existing policy.

Procedure

Step 1 Log in to the Workspace console.

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

The **Protocol Policy** 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 Objects** in the **Policy Object** column to view the target object. You can also click **Modify** to modify the target object.
- To modify a policy object, choose **More** > **Modify Policy Object**.
- To modify the description, choose **More** > **Modify Description**.
- To delete a manually created policy, choose **More** > **Delete**.
- To modify a policy, perform **Step 4** to **Step 7**.

Step 4 In the row containing the target policy, click **Modify Policy Item** in the **Operation** column.

The page for general policy configuration is displayed.

Step 5 On the page displayed, enable or disable the corresponding policy. **Table 1 Policy management** describes the policy.

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

Table 6-2 Policy management

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

Type	Parameter	Policy
	Print Device (such as printer)	
	Storage Device (such as USB flash drives)	
	Smart Card (such as Ukey)	
File Redirection	Client 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.
	Client Removable Driver	
	Client Disc Driver	
	Client 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	-	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 scenarios.	Image Quality	The display quality is excellent and the bandwidth usage is high. The bandwidth is 25 Mbit/s. The parameter details cannot be edited by default.

Type	Parameter	Policy
	Smoothness	The display quality and bandwidth usage are balanced. The bandwidth is 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 decrease the 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 decrease the 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 decrease the 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.

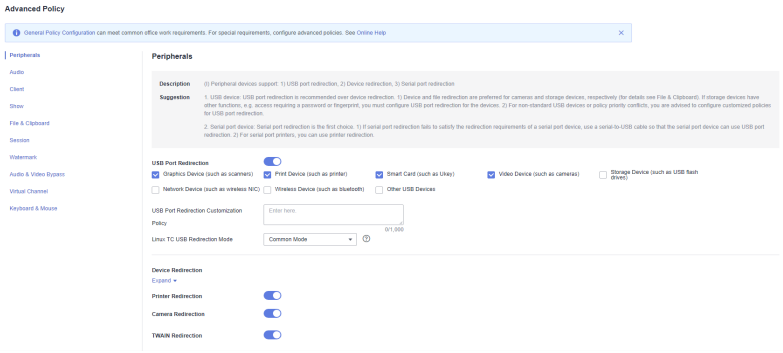
Step 6 Edit an advanced policy.

1. On the **General policy configuration** page, click **Advanced Policy**.

   The **Advanced Policy** page is displayed.

2. Configure an advanced policy as required, as shown in **Figure 6-2**. For details about the advanced policy parameters, see **6.1.3 Configuring Advanced Policy Parameters**.

Figure 6-2 Configuring an advanced policy



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 Configuring Advanced Policy Parameters

Scenario

During policy configuration, you can customize advanced policies for special scenarios.

You can plan and customize application policies of the following types to create efficient policy management solutions for different scenarios.

NOTE

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

- Peripheral
- Audio
- Client
- Display
- File & Clipboard
- Session
- Watermark
- Keyboard & Mouse

Peripheral

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

NOTE

A peripheral may support USB port redirection, device redirection, and serial port (device) redirection.

Table 6-3 Peripheral policies

Type	Parameter	Description	Example Value
USB Port Redirection	USB port redirection switch	• : After this option is selected, Workspace end users can use USB devices connected to terminals by using USB port redirection. • : After this option is selected, Workspace end users cannot use USB devices connected to terminals by using USB port redirection. • Default value:	
	Graphics Device (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:	
	Print Device (such as printer)	• : 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:	

Type	Parameter	Description	Example Value
	Smart Card (such as Ukey)	• ☑: 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: ☑	☑
	Video Device (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 Device (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: ☐	☐

Type	Parameter	Description	Example 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: ☐	☐
	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 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 through printer redirection (a policy of device redirection). • Default value:  **NOTICE** The printer driver must be installed on both TCs and computers.	
	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 Workspace. 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 (a policy of device redirection). • Default value: **NOTE** • The camera driver must be installed on the terminal. • Toggle on the **USB Port Redirection** switch ( ) and select a video device (such as a camera).	
	Camera Frame Rate (FPS)	The value ranges from 1 to 30.	15
	Camera Max Width (Pixel)	The value ranges from 1 to 9999.	3000
	Camera Max Height (Pixel)	The value ranges from 1 to 9999.	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 (a policy of device 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 Workspace, 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 Workspace, client serial ports are not automatically connected. • Default value: ☐	☑
Driver Interface Redirection	Customized Drivers	Applications on Workspace call configured APIs to use hardware on terminals. • 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 ;*?<>|. • 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.	
Play Redirection	Play 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
Record Redirection	Record 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 audio. •  : Recording redirection is disabled so that end users cannot record audio.	

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

Client

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
Anti-Screenshot Policy	After the policy is enabled, users are prevented from saving and sharing screenshots on the cloud desktop. •  : This policy is enabled. •  : This policy is disabled. **NOTE** Only Windows clients and Linux TCs are supported. After this function is enabled, other terminals cannot access the system.	

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**: If this option is selected, video images are compressed at a fixed quality. **Average Video Bitrate (Kbit/s)** takes effect only after **Rendering acceleration** is enabled. • **Bandwidth**: 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. Increasing this value in **Bandwidth** mode 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 **Quality** mode, increasing this value compromises video quality. The value ranges from 5 to 59.	15
	Lowest Video Quality	Lower limit of video quality. In **Quality** mode, increasing this value compromises video quality. The value ranges from 5 to 69.	25
	Highest Video Quality	Upper limit of video quality. In **Quality** 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 Scenario Optimization	•  : Video scenario optimization is enabled to improve smoothness. •  : Video scenario 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 1280.	191
	Min Video Height	It is easier to open a video as the value decreases. The value ranges from 0 to 1280.	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
	Threshold of the Non-Natural Image Area Percentage	It is harder to exit a video as the value increases. The value ranges from 0 to 100.	25

Type	Parameter	Description	Example Value
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
	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 Workspace. •  : 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)	-

File & Clipboard

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
	Client Fixed Driver	• ☑: Users can use fixed drivers, such as local disks, on cloud desktops in file redirection mode. • ☐: Users cannot use fixed drivers, such as local disks, on cloud desktops in file redirection mode. **NOTE** When file redirection is disabled, this function is disabled.	☐
	Client Removable Driver	• ☑: Users can use removable drivers, such as USB flash drives, on cloud desktops in file redirection mode. • ☐: Users cannot use removable drivers, such as USB flash drives, on cloud desktops in file redirection mode. **NOTE** When file redirection is disabled, this function is disabled.	☐
	Client Disc Driver	• ☑: Users can use CD-ROM drivers on cloud desktops in file redirection mode. • ☐: Users cannot use CD-ROM drivers on cloud desktops in file redirection mode.	☐

Type	Parameter	Description	Example Value
	Client Network Driver	• : Users can use network drivers on cloud desktops in file redirection mode. • : Users cannot use network drivers on cloud desktops in 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 1000 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 1000.	900
	File Size Setting on 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 4096.	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 a client. •  : Files on a VM cannot be sent to a 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.	
	Clipboard File Redirection	•  : Clipboard file redirection is enabled. •  : Clipboard file redirection is disabled.	

Session

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

Table 6-8 Session policies

Parameter	Description	Recommended Value
Automatic Screen Locking	•  : A desktop will automatically lock the screen if no keyboard or mouse operation is performed when the screen locking waiting time is due. •  : Automatic screen locking is disabled.	Disabled
Screen lock waiting time (minute)	Specifies the waiting time before the desktop screen is automatically locked. The value ranges from 3 to 86,400.	10
Automatic Disconnection/ Logout/Restart/ Shutdown After Screen Lock	• **Automatic Disconnection After Screen Lock**: After automatic screen locking is enabled and then automatic disconnection is enabled, if no keyboard or mouse operation is performed on the client after the disconnection or logout waiting time, the VM is automatically disconnected. • **Automatic Logout After Screen Lock**: After automatic screen locking is enabled and automatic logout is enabled, if no keyboard or mouse operation is performed on the client after the disconnection or logout waiting time, the VM automatically logs out. • **Automatic Restart After Screen Lock**: After automatic screen lock is enabled, enable automatic restart to trigger automatic screen locking. If no keyboard or mouse operation is performed on the client after the waiting time, the VM automatically restarts. • **Automatic Shutdown After Screen Lock**: After automatic screen locking is enabled, enable automatic shutdown to trigger automatic screen locking. If no keyboard or mouse operation is performed on the client after the waiting time, the VM automatically shuts down. • **Disabled**: The automatic disconnection or logout function is disabled.	Disabled
Automatic Disconnection/ Logout/Restart/ Shutdown After Screen Lock In (Minute)	Specifies the waiting time before a desktop is automatically disconnected, logged out, restarted, or shut down. The value ranges from 1 to 86,400.	1440

Parameter	Description	Recommended Value
Automatic Logout/Restart/Shutdown After Disconnection	• Logout: After a client is disconnected from a VM, the VM automatically logs out if the client does not reconnect to the VM after the waiting time. • Restart: After a client is disconnected from a VM, if the VM is not reconnected after the waiting time, the VM automatically restarts. • Shutdown: After a client is disconnected from a VM, if the VM is not reconnected after the waiting time, the VM automatically shuts down. • Disable: Disable automatic disconnection, logout, restart, or shutdown. **NOTE** • The automatic logout/restart/shutdown function can be used only when **Automatic Disconnection/Logout/Restart/Shutdown After Screen Lock** is disabled or disconnection is selected. • If another logout, restart, or shutdown task is performed on the VM within the waiting time, the automatic logout, restart, or shutdown operation will not be triggered.	Disabled
Automatic Logout/Restart/Shutdown After Disconnection In (Minute)	Specifies the waiting time before a desktop is automatically logged out, restarted, or shut down after disconnection. The value ranges from 10 to 86,400.	10
Hibernation Settings	• After a 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. **NOTE** Currently, the hibernation settings are applicable to the Windows OS.	-
Desktop Hibernation After Disconnection	•  : The desktop hibernation function is enabled. After the waiting time, the disconnected desktop automatically hibernates. •  : The desktop hibernation function is disabled.	Disabled

Parameter	Description	Recommended Value
Automatic Hibernation After Disconnection In (Minute)	Specifies the waiting time for automatic hibernation after the cloud desktop is disconnected. The value ranges from 5 to 600,000.	60
Desktop Hibernation Without Operations	•  : The function of hibernating a desktop when there is no operation is enabled. When no keyboard or mouse operation is performed on the desktop for a specified period of time, the desktop is hibernated. •  : The function of hibernating a desktop when there is no operation is disabled.	Disabled
Desktop Hibernation Without Operations In (Minute)	Specifies the waiting time for automatic hibernation when no operation is performed on the desktop. The value ranges from 5 to 600,000.	60
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.	

Watermark

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

Table 6-9 Watermark policies

Parameter	Description	Example Value
Watermark	•  : 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.	
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
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.	12.5
Quantity	Number of watermarks. This parameter is available when **Display Mode** is set to **Fixed position**. The value ranges from 1 to 17.	1
Tilt	Specifies the tilt of the watermark displayed on the desktop. The value ranges from –90 to 90.	–45

Parameter	Description	Example Value
Custom	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 *Customized content Login username Time displayed on the desktop*. For example, if the customized 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 customized content may not take effect.	-

Keyboard & Mouse

Configure a keyboard & mouse policy, as shown in **Table 6-10**.

Table 6-10 Keyboard & mouse policies

Parameter	Description	Recommended Value
Computer Mouse Device Feedback	• Adaptive • Forcible • Disabled	Adaptive
Computer Mouse Device Simulation Mode	• 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.	☑

Parameter	Description	Recommended Value
Computer external cursor feedback	• ☑: Computer external cursor feedback is enabled. • ☐: Computer external cursor feedback is disabled.	☐

6.1.4 Exporting a Policy

Scenario

You can create workspaces in multiple areas. The policies of each workspace must be the same. You can export the configured policies of a workspace and import the policies to the target workspaces to quickly configure desktop policies in multiple 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 Workspace console**.

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

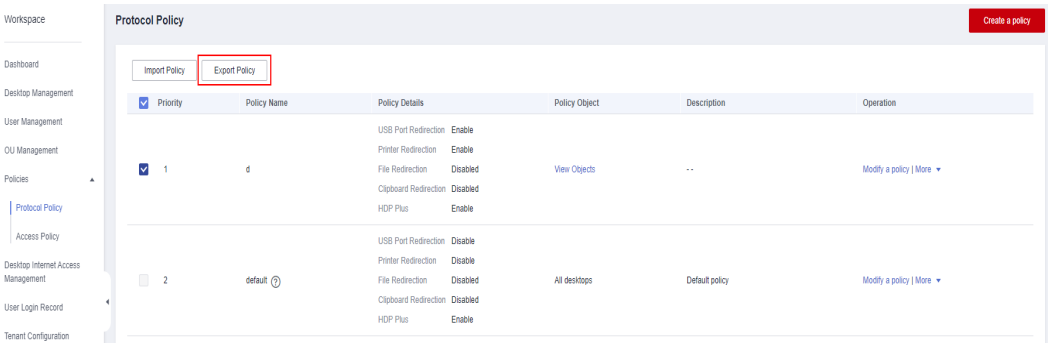
The **Protocol Policy** page is displayed.

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



Step 4

NOTE

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

----End

6.1.5 Importing a Policy

Scenario

You can create workspaces in multiple areas. The policies of each workspace must be the same. You can export the configured policies of a workspace and import the policies to the target workspaces to quickly configure desktop policies in multiple 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 workspace.
- 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 a workspace. If the number of policies exceeds the quota, the file cannot be imported.

Procedure

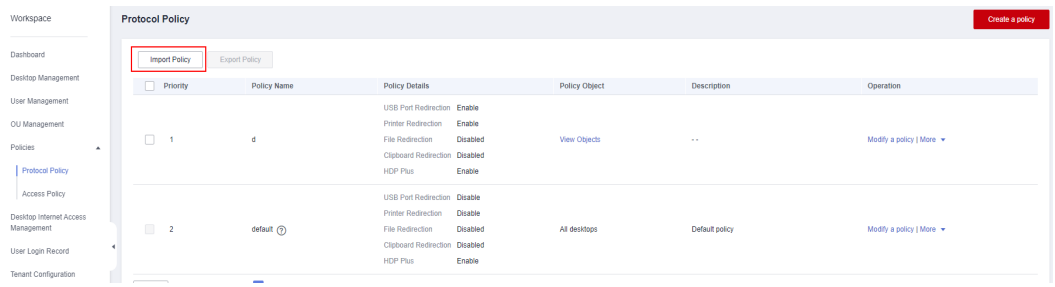
Step 1 **Log in to the Workspace console**.

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

The **Protocol Policy** page is displayed.

Step 3 Click **Import Policy**.

Figure 6-4 Importing a policy



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?**

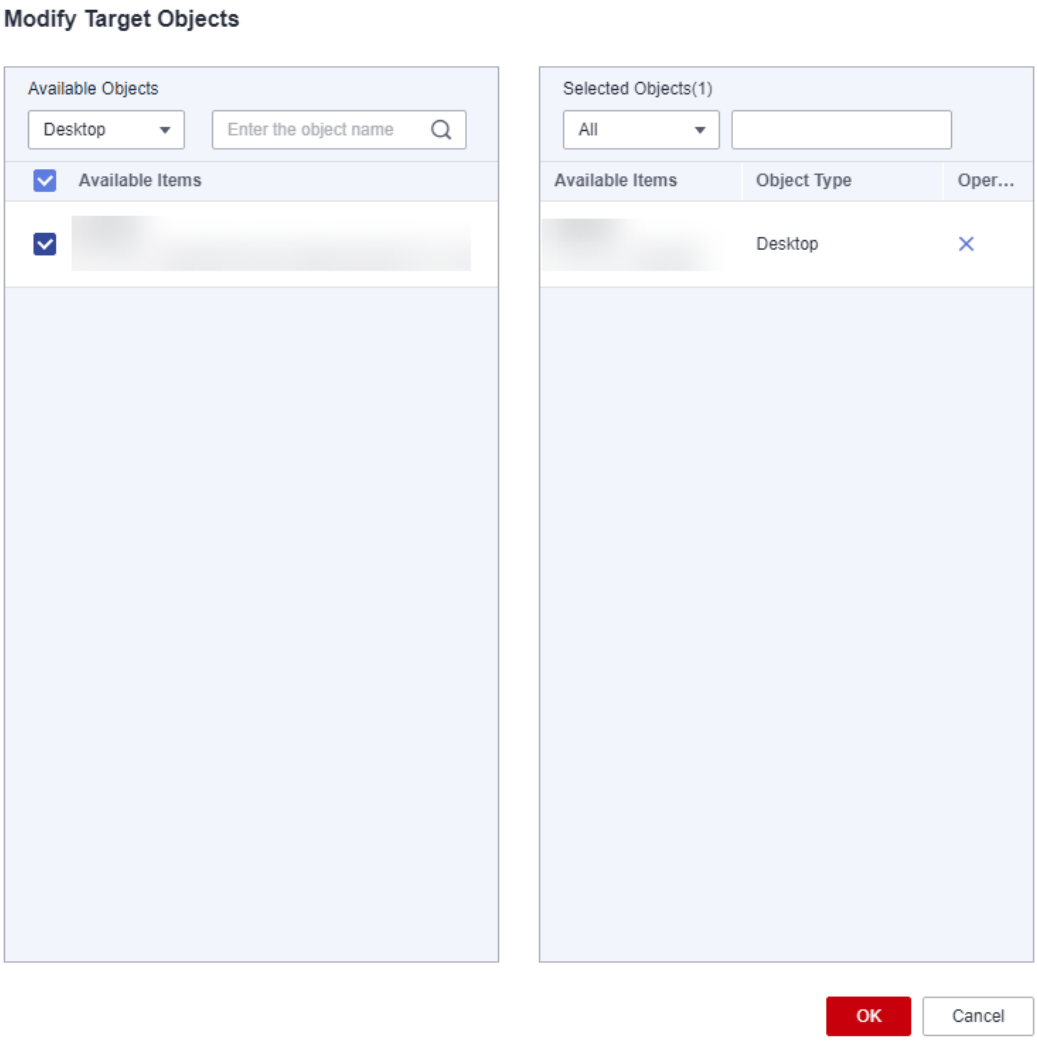
Step 5 Locate the row that contains the imported policy, and click **More** > **Modify Policy Object** in the **Operation** column.

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



Step 7 Click **OK**.

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

6.2 Access Policy Management

6.2.1 Creating an Access Policy

Scenarios

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 **9.1.5 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 management console**.

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

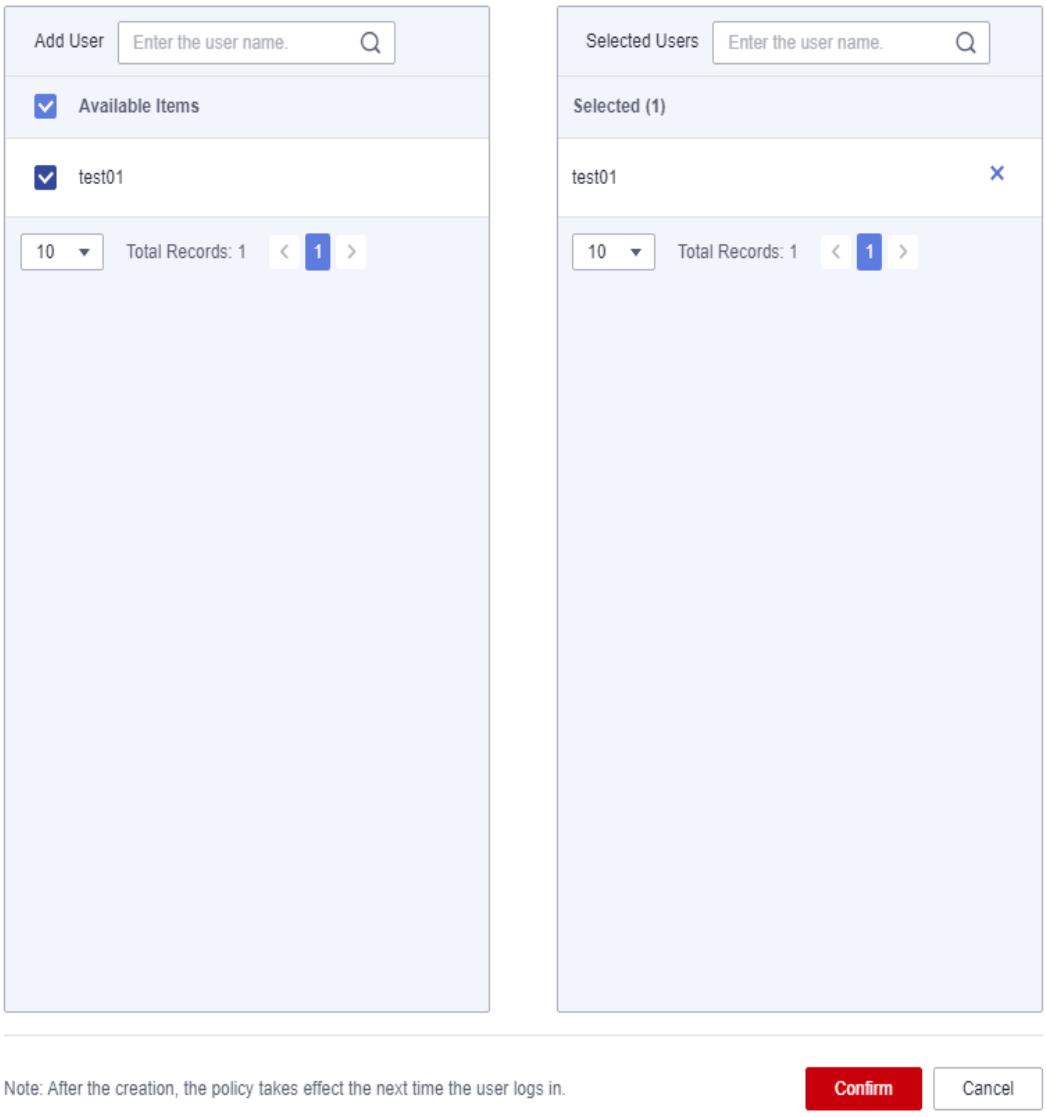
The **Access Policy** page is displayed.

Step 3 Click **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



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

6.2.2 Modifying an Access Policy

Scenarios

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 management console**.

