11 Workspace Application Streaming User Guide

Issue 01

Date 2026-01-26

HUAWEI

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: https://www.huawei.com

Email: support@huawei.com

Security Declaration

Vulnerability

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

Contents

1 Overview....1
1.1 Overview....1
1.2 Introduction....2
1.3 Application Scenarios....4
1.4 Features....4
1.5 Billing....5
1.6 Permissions Management....7
1.7 Supported OSs, Terminals, and Applications....10
1.8 Constraints....10
2 Administrator Operation Guide....12
2.1 Operation Procedure....13
2.2 Logging In to the Workspace Application Streaming Console....13
2.3 Enabling the Service....14
2.4 Creating a User....17
2.5 Applications and Images....18
2.5.1 Application Repositories....18
2.5.2 Image Creation....20
2.5.3 Managing an Image Task....26
2.6 Server Groups....27
2.6.1 Managing Server Groups....27
2.6.1.1 Creating a Server Group....28
2.6.1.2 Modifying a Server Group....33
2.6.1.3 Deleting a Server Group....36
2.6.2 Managing APSs....37
2.6.2.1 Adding a Server....37
2.6.2.2 Unsubscribing from a Server....38
2.6.2.3 Deleting a Server....39
2.6.2.4 Releasing a Server....40
2.6.2.5 APS Management....40
2.7 Application Groups....45
2.7.1 Managing Application Groups....45
2.7.1.1 Creating an Application Group....45
2.7.1.2 Modifying an Application Group....46

2.7.1.3 Deleting an Application Group....47
2.7.2 Managing Applications....47
2.7.2.1 Managing Applications....47
2.7.2.1.1 Adding Applications....48
2.7.2.1.2 Modifying an Application....51
2.7.2.1.3 Deleting an Application....51
2.7.2.1.4 Modifying an Application Icon....52
2.7.2.1.5 Disabling or Enabling an Application....52
2.7.2.2 Managing Authorizations....53
2.7.2.2.1 Authorizing Users or User Groups....53
2.7.2.2.2 Canceling User or User Group Authorization....54
2.7.2.2.3 Resending a Notification....55
2.8 User Management....55
2.9 Policy Groups....56
2.9.1 Creating a Policy Group....56
2.9.2 Modifying a Policy Group....62
2.9.3 Configuring an Advanced Policy....66
2.10 Monitoring Analysis....89
2.10.1 Application Records....89
2.10.2 Sessions....89
2.11 OU Management....91
2.12 Application Internet Access Management....92
2.12.1 Enabling Internet Access....92
2.12.2 Disable Internet Access....95
2.13 Upgrading Protocol Components....95
2.14 Scheduled Tasks....96
2.14.1 Creating a Scheduled Task....96
2.14.2 Managing Scheduled Tasks....98
2.15 Storage....99
2.15.1 Creating NAS....99
2.15.2 Configuring Permission Policies....100
2.15.3 Managing NAS....102
2.15.3.1 Personal Folders....102
2.15.3.1.1 Creating a Personal Folder....102
2.15.3.1.2 Modifying Permissions on a Personal Folder....102
2.15.3.1.3 Deleting a Personal Folder....103
2.15.3.2 Shared Folders....103
2.15.3.2.1 Creating a Shared Folder....103
2.15.3.2.2 Managing Members....104
2.15.3.2.3 Deleting a Shared Folder....105
2.15.4 Deleting NAS....106
2.15.5 Configuring a Server Group Mounting Policy....106

2.16 Tenant Configuration 107
2.17 Private Images 110
2.17.1 Creating a Windows Private Image (Basic Image) 110
2.17.1.1 Required Software 110
2.17.1.2 Registering a Private Image Using an ISO File 113
2.17.1.3 Creating an ECS 117
2.17.1.4 Configuring an ECS 120
2.17.1.5 Creating a Basic Image for Workspace Application Streaming 141
2.18 Configuring Personalized Data 142
2.18.1 Configuring the Desktop Data Synchronization 142
2.19 Subscribing to an Event 150
2.20 Permissions Management 153
2.20.1 Permission Management 153
2.20.2 Creating a Custom Policy 157
2.20.3 Permissions and Supported Actions 158
2.21 Configuring Common Functions 181
2.21.1 Allowing Workspace Application Streaming to Access the Internet 181
2.21.2 Allowing Workspace Application Streaming to Access the Enterprise Intranet 184
2.22 Monitoring 186
2.22.1 Basic Monitoring Metrics Supported by Workspace Application Streaming 186
2.22.2 Cloud Eye Events Supported by Workspace Application Streaming 192
2.23 FAQs 194
2.23.1 What Is the Relationship Between Workspace Application Streaming and Workspace? 194
2.23.2 What Types of Applications Can Be Published? 195
2.23.3 What Can I Do If an Application Fails to Be Published? 195
2.23.4 How Do I Deploy a Windows AD Server? 195
2.23.5 How Do I Deploy an RD Licensing Server? 198
2.23.6 How Do I Configure RDS Licensing and Security Policies? 205
2.23.7 How Do I Create a User OU on the AD Server? 212
2.23.8 How Do I Create a User Group on the AD Server? 212
2.23.9 How Do I Create a User on the AD Server? 213
2.23.10 How Do I Configure Network Connection Between Workspace Application Streaming and the Windows AD? 214
2.23.11 How Do I Log in to an APS? 217
2.23.12 How Do I Purchase the NAT and EIP Services to Enable Cloud Applications to Be Accessed Through the Internet? 218
2.23.13 How Do I Check My Quotas? 221
2.23.14 How Do I Increase My Quotas? 221
2.23.15 How Do I Do If the Application Operation Page Has Black Borders and Cannot Be Moved? 221
2.23.16 How Do I Do If an End User Fails to Log In to a Cloud Application? 224
2.23.17 How Do I Reset a User Password? 225
2.23.18 How Do I Do If I Fail to Add a Computer Back to the Domain? 226
2.23.19 How Do I Add an ECS to the Domain of an APS? 226

2.23.20 How Do I Use the GPO Group Policy to Make a Domain User Become a Local Administrator of a PC? 229
2.23.21 How Do I Install Sandbox Software? 238
2.23.22 How Do I Do If There Is No Sound or the Screen Is Frozen While There Is Sound When Using Google Chrome or Bilibili Player for Video Playback? 240
2.23.23 How Do I Do If the Window Cannot Be Dragged When the Sandbox Application Is Started? 240
2.23.24 RD License Server Fails to Be Added to the AD domain 243
2.23.25 Error Code 6030/6047 Reported When Accessing a Shared Desktop Application 244
2.23.26 File Resources on the APS Cannot Be Automatically Refreshed During Workspace Application Streaming Operations 244
2.23.27 How Do I Update or Add an Application? 245
2.23.28 How Do I Authorize an IAM User to Use Workspace Application Streaming? 246
2.23.29 How Do I Calculate the Number of Concurrent Sessions of a Cloud Application? 250
2.23.30 What If I Can't Open a Cloud Application? 251

3 Terminal User Operation Guide 253

3.1 Process 253
3.2 Using an Application on a Soft Client 254
3.3 Using an Application on a Thin Client 258
3.4 FAQs 261
3.4.1 How Do I Do If the Cloud Application Cannot Be Used? 261
3.4.2 How Do I Do If I Cannot View Cloud Applications on Desktops? 261
3.4.3 How Do I Do If I Forget the Password? 261
3.4.4 How Do I Do If the Account is Locked? 261
3.4.5 How Do I Do If I Fail to Log In to the Client? 261
3.4.6 How Do I Enable a Local Storage Device to Copy Files to an APS? 262
3.4.7 How Do I Recover Important Files and Documents from the Sandbox to the Local Computer? 272
3.4.8 How Do I Delete a Sandbox? 273
3.4.9 How Do I Remove the Yellow Border of an Application After the Sandbox Application Is Started? 274

1 Overview

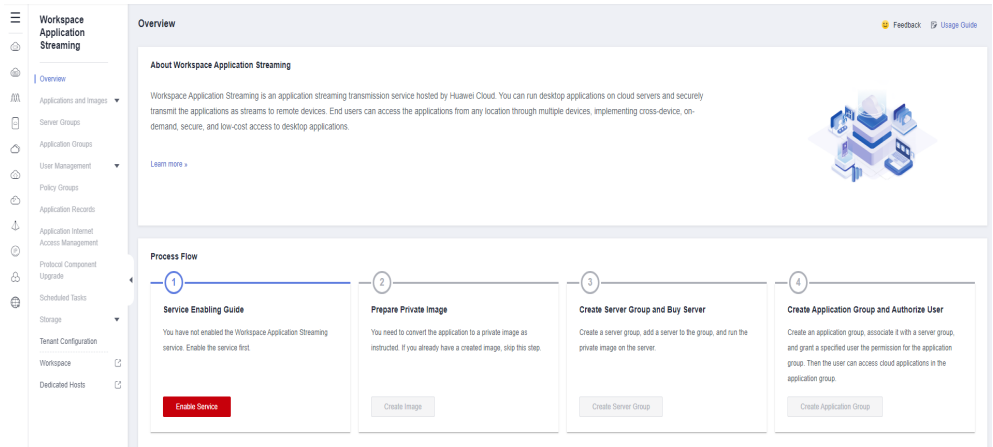
1.1 Overview
1.2 Introduction
1.3 Application Scenarios
1.4 Features
1.5 Billing
1.6 Permissions Management
1.7 Supported OSs, Terminals, and Applications
1.8 Constraints

1.1 Overview

Service Not Enabled

If you have not enabled Workspace Application Streaming, you can learn about what it is and its purchase process on the **Overview** page, as shown in **Figure 1-1**.

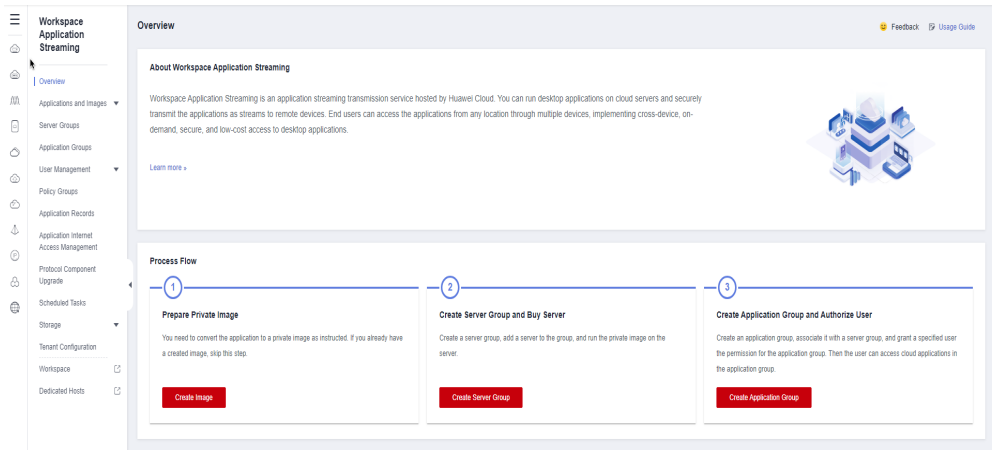
Figure 1-1 Overview



Service Enabled

After enabling Workspace Application Streaming, you can create images, servers, and application groups, as shown in **Figure 1-2**.

Figure 1-2 Process flow



1.2 Introduction

About Workspace Application Streaming

Workspace Application Streaming is an application streaming transmission service hosted on Huawei Cloud. You can run desktop applications on cloud servers and securely transmit the applications to devices through streams. End users can access the applications from multiple devices anywhere, implementing on-demand, secure, and low-cost access.

Working Principles

The administrator purchases a cloud server on the cloud platform management console, logs in to the cloud server, deploys applications, and publishes applications on the console. End users can use these applications on local desktops or Workspace desktops of terminals for office work.

Basic Concepts

- **User**

  Users are classified into end users and administrators based on their permissions. An end user is a user who has the permission to use an application. An administrator is a tenant who assigns applications to end users. An administrator has the permissions to publish and delete applications, configure policies, and manage users.

- **Policy group**

  A policy group is a set of security rules configured for Workspace Application Streaming, including file redirection read/write permission, clipboard read/write permission, session automatic reconnection interval, and image display. Policies are used to control data transmission between user terminals and Workspace Application Streaming.

- **Priority**

  The priority is a basis for determining an execution sequence or an action weight of a policy by Workspace Application Streaming. The priority is represented by a positive integer. A smaller value indicates a higher priority.

- **AD management server**

  The Active Directory (AD) management server is the infrastructure component where the AD service is deployed. It provides a series of directory service functions that allow users to manage and access network resources in a unified manner. Workspace Application Streaming can interconnect with your own AD server for authentication and authorization.

- **Region and AZ**

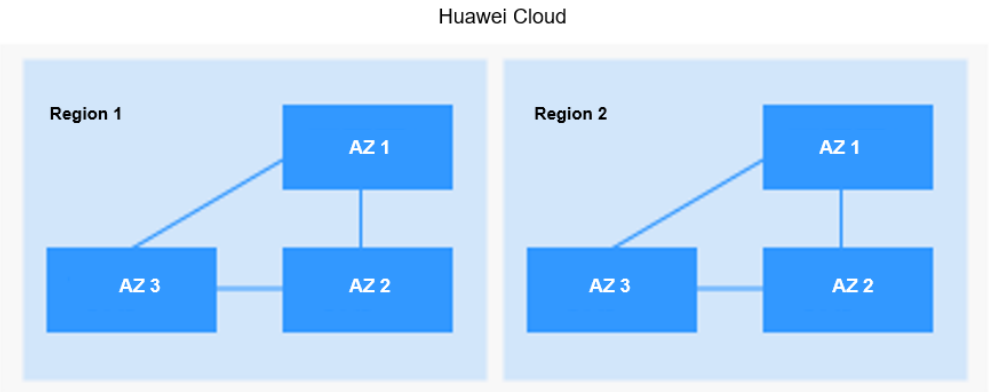
  A region and availability zone (AZ) identify the location of a data center. You can publish applications in a specific region or AZ.

  Regions are determined based on geographical location and network latency. Public service resources, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same cloud region. Regions are either universal or dedicated. A universal region provides universal cloud services for common domains while a dedicated region provides services of the same type only or for specific domains.

  An AZ contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. An AZ's compute, networking, storage, and other resources are logically divided into multiple clusters. AZs within a region are interconnected by high-speed optical fibers for building cross-AZ high-availability systems.

  Figure 1-3 shows the relationship between regions and AZs.

  Figure 1-3 Relationship between regions and AZs

- **Project**

  A project can group and physically isolate compute, storage, and networking resources. A default project is provided for each region, and subprojects can be created under each default project. Users can be granted permissions to access all resources in a specific project. If you need more refined access control, create subprojects under a default project and purchase resources in subprojects. Then you can assign users the permissions required to access only the resources in the specific subprojects.

- **Software client**

  A software client (SC) is a Workspace Application Streaming client installed on a local PC, from which users can access Workspace Application Streaming.

- **Thin client**

  A thin client (TC) is a small-sized commercial PC that is designed based on the PC industry standard. It uses a professional embedded processor, small local flash memory, and simplified OS for accessing Workspace Application Streaming. The TC sends the inputs of the mouse device and keyboard to the background server for processing. Then the server returns the processing result to the monitor connected to the TC for display. The performance, peripheral interfaces, and operation GUIs of TCs vary depending on models, meeting requirements for general office work, security-sensitive office work, and high-performance graphics design.

- **Emergency mode**

  The emergency mode is an emergency channel provided by Workspace Application Streaming. It allows users to log in to Workspace Application Streaming even when third-party authentication is not enabled, and the Workspace Application Streaming authentication module and AD server are normal, but the authentication module cannot connect to the AD server.

1.3 Application Scenarios

Workspace Application Streaming applies to the following scenarios:

General office work

Computers in this scenario are mainly used for routine office work and fixed industry software. If common virtual desktops or PCs are deployed in this scenario, users use only some capabilities of virtual desktops and PCs, causing resource waste and increasing costs. Using Workspace Application Streaming can significantly reduce hardware and OS investment.

The typical remote work scenarios are as follows:

- Task-based office work: Users use the office automation (OA), Notes, and other service systems deployed in a centralized manner through the Intranet or Internet, and do not need to install related software on terminals.
- Dual-network isolation: When users need to access the extranet from the intranet, the application is published on the Workspace Application Streaming platform, and all access operations to the extranet are performed on Workspace Application Streaming. Users do not have permissions for accessing the extranet from their terminals, which ensures user data security.

1.4 Features

Unified Application Provisioning and Management

Applications are centrally managed and virtualized applications are provisioned to users who use different terminals in different regions. The major functions are

application server management, flexible application creation, publishing, query, and deletion.

Unified Application Access

Users can remotely access, start, and stop applications using the Huawei Delivery Protocol (HDP) and access remote applications by using an agent. Remote applications can be managed in lists, pinned on top or unpinned from top, and paginated.

Remote Applications

Remote applications are published on Workspace Application Streaming. Users are isolated by session, and data is stored in the profile file that is located on the file server in roaming mode. End users can access multiple remote applications and switch them in the task bar.

APS Load Balancing

Remote applications are allocated based on the load of the App Server (APS, where applications are installed and deployed), and load scheduling policies based on the number of users, CPU usage, and memory usage are supported.

GUI

Remote applications can be displayed as GUIs on Windows terminals.

User Data Storage

- Remote application desktop data sharing: You can configure folder redirection using an AD group policy to store users' file directories and configurations on shared file servers. In this way, user data and configurations can roam between servers.
- Remote application personal data storage: User personal data is stored on a third-party shared storage system, such as network attached storage (NAS).

Application Session Management

Administrators can manage sessions of remote applications.

Printer Redirection

Local printers connected to a client can be mapped to an application so that the application user can use these printers.

1.5 Billing

Billing Modes

Workspace Application Streaming provides yearly/monthly and pay-per-use billing modes to meet your requirements.

Yearly/Monthly is prepaid. You pay upfront for the amount of time you expect to use Workspace Application Streaming. You will need to make sure you have a top-up account with a sufficient balance or have a valid payment method configured first.

Pay-per-use is postpaid. You use Workspace Application Streaming and then pay as billed for your usage duration.

Billing Items

Pay-per-use instances are not billed when they are stopped. However, the newly purchased sessions will be billed. The billing rules after the instances are stopped are as follows:

- Basic resources (vCPUs, memory, and images) no longer generate costs. Associated resources such as EVS disks, EIPs, and bandwidth will continue to be billed.

A pay-per-use APS can be stopped without being billed. That is, when the APS is stopped but retained, compute resources (vCPUs and memory) are automatically reclaimed. In this case, only storage resources (system disks) will be billed. When you restart the APS, you will apply for vCPUs and memory again. If the resources are insufficient, the startup may fail. Wait several minutes and then restart the APS.

- You are billed based on the number of sessions added to your cloud servers.
- Public/Private NAT gateways are billed based on the public NAT gateway type and service duration. For pricing details, see **NAT Gateway Price Calculator**.
- Windows images are third-party images provided in the Marketplace. A portal is provided for you to select public images. See the price provided by the image provider.
- You will be billed for the storage space of private images. After you delete a created image, you will not be billed anymore. For more information, see **IMS Billing**.
- Network-attached storage (NAS) is billed based on the selected SFS 3.0 Capacity-Oriented file system. See **SFS Billing**.
- Files in the application repository are billed when they are stored in OBS. See .

Renewal

When a billing cycle expires, you can continue using the service through renewal. Alternatively, you can discontinue your service. For details, see **Renewal Management**.

Expiration and Overdue Payment

If your account is in arrears, you can view the arrears details in the Billing Center. To prevent your resources from being stopped or released, top up your account in time. For details, see **Topping Up an Account or Making Repayments**.

1.6 Permissions Management

NOTE

- The Identity and Access Management (IAM) service is used to manage the permissions for accessing cloud services and resources.
- Workspace Application Streaming is a regional project. You can create multiple IAM user groups and grant them the Workspace Application Streaming administrator permissions of different projects to manage users' access to Workspace Application Streaming resources.
- If your Huawei Cloud account does not require individual IAM users for permissions management, skip this section.

Related Concepts

IAM is a free service. You only pay for the resources in your account.

Account

An account is created after you successfully sign up for Huawei Cloud, and you can use it to purchase Huawei Cloud resources. The account has full access permissions for your cloud resources and can be used to make payments for them. You can use the account to reset user passwords, assign permissions, and receive and pay all bills generated by your IAM users for their usage of resources.

You cannot modify or delete your account in IAM, but you can do so in **My Account**.

IAM user

You can use your account to create IAM users and assign permissions for specific resources. Each IAM user has their own identity credentials (passwords or access keys) and uses cloud resources based on 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. New IAM users do not have any permissions assigned by default. You need to add them to one or more groups. The users then inherit permissions from the groups and can perform specified operations on resources or cloud services based on the permissions they have been assigned. If you add a user to multiple user groups, the user inherits all the permissions that are assigned to these groups.

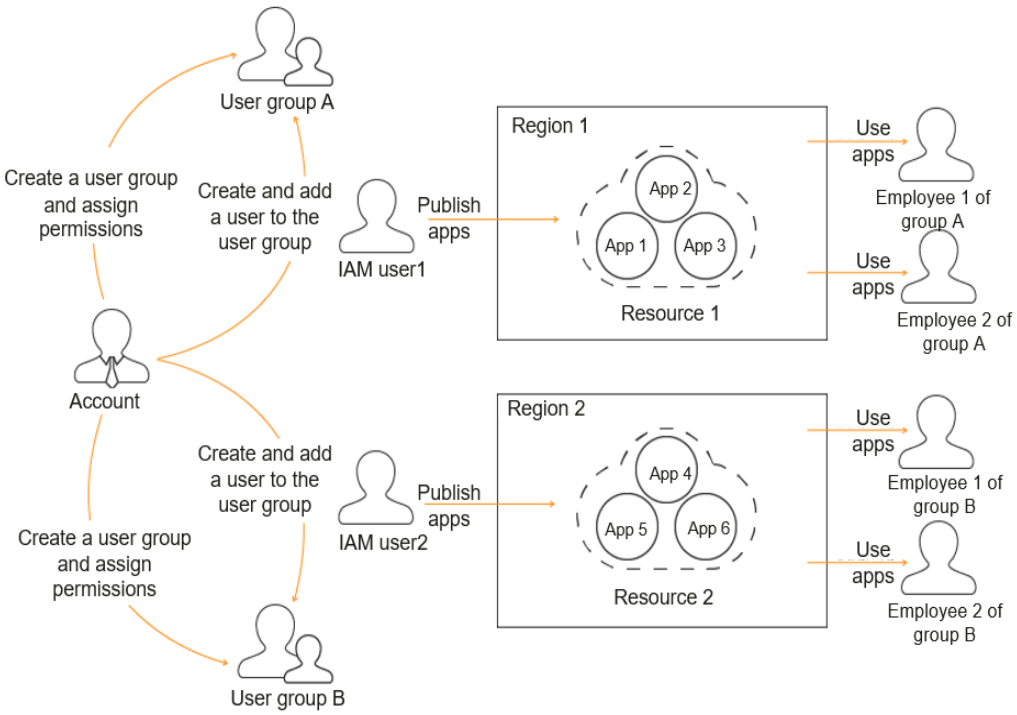
The default user group **admin** has all the permissions for using all of the cloud resources. IAM users in this group can perform operations on all resources, including but not limited to creating user groups and users, assigning permissions, and managing resources.

Examples

For example, you want to isolate permissions of employees in groups a and b. That is, employees in group a use Workspace Application Streaming resources in region 1, and employees in group b use Workspace Application Streaming resources in region 2.

1. You can create user groups A and B and assign them permissions. That is, assign user group A the Workspace Application Streaming administrator permissions in region 1, and assign user group B the Workspace Application Streaming administrator permissions in region 2.
2. Create two IAM users **user1** and **user2**, and add **user1** to user group A and **user2** to user group B. **user1** has the Workspace Application Streaming administrator permissions in region 1, and **user2** has the Workspace Application Streaming administrator permissions 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 Application Streaming console of the project in region 1 to publish applications for the employees of group a and manage the applications 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 Application Streaming console of the project in region 2 to publish applications for the employees of group b and manage the applications of the project in region 2. **Figure 1-4** shows the process. See **Creating an IAM User**.

Figure 1-4 Operation process



Workspace Application Streaming Administrator Permissions

By default, new IAM users do not have permissions assigned. You need to add a user to one or more groups, and grant Workspace Application Streaming administrator permissions to these groups. Users inherit permissions from their groups. After authorization, IAM users can perform operations on Workspace Application Streaming resources in the corresponding projects.

Table 1-1 lists all system permissions of Workspace (Application Streaming) and operation permissions required by dependent services. The **Dependency** column indicates roles on which a Workspace (Application Streaming) system permission depends to take effect. Workspace (Application Streaming) roles are dependent on

the roles of other services because Huawei Cloud services interact with each other. Therefore, when assigning Workspace Application Streaming permissions to a user group, you need to select the permissions listed in **Table 1-1**. Do not cancel other dependent permissions that are selected by default. Otherwise, the Workspace Application Streaming permissions do not take effect.

Table 1-1 System permissions of Workspace (Application Streaming)

System Permission	Description	Dependency
Workspace Administrator	Workspace (Application Streaming) administrator permissions. Users granted these permissions can perform all operations allowed by Workspace (Application Streaming).	This role depends on the **Tenant Guest**, **Server Administrator**, and **VPC Administrator** roles. • **Tenant Guest**: read-only permissions for all cloud services (except IAM) • **Server Administrator**: server administrator • **VPC Administrator**: network administrator
IMS Administrator	Full permissions for IMS.	This role depends on the **Tenant Administrator** role.

Creating an IAM User for Workspace Application Streaming

Step 1 **Creating a user group and assigning permissions**

Create a user group on the IAM console, and assign the **Workspace Administrator**, **IMS Administrator**, and **ECS FullAccess** permissions listed in **Table 1-1** to the group. Then select the authorization scope.

Step 2 **Creating a user and adding them to the user group**

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

Step 3 **Log in** and verify permissions.

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

1. Log in to the Workspace Application Streaming **console**.
2. Select **Authorize**. The Workspace Application Streaming console is displayed.

NOTICE

Workspace Application Streaming supports elastic scaling. You need to obtain user authorization to create an agency account so that the system can automatically scale in or out after elastic scaling is enabled.

3. After the service is enabled, click **Server Groups** in the navigation pane. On the **Server Groups** page, click **Create Server Group** in the upper right corner. If no message indicating insufficient permissions is displayed, the granted permissions have taken effect.

----End

1.7 Supported OSs, Terminals, and Applications

Supported OSs

Applications deployed on Windows Server 2016 and Windows Server 2019 are supported.

- Windows Server 2016 Datacenter edition (Chinese)
- Windows Server 2016 Datacenter edition (English)
- Windows Server 2019 Datacenter edition (Chinese)
- Windows Server 2019 Datacenter edition (English)

Supported Terminal Types

Table 1-2 lists the supported terminal types.

Table 1-2 Supported terminal types

Supported Terminal Type		Remarks
Supported clients	Windows 10 (32-bit and 64-bit)	-

Supported Application Types

Applications in .exe or .msi format obtained from official channels can be published.

1.8 Constraints

Constraints of using Workspace Application Streaming:

- Workspace Application Streaming is available only when the account and password are used for login authentication.
- Only applications deployed on Windows Server 2016 and Windows Server 2019 are supported.
- For login to the APS using the Remote Desktop Protocol (RDP), only the administrator account is currently supported.
- The RD Licensing server must run Windows Server that is not earlier than the RDS CAL version. The RDS CAL version must not be earlier than the Windows Server version of the APS.

- Remote applications do not support screen locking.
- Software compatibility

  Requirements for deploying application software:
  - The software must support multi-instance running at the same time.
  - Software that can be run only by administrators is not supported.
  - Software installed in a personal user directory is not supported.
- Profile and personal data storage

  NOTICE

  To store personal data, users must configure profile and personal data storage. If profile and personal data storage is not configured, do not store personal data on the APS. Otherwise, personal information can be accessed by other users, causing information leakage.

  The user profile data of remote applications is stored on a third-party shared file server using the roaming user configuration and folder redirection functions of Windows. This solution depends on Microsoft's implementation, and users' applications can access only one server. When a user opens multiple applications and accesses multiple APSs at the same time, there will be multiple copies of roaming user configurations. If the user configurations are modified separately, configuration conflicts will occur and the modified configurations cannot be saved to the roaming user configurations.

  User personal data is stored on a third-party shared storage system, such as network attached storage (NAS).
- Cloud applications publish applications using the RDS of Windows Server. Users are isolated by session and do not affect each other. However, if a fault or security problem occurs on the OSs or applications that are shared by all users, all users will be affected. Therefore, cloud applications do not apply to users who have high security and isolation requirements.

2 Administrator Operation Guide

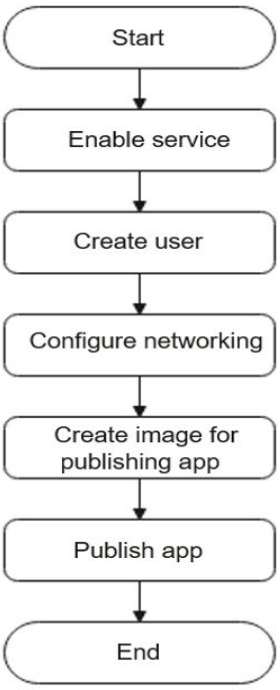
2.1 Operation Procedure
2.2 Logging In to the Workspace Application Streaming Console
2.3 Enabling the Service
2.4 Creating a User
2.5 Applications and Images
2.6 Server Groups
2.7 Application Groups
2.8 User Management
2.9 Policy Groups
2.10 Monitoring Analysis
2.11 OU Management
2.12 Application Internet Access Management
2.13 Upgrading Protocol Components
2.14 Scheduled Tasks
2.15 Storage
2.16 Tenant Configuration
2.17 Private Images
2.18 Configuring Personalized Data
2.19 Subscribing to an Event
2.20 Permissions Management
2.21 Configuring Common Functions
2.22 Monitoring
2.23 FAQs

2.1 Operation Procedure

Figure 2-1

shows the operation process of Workspace Application Streaming.

Figure 2-1 Operation process for administrators



2.2 Logging In to the Workspace Application Streaming Console

Step 1 Log in to the **Huawei Cloud homepage** and click **Console** in the upper right corner.

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

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

The Workspace console page is displayed.

Step 4 In the navigation pane on the left, choose **Workspace Application Streaming**.

----End

2.3 Enabling the Service

Scenarios

Workspace Application Streaming can be enabled after tenant information is configured on the console.

Prerequisites

- The administrator has permission to perform operations on Workspace Application Streaming.

  NOTE

  - By default, a Huawei Cloud account has the operation permissions on all Huawei Cloud services. If you use such an account, you do not need to confirm it.
  - To use Workspace Application Streaming, the IAM account created under the Huawei Cloud account must be added to the **admin** user group or a user group with Workspace Application Streaming 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 Workspace Application Streaming**.

- The AD server and RD Licensing server have been prepared by referring to **2.23.4 How Do I Deploy a Windows AD Server?** and **2.23.5 How Do I Deploy an RD Licensing Server?**, and the licenses have been configured and activated on the servers.

  NOTE

  - Required only when the AD is interconnected.
  - To ensure the continuous availability of the RD Licensing server, configure RDS authorization and security policies for the server by referring to **2.23.6 How Do I Configure RDS Licensing and Security Policies?**.

- You have configured the network communication between Workspace Application Streaming and Windows AD by referring to **2.23.10 How Do I Configure Network Connection Between Workspace Application Streaming and the Windows AD?** and prepared the following data:
  - Domain Name
  - Domain Administrator Account
  - Domain Administrator Password
  - Name of Active Domain Controller
  - IP Address of Active Domain Controller
  - Active DNS IP Address
  - (Optional) Name of Standby Domain Controller
  - (Optional) IP Address of Standby Domain Controller
  - (Optional) Standby DNS IP Address

    NOTE

    Required only when the AD is interconnected.

Procedure

Enabling service self-check

Step 1 Log in to the Workspace Application Streaming **console** as an administrator.

Step 2 Click **Activate the Service**.

Step 3 Service provisioning guides enterprises to determine whether to interconnect with the AD server.

- No: If you choose not to interconnect with the AD server, only single-session applications can be created in the current project. Go to **10**.
- Yes: If you choose to interconnect with the AD server, single-session applications and multi-session applications can be created in the current project. Go to **4**.

Step 4 After the AD server and RDS license server are configured in **Prerequisites**, click **YES**.

Step 5 Click **Finish**.

Configuring the project

Step 6 In the navigation pane on the left, choose **Tenant Configuration**.

Step 7 Select a project, or click **Create Project** to **create one**.

(Optional) Setting the enterprise ID

Step 8 Set the enterprise ID.

NOTE

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

  It is recommended that identifiable fields, such as the enterprise name, be used as the enterprise ID. The enterprise ID can be changed.
- The **enterprise ID** can contain a maximum of 32 characters, including digits, letters, underscores (_), and hyphens (-).

Configuring the AD domain

Step 9 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
- **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
- Deleting Computer Objects on AD
  - **Yes**: When the APS is deleted, the computer objects in the AD domain are also deleted.
  - **No**: When the APS is deleted, the computer objects in the AD domain are not deleted.
- (Optional) Advanced settings
  - Name of Standby Domain Controller
  - IP Address of Standby Domain Controller
  - Standby DNS IP Address

Configuring the network

Step 10 Configure the **VPC** and **Service subnet**, as shown in **Figure 2-2**.

Figure 2-2 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**.

NOTE

- The resources required by Workspace Application Streaming will be created in the selected VPC subnet. After the first successful purchase, the VPC cannot be modified.
- A VPC is an isolated, configurable, and manageable virtual network environment for cloud applications, facilitating internal network management and configuration. Your Workspace Application Streaming service will be created in the selected VPC subnet to facilitate your access to the resources and applications on the enterprise intranet.
- 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 11 Select a network access mode, as shown in **Figure 2-3**. By default, **Internet** is selected. You can select multiple options.

Figure 2-3 Network access

NOTE

- If you require high network quality and security, you can purchase a **Direct Connect** connection and perform network construction in advance.
- 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.
- If you want to upgrade the client online through Direct Connect, you need to **configure a VPC endpoint for accessing OBS using the OBS private address**. You can submit a service ticket to query the endpoint service of the corresponding region.

Step 12 Click **Save Configuration** to start deploying Workspace Application Streaming resources.

When Workspace Application Streaming resources are successfully deployed, Workspace Application Streaming has been enabled. You can go to **create a user**.

If enabling the service fails, perform operations as prompted.

----End

2.4 Creating a User

Workspace Application Streaming and Workspace share the same user list. For details, see section "User Management" in *Workspace Administrator User Guide*.

NOTE

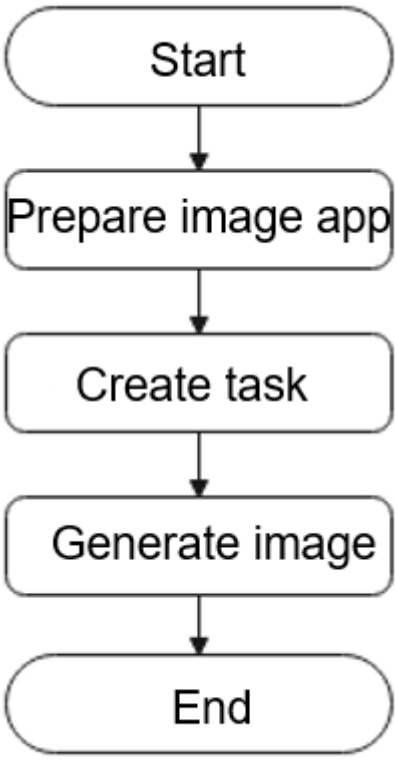
Workspace Application Streaming and Workspace under the same project share the same user list.

2.5 Applications and Images

Process of Creating an Image for Publishing an Application

See **Figure 2-4**.

Figure 2-4 Process of creating an image for publishing an application



2.5.1 Application Repositories

Scenarios

This section describes how to create an image application.

NOTE

Uploading an application for the first time requires an OBS bucket.

Procedure

Step 1 Log in to the Workspace Application Streaming **console** as an administrator.

Step 2 In the navigation pane on the left, choose **Applications and Images** > **Application Repositories**.

Step 3 On the **Application Repositories** page, click **Create App**.

Step 4 Configure the parameters based on **Table 2-1**.

Table 2-1 Parameters for creating an application

Parameter	Description	Example Value
Name	Custom application name. Naming rules: • 1 to 64 characters • Letters, digits, hyphens (-), and underscores (_) only	App01-name
Category	Select a category based on the application function.	Productivity and collaboration
Platform	OS type. Only Windows is supported.	Windows
Version	Custom version name.	-
Version Number	Custom version number to facilitate upgrade and maintenance.	v1
Upload Method	**Upload Application**: valid when uploading an application Click  to select the application installation file obtained from an official channel. Files in .exe, .msi, .rar, or .zip formats are supported. If the file size exceeds 5 GB, select **OBS Path**. Select **I have read and agree to Non-infringement Commitment and Disclaimer**.	-
	OBS Path: where the file is stored Enter the OBS file path. For details, see "Uploading an Object" in **OBS User Guide**. Select **I have read and agree to Non-infringement Commitment and Disclaimer**.	-
Description	Describe the characteristics of the application to facilitate maintenance.	This application is published for the first time and available only to developers.

Parameter	Description	Example Value
Icon	Application icon. Only the PNG format is supported, and the file size must be less than 8 KB. **NOTE** If no icon is uploaded, the default cloud application icon is displayed.	-

Step 5 Click **OK**.

----End

2.5.2 Image Creation

Scenarios

Administrators can publish image applications for users based on actual application scenarios.

Prerequisites

- You have obtained the app installation file from an official channel.
- (Optional) You have created a basic image by referring to **2.17.1 Creating a Windows Private Image (Basic Image)**.
- You have created an image application by referring to **2.5.1 Application Repositories**.

  NOTE

  Workspace Application Streaming supports images on KooGallery as basic images. If a private image is required as the basic image, create one on the image service page.

Creating an Image Task

Step 1 Log in to the Workspace Application Streaming **console** as an administrator.

Step 2 In the navigation pane on the left, choose **Applications and Images** > **Image Creation**.

Step 3 Click **Create Image Task** to access the image creation page.

Step 4 Configure the parameters based on **Table 2-2**.

Table 2-2 Parameters for creating an image task

Parameter	Description	Example Value
Name	Customize the image task name. Naming rules: ● 1 to 64 characters ● Letters, digits, hyphens (-), and underscores (_) only	image-task01-name
Description	Enter the description as required.	Publish an application that is not included in the default application list.
Session Mode	● Single-session ● Multi-session **NOTE** – In scenarios where the AD server is not interconnected, only the single-session mode is supported. – In scenarios where the AD server is interconnected, the single-session mode and multi-session mode are supported.	-
Billing Mode	Only pay-per-use billing is supported.	Pay-per-use
AZ	An AZ is a physical region where resources use independent power supplies and networks. AZs are physically isolated but connected through an intranet. If an AZ becomes faulty, other AZs in the same region will not be affected.	-
CPU Architecture	Currently, only x86 is supported.	x86
Package Type	Select a package for publishing the application based on the application type and specifications.	-
OS	OS type. Only Windows is supported.	Windows

Parameter	Description	Example Value
Image	Images on KooGallery and private images are supported. If you use a private image, ensure that you have created one by referring to **2.17.1 Creating a Windows Private Image (Basic Image)** or an image has been generated with an image task that has successfully published an application.	KooGallery
Disk Type	Select a disk type as required. • EVS • DSS	-
System Disk	Select a system disk type as required. The capacity of a system disk ranges from 10 GB to 1,020 GB. The value must be an integer multiple of 10.	High I/O disk 80 GB
Network	Select an existing subnet or click **click here to create a subnet** to create one. For details, see **Creating a Subnet for the VPC**.	-
OU Name	If an OU is created on the Windows AD server, you can select the OU to be used. **NOTE** This parameter is required only when the AD is connected.	-
Additional Sessions	Additional sessions for a single server. The value varies with the server specifications. **NOTE** After a server group is created, the number of sessions cannot be changed.	-

Parameter	Description	Example Value
Session Scheduling Policy	• Number of Session Connections: Session connections of the server. Set this parameter based on the server specifications. • CPU Usage: CPU usage of the server. The value ranges from 1 to 100. • Memory Usage: Memory usage of the server. The value ranges from 1 to 100. **NOTE** If any metric of a server exceeds the threshold, no more sessions are accepted. The policy schedules available servers in the server group to establish sessions.	-
Account	Select a user account as the management account for creating the image. • If the AD is interconnected, the default account is the administrator account of the AD domain. • If the AD is not interconnected, select a user account as the management account for creating the image.	-

Step 5 Click **Confirm**.

Step 6 Confirm the information and click **Create**.

Go to the image list page to check the status of the created image task. If the status shows **Instance running**, you can find the server group and application group with the same name as the image task in the server group list and application group list.

----End

Generating an Image

Installing an application

Step 1 Log in to the Workspace Application Streaming **console** as an administrator.

Step 2 In the navigation pane on the left, choose **Applications and Images** > **Image Creation**.

Step 3 Locate the image task (in the **Instance running** or **Image task complete** status) created in **Step 6**. Click **Generate Image** in the **Operation** column.

Step 4 Prepare the application.

The administrator can upload an application to the APS in any of the following ways:

- Method 1: Upload the application to the image repository. For details, see **2.5.1 Application Repositories**. Select the application to be installed and synchronize the download link to the server.
- Method 2: Configure the file redirection or clipboard redirection policy for the user or application group. After logging in to the APS, copy the application file from the local PC to the server.
  a. Get the .exe or .msi file of the application from an official channel and store it in a local storage device.
  b. For details about configuring a policy for a user or application group, see **3.4.6 How Do I Enable a Local Storage Device to Copy Files to an APS?**. Set **Policy Object** to the administrator account or application group created in the image task.
- Method 3: Enable the Internet access for the APS by referring to **2.21.1 Allowing Workspace Application Streaming to Access the Internet**. After logging in to the server, you can download the application file from a browser over the Internet.

Step 5 Click **Next: Install Application**.

Step 6 Click **Download** to go to the page for downloading Workspace client.

Step 7 Download the Windows version and install it.

Step 8 Start the Huawei Cloud Workspace client on a local device.

Step 9 Enter the server address, enterprise ID, username, and password on the **Install Application** page to log in.

Step 10 Click **Windows Desktop** to access the APS.

Step 11 After logging in to the APS, select an installation mode based on the uploading method in **Step 4**.

- Method 1: Select the application from the application repository.
  a. Double-click **CloudClientApps** to access the application list page.
  b. Select the target application, and download and install it as prompted.
- Method 2: Copy the application from the local host to the APS using a policy.
  a. Copy the application file to the APS.
  b. Open the corresponding application and install it.
- Method 3: The Internet access has been enabled for the APS.
  a. Open a browser.
  b. Search for the corresponding application, and download and install it.

(Optional) Installing the sandbox software

Verifying the application

Step 12 Click **Next: Verify Image**

Step 13 Publish the application. The application list page is displayed.

Step 14 Click **Add App** and select the application installed in **Step 11**.

Step 15 Click **OK**.

Step 16 Click the **User Authorization** tab.

Step 17 Click **Add User**. The list of users to be added is displayed.

Step 18 Select the user to use the application and click **OK**.

The user will receive a notification email from the Workspace Application Streaming authorization service.

Step 19 The user downloads and installs the Workspace client running Windows according to email instructions, and enters the server address, enterprise ID, username, and password in the email to log in.

Step 20 Use the application.

Creating a built-in administrator account when the AD is not interconnected

Step 21 Access the APS, click  , enter **compmgmt.msc**, and press **Enter**. The **Computer Management** window is displayed.

Step 22 In the navigation pane, choose **Local Users and Groups** > **Users**.

Step 23 Right-click and choose **New User** from the shortcut menu.

Step 24 In the **New User** dialog box, enter the username (example: **admin**) and password, confirm the password, and click **Create**.

NOTE

Keep the new userpassword secure. This account will be used for APS O&M.

Step 25 In the navigation pane, choose **Local Users and Groups** > **Groups**.

Step 26 Right-click **Administrator** 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 27 In the **Administrator Properties** dialog box, click **Add** to add the user to the group.

Step 28 Click **OK** and close the **Administrator Properties** dialog box.

Generating an image

Step 29 Click **Next: Generate Image**.

Step 30 Customize the image name and enter a description.

Step 31 Click **Generate in One Click**.

Return to the image list page. The task status is **Creating**. If the task status is **Image task complete**, you can use the image to update available applications after the image is created.

----End

2.5.3 Managing an Image Task

Scenarios

After creating an image task and generating an image, the administrator can update the application in the image task, change the image task name, and delete the image task.

Prerequisites

An image task has been created.

Procedure

Step 1 Log in to the **management console** of Workspace Application Streaming as an administrator.

Step 2 In the navigation pane on the left, choose **Applications and Images** > **Image Creation**.

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

Table 2-3 Operations on an image task

Operation	Procedure	Description
Updating an application pending installation on the server	1. Click **Generate Image** in the **Operation** column. 2. Select the updated application in the application repository and click **Synchronize Link**. 3. Click **Next: Install Application**. 4. Log in to the APS and install the application. You can copy an application from the local host to the APS for installation using a policy, or download an application from the browser over Internet.	During application publishing, if the verification fails, update the application to check whether the application is faulty.
Viewing an image	1. In the task list, click an image ID to go to the details page. 2. View the images generated by the image task.	Images can be viewed after they are generated by the task.

Operation	Procedure	Description
Viewing all images	Click **View All Images** in the upper left of the image task list, or go to the Image Management Service (IMS) to view all your images on the **Private Images** tab page.	All images created by an administrator are private images and are displayed in the private image list in IMS.
Viewing resources associated with an image	• In the **Operation** column, choose **More** > **Associate Resource** > **Server Groups**. • In the **Operation** column, choose **More** > **Associate Resource** > **Application Groups**.	Administrators can view the server group and application group automatically generated by the image task to facilitate management.
Changing the name of an image task	1. In the **Operation** column, choose **More** > **Edit**. 2. Modify the task name and description. 3. Click **OK**.	If the name of an image task is misleading, the administrator can rename it.
Deleting an image task	1. In the **Operation** column, choose **More** > **Delete**. 2. (Optional) Delete the resources (server group and its servers, and application group) associated with the task. **NOTE** If you do not select **Delete the resources (server group and its servers, and application group) associated with the task**, the server group and application group created using the image task are still available. 3. Click **OK**.	If an image has been generated using an image task, you can delete the task to release the image creation server resources to save costs.

----End

2.6 Server Groups

2.6.1 Managing Server Groups

2.6.1.1 Creating a Server Group

Scenarios

Before publishing an application, the administrator needs to create a server group for deployment.

Prerequisites

You have created an image by referring to **2.5.2 Image Creation**.