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

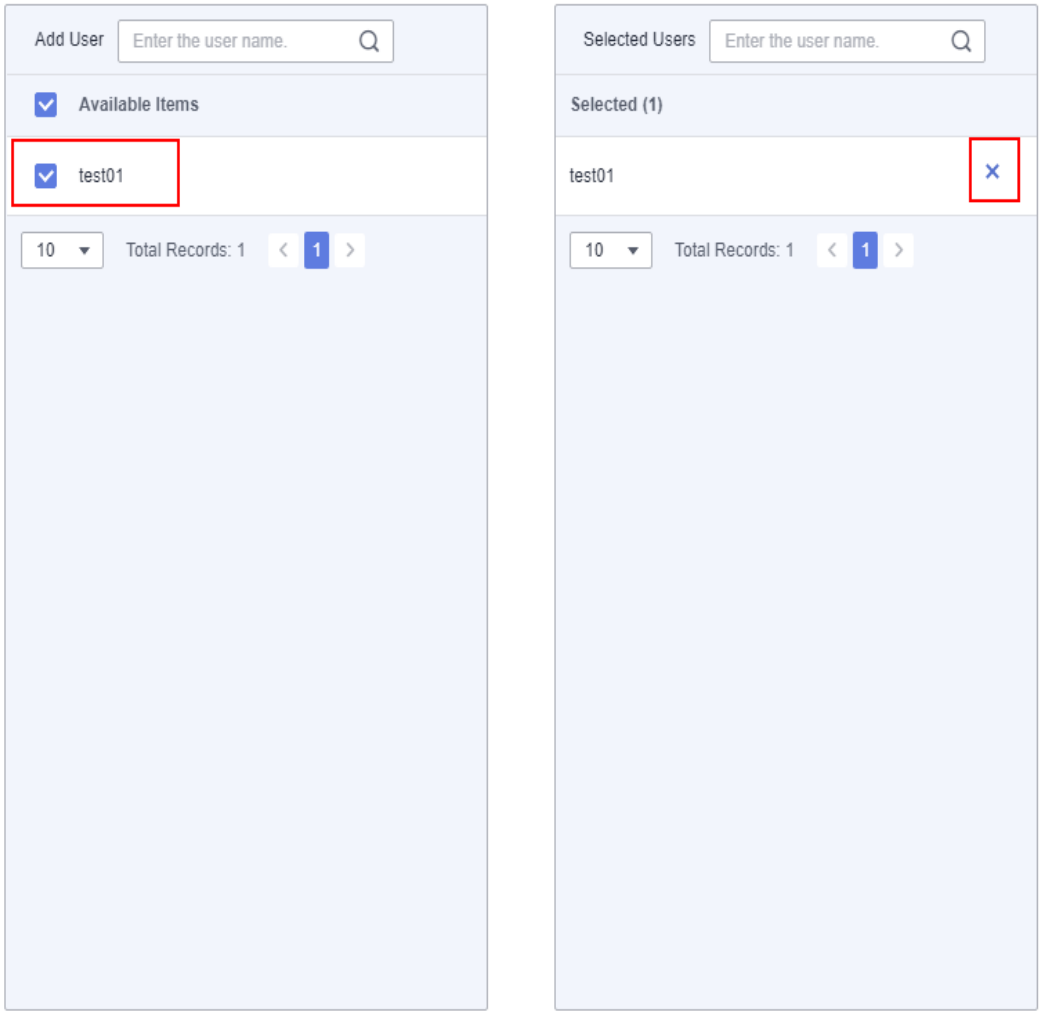
The **Access Policy** page is displayed.

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 application object



Step 5 Click **OK**.

NOTE

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

----End

6.2.3 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

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 User Login Records

Scenarios

This section describes how to view user login records to know the desktop running status and user login status. This helps troubleshooting and system maintenance.

Procedure

Step 1 Log in to the management console.

Step 2 Click **User Login Record**.

The **User Login Record** page is displayed.

Step 3 View user login records, including **Desktop Name**, **Login User**, **Terminal IP Address**, **Terminal System Type**, **Desktop IP Address**, **Connection Start Time**, **Connection End Time**, and **Failure Cause**.

----End

9 Tenant Configuration

9.1 Basic Configuration

9.2 Authentication Configuration

9.1 Basic Configuration

9.1.1 Configuring an AD Domain

Scenarios

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 **16.3 Configuring Network Connection Between Workspace 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) Standby Domain Controller Name
- (Optional) Standby Domain Controller IP Address
- (Optional) Standby DNS Server IP Address

Procedure

(Optional) Setting an enterprise ID

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

Step 2 Click **Tenant Configuration**.

The **Tenant Configuration** 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.

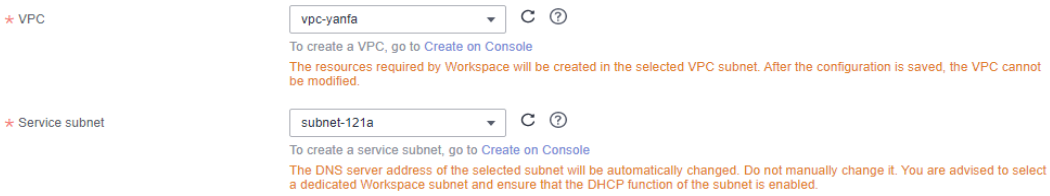
- **Domain Name**: Windows AD domain name
- **Domain Administrator Account**: administrator name for logging in to the Windows AD server
- **Domain Administrator Password**: administrator password for login
- **Active Domain Controller Name**: It can be the host name of the AD service or the combination 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
- Deleting 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 (optional)
  - Name of Standby Domain Controller
  - IP Address of Standby Domain Controller
  - Standby DNS IP Address

Network Configuration

Step 5 Configure the **VPC** and **Service subnet**, as shown in **Figure 9-1**.

Figure 9-1 VPC and **service subnet**



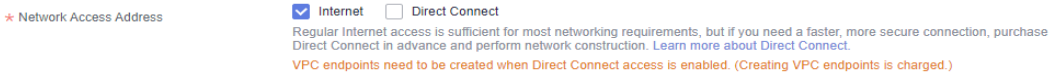
- To configure an existing VPC, select an existing **VPC** and **service subnet**.
- To configure a new VPC, click **Create on Console**, and create a **VPC** and **service subnet**. For details, see **Virtual Private Cloud User Guide**.

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 address, as shown in **Figure 9-2**. By default, **Internet** is selected. You can select multiple options.

Figure 9-2 Network access address



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 **9.1.2 Configuring AD Domain Certificate Authentication**.

9.1.2 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 . 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 management 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

9.1.3 Changing the Domain Administrator Password

Scenarios

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.

Prerequisite

An AD domain has been configured.

Procedure

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

Step 2 Click **Tenant Configuration**.

The **Tenant Configuration** 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

9.1.4 Modifying Domain Configurations

Scenarios

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 management console**.

Step 2 Click **Tenant Configuration**.

The **Tenant Configuration** 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
- **Name of Active Domain Controller**: 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
- Advanced options
  - Name of Standby Domain Controller
  - IP Address of Standby Domain Controller
  - Standby DNS IP Address

Step 5 Click **OK**.

The domain configuration has been modified.

----End

9.1.5 Changing the Internet Access Mode

Scenarios

On the Workspace console, you can change your Internet access mode.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Tenant Configuration**.

The **Tenant Configuration** 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, and you can disable or enable the Internet access or direct connect access. For details, see **Table 9-1**.

NOTE

Workspace supports Internet access and direct connect access at the same time. At least one access mode must be enabled.

Table 9-1 Modifying the network access mode

Operation	Procedure
Disable Internet access	If **Direct Connect Access Address** and **Internet Access Address** 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**.

Operation	Procedure
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**.
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 **Amend** on the right of **Direct Connect network segment** in the network configuration area. In the displayed dialog box, modify the network segment as required. Click **OK**.

----End

9.1.6 Changing the Service Subnet

Scenarios

On the Workspace console, you can change the service subnet based on your plan.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Tenant Configuration**.

The **Tenant Configuration** 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

9.1.7 Changing the Internet Access Port

Scenarios

On the Workspace client (Huawei Cloud Office), change the port used for accessing the Workspace Portal (HTTPS-based access).

Prerequisites

The Internet access mode in **Step 3** has been **enabled**.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Tenant Configuration**.

The **Tenant Configuration** page is displayed.

Step 3 In the **Internet Access Port** column, click **Modify**.

The dialog box for modifying the HTTPS access port is displayed.

Step 4 Change the **HTTPS access port**.

NOTE

Rules for the HTTPS access port number:

- The value ranges from 1025 to 65535.
- The value must be a valid integer.

Step 5 Click **OK**.

----End

9.1.8 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

After the service is canceled, resources (such as desktops and disks) of the tenant will be released. If the Internet function is enabled, the EIP, NAT, and bandwidth that are not released will be charged continuously. If you do not need the EIP, NAT, and bandwidth, disable them in the corresponding service.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Tenant Configuration**.

The **Tenant Configuration** page is displayed.

Step 3 Click **Cancel Workspace** in the **Tenant Configuration** area.

The **Warning** dialog box is displayed.

Step 4 Click **OK**.

Step 5 Click **OK**.

----End

9.1.9 Reactivating a Service

Scenarios

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.

Prerequisite

The service of the current project (no subprojects) or subproject has been locked.

Procedure

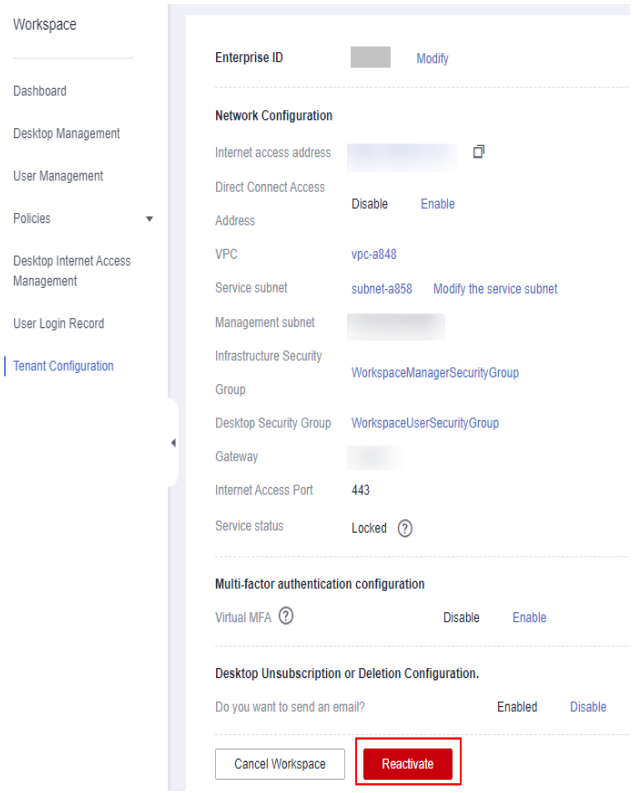
Step 1 Log in to the management console.

Step 2 Click **Tenant Configuration**.

The **Tenant Configuration** page is displayed.

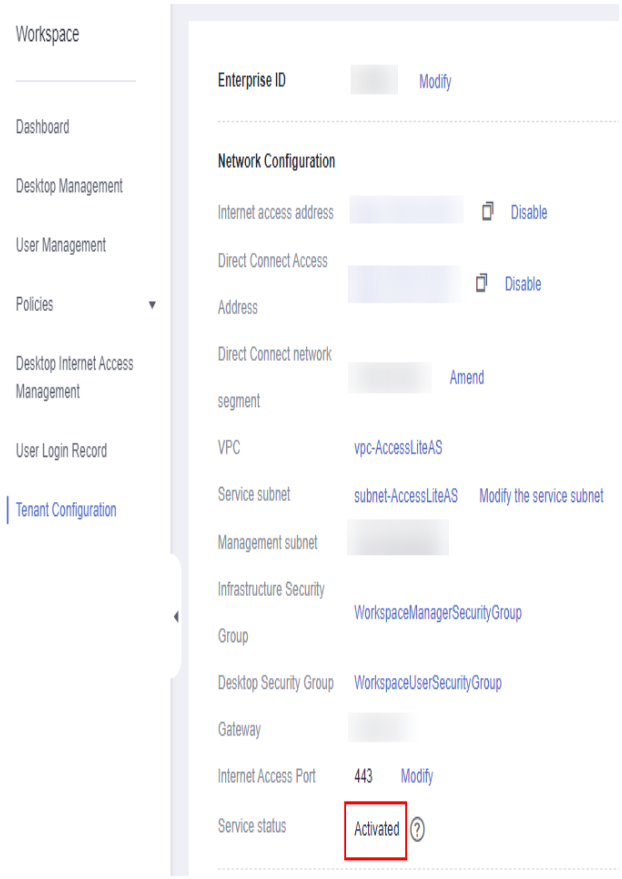
Step 3 In the lower part of the **Tenant Configuration** page, click **Reactivate**, as shown in **Figure 9-3**.

Figure 9-3 Reactivating a service



Wait until **Service status** changes to **Activated**, as shown in **Figure 9-4**. Then, you can purchase desktops or create users again.

Figure 9-4 Service activated



----End

9.1.10 Configuring Multi-Factor Authentication

9.1.10.1 Huawei Cloud Virtual MFA

Scenarios

After you enable virtual MFA, Huawei Cloud virtual MFA authentication is used by default. When an end user uses the account and password to log in to the cloud desktop from a client, the end user must pass the secondary authentication of the MFA dynamic verification code before accessing the cloud desktop.

Prerequisite

You have purchased a cloud desktop.

Use Restrictions

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. For details, see Submitting a Service Ticket.

Procedure

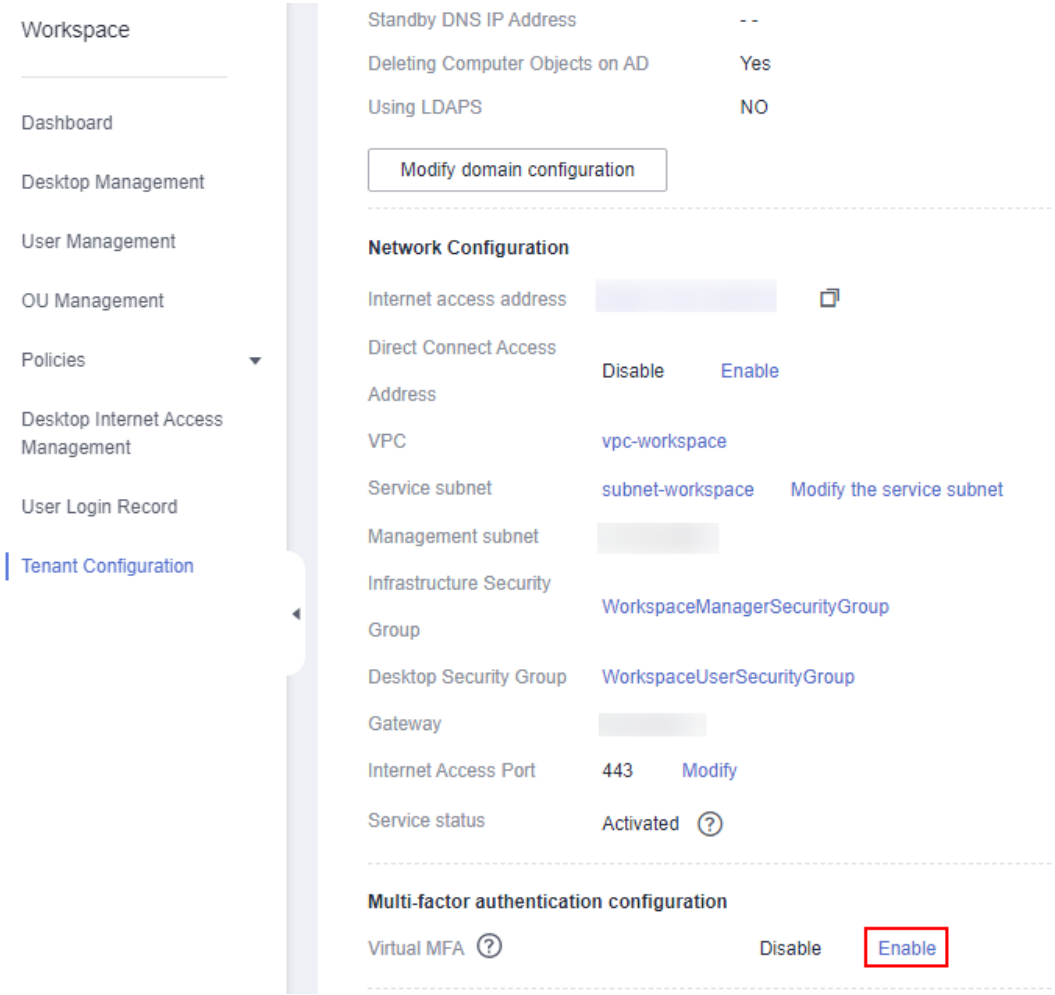
Step 1 Log in to the management console.

Step 2 Click **Tenant Configuration**.

The **Tenant Configuration** page is displayed.

Step 3 Under **Multi-factor authentication configuration**, select **Enable** for **Virtual MFA**.

Figure 9-5 Enabling virtual MFA



Step 4 Click **OK**.

NOTE

After you enable virtual MFA, end users need to use the virtual MFA device in the Huawei Cloud application on a smart device (such as a mobile phone) to obtain a dynamic verification code when logging in to the desktop from a client for Workspace. (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. For details, see **Logging In to a Desktop Using an SC**, **Logging In to a Desktop Using a TC**, **Logging In to a Desktop Using a Mobile Terminal**.

----End

Associated Operations

You can disable virtual MFA under **Multi-factor authentication configuration**. After multi-factor authentication is disabled, users can directly use their accounts and passwords to log in to cloud desktops with no need for secondary authentication of virtual MFA devices.

After virtual MFA is disabled, all information about the bound virtual MFA device is deleted from the system. Notify end users to delete the MFA device from the MFA virtual device list on the mobile device. If you want to enable virtual MFA again, notify end users to bind the virtual MFA device again.

9.1.10.2 Enterprise-owned Authentication System

Scenarios

You can configure the interconnection with an enterprise authentication system so that end users can use the system to perform secondary authentication when logging in to a cloud desktop using accounts and passwords through Workspace.

Prerequisites

- You have purchased a cloud desktop.
- The network between the customer data center of the enterprise authentication server and the VPC has been configured by referring to **Getting Started** of *Direct Connect* or **What's New** of *Virtual Private Network*.

  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

Use Restrictions

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. For details, see Submitting a Service Ticket.

Procedure

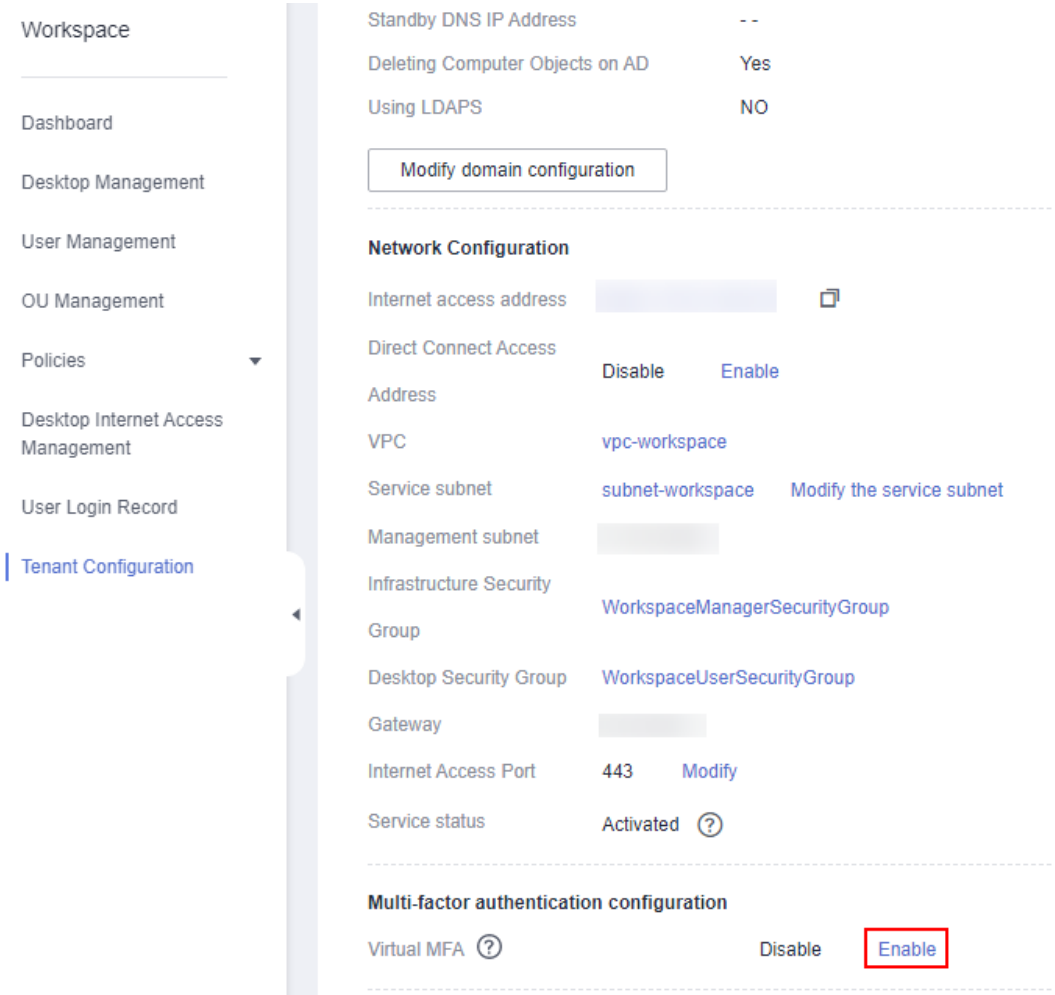
Step 1 Log in to the management console.

Step 2 Click **Tenant Configuration**.

The **Tenant Configuration** page is displayed.

Step 3 Under **Multi-factor authentication configuration**, select **Enable** for **Virtual MFA**.

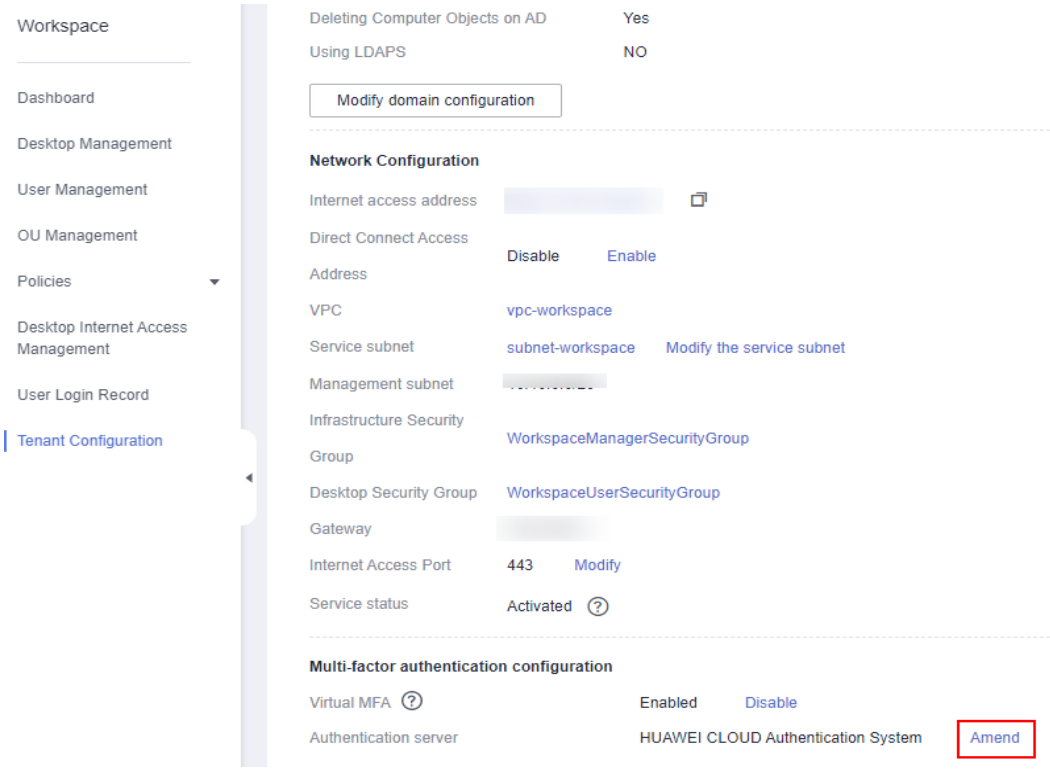
Figure 9-6 Enabling virtual MFA



Step 4 Click **OK**.

Step 5 Click **Amend** next to **Authentication server**, as shown in **Figure 9-7**. The page for modifying multi-factor authentication configuration is displayed.

Figure 9-7 Modifying an authentication server



Step 6 Configure parameters by referring to **Table 9-2**.

Table 9-2 Parameters for interconnecting with an enterprise authentication system

Parameter	Description	Example Value
Authentication server	Select **Interconnection with enterprise authentication system**.	Interconnection with enterprise authentication system
Access mode	Set this parameter based on the network mode of the user's authentication server. • If only the public network is accessible, select **Internet**. • If only the private network is accessible, select **Dedicated**.	Internet

Parameter	Description	Example Value
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
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 **Certificate Upload** and select the SSL/TLS certificate of the enterprise authentication server prepared in **Prerequisites**. 2. Click **Open**.	-

Step 7 Click **OK**.

NOTE

Use enterprise's own authentication system 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**, **Logging In to a Desktop Using a Mobile Terminal**.

----End

9.1.11 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 a user as required. The notification email helps users clearly know the desktop unsubscription or deletion status. However, if you do not send notification emails to users, they will be less disturbed by unnecessary information.

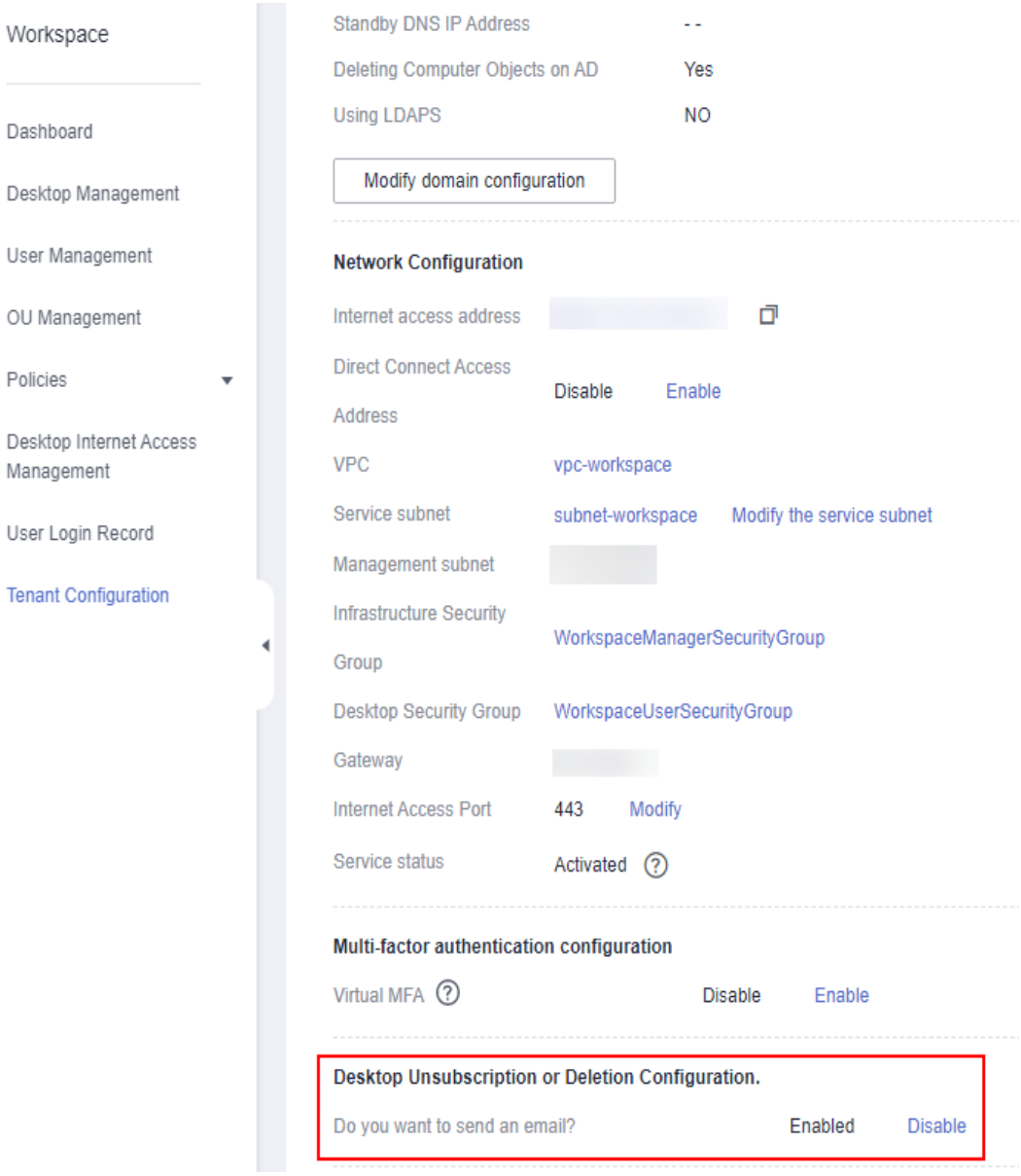
Procedure

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

Step 2 Click **Tenant Configuration**.

The **Tenant Configuration** page is displayed.

Step 3 In the **Desktop Unsubscription/Deletion Configuration** area on the **Tenant Configuration** page, perform the corresponding operations as required.



- The configuration 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 the desktop unsubscription or deletion notification email, click **Disable**.

----End

9.1.12 Multi-VPC Workspace

Scenario

Workspace supports multiple VPCs to meet different network planning requirements. This function is in the open beta test (OBT). For details, submit a service ticket to obtain technical support.

9.2 Authentication Configuration

9.2.1 Third-party SSO Authentication

Scenario

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 9-3 lists the configuration data required for this operation.

Table 9-3 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
	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.	-
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

Protocol	Parameter	Description	Example Value
	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
	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

Protocol	Parameter	Description	Example Value
	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 Workspace 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 URIs** 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 Workspace console.

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

The **Authentication Configuration** page is displayed.

Step 3 Set **Primary Authentication** to **Third-party SSO authentication**.

- If the default protocol type is OAuth2.0, perform **Step 4**.
- If the default protocol type is LDAP, perform **Step 5**.

Step 4 Set **View Type** to **Visual** and configure OAuth 2.0 parameters according to **Table 9-3**.

Step 5 Configure the LDAP parameters according to **Table 9-3**.

Step 6 Click **Save**.

----End

10 Internet Access Management

10.1 Enabling Small-scale Economical Internet Access (EIP)

10.2 Enabling Large-scale Enhanced Internet Access (NAT Gateway+EIP)

10.3 Disabling Internet Access

10.1 Enabling Small-scale Economical Internet Access (EIP)

Scenarios

Administrators can select small-scale economical Internet access (EIP) to enable Internet access for cloud desktops. After Internet access is enabled, cloud desktops can access the Internet.

Prerequisites

You have purchased a desktop.

Procedure

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

Step 2 In the navigation pane, choose **Internet Access Management**.

The **Internet Access** page is displayed.

Step 3 Click the button of enabling the Internet in the upper right corner of the page.

The page of enabling the Internet is displayed.

Step 4 Configure Internet access.

- **Type**.
  - **Economical (EIP)**: Desktops access the Internet through **EIP**. Each desktop is bound to an EIP. This mode is applicable when there are a small number of desktops.

NOTE

Enabling small-scale economical internet access will create the following network resources for you:

EIP provides independent public IP addresses and bandwidth for Internet access.

- **Billing Mode**. You can select a billing mode as required.
  - **Yearly/Monthly**, as shown in **Table 10-1**.
  - **Pay-per-use**, as shown in **Table 10-2**.

Table 10-1 Yearly/Monthly

Parameter	Description	Example
Billing Mode	Select **Yearly/Monthly**.	Yearly/Monthly
Bandwidth	The bandwidth ranges from 1 Mbit/s to 200 Mbit/s. You can customize the bandwidth as prompted.	-
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.	-
Required Duration	Set the required duration. **NOTE** You can determine whether to select **Auto-renew** as required.	-
Select Desktop	Search for the cloud desktop to be enabled with the Internet based on the desktop name.	-

Table 10-2 Pay-per-use

Parameter	Description	Example
Billing Mode	Select **Pay-per-use**.	Pay-per-use

Parameter	Description	Example
Public Network Bandwidth	If you select **By Bandwidth**, the bandwidth ranges from 1 Mbit/s to 200 Mbit/s by default. You can customize the bandwidth as prompted.	-
	If you select **By Traffic**, the bandwidth ranges from 5 Mbit/s to 200 Mbit/s by default. You can customize the bandwidth as prompted.	-
Select Desktop	Search for the cloud desktop to be enabled with the Internet based on the desktop name.	-

- If you set **Billing Mode** to **Yearly/Monthly**, perform operations from **Step 5** to **Step 9**.
- If you set **Billing Mode** to **Pay-per-use**, perform operations from **Step 10** to **Step 11**.

Step 5 Click **Confirming Configuration**. The Internet access configuration page is displayed.

Step 6 Click **OK**. The **Buy Workspace** page is displayed.

Step 7 Check the cloud service order and the fee to be paid.

Step 8 Select one of the following payment methods:

- Balance payment.
- Online payment. It supports multiple online payment modes.

Step 9 After the payment method is selected and the payment is successful, the purchase is complete.

Step 10 Click **Confirming Configuration**. The Internet access configuration page is displayed.

Step 11 Click **OK**, the purchase is complete.

----End

10.2 Enabling Large-scale Enhanced Internet Access (NAT Gateway+EIP)

Scenarios

Administrators can configure a **NAT gateway** and a **EIP** for each subnet as required. After they are enabled, all desktops in the subnet can access the Internet.

Prerequisites

You have purchased a desktop.

Procedure

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

Step 2 In the navigation pane, choose **Internet Access Management**.

The **Internet Access** page is displayed.

Step 3 Click the button of enabling the Internet in the upper right corner of the page.

The page of enabling the Internet is displayed.

Step 4 Configure Internet information, as shown in **Table 10-3**.

NOTE

Enabling large-scale enhanced Internet access will create the following networking resources for you:

1. Public **NAT Gateway** can be used to easily construct the network address translations for VPC.
2. **EIP** provides independent public IP addresses and bandwidth for Internet access.

Table 10-3 Parameter description

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 subnet as required.	-

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 to implement the NAT service. 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 **xlarge**.	-
EIP Name	The Elastic IP (EIP) service provides independent public IP addresses and bandwidth for Internet access. **Learn more.**	-
Public Network Bandwidth	If you select **By Bandwidth**, the bandwidth ranges from 1 Mbit/s to 200 Mbit/s by default. You can customize the bandwidth as prompted.	-
	If you select **By Traffic**, the bandwidth ranges from 5 Mbit/s to 200 Mbit/s by default. You can customize the bandwidth as prompted.	-

Parameter	Description	Example Value
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.	-

Step 5 Click **OK**, the purchase is complete.

----End

10.3 Disabling Internet Access

Scenarios

Cancel the Internet access permission of desktops for which the Internet access function has been enabled.

Prerequisites

You have enabled the small-scale economical or large-scale enhanced Internet access for the workspace.

Procedure

Step 1 **Log in to the management 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**, go to **Step 4**.
- If you select **Enhanced**, go to **Step 8**.

Step 4 Select a target desktop in the list of **Economical**.

Step 5 Click **Disable Internet** in the upper left corner or in the **Operation** column.

The **Disable Internet** page is displayed.

Step 6 Select a disable mode as required.

- Unbinding only the EIP. After that, the desktop can be bound again.
- Unbinding and deleting the EIP. After confirmation, you will be redirected to the EIP management page. Select the EIP to unbind and delete it.

Step 7 Click **OK**.

Step 8 Click **Disable Internet** in the **Operation** column in the list of **Enabled**.

The **Close the Internet** page is displayed.

Step 9 View the configuration information about disabling the Internet access.

NOTE

1. To disable Internet access, you need only to delete the SNAT rule. Related resources will not be deleted.

2. Delete related resources that are not in use. Otherwise, fees will be generated.

- To delete an SNAT rule, click **Delete >>**. In the SNAT rule list, locate the SNAT rule to be deleted, and click **Delete** in the **Operation** column.
- (Optional) To delete an EIP, click **Delete >>**. On the displayed page, locate the EIP to be deleted, and choose **More** > **Release** in the **Operation** column.
- (Optional) To delete a NAT gateway, click **Delete >>**. On the displayed page, locate the NAT gateway to be deleted, and click **Delete** in the **Operation** column.

  NOTE

  Delete related resources that are not in use as required. Otherwise, fees will be generated.

----End

11 Scheduled Tasks

11.1 Scheduled Shutdown

11.2 Scheduled Startup

11.3 Scheduled Restart

11.4 Scheduled Hibernation

11.5 Scheduled System Disk Recomposing

11.1 Scheduled Shutdown

Scenarios

This section describes how to shut down a cloud desktop or a desktop pool periodically.

Impact on the System

Personal application data that is not saved in the desktop may be lost after the desktop is shut down.

Prerequisites

Scheduled shutdown can be performed only on desktops that have been created and are running.

Procedure

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

Step 2 In the navigation pane, choose **Scheduled Task**.

The **Scheduled Task** page is displayed.

Step 3 Click the button of creating a task in the upper right corner of the page.

The dialog box of creating a task is displayed.

Step 4 Configure a scheduled task.

- **Task Type**: Select **power off**.

  NOTE

  Task of forcible shutdown: After configuring a scheduled shutdown task, the desktop will not be shut down when it is still connected, even if the scheduled time arrives. Instead, the shutdown is automatically postponed to the next scheduled time. If you choose to execute the task of forcible shutdown, the desktop will be forcibly shut down when the scheduled time arrives.

- **Scheduled Task Name**: This parameter is user-defined.
- **Execution Cycle**: The following cycles are supported. You can select a cycle as required.
  - **Specified time**: The time is accurate to seconds.
  - **By day**: You can set the specific time, interval (days), and expiration time.
  - **By week**: You can set the specific date, time, and expiration time.
  - **By the month**: You can set the specific month, date, time, and expiration time.

Step 5 Click **Next: Select Objects**.

The **Select Target Object** page is displayed.

Step 6 In the **Available Objects** area, search for the target desktop name in the search box and select it.

Step 7 Click **Create Now**.

----End

11.2 Scheduled Startup

Scenarios

This section describes how to start up a cloud desktop or a desktop pool periodically.

Impact on the System

This operation has no adverse impact on the system.

Prerequisites

Scheduled startup can be performed only on desktops that have been created and are in the **Stopped** status.

Procedure

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

Step 2 In the navigation pane, choose **Scheduled Task**.

The **Scheduled Task** page is displayed.

Step 3 Click the button of creating a task in the upper right corner of the page.

The dialog box of creating a task is displayed.

Step 4 Configure a scheduled task.

- **Task Type**: Select **power on**.
- **Scheduled Task Name**: This parameter is user-defined.
- **Execution Cycle**: The following cycles are supported. You can select a cycle as required.
  - **Specified time**: The time is accurate to seconds.
  - **By day**: You can set the specific time, interval (days), and expiration time.
  - **By week**: You can set the specific date, time, and expiration time.
  - **By the month**: You can set the specific month, date, time, and expiration time.

Step 5 Click **Next: Select Objects**.

The page of selecting target objects is displayed.

Step 6 In the **Available Objects** area, search for the target desktop or desktop pool name in the search box and select it.

Step 7 Click **Create Now**.

----End

11.3 Scheduled Restart

Scenarios

This section describes how to restart a cloud desktop or a desktop pool periodically.

Impact on the System

Personal application data that is not saved in the desktop may be lost after the desktop is restarted.

Prerequisites

Scheduled restart can be performed only on desktops that have been created and are running.

Procedure

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

Step 2 In the navigation pane, choose **Scheduled Task**.

The **Scheduled Task** page is displayed.

Step 3 Click the button of creating a task in the upper right corner of the page.

The dialog box of creating a task is displayed.

Step 4 Configure a scheduled task.

- **Task Type**: Select **reboot**.

  NOTE

  Task of forcible restart: 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 restart is automatically postponed to the next scheduled time. If you choose to execute the task of forcible restart, the desktop will be forcibly restarted when the scheduled time arrives.

- **Scheduled Task Name**: This parameter is user-defined.
- **Execution Cycle**: The following cycles are supported. You can select a cycle as required.
  - **Specified time**: The time is accurate to seconds.
  - **By day**: You can set the specific time, interval (days), and expiration time.
  - **By week**: You can set the specific date, time, and expiration time.
  - **By the month**: You can set the specific month, date, time, and expiration time.

Step 5 Click **Next: Select Objects**.

The page of selecting target objects is displayed.

Step 6 In the **Available Objects** area, search for the target desktop or desktop pool name in the search box and select it.

Step 7 Click **Create Now**.

----End

11.4 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

Scheduled hibernation can be performed only on desktops that have been created and are running.

Procedure

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

Step 2 In the navigation pane, choose **Scheduled Task**.

The **Scheduled Task** page is displayed.

Step 3 Click the button of creating a task in the upper right corner of the page.

The dialog box of creating a task is displayed.

Step 4 Configure a scheduled task.

- **Task Type**: Select **sleep**.

  NOTE

  1. Scheduled hibernation can be performed only on Windows desktops.
  2. Task of forcible hibernation: 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 hibernation is automatically postponed to the next scheduled time. If you choose to execute the task of forcible hibernation, the desktop will be forcibly hibernated when the scheduled time arrives.

- **Scheduled Task Name**: This parameter is user-defined.
- **Execution Cycle**: The following cycles are supported. You can select a cycle as required.
  - **Specified time**: The time is accurate to seconds.
  - **By day**: You can set the specific time, interval (days), and expiration time.
  - **By week**: You can set the specific date, time, and expiration time.
  - **By the month**: You can set the specific month, date, time, and expiration time.

Step 5 Click **Next: Select Objects**.

The page of selecting target objects is displayed.

Step 6 In the **Available Objects** area, search for the target desktop or desktop pool name in the search box and select it.

Step 7 Click **Create Now**.

----End

11.5 Scheduled System Disk Recomposing

Scenarios

This section describes how to recompose a system disk periodically for a cloud desktop or a desktop pool. For details about the impact and restrictions of system disk recomposing on the system, see section **2.4 Recomposing a System Disk**.

Procedure

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

Step 2 In the navigation pane, choose **Scheduled Task**.

The **Scheduled Task** page is displayed.

Step 3 Click the button of creating a task in the upper right corner of the page.

The dialog box of creating a task is displayed.

Step 4 Configure a scheduled task.

- **Task Type**: Select **Rebuild the system disk**.
- **Scheduled Task Name**: This parameter is user-defined.
- **Reestablishment Mode**: The default value is **Reinstall OS**.
- **Execution Cycle**: The following cycles are supported. You can select a cycle as required.
  - **Specified time**: The time is accurate to seconds.
  - **By day**: You can set the specific time, interval (days), and expiration time.
  - **By week**: You can set the specific date, time, and expiration time.
  - **By the month**: You can set the specific month, date, time, and expiration time.
- **Notice The User**: Set this parameter as required. If you select **Notice**, you can configure the notification content as required.

  NOTE

  Notification messages are supported only in Windows.
- Enter **Reinstalling the System Disk** to confirm the system disk recomposing.

Step 5 Click **Next: Select Objects**.

The page of selecting target objects is displayed.

NOTE

After you click **Next: Select Objects**, the authorization description is displayed for the first time.

Cloud service administrator permissions: Workspace supports scheduled system disk recomposing and auto scaling. Therefore, the tenant administrator permissions are required.

After the authorization is approved (for the first time), an agency named **workspace_admin_trust** will be created in IAM. To ensure normal service usage, do not delete or modify the agency when using scheduled tasks or desktop pools. For details, see section **System Entrustment Description**.

Step 6 In the **Available Objects** area, search for the target desktop or desktop pool name in the search box and select it.

Step 7 Click **Create Now**.

----End

12 Application Center

12.1 Application Distribution

12.2 Application Management

12.1 Application Distribution

12.1.1 Adding an Application

Scenario

Administrators can upload enterprise applications or third-party applications and manage and allocate applications through App Center in a unified manner.

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 Workspace 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 12-1** and **Table 12-2**.

Table 12-1 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
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 • 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.	-

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	-

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 12-2 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 12-1**.
Registered Version	Registration item **DisplayVersion** in the registry after the application is installed.	-	Value: 0.0.8.0 See **Figure 12-1**.
Executable Program Name	File name of the application program executed when the application is started.	-	-

NOTE

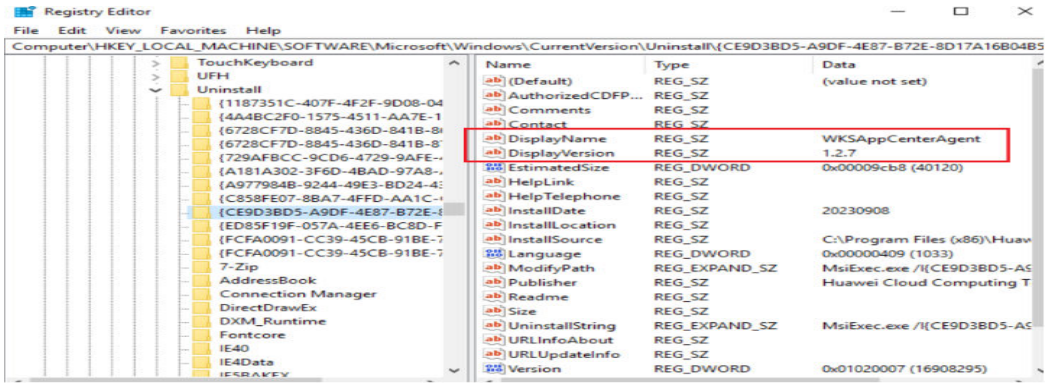
About advanced settings:

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 12-1 Example of App Center



Step 5 Select **I have read and agree to Non-infringement Commitment and Disclaimer**. Click **Confirm**.

----End

12.1.2 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 12-3** as required.

Table 12-3 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

12.1.3 Setting Up a File Server

Scenario

Set up a file server.

Prerequisites

- A Windows Server ECS is available. For details, see **Creating 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**.