Procedure

Step 1 Log in to the Workspace Application Streaming **console** as an administrator.

Step 2 In the navigation pane, choose **Server Groups**.

Step 3 Click **Create Server Group**.

Step 4 Configure the parameters based on **Table 2-4**.

Table 2-4 Server group parameters

Parameter	Description	Example Value
Server Group Name	Custom server group name. Naming rules: • 1 to 64 characters • Letters, digits, hyphens (-), and underscores (_) only	Server_Gp-Win2016
Description	Enter the description as required.	-
Region	Region where the application is to be deployed. Applications in different regions cannot communicate with each other over the intranet, and applications need to be managed by region. You are advised to create applications in the same region.	CN South-Guangzhou
Project	Select a project to be deployed as planned.	cn-south-1

Parameter	Description	Example Value
Session Mode	• Single-session • Multi-session **NOTE** – In scenarios where the AD server is not interconnected, only the single-session mode is supported. – In scenarios where the AD server is interconnected, the single-session mode and multi-session mode are supported.	-
App Group Type	• Application: Users can access an application without installing it. • Desktop: A desktop application group is a complete virtual desktop. Users access the remote desktop.	Application
Associated Application Group	Determine whether to select **Auto create**. **NOTE** After selecting **Auto create** , enter the application group name. The name contains 1 to 64 characters, including letters, digits, hyphens (-), and underscores (_).	Select **Auto create**.
Billing Mode	Select **Yearly/Monthly** or **Pay-per-use** as required.	Pay-per-use
AZ	An AZ is a physical region where resources use independent power supplies and networks. AZs are physically isolated but connected through an intranet. If an AZ becomes faulty, other AZs in the same region will not be affected.	Random
OS	OS type of the server to be created. Currently, only the Windows OS is supported.	Windows
CPU Architecture	Currently, only x86 is supported.	x86
Package Type	Select the office type and specifications based. • General office: general office applications • Graphics-optimized: efficient graphics processing applications	General office -

Parameter	Description	Example Value
Image	Select the image type and version used by the server. • A KooGallery image is a standard OS image provided by Workspace Application Streaming and is visible to all users. It contains an OS and preinstalled applications. KooGallery images are highly stable and authorized. Windows Server 2016/2019 Datacenter edition (English) image is supported. • A private image is created based on a standard OS image file. It is visible only to the user who created it. You can customize pre-installed applications. Select the images generated in **2.5.2 Image Creation**.	Private -
Disk Type	Select a disk type.	-
System Disk	Select a disk type and set the disk size. See **EVS disk types and performance**. • High I/O disks use serial attached SCSI (SAS) drives to store data. • Ultra-high I/O disks use solid state disk (SSD) drives to store data. The disk size ranges from 10 GB to 1,020 GB. The value must be an integer multiple of 10.	High I/O disk 1020
Network	Select a virtual network. If applications need to be available in multiple service subnets, select multiple subnets or click **Click here to manage subnets** under network configuration to create a subnet. A VPC is an isolated, configurable, and manageable virtual network environment for cloud applications, facilitating internal network management and configuration. Your Workspace Application Streaming service will be created in the selected VPC subnet to facilitate your access to the resources and applications on the enterprise intranet.	-

Parameter	Description	Example Value
Additional Sessions	Additional sessions for a single server. The value varies with the server package specifications. **NOTE** • After a server group is created, the number of sessions cannot be changed.	-
Session Scheduling Policy	• Number of Session Connections: Session connections of the server. Set this parameter based on the server package specifications. • CPU Usage: CPU usage of the server. The value ranges from 1 to 100. • Memory Usage: Memory usage of the server. The value ranges from 1 to 100. **NOTE** If any metric of a server exceeds the threshold, no more sessions are accepted. The policy schedules available servers in the server group to establish sessions.	-
OU Name	If an OU is created on the Windows AD server, you can select the OU to be used. **NOTE** This parameter is required only when the AD is connected.	-
Protocol Component	HDP server access component, which is installed in the APS instance and used to communicate with the Workspace Application Streaming client. **NOTE** After this option is selected, if the version of the component in your image is outdated, the component will be upgraded during provisioning, which may prolong the provisioning.	Check the box.

Parameter	Description	Example Value
IP Virtualization	•  : IP virtualization is disabled. •  : IP virtualization is enabled. **NOTE** – If IP virtualization is enabled, each session is assigned a different IP address. The number of virtual IP addresses pre-assigned by the server is the same as the maximum number of sessions in the package. – Maximum number of sessions = Default number of sessions + Additional sessions – This parameter can be configured only in multi-session mode.	
Scaling Policy	•  : The scaling policy is disabled. •  : The scaling policy is enabled. If the scaling policy is enabled, configure the policy. – Scale-out policy: When the session usage exceeds *x*%, pay-per-use elastic resources are automatically created. **NOTE** Session usage = Sum of instance sessions in use/(Maximum number of instance sessions × Available instances) Available instances: number of servers that are in the **Ready** status but not under maintenance Maximum number of sessions = Default number of sessions of the selected package + Additional sessions – *x* (range: 1–10) sessions can be created at a time. A maximum of *x* (range: 1–100) sessions can be created. – Scale-in policy: Elastic resources without session connections can be retained for a maximum of *x* (range: 5–120) minutes.	

Step 5 Configure the purchase quantity and duration.

If the billing mode is **Yearly/Monthly**, configure the required duration.

Step 6 Click **Next step: Confirm Settings**.

If the billing mode is **Yearly/Monthly**, you can choose whether to automatically renew the subscription.

Step 7 Confirm the configuration and click **Buy Now**.

- The billing mode is **Pay-per-use**. After the resource is created, you can view the purchased server group and its servers on the **Server Groups** page.
- If the billing mode is **Yearly/Monthly**, pay for the order first and view the purchased server group and its servers on the **Server Groups** page.

----End

2.6.1.2 Modifying a Server Group

Scenarios

Administrators can change the name of a server group and update the image of the server group based on service requirements.

Procedure

Step 1 Log in to the Workspace Application Streaming **console** as an administrator.

Step 2 In the navigation pane, choose **Server Groups**.

Step 3 Perform the operations listed in **Table 2-5** as required.

Table 2-5 Configuring a server group

Operation	Procedure	Description
Modify a server group image	1. Choose **More** > **Edit**. 2. Switch **Image** to the required one. 3. Select **Confirm the image modification** and click **OK**. **NOTE** If the image is replaced, old applications may fail to be connected.	When adding or upgrading an application, you can change the server group image to the image for installing new applications.
Modify a server group name	1. Choose **More** > **Edit**. 2. Modify the server group name. 3. Click **OK**.	If the server group name is misleading, the administrator can rename the server group.

Operation	Procedure	Description
Change an application group type	1. Choose **More** > **Edit**. 2. Change **App Group Type** to **Application** or **Desktop**. 3. On the **Unbind Application Group** page, select **Unbind all associated application groups** and click **OK**. 4. Determine whether to select **Auto create**. 5. Click **OK**. **NOTE** – After selecting **Auto create**, enter the application group name. The name contains 1 to 64 characters, including letters, digits, hyphens (-), and underscores (_). – To change the application group type of a server group, you need to unbind all associated application groups. After the unbinding, users authorized by the application group cannot use applications in the application group. – After the application group type of the primary server is changed, the change is automatically applied to the standby server.	-
Modify server group description	1. Choose **More** > **Edit**. 2. Modify the description. 3. Click **OK**.	The description records the image and purpose of the server group for easier maintenance.
Adjust the system disk size	1. Choose **More** > **Edit**. 2. Adjust the system disk size. 3. Click **OK**.	Administrators can adjust the system disk size.
Modify OU information	1. Choose **More** > **Edit**. 2. Select the required OU from the **OU Name** drop-down list box. 3. Click **OK**. **NOTE** This parameter is required only when the AD is connected.	If the administrator has not configured OU information for the server, configure OU information here.

Operation	Procedure	Description
Scaling Policy	1. Click **Edit** on the right of **Scaling Policy**. The **Scaling Policy** page is displayed. 2. Toggle on  on the right of **Scaling Policy** to enable the scaling policy. 3. Configure a scaling policy. – **Scale-Out Policy**: When the session usage exceeds *x*%, pay-per-use elastic resources are automatically created. **NOTE** Session usage = Sum of instance sessions in use/ (Maximum number of instance sessions × Available instances) Available instances: number of servers that are in the **Ready** status but not under maintenance Maximum number of sessions = Default number of sessions of the selected package + Additional sessions – *x* (range: 1–10) sessions can be created at a time. A maximum of *x* (range: 1–100) sessions can be created. – **Scale-In Policy**: Elastic resources without session connections can be retained for a maximum of *x* minutes. (value range: 5–120). 4. Click **Edit** on the right of **Scaling Policy**. The **Scaling Policy** page is displayed. 5. Toggle off  on the right of **Scaling Policy** to disable the scaling policy. 6. Click **OK**.	Administrators can enable or disable the scaling policy of a server group.

Operation	Procedure	Description
Server Group Status	1. Click a server group name. The basic information page of the primary server group is displayed. 2. Click **Enable** on the right of **Server Group Status**. In the displayed dialog box, click **OK**. 3. Click **Disable** on the right of **Server Group Status**. In the displayed dialog box, click **OK**.	Administrators can enable or disable a server group.
Mounting Policy	1. Click a server group name. The basic information page of the primary server group is displayed. 2. Click  on the right of **Mounting Policy**. The **Modify Mounting Policy** dialog box is displayed. 3. Modify the directory settings and click **OK**. **NOTE** After the mounting policy of the primary server is changed, the change is automatically applied to the standby server.	Administrators can modify the directory settings of the mounting policy.

----End

2.6.1.3 Deleting a Server Group

Scenarios

Administrators can delete idle server groups based on service scenarios when system resources are sufficient.

Procedure

Step 1 Log in to the Workspace Application Streaming **console** as an administrator.

Step 2 In the navigation pane, choose **Server Groups**.

Step 3 In the **Operation** column, choose **More** > **Delete**.

NOTE

- Before deleting a server group, delete the standby server group (if any).
- When deleting a server group, you need to delete the instances in the server and disassociate the application groups from the server.

----End

2.6.2 Managing APSs

2.6.2.1 Adding a Server

Scenarios

Administrators can add servers to a primary/standby server group when system resources are insufficient.

Procedure

Adding a server

Step 1 Log in to the Workspace Application Streaming **console** as an administrator.

Step 2 In the navigation pane, choose **Server Groups**.

Step 3 In the **Operation** column of the created server group, click **Add Server**.

Step 4 Configure the parameters based on **Table 2-6**.

Table 2-6 Server parameters

Parameter	Description	Example Value
Billing Mode	Select the charging mode of the server. **NOTE** The pay-per-use and yearly/monthly billing modes are supported.	Yearly/Monthly
AZ	An AZ is a physical region where resources use independent power supplies and networks. AZs are physically isolated but connected through an intranet. If an AZ becomes faulty, other AZs in the same region will not be affected. **NOTE** To achieve better disaster recovery, you are advised to create applications in different AZs.	Random

Parameter	Description	Example Value
Required Duration	In yearly/monthly billing mode, you can configure the required duration of the new server. Select the required duration of the server. Configure automatic renewal as required. • If you enable auto-renew, the system automatically deducts the renewal fee after the required duration ends. • If you disable auto-renew, the resource will be frozen and unavailable after the required duration expires.	1 year
Quantity	Select the number of servers of the same specifications.	1
OU Name	If an OU is created on the Windows AD server, you can select the OU to be used. **NOTE** This parameter is required only when the AD is connected.	-
Protocol Component	Huawei Delivery Protocol (HDP) server access component is installed on the APS and used to communicate with the Workspace client. **NOTE** After this option is selected, if the version of the component in your image is too early, the component will be upgraded during provisioning, which may prolong the provisioning.	Check the box.

Step 5 Click **Buy Now**.

----End

2.6.2.2 Unsubscribing from a Server

Scenarios

Administrators can unsubscribe from yearly/monthly servers in a primary/standby server group.

Procedure

Step 1 Log in to the Workspace Application Streaming **console** as an administrator.

Step 2 In the navigation pane, choose **Server Groups**.

Step 3 Click a server group name. The server list page is displayed.

Step 4 Select a yearly/monthly server that has not expired.

- To unsubscribe from a server, perform steps **Step 5** to **Step 8**.
- To unsubscribe from servers in batches, perform steps **Step 9** to **Step 12**.

Step 5 Locate the row that contains the target server and click **More** > **Unsubscribe** in the **Operation** column. The **Unsubscribe from Server** dialog box is displayed.

Step 6 Click **Yes**. The page for unsubscribing from resources is displayed.

Step 7 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.**

Step 8 Select **Confirm** and click **Yes**.

Step 9 Select the servers to be unsubscribed from in batches and click **More** > **Unsubscribe** in the upper left corner. The **Unsubscribe from Server** dialog box is displayed.

Step 10 Click **Yes**. The page for unsubscribing from resources is displayed.

Step 11 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.**

Step 12 Select **Confirm** and click **Yes**.

NOTE

- If your order was paid using a third-party online payment platform, such as WeChat or Alipay, the refund for an unsubscription will be paid to your Huawei Cloud account.
- The actual amount is subject to the amount in the bill.

----End

2.6.2.3 Deleting a Server

Scenarios

Administrators can delete servers of a primary/standby server group when system resources are sufficient.

Procedure

Step 1 Log in to the Workspace Application Streaming **console** as an administrator.

Step 2 In the navigation pane, choose **Server Groups**.

Step 3 Click a server group name. The server list page is displayed.

Step 4 Select the pay-per-use server to be deleted.

- To delete a server, perform **Step 5** to **Step 6**.
- To delete servers in batches, perform **Step 7** to **Step 8**.

Step 5 Locate the row that contains the desired server, and click **More** > **Delete** in the **Operation** column. The **Delete Server** page is displayed.

Step 6 Confirm the server information, select **Confirm**, and click **Yes**.

Step 7 Select the desired servers and click **More** > **Delete** in the upper left corner. The **Delete Server** page is displayed.

Step 8 Confirm the server information, select **Confirm**, and click **Yes**.

----End

2.6.2.4 Releasing a Server

Scenarios

Administrators can release yearly/monthly servers that have expired but have not been renewed in a primary/standby server group.

Procedure

Step 1 Log in to the Workspace Application Streaming **console** as an administrator.

Step 2 In the navigation pane, choose **Server Groups**.

Step 3 Click a server group name. The server list page is displayed.

Step 4 Locate the row that contains a yearly/monthly server that has expired but has not been renewed, and click **More** > **Release** in the **Operation** column. The **Release Server** page is displayed.

Step 5 Click **Yes**. The **Release** page is displayed.

Step 6 Click **Release**. On the page for confirming resource release, click **Yes**.

----End

2.6.2.5 APS Management

Scenarios

Administrators can maintain, restart, or rename servers in a primary/standby server group.

Procedure

Step 1 Log in to the Workspace Application Streaming **console** as an administrator.

Step 2 In the navigation pane, choose **Server Groups**.

Step 3 Click a server group name and perform operations listed in **Table 2-7** as required.

Table 2-7 Server operations

Operation	Procedure	Description
View APS information	1. Select **All**, **Maintaining**, or **Non-maintenance** from the **Maintenance Status** drop-down list. Administrators can filter the required servers by instance name, instance ID, server name, or server IP address, and click  to filter.	Administrators can filter the required servers.
Modify a server name	1. Click  next to **Name**. 2. Enter the new name and click **√**. **NOTE** The server name can contain 1 to 64 characters, including uppercase letters, lowercase letters, digits, hyphens (-), and underscores (_).	If a server name is misleading, administrators can rename the server.
Stop a server	1. Select the servers to be stopped and click **Shut Down** in the upper left corner to stop them in batches. Alternatively, locate the row that contains the target server and click **More** > **Shut Down** in the **Operation** column to stop the server. 2. Select **Confirm**. 3. Click **Yes**.	Administrators can stop a server. After the server is stopped, applications cannot run on the server.
Start a server	1. Select the servers to be started and click **Start** in the upper left corner to start them in batches. Alternatively, locate the row that contains the target server and click **More** > **Start** in the **Operation** column to start the server. 2. Select **Confirm**. 3. Click **Yes**.	Administrators can start a stopped server so that applications can run on the server.

Operation	Procedure	Description
Restart a server	1. Select the servers to be restarted and click **Restart** in the upper left corner to restart them in batches. Alternatively, locate the row that contains the target server and click **More** > **Restart** in the **Operation** column to restart the server. 2. Select **Confirm**. 3. Click **Yes**.	Administrators can restart a server.
Maintain a server	1. Select the servers to be maintained and click **More** > **Maintain** in the upper left corner to maintain them in batches. Alternatively, locate the row that contains the target server and click **More** > **Maintain** in the **Operation** column to maintain the server. 2. Select **Confirm**. 3. Click **Yes**.	Administrators can select a server for maintenance. In this case, applications cannot run on the server.
Cancel server maintenance	1. Select the servers whose maintenance needs to be canceled and click **More** > **Cancel Maintenance** in the upper left corner to cancel the maintenance of the selected servers in batches. Alternatively, locate the row that contains the target server and click **More** > **Cancel Maintenance** in the **Operation** column to cancel maintenance of the server. 2. Select **Confirm**. 3. Click **Yes**.	Administrators can cancel the maintenance of a server so that applications can run on the server.
Remotely log in to a server	1. Click **Remote Login** in the **Operation** column. The server screen lock page is displayed. 2. Click **Send CtrlAltDel** in the upper right corner. 3. Enter the account and password to log in.	Administrators can remotely log in to a server.

Operation	Procedure	Description
Renew a server	1. Select the servers to be renewed and click **More** > **Renew** in the upper left corner to renew them in batches. Alternatively, locate the row that contains the target server and click **More** > **Renew** in the **Operation** column to renew the server. 2. Click **Yes**.	Administrators can renew a yearly/monthly server.
Rejoin a domain	1. Select the servers to rejoin the domain and click **More** > **Rejoin Domain** in the upper left corner to add them in batches. Alternatively, locate the row that contains the target server and click **More** > **Rejoin Domain** in the **Operation** column to add the server to the domain. 2. Confirm the operation. 3. Click **Yes**. **NOTE** Rejoining a domain is supported only when the AD is interconnected with.	If login to a server fails, you can rejoin a domain. **NOTE** If rejoining a domain fails, rectify the fault by referring to **2.23.18 How Do I Do If I Fail to Add a Computer Back to the Domain?**.
Update a virtual IP address	1. Select the servers whose virtual IP addresses need to be updated and click **More** > **Update Virtual IP** in the upper left corner to update them in batches. Locate the row that contains the target server and click **More** > **Update Virtual IP** in the **Operation** column to update the virtual IP address for the server. 2. Select **Confirm** and click **Yes**.	If the virtual IP address of the server is abnormal, you can update the virtual IP address.

Operation	Procedure	Description
Change the OS	1. For one APS: Select the desired server and choose **More** > **Image** > **Switch Operating System** in the **Operation** column. The page for changing the OS is displayed. 2. For multiple APSs: Select the desired APSs and choose **More** > **Image** > **Switch Operating System** above the list. 3. Click ⌄ on the right of **Server Group Image** and select an OS and image as required. 4. Determine whether to select **Automatically upgrade protocol components**. **NOTE** After this option is selected, if the version of the component in your image is too early, the component will be upgraded, which may prolong the time needed for completing the operation. 5. Enter **rebuild** in the text box as prompted. 6. Click **OK**. **NOTE** 1. Changing the OS will clear the system disk data. Back up the data in advance. 2. This operation is applicable only to images of the same type, such as paid images with the same source and price, and free images. 3. If the image types are different, you are advised to purchase a new server.	If a server malfunctions and cannot be restored, you can change the OS.

Operation	Procedure	Description
Reinstall the OS	1. For one APS: Select the desired server and choose **More** > **Image** > **Reinstall Operating System** in the **Operation** column. The page for reinstalling the OS is displayed. 2. For multiple APSs: Select the desired APSs and choose **More** > **Image** > **Reinstall Operating System** above the list. 3. Determine whether to select **Automatically upgrade protocol components**. **NOTE** After this option is selected, if the version of the component in your image is too early, the component will be upgraded, which may prolong the time needed for completing the operation. 4. Enter **rebuild** in the text box as prompted. 5. Click **OK**. **NOTE** Reinstalling the OS will clear the system disk data. Back up the data in advance.	If a server malfunctions and cannot be restored, you can rebuild the image.

----End

2.7 Application Groups

2.7.1 Managing Application Groups

2.7.1.1 Creating an Application Group

Scenarios

After deploying an application on a server, you need to create an application group associated with the server on the console to manage the application used by users.

Prerequisites

You have created an APS.

Procedure

Step 1 Log in to the Workspace Application Streaming **console** as an administrator.

Step 2 In the navigation pane, choose **Application Groups**. The **Application Groups** is displayed.

Step 3 In the upper right corner of the page, click **Create Application Group**.

Step 4 Configure the parameters based on **Table 2-8**.

Table 2-8 Application group parameters

Parameter	Description	Example Value
Name	User-defined application group name. Naming rules: • The name can contain 1 to 64 characters. • The name can contain uppercase letters, lowercase letters, digits, hyphens (-), and underscores (_).	App_Gp-Win2016
App Group Type	• **Application**: An application is a single application. Users can access the application without installing it. • **Desktop**: A desktop application group is a complete virtual desktop. Users access the remote desktop.	-
Associated Server Group	Select the server group created in **2.6.1.1 Creating a Server Group**.	-
Description	Describe the characteristics of the application group to facilitate maintenance.	-

Step 5 Click **OK**.

----End

2.7.1.2 Modifying an Application Group

Scenarios

An enterprise administrator can modify an application group on the console.

Procedure

Step 1 Log in to the Workspace Application Streaming **console** as an administrator.

Step 2 In the navigation pane, choose **Application Groups**. The **Application Groups** is displayed.

Step 3 Locate the row that contains the target application group and click **Edit** in the **Operation** column. The **Modify Application Group** page is displayed.

Step 4 Modify the **Name**, **Associate Server Group**, and **Description** as required.

NOTE

- Click **Create Server Group**.
- If the image type of an added application conflicts with that of the new server group or the new server group does not exist, the application is unavailable.

Step 5 Click **OK**.

----End

2.7.1.3 Deleting an Application Group

Scenarios

If all applications have been deleted from an application group, enterprise administrators can directly delete the application group.

Prerequisites

All applications in the application group have been deleted.

Procedure

Step 1 Log in to the Workspace Application Streaming **console** as an administrator.

Step 2 In the navigation pane, choose **Application Groups**. The **Application Groups** is displayed.

Step 3 Select the application group to be deleted.

- To delete an application group, perform steps **Step 4** and **Step 5**.
- To delete application groups in batches, perform steps **Step 6** and **Step 7**.

Step 4 Locate the row that contains the target application group and click **Delete** in the **Operation** column. The **Delete Application Group** dialog box is displayed.

Step 5 Select **Confirm** and click **OK**.

Step 6 Select the target application groups and click **Delete** in the upper left corner. The **Delete** dialog box is displayed.

Step 7 Select **Confirm** and click **OK**.

----End

2.7.2 Managing Applications

2.7.2.1 Managing Applications

2.7.2.1.1 Adding Applications

Scenarios

After deploying an application on a server, the administrator needs to create an application group associated with the server on the console, add the application to be used by users to the application group, and authorize users to use the application.

Prerequisites

An application group has been created and associated with a server group.

Procedure

Step 1 Log in to the Workspace Application Streaming **console** as an administrator.

Step 2 In the navigation pane, choose **Application Groups**. The **Application Groups** is displayed.

Step 3 Click an application group name. The **Applications** page is displayed.

Step 4 Click **Add App**. The **Publish Application** page is displayed.

- If **App Source** is set to **Private**, perform steps **Step 5** to **Step 6**.
- If **App Source** is set to **Custom**, perform steps **Step 7** to **Step 8**.

Step 5 Select applications to be published from the application list.

NOTE

Applications with the same name cannot be added to the same application group.

Step 6 Click **OK**.

Step 7 See the following table for adding a custom application.

Table 2-9 Application configuration parameters

Parameter	Description	Example Value
Application Name	• The application name can contain visible characters or spaces but cannot contain only spaces. • The name can contain 1 to 64 characters.	-

Parameter	Description	Example Value
Running in Sandbox Mode	Sandbox application scenarios: • Software that cannot be opened in multiple remote sessions at the same time can be opened in the sandbox. Sandbox usage restrictions: • The sandbox data is stored in the sandbox. If the sandbox is deleted, everything will be cleared. • If the file is too large, it cannot be copied to the sandbox for editing. It can only be read-only. **NOTE** Ensure that the application sandbox software has been installed on the associated server group instance. Otherwise, the application cannot be started.	Selected
Sandbox Application Path	Installation location of the sandbox application file.	For example, **Sandboxie software: C:\Program Files\Sandboxie \Start.exe\Start.exe**
Version	You can set this parameter based on the actual situation. If the application is running in sandbox mode, add the sandbox application version.	-
Publisher	You can set this parameter based on the actual situation. If the application is running in sandbox mode, add the sandbox application publisher.	-

Parameter	Description	Example Value
Working Directory	• Installation directory of the running file in non-sandbox mode, for example, **C:\Program Files \Internet Explorer** • Installation directory of sandbox application files, for example, **Sandboxie software: C:\Program Files\Sandboxie** The working directory involves reading the configuration file and searching for the dependent library path.	-
Command Parameter	• Command line format for common applications: Add command lines as required. • Format: *Command* + Space + *Path of the app started in sandbox mode*. Example: **/box:DefaultBox "C:\Program Files \Internet Explorer \iexplore.exe"** **NOTE** The path of the app to be started in sandbox mode must be enclosed in double quotation marks ("").	-
Description	Enter the required information.	-

Step 8 Click **OK**.

----End

2.7.2.1.2 Modifying an Application

Scenarios

Enterprise administrators can modify application parameters to better maintain applications.

Prerequisites

An application has been published.

Modifying an Application

Step 1 Log in to the Workspace Application Streaming **console** as an administrator.

Step 2 In the navigation pane, choose **Application Groups**. The **Application Groups** is displayed.

Step 3 Click an application group name. The **Applications** page is displayed.

Step 4 Locate the row that contains the target application and click **Modify** in the **Operation** column. The **Modify Application** page is displayed.

Step 5 Modify the **Application Name**, **Running in Sandbox Mode**, **Path**, **Version**, **Publisher**, **Working Directory**, **Command Parameter**, and **Description** as required.

Step 6 Click **OK**.

----End

2.7.2.1.3 Deleting an Application

Scenarios

- If a published application is idle and will not be used anymore, or needs to be updated, you can delete the application. After the application is deleted, you can uninstall the application from the server to reduce resource consumption on the server.

  Before deleting an application, ensure that the application is idle. In addition, it is recommended that enterprise administrators send a deletion notification to end users.
- This section describes how to delete application authorization when a user does not need to use the application anymore.

Prerequisites

An application has been published.

Deleting an Application

Step 1 Log in to the Workspace Application Streaming **console** as an administrator.

Step 2 In the navigation pane, choose **Application Groups**. The **Application Groups** is displayed.

Step 3 Click the name of the application group to which the application to be deleted belongs. The **Applications** page is displayed.

Step 4 You can choose to delete an application or delete applications in batches.

- To delete an application, perform steps **Step 5** to **Step 6**.
- To delete applications in batches, perform steps **Step 7** to **Step 8**.

Step 5 Locate the row that contains the target application and click **More** > **Delete** in the **Operation** column. The **Delete** dialog box is displayed.

Step 6 Click **OK**.

Step 7 Select the applications to be deleted in batches and click **Delete** in the upper left corner of the **Applications** page. The **Batch Delete App(s)** dialog box is displayed.

Step 8 Select **Confirm** and click **Yes**.

----End

2.7.2.1.4 Modifying an Application Icon

Scenarios

If the icon of a published application is inconsistent with that of the actual application, you can modify the icon on the management console.

Prerequisites

An application has been published.

Procedure

Step 1 Log in to the Workspace Application Streaming **console** as an administrator.

Step 2 In the navigation pane, choose **Application Groups**. The **Application Groups** is displayed.

Step 3 Click an application group name. The **Applications** page is displayed.

Step 4 Locate the application whose icon needs to be modified and click **Modify Icon** in the **Operation** column. The **Modify Icon** page is displayed.

Step 5 Click  to delete the existing icon.

Step 6 Click  , select the required icon on your local PC, and click **Open**.

Step 7 After the icon image is uploaded successfully, close the **Modify Icon** dialog box.

----End

2.7.2.1.5 Disabling or Enabling an Application

Scenarios

A published application has been replaced by a new application, or the application needs to be stopped temporarily in certain cases. In this case, you can disable a

single enabled application. After an application is disabled, the application cannot be viewed on the terminal user side.

If you want to use a disabled application, you can enable it again.

Enabling or disabling an application allows you to flexibly use resources on the server and help administrators better manage and maintain applications.

Prerequisites

An application has been published.

Procedure

Step 1 Log in to the Workspace Application Streaming **console** as an administrator.

Step 2 In the navigation pane, choose **Application Groups**. The **Application Groups** is displayed.

Step 3 Click the name of the application group whose applications are to be disabled or enabled. The **Applications** page is displayed.

Step 4 Select applications and perform the following operation as required:

- Select **Disable** to disable the selected applications.
  - Locate the row that contains the target application and click **More** > **Disable** in the **Operation** column. In the displayed **Disable** dialog box, click **OK**.
  - Select the applications to be disabled in batches and click **Disable** in the upper left corner. In the displayed **Batch Disable App(s)** dialog box, select **Confirm** and click **Yes**.
- Select **Enable** to enable the selected applications.
  - In the **Operation** column of the disabled application, click **More** > **Enable**. In the displayed **Enable** dialog box, click **OK**.
  - Select the applications to be enabled in batches and click **Enable** in the upper left corner. In the displayed **Batch Enable App(s)** dialog box, select **Confirm** and click **Yes**.

----End

2.7.2.2 Managing Authorizations

2.7.2.2.1 Authorizing Users or User Groups

Scenarios

The enterprise administrator can authorize a specific user to use an application.

Prerequisites

An application has been published.

Procedure

Step 1 Log in to the Workspace Application Streaming **console** as an administrator.

Step 2 In the navigation pane, choose **Application Groups**. The **Application Groups** is displayed.

Step 3 Click an application group name. The **Applications** page is displayed.

Step 4 Click **User Authorization**. The user list page is displayed.

Step 5 Click **Add User**. The list of users to be added is displayed.

Step 6 Select the users or user groups that you want to use the application and click **OK**.

Users will receive a notification email or message from the Workspace Application Streaming authorization service.

NOTE

- Users in the AD user group cannot send notifications.
- Users whose usernames contain more than 20 characters cannot access Windows applications.
- The user permission is recommended for authorized users of Workspace Application Streaming.

----End

2.7.2.2.2 Canceling User or User Group Authorization

Scenarios

Enterprise administrators can cancel the authorization of a user or user group to use an application.

Prerequisites

The application has been authorized to a user or user group.

Procedure

Step 1 Log in to the Workspace Application Streaming **console** as an administrator.

Step 2 In the navigation pane, choose **Application Groups**. The **Application Groups** is displayed.

Step 3 Click an application group name. The **Applications** page is displayed.

Step 4 Click **User Authorization**. The user list page is displayed.

Step 5 Select the user or user group whose authorization is to be canceled.

- To delete a user or user group, perform steps **Step 6** to **Step 7**.
- To delete users or user groups in batches, perform steps **Step 8** to **Step 9**.

Step 6 Click **Delete** in the **Operation** column of the user or user group to be deleted. The **Delete** dialog box is displayed.

Step 7 Click **OK**.

Step 8 Select the users or user groups to be deleted and click **Delete** in the upper left corner. The **Batch Delete User(s)** dialog box is displayed.

Step 9 Select **Confirm** and click **Yes**.

Users will receive a notification email or message from the Workspace Application Streaming canceling authorization service.

NOTE

Users in the AD user group cannot send notifications.

----End

2.7.2.2.3 Resending a Notification

Scenarios

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

Procedure

Step 1 Log in to the Workspace Application Streaming **console** as an administrator.

Step 2 In the navigation pane, choose **Application Groups**. The **Application Groups** is displayed.

Step 3 Click on the application group name of the user who needs to receive the notification again. The **Applications** page is displayed.

Step 4 Click **User Authorization**. The user list page is displayed.

Step 5 Click **Resend Notification** in the **Operation** column of the user or user group to which the notification is to be resent. The **Resend Notification** dialog box is displayed.

Step 6 Select a sending mode as prompted and click **OK**.

NOTE

- Click **Notification Failure Records** to view **Failed** and **Successful** records.
- On the **Failed** records page, you can select **Resend Notification** in the **Operation** column or **Batch Resend** in the upper left corner of the page.

----End

2.8 User Management

Scenarios

Workspace Application Streaming and Workspace share the same user list. Therefore, users added, modified, or deleted on the Workspace console are synchronized to the Workspace Application Streaming console.

Procedure

Step 1 Log in to the Workspace Application Streaming **console** as an administrator.

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

Step 3 Perform the operations listed in **Table 2-10** as required.

Table 2-10 User management operations

Operation	Procedure	Description
Users	Click **Users**, and the **User Management** page is displayed. For details, see section "User Management" in the *Administrator User Guide*.	Administrators can view users on Workspace.
User Groups	Click **User Groups**, and the **User Groups** page is displayed. For details, see section "User Groups" in the *Administrator User Guide*.	Administrators can view user groups on Workspace.
User Application Group Authorization	Click **User Application Group Authorization**. On the displayed page, locate the row that contains the target user or user group, and click **View Authorized Application Group** in the **Operation** column. On the displayed page, click an application group name to view the available applications.	Administrators can view authorized application groups to obtain the available applications for a user or user group.

----End

2.9 Policy Groups

2.9.1 Creating a Policy Group

Scenarios

A policy group is a set of security rules configured for Workspace Application Streaming, including file redirection read/write permission, clipboard read/write permission, session automatic reconnection interval, and image display. Policies are used to control data transmission between user terminals and Workspace Application Streaming.

You can plan and customize application policies to create the most efficient policy management solution for different scenarios.

Procedure

Step 1 Log in to the **Workspace Application Streaming console** as an administrator.

Step 2 In the navigation pane, click **Policy Groups**. The **Policy Groups** page is displayed.

Step 3 In the upper right corner of the page, click **Create Policy Group**. The **Create Policy Group** page is displayed.

Step 4 Configure **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**: Use the default blank template to create a policy group.
- **Create with template**: Create a policy group using an existing policy group template, with the same configurations as those of the template by default.

  NOTE

  You 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 Workspace Application Streaming policies in four different scenarios.

  - In security scenarios, Huawei Delivery Protocol (HDP) prevents data in Workspace Application Streaming from being transferred to or even stored on personal storage devices and keeps data in an on-premises data center.
  - In (GPU-dependent) gaming scenarios, cursor follow-up and image display are optimized to ensure smoothness even in poor bandwidth conditions.
  - In (GPU-dependent) 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 (GPU-dependent) 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 the existing policy group. The configurations are the same as those of the policy by default.

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

The policy configuration page is displayed.

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

NOTE

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

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

For details about configuring a general policy, see **Table 2-11**.

Table 2-11 Policy management

Type	Parameter	Description
File Redirection	Fixed driver	• **Read-only**: Files in drivers and storage devices can only be pre-viewed. • **Read/write**: Files in drivers and storage devices can be modified. Users can use drivers through file redirection in VMs on Workspace Application Streaming.
	Removable driver	
	CD/DVD-ROM driver	
	Network driver	
Clipboard Redirection	Bidirectional	After this function is enabled, end users can copy data from Workspace Application Streaming and paste the data on local desktops, or vice versa.
	Server to client	After this function is enabled, end users can only copy data on Workspace Application Streaming 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 Workspace Application Streaming. **NOTE** Files can be copied only from a Windows client to a server, and file redirection and the corresponding driver must be enabled.
Print Device Redirection	Server to client	Users can use print devices connected to TCs.
Sessions	Auto Disconnection Without Keyboard/ Mouse Device Operations	**Enabled**: If no keyboard or mouse device operation is performed on the client for a specified period of time, the client automatically disconnects from the server and the application is closed. **Disabled**: The automatic disconnection function is disabled.

Type	Parameter	Description
	Waiting Time (Min)	Sets the waiting time for automatic disconnection when no keyboard or mouse device operation is performed. Value range: 3–86,400.
	Auto Logout	If **Auto Disconnection Without Keyboard/Mouse Device Operations** is enabled, you can configure the waiting time before the session is automatically logged out of.
	Session Retention After Disconnection (Min)	If **Auto Disconnection Without Keyboard/Mouse Device Operations** is enabled, in the case of automatic disconnection, the session is automatically logged out of after the session retention period expires. Value range: 1–86,400.

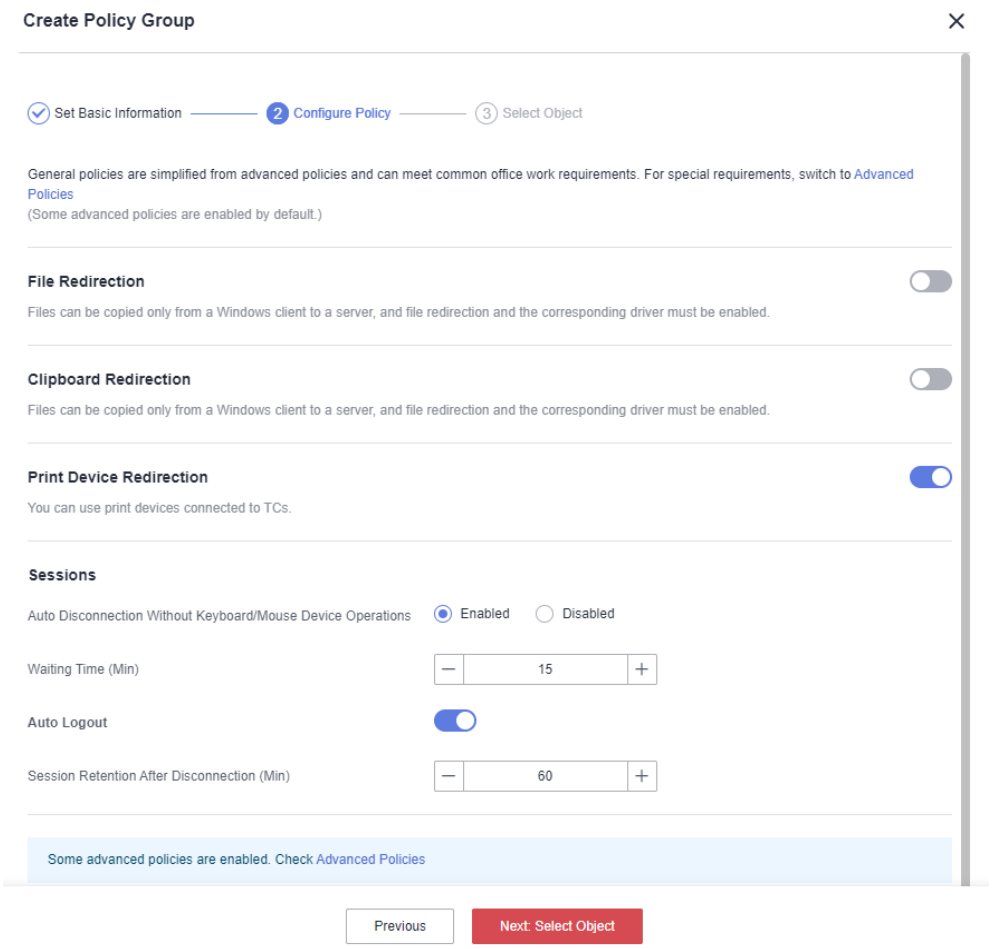
Step 8 Configure an advanced policy.

General policies are simplified from advanced policies and can meet common office work requirements. For special requirements, configure an advanced policy.

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

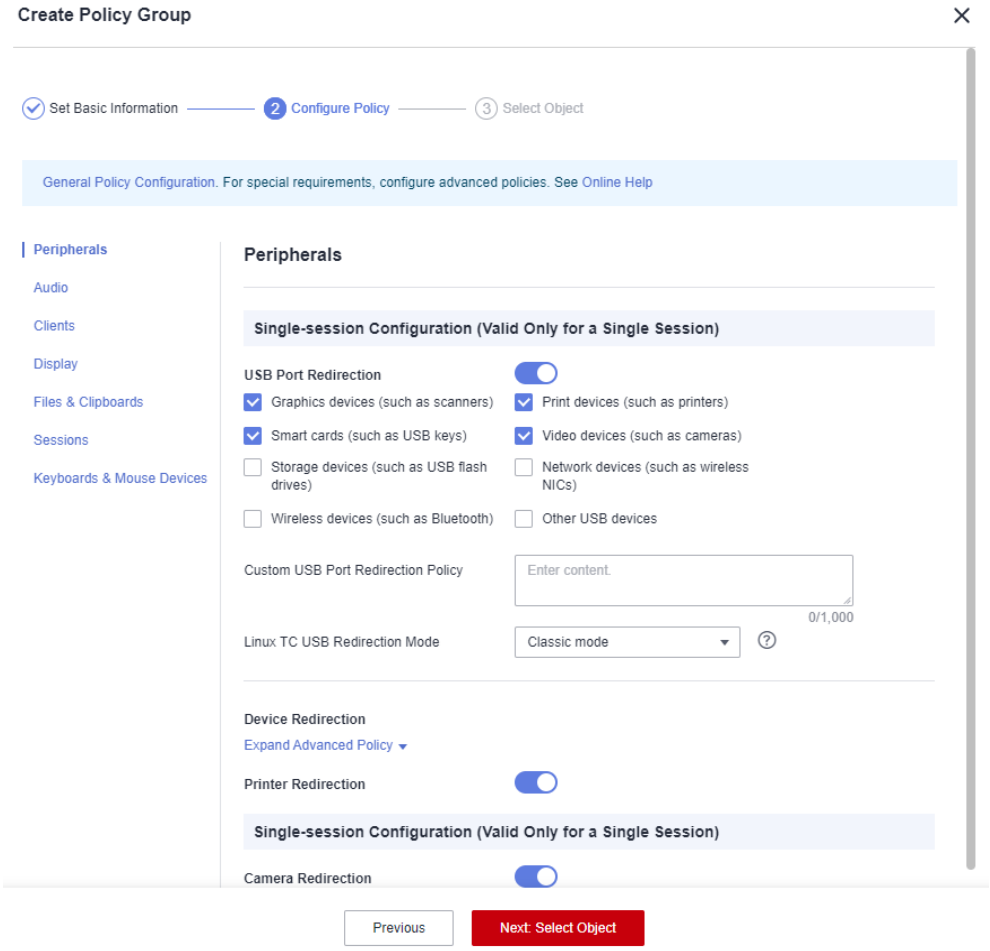
   The advanced policy configuration page is displayed.

Figure 2-5 Advanced policy configuration page



2. Configure an advanced policy, as shown in **Figure 2-6**. For details about the advanced policy parameters, see **2.9.3 Configuring an Advanced Policy**.

Figure 2-6 Configuring an advanced policy

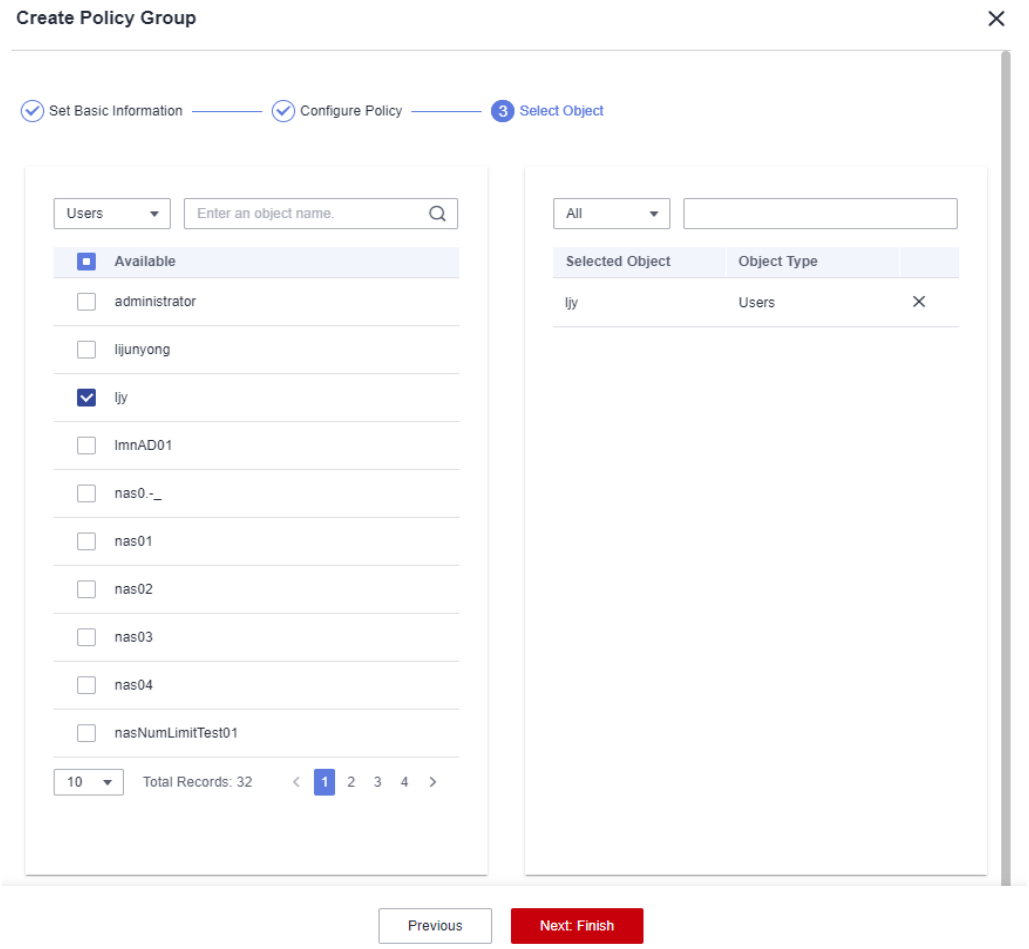


Step 9 Click **Next: Select Object**.

Select an **Object Type** as required and then select an object, as shown in **Figure 2-7**.

- **All Objects**
- **Users**
- **User Groups**
- **Application Groups**

Figure 2-7 Selecting an object



Step 10 Click **Next: Finish**.

The policy has been created. The policy takes effect upon the user's next login to the Workspace Application Streaming client.

----End

2.9.2 Modifying a Policy Group

Scenarios

You can modify the policy configuration (including the default policy group), basic information, and policy objects in an existing policy group, or delete a policy group that is no longer used.

Modifying Basic Information

NOTE

The basic information about the default policy group cannot be modified.

Step 1 Log in to the **Workspace Application Streaming console** as an administrator.

Step 2 In the navigation pane, click **Policy Groups**. The **Policy Groups** page is displayed.