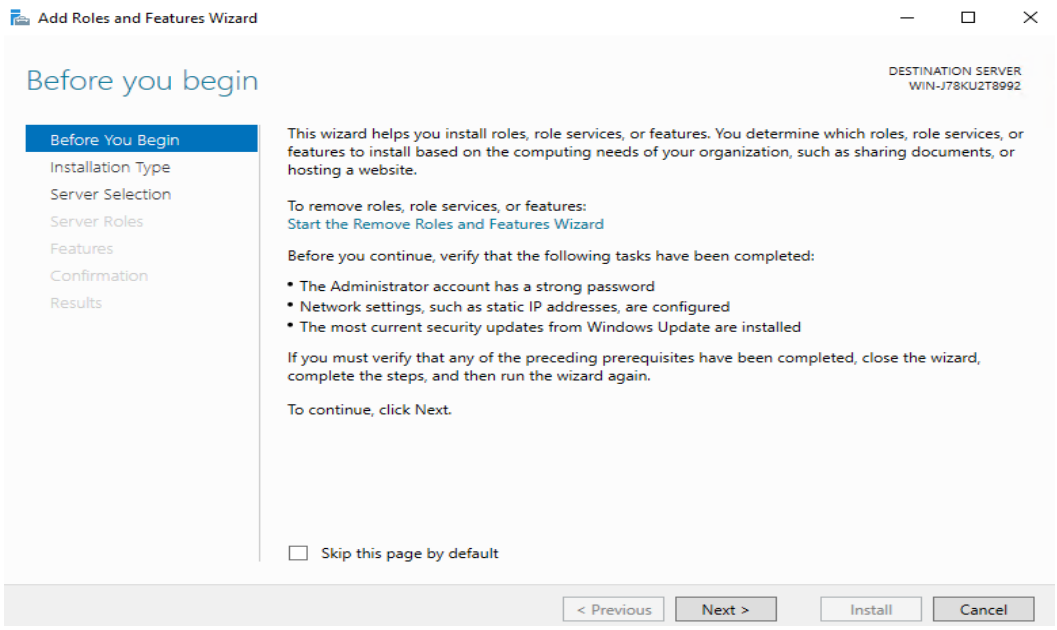
Step 3 Locate the row that contains the target ECS, click **Remote Login** in the **Operation** column, and enter the username and password created during ECS purchase.

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.

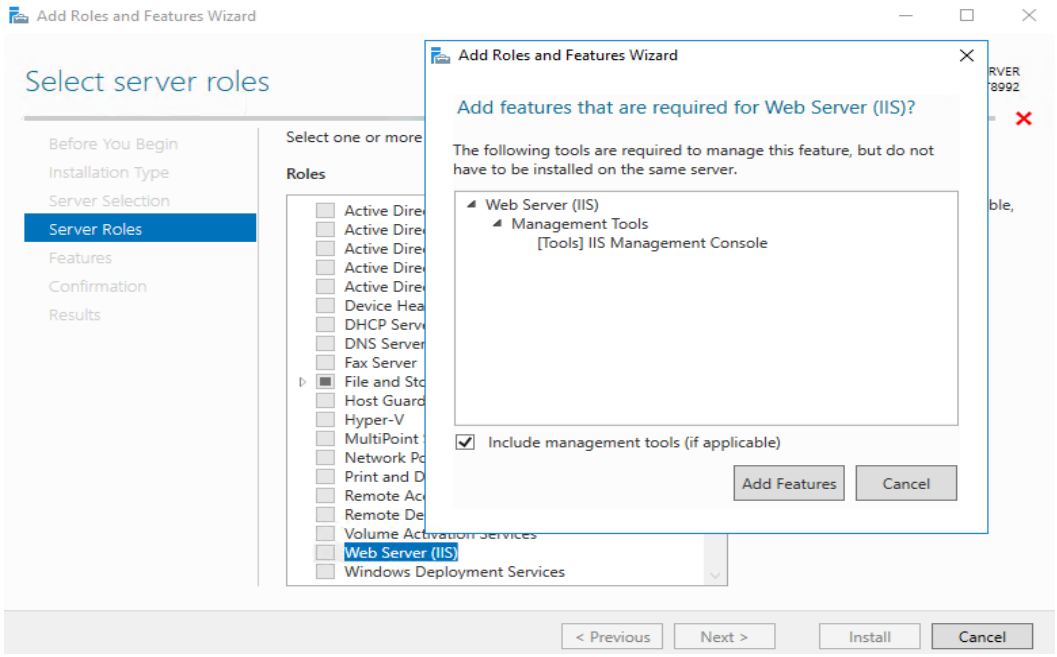
Step 5 On the **Server Manager** page, click **Add role and features**. The **Add Roles and Features Wizard** dialog box is displayed, as shown in **Figure 12-2**.

Figure 12-2 Installation wizard



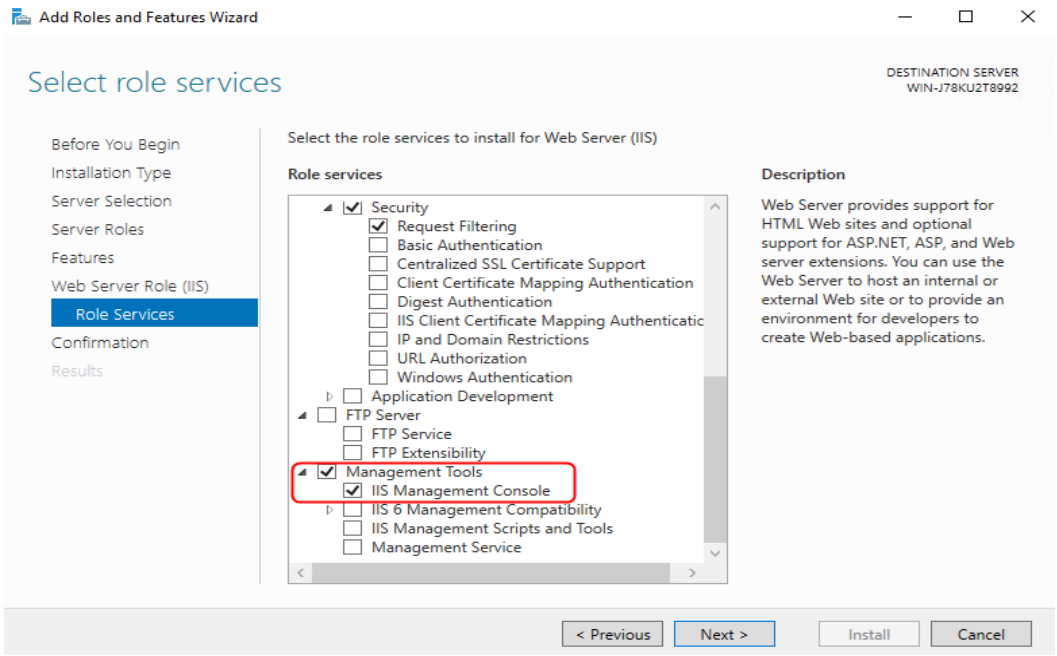
Step 6 Click **Next** as prompted. On the **Server Roles** page, select **Web Server (IIS)**. In the displayed **Add features that are required for Web Server (IIS)** dialog box, click **Add Features**, as shown in **Figure 12-3**.

Figure 12-3 Configuring a server role



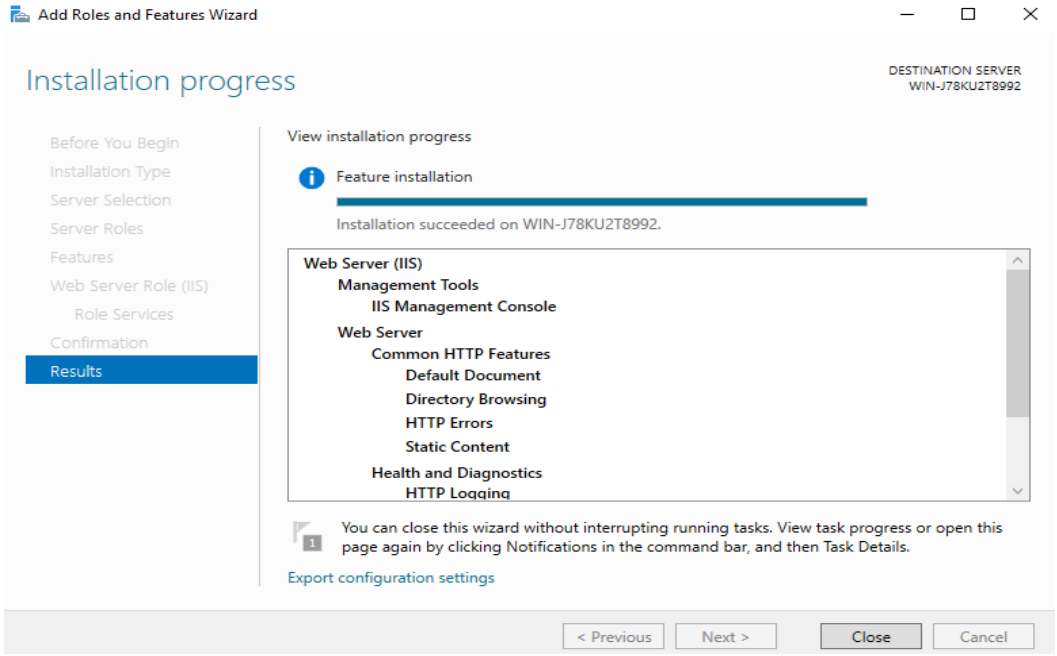
Step 7 Click **Next**. On the **Role Services** page, ensure that **IIS Management Console** under **Management Tools** has been selected, as shown in **Figure 12-4**.

Figure 12-4 IIS management console



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 12-5** is displayed, the installation is successful.

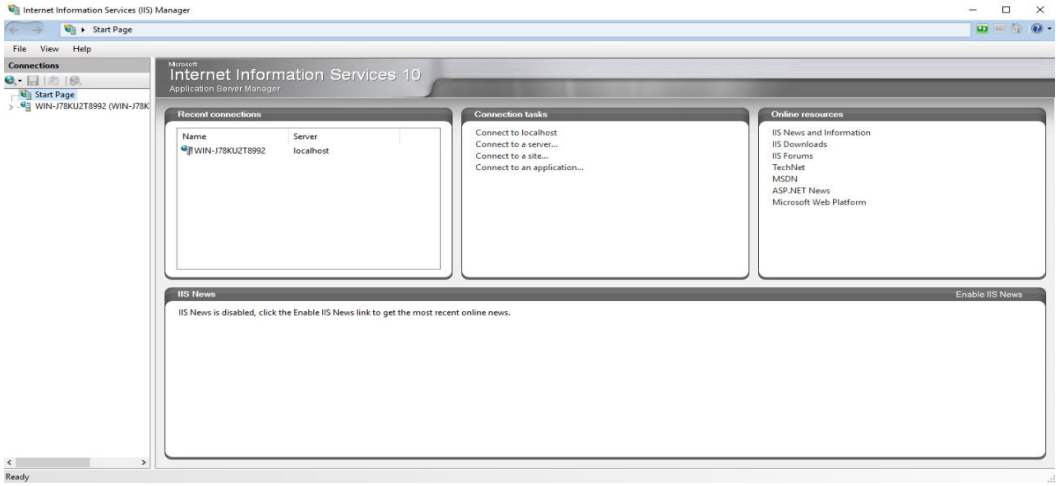
Figure 12-5 Example installation result



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 12-6**.

Figure 12-6 IIS Manager



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.

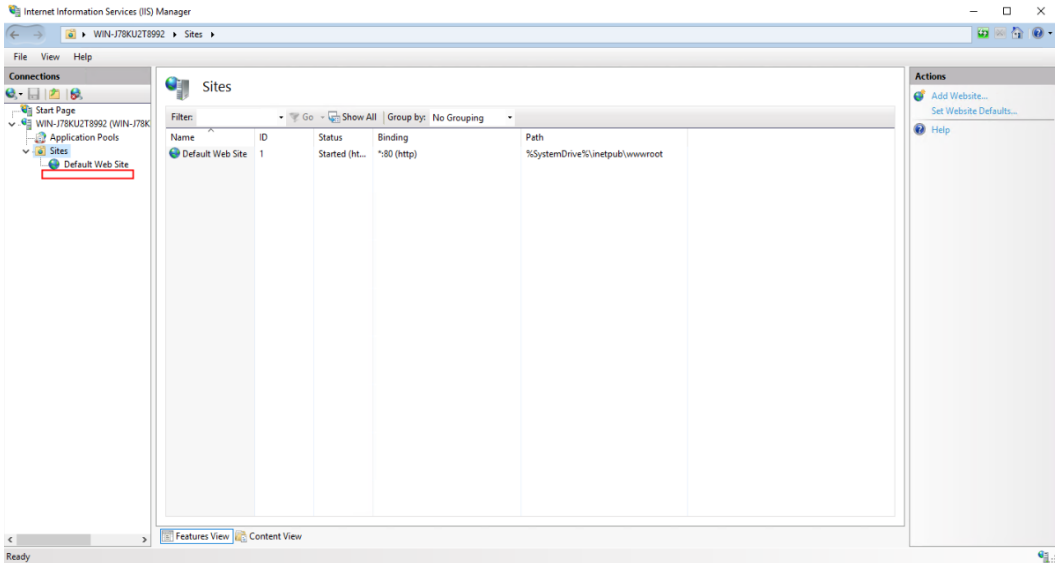
Step 11 Right-click **Sites** and choose **Add Website** from the shortcut menu to configure website information.

- **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 12-7**.

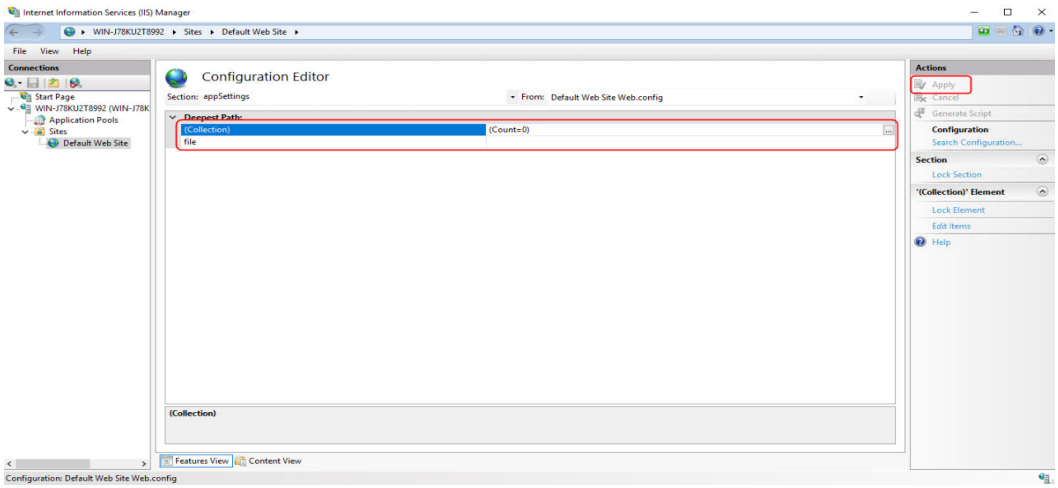
Figure 12-7 Adding a website



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 12-8**.

Figure 12-8 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 12-9**.

Figure 12-9 Opening an application

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 12-1**. 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**.

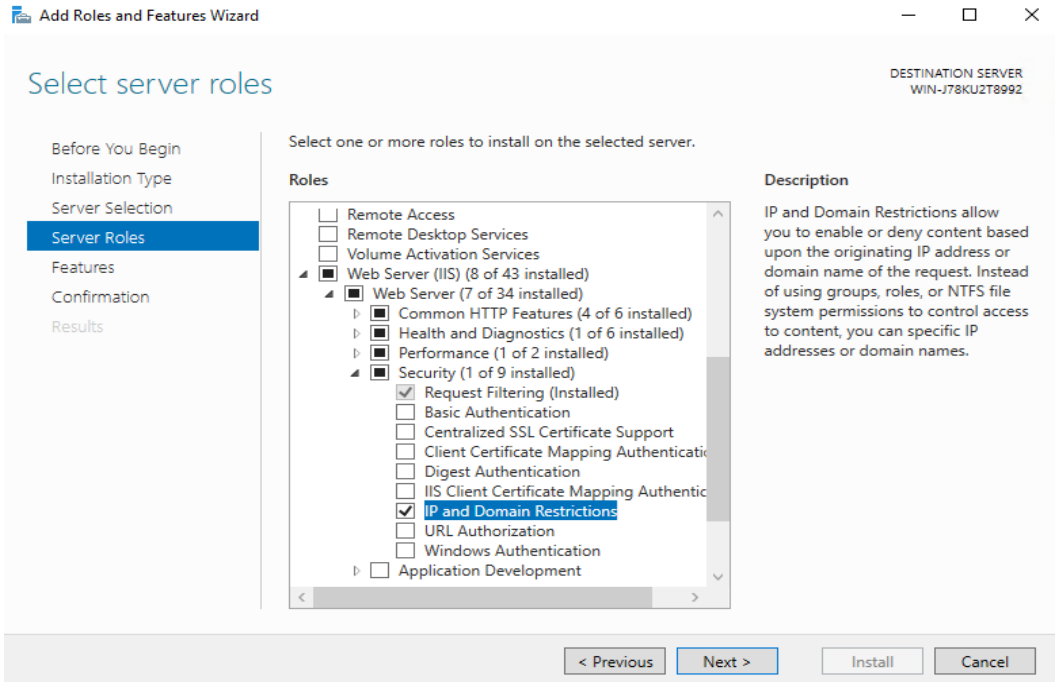
Step 3 Locate the row that contains the target ECS, click **Remote Login** in the **Operation** column, and enter the username and password created during ECS purchase.

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.

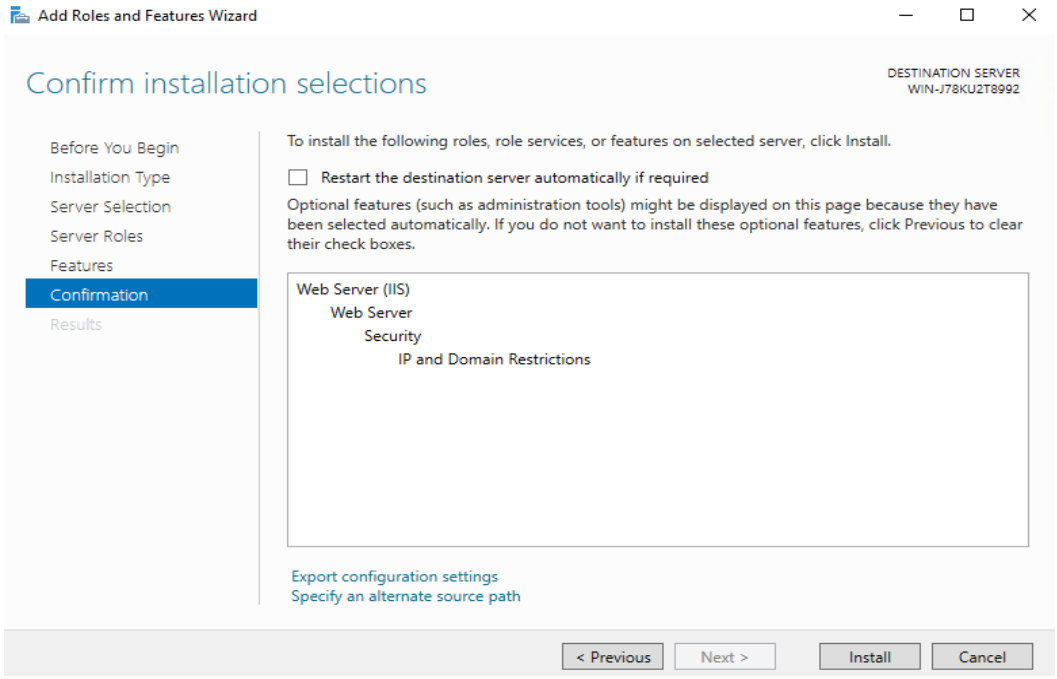
Step 6 On the **Server Roles** page, select **Web Server (IIS)**, choose **Web Server** > **Security**, and select **IP and Domain Restrictions**, as shown in **Figure 12-10**.

Figure 12-10 Adding a server role



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 12-11**.

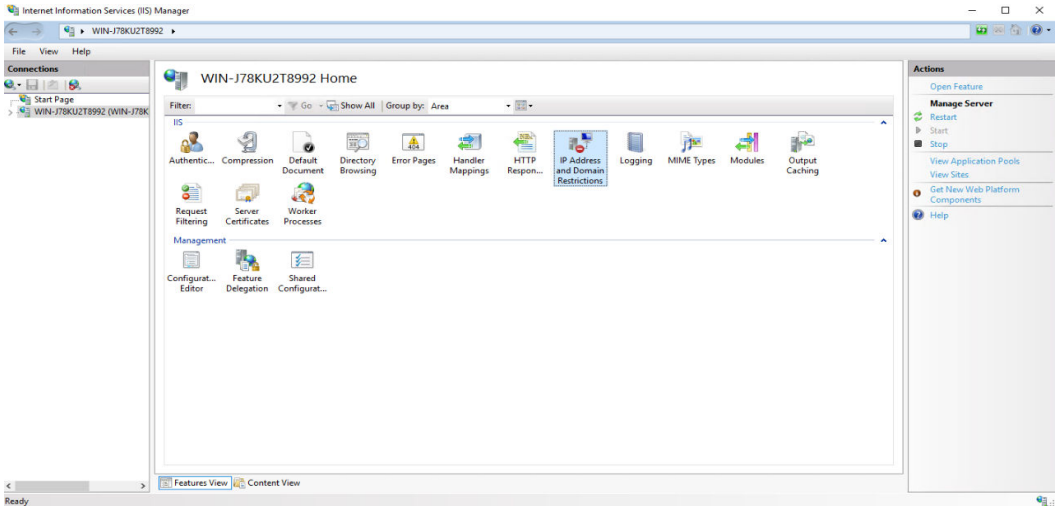
Figure 12-11 Confirmation page



Step 8 Click **Install**.

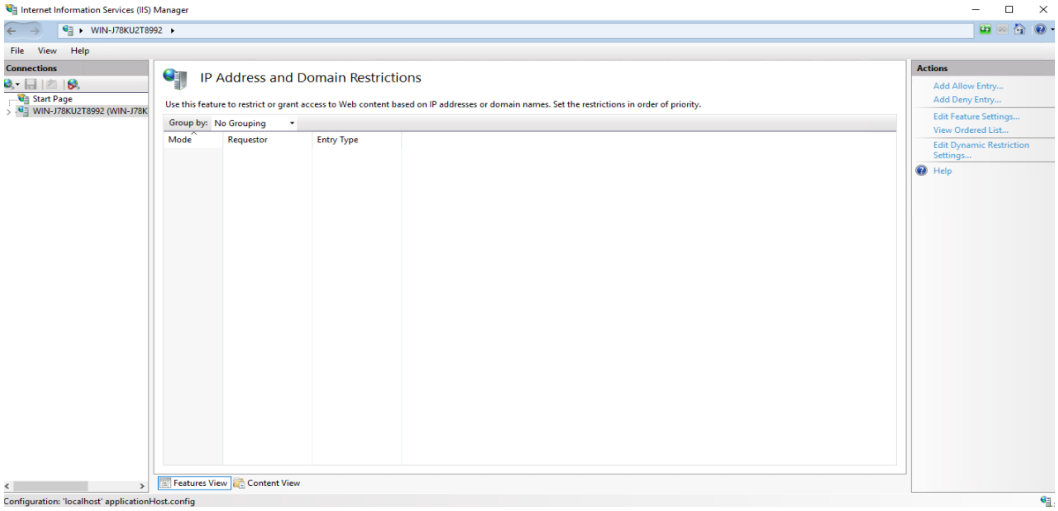
Step 9 Click in the lower left corner of the ECS and choose **Administrative Tools** > **Internet Information Service (IIS) Manager**. The **Internet Information Service (IIS) Manager** page is displayed. Click the *host name*, as shown in **Figure 12-12**.

Figure 12-12 Host name home page



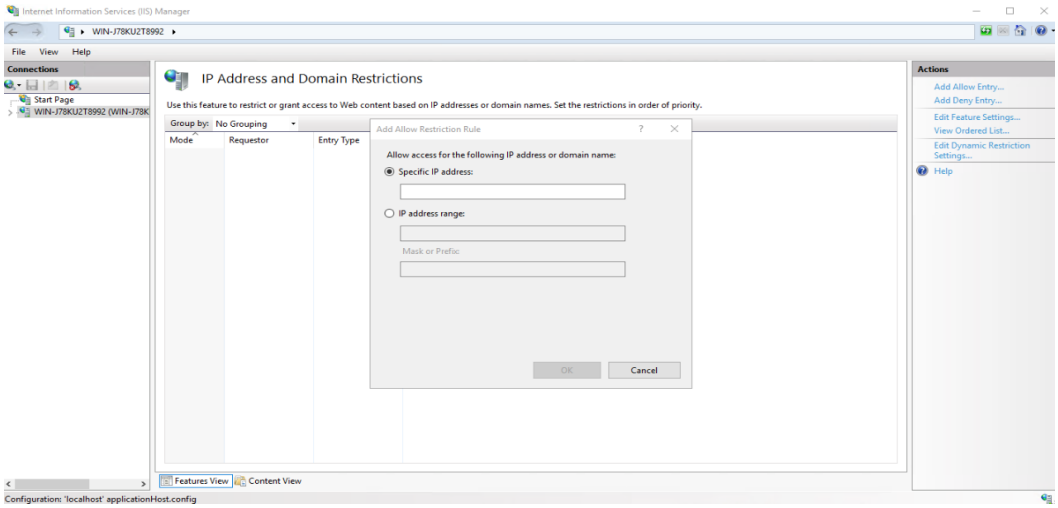
Step 10 Double-click **IP Address and Domain Restrictions** on the host name page. The **IP Address and Domain Restrictions** page is displayed, as shown in **Figure 12-13**.

Figure 12-13 IP address and domain restrictions



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 12-14**.

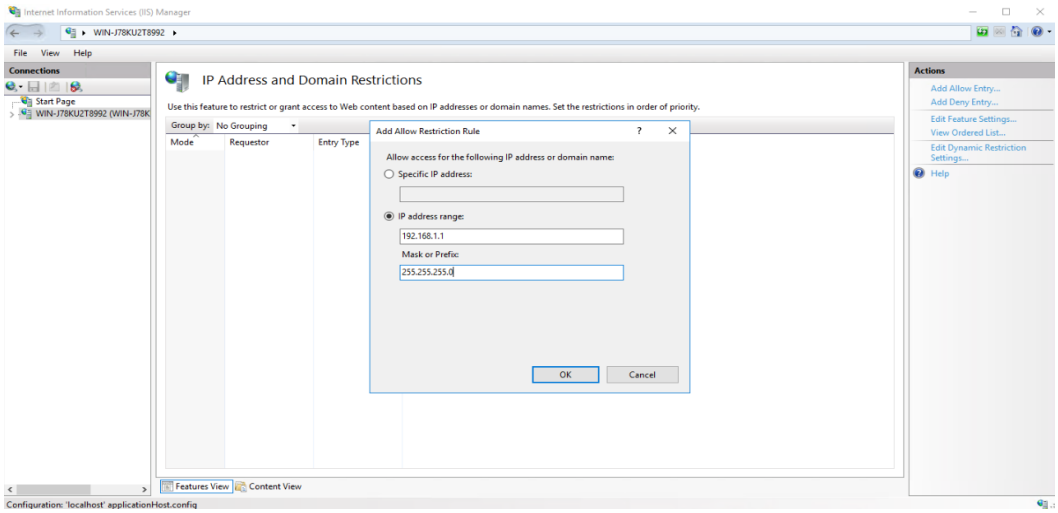
Figure 12-14 Adding allow restriction rules



Step 12 In the **Add Allow Restriction Rule** dialog box, select and configure **IP address range**, as shown in **Figure 12-15**.

- **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 12-15 Configuring restriction rules



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

12.2 Application Management

Scenario

You can configure tenant application management rules on the Workspace console to manage applications in a unified manner.

Prerequisites

Identification conditions for a product information rule have been created.

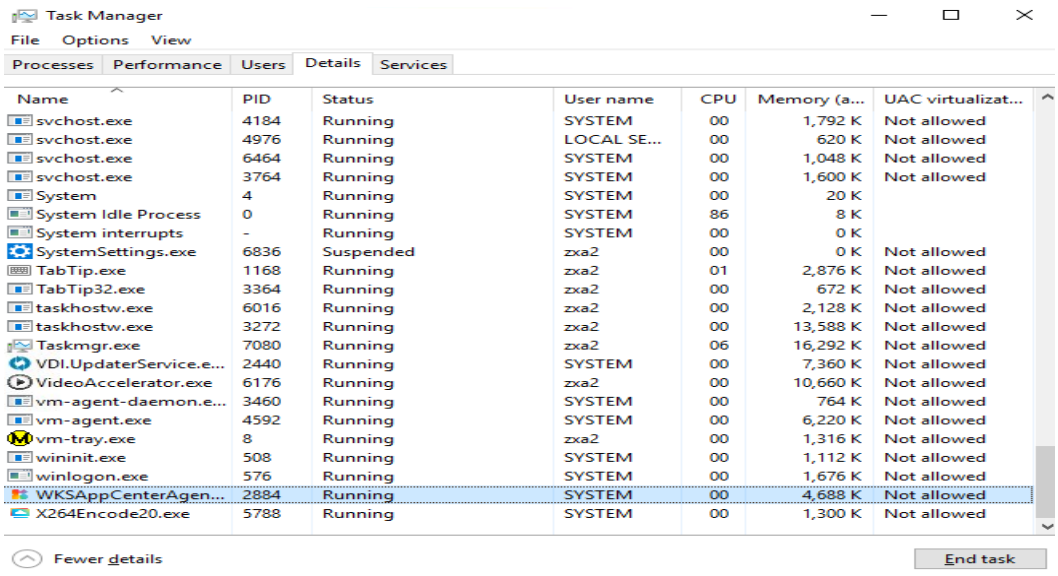
Obtaining the process name

Step 1 The administrator runs the applications 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 12-16**.

Figure 12-16 Process name



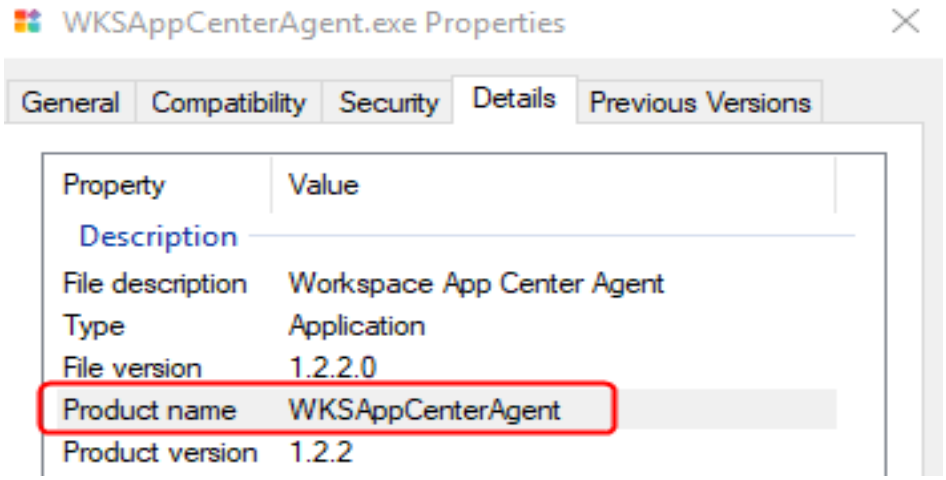
Obtaining the product name

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 12-17**.

Figure 12-17 Product name



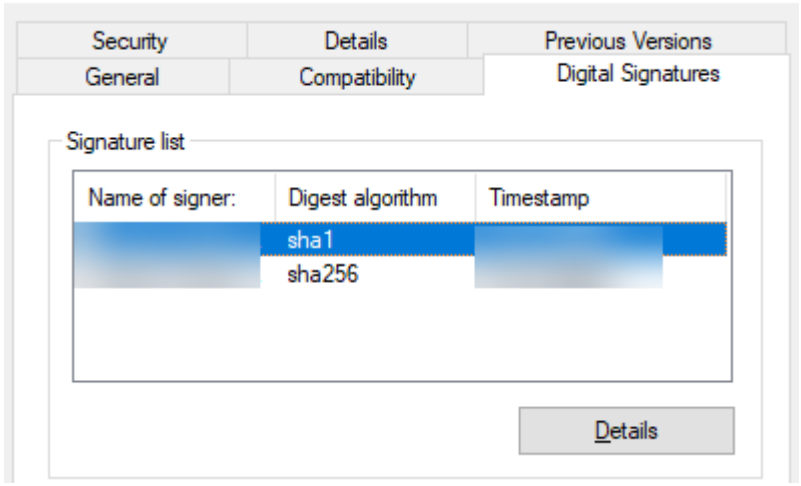
Obtaining the publisher name

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 12-18**.

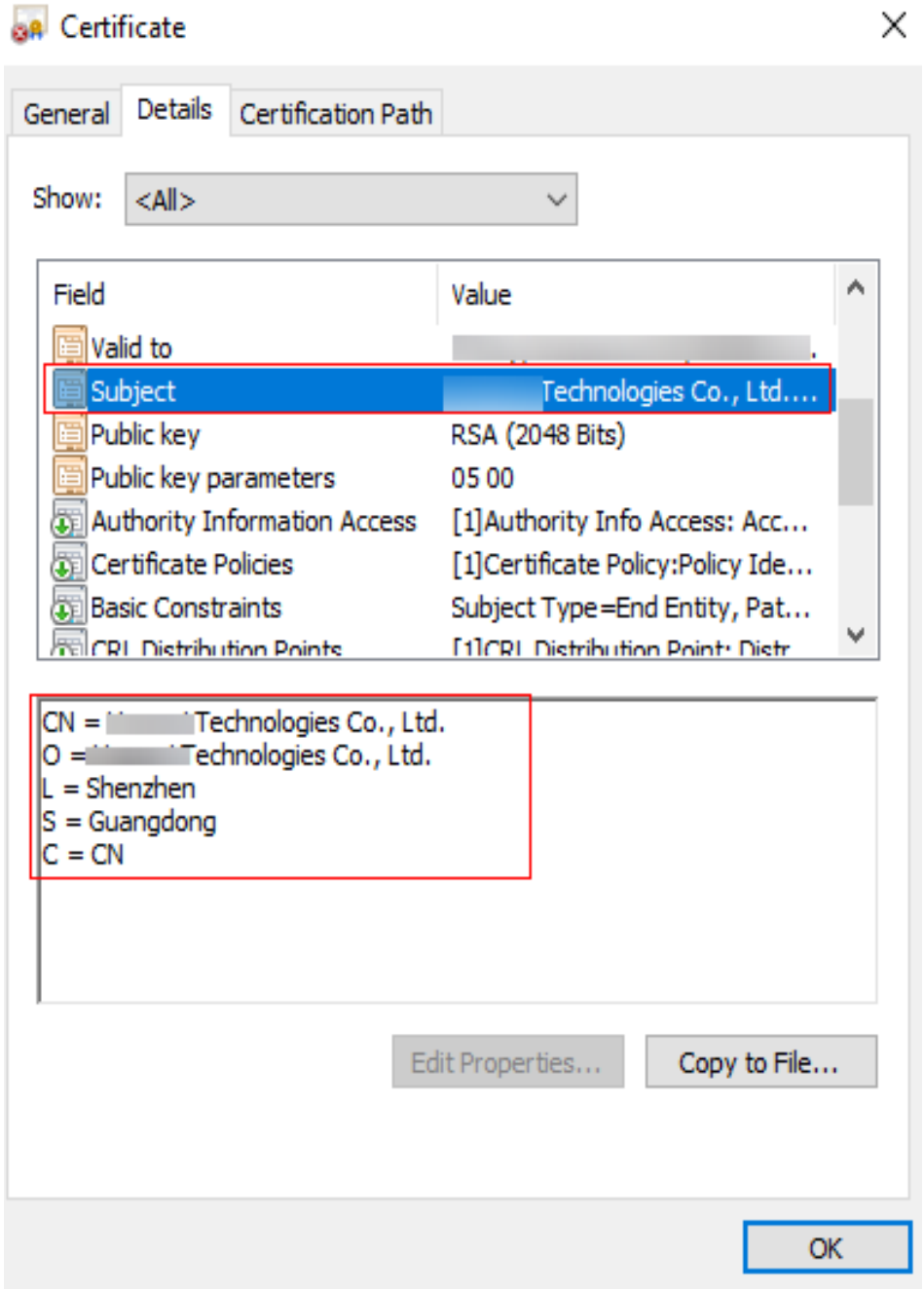
Figure 12-18 Digital signature



Step 10 On the displayed page of digital signature details, click **View Certificate**. The **Certificate** page is displayed.

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 12-19**.

Figure 12-19 Subject information



----End

Procedure

Step 1 Log in to the Workspace 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**. The **Create Path Rule** page is displayed.

- **Rule Name**: The name can contain 1 to 64 characters (spaces included), but cannot contain only spaces.
- **Rule Description**: The description can contain up to 128 characters (spaces included), but cannot contain 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**. The **Create Product Information Rule** page is displayed.

- **Rule Name**: The name can contain 1 to 64 characters (spaces included), but cannot contain only spaces.
- **Rule Description**: The description can contain up to 128 characters (spaces included), but cannot contain only spaces.
- **Identified By**
  - **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 row that contains the desired path rule. The **Modify Path Rule** page is displayed.

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 row that contains the desired product information rule. The **Modify Product Information Rule** page is displayed.

Step 11 You can modify the rule name, rule description, and identification conditions as required.

Step 12 Click **OK**.

Deleting a rule

Step 13 On the top navigation bar, click **App Rule Library**.

Step 14 Delete the created rule as required.

- To delete a single application rule, click **Delete** in the **Operation** column of the application rule to be deleted. In the displayed dialog box, click **OK**.

- To delete rules in batches, select the application rules to be deleted and click **Batch Delete**. In the displayed dialog box, click **OK**.

Application management: Adding an application rule

Step 15 On the top navigation bar, click **App Management**.

- **App Management**:
  -  : Disabled
  -  : Enabled

    NOTE

    Blacklist policy rules:

    1. When a desktop user opens a blacklisted app, the app will not run.
    2. The policy cannot take effect on running processes.
    3. The policy takes effect after 5 minutes.
- **App Management Mode**: **Do not run apps in the list**

Step 16 Click **Add App Rule**. The **Add App Rule** dialog box is displayed.

Step 17 Search for and select the application rule to be added based on the rule name, and click **OK**.

Application management: Deleting an application rule

Step 18 On the top navigation bar, click **App Management**.

Step 19 Delete the added application rule as required.

- To delete a single application rule, click **Delete** in the **Operation** column of the application rule to be deleted. In the displayed dialog box, click **OK**.
- To delete rules in batches, select the application rules to be deleted and click **Batch Delete**. In the displayed dialog box, click **OK**.

----End

13 Private Images

13.1 Creating a Windows Private Image

13.1 Creating a Windows Private Image

13.1.1 Required Software

Table 13-1 lists the software packages required for creating a Windows private image.

Table 13-1 Required software packages

Name	Description	How to Obtain
Workspace_HDP_WindowsDesktop_Installer_x.x.x.iso	Windows image creation tool	Contact technical support engineers.
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.

Name	Description	How to Obtain
VMTools driver package	VMTools driver	Contact technical support engineers.
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.
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. **NOTE**
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.

Name	Description	How to Obtain
WKSAppCenterAgent.msi WKSAppCenter.msi	Needs to be installed when Workspace uses the application center. Double-click to install.	Contact technical support engineers.

13.1.2 Registering a Private Image Using an ISO File

Scenario

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 13-1**.

  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 VMTools driver into an ISO File using AnyBurn

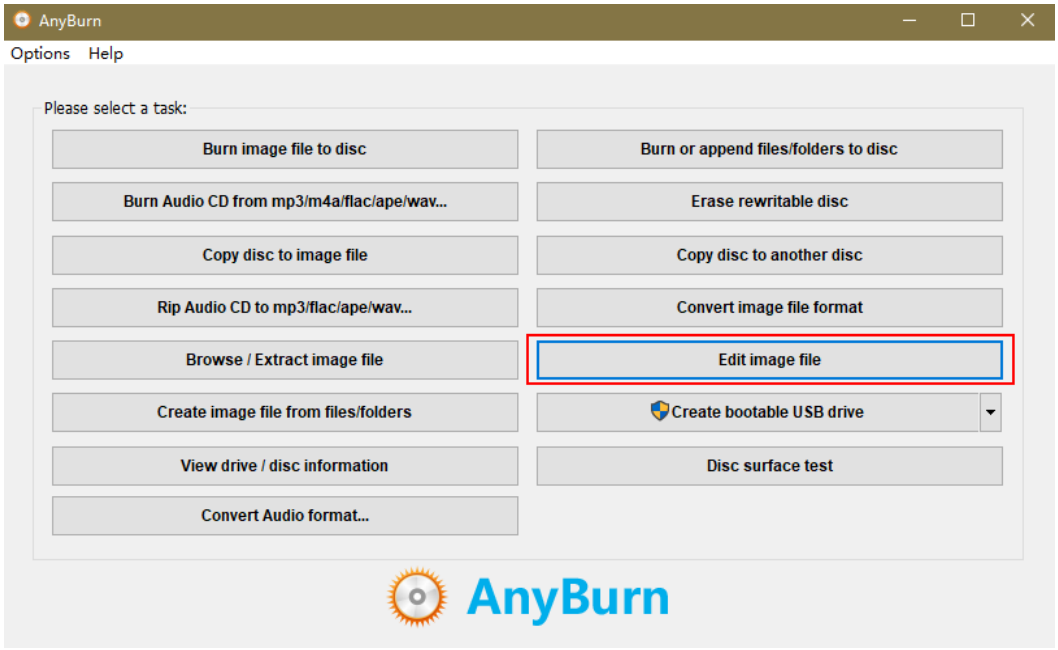
Step 1 Install AnyBurn on the local PC.

Step 2 Download the VMTools driver package and decompress it to your local PC.

Step 3 Use AnyBurn to open the ISO file.

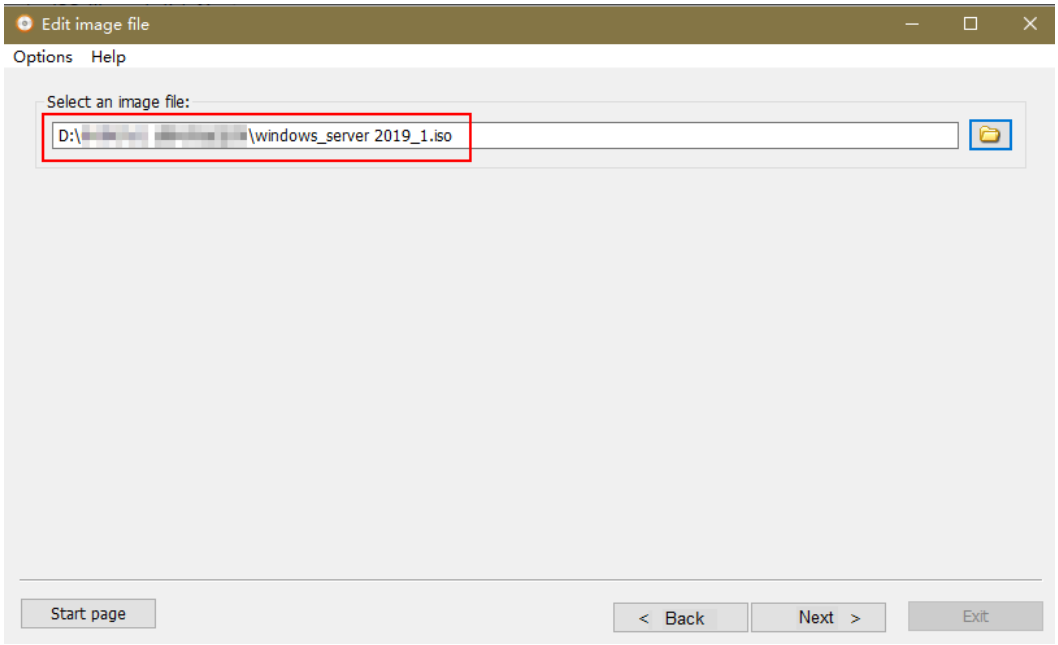
Open the AnyBurn software and select **Edit Image File**, as shown in **Figure 13-1**.

Figure 13-1 Editing an image file



Select the ISO file and click **Next**, as shown in **Figure 13-2**.

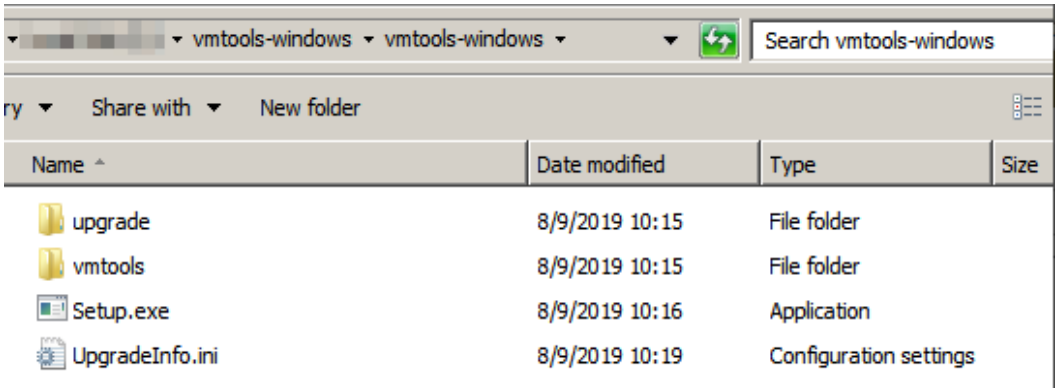
Figure 13-2 Selecting the ISO file



Step 4 Edit the ISO file to integrate the VMTools driver.