Step 3 Click **Basic Info** in the **Operation** column of the policy to be modified. The **Basic Info** page is displayed.

Step 4 Modify the name, priority, and description as required.

NOTE

- The policy name can contain up to 55 characters in digits, letters, and underscores (_).
- The priority value must be less than the total number of policy groups. The priority is a basis for determining an execution sequence or an action weight of a policy by Workspace Application Streaming. The priority is represented by a positive integer. A smaller value indicates a higher priority.
- The description contains up to 255 characters.

Step 5 Click **Save**.

----End

Modifying Policy Configuration

Step 1 Log in to the **Workspace Application Streaming console** as an administrator.

Step 2 In the navigation pane, click **Policy Groups**. The **Policy Groups** page is displayed.

Step 3 Click **Policy Configuration** in the **Operation** column of the policy to be modified. The **General Policy Configuration** page is displayed.

Step 4 Enable or disable policy items as required. **Table 2-12** describes the policy items.

Table 2-12 Policy management

Type	Parameter	Description
File Redirection	Fixed driver	• **Read-only**: Files in drivers and storage devices can only be pre-viewed. • **Read/write**: Files in drivers and storage devices can be modified. Users can use drivers through file redirection in VMs on Workspace Application Streaming.
	Removable driver	
	CD/DVD-ROM driver	
	Network driver	
Clipboard Redirection	Bidirectional	After this function is enabled, end users can copy data from Workspace Application Streaming and paste the data on local desktops, or vice versa.
	Server to client	After this function is enabled, end users can only copy data on Workspace Application Streaming and paste the data on local desktops.

Type	Parameter	Description
	Client to server	After this function is enabled, end users can only copy data on local desktops and paste the data on Workspace Application Streaming. **NOTE** Files can be copied only from a Windows client to a server, and file redirection and the corresponding driver must be enabled.
Print Device Redirection	Server to client	Users can use print devices connected to TCs.
Sessions	Auto Disconnection Without Keyboard/ Mouse Device Operations	**Enabled**: If no keyboard or mouse device operation is performed on the client for a specified period of time, the client automatically disconnects from the server and the application is closed. **Disabled**: The automatic disconnection function is disabled.
	Waiting Time (Min)	Sets the waiting time for automatic disconnection when no keyboard or mouse device operation is performed. Value range: 3–86,400.
	Auto Logout	If **Auto Disconnection Without Keyboard/Mouse Device Operations** is enabled, you can configure the waiting time before the session is automatically logged out of.
	Session Retention After Disconnection (Min)	If **Auto Disconnection Without Keyboard/Mouse Device Operations** is enabled, in the case of automatic disconnection, the session is automatically logged out of after the session retention period expires. Value range: 1–86,400.

Step 5 Click **Advanced Policies** and modify advanced policy items as required.

Step 6 Click **Save**.

----End

Modifying a Policy Object

NOTE

The policy object of the default policy group cannot be modified.

Step 1 Log in to the **Workspace Application Streaming console** as an administrator.

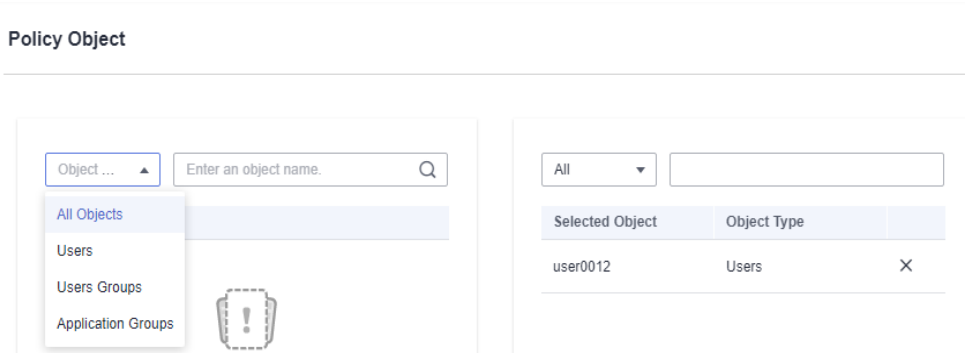
Step 2 In the navigation pane, click **Policy Groups**. The **Policy Groups** page is displayed.

Step 3 Click **Policy Object** in the **Operation** column of the policy to be modified. The **Policy Object** page is displayed.

Step 4 Modify the policy object as required.

You can add an object in the drop-down list box on the left. In the selected object list on the right, click ✕ to delete an object, as shown in **Figure 2-8**.

Figure 2-8 Modifying a policy object



NOTE

Rules for a policy to take effect:

- If a policy object is included in multiple policy groups, the object takes effect in the policy group with the highest priority.
- When an application is connected, if there is a policy group in both the application groups of user (group) and application, the object takes effect in the policy group with the highest priority.

Step 5 Click **Save**.

----End

Deleting a Policy Group

NOTE

The default policy group cannot be deleted.

Step 1 Log in to the **Workspace Application Streaming console** as an administrator.

Step 2 In the navigation pane, click **Policy Groups**. The **Policy Groups** page is displayed.

Step 3 Click **Delete** in the **Operation** column of the policy to be deleted. The page for confirming the deletion is displayed.

Step 4 Click **OK**.

----End

2.9.3 Configuring an Advanced Policy

Scenarios

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

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

NOTE

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

- Peripherals
- Audio
- Clients
- Display
- Files & Clipboards
- Sessions
- Keyboards & Mouse Devices

Peripherals

Configure peripheral application policies, as shown in **Table 2-13**.

Table 2-13 Peripheral policies

Type	Parameter	Description	Example Value
USB port redirection (valid only for a single session)	USB Port Redirection	•  : End users can use USB devices connected to terminals by using USB port redirection. •  : End users cannot use USB devices connected to terminals by using USB port redirection. • Default value: 	

Type	Parameter	Description	Example Value
	Graphics devices (such as scanners)	• ☑: End users can use USB graphics devices connected to terminals through USB port redirection. • ☐: End users cannot use USB graphics devices connected to terminals through USB port redirection. • Default value: ☑	☑
	Print devices (such as printers)	• ☑: End users can use USB print devices connected to terminals through USB port redirection. • ☐: End users cannot use USB print devices connected to terminals through USB port redirection. • Default value: ☑	☑
	Smart cards (such as USB keys)	• ☑: 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 devices (such as cameras)	• ☑: End users can use USB video devices connected to terminals through USB port redirection. • ☐: End users cannot use USB video devices connected to terminals through USB port redirection. • Default value: ☑	☑

Type	Parameter	Description	Example Value
	Storage devices (such as USB flash drives)	• ☑: End users can use USB storage devices connected to terminals through USB port redirection. • ☐: End users cannot use USB storage devices connected to terminals through USB port redirection. • Default value: ☐	☐
	Network devices (such as wireless NICs)	• ☑: End users can use network devices on a computer through USB port redirection. • ☐: End users cannot use network devices on a computer through USB port redirection. • Default value: ☐	☐
	Wireless devices (such as Bluetooth)	• ☑: End users can use wireless devices on a computer through USB port redirection. • ☐: End users cannot use wireless devices on a computer through USB port redirection. • Default value: ☐	☐

Type	Parameter	Description	Example Value
	Other USB devices	• ☑: End users can use other USB devices (excluding graphics devices, video devices, printers, storage devices, and smart cards) connected to terminals through USB port redirection. • ☐: End users cannot use other USB devices (excluding graphics devices, video devices, printers, storage devices, and smart cards) connected to terminals through USB port redirection. • Default value: ☐	☐
	Custom USB Port Redirection Policy	Users can customize USB policies. • The policy configuration format is ID:90C:937B:1:0|CLASS:00:00:00:08:06:50:1:0|USBKEY:14E:201|SPECIAL:47E:471|ADV:78e:79f:1:1:1:1. • The value contains up to 1000 characters and cannot contain spaces, double quotation marks (""), and the following characters: !@#$%^&*()>/?	ID:90C:937B:1:0|CLASS:00:00:00:08:06:50:1:0|USBKEY:14E:201|SPECIAL:47E:471|ADV:78e:79f:1:1:1:1

Type	Parameter	Description	Example Value
	Linux TC USB Redirection Mode	• This option is used to set the USB redirection mode only for Linux TCs. • When a Huawei Linux TC is used and a USB device is not compatible with the classic mode (recommended for Linux TCs), you can try the general mode. The Linux TC model supported by Huawei is HT3300. • **General mode**: The client USB driver is implemented using a user mode driver. Set it to **General mode** for non-Huawei Linux TCs.	Classic mode
Printer redirection	Printer Redirection	•  : End users can use printers connected to TCs through printer redirection. •  : End users cannot use printers connected to TCs through printer redirection. • Default value:  **NOTICE** The printer driver must be installed on both TCs and computers.	
	Synchronize with the 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**, **Universal Printing PS** is loaded for printer redirection on a Linux client and **HDP XPSDrv Driver** is loaded for printer redirection on a Windows client. **NOTICE** To simplify the printer service, ensure that all users use SCs and TCs running the same OS to log in to Workspace Application Streaming. For example, all TCs run Windows OS.	Default
Session printer	Session Printer	•  : 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
	Custom Session Printer 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 255 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 (valid only for a single session)	Camera Redirection	• : 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. • Set **USB Port Redirection** to and select **Video Device (Such as Cameras)**.	
	Camera Frame Rate (FPS)	The value ranges from 1 to 30.	15
	Camera Max Width (Pixel)	The value ranges from 1 to 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 device redirection (valid only for a single session)	TWAIN Redirection	•  : 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)

Audio

Configure audio policies, as shown in **Table 2-14**.

Table 2-14 Audio policies

Type	Parameter	Description	Example
Audio redirection	Audio Redirection	Applications on the Workspace Application Streaming client can use audio devices on terminals to record and play audio.	

Type	Parameter	Description	Example
Playback redirection	Playback Redirection	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 audio. •  : Playback redirection is disabled so that end users cannot play audio.	
	Playback Scenario	• **Lossless**: The voice quality is the best, 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. • **Auto identification**: The user's behavior, such as voice call or music playback, can be identified. The accuracy rate exceeds 90%. The system automatically switches to a better algorithm based on user behavior.	Music playback
Recording redirection	Recording Redirection	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
	Recording Scenario	• **Lossless**: The voice quality is the best, 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. • **Auto identification**: This option is reserved and is equivalent to **Voice call**.	Voice call

Clients

Configure client policies, as shown in **Table 2-15**.

Table 2-15 Client policies

Parameter	Description	Example
Automatic Reconnection Interval (s)	Specifies the interval at which the Workspace Application Streaming client attempts to connect to the server after the client is disconnected abnormally. The value ranges from 1 to 50.	5
Session Persistence Time (s)	Specifies the longest duration allowed for automatic reconnection attempts after the Workspace Application Streaming client is disconnected abnormally. The value ranges from 0 to 180.	180

Parameter	Description	Example
Anti-Screenshot Policy	After the policy is enabled, users are prevented from taking screenshots on the Workspace Application Streaming client for local storage and sharing. •  : The policy is enabled. •  : The policy is disabled. **NOTE** This function only applies to Windows clients and Linux TCs. After this function is enabled, other terminals cannot access the system.	

Display

Configure display policies, as shown in **Table 2-16**.

Table 2-16 Display policies

Type	Parameter	Description	Example
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 the optimal video playback.	Level 4 (Recommended)

Type	Parameter	Description	Example
	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.	-
	Bandwidth (Kbit/s)	Limits the peak bandwidth of a user. The value ranges from 256 to 25,000.	20,000
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 this 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 without compression. This level consumes the fewest CPU resources but the most bandwidth resources.	Level 0

Type	Parameter	Description	Example
	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 in office scenarios is enabled. •  : Color enhancement in office scenarios is disabled.	
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 the **Bandwidth** mode improves display quality. The value ranges from 256 to 100,000.	18,000
	Peak Video Bitrate (Kbit/s)	Video compression algorithm parameter. Increasing this value improves display quality. The value ranges from 256 to 100,000.	18,000
	Average Video Quality	Average quality coefficient of video. In the **Quality** mode, increasing this value compromises display quality. The value ranges from 5 to 59.	15
	Lowest Video Quality	Lower limit of video quality. In the **Quality** mode, increasing this value compromises display quality. The value ranges from 5 to 69.	25
	Highest Video Quality	Upper limit of video quality. In the **Quality** mode, increasing this value compromises display quality. The value ranges from 1 to 59.	7

Type	Parameter	Description	Example
	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
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.	
	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.	
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.	

Type	Parameter	Description	Example
	Driver Delegation Latency (*30 ms)	The value ranges from 1 to 100.	80
	Video Delegation Latency (*30 ms)	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 resolution in system settings on the Workspace Application Streaming client. •  : After the computer resolution change policy is disabled, end users cannot change the resolution in system settings on the Workspace Application Streaming client.	

Files & Clipboards

Configure file & clipboard policies, as shown in **Table 2-17**.

Table 2-17 File & clipboard policies

Type	Parameter	Description	Example
Bidirectional redirection	Bidirectional Redirection	• When Workspace Application Streaming is used on Workspace desktops, file redirection and clipboard redirection (bidirectional) are enabled by default. In this way, data can be copied between Workspace desktops and Workspace Application Streaming on the cloud. • When Workspace Application Streaming is used on TCs or local desktops, file and clipboard data copy is controlled based on file redirection and clipboard redirection.	

Type	Parameter	Description	Example
File redirection	File Redirection	• **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 Workspace Application Streaming through file redirection.	Read-only
	Fixed driver	• ☑: Users can use fixed drivers, such as local disks, on Workspace Application Streaming in the file redirection mode. • ☐: Users cannot use fixed drivers, such as local disks, on Workspace Application Streaming in the file redirection mode. **NOTE** When file redirection is disabled, this function is disabled.	☐
	Removable driver	• ☑: Users can use removable drivers, such as USB flash drives, on Workspace Application Streaming in the file redirection mode. • ☐: Users cannot use removable drivers, such as USB flash drives, on Workspace Application Streaming in the file redirection mode. **NOTE** When file redirection is disabled, this function is disabled.	☐

Type	Parameter	Description	Example
	CD/DVD-ROM driver	• ☑: Users can use CD/DVD-ROM drivers on Workspace Application Streaming in the file redirection mode. • ☐: Users cannot use CD/DVD-ROM drivers on Workspace Application Streaming in the file redirection mode.	☐
	Network driver	• ☑: Users can use network drivers on Workspace Application Streaming in the file redirection mode. • ☐: Users cannot use network drivers on Workspace Application Streaming in the file redirection mode.	☐
	Send File From VM to Client	•  : This function is enabled. •  : This function is disabled.	
	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

Type	Parameter	Description	Example
	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
	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
	Linux Root Directory Mounting	•  : Root directory mounting is enabled on Linux. •  : Root directory mounting is disabled on Linux.	

Type	Parameter	Description	Example
	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
	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)	The value ranges from 0 to 2,147,483,647.	0
	Mobile Client Redirection	•  : Mobile client redirection is enabled. •  : Mobile client redirection is disabled.	

Type	Parameter	Description	Example
Clipboard redirection	Clipboard Redirection	• **Bidirectional**: After this function is enabled, end users can copy data from the Workspace Application Streaming client and paste the data on local desktops, or vice versa. • **Server to client**: After this function is enabled, end users can only copy data on the Workspace Application Streaming client 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 the Workspace Application Streaming client. • **Plain Text Length Limit** – **Allow server-to-client copy**: 1 to 4,096 characters – **Allow client-to-server copy**: 1 to 4,096 characters **NOTE** • Rich text copy and file copy are supported only when both the client (TC/SC) OS and cloud application OS are Windows. A maximum of 500 files can be copied at a time. • If the OS of a client (TC/SC or mobile client) is not Windows, only text can be copied.	Bidirectional

Type	Parameter	Description	Example
	Clipboard Rich Text Redirection	• **Bidirectional**: After this function is enabled, end users can copy rich text from the Workspace Application Streaming client and paste the rich text on local desktops, or vice versa. • **Server to client**: After this function is enabled, end users can only copy rich text on the Workspace Application Streaming client and paste the rich text on local desktops. • **Client to server**: After this function is enabled, end users can only copy rich text on local desktops and paste the rich text on the Workspace Application Streaming client.	Bidirectional
	Clipboard File Redirection	• **Bidirectional**: After this function is enabled, end users can copy files from the Workspace Application Streaming client and paste the files on local desktops, or vice versa. • **Server to client**: After this function is enabled, end users can only copy files on the Workspace Application Streaming client and paste the files on local desktops. • **Client to server**: After this function is enabled, end users can only copy files on local desktops and paste the files on the Workspace Application Streaming client.	Bidirectional

Sessions

Configure session policies, as shown in **Table 2-18**.

Table 2-18 Session policies

Parameter	Description	Recommended Value
Auto Disconnection Without Keyboard/ Mouse Device Operations	**Enabled**: If no keyboard or mouse device operation is performed on the client for a specified period of time, the client automatically disconnects from the server and the application is closed. **Disabled**: The automatic disconnection function is disabled.	Enabled
Waiting Time (Min)	Sets the waiting time for automatic disconnection when no keyboard or mouse device operation is performed. Value range: 3–86,400.	15
Auto Logout	If **Auto Disconnection Without Keyboard/Mouse Device Operations** is enabled, you can configure the waiting time before the session is automatically logged out of.	Enabled
Session Retention After Disconnection (Min)	If **Auto Disconnection Without Keyboard/Mouse Device Operations** is enabled, in the case of automatic disconnection, the session is automatically logged out of after the session retention period expires. Value range: 1–86,400.	480

Keyboards & Mouse Devices

Configure keyboard & mouse device policies, as shown in **Table 2-19**.

Table 2-19 Keyboard & mouse device policies

Parameter	Description	Recommended Value
Computer Mouse Device Feedback	• **Adaptive** • **Forcible** • **Disabled**	Adaptive
Computer Mouse Device Simulation Mode	• **Absolute positioning** • **Relative positioning**	Absolute positioning
Computer external cursor feedback	• ☑: Computer external cursor feedback is enabled. • ☐: Computer external cursor feedback is disabled.	☐

2.10 Monitoring Analysis

2.10.1 Application Records

Scenarios

The administrator can view application usage records of end users, including the application name, login time, and connection status. In addition, the administrator can view the login records of users for security audit.

Procedure

Step 1 Log in to the Workspace Application Streaming **console** as an administrator.

Step 2 In the navigation pane, choose **Monitoring Analysis** > **Application Records**. The **Application Records** page is displayed.

Step 3 Perform the operations listed in **Table 2-20** as required.

Table 2-20 Application record operations

Operation	Procedure	Description
Viewing application usage records	On the **Application Usage** tab page, view related information. Search for applications by login time, application name, login user, client name, APS name, APS IP address, APS HDA version, and virtual IP address.	To check the usage of applications, the administrator can view the usage records of applications on the console.
Viewing user login records	On the **User Login** tab page, view user login information. Search for applications by usage time, login user, client name, APS name, APS HDA version, and virtual IP address.	To check the application usage of a user, the administrator can view the login records of the user on the console.

----End

2.10.2 Sessions

Scenarios

Through session management, the administrator can view the session records of a terminal user, including the username, server name/IP address, server group name/ID, session type, and session status. The administrator can also log out of user sessions.

Procedure

Viewing sessions

Step 1 Log in to the Workspace Application Streaming **console** as an administrator.

Step 2 In the navigation pane on the left, choose **Monitoring Analysis** > **Session Management**. The **Session Management** page is displayed.

Step 3 On the page displayed, search for sessions by start time, server group, session status, server IP address, and username. You can view the following information of a session: username, server name/IP address, server group name/ID, session type, applications in use, session status, start time, end time, connection failure status code, connection failure cause, client name, client IP address, client MAC address, client version, client system, and APS HDA version.

Logging out of a session

Step 4 You can log out of the session record on the session management page.

- For one session record, perform **Step 5**.
- For more than one session record, perform **Step 6**.

Step 5 Click **Log Out** in the **Operation** column of the desired session. The logout dialog box is displayed.

- **Notification**
  - **Disable**: No notification is sent when a session is logged out of.
  - **Enable**: Set the notification title and content. After the setting is complete, a dialog box will be displayed to notify the user before the session is logged out of.
- **Execution**
  - **Now**: The session is logged out of immediately after you click **OK**.
  - **In 1 minute**: The session is logged out of one minute after you click **OK**.
  - **In 5 minutes**: The session is logged out of five minutes after you click **OK**.
  - **In 10 minutes**: The session is logged out of 10 minutes after you click **OK**.
  - **In 15 minutes**: The session is logged out of 15 minutes after you click **OK**.

Step 6 Batch select the sessions to be logged out of and click **Logout** above the list. The logout dialog box is displayed.

- **Notification**
  - **Disable**: No notification is sent when a session is logged out of.
  - **Enable**: Set the notification title and content. After the setting is complete, a dialog box will be displayed to notify the user before the session is logged out of.
- **Execution**
  - **Now**: The sessions are logged out of immediately after you click **OK**.
  - **In 1 minute**: The sessions are logged out of one minute after you click **OK**.

- **In 5 minutes**: The sessions are logged out of five minutes after you click **OK**.
- **In 10 minutes**: The sessions are logged out of 10 minutes after you click **OK**.
- **In 15 minutes**: The sessions are logged out of 15 minutes after you click **OK**.

Step 7 Click **OK**.

----End

2.11 OU Management

Scenarios

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

After maintaining OUs on the AD server, the administrator needs to synchronize OU information on the Workspace Application Streaming console.

If the same project is used by Workspace Application Streaming and Workspace, they share the same OU list. Therefore, OU information modified on the Windows AD server needs to be synchronized to the console of Workspace Application Streaming or Workspace. OUs added on the Workspace Application Streaming console are synchronized to the Workspace console and vice versa.

Prerequisites

- A Windows AD domain has been configured.
- An OU has been created on the AD server.

Procedure

Step 1 Log in to the Workspace Application Streaming **console** as an administrator.

Step 2 In the navigation pane, click **OUs**.

Step 3 Perform the operations listed in **Table 2-21** as required.

Table 2-21 OU management operations

Operation	Procedure	Description
Create an OU	1. Click **Create OU**. 2. Enter the OU name on the AD server, and select a configured domain name. Enter the description (optional). 3. Click **OK**.	After the administrator adds an OU on the AD server, the OU information needs to be synchronized to the Workspace Application Streaming console.

Operation	Procedure	Description
Modify OU information	1. Locate the row that contains the OU to be modified, and click **Modify**. 2. Change the OU name based on the OU information on the AD server. Enter the description (optional). 3. Click **OK**.	After the administrator updates the OU information on the AD server, the OU information needs to be synchronized to the Workspace Application Streaming console.
Delete an OU	1. Locate the row that contains the OU to be deleted, and click **Delete**. 2. Click **OK**.	After the administrator deletes an OU on the AD server, the OU information needs to be deleted from the Workspace Application Streaming console.

----End

2.12 Application Internet Access Management

2.12.1 Enabling Internet Access

Scenarios

The administrator can configure a **NAT gateway** and an **EIP** for each subnet as required. After they are enabled, all cloud applications in the subnet can access the Internet.

Prerequisites

You have purchased Workspace Application Streaming.

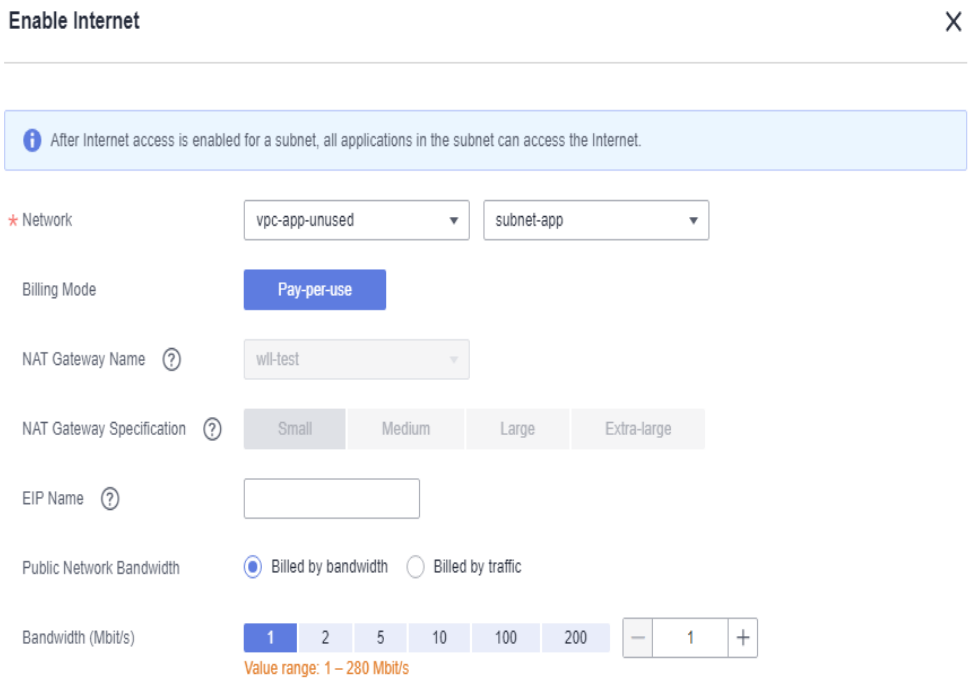
Procedure

Step 1 Log in to the Workspace Application Streaming **console** as an administrator.

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

Step 3 Click **Enable Internet**. The Internet configuration page is displayed, as shown in **Figure 2-9**.

Figure 2-9 Enabling the Internet



Step 4 Configure network parameters by referring to **Table 2-22**. Retain the default values for parameters not listed.

Table 2-22 Internet parameters

Parameter	Description	Example Value
Network	Virtual subnet where the application to be enabled with the Internet access is.	-
Billing Mode	The billing mode of Internet resources that can be purchased are **Pay-Per-Use**.	Pay-Per-Use
NAT Gateway Name	Name of the public NAT gateway. • 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, including letters, digits, underscores (_), and hyphens (-).	NATNetname-workspace_subnet01

Parameter	Description	Example Value
NAT Gateway Specification	Specifications of the public NAT gateway. • If an existing NAT gateway is used, you do not need to configure this parameter. • To create an NAT gateway, you need to configure the NAT gateway specifications. There are four specifications of NAT gateways: small, medium, large, and extra-large. You can click **Learn more** on the page to view details about each specification.	Small
EIP Name	The name of the elastic IP. Only letters, digits, hyphens (-), and underscores (_) are allowed.	EIP-workspace_subnet01
Public Network Bandwidth	Select the bandwidth billing mode based on the service scenario. • **Billed by bandwidth**: You specify a bandwidth limit and pay for the amount of time you use the bandwidth. This works well for workloads with heavy or stable traffic. • **Billed by traffic**: You specify a maximum bandwidth and pay for the outbound traffic you use. This suits workloads with low but fluctuating traffic.	Billed by traffic
Bandwidth (Mbit/s)	Select a bandwidth size. • If you select **Billed 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 **Billed by traffic**, the bandwidth ranges from 5 Mbit/s to 200 Mbit/s by default. You can customize the bandwidth as prompted.	99

Step 5 Click **OK**.

After configuring the parameters, you can view the Internet information configured for the corresponding service subnet in the list of application Internet access.

NOTE

If the current tenant VPC has multiple service subnets and cloud applications in each service subnet need to access the Internet, enable the Internet for each service subnet by referring to **Step 3** to **Step 5**.

----End

2.12.2 Disable Internet Access

Scenarios

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

Prerequisites

The Internet access function has been enabled for cloud applications.

Procedure

Step 1 Log in to the **management console** of Workspace Application Streaming as an administrator.

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

The **Application Internet Access Management** page is displayed.

Step 3 Click **Disable Internet** in the **Operation** column.

The **Disable Internet** page is displayed.

Step 4 Perform the following operations to disable Internet access:

- Click **Go to Cancel** to cancel the SNAT rule.
- Click **Go to Unsubscribe** in the **Unsubscribing from EIP** area.
- Click **Go to Unsubscribe** in the **Unsubscribing from NAT** area.

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 as required. Otherwise, fees will be generated.

----End

2.13 Upgrading Protocol Components

Scenarios

When a new AccessAgent version is available, the administrator can upgrade the AccessAgent of the corresponding server on the Workspace Application Streaming console. After the upgrade command is delivered, the administrator can view the AccessAgent upgrade status of each server.

Prerequisites

- The server is in the **Ready** state.
- The latest AccessAgent version is available on the protocol component upgrade page.

Procedure

Step 1 Log in to the **management console** of Workspace Application Streaming as an administrator.

Step 2 In the navigation tree on the left, click **Protocol Component Upgrade**.

Step 3 Locate the row that contains the server to be upgraded and click **AccessAgent Upgrade** in the **Operation** column. Alternatively, select multiple servers to be upgraded and click **Batch Update**.

Step 4 On the upgrade confirmation page, click **OK**.

Step 5 Switch to the **AccessAgent Upgrade Tracing** page to view the upgrade details.

Step 6 After the server upgrade status changes to **upgrade success**, switch back to the **AccessAgent Upgrade** page. Select the server and click **Batch Cancel Maintenance**.

Step 7 On the page for canceling maintenance, click **OK**.

----End

2.14 Scheduled Tasks

2.14.1 Creating a Scheduled Task

Scenarios

This section describes how to start, shut down, restart an APS and recompose system disks periodically.

Impact on the System

After an APS is shut down, unsaved personal data may be lost.

Prerequisites

An APS has been created.

Procedure

Step 1 Log in to the **management console** of Workspace Application Streaming as an administrator.

Step 2 On the console page, click **Scheduled Tasks**.

The **Scheduled Tasks** page is displayed.

Step 3 Click **Create Task** in the upper right corner of the page.

The **Create Scheduled Task** page is displayed.

Step 4 Configure a scheduled task.

- **Task type**:
  - **Shut down**

    NOTE

    After a scheduled shutdown task is set, the system does not execute the task if there are users accessing the server at the scheduled time. Instead, the system automatically postpones the task to the next scheduled time to ensure user experience.

    If the forcible shutdown option is selected, the system forcibly shuts down the server as scheduled.
  - **Start**
  - **Restart**

    NOTE

    After a scheduled restart task is set, the system does not execute the restart task if there are users accessing the server at the scheduled time. Instead, the system automatically postpones the task to the next scheduled time to ensure user experience.

    If the forcible restart option is selected, the system forcibly restarts the server as scheduled.
  - **Recompose system disk**

    NOTE

    - After a scheduled system disk recomposing task is set, the system does not execute the recomposing task if there are users accessing the server at the scheduled time. Instead, the system automatically postpones the task to the next scheduled time to ensure user experience.
    - If the forcible system disk recomposing option is selected, the system forcibly recomposes the system disk when the scheduled time arrives.
    - Restriction: When recomposing the system disk, ensure that the initial image still exists. Otherwise, the system disk cannot be recomposed.
    - After recomposing the system disk, the data on the system disk will be lost. If the data is needed after the system disk is recomposed, notify the user to back up the data in advance.
- **Scheduled Task Name**: This parameter is user-defined.
- **Execution Interval**: The following intervals are supported. Select one as required.
  - **Time Zone**: Time zone of users.
  - **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 month**: You can set the specific month, date, time, and expiration time.

NOTE

- Dates that do not exist are automatically skipped, for example, February 30.
- If the daylight saving time (DST) is used, view **To Execute at** to check the time when the task is to be executed.

Step 5 Click **Next**.

The page of selecting target objects is displayed.

Step 6 In the **Available Object** area, search for the server name or server group name in the search box and select it.

Step 7 Click **Create Now**.

----End

2.14.2 Managing Scheduled Tasks

Scenarios

This section describes how to delete or modify scheduled tasks on the management console.

Prerequisites

A scheduled task has been created.

Procedure

Enabling or disabling a scheduled task

Step 1 Log in to the **management console** of Workspace Application Streaming as an administrator.

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

The **Scheduled Tasks** page is displayed.

Step 3 In the status column of the scheduled task, click the switch to enable or disable it.

NOTE

-  indicates that the scheduled task is enabled.
-  indicates that the scheduled task is disabled.

Viewing the execution logs of a scheduled task

Step 4 Click **Log Details** on the right of the scheduled task.

Step 5 On the **Execution Log Details** page, you can view the execution time, task type, execution interval, execution result, and number of successful and failed tasks of the scheduled task.

Modifying a scheduled task

Step 6 Click **Modify** on the right of the scheduled task.

Step 7 Modify the scheduled task name, execution interval, time zone, time, and description as required.

Step 8 Click **Next: Select Objects**.

Step 9 On the **Modify Task** page, modify the object and click **OK**.

Modifying the execution objects of a scheduled task

Step 10 Choose **More** > **Modify Object** on the right of the scheduled task.

Step 11 Modify the object as required and click **OK**.

Copying a scheduled task

Step 12 Click **More** > **Copy** on the right of the scheduled task.

Step 13 Select the name and description of the scheduled task as required, and click **OK**.

Deleting a scheduled task

Step 14 Select the scheduled tasks to be deleted. You can delete one scheduled task or batch delete multiple scheduled tasks.

- To delete one scheduled task, perform **Step 15** to **Step 16**.
- To batch delete multiple scheduled tasks, perform **Step 17** to **Step 18**.

Step 15 Choose **More** > **Delete** on the right of the scheduled task.

Step 16 Click **OK**.

Step 17 Select the scheduled tasks to be deleted and click **Delete** in the upper part of the page.

Step 18 Select **Confirm** and click **Yes**.

----End

2.15 Storage

2.15.1 Creating NAS

Scenarios

Cloud persistent storage space is automatically created for each user (group) to store user files. Users can access files in directories on the GUI, upload and download files, create folders and subdirectories, and delete files and directories.

NOTE

Currently, the storage does not support IAM 5.0. You need to add IAM 3.0 to use the storage.

IAM 5.0: The console URL is **https://console.*xxxxxx*.com/iam5**. When a user is granted the storage permission, a message is displayed indicating insufficient permissions and the storage function cannot be used.

IAM 3.0: The console URL is **https://console.*xxxxxx*.com/iam**. When a user is granted the storage permission, the storage function is available.

Procedure

Step 1 Create a general-purpose file system by referring to section "Creating a General-Purpose File System" in *Scalable File Service User Guide*.

NOTE

Install the WKSRStorageAgent component on the APS before using NAS.

Step 2 Log in to the Workspace Application Streaming **console** as an administrator.

Step 3 In the navigation pane on the left, choose **Storage** > **NAS**. The **NAS** page is displayed.

Step 4 Click **Create NAS** in the upper right corner of the **NAS** page. The **Create NAS** page is displayed.

Step 5 Configure the following NAS parameters:

- **Storage Type**: **NAS** is selected by default.
- **SFS File Storage**: Select the name of the file system created in **Step 1**.

Step 6 Select the required file storage and click **OK**.

----End

2.15.2 Configuring Permission Policies

Scenarios

Configure permission policies for personal/shared folders of each cloud application to better manage permissions on these folders.

Policy Introduction

Table 2-23 describes the default policies.

Table 2-23 Default policies

Policy	Cloud Storage and Client Permissions	Cloud Storage and Server Permissions
High-risk Policy	Upload and download	Read and write
Medium-risk Policy 1	Download	Read and write

Policy	Cloud Storage and Client Permissions	Cloud Storage and Server Permissions
Medium-risk Policy 2	Upload	Read and write
Low-risk Policy	-	Read-only

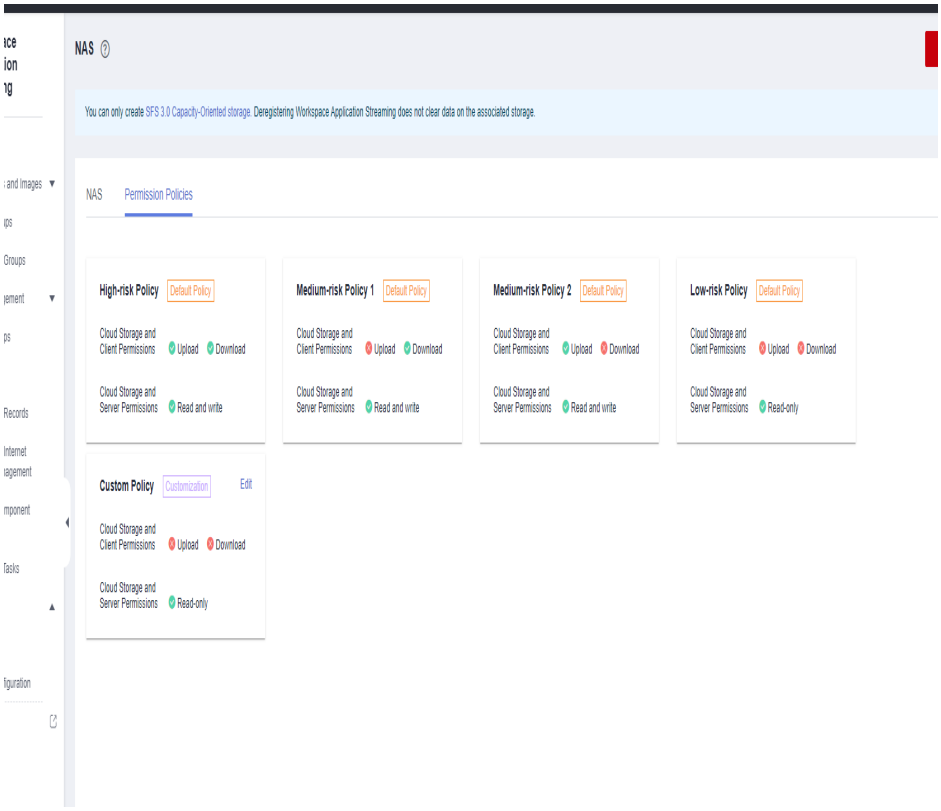
Creating a custom policy

Step 1 Log in to the **Workspace Application Streaming console** as an administrator.

Step 2 In the navigation pane on the left, choose **Storage** > **NAS**. The **NAS** page is displayed.

Step 3 Select the **Permission Policies** tab and click + to create a custom permission policy, as shown in **Figure 2-10**.

Figure 2-10 Creating a custom policy



Step 4 In the displayed dialog box, select the permissions required for **Cloud Storage and Client Permissions** and **Cloud Storage and Server Permissions**.

Step 5 Click **OK**.

NOTE

Click **Edit** on the right of a custom policy to modify it.

----End

2.15.3 Managing NAS

2.15.3.1 Personal Folders

2.15.3.1.1 Creating a Personal Folder

Scenarios

Create a personal folder on NAS.

Procedure

Step 1 Log in to the **Workspace Application Streaming console** as an administrator.

Step 2 In the navigation pane on the left, choose **Storage** > **NAS**. The **NAS** page is displayed.

Step 3 Click **Manage NAS** on the right of the NAS name to go to the NAS details page.

Step 4 Click **Create Personal Folder**. The **Create Personal Folder** page is displayed.

Step 5 Enter a username in the search box to search for the user, select the user, and click **Next**.

Step 6 Configure permission policies. Select required permissions from the **Permission Policy** drop-down list box.

Step 7 Click **Next** and confirm the configurations.

Step 8 Click **OK**.

----End

2.15.3.1.2 Modifying Permissions on a Personal Folder

Scenarios

Modify permissions on a personal folder on NAS.

Procedure

Step 1 Log in to the **Workspace Application Streaming console** as an administrator.

Step 2 In the navigation pane on the left, choose **Storage** > **NAS**. The **NAS** page is displayed.

Step 3 Click **Manage NAS** on the right of the NAS name to go to the NAS details page.

Step 4 On the NAS details page, select **Personal Folders** and modify the permission of a personal folder as required.

- **Modifying permissions of one user**: Locate the row of the target user, click **Modify Permission** in the **Operation** column, and select a user permission policy from the **Permission Policy** drop-down list.

- **Batch modifying permissions of users**: Select the users whose permissions are to be modified, click **Modify Permission**, and select a user permission policy from the **Permission Policy** drop-down list.

Step 5 Click **OK**.

----End

2.15.3.1.3 Deleting a Personal Folder

Scenarios

Delete a personal folder on NAS.

Procedure

Step 1 Log in to the **Workspace Application Streaming console** as an administrator.

Step 2 In the navigation pane on the left, choose **Storage** > **NAS**. The **NAS** page is displayed.

Step 3 Click **Manage NAS** on the right of the NAS name to go to the NAS details page.

Step 4 On the **Personal Folders** tab, select the personal folder that you want to delete.

- To delete one folder, perform **Step 5** to **Step 6**.
- To delete folders in batches, perform **Step 7** to **Step 8**.

Step 5 Locate the row that contains the folder to be deleted and click **Delete** in the **Operation** column. The **Delete** page is displayed.

Step 6 Select **I understand the impact and want to continue** and click **Yes**.

Step 7 Select the folders to be deleted in batches and click **Delete** in the upper left corner. The **Batch Delete** page is displayed.

Step 8 Select **I understand the impact and want to continue** and click **Yes**.

NOTE

- The NAS folder data will be permanently deleted and cannot be restored.
- After deleting personal folders, log in to the client again to view the folder status.

----End

2.15.3.2 Shared Folders

2.15.3.2.1 Creating a Shared Folder

Scenarios

Create a shared folder on NAS.

Procedure

Step 1 Log in to the **Workspace Application Streaming console** as an administrator.

Step 2 In the navigation pane on the left, choose **Storage** > **NAS**. The **NAS** page is displayed.

Step 3 Click **Manage NAS** on the right of the NAS name to go to the NAS details page.

Step 4 On the **Shared Folders** tab, click **Create Shared Folder**. The **Create Shared Folder** dialog box is displayed.

Step 5 Enter the folder name as required and click **OK**.

NOTE

- Only single-level folders can be created.
- A folder name can contain a maximum of 32 characters, including letters, digits, spaces, underscores (_), and hyphens (-).
- A folder name cannot contain only spaces or start with a space.
- Rules for user permissions to take effect:
  - **Cloud Storage and Client Permissions**: The permissions take effect after the user refreshes the cloud storage file list.
  - **Cloud Storage and Server Permissions**: The permissions take effect after the user logs out of the session and logs in again.

----End

2.15.3.2.2 Managing Members

Scenarios

You can add, delete, and modify members in a shared folder.

Procedure

Step 1 Log in to the **Workspace Application Streaming console** as an administrator.

Step 2 In the navigation pane on the left, choose **Storage** > **NAS**. The **NAS** page is displayed.

Step 3 Click **Manage NAS** on the right of the NAS name to go to the NAS details page.

Step 4 Select **Shared Folders** and click **Member Management**. The **Member Management** page is displayed.

Adding a member

Step 5 On the **Member Management** page, click **Add Member**. The **Add Member** dialog box is displayed.

Step 6 Select the user or user group to be added and click **Next**.

Step 7 Select the required permissions from the **Permission Policy** drop-down list or click **Storage Policy Management** to add or edit a custom policy.

Step 8 Click **Next** and confirm the configurations.

Step 9 Click **OK**.

Modifying permissions

Step 10 On the NAS details page, select **Shared Folders**.

Step 11 Select the folder to be modified and click **Member Management**. The **Member Management** page is displayed.

- **Modifying permissions of one user or user group**: Locate the row that contains the target user or user group, click **Modify Permission** in the **Operation** column, and select a user or user group permission policy from the **Permission Policy** drop-down list as required.
- **Batch modifying permissions of users or user groups**: Select the users or user groups whose permissions are to be modified, click **Modify Permission**, and select a user or user group permission policy from the **Permission Policy** drop-down list as required.

Step 12 Click **OK**.

Deleting a member

Step 13 To delete one user or user group, click **Delete** in the **Operation** column on the **Member Management** page. On the displayed page, click **OK**.

Step 14 To batch delete users or user groups, select the users or user groups to be deleted on the left of the **Member Management** page and click **Delete**. On the page displayed, select **Confirm** and click **Yes**.

NOTE

- After adding or deleting a user or user group of the shared folder, log in to the client again to view the user or user group.
- Rules for member permissions to take effect:
  - **Cloud Storage and Client Permissions**: The permissions take effect after the user refreshes the cloud storage file list.
  - **Cloud Storage and Server Permissions**: The permissions take effect after the user logs out of the session and logs in again.

----End

2.15.3.2.3 Deleting a Shared Folder

Scenarios

Delete a shared folder on NAS.

Procedure

Step 1 Log in to the **Workspace Application Streaming console** as an administrator.

Step 2 In the navigation pane on the left, choose **Storage** > **NAS**. The **NAS** page is displayed.

Step 3 Click **Manage NAS** on the right of the NAS name to go to the NAS details page.

Step 4 On the **Shared Folders** tab page, select the shared folder that you want to delete.

- To delete one folder, perform **Step 5** to **Step 6**.
- To delete folders in batches, perform **Step 7** to **Step 8**.

Step 5 Locate the row that contains the folder to be deleted and click **Delete** in the **Operation** column. The **Delete** page is displayed.

Step 6 Select **I understand the impact and want to continue** and click **Yes**.

Step 7 Select the files to be deleted in batches and click **Delete** in the upper left corner. The **Batch Delete** page is displayed.

Step 8 Select **I understand the impact and want to continue** and click **Yes**.

NOTE

- The NAS folder data will be permanently deleted and cannot be restored.
- To delete a shared folder, delete the users and user groups bound to the shared folder on the **NAS** > **Shared Folders** > **Member Management** page first.
- After deleting shared folders, log in to the client again to view the folder status.

----End

2.15.4 Deleting NAS

Procedure

Step 1 Log in to the **Workspace Application Streaming console** as an administrator.

Step 2 In the navigation pane on the left, choose **Storage** > **NAS**. The **NAS** page is displayed.

Step 3 Select the NAS to be deleted and click **Delete** on the right. The confirmation dialog box is displayed.

Step 4 Click **OK**.

NOTE

- The deletion operation only disassociates the NAS from the file system, but does not delete the file system.
- Before deleting NAS, delete the created personal or shared folder by referring to **2.15.3.1.3 Deleting a Personal Folder** and **2.15.3.2.3 Deleting a Shared Folder**.
- When a user or user group is deleted, the permission on the shared directory is automatically removed. When a user is deleted, the personal directory of the user is automatically deleted.

----End

2.15.5 Configuring a Server Group Mounting Policy

Scenarios

Mount shared folders, personal folders, or both folder types at the server group level.

Prerequisites

- An NAS instance has been created.
- An APS group has been created.

Procedure

Step 1 Log in to the **Workspace Application Streaming console** as an administrator.

Step 2 In the navigation pane, choose **Server Groups**.

Step 3 Click the name of the server group for which you want to modify the mounting policy. The server group details page is displayed.

Step 4 Click  on the right of **Mounting Policy**. The **Modify Mounting Policy** dialog box is displayed.

Step 5 Configure **Directory Settings** as required.

- **Personal directory**: Only personal folders are mounted to the server.
- **Shared directory**: Only shared folders are mounted to the server.
- **All directories**: Both personal folders and shared folders are mounted to the server.

Step 6 Click **OK**.

----End

2.16 Tenant Configuration

Scenarios

The administrator can adjust the enterprise ID, domain configuration, access mode, service subnet, and Internet access port as required.

If the same project is used by Workspace Application Streaming and Workspace, they share the same tenant list. Therefore, tenant information modified on the Workspace Application Streaming console needs to be synchronized to the Workspace console and vice versa.

Procedure

Step 1 Log in to the Workspace Application Streaming **console** as an administrator.

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

Step 3 Perform the operations listed in **Table 2-24** as required.

Table 2-24 Tenant configuration operations

Operation	Procedure	Description
Setting a project	1. Click ▼ on the right of the project area and select the required project from the drop-down list box. 2. If no project is available, click **Create Project** to create one. For details, see **Creating a Project**.	Projects group and isolate resources (including compute, storage, and network resources) in the same Huawei Cloud region. Users can be granted permissions to access all resources in a specific project. A default project is provided for each Huawei Cloud region. Create one if no project is available when enabling Workspace Application Streaming.
Modifying an enterprise ID	1. In the **Basic Information** area, click **Modify**. 2. Enter the custom enterprise ID in the displayed dialog box. 3. Click **OK**.	After the service is enabled, an enterprise ID is automatically generated. The administrator can modify the enterprise ID.
MFA configuration > Virtual MFA	1. In the **MFA Configuration** area, click **Enable**. 2. Click **OK**.	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**, and **Logging In to a Desktop Using a Mobile Terminal**.

Operation	Procedure	Description
MFA configuration > Authentication Server	1. Click **Modify** next to **Authentication Server**. 2. Select **Enterprise Authentication System** and set the parameters as follows: 1. **Server Address**: the IP address of the enterprise's authentication server. 2. **APP ID**: the access key (AK) of the enterprise's authentication server. The AK can contain a maximum of 24 characters. 3. **APP Secret**: the secret access key (SK) of the enterprise's authentication server. The SK can contain a maximum of 128 characters. 4. Set this parameter based on the network mode of the user's authentication server. a. If only the public network is accessible, select **Internet Access Users**. b. If only the private network is accessible, select **Direct Connect Access User**. 5. Click **Upload Certificate**, select the SSL/TLS certificate of the enterprise authentication server, and click **Open** to upload the certificate.	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 an APS from the Workspace client using accounts and passwords. For details, see **Logging In to a Desktop Using an SC**, **Logging In to a Desktop Using a TC**, and **Logging In to a Desktop Using a Mobile Terminal**.
Changing the domain administrator password	1. In the **AD Domain Configuration** area, click **Change Password**. 2. Reset the password. 3. Click **OK**.	After resetting the domain administrator password on the AD server, the administrator needs to synchronize the password information on the Workspace Application Streaming console.

Operation	Procedure	Description
Modifying domain configurations	1. In the lower part of the **AD Domain Configuration** area, click **Modify**. 2. Enter the password of the domain administrator and modify the domain configuration. 3. Click **OK**.	After modifying the domain configuration items on the AD server, the administrator needs to synchronize the domain configuration information on the Workspace Application Streaming console.
Modifying the access mode	In the **Network Settings** area, enable or disable the corresponding access address. **NOTE** • The Internet access address is enabled by default. • The Internet access address and Direct Connect access address cannot be disabled at the same time. At least one access address must be enabled.	The administrator can change the network access mode.
Changing the service subnet	1. In the **Network Settings** area, click **Edit the subnet**. 2. Select the service subnet to be used, or deselect the selected service subnet. 3. Click **OK**.	The administrator can change the service subnet.
Changing the Internet access port	1. In the **Network Settings** area, click **Modify** near the **Internet Access Port** part. 2. Change the port number. 3. Click **OK**.	The administrator can change the HTTPS port used for accessing the Workspace Application Streaming portal through the client.

----End

2.17 Private Images

2.17.1 Creating a Windows Private Image (Basic Image)

2.17.1.1 Required Software

Table 2-25 lists the software packages required for creating a Windows private image.

Table 2-25 Required software packages

Name	Description	How to Obtain
Workspace_HDP_WindowsDesktop_Installer_*x.x.x*.iso	Windows image creation tool	Contact technical support engineers.
OS ISO file	• Windows Server 2016 Datacenter 64-bit • Windows Server 2019 Datacenter 64-bit	Obtain the required OS ISO image file from Microsoft or other official sources. **NOTICE** The OS ISO file must be a pure image obtained from an official channel. Do not use non-official 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	**Click here**.
VirtIO driver package	VirtIO driver	**Click here**. **Click here for other versions**. Install the VirtIO driver by referring to **Installing VirtIO Drivers**.
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.	**Click here**.

Name	Description	How to Obtain
CloudbaseInitSet-up_*xxx*.msi	Customize usernames, passwords, and the **hostname** and **hosts** files during cloud server creation using images.	Download the appropriate version of Cloudbase-Init installation package based on the Windows bit version. Cloudbase-Init has two versions: stable and beta. To obtain the stable version, visit the following paths: • 64-bit: **Click here**. • 32-bit: **Click here**. To obtain the beta version, visit the following paths: • 64-bit: **Click here**. • 32-bit: **Click here**.
CloudResetPwdAgent.zip	Cloud server password reset plug-in.	Contact technical support engineers.
GPU driver	Required only in GPU image creation.	Workspace Application Streaming supports RTX5000 passthrough cards. Do as follows to obtain the RTX5000 driver: Log in to the **NVIDIA official website** using a browser. On the **Download Drivers** page, configure parameters based on the OS (including the Windows driver type and language) and GPU type, and download the latest driver. For example, if you want to use the RTX 5000 graphics card on the desktop running the Windows Server 2019 Datacenter, configure parameters as follows: • **Product Type**: NVIDIA RTX / Quadro • **Product Series**: Quadro RTX Series • **Product**: Quadro RTX 5000 • **Operating System**: Windows Server 2019 • **Language**: English (US)
Peripheral driver	Prepare the peripheral drivers as required.	Prepared by users

Name	Description	How to Obtain
HW.SysAgent.Installer_64.msi and HW.SysPrep.Installer_64.msi	For APS provisioning and HDA upgrade. Double-click the .msi file to install.	Contact technical support engineers.
WKSAppDhcpd_windows-amd64.msi	Assign virtual IP addresses during APS creation. Double-click the .msi file to install.	Contact technical support engineers.
WKSRStorageAgent_windows-amd64.msi	For the cloud storage function. Double-click the .msi file to install.	Contact technical support engineers.
Sandboxie	Enable applications to run in sandbox mode. For details about how to install the Sandboxie software, see **2.23.21 How Do I Install Sandbox Software?**.	**Click here**.

2.17.1.2 Registering a Private Image Using an ISO File

Scenarios

This section describes how to create a Windows private image.

Prerequisites

- You have obtained the username and password for logging in to the console.
- You have prepared the OS ISO file. For details, see **Table 2-25**.

  NOTE

  The name of the ISO image file can contain only letters, digits, hyphens (-), and underscores (_).

Procedure

Integrating the VirtIO driver into an ISO file using AnyBurn

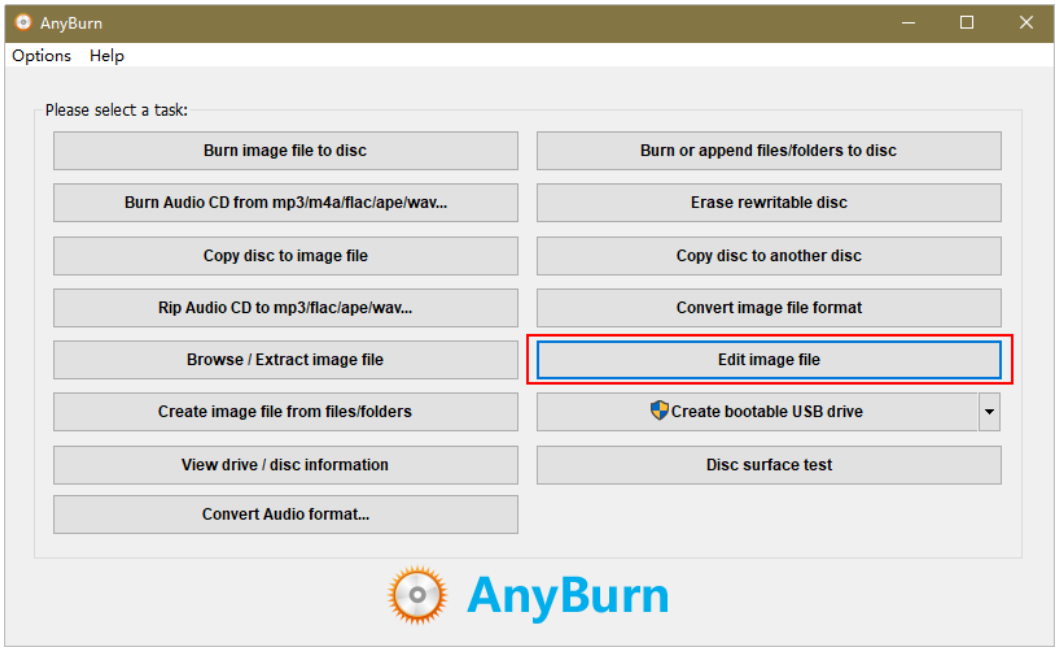
Step 1 Install AnyBurn on the local PC.

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

Step 3 Use AnyBurn to open the ISO file.

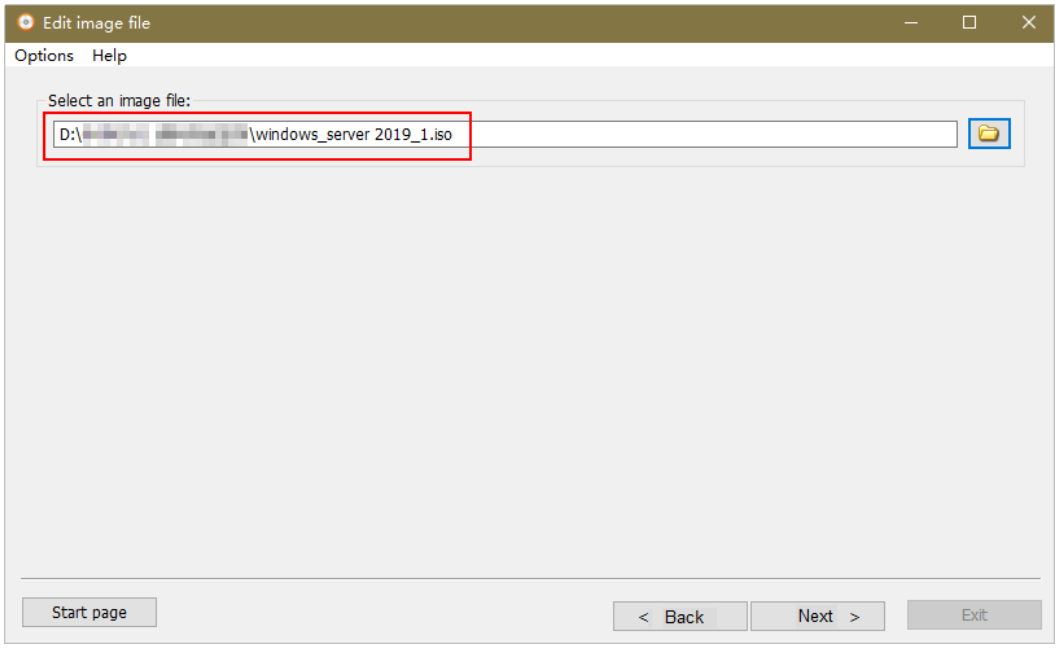
Open the AnyBurn software and select **Edit image file**, as shown in Figure 2-11.

Figure 2-11 Editing an image file



Select the ISO file and click **Next**, as shown in Figure 2-12.

Figure 2-12 Selecting the ISO file

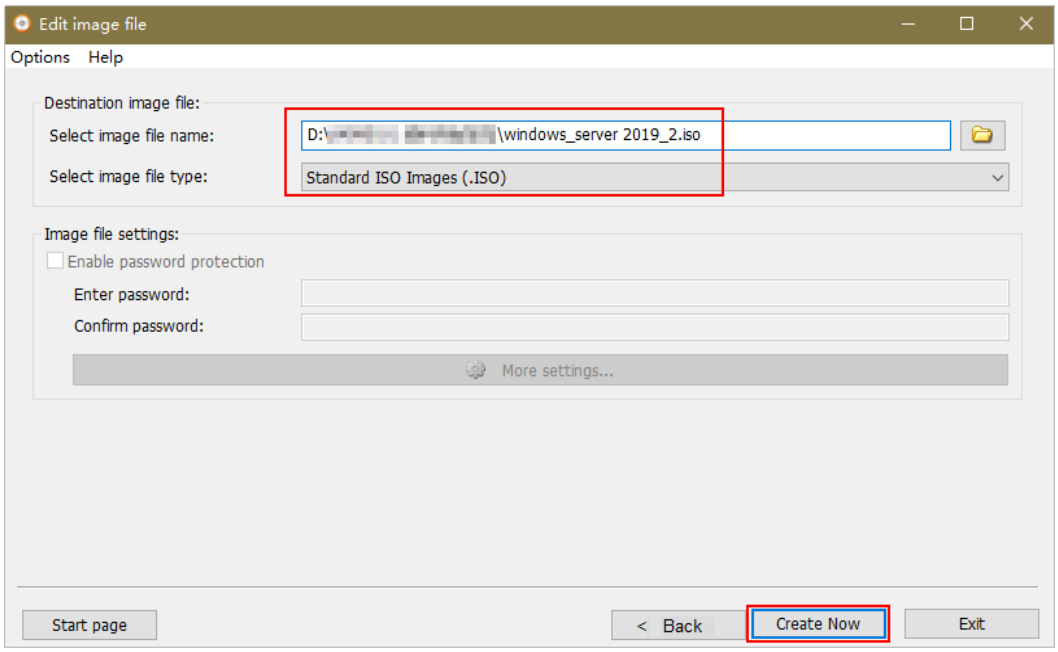


Step 4 Edit the ISO file to integrate the VirtIO driver.

1. Click **Add** to add all files in the **virtio-win.iso** file downloaded in 2 to the parent node of the ISO file, and click **Next**.
2. Specify the path for saving the file and the ISO file name, select the ISO format, and click **Create Now**.

After the ISO file is generated, view the ISO file integrated with the VirtIO driver, as shown in **Figure 2-13**.

Figure 2-13 Viewing the ISO file integrated with the VirtIO driver



Registering a private image

Step 5 Log in to Huawei Cloud management console.

Step 6 Upload an image file.

You are advised to use OBS Browser+ to upload external image files to a personal OBS bucket. For details, see **OBS Browser+ Best Practices**.

For details about how to download, install, and log in to OBS Browser+, see "**OBS Browser+**" in the *Tools Guide* of OBS.

NOTE

- If no OBS bucket is available, create one by referring to "**Creating a Bucket**" in the *Getting Started* of OBS.
- The bucket file and the image to be registered must in 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 and the image file 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 ISO file.

Step 11 On the **Image Information** page, configure basic information about the image according to **Table 2-26**. Retain the default values for the parameters that are not listed below.

Table 2-26 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, **60** GB.
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**. **NOTE** This parameter is mandatory if the enterprise project has been enabled.

Step 12 Confirm the image parameters, select **I have read and agree to the Statement of Commitment to Image Creation and Image Disclaimer.**, and click **Next**.

Step 13 Click **Submit**.

View the image status on the displayed private image list.

When the image status becomes **Normal**, the image has been created.

----End

2.17.1.3 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. For details, see **2.17.1.2 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 **Create ECS** in the **Operation** column of the private image created in **2.17.1.2 Registering a Private Image Using an ISO File**.

Step 4 On the displayed page, configure the parameters in **Table 2-27** and retain the default values for other parameters.

Table 2-27 ECS configuration

Parameter	Description	Example
Flavor	Select the desired ECS flavor. For example, select **s6.xlarge.2** for a common image. If the GPU image type is RTX, the value can be **g5r**.	s6.xlarge.2
VPC	Select the desired VPC.	fa_vpc
Subnet	Select the desired subnet.	subnet-fa
Name	The value can be customized.	WKS-desktop_temp

Parameter	Description	Example
Enterprise Project	Select an enterprise project. **NOTE** This parameter is mandatory if the enterprise project has been enabled.	default

Step 5 Click **OK**.

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 2-28**.

Table 2-28 Security group configuration

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

Parameter	Description	Example
Template	• **General-purpose web server**: allows all inbound ICMP traffic and inbound traffic on ports **22**, **80**, **443**, and **3389**. This template applies to ECS for remote login, public network ping, and website services. • **All ports open**: allows inbound traffic on all ports. Note that this poses security risks. • **Fast-add rule**: You can select common protocols and ports to quickly add inbound rules. If you do not select any protocols or ports, all of them will be closed. You can add or modify security group rules as required after a security group is created.	-

Step 10 Locate the row that contains the security group created in **Step 9**, and click **Manage Rules**. On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, set **Protocol & Port**, as shown in **Table 2-29**.

Table 2-29 Security group rules

Protocol & Port	Type	Source
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 Instances**.

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

2.17.1.4 Configuring an ECS

Scenarios

This section describes how to install application software, configure patch updates, 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. For details, see **2.17.1.3 Creating an ECS**.
- You have obtained the files listed in **2.17.1.1 Required Software** and decompressed the **Workspace_HDP_WindowsDesktop_Installer**_*x.x.x*.**iso** file to obtain the **Workspace_HDP_WindowsDesktop_Installer**_*x.x.x* folder.

Procedure

NOTE

The operations vary depending on the OS. Follow the instructions on the GUI.

Installing a Windows OS and the VirtIO driver

Step 1 Log in to the console.

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

Step 3 Locate the row that contains the ECS created in **2.17.1.3 Creating an ECS**, and click **Remote Login** to log in to the Windows VM.

Step 4 For details, see **Installing a Windows OS and VirtIO Drivers**.

Modifying the group policy

NOTE

- If you modify the group policy, no confirmation dialog box is displayed when you disable the Windows ECS created using the image.
- If you do not modify the group policy, you can perform this task on a Windows ECS created using the image.
- Remote desktop connection is available only after you configure the group policy of the remote desktop service.

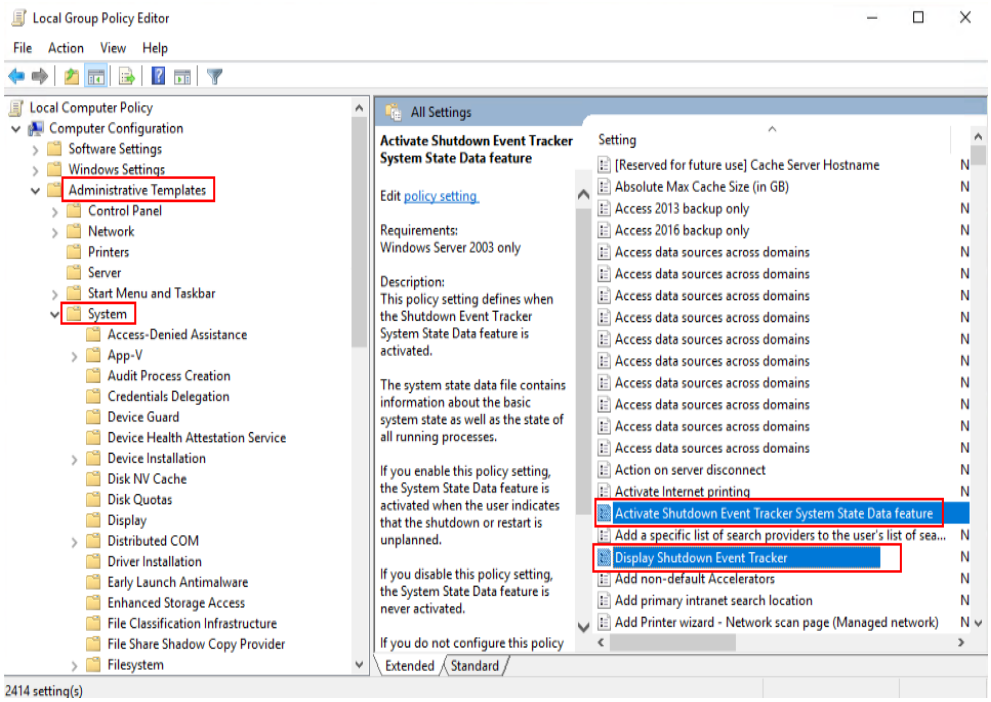
Step 5 On the ECS, right-click  in the lower left corner, enter **gpedit.msc** in the **Run** dialog box, and press **Enter**.

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

Step 6 In the navigation tree of the **Local Group Policy Editor** window, choose **Computer Configuration** > **Administrative Templates** > **System**.

Step 7 Disable **Activate Shutdown Event Tracker System State Data feature** and **Display Shutdown Event Tracker**, as shown in **Figure 2-14**.

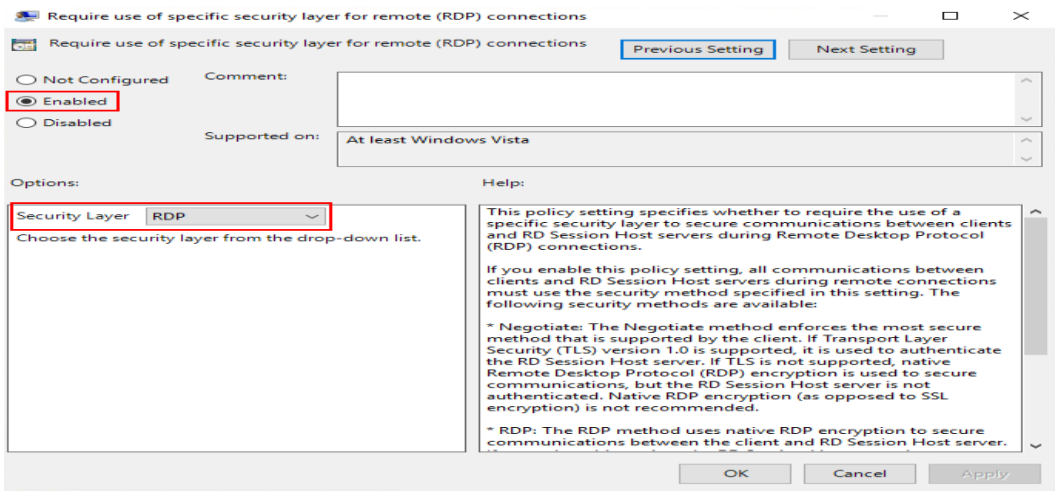
Figure 2-14 Modifying the group policy



Step 8 In the navigation pane, choose **Computer Configuration** > **Policy** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Security**.

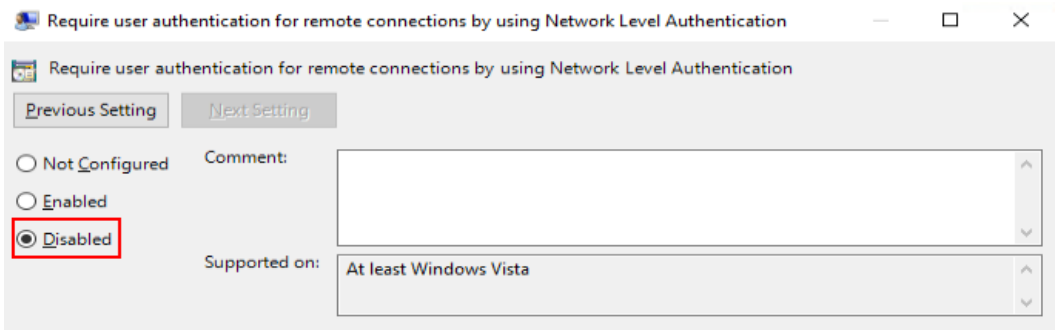
Step 9 Set **Require use of specific security layer for remote (RDP) connections** to **Enabled**, and set **Security Layer** to **RDP**, as shown in **Figure 2-15**.

Figure 2-15 Setting security layer



Step 10 Set **Require user authentication for remote connections by using Network Level Authentication** to **Disabled**, as shown in **Figure 2-16**.

Figure 2-16 Setting user authentication

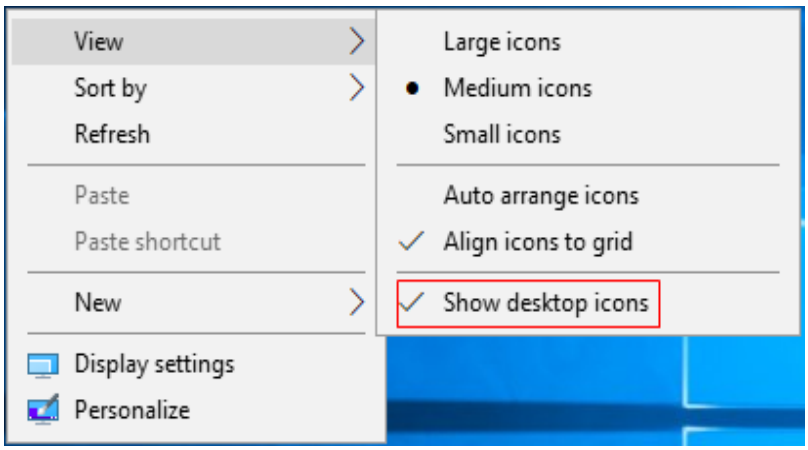


----End

Hiding Desktop Icons

Step 1 Right-click the blank area on the ECS and deselect **Show desktop icons** under **View**, as shown in **Figure 2-17**.

Figure 2-17 Desktop icon settings



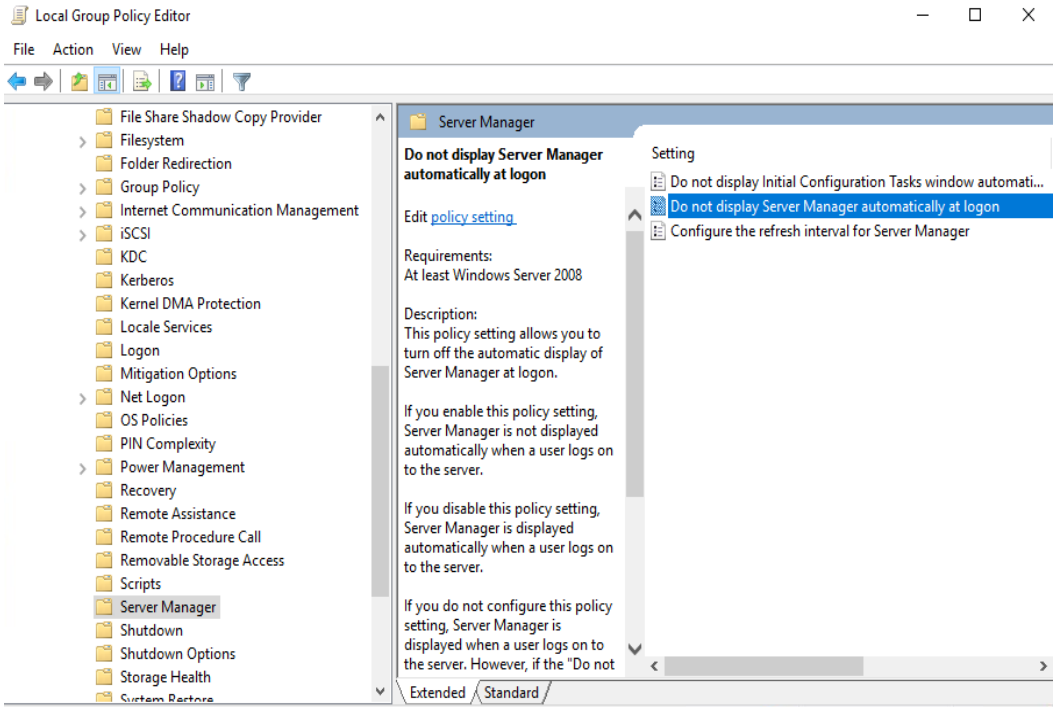
NOTE

This configuration is required only for the VDI single session.

Not displaying Server Manager page upon login

Step 2 In the navigation tree, choose **Computer Configuration** > **Administrative Templates** > **System** > **Server Manager**, as shown in **Figure 2-18**.

Figure 2-18 Not displaying Server Manager page upon login



Step 3 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 4 Select **Enabled**.

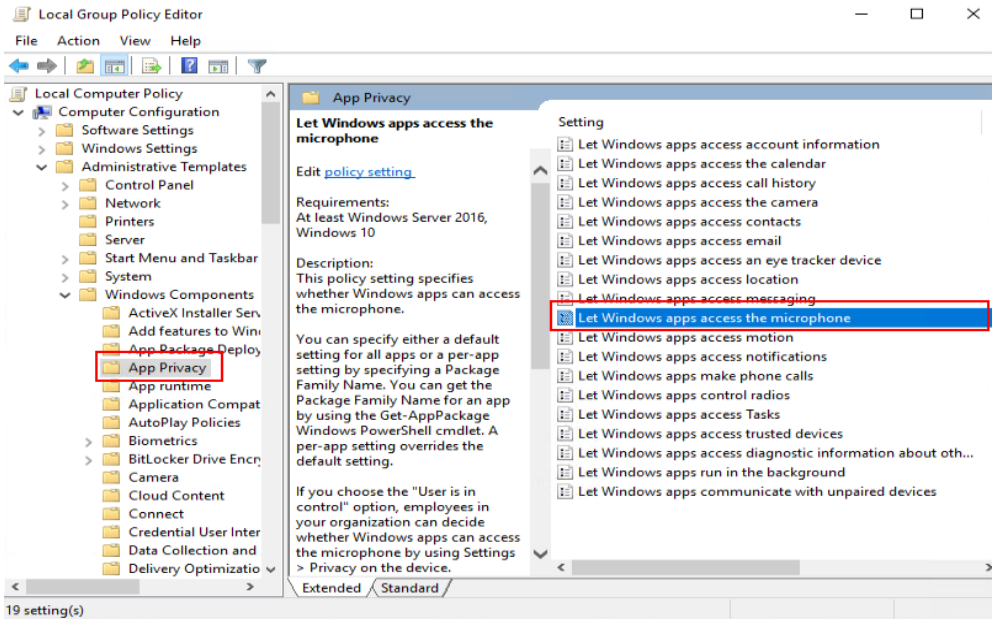
Step 5 Click **OK**.

Enabling the microphone access permission for applications

Step 6 In the navigation tree of the **Local Group Policy Editor** window, choose **Computer Configuration** > **Administrative Templates** > **Windows Components** > **App Privacy**.

Access the app privacy configuration list page and allow Windows applications to access the microphone, as shown in **Figure 2-19**.

Figure 2-19 Allowing Windows applications to access the microphone

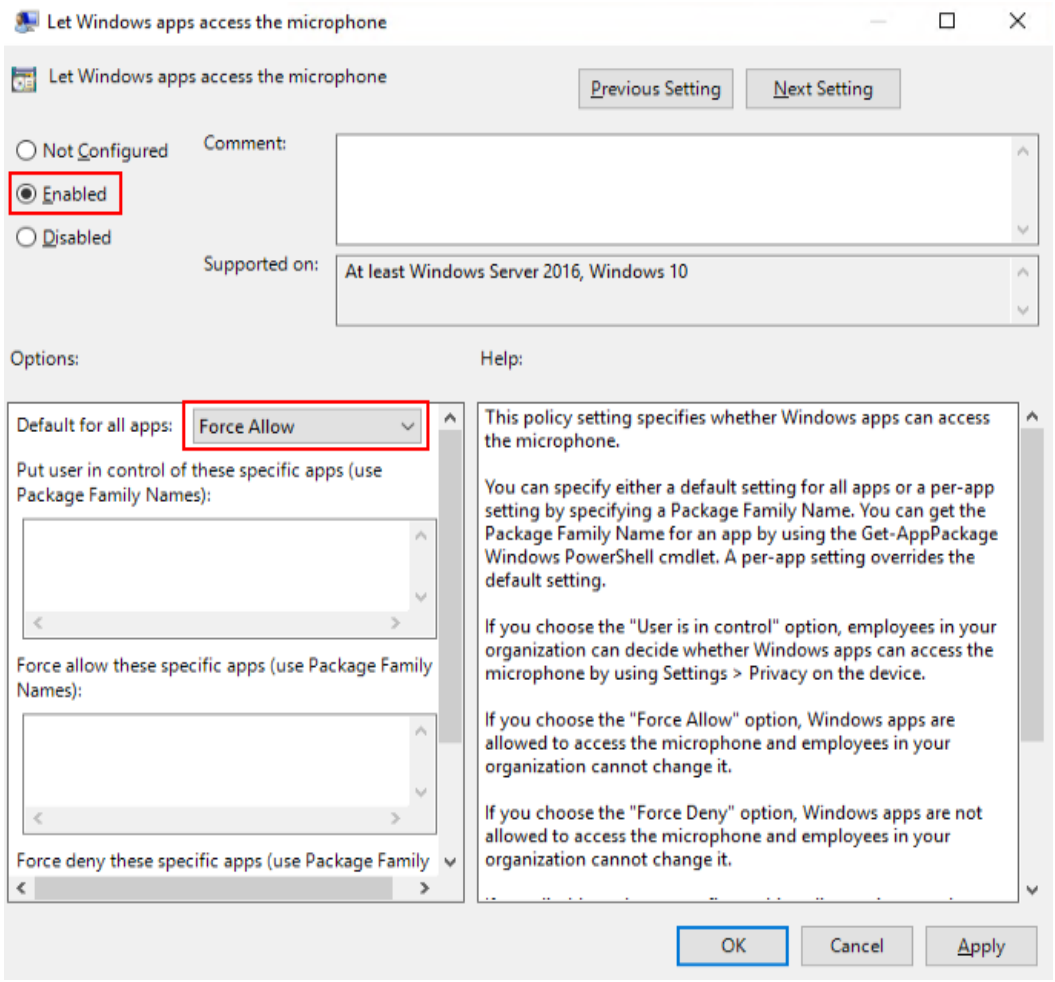


Step 7 In the right pane, double-click **Let Windows apps access the microphone**.

The **Let Windows apps access the microphone** dialog box is displayed.

Step 8 Select **Enabled**. In the **Options** list, set **Default for all apps** to **Force Allow**, as shown in **Figure 2-20**.

Figure 2-20 Configuring the microphone access permission for applications



Step 9 Click **OK**.

Enabling the camera access permission for applications

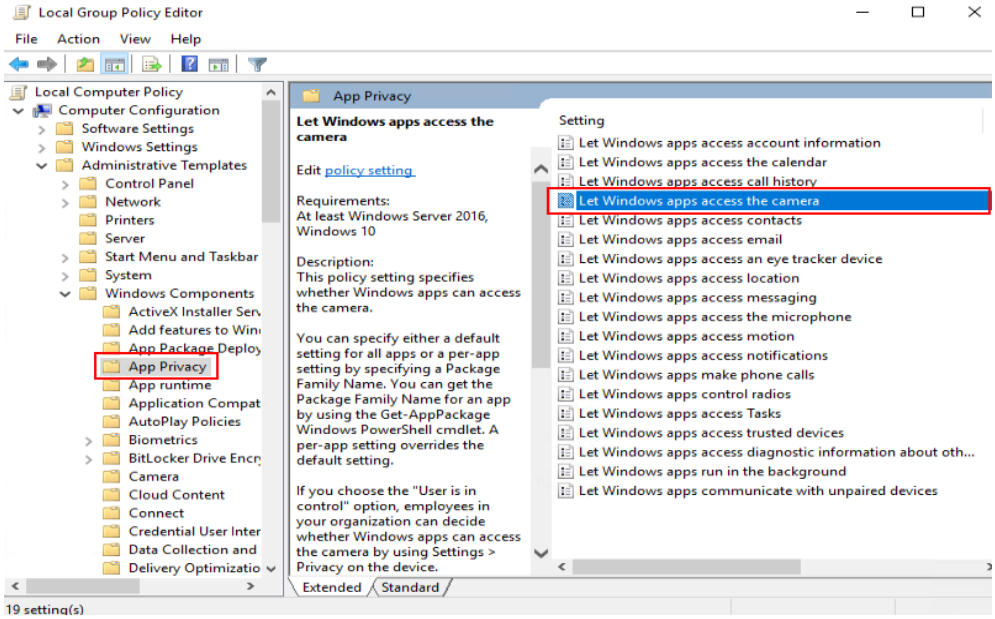
NOTE

This configuration is required only for the VDI single session.

Step 10 In the navigation tree of the **Local Group Policy Editor** window, choose **Computer Configuration** > **Administrative Templates** > **Windows Components** > **App Privacy**.

Access the app privacy configuration list page and allow Windows applications to access the camera, as shown in **Figure 2-21**.

Figure 2-21 Allowing Windows applications to access the camera

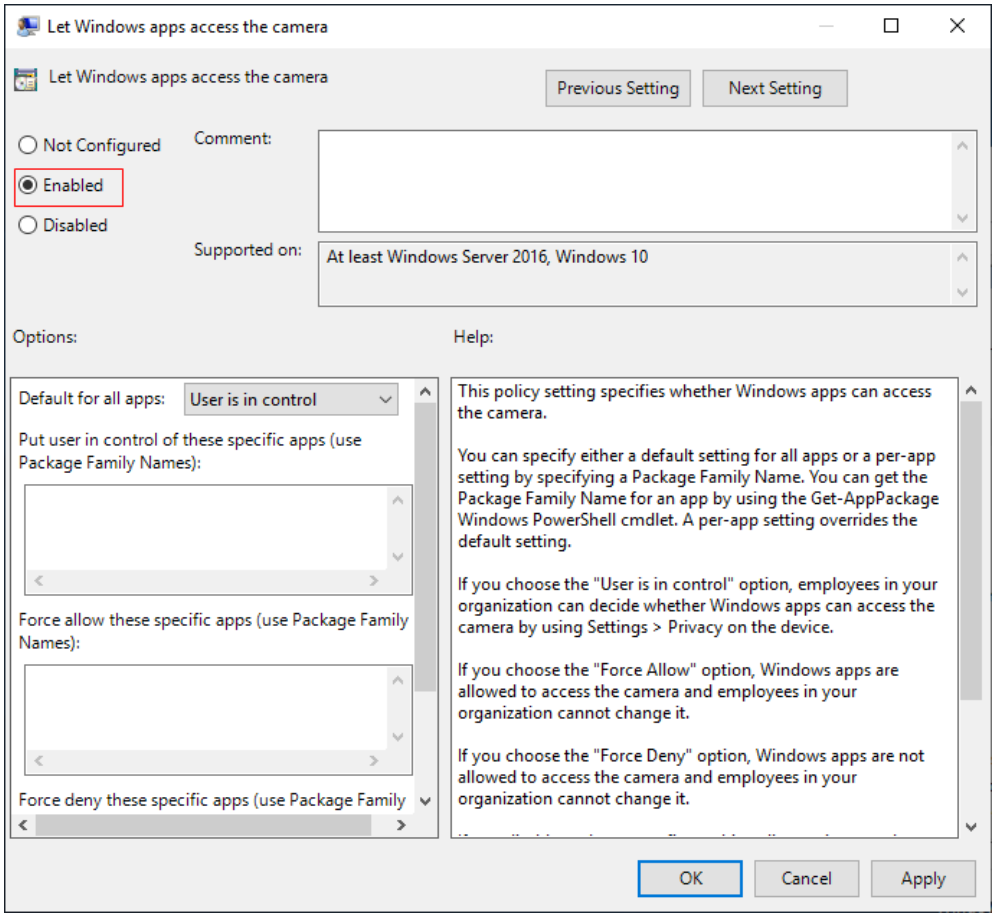


Step 11 In the right pane, double-click **Let Windows apps access the camera**.

The **Let Windows apps access the camera** dialog box is displayed.

Step 12 Select **Enabled**. In the **Options** list, set **Default for all apps** to **Force Allow**, as shown in **Figure 2-22**.

Figure 2-22 Configuring the camera access permission for applications



Step 13 Click **OK**.

Enabling the graphics adapter for the GPU remote desktop

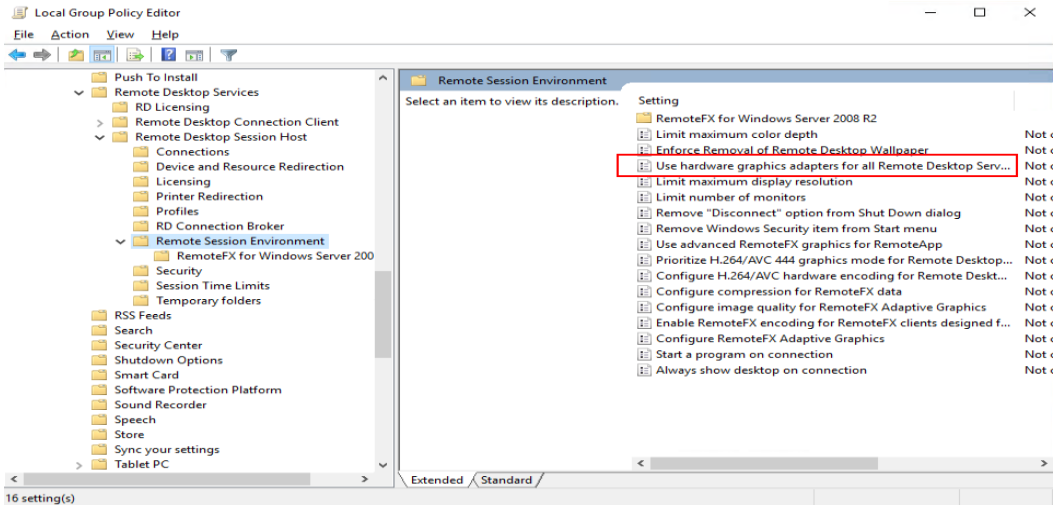
NOTE

This configuration is required only for GPU feature usage.

Step 14 In the navigation tree of the **Local Group Policy Editor** window, choose **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Remote Session Environment**.

The remote session environment configuration list page is displayed, as shown in **Figure 2-23**.

Figure 2-23 Remote session environment configuration



Step 15 In the right pane, double-click **Use the hardware graphics adapter for all Remote Desktop Services sessions**.

The **Use the hardware graphics adapter for all Remote Desktop Services sessions** dialog box is displayed.

Step 16 Select **Enabled**.

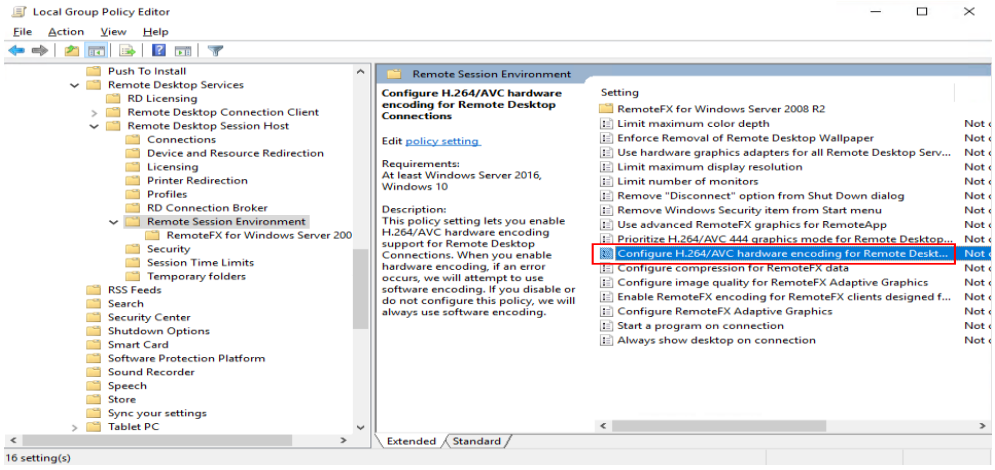
Step 17 Click **OK**.

Configuring H.264/AVC hardware encoding for remote desktop connection

Step 18 In the navigation tree of the **Local Group Policy Editor** window, choose **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Remote Session Environment**.

The remote hardware encoding configuration page is displayed, as shown in **Remote hardware encoding**.

Figure 2-24 Remote hardware encoding



Step 19 Select **Enabled**.

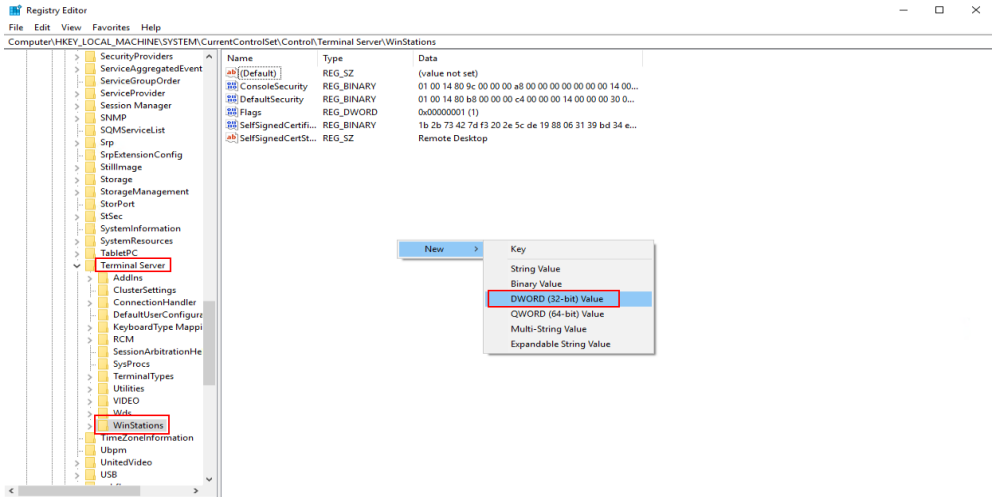
Step 20 Click **OK**.

Setting the maximum frame rate

Step 21 Click  and enter **Regedit** to open the registry editor.

Step 22 In the **Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations** directory, right-click the blank area and click **New** > **DWORD (32-bit) Value** in the right pane, enter a new value for **DWMFRAMEINTERVAL**, and press **Enter**, as shown in **Figure 2-25**.

Figure 2-25 Creating a DWMFRAMEINTERVAL



Step 23 Right-click **DWMFRAMEINTERVAL** and choose **Modify** from the shortcut menu.

Step 24 Select **Decimal**, enter **15** in the **Value data** box, and select **OK**.

Disabling the firewall

Step 25 In the navigation tree of the **Local Group Policy Editor** window, choose **Computer Configuration** > **Administrative Templates** > **Network** > **Network Connections** > **Windows Defender Firewall** > **Domain Profile**.