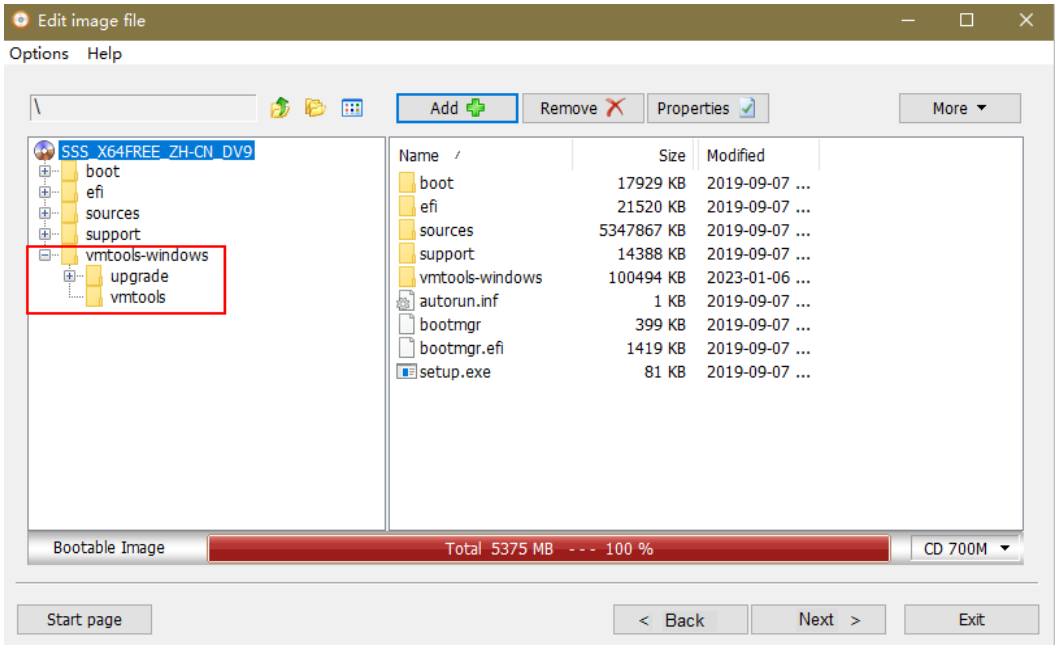
Decompress the **vmtools-windows.zip** file downloaded in **2** to obtain **vmtools-windows.iso**, and then decompress **vmtools-windows.iso** to obtain the **vmtools-windows** folder, as shown in **Figure 13-3**.

Figure 13-3 vmtools-windows folder



Drag the decompressed **vmtools-windows** folder to the parent node of the ISO file (or click **Add** and select the **vmtools-windows** folder), and click **Next**, as shown in **Figure 13-4**.

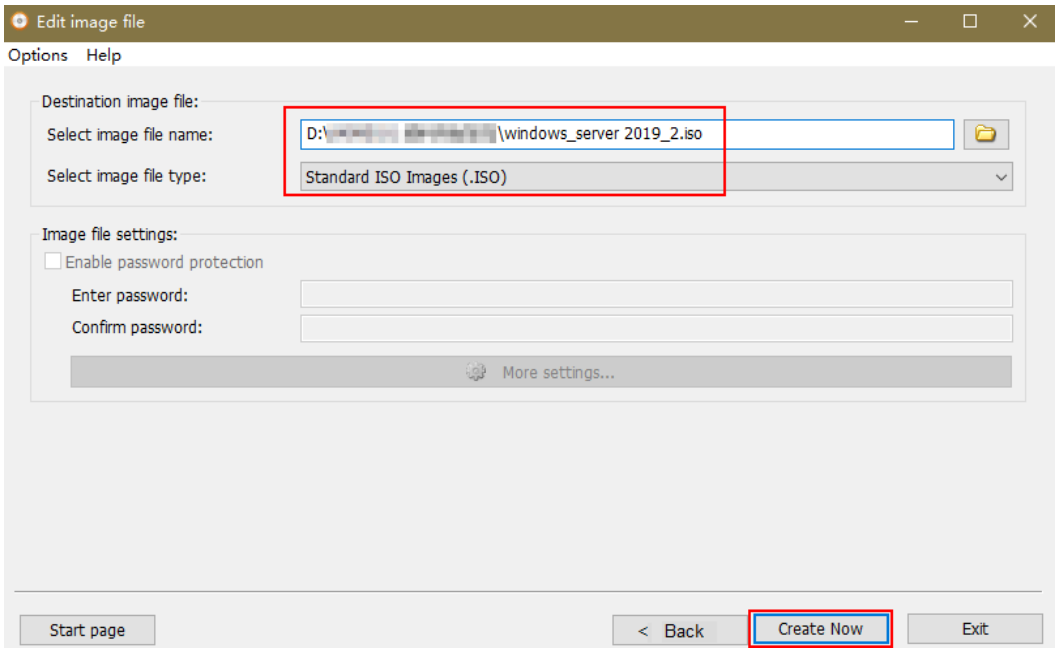
Figure 13-4 Adding the **vmtools-windows** folder to the parent node of the ISO file



Specify the save path and ISO file name, select the ISO format, and click **Create Now**.

After the ISO file is generated, view the ISO file integrated with the VMTools driver in the save path, as shown in **Figure 13-5**.

Figure 13-5 Viewing the ISO file integrated with the VMTools driver



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 13-2**. Retain the default values for the parameters that are not listed below.

Table 13-2 Image parameters

Parameter	Description
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

13.1.3 Creating an ECS

Scenario

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 **13.1.2 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 **13.1.2 Registering a Private Image Using an ISO File**.

Step 4 On the displayed page, configure the parameters in **Table 13-3** and retain the default values for other parameters.

Table 13-3 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 13-4**.

Table 13-4 Security group configuration

Parameter	Description	Example Value
Name	The value can be customized.	-
Enterprise Project	Use the enterprise project selected in **Step 4**. **NOTE** This parameter is mandatory when the enterprise project function is enabled.	default

Parameter	Description	Example Value
Template	• **General-purpose web server**: The security group that you create using this template is for general-purpose web servers and includes default rules that allow all inbound ICMP traffic and allow inbound traffic on ports 22, 80, 44, 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 13-5**.

Table 13-5 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

13.1.4 Configuring an ECS

Scenario

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 **13.1.1 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.

Installing a Windows OS and the VMTools Driver

Step 1 Log in to the console.

Step 2 Choose **Service List** > **Computing** > **Elastic Cloud Server**.

Step 3 Locate the row that contains the ECS created in **13.1.3 Creating an ECS**, and click **Remote Login** to log in to the Windows VM.

Step 4 For details, see **Installing a Windows OS and the VMTools Driver**.

NOTE

When selecting the OS installation location, ensure that the driver version of Windows Server 2019 is the same as that of Windows Server 2016. That is, set **$OS_Version** in **vmtools-windows/upgrade/$OS_Version/drivers/viostor** to Windows 2016.

Manage Your Server page not displayed upon login

Step 5 Click **Start** > **Run**.

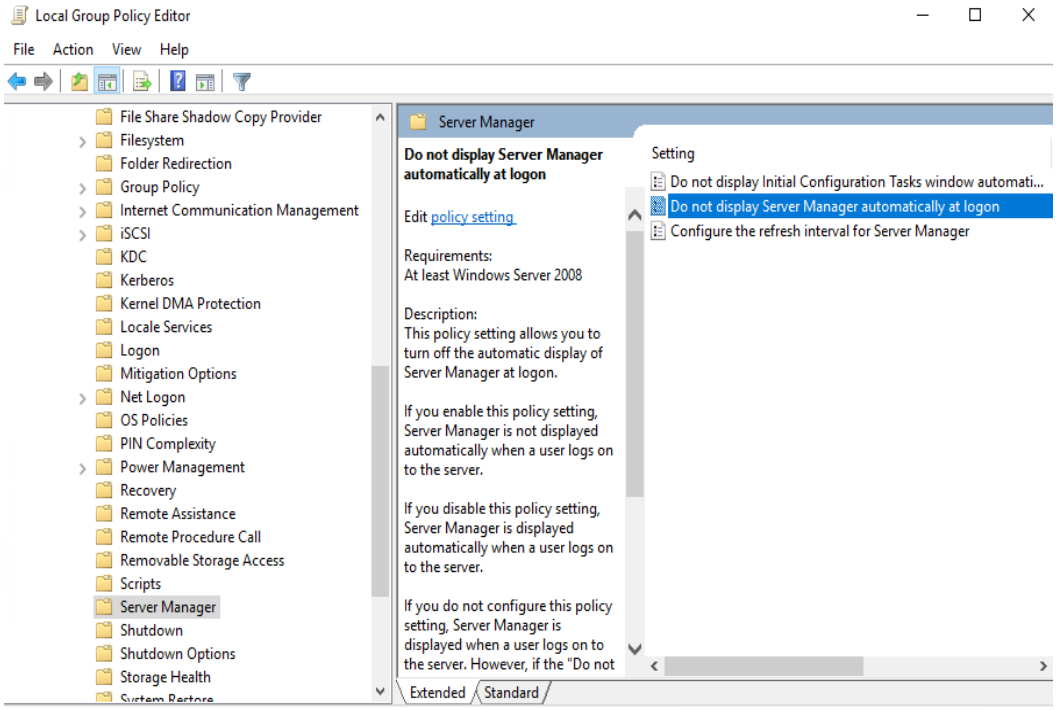
The **Run** dialog box is displayed.

Step 6 Enter **gpedit.msc** in the **Open** text box and press **Enter**.

The **Local Group Policy Editor** window is displayed.

Step 7 In the navigation pane, choose **Computer Configuration** > **Policy** > **Administrative Templates** > **System** > **Server Manager**, as shown in **Figure 13-6**.

Figure 13-6 Manage Your Server page not displayed upon login



Step 8 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 9 Select **Enabled**.

Step 10 Click **OK**.

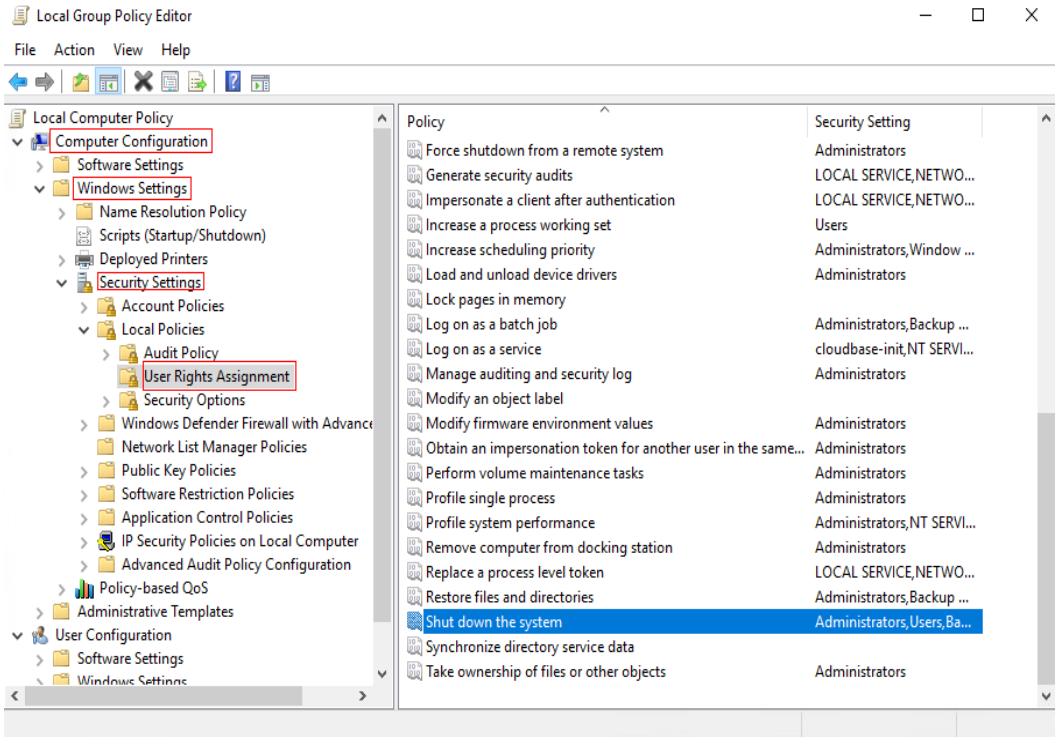
Enabling the group policy that allows the standard user group to shut down Windows

NOTE

Perform this operation for Windows Server 2016 and Windows Server 2019.

Step 11 In the **Local Group Policy Editor** navigation pane, choose **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies** > **User Rights Assignment**, as shown in **Figure 13-7**.

Figure 13-7 User rights assignment



Step 12 In the right pane, double-click **Shut down the system**.

The **Shut down the system properties** dialog box is displayed.

Step 13 Click **Add User or Group**. The **Select Users or Groups** dialog box is displayed.

Step 14 Click **Object Types**, select **Groups**, and click **OK**.

Step 15 In the **Enter the object names to select** area, enter **Users** to query and add the **Users** group to the policy.

Step 16 Click **OK**.

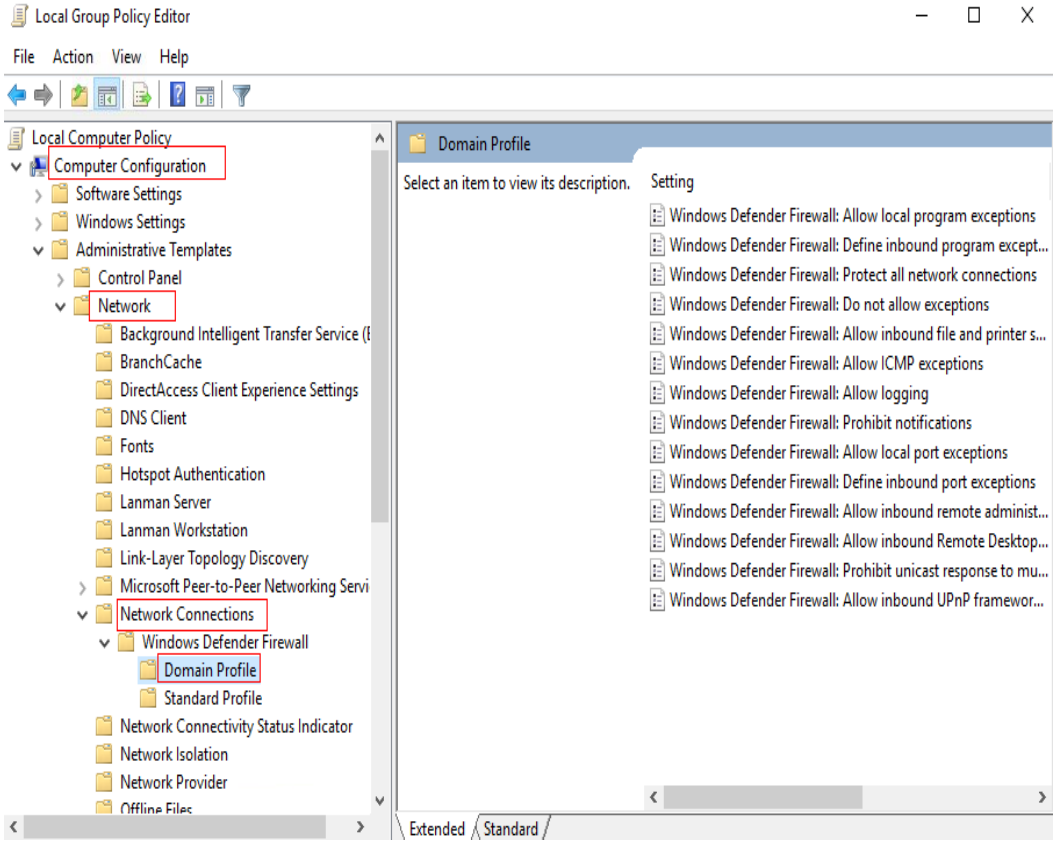
Step 17 Click **OK**.

Disabling the firewall

Step 18 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 13-8**.

Figure 13-8 Domain profiles



Step 19 In the right pane, double-click **Windows Firewall: Protect all network connections**.

The **Windows Firewall: Protect all network connections** dialog box is displayed.

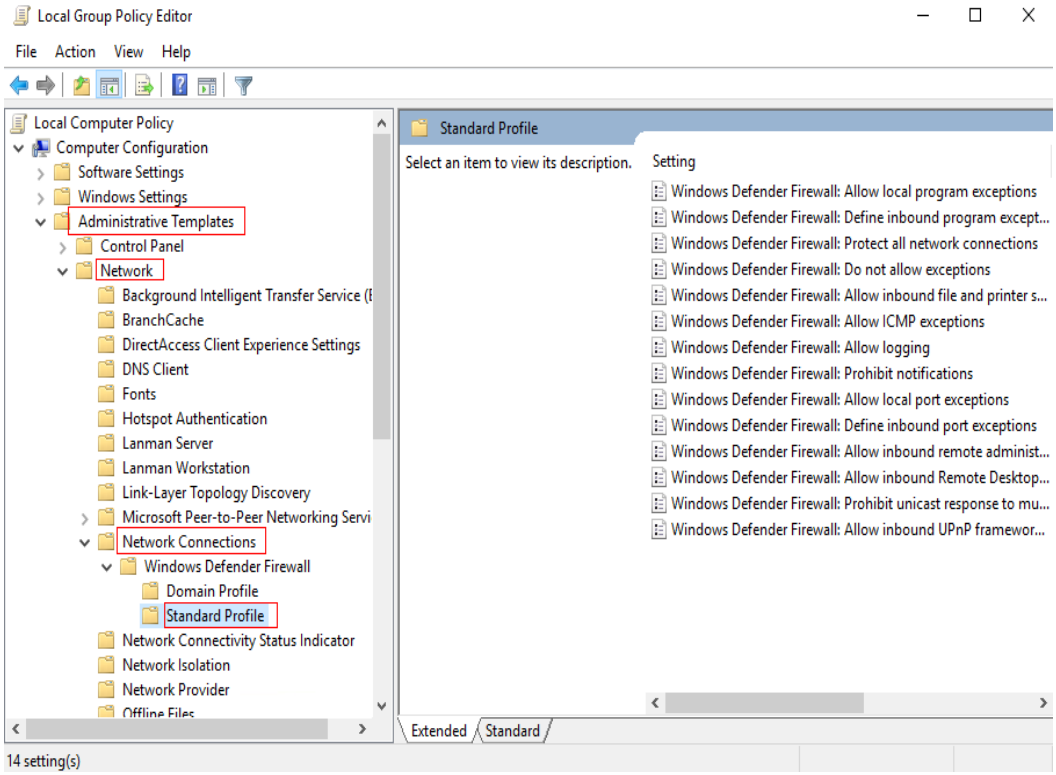
Step 20 Select **Disabled**.

Step 21 Click **OK**.

Step 22 In the navigation pane, choose **Standard Profile**.

The **Standard Profile** page is displayed, as shown in **Figure 13-9**.

Figure 13-9 Standard profiles



Step 23 In the right pane, double-click **Windows Firewall: Protect all network connections**.

The **Windows Firewall: Protect all network connections** dialog box is displayed.

Step 24 Select **Disabled**.

Step 25 Click **OK**.

Step 26 Close the **Local Group Policy Editor** window.

Step 27 Click **Start** > **Run**.

The **Run** dialog box is displayed.

Step 28 Enter **services.msc** in the **Open** text box and press **Enter**.

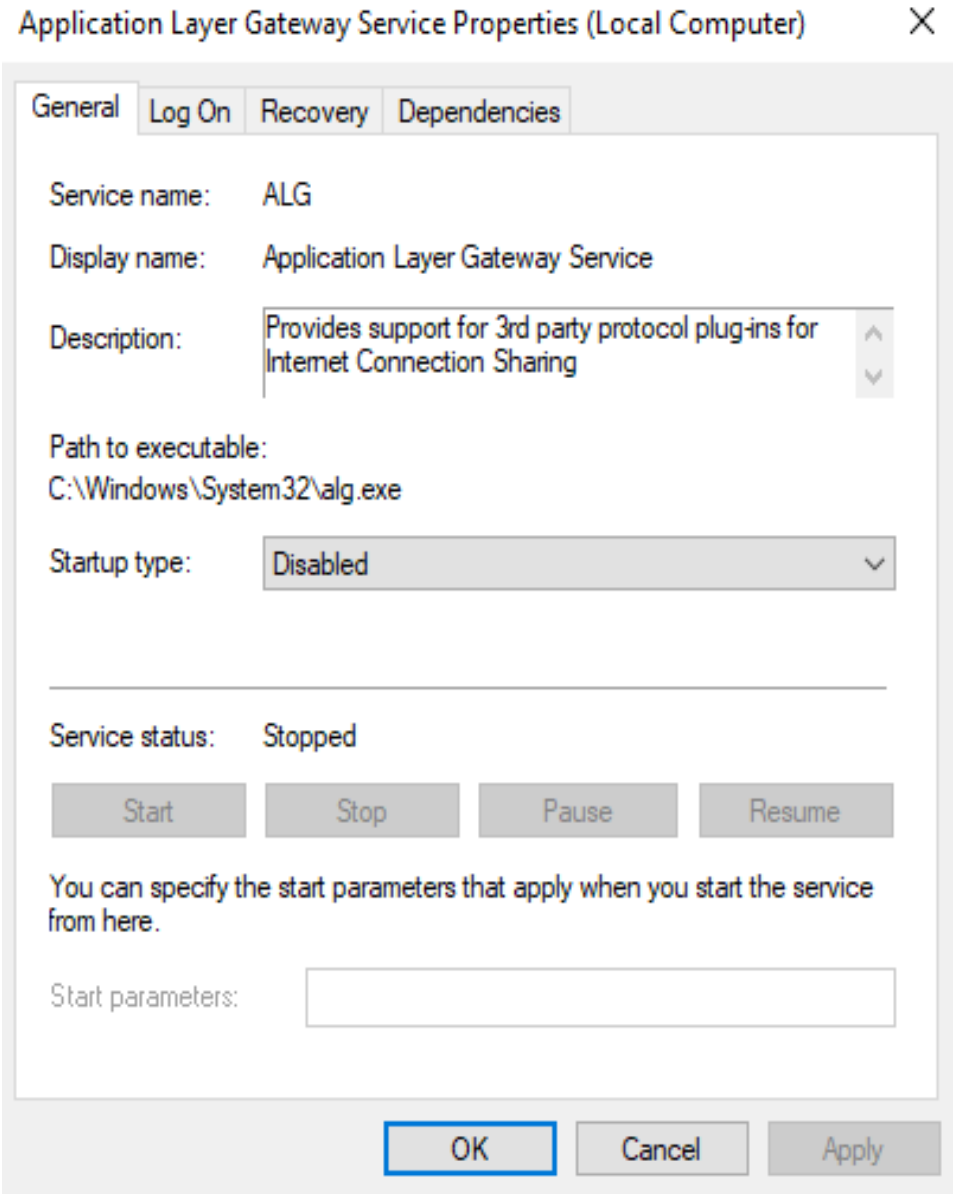
The **Services** window is displayed.

Step 29 In the right pane, double-click **Application Layer Gateway Service**.

The **Application Layer Gateway Service Properties (Local Computer)** page is displayed.

Step 30 On the **General** tab, set **Startup Type** to **Disabled**, as shown in **Figure 13-10**.

Figure 13-10 Configuring the startup type



Step 31 Click **OK**.

Step 32 Set the **Startup Type** of **Internet Connection Sharing (ICS)** and **Windows Firewall** to **Disabled** by referring to **Step 29** to **Step 31**.

NOTE

You do not need to configure **Windows Defender Firewall** for Windows Server 2019.

Step 33 Close the **Services** window.

Disabling Windows update

Step 34 Click **Start** > **Run**.

The **Run** dialog box is displayed.