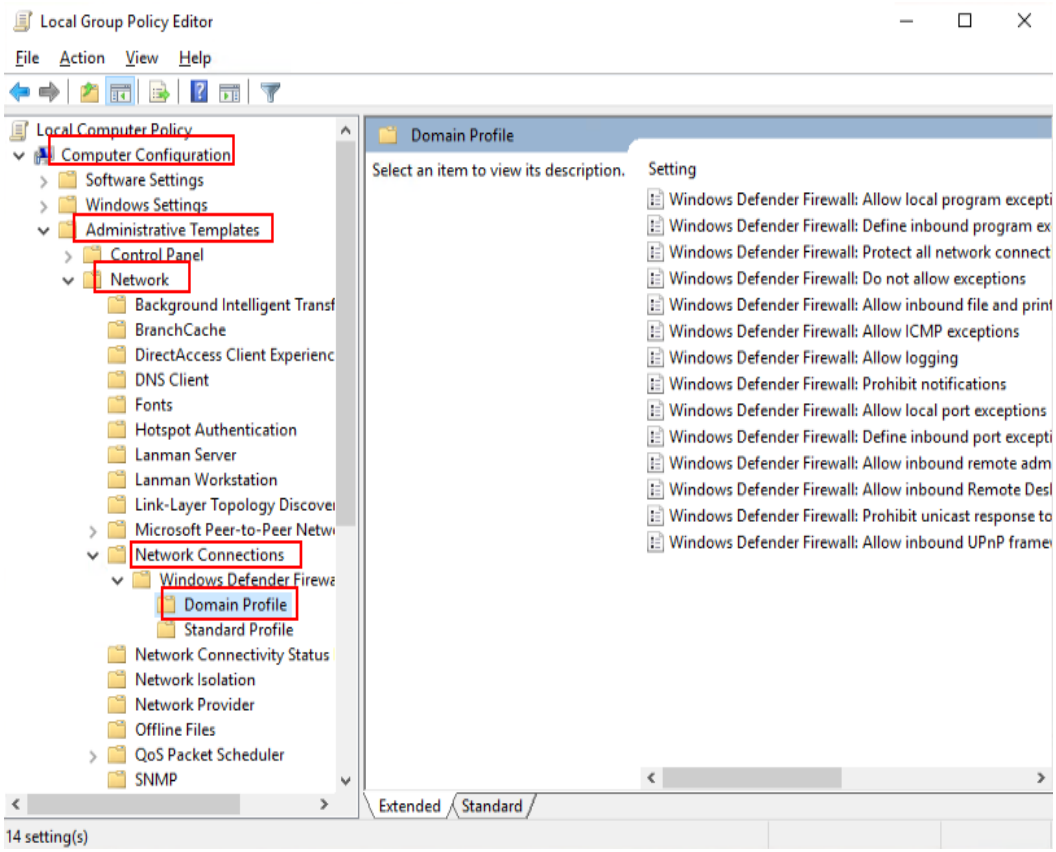
NOTE

The Windows firewall name varies with the OS version. The actual configured name is used.

For example, **Windows Firewall** is displayed on Windows Server 2016, and **Windows Defender Firewall** is displayed on Windows Server 2019.

The **Domain Profile** page is displayed, as shown in **Figure 2-26**.

Figure 2-26 Domain profiles



Step 26 In the right pane, double-click **Windows Defender Firewall: Protect all network connections**.

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

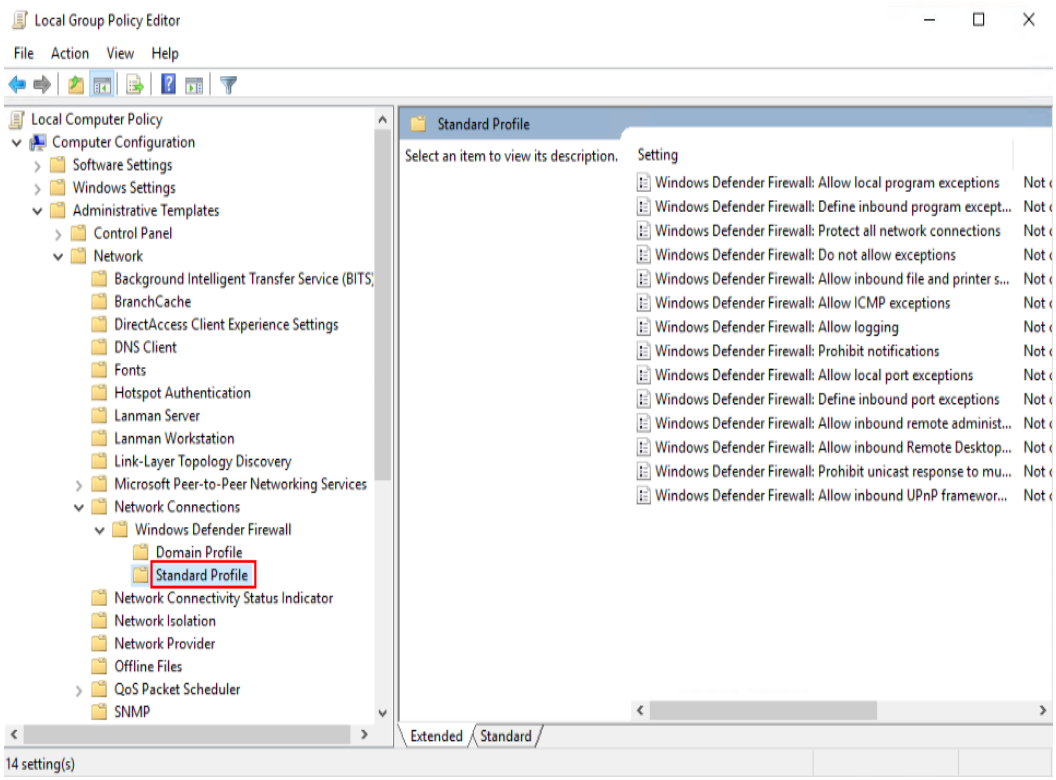
Step 27 Select **Disabled**.

Step 28 Click **OK**.

Step 29 In the navigation tree of the **Local Group Policy Editor** window, click **Standard Profile**.

The **Standard Profile** page is displayed, as shown in **Figure 2-27**.

Figure 2-27 Standard profiles



Step 30 In the right pane, double-click **Windows Defender Firewall: Protect all network connections**.

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

Step 31 Select **Disabled**.

Step 32 Click **OK**.

Step 33 Close the **Local Group Policy Editor** window.

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

The **Run** dialog box is displayed.

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

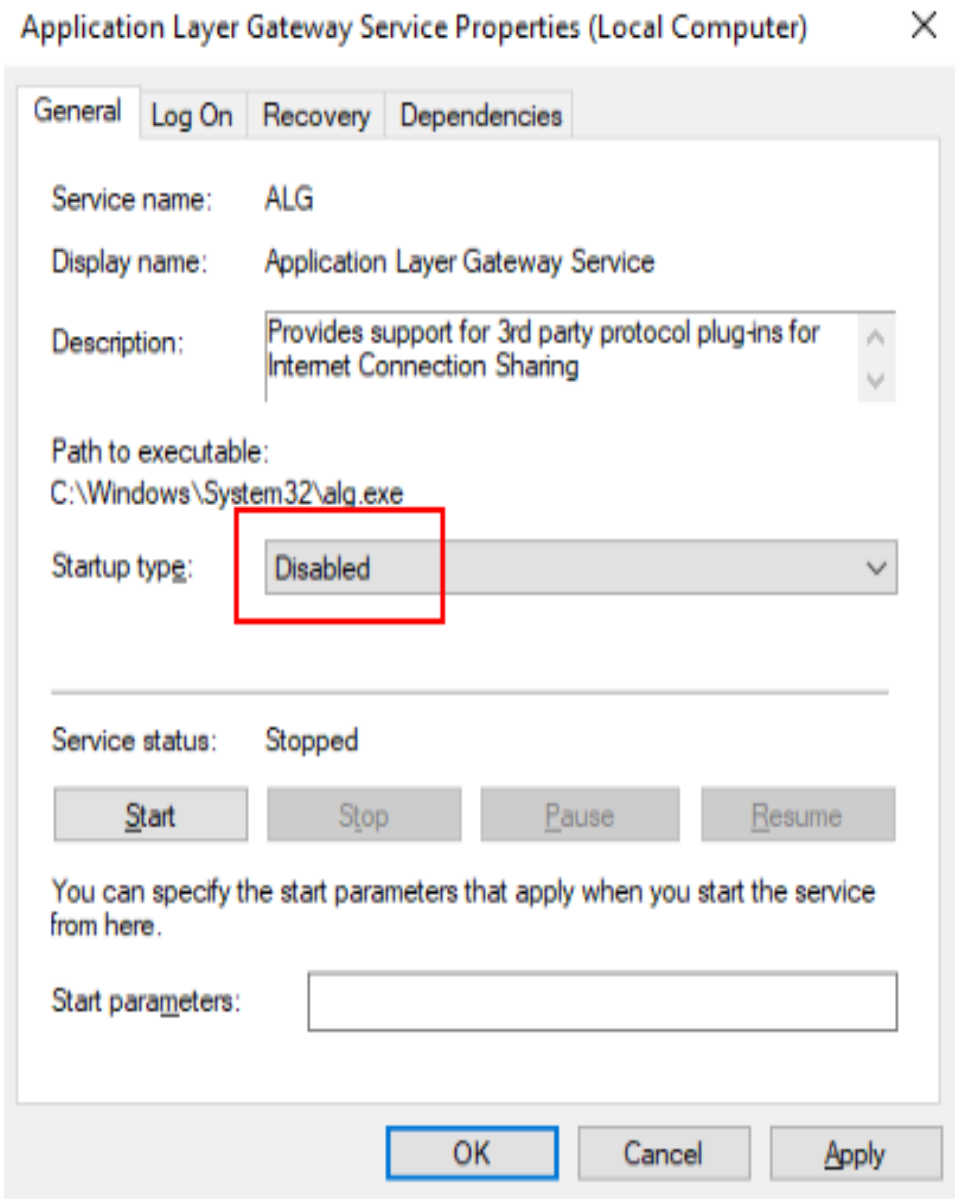
The **Services** window is displayed.

Step 36 In the right pane, double-click **Application Layer Gateway Service**.

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

Step 37 On the **General** tab, set **Startup type** to **Disabled**, as shown in **Figure 2-28**.

Figure 2-28 Configuring the startup type



Step 38 Click **OK**.

Step 39 Set the **Startup Type** of **Internet Connection Sharing (ICS)** and **Windows Firewall** to **Disabled** by referring to **Step 36** to **Step 38**.

NOTE

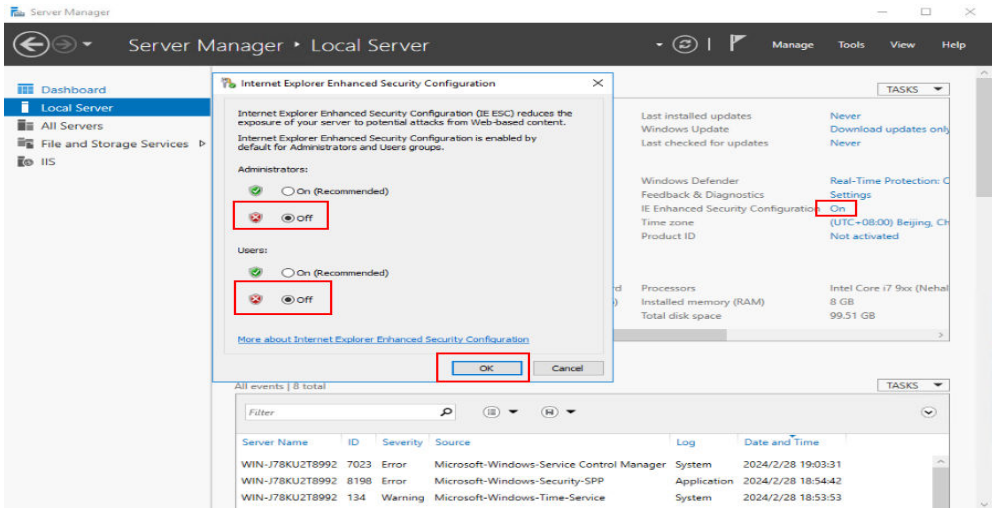
- The Windows firewall name varies with the OS version. The actual configured name is used. For example, **Windows Defender Firewall** is displayed on Windows Server 2019.
- You do not need to configure **Windows Defender Firewall** for Windows Server 2019.

Closing the Internet Explorer ESC on the server

Step 40 Click  to open the **Server Manager** page.

Step 41 Select **Local Server**. On the **Local Server** page, click current settings in the **Internet Explorer Enhanced Security Configuration** to open the property page. Select **Off** for the required user and click **OK**, as shown in **Figure 2-29**.

Figure 2-29 Modifying the Internet Explorer enhanced security configuration



Disabling Windows updates

Step 42 In the right pane of the **Services** window, double-click **Windows Update**.

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

Step 43 Set **Startup type** to **Disabled**.

Step 44 Click **OK**.

Configuring the remote desktop service

NOTE

- This operation ensures that each Windows ECS created using the image can be logged in to from the remote desktop.
- To use remote desktop connection, you need to **modify the group policy** of the remote desktop service.

Step 45 In the right pane of the **Services** window, right-click **Remote Desktop Services** and choose **Properties** from the shortcut menu.

The **Remote Desktop Services Properties (Local Computer)** window is displayed.

Step 46 On the **General** tab, set **Startup type** to **Automatic** and click **OK**.

Step 47 Close the **Services** window.

Enabling remote service connection

NOTE

After remote service connection is enabled, each Windows ECS created using the image can be accessed remotely.

Step 48 In the ECS, right-click  in the lower left corner and choose **Run** from the shortcut menu.

Step 49 In the **Run** dialog box, enter **sysdm.cpl** and press **Enter**.

The **System Properties** window is displayed.

Step 50 On the **Remote** tab, select **Allow remote connections to this computer**.

NOTE

For some OS types, if you select **Allow remote connections to this computer**, the remote desktop connection dialog box will be displayed. In this case, click **OK** to go to the next step.

Step 51 Click **OK**.

Remote desktop connection has been enabled.

Creating a temporary local admin user

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 52 Access the ECS, click  , enter **compmgmt.msc**, and press **Enter**. The **Computer Management** window is displayed.

Step 53 Choose **System Tools** > **Local Users and Groups** > **Users**.

Step 54 Right-click and choose **New User** from the shortcut menu.

Step 55 In the **New User** dialog box, enter the user name and password, confirm the password, and click **Create**.

Step 56 In the navigation pane, choose **Local Users and Groups** > **Groups**.

Step 57 Right-click **Administrators** and choose **Add to Group** from the shortcut menu.

Step 58 In the **Administrators Properties** dialog box, click **Add** to add the user to the group and click **OK**.

Step 59 Click **OK** and close the **Administrators Properties** dialog box.

Step 60 Close **Computer Management**.

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

Step 62 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 Huawei Cloud Private DNS Server Addresses?**

Step 63 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

Select the private DNS server address based on the region where the ECS is located. For details, see **What Are Huawei Cloud Private DNS Server Addresses?**

Obtaining required installation packages

Step 64 Upload the packages obtained in **2.17.1.1 Required Software**, except the OS ISO file, to the OBS bucket used in **2.17.1.2 Registering a Private Image Using an ISO File**.

NOTE

Set the object permission to **Public Read**.

Step 65 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 66 In the root directory of drive C on the ECS, create a folder, for example, **software**, for storing the package to be installed.

Step 67 Open the browser on the ECS, copy the package link recorded in **Step 65** 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 68 Copy the obtained software packages to the **C:\software** directory.

Installing the 7-Zip

Step 69 Go to **C:\software** to find and decompress the 7-Zip installation package.

Installing Visual Studio 2017 runtime library

Step 70 Go to **C:\software** to find the **vc_redist.x64.exe** and **vc_redist.x86.exe** packages, and double-click to install the Visual Studio 2017 runtime library.

Step 71 Restart the ECS.

(Optional) Installing the OS patch

Step 72 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.

Installing the GPU driver

NOTE

This configuration is required only for GPU feature usage.

Step 73 Go to **C:\software** where the driver is stored, start and install the driver as prompted.

(Optional) Installing applications

Step 74 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

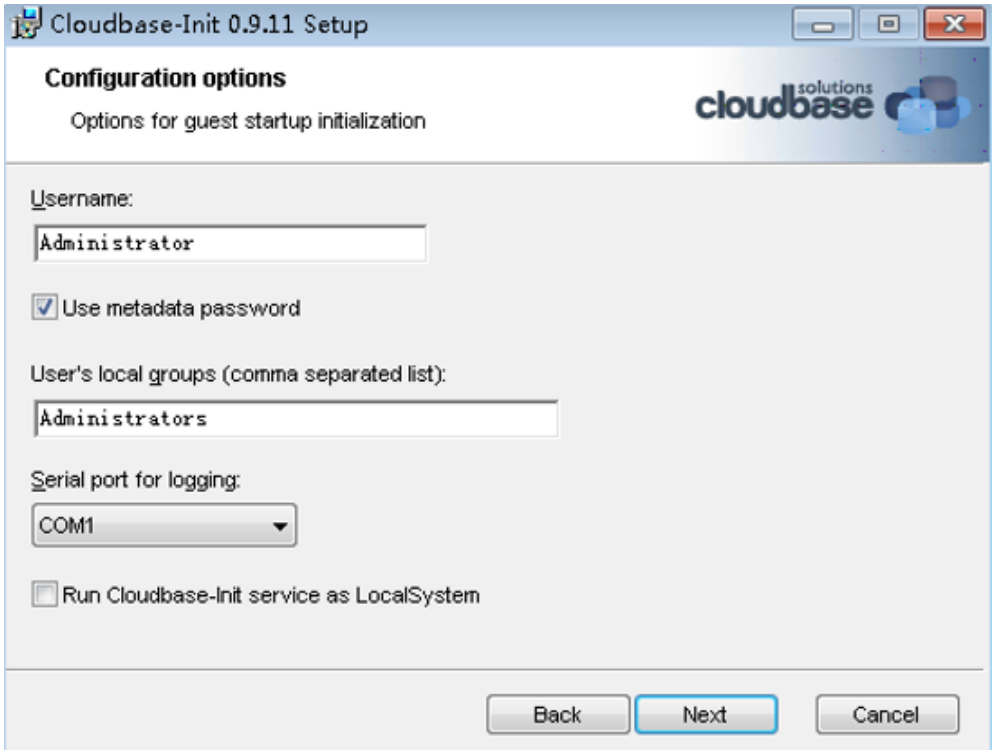
Step 75 Go to **C:\software** where the package is stored and install the peripheral driver as required.

Installing the Cloudbase-Init software

Step 76 Go to **C:\software** where the package is stored, open the Cloudbase-Init installation package, and install Cloudbase-Init as prompted.

Step 77 On the **Configuration options** page, configure parameters by referring to **Figure 2-30**.

Figure 2-30 Configuration options

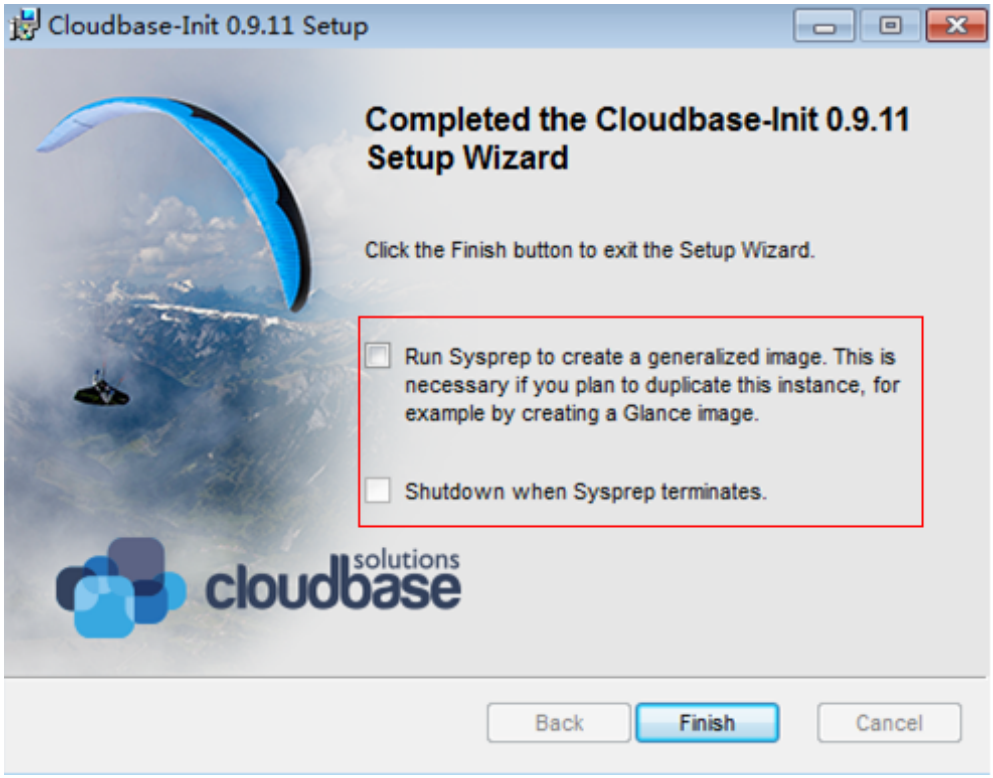


NOTE

Set parameters by referring to the following figure.

Step 78 After the configuration is complete, deselect the options shown in **Figure 2-31**.

Figure 2-31 Finish



Step 79 Click **Finish**.

Configuring Cloudbase-Init

Step 80 Edit the configuration file **C:\Program Files\Cloudbase Solutions\Cloudbase-Init\conf\cloudbase-init.conf** in the Cloudbase-Init installation path.

1. Add the configuration item **netbios_host_name_compatibility=false** 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 81 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.

Installing the password reset plug-in

Step 82 Install the ECS password reset plug-in by referring to .

Installing SysAgent and SysPrep

Step 83 Copy the **HW.SysAgent.Installer_64.msi** and **HW.SysPrep.Installer_64.msi** installation packages to the ECS.

Step 84 Double-click the **HW.SysAgent.Installer_64.msi** and **HW.SysPrep.Installer_64.msi** files to install them.

Installing WKSRStorageAgent component

Step 85 Copy the **WKSRStorageAgent_windows-amd64.msi** installation package to the ECS.

Step 86 Double-click the **WKSRStorageAgent_windows-amd64.msi** file to install it.

(Optional) Backing up an image

NOTE

After an image is encapsulated, if the ECS is stopped and restarted, the image is decapsulated and cannot be used directly. You need to configure and encapsulate the ECS again. If necessary, you can back up the ECS before encapsulation.

Step 87 On the ECS list page, locate the configured ECS and choose **More** > **Stop** to stop it.

Step 88 After the ECS is stopped, choose **More** > **Manage Image/Backup** > **Create Server Backup** to create an ECS backup.

Step 89 After the ECS backup is created, restart the ECS and perform encapsulation on the ECS.

Encapsulating an image

Step 90 On the ECS, find the Windows image creation tool in **C:\software** and decompress it to obtain the **Workspace_HDP_WindowsDesktop**_*XXX* folder.

Step 91 Right-click  in the lower left corner, enter **cmd**, and press **Enter**.

Step 92 Run the following command to switch to the directory containing the template tool:

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

Step 93 In the displayed CLI, run the following command to encapsulate the image:

To create a multi-session common/GPU image: **run_silent.bat --passive --environment_type 2 --hda_type 3 --nocheck -noshutdown**

To create a single-session common image: **run_silent.bat --passive --environment_type 2 --hda_type 1 --appmode --nocheck -noshutdown**

To create a single-session GPU image: **run_silent.bat --passive --hda_type 2 --environment_type 2 --appmode --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.

After the encapsulation tool displays a message indicating that the encapsulation is successful, you can close the tool.

Deleting the temporary admin user

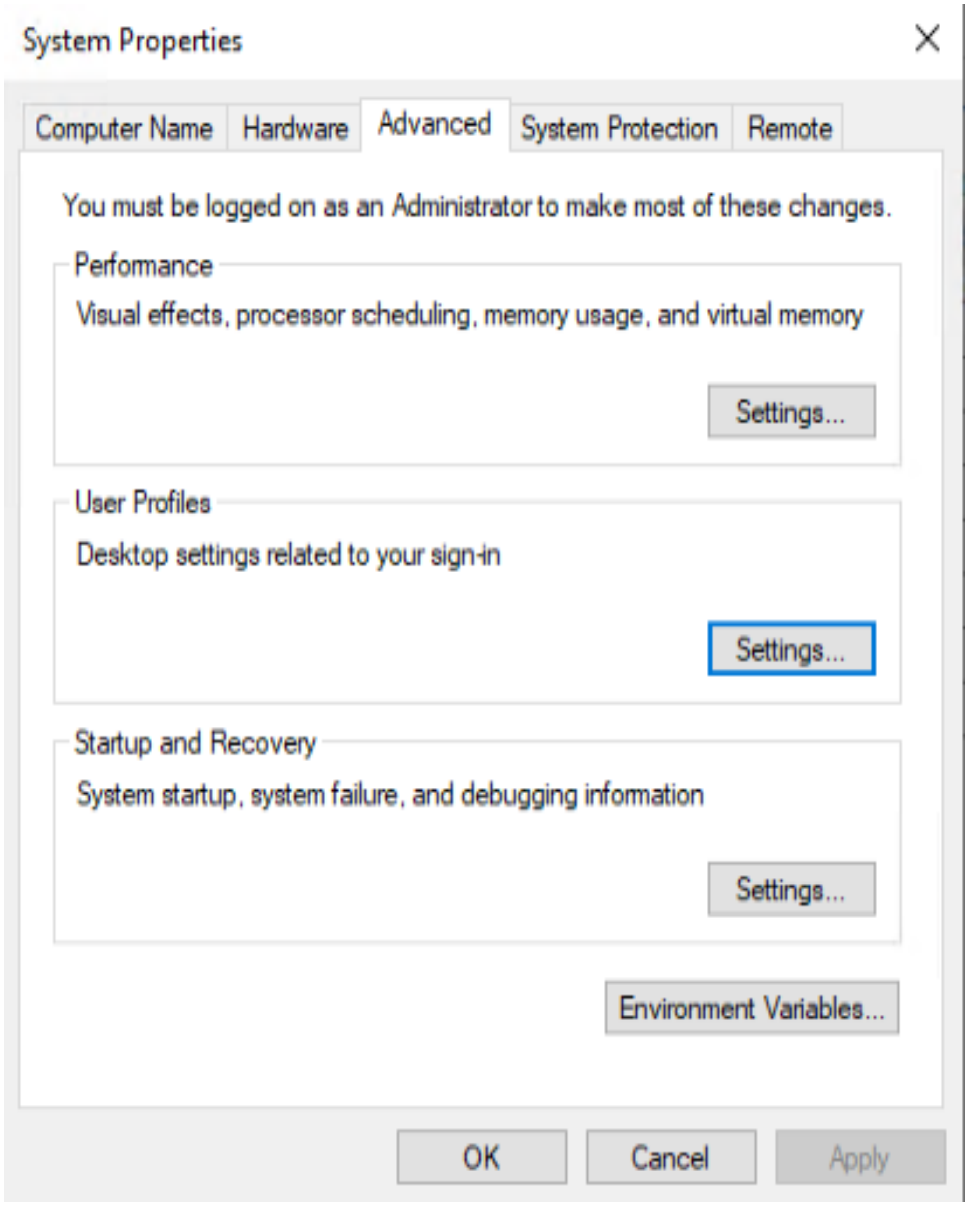
Step 94 Click **Start** > **Run**.

The **Run** dialog box is displayed.

Step 95 Enter **sysdm.cpl** in the **Open** text box and press **Enter**.

The **System Properties** dialog box is displayed.

Step 96 On the **Advanced** tab page, click **Settings** under **User Profiles**.



Step 97 On the **User Profiles** page, select the profiles of the user to be deleted and click **Delete**.

Step 98 Click **OK**.

Step 99 Close the **System Properties** window.

Step 100 Click **Start** > **Run**.

The **Run** dialog box is displayed.

Step 101 Enter **compmgmt.msc** in the **Open** text box and press **Enter**.

The **Computer Management** window is displayed.

Step 102 In the navigation pane on the left, choose **System Tools** > **Local Users and Groups** > **Users**.

Step 103 In the right pane, right-click the username to be deleted and choose **Delete**.

Step 104 In the displayed dialog box, click **Yes**.

Step 105 Click **OK**.

Step 106 Close the **Computer Management** window.

Stopping an ECS

Step 107 On the ECS list page of the console, locate the row that contains the ECS created in **2.17.1.3 Creating an ECS**, and choose **More** > **Stop** to stop the ECS.

----End

2.17.1.5 Creating a Basic Image for Workspace Application Streaming

Scenario

This section describes how to create a private image for Workspace Application Streaming.

Prerequisites

You have obtained the username and password for logging in to the console.

Procedure

Step 1 Log in to the cloud server 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/Backup** > **Create Image**.

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

- **Type**: Select **Create Image**.
- **Image Type**: Select **System disk image**.
- **Source**: ECS. Select an ECS that has been stopped in **2.17.1.4 Configuring an ECS**.

- **Name**: Configure this parameter based on the actual OS, for example, **Workspace_Image_01**.
- **Enterprise Project**: Select the enterprise project to which the resource belongs, for example, **default**.
- **Tag**: Set **Tag key** to **wks_biz_type** and set **Tag value** to **AppStream**.
- **Tag**: Set **Tag key** to **wks_hdp_mode**, set **Tag value** for single-session to **VDI**, and set **Tag value** for multi-session to **SBC**.

Step 5 Confirm the image parameters, select **I have read and agree to the Statement of Commitment to Image Creation and Image Disclaimer.**, and click **Next**.

Step 6 Click **Submit**.

Image creation takes about 10 to 15 minutes. The created image is displayed in the list under **Cloud Server Console** > **Image Management Service** > **Private Image**.

----End

2.18 Configuring Personalized Data

2.18.1 Configuring the Desktop Data Synchronization

Scenarios

You can use AD group policies to configure folder redirection policies to save users' files and configurations to a remote storage system. When a user logs in to the system, the user can directly read personal files from the remote file system.

Constraints

The file system need to support the SMB (CIFS) protocol.

Procedure

Purchasing a file storage server

Step 1 Purchase a cloud desktop or ECS as the file storage server.

In the current project, administrators can purchase a Windows desktop with a large disk capacity or a Windows ECS as the file storage server.

- Purchase a Windows desktop with a large disk capacity by referring to **Workspace Getting Started**.

  NOTE

  - Configure the data disk size as required. It is recommended that the data disk size be greater than 100 GB.
  - Cloud desktops and cloud applications in the same project are in the same domain. You do not need to manually add them to a domain.

- **Buy an ECS** and add the ECS to the domain of an APS by referring to **2.23.19 How Do I Add an ECS to the Domain of an APS?**.

NOTE

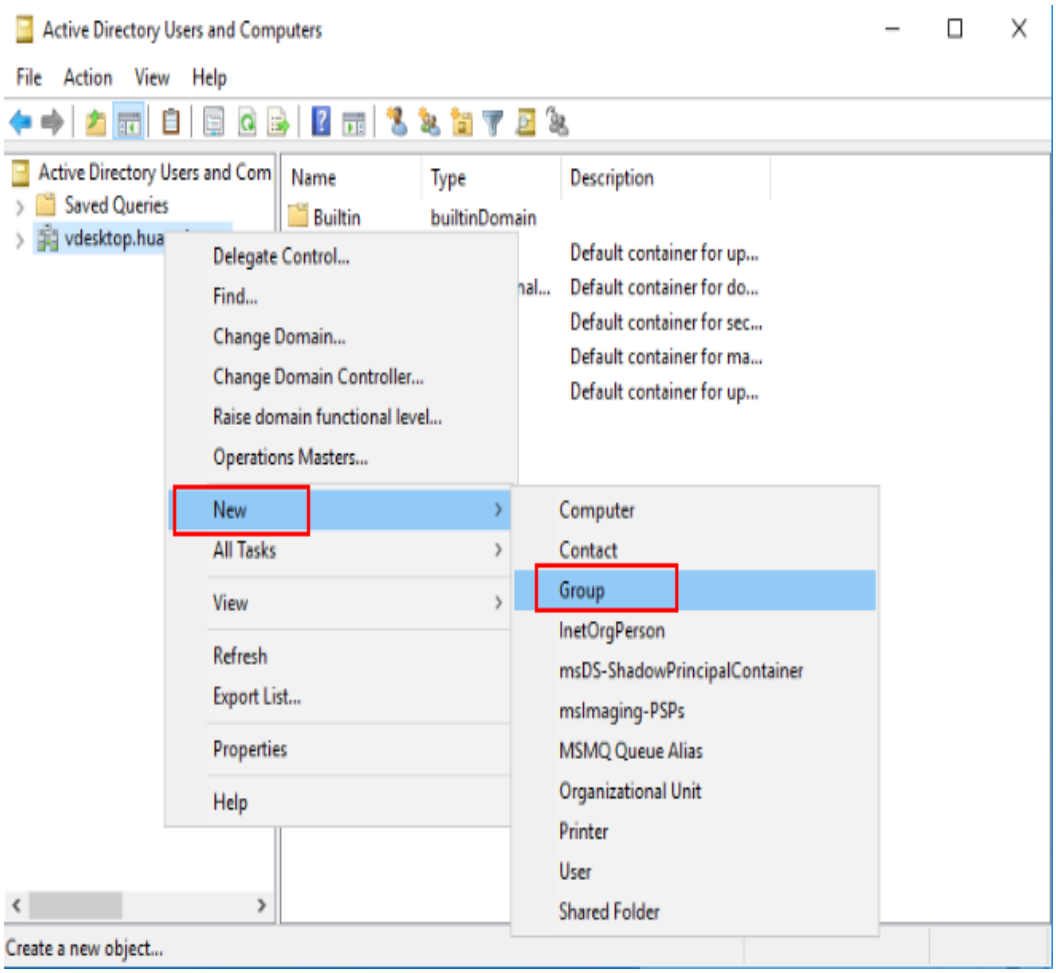
You are advised to purchase general computing-plus ECSs with **c6.4xlarge.4** or higher specifications, prepare sufficient bandwidth, and use data disks with ultra-high I/O or extreme SSD storage types.

Creating a folder redirection security group on the AD server

Step 2 Log in to the AD server and open the server manager.

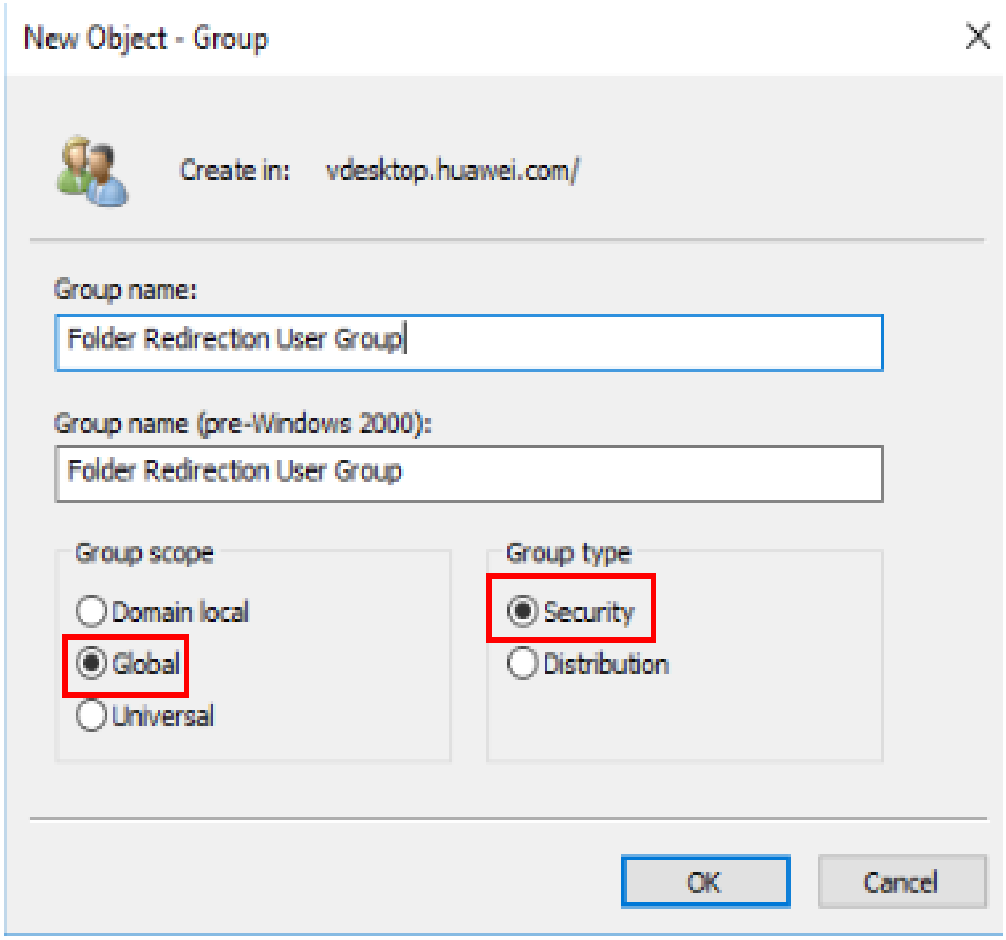
Step 3 Choose **Tools** > **Active Directory Users and Computers**.

Step 4 Right-click a domain or OU and choose **New** > **Group** from the shortcut menu.



Step 5 Enter group information.

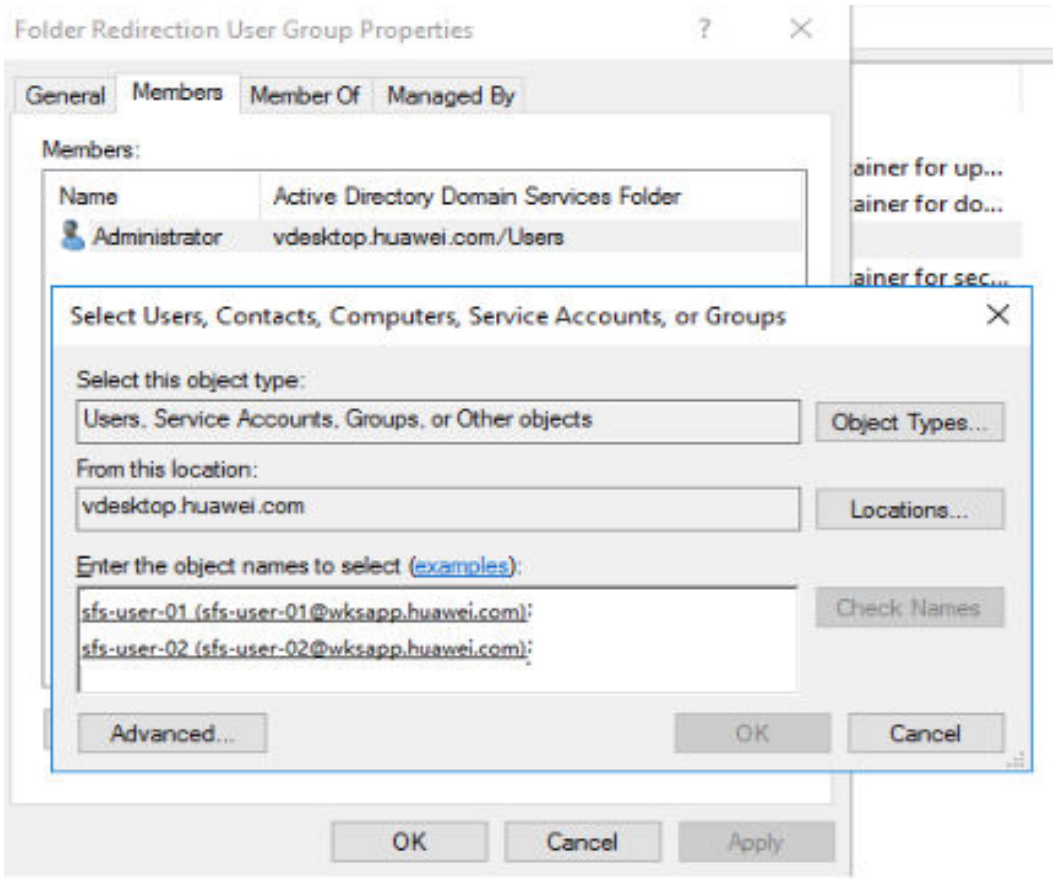
- Set a custom group name. For example, **Folder Redirection User Group**.
- Set **Group scope** to **Global**.
- Set **Group type** to **Security**.



Step 6 Click **OK**.

Step 7 Right-click the created user group and choose **Properties** from the shortcut menu.

Step 8 Switch to the **Members** tab and click **Add**.



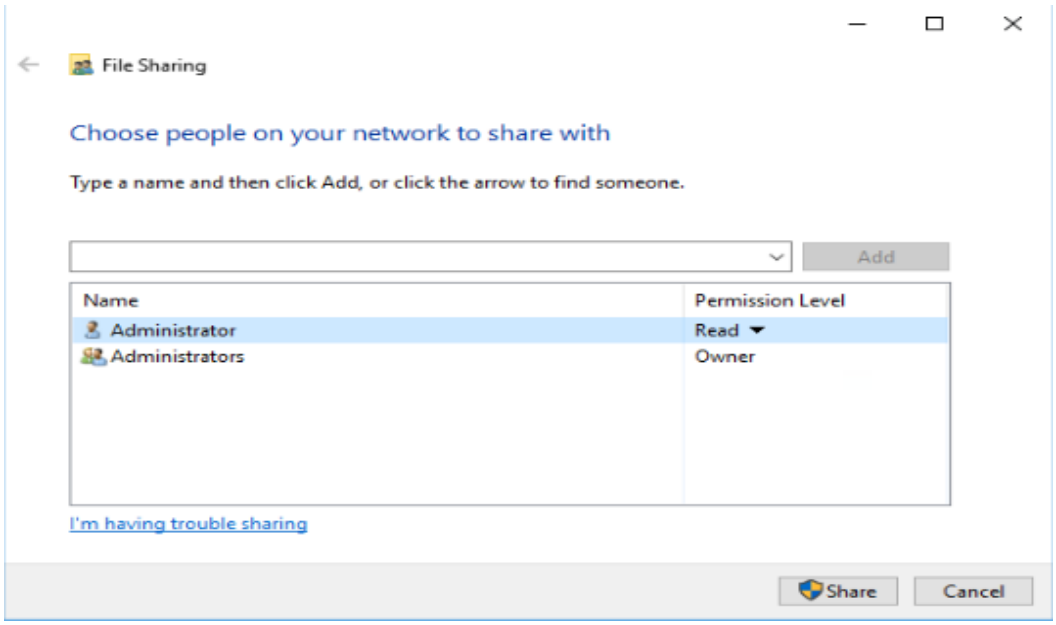
Step 9 Enter the user or group to be added to the folder redirection group, click **OK**, and then click **OK**.

Creating a shared folder on the file storage server

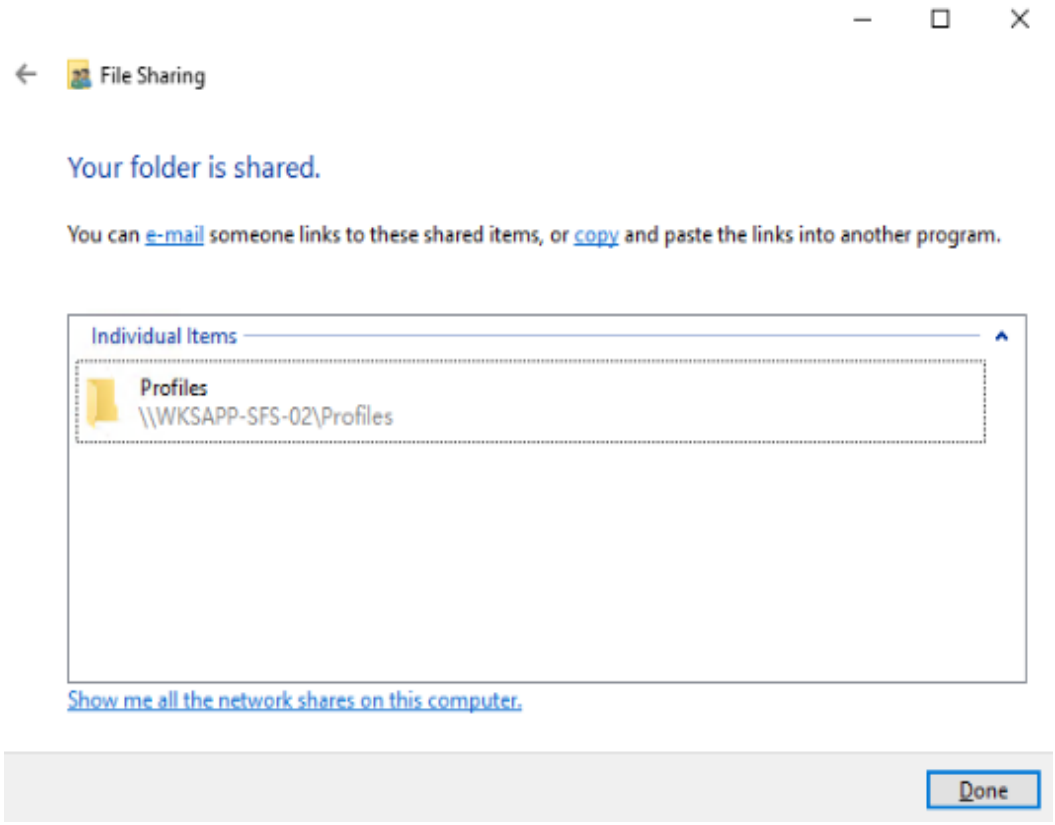
Step 10 Create a folder (for example, **Profiles**) in the root directory of the data disk on the file storage server.

Step 11 Right-click the new folder and choose **Share** > **Specific people** from the shortcut menu.

Step 12 Search for the security group created in the AD server in the step **Step 5** and add it to the share list.



Step 13 Click **Share**.

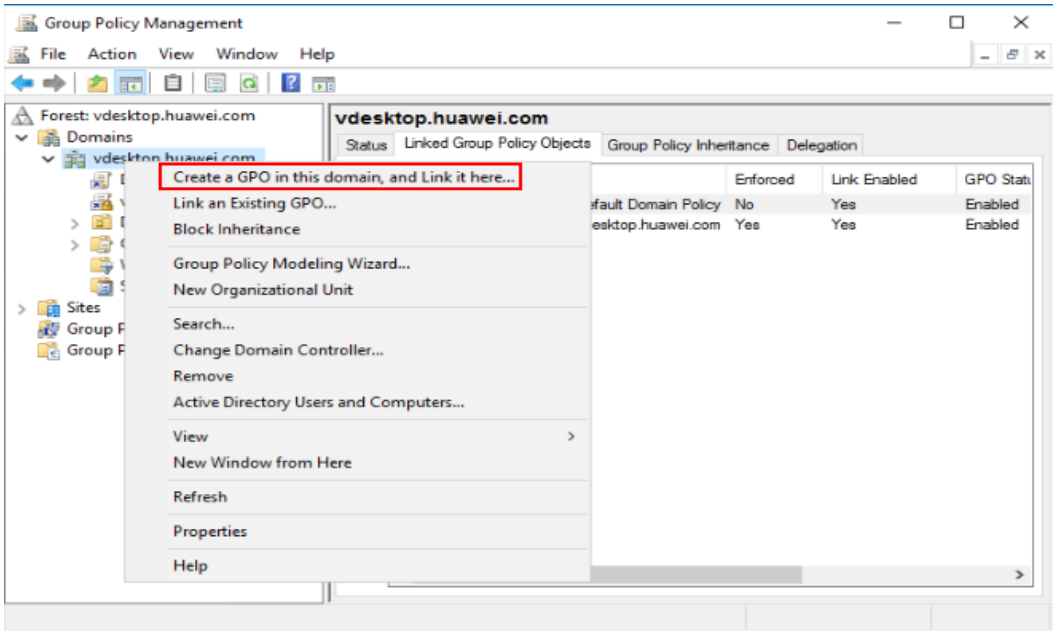


The generated shared directory **\WKSAPP-SFS-02\Profiles** is the UNC name of the shared folder.