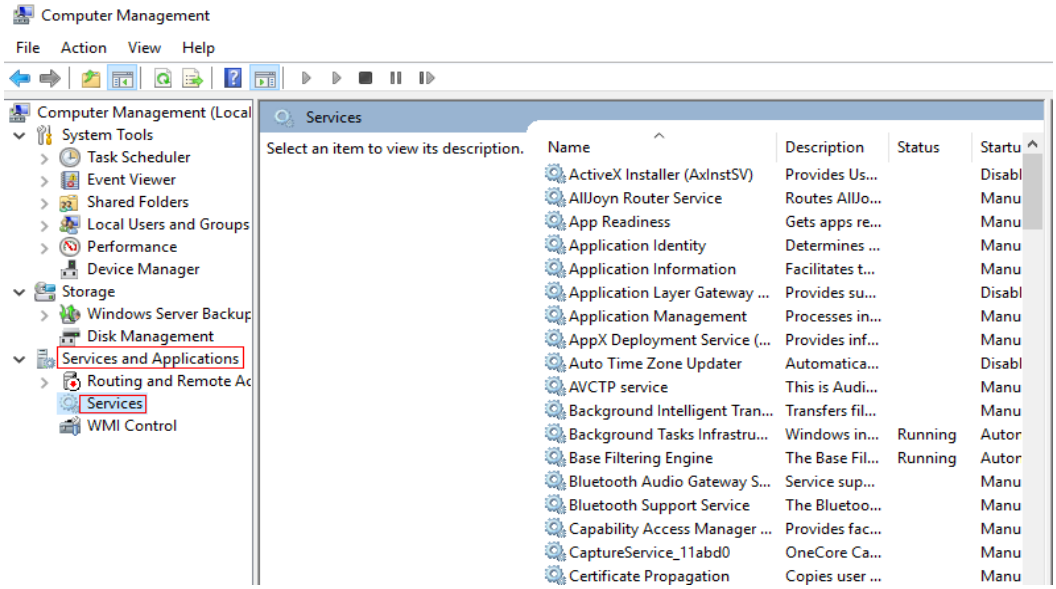
Step 35 Enter **compmgmt.msc** in the **Open** text box and press **Enter**.

The **Computer Management** window is displayed.

Step 36 In the navigation pane, choose **Services and Applications** > **Services**.

The **Services** page is displayed, as shown in **Figure 13-11**.

Figure 13-11 Services



Step 37 In the right pane, double-click **Windows Update**.

The **Windows Update Properties** page is displayed.

Step 38 On the **General** tab, set **Startup Type** to **Disabled**.

Step 39 Go to **Recovery**. Set **First failure** to **Take No Action**.

Step 40 Click **OK**.

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 use the **Administrator** account to log in again.

Step 41 On the ECS, click  , enter **compmgmt.msc**, and press **Enter**.

The **Computer Management** window is displayed.

Step 42 In the navigation pane, choose **Local Users and Groups** > **Users**.

Step 43 Right-click and choose **New User** from the shortcut menu.

Step 44 In the **New User** dialog box, enter the username and password, confirm the password, and click **Create**.

Step 45 In the navigation pane, choose **Local Users and Groups** > **Groups**.

Step 46 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 47 In the **Administrators Properties** dialog box, click **Add** to add the user to the group.

Step 48 Click **OK** and close the **Administrators Properties** dialog box.

Step 49 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 50 On the ECS, click  in the lower left corner, enter **cmd**, and press **Enter**.

Step 51 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 52 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 53 Choose **Start** > **Settings**. The OS setting page is displayed.

Step 54 Click **Privacy**. The privacy setting page is displayed.

Step 55 In the list on the left, click **Microphone**. The page for setting microphone permissions is displayed.

Step 56 Set **Microphone access** to **On**.

Obtaining required installation packages

Step 57 Upload the packages obtained in **13.1.1 Required Software**, except the OS ISO file, to the OBS bucket used in **13.1.2 Registering a Private Image Using an ISO File**.

NOTE

Set the object permission to **public-read**.

Step 58 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 59 In the root directory of drive C on the ECS, create a folder, for example, **software**, for storing the package to be installed.

Step 60 Open the browser on the ECS, copy the package link recorded in **Step 58** to the address box, and press **Enter** to download the package.

NOTE

- Switch the input mode of the ECS to English.
- Download the required packages in sequence.

Step 61 Copy the obtained packages to **C:\software**.

Installing the 7-Zip

Step 62 Go to **C:\software** to find and decompress the 7-Zip installation package.

Installing the Visual Studio 2017 runtime library

Step 63 Go to **C:\software** to find the **vc_redist.x64.exe** package, and double-click **vc_redist.x64.exe** to install the Visual Studio 2017 runtime library.

Step 64 Restart the ECS.

(Optional) Deleting the Microsoft language package

NOTE

To ensure that users can successfully purchase Workspace desktops, you need to delete the Microsoft language package when creating only Windows 10 2004 images.

Step 65 Search for **Windows PowerShell** in the **Start** menu and click **Run as administrator**. The Windows PowerShell running page is displayed.

Step 66 Run the following command to delete the Microsoft language package:

Get-Appxpackage -allusers *Microsoft.LanguageExperiencePackzh-CN* | remove-appxpackage

(Optional) Installing the OS patch

Step 67 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 68 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

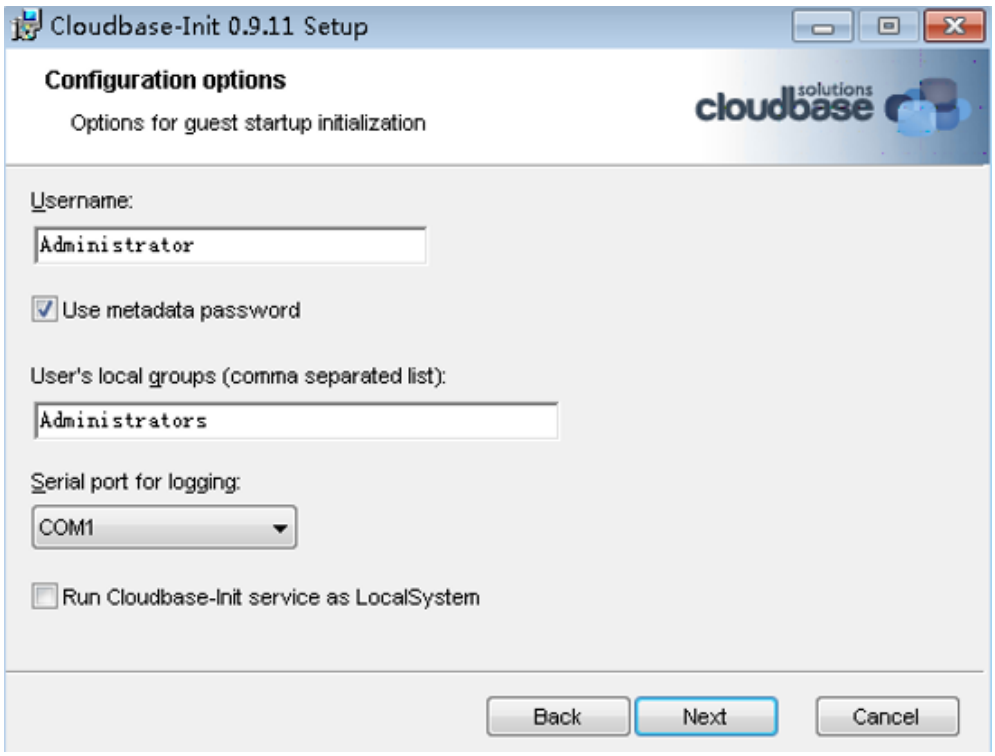
Step 69 Go to **C:\software** where the package is stored and install the peripheral driver.

Installing the Cloudbase-Init software

Step 70 Go to **C:\software** where the package is stored, open the Cloudbase-Init installation package, and install Cloudbase-Init as prompted.

Step 71 On the **Configuration options** page, configure parameters by referring to **Figure 13-12**.

Figure 13-12 Configuration options

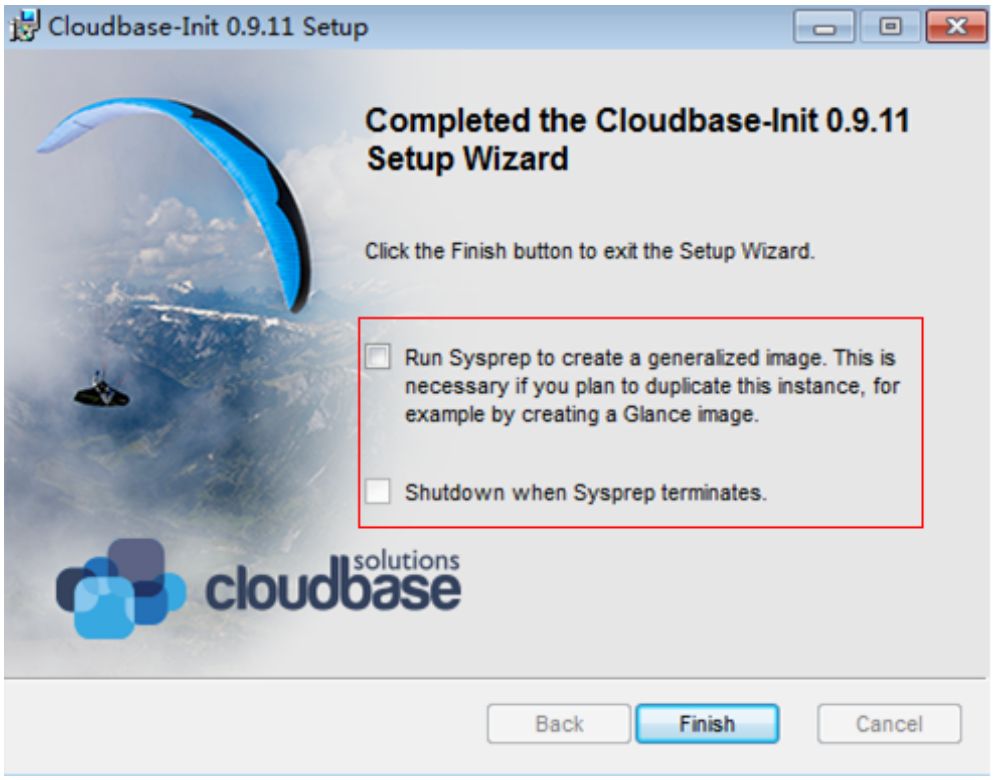


NOTE

The version number in the figure is for reference only. Use the actual version number.

Step 72 After the configuration is complete, deselect the options shown in **Figure 13-13**.

Figure 13-13 Finish



Step 73 Click **Finish**.

Configuring Cloudbase-Init

Step 74 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 75 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 76 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 13-6 SAN policies of Windows

Type	Description
OnlineAll	All newly detected disks are online.
OfflineShared	All 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 detected disks are 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 **76.3**.
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**.

Installing SysAgent and SysPrep

Step 77 Open **Control Panel** on the computer and uninstall HW.SysAgent and HW.SysPrep.

Step 78 Double-click **HW.SysAgent.Installer_64.msi** and **HW.SysPrep.Installer_64.msi** in **C:\software**.

Installing AppCenterAgent and AppCenter

Step 79 Open **Control Panel** on the computer and uninstall WKSAppCenterAgent.

Step 80 Double-click **WKSAppCenterAgent.msi** and **WKSAppCenter.msi** in **C:\software**.

Encapsulating the image

- To create an encapsulated image, perform **Step 81** to **Step 84**.
- To create an image that is not encapsulated, perform **Step 81** to **Step 83**, and **Step 85**.

  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 quickly.

Step 81 On the ECS, find the Windows image creation tool in **C:\software** and decompress it to obtain the **Workspace_HDP_WindowsDesktop**_*XXX* folder.

Step 82 Right-click  in the lower left corner, enter **cmd**, and press **Enter**.

Step 83 Run the following command to switch to the directory containing the template tool:

cd C:\software\Workspace_HDP_WindowsDesktop_Installer_*x.x.x*

Step 84 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 85 (Optional) In the displayed CLI, run the following command to encapsulate the image:

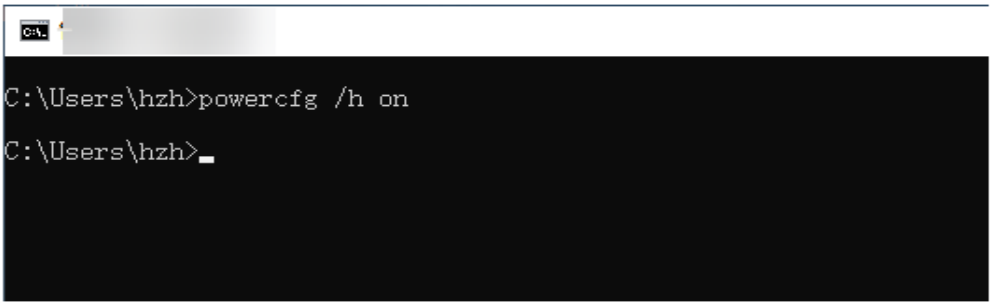
run_silent.bat --passive --environment_type 2 --nocheck –noshutdown --nosysprep

Enabling hibernation

Step 86 Click **Start** > **Run**.

The **Run** dialog box is displayed.

Run the **powercfg -h on** command to enable hibernation.



NOTE

Configure this parameter only for Windows Server 2016 and 2019.

Deleting the temporary admin user

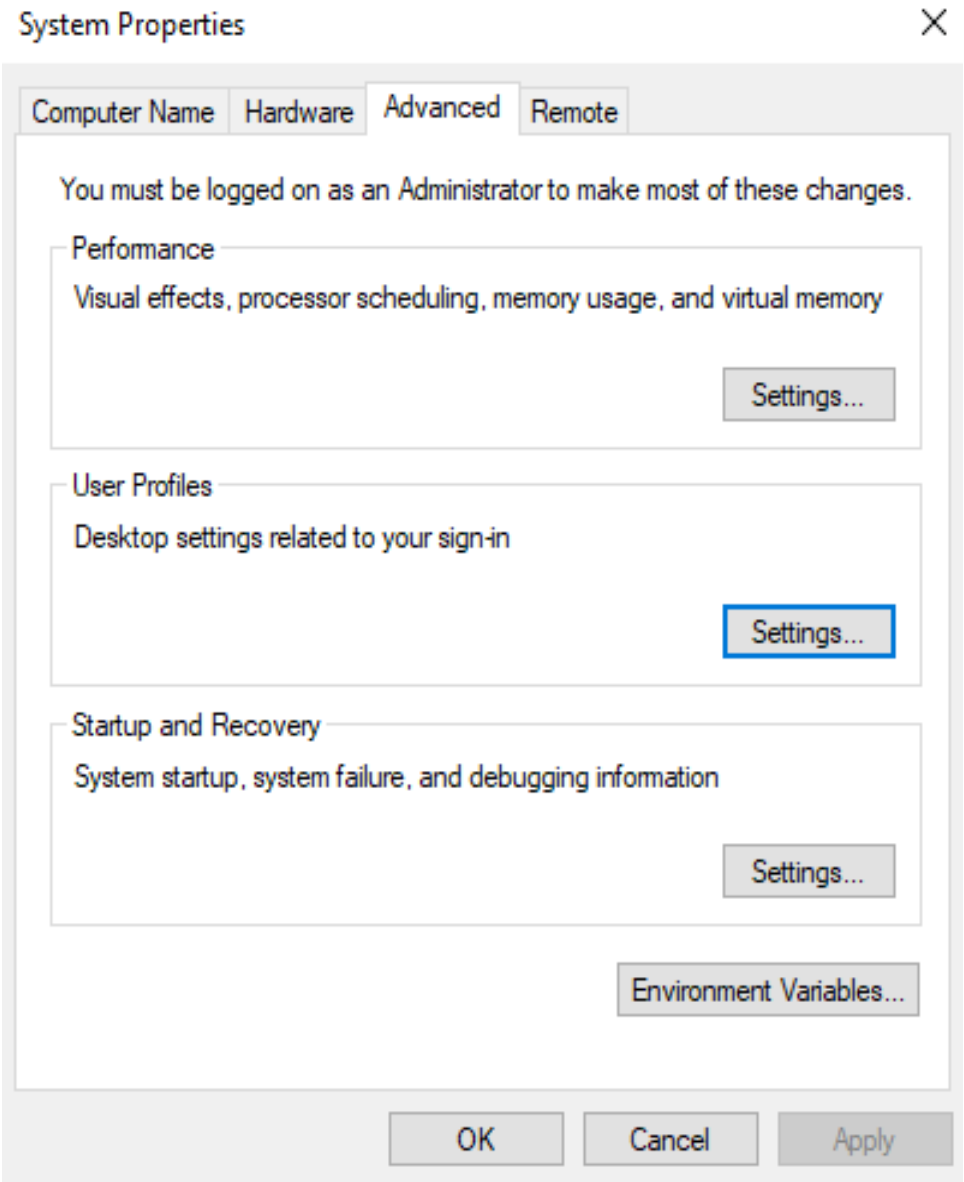
Step 87 Click **Start** > **Run**.

The **Run** dialog box is displayed.

Step 88 Enter **sysdm.cpl** in the **Open** text box and press **Enter**.

The **System Properties** window is displayed.

Step 89 On the **Advanced** tab, click **Settings** under **User Profiles**.



Step 90 On the **User Profiles** page, select the profiles of the user to be deleted and click **Delete**.

Step 91 Click **OK**.

Step 92 Close the **System Properties** window.

Step 93 Click **Start** > **Run**.

The **Run** dialog box is displayed.

Step 94 Enter **compmgmt.msc** in the **Open** text box and press **Enter**.

The **Computer Management** window is displayed.

Step 95 In the navigation pane on the left, choose **System Tools** > **Local Users and Groups** > **Users**.

Step 96 In the right pane, right-click the username to be deleted and choose **Delete**.

Step 97 Click **Yes**.

Step 98 Click **OK**.

Step 99 Close the **Computer Management** window.

Stopping the ECS

Step 100 On the ECS list page of the console, locate the row that contains the ECS created in **13.1.3 Creating an ECS**, and choose **More** > **Stop** to stop the ECS.

----End

13.1.5 Creating a User Desktop Image

Scenario

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 that contains the desired ECS, and choose **More** > **Manage Image/Disk** > **Create Image**.

Step 4 On the page for creating a private image, configure parameters as prompted.

- **Type**: **System Disk Image**
- **Source**: cloud server. Select the cloud server that has been stopped in **13.1.4 Configuring an ECS**.
- **Name**: Configure this parameter based on the actual OS, for example, **Workspace_Image_01**.

Step 5 Click **Create Now**.

Step 6 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

14 Permission Management

14.1 Workspace Permissions

14.2 Creating an IAM User and Granting Permissions

14.3 Entrustment Description

14.4 Enterprise Projects

14.1 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 assign 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 credentials (password and access keys) and can access 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. By default, new IAM users do not have permissions. To assign permissions to new users, add them to one or more groups, and grant permissions to these groups. The users then inherit permissions from the groups to which the users belong, and can perform specific

operations on cloud services. If you add a user to multiple user groups, the user inherits the permissions that are assigned to all the groups.

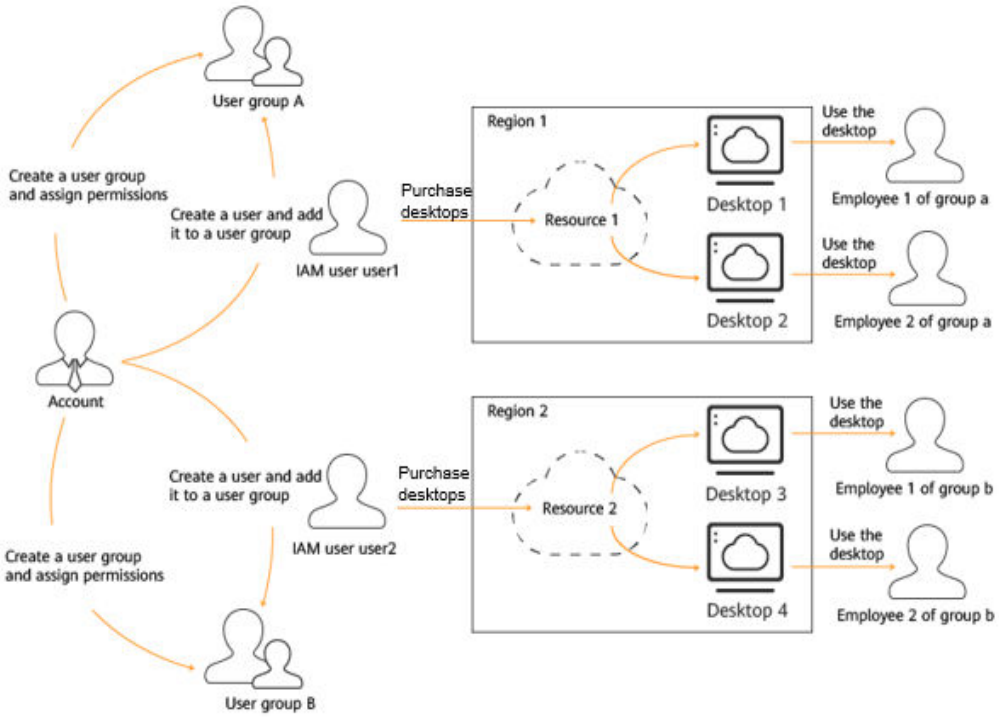
The default user group **admin** has all the permissions for using all of the cloud resources. Users in this group can perform operations on all resources, including but not limited to creating user groups and users, assigning permissions, and managing resources.

Example

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 14-1** shows the operation process. For details about how to create an IAM user, see **Creating an IAM User and Assigning Permissions**.

Figure 14-1 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 14-1 lists all system 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 14-1 Workspace permissions

System Permission	Description	Details
Workspace FullAccess	All permissions for Workspace	All permissions for Workspace

System Permission	Description	Details
Workspace DesktopsManager	Desktop administrator permissions for Workspace	Desktop-related operations, including creating and deleting a desktop (general-purpose desktop, dedicated host, rendering desktop, exclusive desktop, and desktop pool), and Internet access, scheduled tasks, App Center, and image management
Workspace UserManager	User administrator permissions for Workspace	User management operations, such as creating users, deleting users, and resetting passwords
Workspace SecurityManager	Security administrator permissions for Workspace	All security-related operations, such as policy management and user connection recording
Workspace TenantManager	Tenant administrator permissions for Workspace	All tenant configuration functions
Workspace ReadOnlyAccess	Read-only permissions for Workspace	Read-only permissions for Workspace

Table 14-2 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 14-2 Additional permissions

Operation	Dependent System 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.	System role: BSS Administrator Add the following actions to the custom policy: bss:discount:view bss:order:update bss:order:view	Select either a system role or a custom policy.