Create a folder redirection GPO in the group policy management of the AD server.

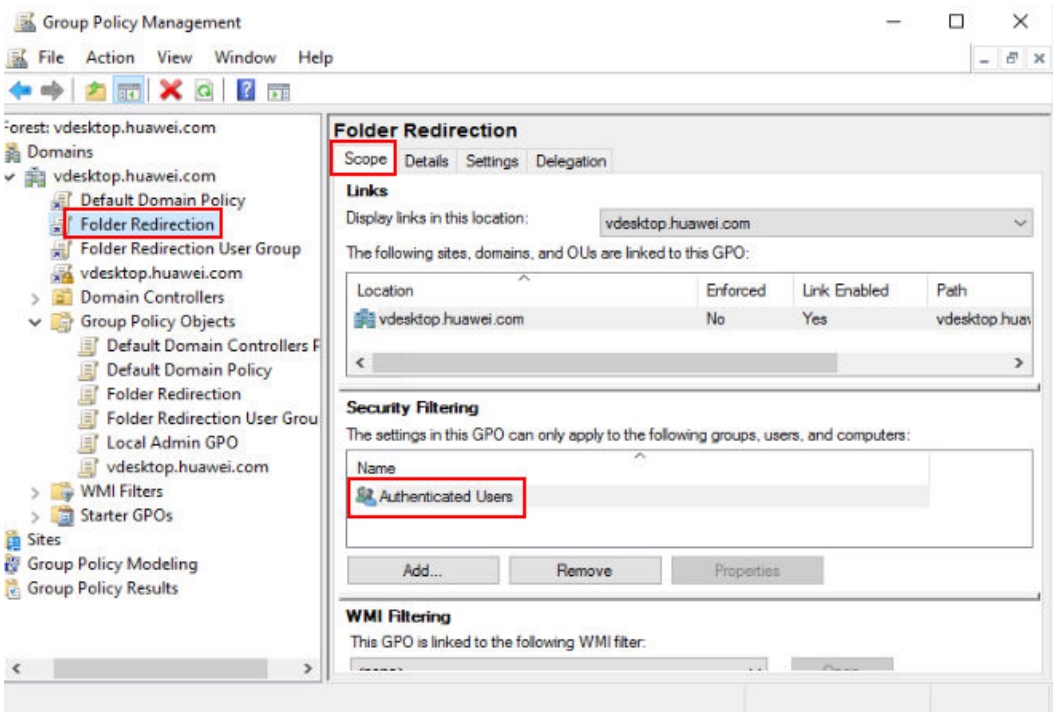
Step 14 Open the server manager on the AD server and choose **Tools** > **Group Policy Management**. The Group Policy Management page is displayed.

Step 15 Right-click the domain or OU in which you want to create a file redirection policy, and select **Create a GPO in this domain, and Link it here**.

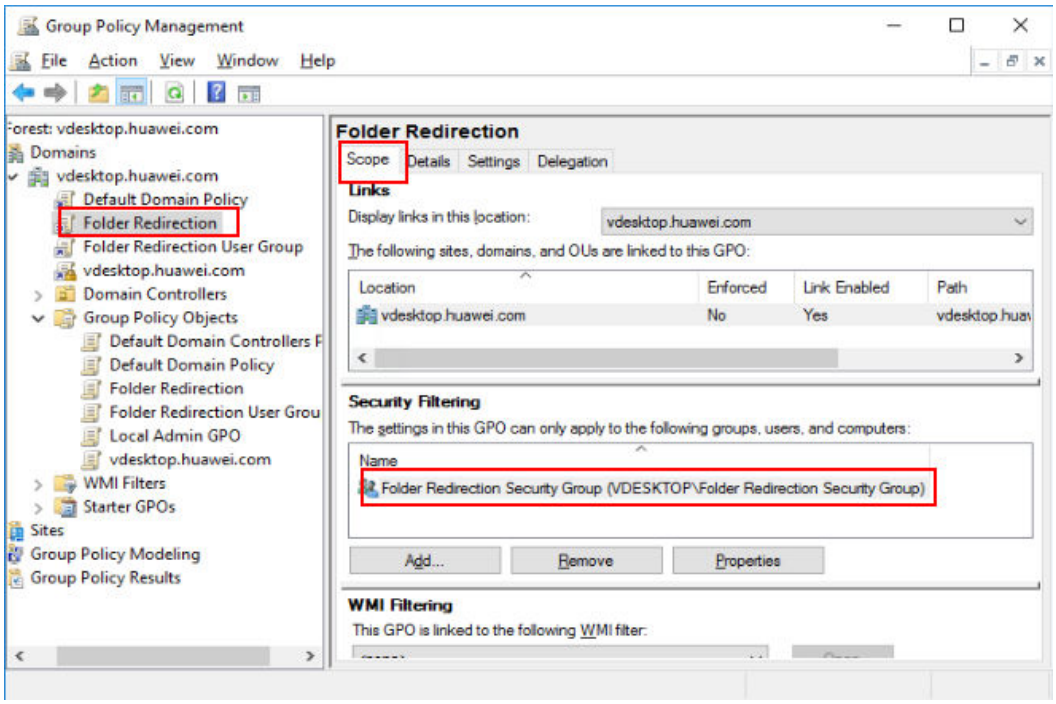


Step 16 In the displayed dialog box, enter the GPO name (for example, **Folder Redirection**) and click **OK**.

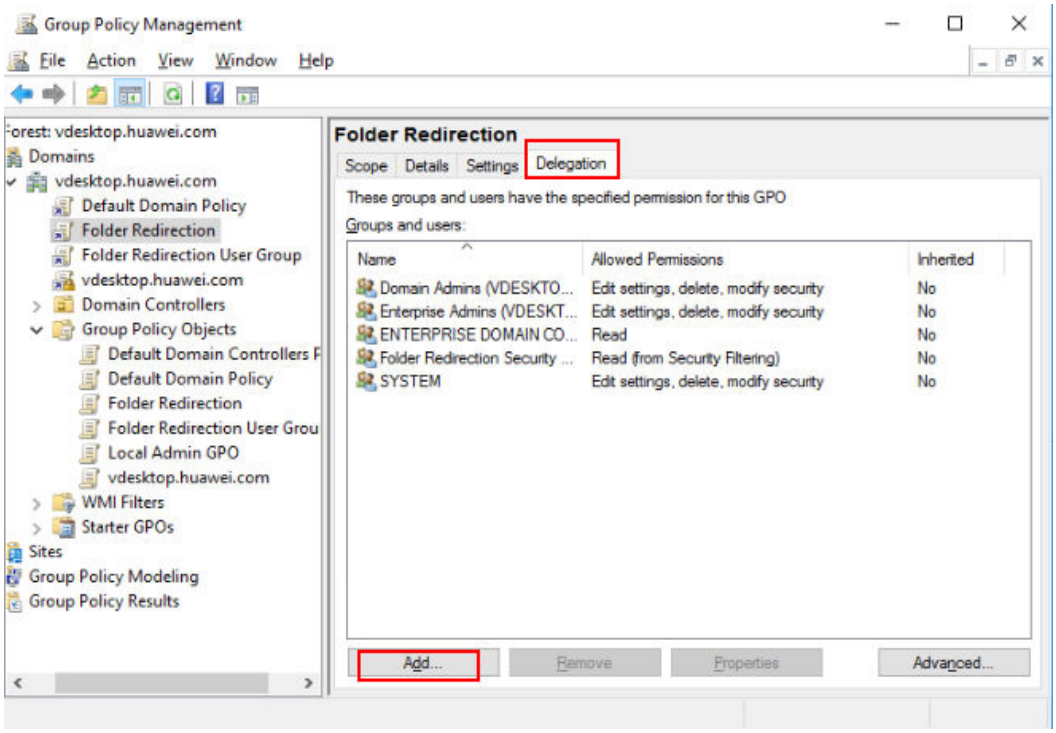
Step 17 Select the created GPO. In the right pane, choose **Scope** > **Security Filtering**. In the security filtering area, select **Authenticated Users** and click **Remove**.



Step 18 Click **Add**, search for the created user group, and click **OK** to add the user group to the list.

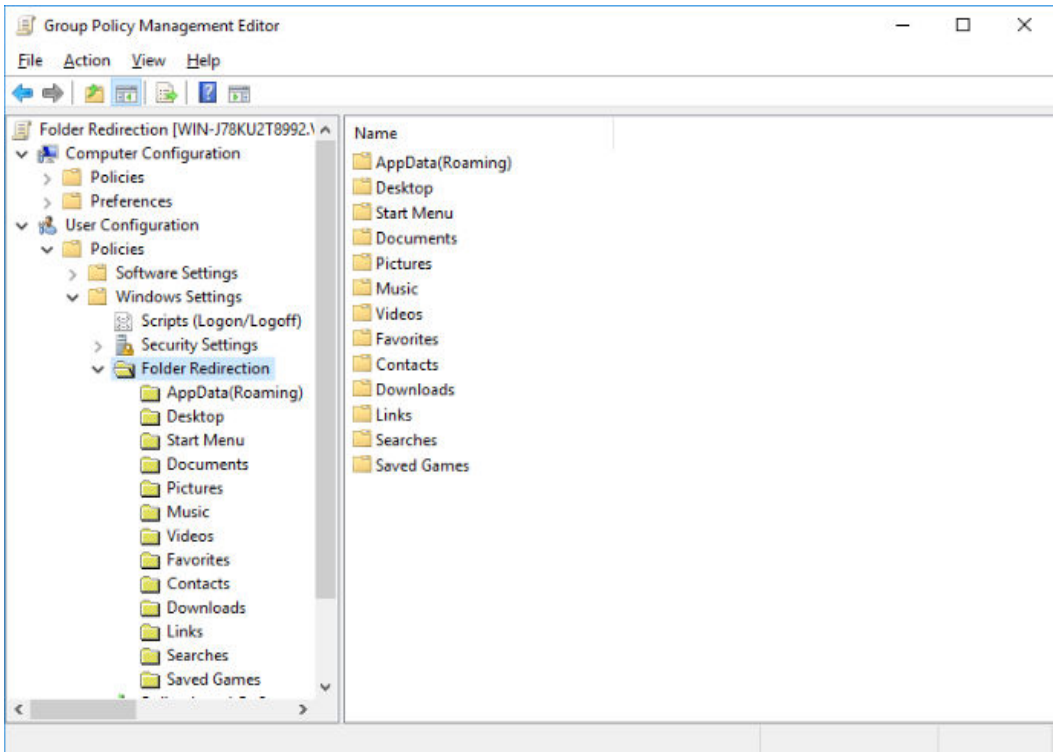


Step 19 Choose **Delegation** > **Add**, and enter **Authenticated Users**. Click **OK**, and then click **OK** again to accept the default read permission.



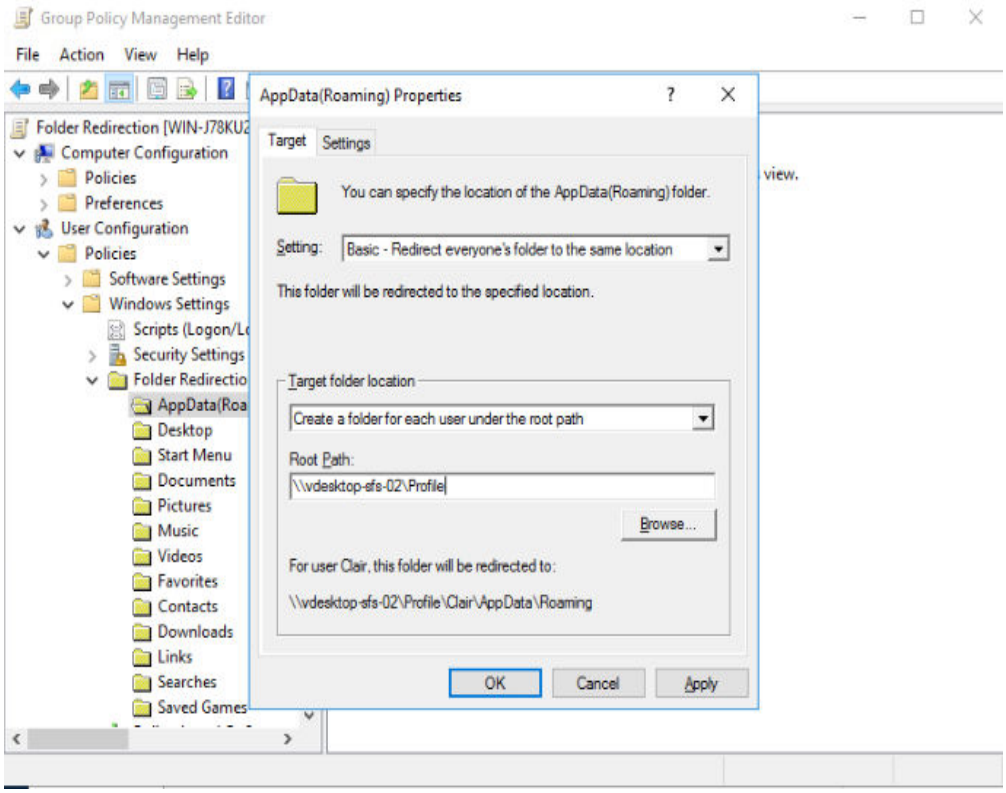
Configuring group policies for folder redirection GOP on the AD server

Step 20 Right-click the **Folder Redirection** GPO object and choose **Edit** from the shortcut menu. Choose **User Configuration** > **Policies** > **Windows Settings** > **Folder Redirection** on the displayed page.



Step 21 Right-click the folder to be redirected and choose **Properties** from the shortcut menu.

- In the **Target** tab page, set **Setting** to **Basic - Redirect everyone's folders to the same location**.
- Set **Root Path** to the UNC name of the shared folder generated in **Step 13**, for example, **\\WKSAPP-SFS-02\Profiles**.



Step 22 Click **OK**.

Testing the function of redirecting a user folder

Step 23 Log in to the computer in the domain using a user account that is configured to use the redirection folder. Then confirm the folders and configuration files that have been redirected.

If you have logged in to the computer before, open the command-line interface (CLI) and enter the following command to force the update:

gpupdate /force

Step 24 Log in to the file sharing server and check whether the corresponding folder is created in the shared directory.

----End

2.19 Subscribing to an Event

Scenarios

This section describes how to configure SMN to obtain server status information of cloud applications, such as creation, startup, shutdown, restarting, deletion, recomposing, upgrading, as well as image creation, and report the information to Cloud Trace Service (CTS) to improve the APS access speed and operation accuracy.

NOTE

Message queues may be blocked or CTS may fail to be called due to the event notification mechanism. Therefore, users cannot completely depend on event notifications. Instead, they need to periodically call APIs to update data. For details, see Workspace Application Streaming API Reference. 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_WorkspaceAPP**.
- Operation type: Select **Custom**. In the operation list, set **Select Service** to **WorkspaceAPP**, **Select Resource** to **server** or **session**, and **Select Operation** to **createServer**, **rebootServer**, **startServer**, **stopServer**, **deleteServer**, **reinstallServer**, **changeServerImage**, **createServerImage**, **sessionConnect**, **sessionDisconnect**, or **sessionLogout**.
- User: not specified.
- Notification: yes.
- Topic: Select the topic created in 2.

Verifying the subscription event

NOTE

- Whenever a cloud server is created, started, shut down, restarted, deleted, recomposed, or upgraded, whether successful or failed, an image is successfully created or fails to be created, or a session is connected, disconnected, or logged out, 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 console.

Step 6 Expand the service list and choose **Management & Governance** > **Cloud Trace Service**.

Step 7 On the **Trace List** page, set **Trace Source** to **WorkspaceAPP**, **Resource Type** to **server** or **session**, and search by **Trace Name**. The trace name is shown in **Table 2-30**.

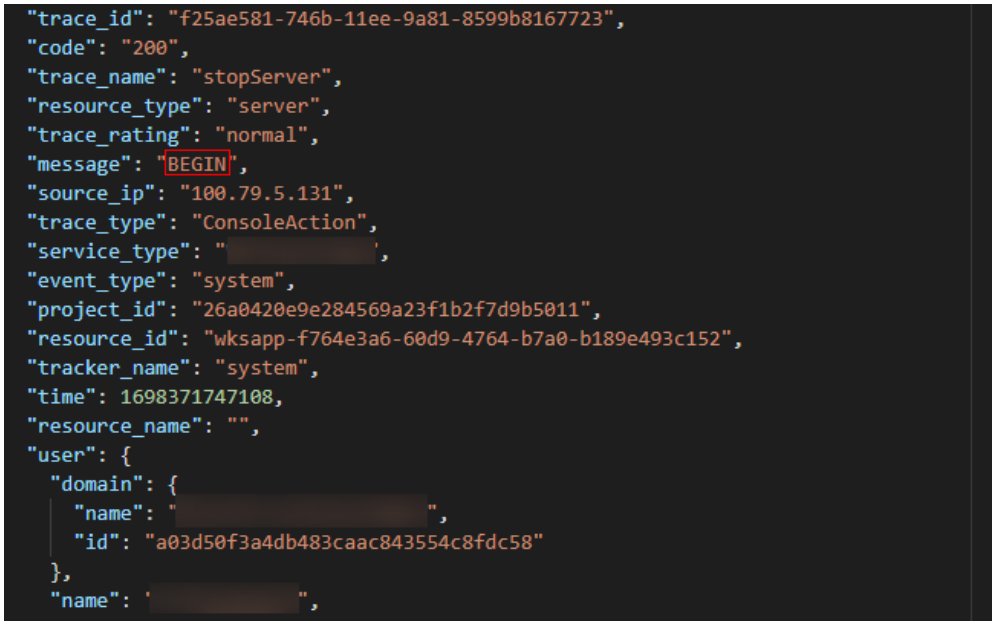
Table 2-30 Types of events that can be traced

Operation	Resource Type	Trace Name
Creating a server	server	createServer
Deleting a server	server	deleteServer
Shutting down a server	server	stopServer
Starting a server	server	startServer
Restarting a server	server	rebootServer
Creating an image	server	createServerImage
Upgrading an image	server	changeServerImage
Reinstalling a server	server	reinstallServer
Session connection	session	sessionConnect
Session disconnection	session	sessionDisconnect
Session logout	session	sessionLogout

Step 8 Press **Enter** to query the result.

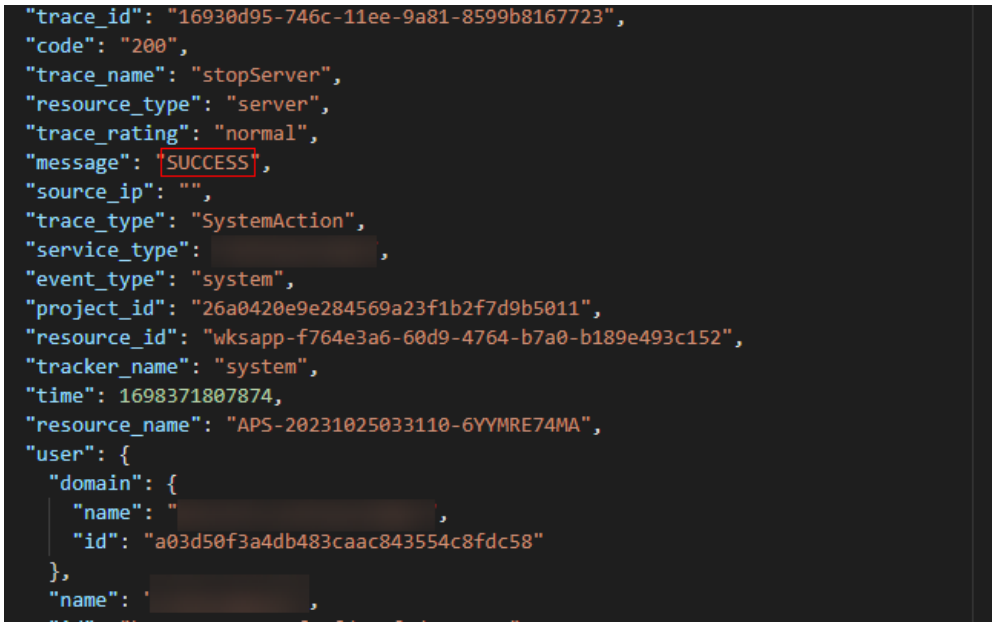
Step 9 Take shutting down a cloud server as an example. View **Trace Overview** of the event. The status is **BEGIN**, as shown in **Figure 2-32**.

Figure 2-32 Starting to shut down a server



Step 10 View **Trace Overview** of the shutdown event. The server has been shut down, as shown in **Figure 2-33**.

Figure 2-33 Server shut down



NOTE

- When server creation or deletion fails, a failure trace is reported. In the trace details, the value of **Message** is **FAIL**.
- If a server is powered off or not shut down on the homepage of the Workspace client, it is shut down abnormally. In this case, the **BEGIN** message is not reported in CTS. Only the message indicating that the server has been shut down will be reported.
- Three minutes after the server is started, if the login status is not **Ready** on the server management page, a failure trace is reported. In the trace details, the value of **Message** is **FAIL**.
- Three minutes after the server is shut down, if the login status is not **Stopped** on the server management page, a failure trace is reported. In the trace details, the value of **Message** is **FAIL**.

----End

2.20 Permissions Management

2.20.1 Permission Management

NOTE

- The Identity and Access Management (IAM) service is used to manage the permissions for accessing cloud services and resources.
- Workspace Application Streaming is a regional project. You can create multiple IAM user groups and grant them the Workspace Application Streaming administrator permissions of different projects to manage users' access to Workspace Application Streaming resources.
- If your Huawei Cloud account does not require individual IAM users for permissions management, skip this section.

Related Concepts

IAM is a free service. You pay only for the resources in your account. For details about IAM, see **IAM Service Overview**.

Account

An account is created after you successfully sign up for Huawei Cloud, and you can use it to purchase Huawei Cloud resources. The account has full access permissions for your cloud resources and can be used to make payments for them. You can use the account to reset user passwords, assign permissions, and receive and pay all bills generated by your IAM users for their usage of resources.

You cannot modify or delete your account in IAM, but you can do so in **My Account**.

IAM user

You can use your account to create IAM users and assign permissions for specific resources. Each IAM user has their own identity credentials (passwords or access keys) and uses cloud resources based on 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. New IAM users do not have any permissions assigned by default. You need to add them to one or more groups. The users then inherit permissions from the groups and can perform specified operations on resources or cloud services based on the permissions they have been assigned. If you add a user to multiple user groups, the user inherits all the permissions that are assigned to these groups.

The default user group **admin** has all the permissions for using all of the cloud resources. IAM 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.

Enterprise project permissions

For details, see **Enterprise Project Permissions**.

Workspace Application Streaming Administrator Permissions

You can grant users permissions by using roles and policies. Workspace Application Streaming grants administrator permissions to IAM users by using roles. If Workspace Application Streaming and Workspace use the same project, they share one user list. When a user group of Workspace Application Streaming is granted permissions, a user group of Workspace also has these permissions.

By default, new IAM users do not have permissions assigned. You need to add a user to one or more groups, and grant Workspace Application Streaming administrator permissions to these groups. Users inherit permissions from their groups. After being granted permissions, IAM users can perform operations on Workspace Application Streaming resources in the corresponding projects.

See **Table 2-31**. In **Table 2-32**, the **Dependent System-defined Role, Policy, or Custom Policy** column indicates roles on which a Workspace Application Streaming permission depends to take effect. Workspace Application Streaming

roles are dependent on the roles of other services because Huawei Cloud services interact with each other. Therefore, when assigning Workspace Application Streaming permissions to a user group, do not deselect other dependent permissions. Otherwise, Workspace Application Streaming permissions do not take effect.

Table 2-31 Workspace Application Streaming system-defined permissions

System-defined Permission	Description	Details
Workspace FullAccess	All permissions for Workspace Application Streaming	All permissions for Workspace Application Streaming
Workspace AppManager	Application administrator permissions for Workspace Application Streaming	Cloud application-related operations, including creating and deleting an application, and operations such as accessing the Internet and performing scheduled tasks
Workspace UserManager	User administrator permissions for Workspace Application Streaming	User management operations, such as creating users, deleting users, and resetting passwords
Workspace SecurityManager	Security administrator permissions for Workspace Application Streaming	All security-related operations, such as policy management and user connection recording
Workspace TenantManager	Tenant administrator permissions for Workspace Application Streaming	All tenant configuration functions
Workspace ReadOnlyAccess	Read-only permissions for Workspace Application Streaming	Read-only permissions for Workspace Application Streaming

Table 2-32 lists the permissions to be added for the following operations.

NOTE

For details about the dependent permissions of Workspace Application Streaming, see **Assigning Permissions to an IAM User** or **Creating a Custom Policy**.

Table 2-32 Additional permissions required for Workspace Application Streaming

Operation	Dependencies	Description
BSS-related permissions: for yearly/monthly operations, such as purchasing and changing resources, and switching from pay-per-use to yearly/monthly. You need to view the renewal information management permission when querying the number of applications to be renewed on the **Overview** page.	The policy must contain the following action permissions: bss:discount:view bss:order:update bss:order:view bss:order:pay bss:renewal:view	-
IAM-related permissions: for creating and querying agencies in a scheduled task	**Permissions required for creating and querying agencies:** The policy must contain the following action permissions: iam:roles:getRole iam:roles:listRoles iam:agencies:getAgency iam:agencies:listAgencies iam:agencies:createAgency iam:permissions:listRolesForAgencyOnProject iam:permissions:grantRoleToAgencyOnProject **Permissions required for querying agencies:** The policy must contain the following action permissions: iam:agencies:getAgency iam:agencies:listAgencies iam:permissions:listRolesForAgencyOnProject	-
TMS-related permissions: for querying predefined tags during application creation	The policy must contain the following action permissions: tms:predefineTags:list	TMS-related permissions do not support enterprise project authorization.

Operation	Dependencies	Description
VPCEP-related permissions: for enabling or disabling Direct Connect access (required for fine-grained authentication of enterprise projects).	System-defined role: VPCEndpoint Administrator	VPCEP does not support fine-grained authentication of enterprise projects.
VPC-related permissions: for creating images, application groups, and server groups, performing related operations, and enabling economical Internet access (required for fine-grained authentication of enterprise projects).	IAM project-level permissions System-defined policy: VPC ReadOnlyAccess System-defined role: VPC Administrator	You must have the VPC permission of the enterprise project to which the VPC used for enabling Workspace Application Streaming belongs.
IMS-related permissions: for creating images, server groups, and performing operations on server groups (required for fine-grained authentication of enterprise projects).	The policy must contain the following action permissions: ims:images:get ims:images:share	IMS does not support fine-grained authentication of enterprise projects.

2.20.2 Creating a Custom Policy

Scenarios

Custom policies can be created as a supplement to the system permissions of Workspace.

You can create custom policies in either of the following ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Create a JSON policy or edit an existing one.

For details about how to create custom policies, see **Creating a Custom Policy**. The section contains examples of common Workspace custom policies.

Policy Examples

- Example 1: Assigning the permissions for desktop startup and shutdown to users.

```
{
   "Version": "1.1",
   "Statement": [
      {
```



```
        "Effect": "Allow",
        "Action": [
            "workspace:*:get*",
            "workspace:*:list*",
            "workspace:*:export*",
            "ims:images:get",
            "ims:images:list",
            "ims:quotas:get",
            "nat:natGateways:list",
            "nat:snatRules:list",
            "vpc:bandwidths:list",
            "vpc:networks:get",
            "vpc:ports:get",
            "vpc:publicIps:get",
            "vpc:publicIps:list",
            "vpc:quotas:list",
            "vpc:securityGroupRules:get",
            "vpc:securityGroups:get",
            "vpc:subnets:get",
            "vpc:vpcs:get",
            "vpc:vpcs:list",
            "vpcep:endpoints:get",
            "dss:pools:list",
            "workspace:desktops:operate"
        ]
    }
  ]
}
```

2.20.3 Permissions and Supported Actions

This section describes fine-grained permissions management for your Workspace Application Streaming. If your account does not need individual IAM users, you can skip this section.

By default, new IAM users do not have permissions assigned. You need to add a user to one or more groups, and attach permissions policies or roles to these groups. Users inherit permissions from the groups to which they are added and can perform specified operations on cloud services based on the permissions.

You can grant users permissions by using roles and policies. Roles are a type of coarse-grained authorization mechanism that defines permissions related to user responsibilities. Policies define API-based permissions for operations on specific resources under certain conditions, allowing for more fine-grained, secure access control of cloud resources.

NOTE

Policy-based authorization is useful if you want to allow or deny the access to an API.

Supported Actions

You can create custom policies for more specific access control. Operations supported by policies are specific to APIs. The following are common concepts related to policies:

- Permissions: Statements in a policy that allow or deny certain operations.
- APIs: REST APIs that can be called by a user who has been granted specific permissions.

- Actions: Specific operations that are allowed or denied.
- Related actions: Actions on which a specific action depends to take effect. When assigning permissions for the action to a user, you also need to assign permissions for the related actions.
- IAM projects or enterprise projects: Applicable scope of custom policies. Policies that contain actions for both IAM and enterprise projects can be used and take effect for both IAM and Enterprise Management. Policies that only contain actions for IAM projects can be used and only take effect for IAM. For details about the differences between IAM projects and enterprise projects, see **What Are the Differences Between IAM and Enterprise Management?**

Action	API Method	API	Supported Action	IAM Project	Enterprise Project
workspace:appGroup:list	GET	/v1/{project_id}/app-groups	Query application groups	√	x
workspace:appGroup:create	POST	/v1/{project_id}/app-groups	Create an application group	√	x
workspace:appGroup:delete	DELETE	/v1/{project_id}/app-groups/{app_group_id}	Delete an application group	√	x
workspace:appGroup:get	GET	/v1/{project_id}/app-groups/{app_group_id}	Query application group details	√	x
workspace:appGroup:update	PATCH	/v1/{project_id}/app-groups/{app_group_id}	Modify an application group	√	x
workspace:app:listPublishedApp	GET	/v1/{project_id}/app-groups/{app_group_id}/apps	Query published applications	√	x

Action	API Method	API	Supported Action	IAM Project	Enterprise Project
workspace:app:publish	POST	/v1/{project_id}/app-groups/{app_group_id}/apps	Publish an application	√	x
workspace:app:get	GET	/v1/{project_id}/app-groups/{app_group_id}/apps/{app_id}	Query application details	√	x
workspace:app:update	PATCH	/v1/{project_id}/app-groups/{app_group_id}/apps/{app_id}	Modify application information	√	x
workspace:app:deleteIcon	DELETE	/v1/{project_id}/app-groups/{app_group_id}/apps/{app_id}/icon	Delete a custom application icon	√	x
workspace:app:uploadIcon	POST	/v1/{project_id}/app-groups/{app_group_id}/apps/{app_id}/icon	Modify a custom application icon	√	x
workspace:app:check	POST	/v1/{project_id}/app-groups/{app_group_id}/apps/actions/check	Verify an application	√	x
workspace:app:batchDisable	POST	/v1/{project_id}/app-groups/{app_group_id}/apps/actions/disable	Disable applications in batches	√	x
workspace:app:batchEnable	POST	/v1/{project_id}/app-groups/{app_group_id}/apps/actions/enable	Enable applications in batches	√	x

Action	API Method	API	Supported Action	IAM Project	Enterprise Project
workspace:app:unpublish	POST	/v1/{project_id}/app-groups/{app_group_id}/apps/batch-unpublish	Unpublish applications in batches	√	x
workspace:appGroup:listPublishableApp	GET	/v1/{project_id}/app-groups/{app_group_id}/publishable-app	Publishable applications	√	x
workspace:appGroup:batchDeleteAuthorization	POST	/v1/{project_id}/app-groups/actions/batch-delete-authorization	Cancel application group authorization	√	x
workspace:appGroup:disassociate	POST	/v1/{project_id}/app-groups/actions/disassociate-app-group	Disassociate a service group from all application groups	√	x
workspace:appGroup:listAuthorization	GET	/v1/{project_id}/app-groups/actions/list-authorizations	Query application group authorization records	√	x
workspace:appGroup:addAuthorization	POST	/v1/{project_id}/app-groups/authorizations	Add application group authorization	√	x

Action	API Method	API	Supported Action	IAM Project	Enterprise Project
workspace:appGroup:batchDelete	POST	/v1/{project_id}/app-groups/batch-delete	Delete application groups in batches	√	x
workspace:appGroup:check	POST	/v1/{project_id}/app-groups/rules/validate	Verify an application group	√	x
workspace:serverGroup:list	GET	/v1/{project_id}/app-server-groups	Query server groups	√	√
workspace:serverGroup:create	POST	/v1/{project_id}/app-server-groups	Create a server group	√	√
workspace:serverGroup:delete	DELETE	/v1/{project_id}/app-server-groups/{server_group_id}	Delete a server group	√	√
workspace:serverGroup:get	GET	/v1/{project_id}/app-server-groups/{server_group_id}	Query a specified server group	√	√
workspace:serverGroup:update	PATCH	/v1/{project_id}/app-server-groups/{server_group_id}	Modify a server group	√	√
workspace:serverGroup:getServerState	GET	/v1/{project_id}/app-server-groups/{server_group_id}/state	Query server statuses in a specified server group	√	√

Action	API Method	API	Supported Action	IAM Project	Enterprise Project
workspace:serverGroup:listDetail	GET	/v1/{project_id}/app-server-groups/actions/list	Query basic information about a tenant server group	√	√
workspace:serverGroup:getRestrict	GET	/v1/{project_id}/app-server-groups/resources/restrict	Query specified tenant server groups	√	x
workspace:serverGroup:validate	POST	/v1/{project_id}/app-server-groups/rules/validate	Verify a server group	√	x
workspace:serverGroup:tagResource	POST	/v1/{project_id}/server-group/{server_group_id}/tags/create	Add a tag to a server group	√	√
workspace:serverGroup:unTagResource	DELETE	/v1/{project_id}/server-group/{server_group_id}/tags/delete	Delete a tag from a server group	√	√
workspace:serverGroup:listTagsForResource	GET	/v1/{project_id}/server-group/{resource_id}/tags	Query server group tags	√	√
workspace:serverGroup:listTags	GET	/v1/{project_id}/server-group/tags	Query tags on all servers of a tenant	√	√

Action	API Method	API	Supported Action	IAM Project	Enterprise Project
workspace:serverGroup:batchCreateTags	POST	/v1/{project_id}/server-group/tags/batch-create	Add server group tags in batches	√	√
workspace:serverGroup:batchDeleteTags	POST	/v1/{project_id}/server-group/tags/batch-delete	Delete server group tags in batches	√	√
workspace:server:list	GET	/v1/{project_id}/app-servers	Query servers	√	√
workspace:server:delete	DELETE	/v1/{project_id}/app-servers/{server_id}	Delete a server	√	√
workspace:server:get	GET	/v1/{project_id}/app-servers/{server_id}	Query a specified server	√	√
workspace:server:update	PATCH	/v1/{project_id}/app-servers/{server_id}	Modify a server	√	√
workspace:server:changeImage	POST	/v1/{project_id}/app-servers/{server_id}/actions/change-image	Modify a server image	√	√
workspace:server:reinstall	POST	/v1/{project_id}/app-servers/{server_id}/actions/reinstall	Reinstall a server	√	√
workspace:server:getVncUrl	GET	/v1/{project_id}/app-servers/{server_id}/actions/vnc	Obtain a VNC login address	√	√

Action	API Method	API	Supported Action	IAM Project	Enterprise Project
workspace:accessAgent:list	GET	/v1/{project_id}/app-servers/access-agent/actions/show-latest-version	Query the latest versions of all HDAs of a tenant	√	x
workspace:accessAgent:batchUpgrade	PATCH	/v1/{project_id}/app-servers/access-agent/actions/upgrade	Upgrade the HDA version of servers in batches	√	√
workspace:accessAgent:listLatestVersion	GET	/v1/{project_id}/app-servers/access-agent/latest-version	Query the latest HDA version of a tenant	√	x
workspace:server:listAccessAgentDetails	GET	/v1/{project_id}/app-servers/access-agent/list	Query HDA information of a server	√	√
workspace:accessAgent:getUpgradeFlag	GET	/v1/{project_id}/app-servers/access-agent/upgrade-flag	Query HDA upgrade notification flags	√	x

Action	API Method	API	Supported Action	IAM Project	Enterprise Project
workspace:accessAgent:updateUpgradeFlag	PATCH	/v1/{project_id}/app-servers/access-agent/upgrade-flag	Update an HDA upgrade notification flag	√	x
workspace:accessAgent:listUpgradeRecords	GET	/v1/{project_id}/app-servers/access-agent/upgrade-record	Query HDA upgrade tracing records of a server	√	x
workspace:server:batchDelete	POST	/v1/{project_id}/app-servers/actions/batch-delete	Delete servers in batches	√	√
workspace:server:batchChangeMaintainMode	PATCH	/v1/{project_id}/app-servers/actions/batch-maint	Mark the server maintenance status	√	√
workspace:server:batchReboot	PATCH	/v1/{project_id}/app-servers/actions/batch-reboot	Restart a server	√	√
workspace:server:batchRejoinDomain	PATCH	/v1/{project_id}/app-servers/actions/batch-rejoin-domain	Rejoin servers to a domain in batches	√	√
workspace:server:batchStart	PATCH	/v1/{project_id}/app-servers/actions/batch-start	Start a server	√	√

Action	API Method	API	Supported Action	IAM Project	Enterprise Project
workspace:server:batchStop	PATCH	/v1/{project_id}/app-servers/actions/batch-stop	Stop a server	√	√
workspace:server:batchUpdateTsvi	PATCH	/v1/{project_id}/app-servers/actions/batch-update-tsvi	Update virtual session IP configurations of servers in batches	√	√
workspace:server:create	POST	/v1/{project_id}/app-servers/actions/create	Create an ECS	√	√
workspace:server:batchMigrateHosts	PATCH	/v1/{project_id}/app-servers/hosts/batch-migrate	Migrate servers at the source Workspace host to the destination one	√	√
workspace:server:getMetricData	GET	/v1/{project_id}/app-servers/metric-data/{server_id}	Query monitoring information of an APS	√	√
workspace:jobs:listSubJobs	GET	/v1/{project_id}/app-server-sub-jobs	Query subtasks	√	x

Action	API Method	API	Supported Action	IAM Project	Enterprise Project
workspace:jobs:batchDeleteSubJobs	POST	/v1/{project_id}/app-server-sub-jobs/actions/batch-delete	Delete subtasks in batches	√	x
workspace:jobs:countSubJobs	GET	/v1/{project_id}/app-server-sub-jobs/actions/count	Query the number of subtasks	√	x
workspace:appWarehouse:authorizeObs	POST	/v1/{project_id}/app-warehouse/action/authorize	Obtain the AK/SK uploaded to an OBS bucket	√	x
workspace:appWarehouse:batchDeleteApp	POST	/v1/{project_id}/app-warehouse/actions/batch-delete	Delete specified applications from the application repository in batches	√	x
workspace:appWarehouse:ListWarehouseApps	GET	/v1/{project_id}/app-warehouse/apps	Query applications in a tenant application repository	√	x

Action	API Method	API	Supported Action	IAM Project	Enterprise Project
workspace:appWarehouse:createApp	POST	/v1/{project_id}/app-warehouse/apps	Add an application to the application repository	√	x
workspace:appWarehouse:deleteApp	DELETE	/v1/{project_id}/app-warehouse/apps/{id}	Delete a specified application from the application repository	√	x
workspace:appWarehouse:uploadAppIcon	POST	/v1/{project_id}/app-warehouse/apps/icon	Upload an icon file to the application repository	√	x
workspace:appWarehouse:createBucketOrAcl	POST	/v1/{project_id}/app-warehouse/bucket-and-acl/create	Add a bucket or bucket authorization	√	x
workspace:orders:create	POST	/v1/{project_id}/bundles/subscribe/order	Create an order	√	x
workspace:quotas:get	GET	/v1/{project_id}/check/quota	Verify quota	√	x

Action	API Method	API	Supported Action	IAM Project	Enterprise Project
workspace:volumes:listDssPoolsDetail	GET	/v1/{project_id}/dss-pools/detail	Query details about dedicated distributed storage pools	√	x
workspace:images:listImageJobs	GET	/v1/{project_id}/image-server-jobs	Query tasks of a tenant	√	x
workspace:images:getImageJob	GET	/v1/{project_id}/image-server-jobs/{job_id}	Query task details	√	x
workspace:imageServer:list	GET	/v1/{project_id}/image-servers	Query image instances	√	√
workspace:imageServer:create	POST	/v1/{project_id}/image-servers	Create an image instance	√	√
workspace:imageServer:get	GET	/v1/{project_id}/image-servers/{server_id}	Query a specified image instance	√	√
workspace:imageServer:update	PATCH	/v1/{project_id}/image-servers/{server_id}	Modify an image instance	√	√

Action	API Method	API	Supported Action	IAM Project	Enterprise Project
workspace:imageServer:attachApp	POST	/v1/{project_id}/image-servers/{server_id}/actions/attach-app	Distribute software information to image instances	√	√
workspace:imageServer:listLatestAttachedApp	GET	/v1/{project_id}/image-servers/{server_id}/actions/latest-attached-app	Query information about the latest distributed software	√	x
workspace:imageServer:recreate	POST	/v1/{project_id}/image-servers/{server_id}/actions/recreate-image	Build an Application Streaming image	√	√
workspace:imageServer:batchDelete	PATCH	/v1/{project_id}/image-servers/actions/batch-delete	Delete image instances in batches	√	√
workspace:imageServer:listImageSubJobs	GET	/v1/{project_id}/image-server-sub-jobs	Query subtasks	√	x
workspace:imageServer:batchDeleteImageSubJobs	PATCH	/v1/{project_id}/image-server-sub-jobs/actions/batch-delete	Delete subtasks in batches	√	x

Action	API Method	API	Supported Action	IAM Project	Enterprise Project
workspace:imageServer:countImageSubJobs	GET	/v1/{project_id}/image-server-sub-jobs/actions/count	Query the number of subtasks	√	x
workspace:jobs:get	GET	/v1/{project_id}/job/{job_id}	Query the task execution status	√	x
workspace:appGroup:listMailRecord	GET	/v1/{project_id}/mails	Query records of sending emails on application group authorization	√	x
workspace:appGroup:resendMail	POST	/v1/{project_id}/mails/actions/send	Resend an email on application group authorization (based on authorization email records)	√	x

Action	API Method	API	Supported Action	IAM Project	Enterprise Project
workspace:appGroup:resendMail	POST	/v1/{project_id}/mails/actions/send-by-authorization	Resend an email on application group authorization (based on authorization records)	√	x
workspace:storage:listPersistentStorage	GET	/v1/{project_id}/persistent-storages	Query Workspace storage space	√	x
workspace:storage:createPersistentStorage	POST	/v1/{project_id}/persistent-storages	Create Workspace storage space	√	x
workspace:storage:deletePersistentStorage	DELETE	/v1/{project_id}/persistent-storages/{storage_id}	Delete Workspace storage space	√	x
workspace:storage:updateUserFolderAssignment	POST	/v1/{project_id}/persistent-storages/{storage_id}/actions/assign-folder	Create a personal storage directory	√	x

Action	API Method	API	Supported Action	IAM Project	Enterprise Project
workspace:storage:updateShareFolderAssignment	POST	/v1/{project_id}/persistent-storages/{storage_id}/actions/assign-share-folder	Change members of a shared directory	√	x
workspace:storage:createShareFolder	POST	/v1/{project_id}/persistent-storages/{storage_id}/actions/create-share-folder	Create a shared storage directory	√	x
workspace:storage:deleteStorageClaim	POST	/v1/{project_id}/persistent-storages/{storage_id}/actions/delete-storage-claim	Delete a shared directory	√	x
workspace:storage:deleteUserStorageAttachment	POST	/v1/{project_id}/persistent-storages/{storage_id}/actions/delete-user-attachment	Delete a personal storage directory	√	x
workspace:storage:batchDeletePersistentStorage	POST	/v1/{project_id}/persistent-storages/actions/batch-delete	Delete Workspace storage space	√	x
workspace:storage:listStorageAssignment	GET	/v1/{project_id}/persistent-storages/actions/list-attachments	Query personal storage directories	√	x

Action	API Method	API	Supported Action	IAM Project	Enterprise Project
workspace:storage:listShareFolder	GET	/v1/{project_id}/persistent-storages/actions/list-share-folders	Query shared storage directories	√	x
workspace:policyGroups:list	GET	/v1/{project_id}/policy-groups	Query policy groups	√	x
workspace:policyGroups:create	POST	/v1/{project_id}/policy-groups	Add a policy group	√	x
workspace:policyGroups:delete	DELETE	/v1/{project_id}/policy-groups/{policy_group_id}	Delete a policy group	√	x
workspace:policyGroups:get	GET	/v1/{project_id}/policy-groups/{policy_group_id}	Query details about a policy group	√	x
workspace:policyGroups:update	PATCH	/v1/{project_id}/policy-groups/{policy_group_id}	Modify a policy group	√	x
workspace:policyGroups:listPolicies	GET	/v1/{project_id}/policy-groups/{policy_group_id}/policy	Query policy items of a policy group	√	x
workspace:policyGroups:listTargets	GET	/v1/{project_id}/policy-groups/{policy_group_id}/target	Query objects to which a policy group is applied	√	x

Action	API Method	API	Supported Action	IAM Project	Enterprise Project
workspace:policyGroups:getOriginalPolicies	GET	/v1/{project_id}/policy-groups/actions/list-original-policy	Query initial policy items	√	x
workspace:policyGroups:listDetail	GET	/v1/{project_id}/policy-groups/show/detail	Query details about policy groups	√	x
workspace:policyGroups:listTemplate	GET	/v1/{project_id}/policy-templates	Query policy templates	√	x
workspace:policyGroups:createTemplate	POST	/v1/{project_id}/policy-templates	Add a policy template	√	x
workspace:policyGroups:deleteTemplate	DELETE	/v1/{project_id}/policy-templates/{policy_template_id}	Delete a policy template	√	x
workspace:policyGroups:updateTemplate	PATCH	/v1/{project_id}/policy-templates/{policy_template_id}	Modify a policy template	√	x
workspace:privacystatements:get	GET	/v1/{project_id}/privacy-statement	Query the latest privacy statement	√	x
workspace:privacystatements:sign	POST	/v1/{project_id}/privacy-statement	Sign the privacy statement	√	x

Action	API Method	API	Supported Action	IAM Project	Enterprise Project
workspace:scalingPolicy:delete	DELETE	/v1/{project_id}/scaling-policy	Delete an Auto Scaling policy	√	x
workspace:scalingPolicy:list	GET	/v1/{project_id}/scaling-policy	Query Auto Scaling policies of a server group	√	x
workspace:scalingPolicy:create	PUT	/v1/{project_id}/scaling-policy	Add or modify an Auto Scaling policy	√	x
workspace:scheduledTasks:list	GET	/v1/{project_id}/schedule-task	Query scheduled tasks	√	x
workspace:scheduledTasks:create	POST	/v1/{project_id}/schedule-task	Add a scheduled task	√	x
workspace:scheduledTasks:getRecord	GET	/v1/{project_id}/schedule-task/{execute_history_id}/execute-detail	Query executed subtasks of a scheduled task	√	x
workspace:scheduledTasks:delete	DELETE	/v1/{project_id}/schedule-task/{task_id}	Delete a task	√	x

Action	API Method	API	Supported Action	IAM Project	Enterprise Project
workspace:scheduledTasks:get	GET	/v1/{project_id}/schedule-task/{task_id}	Query details about a specified scheduled task	√	x
workspace:scheduledTasks:update	PATCH	/v1/{project_id}/schedule-task/{task_id}	Modify a scheduled task	√	x
workspace:scheduledTasks:listRecords	GET	/v1/{project_id}/schedule-task/{task_id}/execute-history	Query the execution list of scheduled tasks	√	x
workspace:scheduledTasks:batchDelete	POST	/v1/{project_id}/schedule-task/actions/batch-delete	Delete scheduled tasks in batches	√	x
workspace:scheduledTasks:getFuture	POST	/v1/{project_id}/schedule-task/future-executions	Query the list of future execution time	√	x
workspace:session:listAppConnection	POST	/v1/{project_id}/session/app-connection	Query application usage records	√	x
workspace:session:logoffUserSession	POST	/v1/{project_id}/session/logoff	Log out of a session	√	x

Action	API Method	API	Supported Action	IAM Project	Enterprise Project
workspace:session:listUserConnection	POST	/v1/{project_id}/session/user-connection	Query user login records	√	x
workspace:session:listSessionByUserName	GET	/v1/{project_id}/session/user-session-info	Query current sessions by username	√	x
workspace:storagePolicy:create	PUT	/v1/{project_id}/storages-policy/actions/create-statements	Add or update a custom policy for storage directory access	√	x
workspace:storagePolicy:list	GET	/v1/{project_id}/storages-policy/actions/list-statements	Query policies for storage directory access	√	x
workspace:users:list	GET	/v1/{project_id}/users	Query users or user groups	√	x
workspace:storage:listSfs3Storage	GET	/v1/persistent-storages/actions/list-sfs-storages	Query SFS 3.0	√	x
workspace:baseResource:list	GET	/v1/{project_id}/availability-zone	Query AZs	√	x

Action	API Method	API	Supported Action	IAM Project	Enterprise Project
workspace:tenants:listConfigInfo	POST	/v1/{project_id}/bundles/batch-query-config-info	Query enterprise system configurations	√	x
workspace:baseResource:list	GET	/v1/{project_id}/product	Query Application Streaming packages	√	x
workspace:baseResource:list	GET	/v1/{project_id}/session-type	Query session packages	√	x
workspace:tenants:active	POST	/v1/{project_id}/tenant/action/active	Activate and initialize a tenant service	√	x
workspace:tenants:listTenantProfile	GET	/v1/{project_id}/tenant/profile	Query tenant information	√	x
workspace:baseResource:list	GET	/v1/{project_id}/volume-type	Query available disk types	√	x
workspace:server:listServerMetricData	GET	/v1/{project_id}/app-servers/server-metric-data/{server_id}	Query server monitoring data	√	x

Action	API Method	API	Supported Action	IAM Project	Enterprise Project
workspace:session:listSessions	GET	/v1/{project_id}/session/list-sessions	Query enterprise sessions	√	x

2.21 Configuring Common Functions

2.21.1 Allowing Workspace Application Streaming to Access the Internet

Scenarios

After the administrator publishes an application, the cloud application is in the VPC subnet by default and cannot access the Internet. The administrator needs to configure a shared EIP for the NAT gateway so that users can access the Internet after connecting to applications with the Internet access function. If a cloud application has multiple service subnets, the Internet function must be enabled for each service subnet.

NOTE

Workspace Application Streaming and Workspace share the same network. If a desktop exists in the same subnet of the same project and the administrator has enabled enhanced Internet access for the desktop in the subnet, end users can directly access the Internet using applications. If only cloud applications exist in the subnet of the current project, the administrator needs to enable the Internet by referring to **2.23.12 How Do I Purchase the NAT and EIP Services to Enable Cloud Applications to Be Accessed Through the Internet?**.

Prerequisites

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

NOTE

- By default, a Huawei Cloud account has the operation permissions on all Huawei Cloud services. If you use such an account, you do not need to confirm it.
- To use NAT and EIP, the IAM account created under the Huawei Cloud 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 **NAT** and **EIP**.

Procedure

Step 1 Log in to the Workspace Application Streaming **console** as an administrator.

Step 2 Check whether the Internet access address is enabled.

NOTE

After the service is enabled, 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 **Disabled** 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 the Internet access address again. After the function is enabled again, the IP address changes. You need to notify the user to use the new IP address for access.

Step 3 Enable the Internet by referring to **2.12.1 Enabling Internet Access**.

Step 4 Configure the DNS forwarding function (optional).

If Workspace Application Streaming is interconnected with the Windows AD server, you need to configure DNS domain name resolution on the Windows AD server. For details, see **Step 4.1** to **Step 4.10**. If not, go to the next step.

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 left navigation pane, 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 cloud application region in the text box, and click **OK**.

    NOTE

    The default DNS server IP address of the Workspace Application Streaming region can be obtained from **Huawei Cloud Private DNS Server Addresses**.

Step 5 Notify end users to use the Internet access address to access Workspace Application Streaming.

----End

Follow-up Operations

If users do not need to access the Internet, users can disable the Internet to save resources. The process is: Disable the SNAT bound to the EIP, disable the NAT, and release the EIP.

NOTE

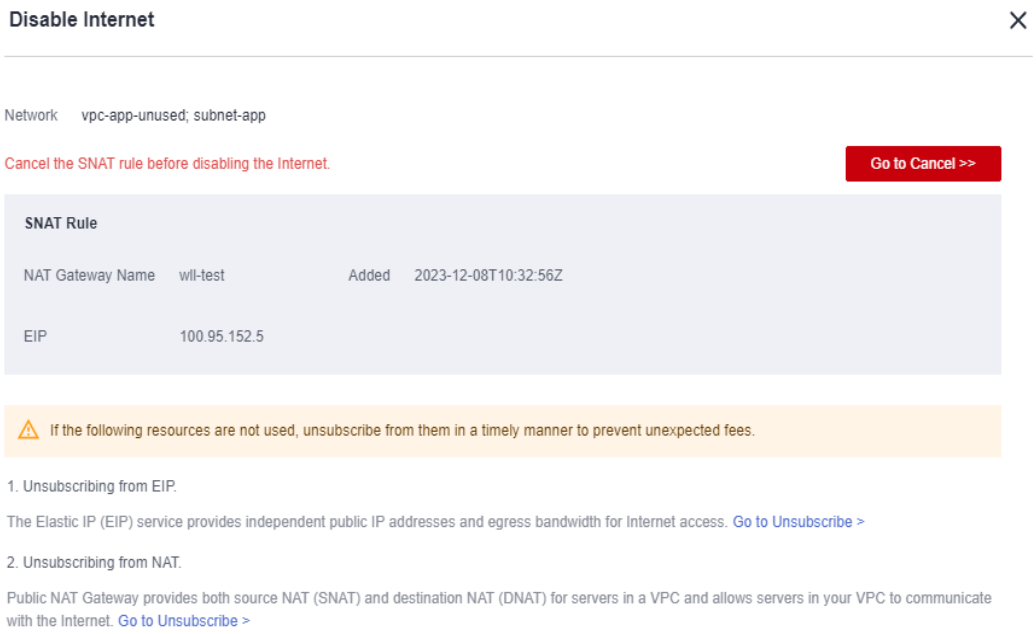
After SNAT is disabled, Workspace Application Streaming cannot access the Internet. Determine whether to disable the NAT and EIP as required.

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

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

The page for disabling the Internet is displayed, as shown in **Figure 2-34**.

Figure 2-34 Disabling the Internet



Record the NAT gateway name and the EIP bound to the SNAT rule. After the SNAT rule is disabled, the EIP is unbound from the SNAT rule. You need to disable 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.

Disabling an SNAT rule

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

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

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

(Optional) Disabling a NAT

NOTE

Multiple SNAT and DNAT rules can be created for a NAT, and the NAT can be disabled only after all related SNAT and DNAT rules are disabled. Determine whether to disable the NAT as required. If you decide to disable the NAT, disable it when it is used only by the cloud application 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 disabled and choose **Operation** > **Delete**.

NOTE

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

Step 8 In the displayed dialog box, enter **DELETE** and click **OK**.

Disabling 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

2.21.2 Allowing Workspace Application Streaming to Access the Enterprise Intranet

Scenarios

After the administrator publishes an application, Workspace Application Streaming is in the VPC subnet by default and cannot access the enterprise intranet. The administrator needs to configure a Direct Connect or VPN connection so that users can access the enterprise intranet after accessing applications with the Internet access function.

Prerequisites

You have used Direct Connect to connect the enterprise intranet to the VPC where the cloud application resides by referring to Direct Connect - **Getting Started**. Alternatively, you have connected the local data center to the VPC where the cloud application resides by referring to ***VPN What's New***. A typical example is **Interconnection with a Huawei AR Router (Active-Active Connections)**.

Constraints

If a firewall is used, ensure that ports 8443 and 443 in the outbound direction of the firewall are enabled.

Procedure

Step 1 Log in to the Workspace Application Streaming **console** as an administrator.

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

Step 3 In the **Network Settings** 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 Workspace Application Streaming and the subnet of Direct Connect are in the same range.

    If yes, you do not need to configure the Direct Connect network segment.

    If no, configure the Direct Connect network segment in the **Direct Connect Network Segment** area. You can view the service subnet of Workspace Application Streaming and the subnet network segment of 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 Workspace Application Streaming 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 Workspace Application Streaming.

----End

2.22 Monitoring

2.22.1 Basic Monitoring Metrics Supported by Workspace Application Streaming

This section describes the monitoring metrics reported by Workspace Application Streaming to Cloud Eye and defines the namespace for the metrics. You can use Cloud Eye to query metrics and alarms generated by Workspace Application Streaming.

Namespaces

SYS.AppStream

Table 2-33 describes the basic monitoring metrics of Workspace Application Streaming.

The monitoring intervals for the following raw metrics are as follows:

Table 2-33 Basic monitoring metrics supported by Workspace Application Streaming

Metric ID	Metric Name	Metric Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Interval (Raw Metrics and KVM Only)
cpu_util	CPU Usage	CPU usage of an ECS. This metric is used to show the CPU usage of the physical server accommodating the monitored ECS, which is not as accurate as the CPU usage obtained on the monitored ECS. For details, see Formula: CPU usage of an ECS/ Number of CPU cores on the ECS	0-100	%	N/A	Application Streaming instance	1 minute
mem_util	Memory Usage	Memory usage of an ECS. Formula: Memory usage of an ECS/ Total memory of the ECS	0-100	%	N/A	Application Streaming instance	1 minute

Metric ID	Metric Name	Metric Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Interval (Raw Metrics and KVM Only)
disk_util_inband	Disk Usage	Disk usage of an ECS. Formula: Disk usage of an ECS/ Total disk capacity of the ECS	0-100	%	N/A	Application Streaming instance	1 minute
disk_read_bytes_rate	Disk Read Rate	Number of bytes read from an ECS per second. Formula: Total number of bytes read from an ECS/ Monitoring interval byte_out = (rd_bytes - last_rd_bytes)/Time difference	≥ 0	byte/s	1024(IEC)	Application Streaming instance	1 minute
disk_write_bytes_rate	Disk Write Rate	Number of bytes written to an ECS per second. Formula: Total number of bytes written to a disk of the ECS/ Monitoring interval	≥ 0	byte/s	1024(IEC)	Application Streaming instance	1 minute

Metric ID	Metric Name	Metric Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Interval (Raw Metrics and KVM Only)
disk_read_requests_rate	Disk Read IOPS	Number of read requests sent to an ECS per second. Formula: Total number of read requests sent to a disk of the ECS/ Monitoring interval req_out = (rd_req - last_rd_req)/Time difference	≥ 0	Request/s	N/A	Application Streaming instance	1 minute

Metric ID	Metric Name	Metric Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Interval (Raw Metrics and KVM Only)
disk_write_requests_rate	Disk Write IOPS	Number of write requests sent to an ECS per second. Formula: Total number of write requests sent to a disk of the ECS/ Monitoring interval req_in = (wr_req - last_wr_req)/Time difference	≥ 0	Request/s	N/A	Application Streaming instance	1 minute
network_incoming_bytes_rate_inband	Inband Incoming Rate	Number of incoming bytes on an ECS per second. Formula: Total number of inband incoming bytes on an ECS/ Monitoring interval	≥ 0	byte/s	1024(IEC)	Application Streaming instance	1 minute

Metric ID	Metric Name	Metric Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Interval (Raw Metrics and KVM Only)
network_outgoing_bytes_rate_inband	Inband Outgoing Rate	Number of outgoing bytes on an ECS per second. Formula: Total number of inband outgoing bytes on an ECS/ Monitoring interval	≥ 0	byte/s	1024(IEC)	Application Streaming instance	1 minute
network_incoming_bytes_aggregate_rate	Outband Incoming Rate	Number of incoming bytes on an ECS per second on the hypervisor. Formula: Total number of outband incoming bytes on an ECS/ Monitoring interval This metric is unavailable if SR-IOV is enabled.	≥ 0	byte/s	1024(IEC)	Application Streaming instance	1 minute

Metric ID	Metric Name	Metric Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Interval (Raw Metrics and KVM Only)
network_outgoing_bytes_aggregate_rate	Outband Outgoing Rate	Number of outgoing bytes on an ECS per second on the hypervisor. Formula: Total number of outband outgoing bytes on an ECS/ Monitoring interval This metric is unavailable if SR-IOV is enabled.	≥ 0	byte/s	1024(IEC)	Application Streaming instance	1 minute
user_session_num	Number of User Sessions	Number of user sessions on an ECS.	0-100	%	N/A	Application Streaming instance	1 minute

2.22.2 Cloud Eye Events Supported by Workspace Application Streaming

Functions

The Cloud Eye event monitoring supported by Workspace Application Streaming provides event data reporting, query, and alarm reporting. When there are specified events, you will receive alarm notifications from Cloud Eye.

Namespaces

SYS.AppStream

Monitored Events

Table 2-34 Events supported by Workspace Application Streaming

Event Name	Event ID	Event Severity	Event Description	Handling Suggestion	Impact
Abnormal APS heartbeat	appServerStatusAbnormal	Major	The APS network is disconnected, the key is lost, or the APS agent process malfunctions.	1. Restart the APS. 2. Check whether special security software or network connection software is installed on the APS. If yes, uninstall the software and restart the server. Alternatively, uninstall the software, reinstall the HDPAgent, and restart the server.	The APS is unavailable.

Event Name	Event ID	Event Severity	Event Description	Handling Suggestion	Impact
Application access failure	appAccessFailed	Major	The client network is disconnected, the AD network is disconnected, or the AD access times out.	1. Log in to the Workspace Application Streaming console as an administrator. 2. Choose **Application Records**. On the **Application Usage** tab, query the application opening records of users by login user account. 3. If **authenticate failed** is displayed, the AD server authentication may fail. Check whether the network connection and running status of the AD server are normal. 4. If the network connection or running status of the AD server is abnormal, troubleshoot the AD server or switch to another region.	Application access failed.

2.23 FAQs

2.23.1 What Is the Relationship Between Workspace Application Streaming and Workspace?

- Workspace and Workspace Application Streaming can be enabled at the same time in the same project in the same region. If the same Windows AD is connected, the user list can be shared.

- You can apply for and use Workspace Application Streaming as a Workspace administrator.

2.23.2 What Types of Applications Can Be Published?

Currently, only Windows applications can be published. The file type can be **.exe** or **.msi**.

2.23.3 What Can I Do If an Application Fails to Be Published?

Applications with the same name cannot be published in the same application group. Change the application name and try again. If the application still fails to be published, **submit a service ticket** for technical support.

2.23.4 How Do I Deploy a Windows AD Server?

Scenarios

Workspace Application Streaming needs to interconnect with Windows AD. This section describes how to deploy a Windows AD server. If a Windows AD server is available, skip this section.

NOTE

Huawei does not provide Windows AD servers. Users need to purchase and configure Windows AD servers.

Prerequisites

You have **purchased an ECS**.

Data

The required parameters are described in the following procedure.

Procedure

Logging in to an ECS

Step 1 In the ECS list, locate the created ECS and click **Remote Login** in the **Operation** column.

Step 2 Click **Send CtrlAltDel** in the upper right corner of the remote login screen.

Step 3 Enter the password of the ECS to log in.

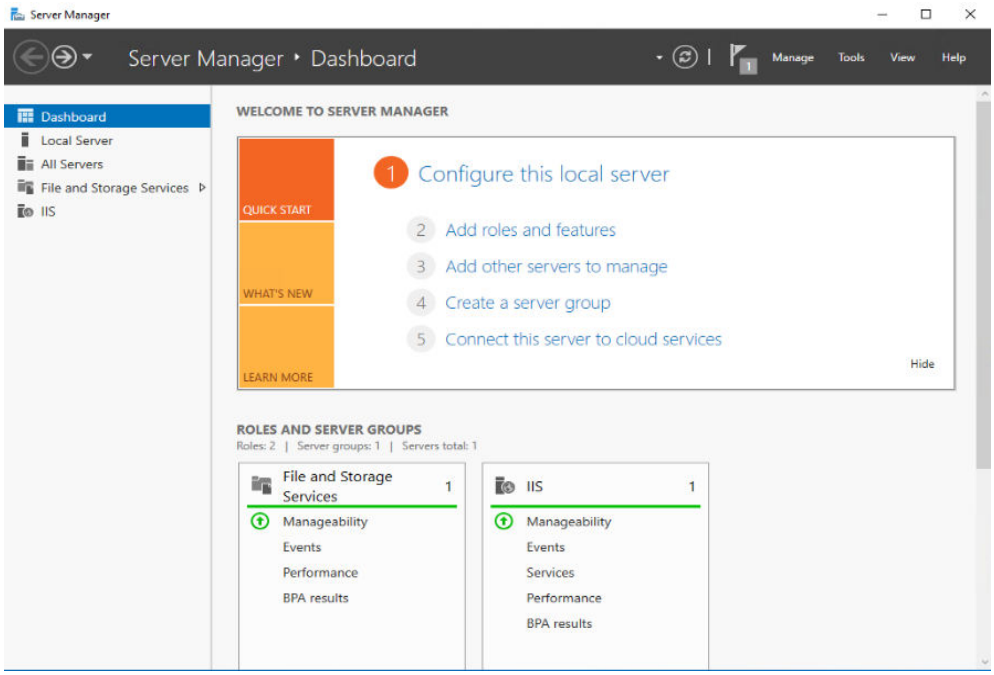
Adding the AD role and backup function

Step 4 On the taskbar, click  .

Step 5 Click  on the right of the **Start** menu.

The **Server Manager** window is displayed, as shown in **Figure 2-35**.

Figure 2-35 Server manager



Step 6 In the middle of the page, click **Add roles and features**.

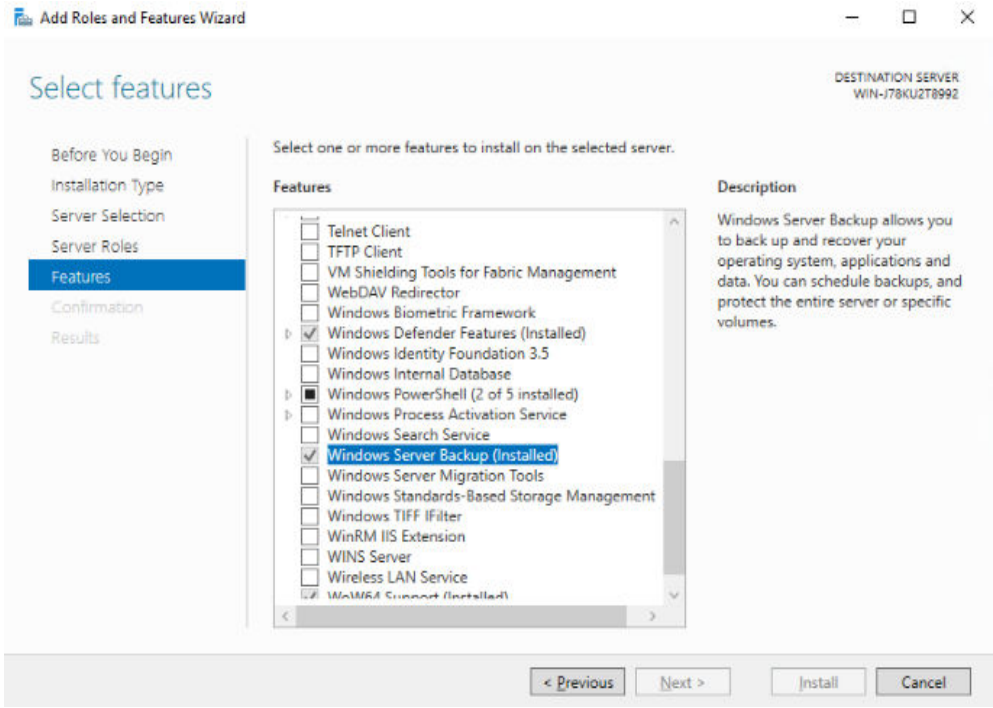
The **Add Roles and Features Wizard** dialog box is displayed.

Step 7 Click **Next** for three times.

Step 8 In the **Roles** area, select **Active Directory Domain Services**. In the dialog box that is displayed, click **Add Features**. Then, click **Next**.

Step 9 In the **Features** area, select **Windows Server Backup**, as shown in **Figure 2-36**.

Figure 2-36 Deploying the backup function



Step 10 Click **Next** until the **Confirm** dialog box is displayed.

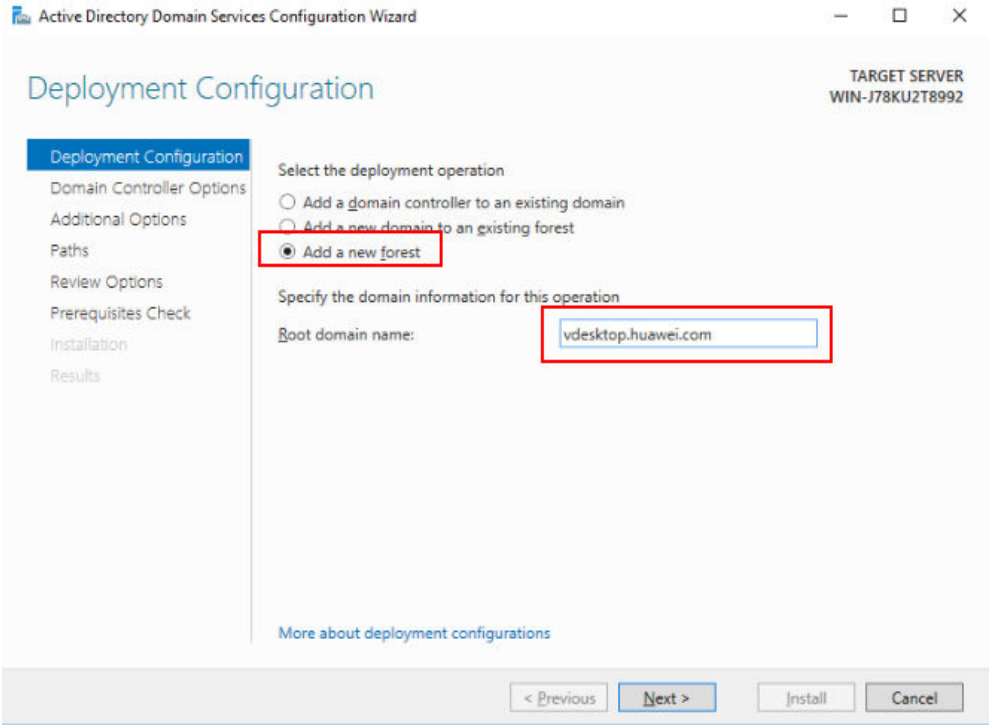
Step 11 Click **Install**.

The installation progress bar is displayed. When **Installation succeeded** is displayed, the installation is successful.

Step 12 In the upper right corner of the **Server Manager** page, click , and select **Promote this server to a domain controller**.

The **Active Directory Domain Services Configuration Wizard** window is displayed, as shown in **Figure 2-37**.

Figure 2-37 Active Directory Domain Services Configuration Wizard



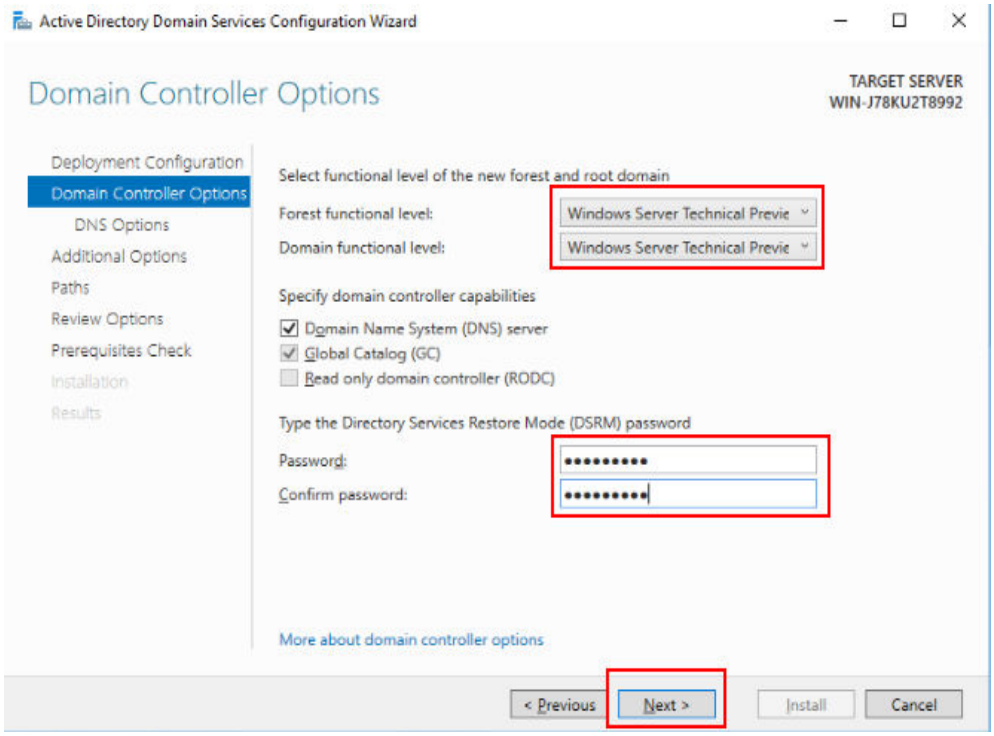
Step 13 Select **Add a new forest**, specify **Root domain name**, and click **Next**.

Step 14 Set both **Forest functional level** and **Domain functional level** to **Windows Server 2016**, set **Type the Directory Services Restore Mode (DSRM) password**, and click **Next**, as shown in **Figure 2-38**.

NOTE

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

Figure 2-38 Configuring the domain controller



Step 15 Retain the default values, click **Next** for four times, and click **Install**.

Install the AD service and restart the VM as prompted.

Step 16 Log in to the AD server using the administrator account.

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

Installing the AD service on the standby server

Step 17 Configure the standby AD server. For details, see **Step 1** to **Step 16**.

----End

2.23.5 How Do I Deploy an RD Licensing Server?

Scenarios

Workspace Application Streaming must obtain remote desktop authorization. This section describes how to deploy an RD Licensing server. If an RD Licensing server is available, skip this section.

NOTE

- Huawei does not provide RD Licensing servers. Users need to purchase and configure RD Licensing servers.
- RDS CAL type must be set to **Per User CALs**.
- For details about the RDS CAL version compatibility, visit **RDS CAL version compatibility**.

Prerequisites

- You have **purchased an ECS**.
- You have obtained the serial number (SN) of the Windows OS from Microsoft or other official channels.
- You have obtained licenses for remote applications from Microsoft.
- You have created a domain account of the RD Licensing server on Windows AD, for example, **vdesktop\vdsuser**. For details, see **2.23.9 How Do I Create a User on the AD Server?**.

Procedure

Logging in to a server

Step 1 In the ECS list, locate the created ECS and click **Remote Login** in the **Operation** column.

Step 2 Click **Send CtrlAltDel** in the upper right corner of the remote login screen.

Step 3 Enter the password of the ECS to log in.

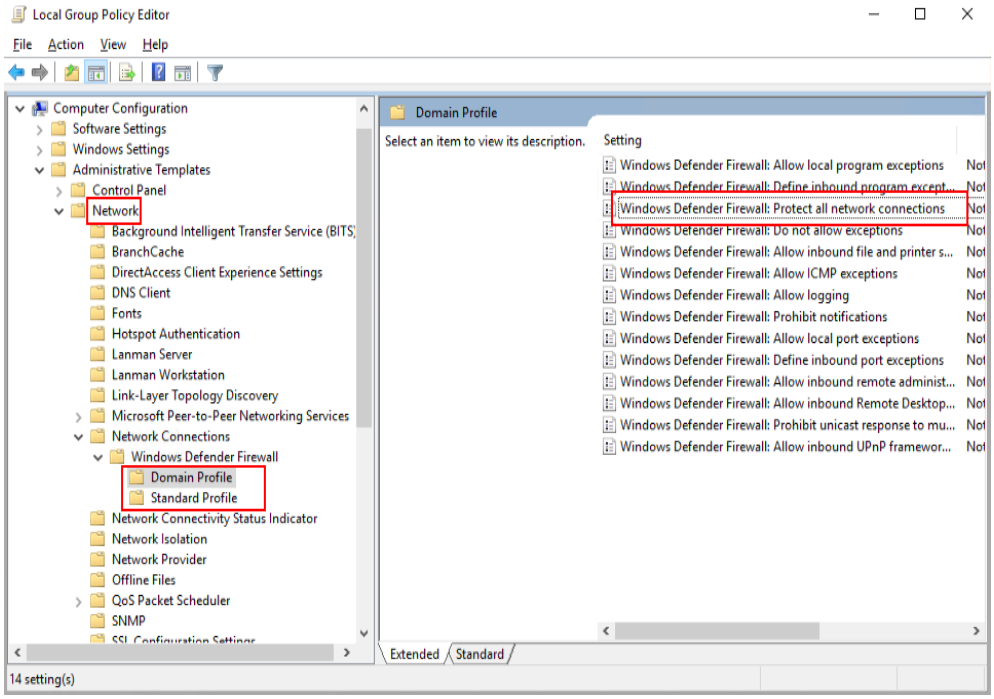
Disabling the firewall

Step 4 Right-click  in the lower left corner, enter **gpedit.msc** in the **Run** text box, and press **Enter**.

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

Step 5 In the navigation pane on the left, choose **Computer Configuration** > **Administrative Templates** > **Network** > **Network Connections** > **Windows Firewall**. Click **Domain Profile** and disable **Windows Firewall: Protect all network connections**. Click **Standard Profile** and disable **Windows Firewall: Protect all network connections**, as shown in **Figure 2-39**.

Figure 2-39 Disabling the firewall



Step 6 Close the **Local Group Policy Editor** window.

Configuring the AD domain address to the DNS server of the RD Licensing server

Step 7 Log in to the RD Licensing server.

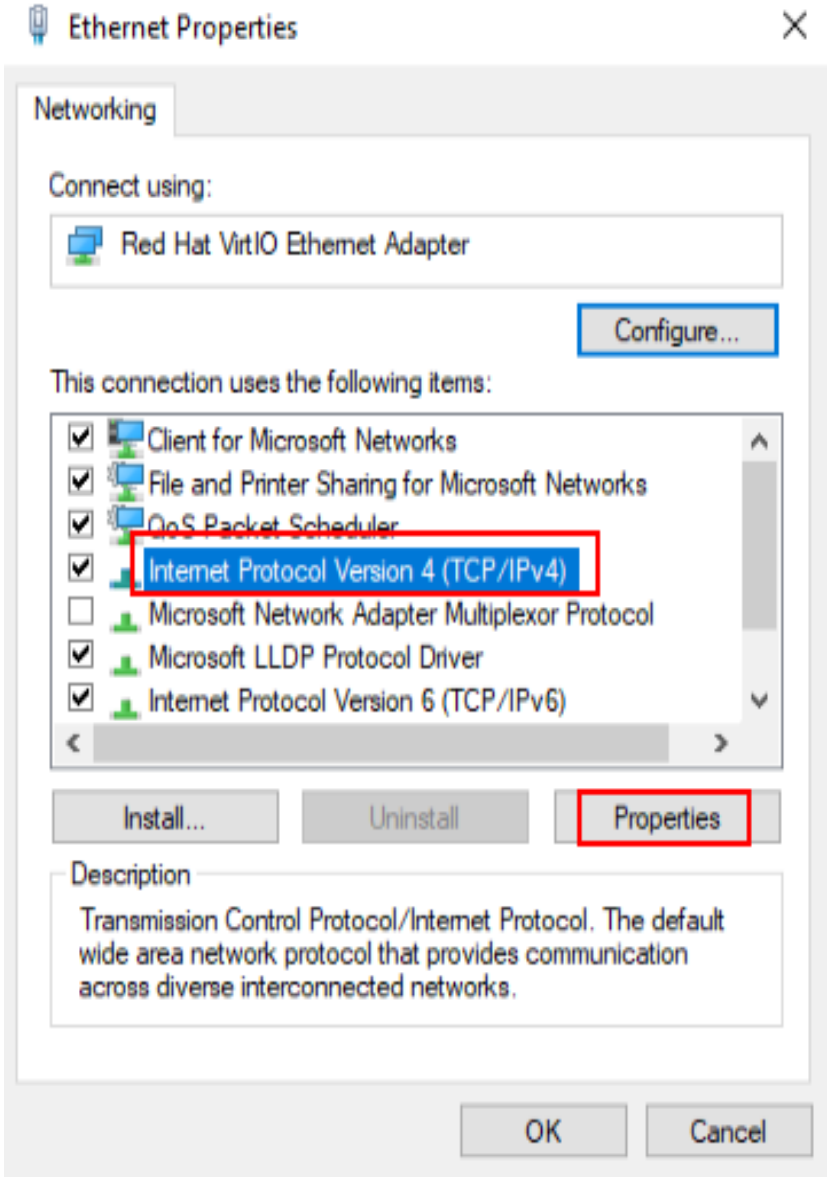
Step 8 Right-click the NIC connection status icon in the lower right corner and choose **Open Network and Sharing Center** from the shortcut menu. The network configuration page is displayed.

Step 9 Click **Change adapter settings**. The network connection page is displayed.

Step 10 Right-click the NIC and choose **Properties** from the shortcut menu. The NIC's properties page is displayed.

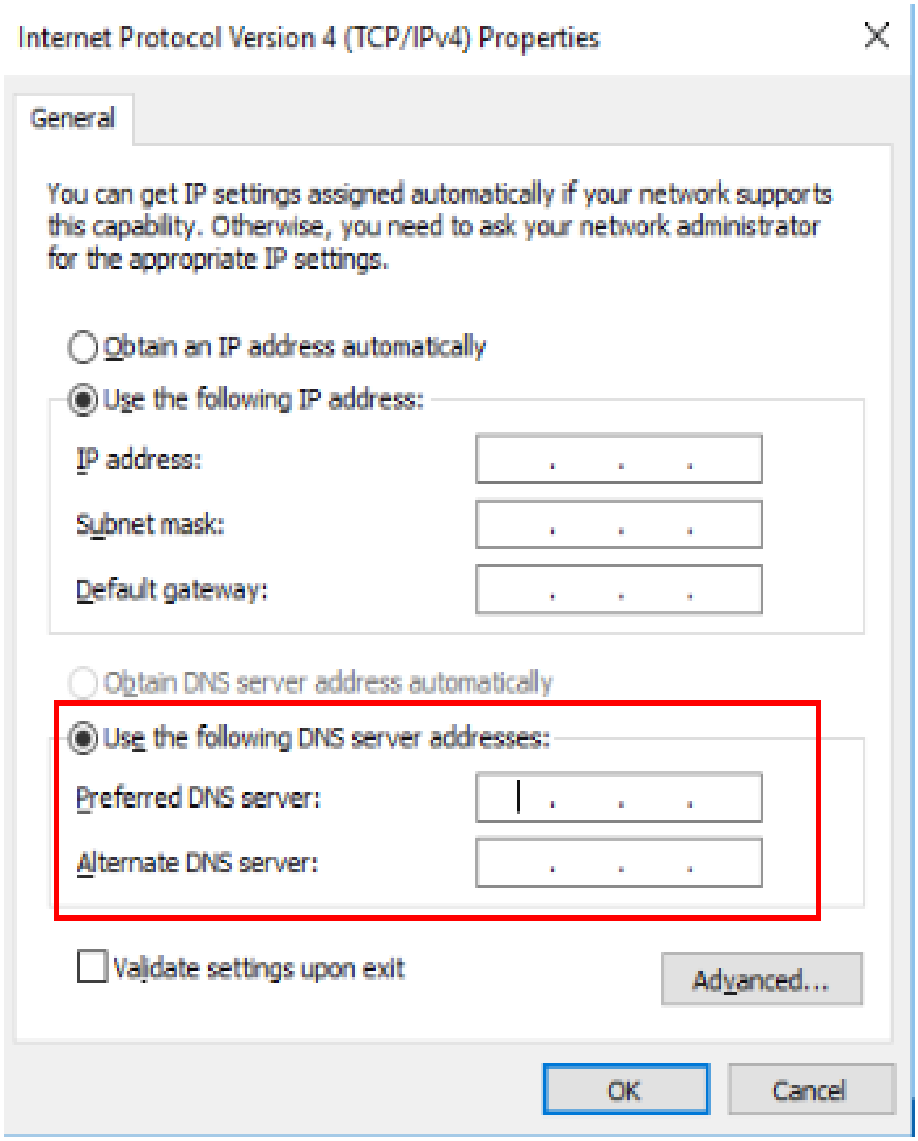
Step 11 In the connection item list on the **Networking** tab page, click the Internet protocol version with the IPv4 suffix, and click **Properties**. The IPv4 Internet protocol properties page is displayed, as shown in **Figure 2-40**.

Figure 2-40 Ethernet properties



Step 12 On the **General** tab page, choose **Use the following DNS server address:**, and set **Preferred DNS server:** to the **AD domain** address, as shown in **Figure 2-41**.

Figure 2-41 Setting the DNS address



Step 13 Click **OK**.

Adding the server to the domain

Step 14 On the server, right-click in the lower left corner, enter **sysdm.cpl** in the **Run** text box, and press **Enter**.

The **System Properties** window is displayed.

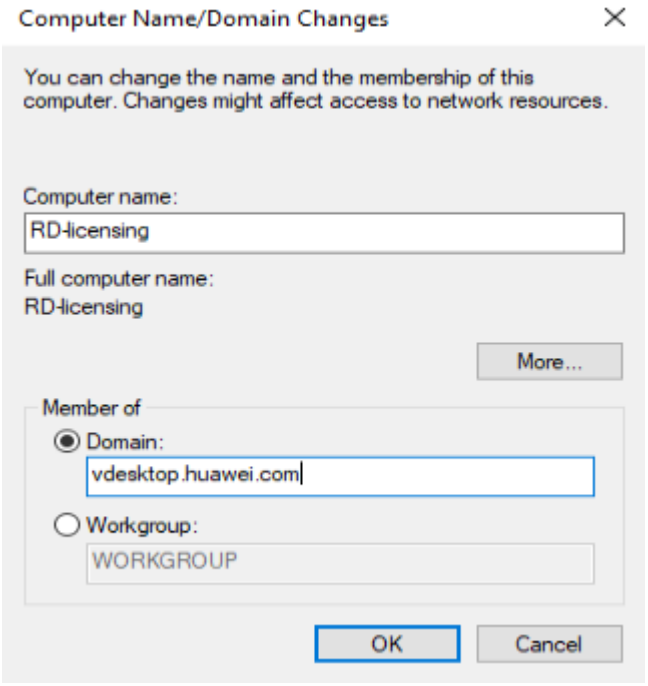
Step 15 Click **Change**.

The **Computer Name/Domain Changes** dialog box is displayed.

Step 16 Set the following parameters and click **OK**, as shown in **Figure 2-42**.

- **Computer name**: Enter the planned computer name, for example, **RD-licensing**.
- **Domain**: Enter the fully qualified domain name (FQDN) of the domain, for example, **vdesktop.huawei.com**.

Figure 2-42 System properties



Step 17 Enter the username and password of the domain administrator to be added to the domain and click **OK**.

Step 18 Complete the configuration as prompted, restart the VM, and log in to the VM using the administrator account.

Adding the domain account to the administrator group

Add the following accounts to the administrator group:

- **Domain administrator account** (for example, **vdesktop\vdsadmin**)
- **Domain account for logging in to a server** (for example, **vdesktop\vdsuser**)

Step 19 In the server, right-click  in the lower left corner, enter **compmgmt.msc**, and press **Enter**.

The **Computer Management** window is displayed.

Step 20 Choose **System Tools** > **Local Users and Groups** > **Groups**.

The group list is displayed in the right pane.

Step 21 Right-click **Administrators** and choose **Add to Group** from the shortcut menu.

Step 22 Click **Add**. In the **Enter the object names to select** area, enter **Domain account for logging in to a server**, for example, **vdesktop\vdsuser**, and click **OK**.

The **Enter Network Credentials** dialog box is displayed.

Step 23 Enter the username and password of the domain administrator and click **OK** twice.

Step 24 Repeat **Step 19** to **Step 23** to add other domain accounts to the administrator group.

Installing the remote desktop licensing service

Step 25 Log out of the RD Licensing server, and log in to the RD Licensing server again using a domain account, for example, **vdesktop\vdsuser**.

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

Step 27 On the taskbar, click  .

The **Server Manager** window is displayed.

NOTE

If the system displays the **Server Manager** window after the VM is logged in to, you do not need to perform this operation. Refer to this note if similar cases occur.

Step 28 In the **Server Manager** window, click **Add roles and features** in the right pane.

The **Add Roles and Features Wizard** window is displayed.

Step 29 Retain the default settings and repeatedly click **Next**.

The **Select server roles** window is displayed.

Step 30 Select **Remote Desktop Services** and repeatedly click **Next**.

The **Select role services** window is displayed.

Step 31 Select **Remote Desktop Licensing**.

The **Add Roles and Features Wizard** window is displayed.

Step 32 Click **Add Features**.

Step 33 Click **Next**.

Step 34 Click **Install**.

Step 35 Close the installation page when the remote desktop licensing function is installed.

Activating the RD Licensing server

Step 36 Log in to the RD Licensing server using a domain account, for example, **vdesktop\vdsuser**.

Step 37 Activate the server by referring to **Activate the Remote Desktop Services license server**.

Configuring RDS CALs

Step 38 Configure RDS client access licenses by referring to **Install RDS client access licenses on the Remote Desktop license server**.

----End

2.23.6 How Do I Configure RDS Licensing and Security Policies?

Scenarios

This section describes how to configure RDS licensing and security policies on the AD domain server by setting group policies.

After VMs are added to an application group, you need to configure the RDS service authorization function of the APS on the AD domain server to ensure that users obtain RDS service authorization of the RD Licensing server when accessing applications published by the APS. Otherwise, users cannot use remote applications after a trial period of 120 days.

Before publishing applications on the APS, harden the security by configuring security policies of the APS to ensure secure access of authorized users.

Prerequisites

- You have logged in to the AD domain server as an administrator.
- You have obtained RDS service licensing options and security policies.

Data

Table 2-35 lists the data to be obtained.

Table 2-35 Data to be obtained

Parameter	Description	Example Value
Name	Identifies an APS organization unit (OU) in the cloud application scenario.	SBCOU
Name of the group policy	Identifies a group policy of the APS. The name consists of digits, letters, and underscores (_), and cannot exceed 30 characters.	SBCGRP
IP address of the license server to use	Specifies the server that provides the RDS service licensing function to the APS, that is, the RD Licensing server.	192.168.1.60

Procedure

Creating an APS OU

In the cloud application scenario, control authorization and configure security policies for the APS by configuring group policies. In this case, an independent OU must be created for the APS.

Step 1 On the active AD domain server, choose  > **Administrative Tools** > **Active Directory Users and Computers**.

NOTE

This section uses a Windows AD domain server running Windows Server 2016 as an example to describe the configuration procedure.

The **Active Directory Users and Computers** window is displayed.

Step 2 In the navigation pane, right-click a *domain name* and choose **New** > **Organizational Unit**.

The **New Object-Organizational Unit** dialog box is displayed.

Step 3 Enter the name of the application virtualization OU to be created, for example, **SBCOU**, and click **OK**.

Step 4 Add the APS to the new OU.

Creating an APS group policy

Step 5 On the active AD domain server, click  .

The **Windows PowerShell** dialog box is displayed.

Step 6 Enter **gpmc.msc** to open the **Group Policy Management** window.

Step 7 Right-click the selected OU and choose **Create a GPO in this domain, and Link it here**.

Step 8 In the displayed dialog box, enter the group policy name, for example, **SBCGRP**.

Step 9 Click **OK**.

Configuring the RDS service licensing function of the APS

Step 10 Right-click the new group policy and choose **Edit** from the shortcut menu.