Operation	Dependent System Role, Policy, or Custom Policy	Description
IAM-related permissions: Perform scheduled tasks, perform operations on desktop pools, and create and query agencies.	**Permissions required for creating and querying agencies:** System role: Security Administrator Add the following actions to the custom policy: 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:** System policy: IAM ReadOnlyAccess Add the following actions to the custom policy: iam:agencies:getAgency iam:agencies:listAgencies iam:permissions:listRolesForAgencyOnProject	When creating an agency, select either the system role Security Administrator or the custom policy. For agency query only, select either the system policy IAM ReadOnlyAccess or the custom policy.
TMS-related permissions: Query predefined tags during desktop creation.	System policy: TMS FullAccess Add the following actions to the custom policy: tms:predefineTags:list	Select either a system policy or a custom policy.
VPCEP-related permissions: Enable or disable Direct Connect access (required for fine-grained authentication of enterprise projects).	System role: VPCEndpoint Administrator	VPCEP does not support fine-grained authentication of enterprise projects.

Operation	Dependent System Role, Policy, or Custom Policy	Description
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 policy: VPC ReadOnlyAccess System role: VPC Administrator	You must have the VPC permission of the enterprise project to which the VPC used for enabling Workspace belongs.
IMS-related permissions: Create an image (required for fine-grained authentication of enterprise projects).	Add the following actions to the custom policy: ims:images:get ims:images:share	IMS does not support fine-grained authentication of enterprise projects.

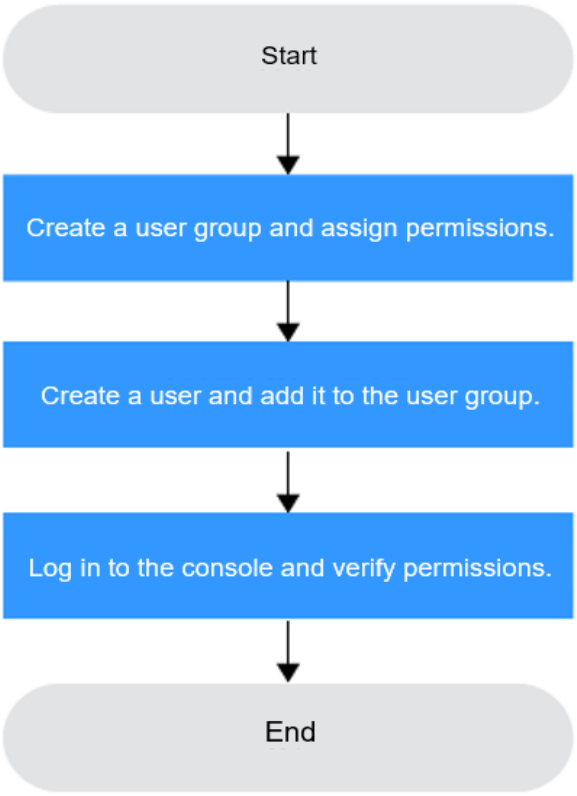
14.2 Creating an IAM User and Granting Permissions

Prerequisites

Before assigning permissions to user groups, you should learn about available Workspace system permissions for user groups and select the permissions based on service requirements. For details about the system permissions supported by Workspace, see **Workspace System Policies**. For the permissions of other services, see .

Example Process

Figure 14-2 Assigning permissions for Workspace resources to a user



1. **Create a user group and assign permissions**

   Create a user group on the IAM console, assign the **Workspace Administrator** permission to the group, and select the authorization scope.

2. **Create an IAM user and add the user 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 an IAM user** and verify permissions.

   Log in to the Workspace console as the newly created user, and verify whether it has the administrator permissions.

   Click ☰, choose **Service List** > **Workspace**, and click **Buy Desktop** in the upper right corner. If no message appears indicating insufficient permissions, the **Workspace Administrator** permission has already taken effect.

14.3 Entrustment Description

Workspace works closely with multiple cloud service resources, such as computing, network, and images. When you create a scheduled task for recomposing a system disk or create a desktop pool, Workspace automatically requests permissions to access the cloud services in the region. Specifically:

- ECS permissions

  When you create a desktop, an ECS is created accordingly. Therefore, the permission to access ECS is required.

- IMS permissions

  Workspace supports image creation. Therefore, the permission to access IMS is required.

- Administrator permissions for related cloud services

  Workspace supports scheduled disk recomposing and auto scaling. Therefore, the tenant administrator permissions are required.

- VPC service permissions

  Workspace allows created networks to run on VPCs. Therefore, the permission to access the VPC service is required.

- OBS permissions

  Workspace supports scale-out and storage addition. Therefore, the permissions to access EVS disks, SFS, and OBS are required.

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.

14.4 Enterprise Projects

Creating an enterprise project

Step 1 **Log in to the Workspace 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 management console only if you have enabled the enterprise project, or your 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**.

15 Data Backup and Restoration

15.1 Backing Up Desktop Data

15.2 Restoring Desktop Data

15.1 Backing Up Desktop Data

Scenario

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

- You have purchased a cloud desktop.
- The administrator account 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 for using CBR**.

Procedure

Step 1 **Purchase a disk backup vault**.

NOTE

When creating a desktop backup vault, select the cloud desktop to be backed up.

Step 2 Create a desktop backup.

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

15.2 Restoring Desktop Data

Scenario

If a cloud desktop goes wrong, you can purchase a new cloud desktop and 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 services.

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 using a cloud desktop backup.

----End

16 Common Function Configuration

16.1 Configuring Workspace to Access the Internet

16.2 Configuring Workspace to Access the Enterprise Intranet

16.3 Configuring Network Connection Between Workspace and Windows AD

16.1 Configuring Workspace to Access the Internet

Scenario

After you purchase a cloud desktop, the cloud desktop is in the VPC subnet by default and cannot access the Internet. You need to configure the NAT gateway to share an EIP so that 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 described how to enable the Internet using the purchasing NAT and EIP pages provided by Workspace. 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 Workspace 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**.
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, click **Desktop Management**.
2. Check the **Enabling the Internet** column of the target desktop.
   - If the value is **disabled**, end users cannot access the Internet through cloud desktop. In this case, go to **Step 4**.
   - If the value is **enabled**, end users can access the Internet through the cloud desktop. In this case, skip subsequent operations.

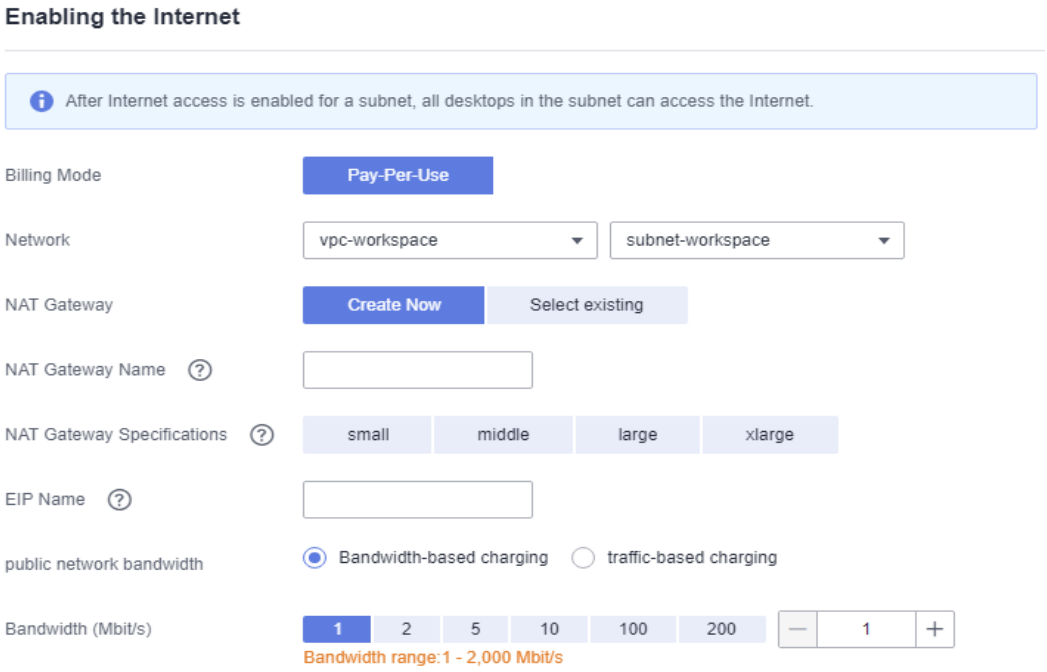
Step 4 In the navigation tree on the left, click **Desktop Internet Access Management**.

The desktop Internet access management page is displayed.

Step 5 In the upper right corner of the page, click **Enabling the Internet**.

The Internet configuration page is displayed, as shown in **Figure 16-1**.

Figure 16-1 Enabling the Internet



Step 6 Configure network parameters by referring to **Table 16-1**. Retain the default values for parameters not listed.

Table 16-1 Internet parameters

Parameter	Description	Example Value
Billing Mode	The billing mode of Internet resources that can be purchased are **Pay-Per-Use**.	Pay-Per-Use
Network	Select the virtual subnet to which the desktop to be enabled with the Internet function belongs.	-

Parameter	Description	Example Value
NAT Gateway	The name of the public NAT gateway. ● If the cloud desktop has multiple service subnets: You need to configure NAT for each service subnet. Multiple service subnets can share the same NAT or has their own independent NAT. Select an existing NAT or create a NAT as required. The NAT gateway name can contain a maximum of 64 characters and include only digits, letters, underscores (_), and hyphens (-). ● If the cloud desktop has only one service subnet: – If a public NAT gateway has been configured for the virtual subnet, you do not need to configure this parameter. – If no public NAT gateway is configured for the virtual subnet, you need to customize the NAT gateway name. The name can contain a maximum of 64 characters and include only digits, letters, underscores (_), and hyphens (-).	NATNetname-workspace_subnet01
NAT Gateway Specifications	The specification of the public NAT gateway ● If an existing NAT gateway is used, you do not need to configure this parameter. ● To create a NAT gateway, you need to configure the NAT gateway specifications. There are four specifications of NAT gateways: small, middle, large, and xlarge. You can click **Find out more** on the page to view details about each specification.	small
EIP Name	The name of the EIP.	EIP-workspace_subnet01

Parameter	Description	Example Value
Public Network Bandwidth	Select the bandwidth billing mode based on the service scenario. • **Bandwidth-based charging**: You need to specify a bandwidth limit and pay for the amount of time you use the bandwidth. This is suitable for scenarios with heavy or stable traffic. • **Traffic-based charging**: You specify a maximum bandwidth and pay for the total traffic you generate. This is suitable for scenarios with light or sharply fluctuating traffic.	Traffic-based charging
Bandwidth (Mbit/s)	Select a bandwidth size. If you pay by traffic, you can customize the value from 1 Mbit/s to 300 Mbit/s.	99

Step 7 Click **OK**.

After configuring the parameters, you can view the Internet information configured for the corresponding service subnet on the **Desktop Internet Access Management** page.

NOTE

- If the current tenant VPC has multiple service subnets and cloud desktops in each service subnet need to access the Internet, enable the Internet for each service subnet by referring to **Step 5** to **Step 7**.
- If multiple NAT gateways are created in the same VPC, ensure that the default route to all NAT gateways is configured in the route table. For details, see

Step 8 (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 8.1** to **Step 8.10**. 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 9 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, delete the SNAT bound to the EIP, delete the NAT, and release the EIP to disable the Internet to save resources.

NOTE

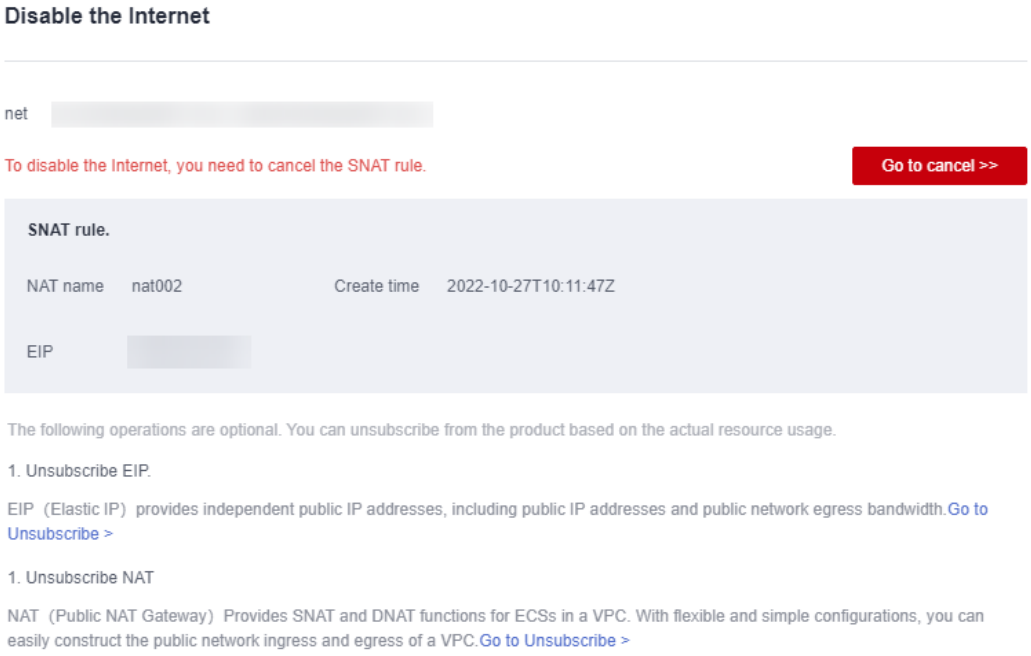
After SNAT is deleted, Workspace cannot access the Internet. Determine whether to delete the NAT and EIP as required.

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

Step 2 On the **Desktop Internet Access Management** page, click **Disable the Internet**.

The page for disabling the Internet is displayed, as shown in **Figure 16-2**.

Figure 16-2 Disabling the Internet



Record the NAT gateway name and the EIP bound to the SNAT rule. After the SNAT rule is deleted, the EIP is unbound from the SNAT rule. You need to delete the corresponding EIP and NAT gateway on the EIP list and NAT gateway list.

Step 3 Click **Go to cancel**.

The SNAT rule list is displayed.

Deleting an SNAT Rule

Step 4 Locate the SNAT rule bound to the EIP used by the cloud desktop and click **Delete** in the **Operation** column.

You can determine which SNAT needs to be deleted based on the EIP recorded in **Step 2**.

Step 5 In the displayed dialog box, click **Yes**.

(Optional) Deleting a NAT

NOTE

Multiple SNAT and DNAT rules can be created for a NAT, and the NAT can be deleted only after all related SNAT and DNAT rules are deleted. Determine whether to delete the NAT as required. If you decide to delete the NAT, delete it when it is used only by the cloud desktop of the current subnet.

Step 6 Click < in the upper left corner to return to the public NAT gateway list.

Step 7 Locate the public NAT gateway to be deleted and choose **More** > **Delete** in the **Operation** column.

NOTE

All SNAT and DNAT rules created for the public NAT gateway must be deleted.

Step 8 In the displayed dialog box, click **Yes**.

Deleting an EIP

Step 9 In the navigation pane on the left, choose **Elastic IP and Bandwidth** > **EIPs**.

The EIP list is displayed.

Step 10 Select the EIP recorded in **Step 2**.

Step 11 In the upper part of the list, choose **More** > **Release**.

Step 12 In the displayed dialog box, click **Yes**.

----End

16.2 Configuring Workspace to Access the Enterprise Intranet

Scenario

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 cloud desktops after accessing cloud desktops.

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 local data center to the VPC where the cloud desktop resides by referring to ***VPN Administrator Guide***, for example, Using TheGreenBow IPsec VPN Client to Configure On- and Off-Cloud Communication.

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 Workspace console**.

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

Step 3 In the **Network Configuration** area, click **Enable** next to **Direct Connect Access Address**.

Step 4 In the displayed dialog box, configure **Direct Connect network segment**.

- Using Direct Connect:
  - 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
- Using a VPN connection:

  Enter the network segment of the local data center to be connected, for example, 10.119.156.0/24. The network segment of the local data center 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

16.3 Configuring Network Connection Between Workspace and Windows AD

Scenario

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.

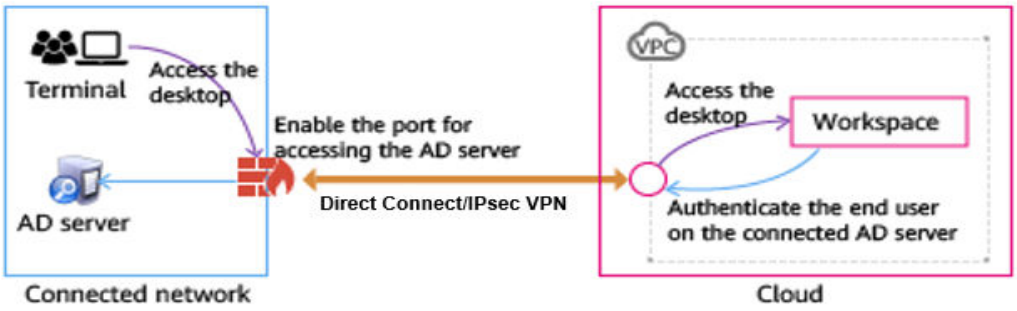
Prerequisites

You have obtained the domain administrator account and password.

Procedure

Scenario 1: Deploying the Windows AD in the customer's data center intranet

Figure 16-3 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 16-2**.

Table 16-2 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)

Role	Port	Agreement	Description
	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)
	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

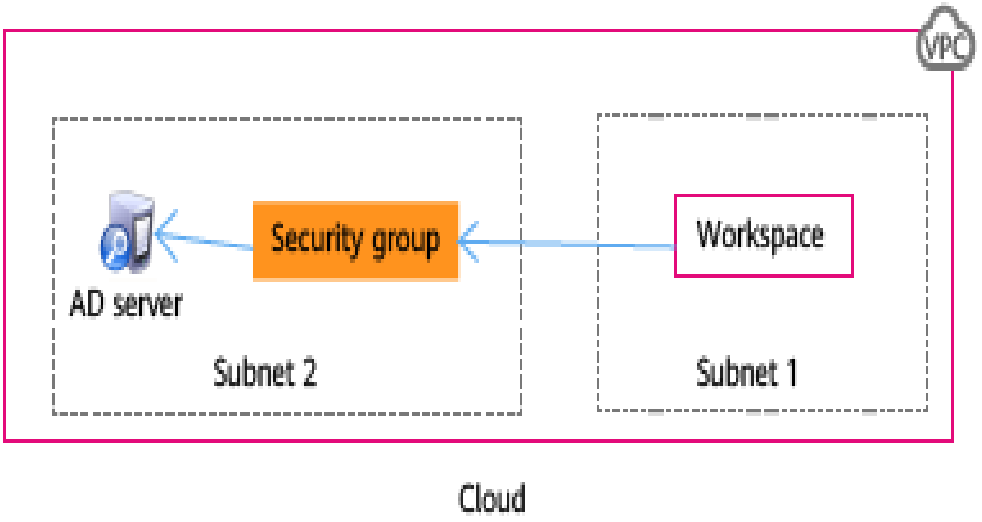
Step 3 After the configuration is complete, check whether the networks and ports are working properly by referring to **Verification Method**.

----End

Scenario 2: Deploying the Windows AD in another subnet of the VPC where the workspace 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 workspace so that the workspace can connect to the Windows AD.

Figure 16-4 Deploying the Windows AD in another subnet of the VPC where the workspace 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 instance so that the workspace 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 16-2**.

Step 4 After the configuration is complete, check whether the networks and ports are working properly by referring to **Verification Method**.

----End

Verification Method

Step 1 Check the firewall or security group settings of the AD server and ensure that ports in **Table 16-2** 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

17 Subscribing to an Event

Scenario

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

With event notifications, message queues may be blocked or CTS may fail to be called. Therefore, users cannot completely 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

When CTS is enabled, a system tracker is automatically created. You can use this tracker.

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

- When a cloud desktop is started, shut down, or fails to be created, started, shut down, or deleted, the system automatically reports an event 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 Workspace console.

Step 6 Click **Service List** and choose **Management & Governance** > **Cloud Trace Service**.

Step 7 On the **Trace List** page, set **Trace Source** to **Workspace** and **Resource Type** to **workspace**, and enter a resource name as required to find the corresponding trace name. For details, see the following note.

NOTE

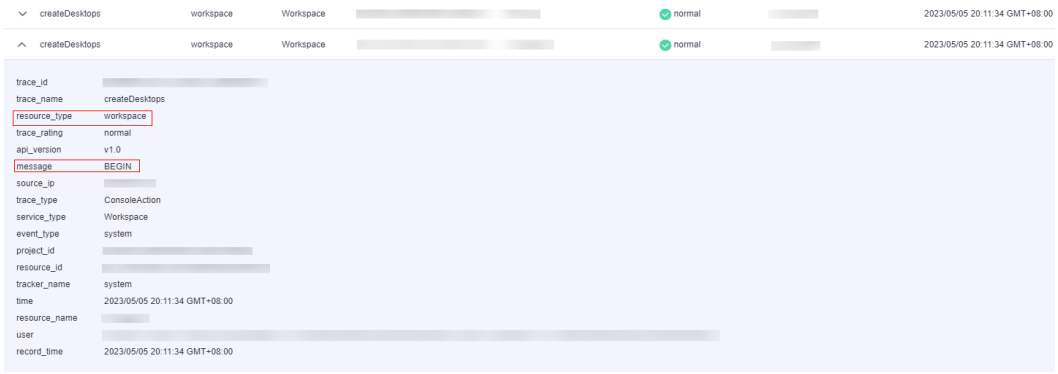
Traces are classified into the following types:

- **createDesktops**: creates a desktop
- **stopDesktops**: shuts down a desktop
- **startDesktops**: starts a desktop
- **deleteDesktops**: deletes a desktop

Step 8 Click **Query**.

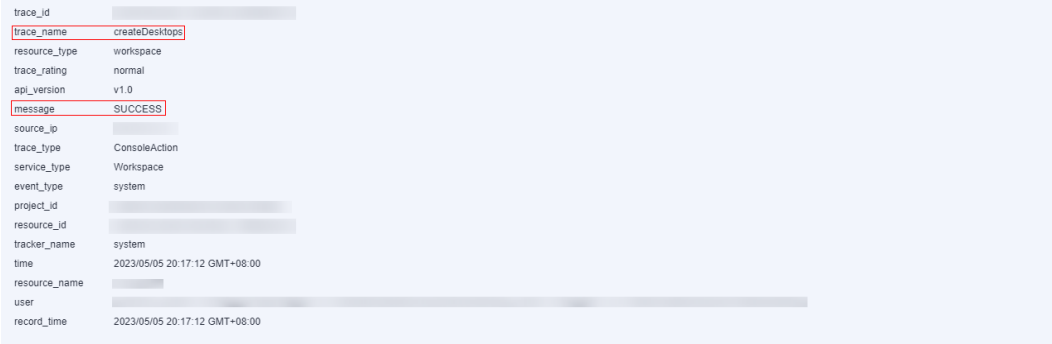
Step 9 Take desktop purchase as an example. View the desktop purchase trace and start the purchase, as shown in **Figure 17-1**.

Figure 17-1 Starting the purchase



View the desktop purchase trace to complete the purchase, as shown in **Figure 17-2**.

Figure 17-2 Completing the purchase



NOTE

- When desktop purchase or deletion fails, a failure trace is reported. In the trace details, the value of **Message** is **FAILED**.
- If the VM is shut down, the **BEGIN** message is not reported in CTS. Only the message indicating that the VM has been shut down 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 shut down, 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

A Change History

Release Date	Description
2023-10-13	This issue is the first official release.