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

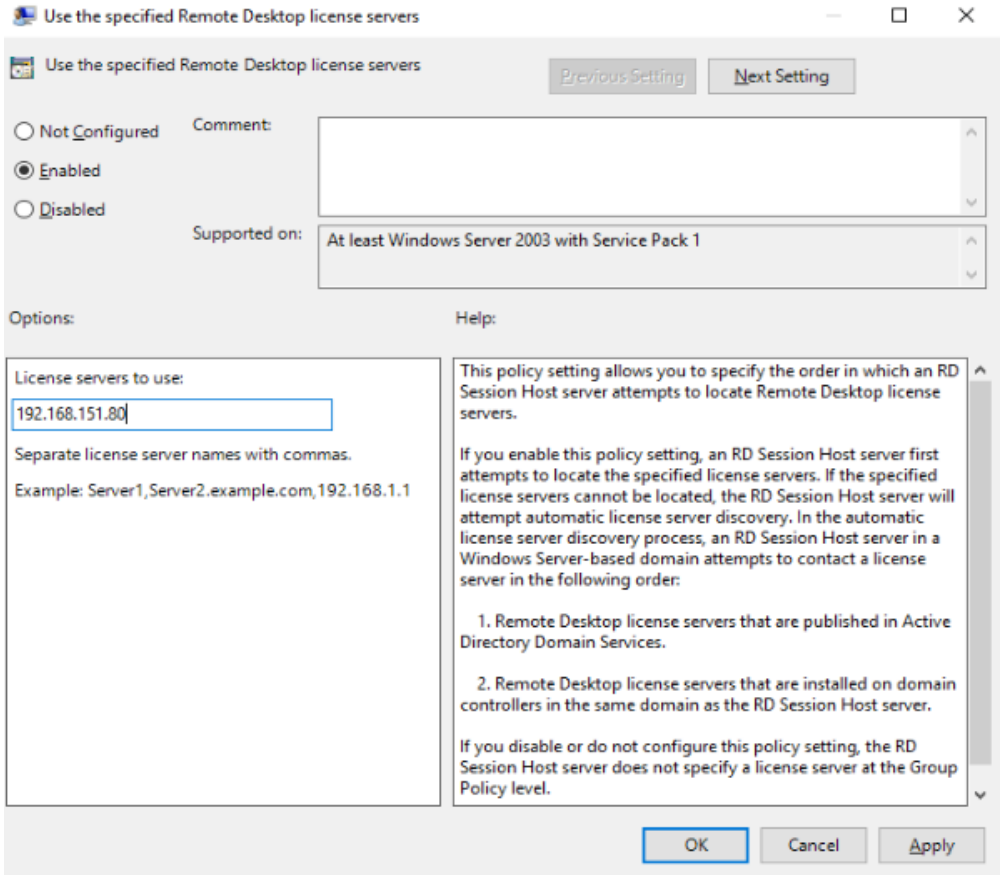
Step 11 In the navigation pane, choose **Computer Configuration** > **Policy** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Licensing**.

Step 12 In the **Licensing** area, right-click **Use the specified Remote Desktop license servers** and choose **Edit**.

The **Use the specified Remote Desktop license servers** dialog box is displayed.

Step 13 Set parameters as shown in **Figure 2-43**, and click **OK**.

Figure 2-43 Using the specified remote desktop license servers

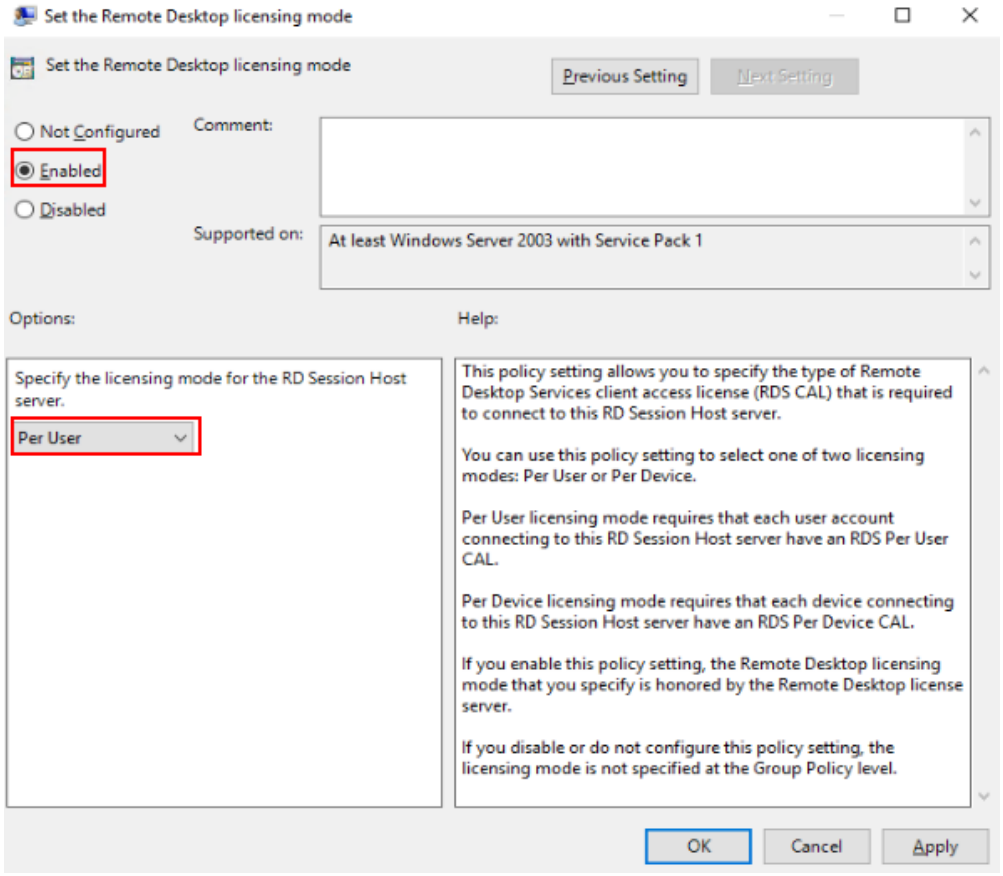


Step 14 In the **Licensing** area, right-click **Set the Remote Desktop licensing mode** and choose **Edit**.

The **Set the Remote Desktop licensing mode** dialog box is displayed.

Step 15 Set parameters as shown in **Figure 2-44**, and click **OK**.

Figure 2-44 Setting the remote desktop licensing mode



(Optional) Configuring APS security policies

NOTICE

Security policies are mandatory if users have specific security requirements.

For the APS, two security policies are available. **Table 2-36** provides the specific operations and application scenarios of the two security policies.

Table 2-36 Security policies

Security Policy	Operation	Scenario
Common office mode	• Use all applications provisioned by the administrator. • Enable **Control Panel** and system settings. • Enable **Task Manager**. • Enable the Internet control panel function. • Enable **powershell.exe** and **cacls.exe**. • Disable the Windows updating, registry editing, CLI, and **Run** functions. • Disable the **Shut Down**, **Restart**, **Sleep**, and **Hibernate** functions.	Scenarios that require the advantages of cloud applications for efficient office and that do not require high security.
Security isolation mode	• Use specified Windows applications. • Disable most system settings.	Scenarios that have high security requirements and must strictly control application and session rights

Step 16 Right-click the new group policy and choose **Edit** from the shortcut menu.

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

Step 17 Set an APS security policy for common office or security isolation mode. For details about how to configure security policies of the APS, see the following file.

Submit a service ticket for technical support of security policies.

Step 18 The following uses the **Prohibit access to the Control Panel** policy as an example to describe how to configure security policies.

1. In the navigation pane of the **Local Group Policy Management Editor** window, choose **User Configuration** > **Policies** > **Administrative Templates** > **Control Panel**.
2. In the right pane, right-click **Prohibit access to the Control Panel** and choose **Edit**.
3. Select **Enabled** and click **OK**.

Denying Apply group policy to the APS domain account

Step 19 In the navigation pane of the **Group Policy Management** window, choose **Forest:*Domain name*** > **Domains** > ***Domain name*** > ***APS OU*** > ***Group policy name***.

NOTE

The APS group policy has been created in **Creating the APS group policies**, for example, **SBCGRP**.

The **Group Policy Management Console** dialog box is displayed.

Step 20 Click **OK**.

The APS group policy is displayed in the right pane.

Step 21 Click the **Delegation** tab and then click **Add**.

The **Select User, Computer, or Group** dialog box is displayed.

NOTE

This policy applies to all users by default. You need to deny this policy to the APS domain account to facilitate the APS maintenance.

Step 22 Enter the APS domain account and click **Check Names**.

The queried domain account is displayed.

Step 23 Click **OK**.

The **Add Group or User** dialog box is displayed.

Step 24 Grant the **Read** permission for a group or user, and click **OK**.

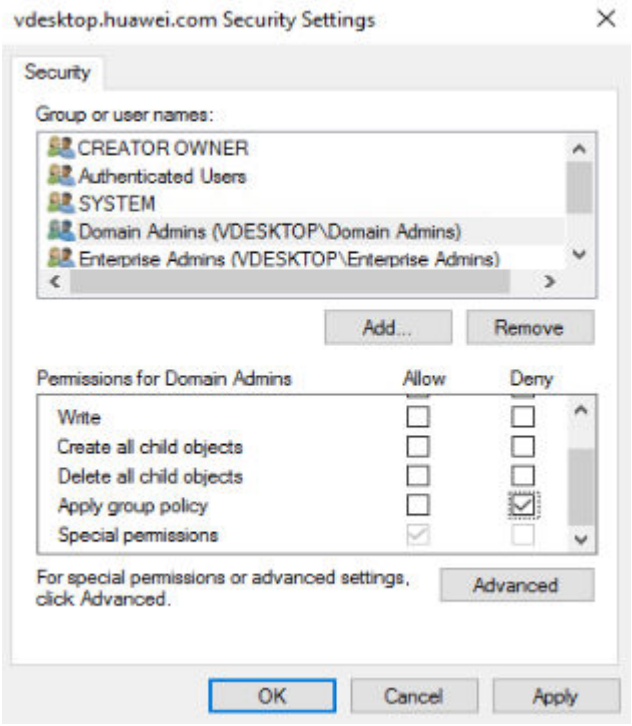
The APS group policy window is displayed.

Step 25 Click **Advanced**.

The *Group policy name* **Security Settings** dialog box is displayed.

Step 26 Select the APS domain account, and select **Deny** in **Apply group policy**, as shown in **Figure 2-45**.

Figure 2-45 Denying the policy to the APS domain account



Step 27 Click **Apply**.

The **Windows Security** window is displayed.

Step 28 In the displayed dialog box, click **Yes**.

Step 29 Click **OK**.

Refreshing the policy

Step 30 Click  .

The **Windows PowerShell** dialog box is displayed.

Step 31 Run the following command to refresh the policy:

gpupdate /force

Step 32 Press **Enter**. The task is complete.

If the following information is displayed, the policy is successfully refreshed:

```
Updating Policy...
User Policy update has completed successfully.
Computer Policy update has completed successfully.
```

NOTE

- Other component servers will synchronize the new policy. The synchronization mechanism determines the specific synchronization time.
- The new policy is synchronized after component servers are restarted.

----End

2.23.7 How Do I Create a User OU on the AD Server?

Create an organization unit (OU) for the user domain on the active AD server to manage all the domain users and user groups. Child OUs can also be created in the OU based on the enterprise organization structure.

Step 1 Log in to the active AD server using the administrator account.

Step 2 On the active AD server, choose  > **Windows Administrative Tools** > **Active Directory Users and Computers**.

The **Active Directory Users and Computers** window is displayed.

Step 3 In the navigation pane on the left, right-click a *domain name*, and choose **New** > **Organizational Unit**.

The **New Object - Organizational Unit** window is displayed.

Step 4 Enter the OU name in the **Name** text box and click **OK**.

NOTE

The OU name cannot contain the following special characters: ^<>|#+",=;\%

To create a child OU, right-click the name of the parent OU and choose **New** > **Organizational Unit**.

----End

2.23.8 How Do I Create a User Group on the AD Server?

Administrators can create a user group in the user OU of the active AD server to centrally manage users in different user groups.

Step 1 Log in to the active AD server using the administrator account.

Step 2 On the active AD server, choose  > **Windows Administrative Tools** > **Active Directory Users and Computers**.

The **Active Directory Users and Computers** window is displayed.

Step 3 In the navigation pane on the left, right-click the target OU name and choose **New** > **Group**.

The **New Object - Group** window is displayed.

Step 4 Set **Group name**, retain the default values for **Group scope** and **Group type**, and click **OK**.

NOTE

The group name consists of digits, letters, spaces, and special characters: `~!#$%^&()-_{}.

The user group is created. The new user group is displayed in the right pane.

----End

2.23.9 How Do I Create a User on the AD Server?

Administrators can create a domain user in the user OU of the active AD server and add the domain user to a user group to manage domain users with different rights.

Step 1 On the active AD server, choose > **Windows Administrative Tools** > **Active Directory Users and Computers**.

The **Active Directory Users and Computers** window is displayed.

Step 2 In the navigation pane on the left, right-click the target OU name and choose **New** > **User**.

The **New Object - User** window is displayed.

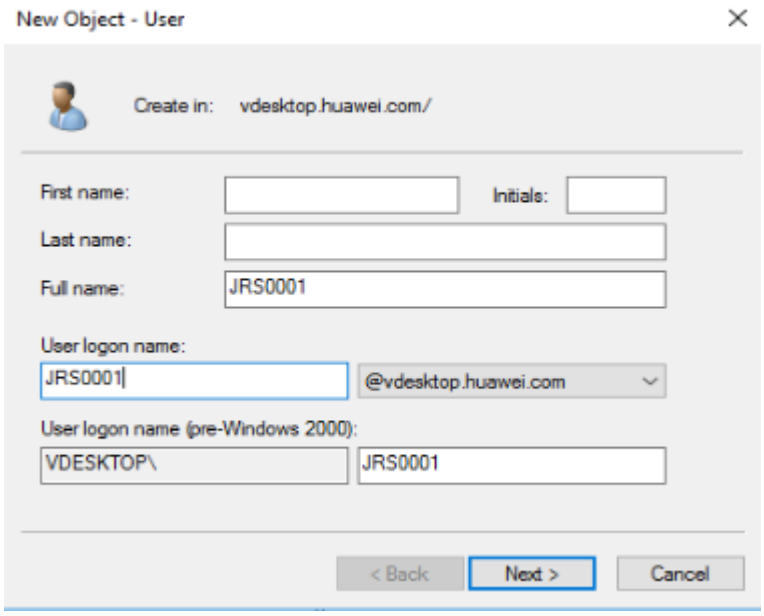
Step 3 Configure registration information of the domain user.

Figure 2-46 shows an example.

NOTE

- The user login name contains 1 to 20 characters, including uppercase letters, lowercase letters, digits, hyphens (-), and underscores (_).
- **User logon name** indicates the domain account for the user. The username created on the Workspace Application Streaming console must be the same as the user login name.
- If **User logon name** is different from **User logon name (pre-Windows 2000)**, **User logon name (pre-Windows 2000)** is used as the user login domain account. Ensure the username created on the Workspace Application Streaming console is as same as the **User logon name (pre-Windows 2000)**.

Figure 2-46 Creating a user



Step 4 Click **Next**.

Step 5 In **Password** and **Confirm Password**, enter the password of the domain user.

Step 6 Select **User must change password at next logon** and click **Next**.

Step 7 Click **Finish**.

The domain user is successfully created. The new domain user is displayed in the right pane.

Step 8 Decide whether to add the domain user to a user group.

- If yes, go to **Step 9**.
- If no, no further operation is required.

Step 9 In the right pane, right-click *User name* and choose **Add to a group**.

The **Select Groups** window is displayed.

Step 10 Enter the user group name in **Enter the object names to select**.

Step 11 Click **OK**.

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

----End

2.23.10 How Do I Configure Network Connection Between Workspace Application Streaming and the Windows AD?

Scenarios

When the Windows AD is deployed on the enterprise intranet or in the same VPC as Workspace Application Streaming, you need to configure the network connection between Workspace Application Streaming and the Windows AD.

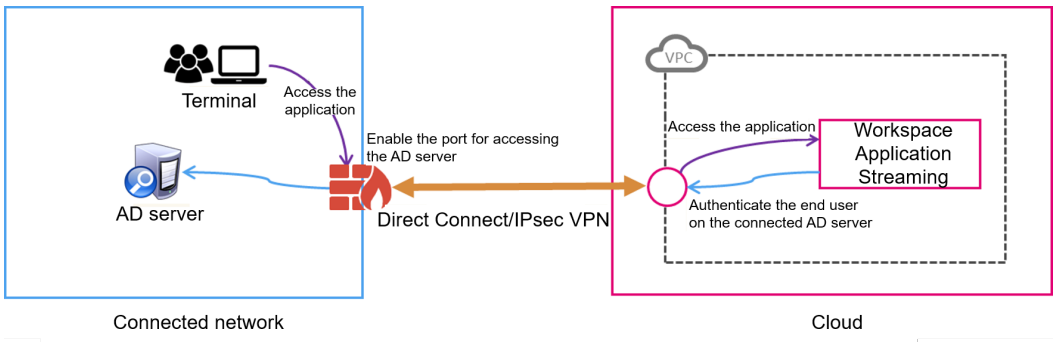
Prerequisites

You have obtained the domain administrator account and password.

Procedure

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

Figure 2-47 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 Virtual Private Network **Administrator Guide**.

Step 2 If a firewall is deployed between the Windows AD and the cloud application, enable the following ports on the firewall for successful connection, as shown in **Table 2-37**.

Table 2-37 Port list

Role	Port	Protocol	Description
AD	135	TCP	Port for the Remote Procedure Call (RPC) protocol (LDAP, DFS, and DFSR)
	137	UDP	Port for NetBIOS name resolution (network login service)
	138	UDP	Port for the NetBIOS data gram service (DFS and network login service)
	139	TCP	Port for the NetBIOS-SSN service (network basic input/output)
	445	TCP	Port for the NetBIOS-SSN service (network basic input/output)
	445	UDP	Port for the NetBIOS-SSN service (network basic input/output)
	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

Role	Port	Protocol	Description
DNS	53	TCP	DNS server
	53	UDP	DNS server

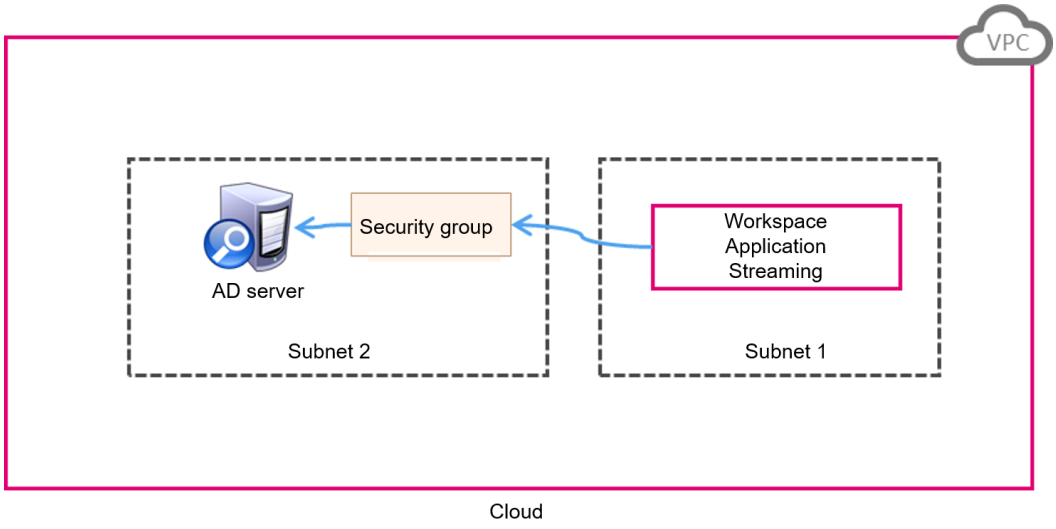
Step 3 After the configuration is complete, check whether the networks and ports are working properly by referring to **Verification Method**.

----End

Scenario 2: Deploying the Windows AD in another subnet of the VPC where the cloud application is located

In this scenario, you need to add security group rules for the Windows AD and open some ports of the Windows AD to the cloud application so that the cloud application can connect to the Windows AD.

Figure 2-48 Deploying the Windows AD in another subnet of the VPC where the cloud application is located



Step 1 **Create a security group** in the VPC.

Step 2 **Add an inbound rule to the security group**.

Step 3 After the security group is created, apply the security group to the Windows AD management server instance so that the cloud application 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 2-37**.

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 2-37** 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 APS is located and add the instance to an existing domain.

NOTE

For details about ECS configurations and operations, see **ECS User Guide**.

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

2.23.11 How Do I Log in to an APS?

- Use the server login tool to log in to an APS as a local or domain administrator.
- Log in to an APS from the Workspace Application Streaming console in remote login mode.
  a. Log in to the Workspace Application Streaming **console** as an administrator.
  b. In the navigation pane, choose **Server Groups**.
  c. Click the name of the server group to which the server belongs.
  d. Click **Remote Login** in the **Operation** column of the server.

2.23.12 How Do I Purchase the NAT and EIP Services to Enable Cloud Applications to Be Accessed Through the Internet?

Scenarios

After the administrator publishes an application, the cloud application is in the VPC subnet by default and cannot access the Internet. The administrator needs to configure the NAT gateway to share an EIP so that users can access and use Workspace Application Streaming using the Internet access address. If a cloud application has multiple service subnets, the Internet function must be enabled for each service subnet.

NOTE

Workspace Application Streaming and Workspace share the same network. If a desktop exists in the same subnet of the same project and the administrator has enabled Internet access for the desktop, end users can directly access the application. If only cloud applications exist in the subnet of the current project, the administrator needs to access the NAT and EIP pages to purchase the corresponding services and enable the Internet.

Prerequisites

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

  NOTE

  - By default, a Huawei Cloud account has the operation permissions on all Huawei Cloud services. If you use such an account, you do not need to confirm it.
  - To use NAT and EIP, the IAM account created under the Huawei Cloud 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 **NAT** and **EIP**.

Procedure

Creating an EIP

Step 1 Log in to the console as an administrator.

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

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

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

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

NOTE

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

Step 6 Click **Next**.

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

Buying a public NAT gateway

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

Step 9 Click **Buy Public NAT Gateway**. The **Buy Public NAT Gateway** page is displayed.

Step 10 Configure the parameters by referring to the parameter description in **Buying a Public NAT Gateway**.

NOTE

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

Step 11 Click **Next**.

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

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

Checking whether the VPC has a route to the NAT gateway

Step 14 Log in to the Workspace Application Streaming console and choose **Tenant Configuration**.

Step 15 Click the VPC name of the tenant to go to its basic information page.

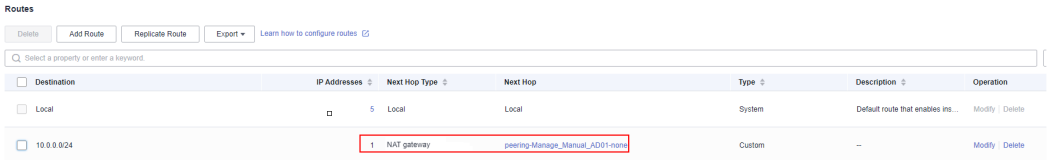
Step 16 In the **Networking Components** area on the right of the page, click the *number next to* ***Route Tables*** to go to the route table list page of the VPC.

Step 17 Click *the name of the target route table*. The basic information list is displayed.

Step 18 Check whether there is a route whose next hop is the NAT gateway in the route list.

The NAT gateway automatically creates a route 0.0.0.0/0 from the VPC to the NAT gateway to allow traffic from the VPC to the NAT gateway, as shown in **Figure 2-49**.

Figure 2-49 Route to the NAT gateway



- If the route shown in **Figure 2-49** exists, go to **Step 19**.
- If the route shown in **Figure 2-49** does not exist, add such a route and go to **Step 19**.

Adding an SNAT rule

Step 19 Click ☰ and choose **Networking** > **NAT Gateway** in the service list.

Step 20 On the displayed page, locate the NAT gateway created in **Step 12** and choose **Operation** > **Configure Rules**.

Step 21 On the **SNAT Rules** tab page, click **Add SNAT Rule**.

Step 22 Configure the parameters by referring to the parameter description in **Adding an SNAT Rule**.

NOTE

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

Step 23 Click **OK**.

If the added SNAT rule is in the **Running** state, the rule is added successfully.

Configuring DNS forwarding

Step 24 Log in to the DNS server as the administrator.

Step 25 On the taskbar in the lower left corner, click  .

Step 26 Click  on the right of the **Start** menu.

Step 27 The **Server Manager** window is displayed.

Step 28 In the left navigation pane, click **DNS**.

Step 29 In the **SERVERS** area, right-click a *Server name* and choose **DNS Manager** from the shortcut menu.

Step 30 The **DNS Manager** dialog box is displayed.

Step 31 Expand **DNS**. Right-click the computer name, and choose **Properties** from the shortcut menu.

Step 32 On the **Advanced** tab page, deselect **Disable recursion (also disable forwarders)** and click **Apply**.

Step 33 On the **Forwarder** tab page, click **Edit**, enter the default DNS server IP address of the cloud application region in the text box, and click **OK**.

NOTE

The default DNS server IP address of the Workspace Application Streaming region can be obtained from **Huawei Cloud Private DNS Server Addresses**.

Verifying whether Workspace Application Streaming can be accessed using the NAT gateway

Step 34 Log in to Workspace Application Streaming as an end user using the Huawei Cloud Workspace client to check whether the service can be used.

----End

2.23.13 How Do I Check My Quotas?

NOTE

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

Step 1 Open the **Huawei Cloud homepage** and click **Console** in the upper right corner. Log in to the console as an administrator.

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

Step 3 Choose **Resources** > **My Quotas** in the upper right corner of the page.

The **Quotas** page is displayed.

----End

2.23.14 How Do I Increase My Quotas?

NOTE

You can only increase quotas of the current administrator account.

Step 1 Open the **Huawei Cloud homepage** and click **Console** in the upper right corner. Log in to the console as an administrator.

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

Step 3 Choose **Resources** > **My Quotas** in the upper right corner of the page.

The **Quotas** page is displayed.

Step 4 Click **Increase Quota**.

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

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

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

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

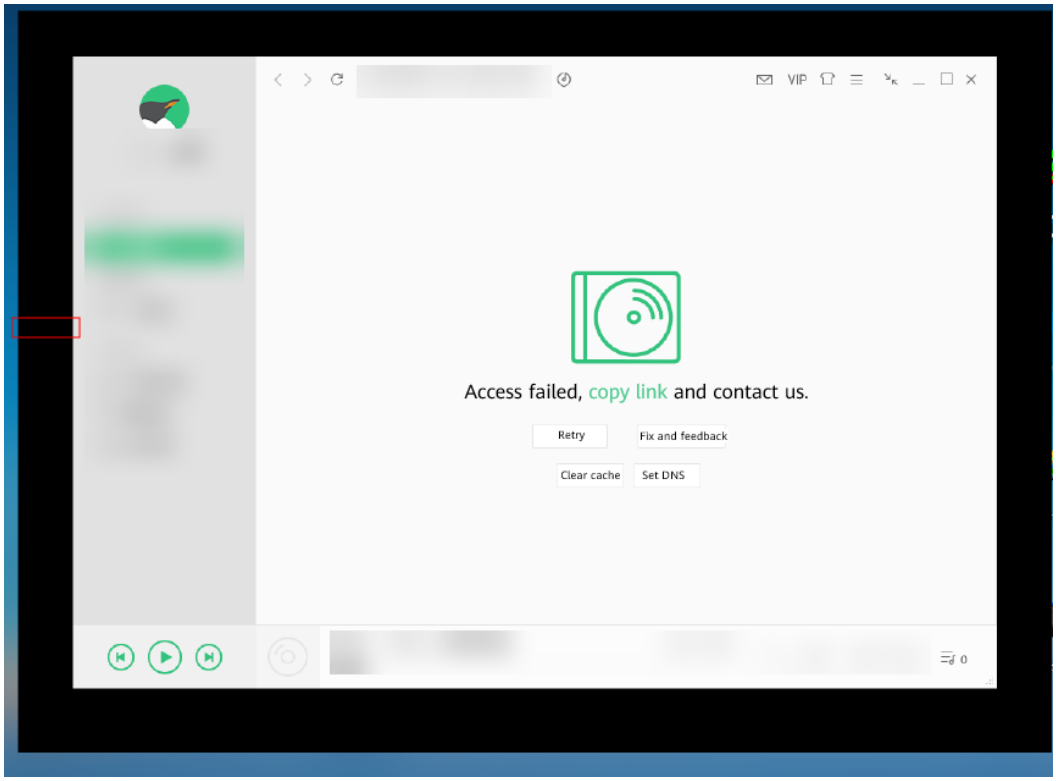
----End

2.23.15 How Do I Do If the Application Operation Page Has Black Borders and Cannot Be Moved?

Symptom

The operation pages of some applications have black borders and cannot be moved. See **Figure 2-50**.

Figure 2-50 Symptom example



Solution

Step 1 Log in to the APS where the application is published as the administrator.

Step 2 Click and enter **Regedit** to open the registry editor.

Step 3 Check whether the **TransparentWindows** registry exists in **Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Huawei\HDPServer\Rail**.

- If no, go to **Step 4**.
- If yes, go to **Step 6**.

Step 4 Right-click in the blank area on the right and choose **New** > **Multi-String Value**.

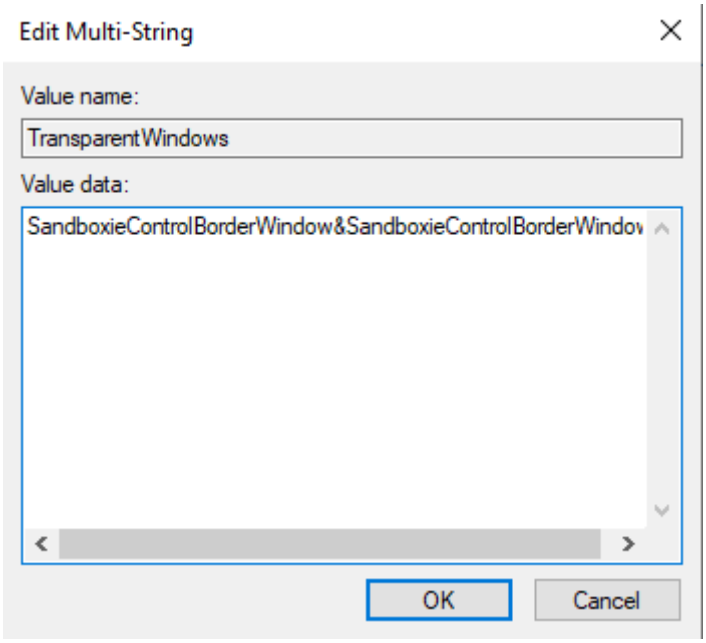
Step 5 Name the registry **TransparentWindows**.

Step 6 Double-click **TransparentWindows**. The page for editing multiple strings is displayed.

Step 7 Enter **QMShadowWndClass;TXGuiFoundation&playerShadow** in **Value data** based on whether the value data exists in the value data list.

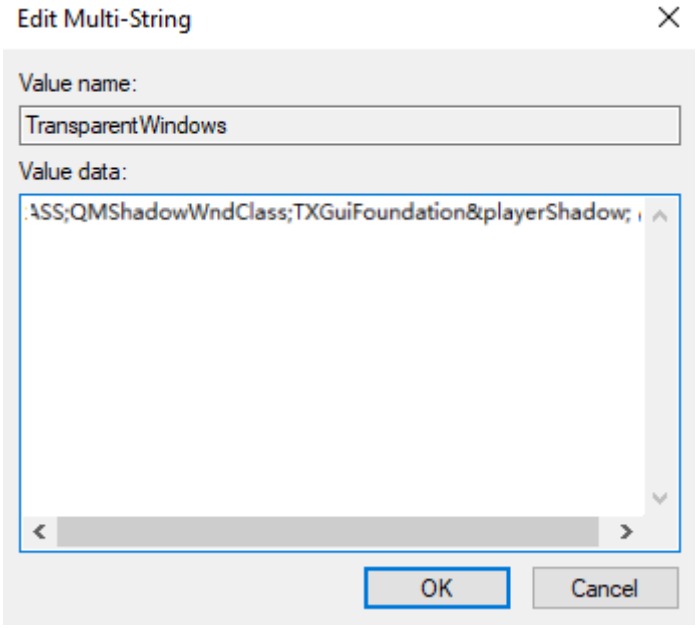
- If the **TransparentWindows** registry does not contain other values, add **QMShadowWndClass;TXGuiFoundation&playerShadow**. See **Figure 2-51**.

Figure 2-51 Example of registry containing no other values



- If other value data already exists in the **TransparentWindows** registry, add **;QMShadowWndClass;TXGuiFoundation&playerShadow** to the end of the value data. See **Figure 2-52**.

Figure 2-52 Example of registry containing other values



The value varies with applications. Select a value based on the application.

- WeChat: **EmotionWnd; popupshadow; CMenuWnd**
- WPS: **KPromeMainWindowShadowBorder;Qt5QWindowIcon;KDlgBorder**
- NetEase Music: **OrpheusShadow**

- QQ Music and QQ Player: **QMShadowWndClass;TXGuiFoundation&playerShadow**
- Google Chrome: **Chrome_WidgetWin_1&0x96000000**
- WeCom: **PerryShadowWnd**
- Sogou IME: **SoPY_Hint&HintWnd;SoPY_Status**
- DingTalk: **DuiShadowWnd**
- iArtist: **Qt5152QWindow&iArtist**
- Sandboxie: **SandboxieControlBorderWindow&SandboxieControlBorderWindow**

NOTE

Use semicolons (;) to separate multiple values.

Step 8 Click **OK** and close the registry editor.

Step 9 Click  and choose **Power** > **Restart** to restart the APS.

----End

2.23.16 How Do I Do If an End User Fails to Log In to a Cloud Application?

Scenarios

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

Procedure

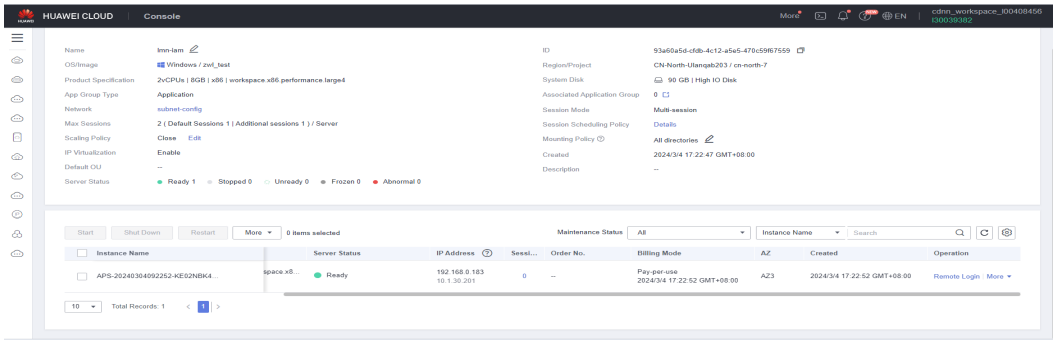
Step 1 Check whether the APS is running properly.

1. Open the **Huawei Cloud homepage** and click **Console** in the upper right corner. Log in to the Workspace Application Streaming console as an administrator.
2. Click **Server Groups**.
3. Click the name of the corresponding server group. On the displayed server list page, check the running status of the server.
   - If the status is **Running**, go to **Step 2**.
   - For other statuses, perform the following operations based on the actual status: If it is still not running, **submit a service ticket** for technical support.
     - When the running status is **Creating**, **Not ready**, or **Restarting**, the waiting status is not **Creating**, **Restarting**, or **Not ready**.
     - If the running status is **Stopped**, you can select a server and click **Start** to restart the server.
     - If the running status is **Abnormal**, restart the server.

Step 2 Check whether the number of sessions on the server reaches the upper limit.

On the server list page, check whether the number of sessions of the server reaches the upper limit, as shown in **Figure 2-53**.

Figure 2-53 Comparing the number of sessions on the server with the maximum number of sessions



- If the number of sessions on the server has reached the upper limit, you can increase the upper limit of sessions for the server group by referring to **2.6.1 Managing Server Groups** and ask the end user to try again later. If the login still fails, **submit a service ticket** for technical support.
- If the number of sessions on the server has not reached the upper limit, **submit a service ticket** for technical support.

----End

2.23.17 How Do I Reset a User Password?

Workspace Application Streaming uses the AD server. To reset the user password, you must log in to the AD server.

Step 1 Log in to the AD server using the administrator account.

Step 2 Choose  > **Windows Administrative Tools** > **Active Directory Users and Computers**.

Step 3 In the navigation pane, expand the directories where user accounts are located in sequence.

The domain user list is displayed in the right pane.

Step 4 Right-click the account whose password is to be changed, and choose **Reset Password** from the shortcut menu.

The **Reset Password** dialog box is displayed.

Step 5 Enter the new password and confirm the new password.

Step 6 Click **OK**.

A dialog box is displayed indicating that the password has been changed.

Step 7 Click **OK**.

Step 8 Inform the end user of the new password.

----End

2.23.18 How Do I Do If I Fail to Add a Computer Back to the Domain?

There are many causes for the failure to add a computer back to the domain. The following uses the error code **1332** as an example to describe how to rectify the fault.

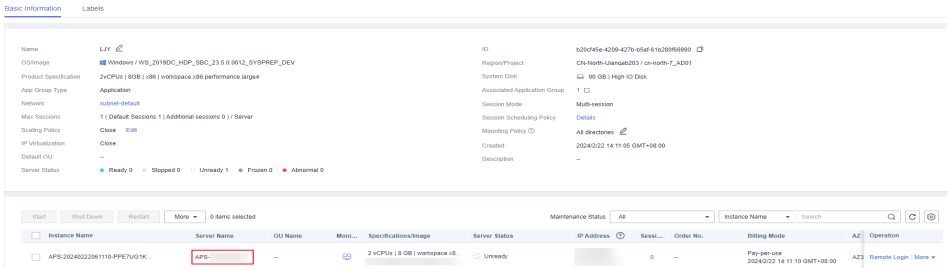
Error code **1332** indicates that a computer may have been deleted from the AD server. Perform the following steps to rectify the fault. If the fault persists, **submit a service ticket** for technical support.

Step 1 Log in to the AD server using the administrator account.

Step 2 Add a desktop in the **Active Directory Users and Computers** dialog box.

1. Choose > **Windows Administrative Tools** > **Active Directory Users and Computers**.
2. Expand the domain server information, right-click **Computers**, and choose **New** > **Computer** from the shortcut menu.
3. Enter the name of the computer to be added to the domain as prompted.
4. Name of the computer to be added back to the domain, that is, the name of the server in the server group, as shown in **Figure 2-54**.

Figure 2-54 Obtaining the computer name



Step 3 Return to the Workspace Application Streaming console. In the navigation pane, choose **Server Groups**.

Step 4 Click the server group name. On the displayed server list page, locate the row that contains the target server, click **More** > **Rejoin Domain**.

Step 5 Confirm the operation.

Step 6 Click **Yes**.

----End

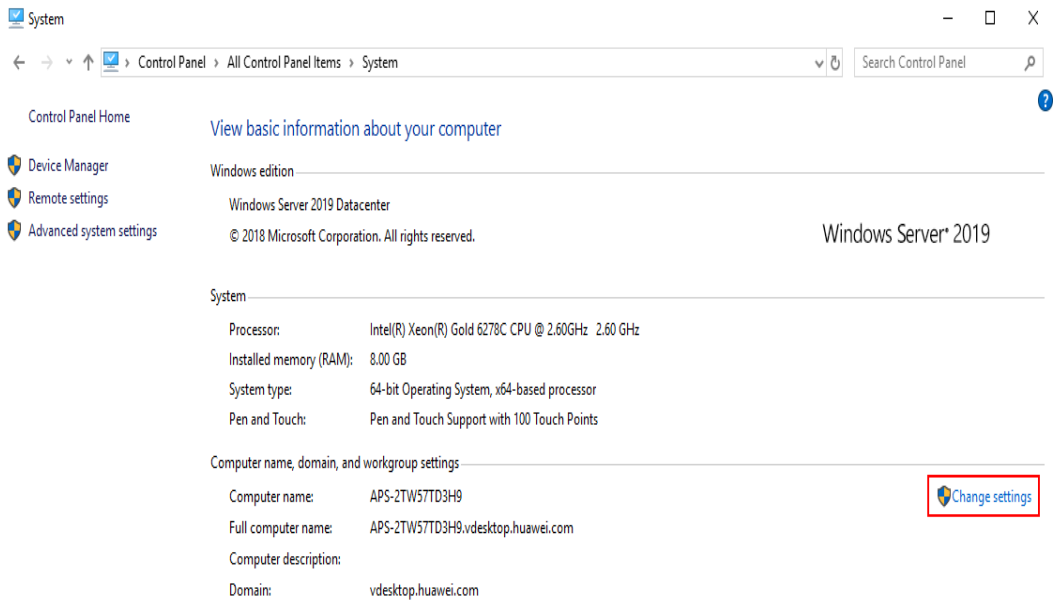
2.23.19 How Do I Add an ECS to the Domain of an APS?

The newly purchased ECS is not added to the domain where the APS resides. Therefore, the sharing configuration cannot be performed. Perform the following operations to add the ECS to the corresponding domain:

The Windows Server 2019 server is used as an example.

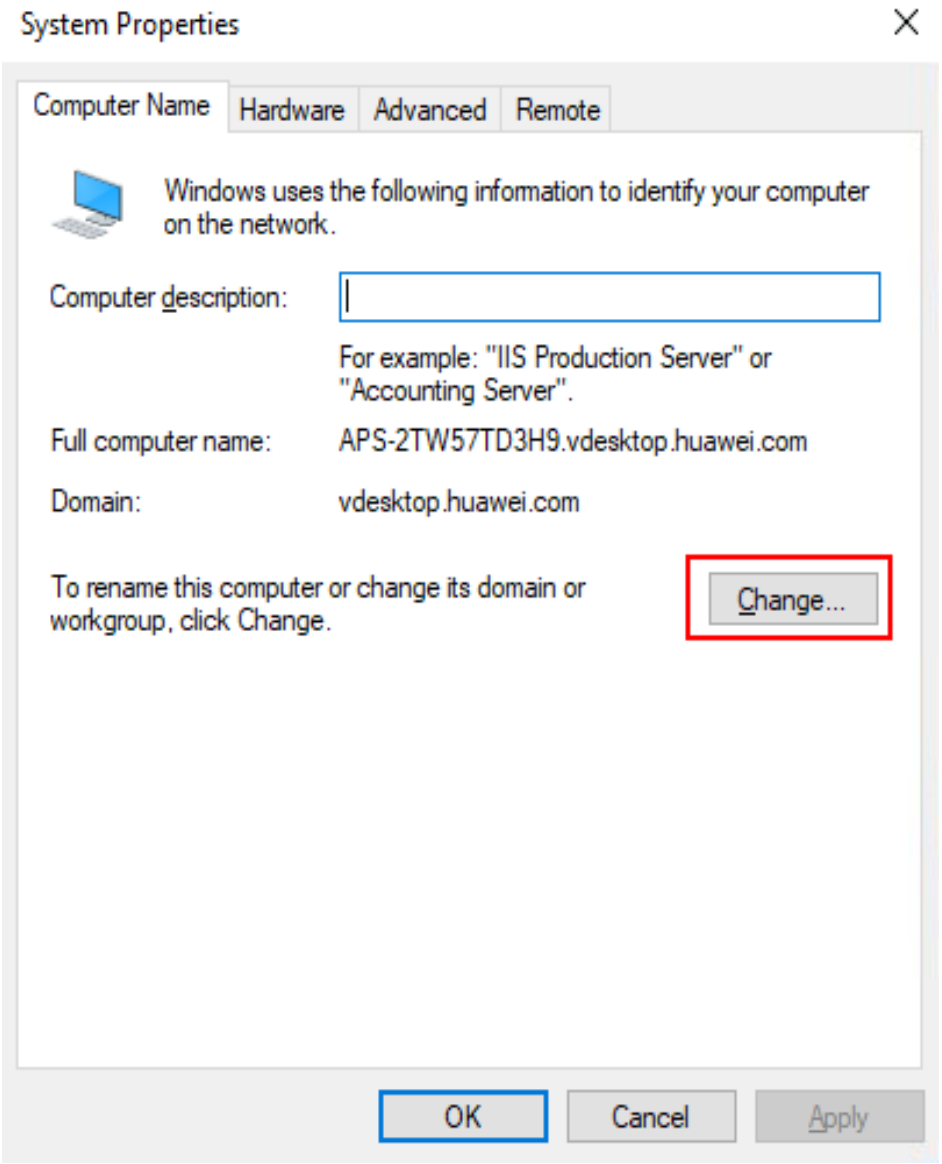
Step 1 On the ECS list page, locate the row that contains the newly purchased ECS, click **Remote Login**, and enter the username and password to log in to the ECS.

Step 2 Go to the Windows Server 2019 desktop, right-click **This PC**, and choose **Properties** from the shortcut menu. The system page is displayed.

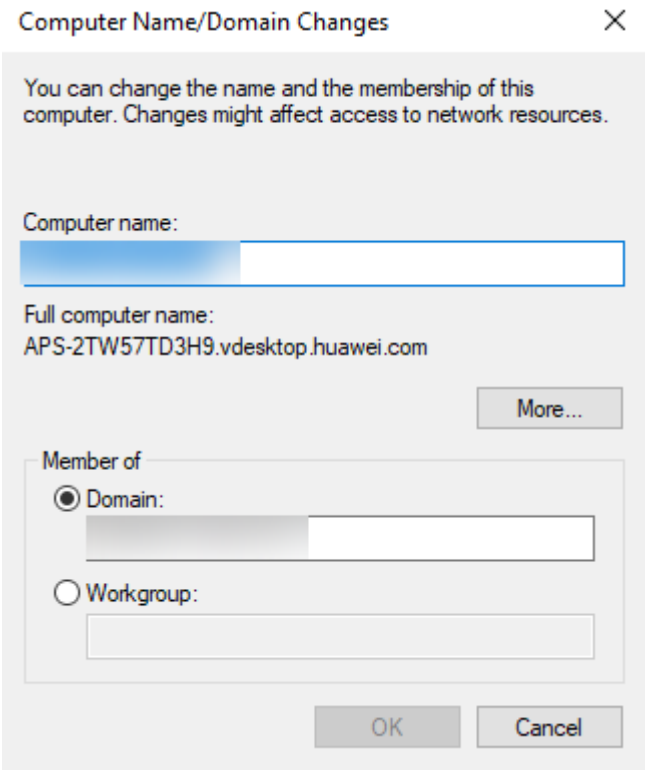


Step 3 In the **Computer name, domain, and workgroup settings** area, click **Change settings**. The **System Properties** page is displayed.

Step 4 On the **Computer Name** tab page, click **Change**. The **Computer Name/Domain Changes** page is displayed.



Step 5 In the **Member of** area, enter the domain name of the cloud application in the **Domain** text box and click **OK**.



Step 6 Enter the administrator account and password of the Workspace Application Streaming domain server, and click **OK**.

Step 7 After the system displays a message indicating that the ECS has been added to the domain, restart the ECS.

----End

2.23.20 How Do I Use the GPO Group Policy to Make a Domain User Become a Local Administrator of a PC?

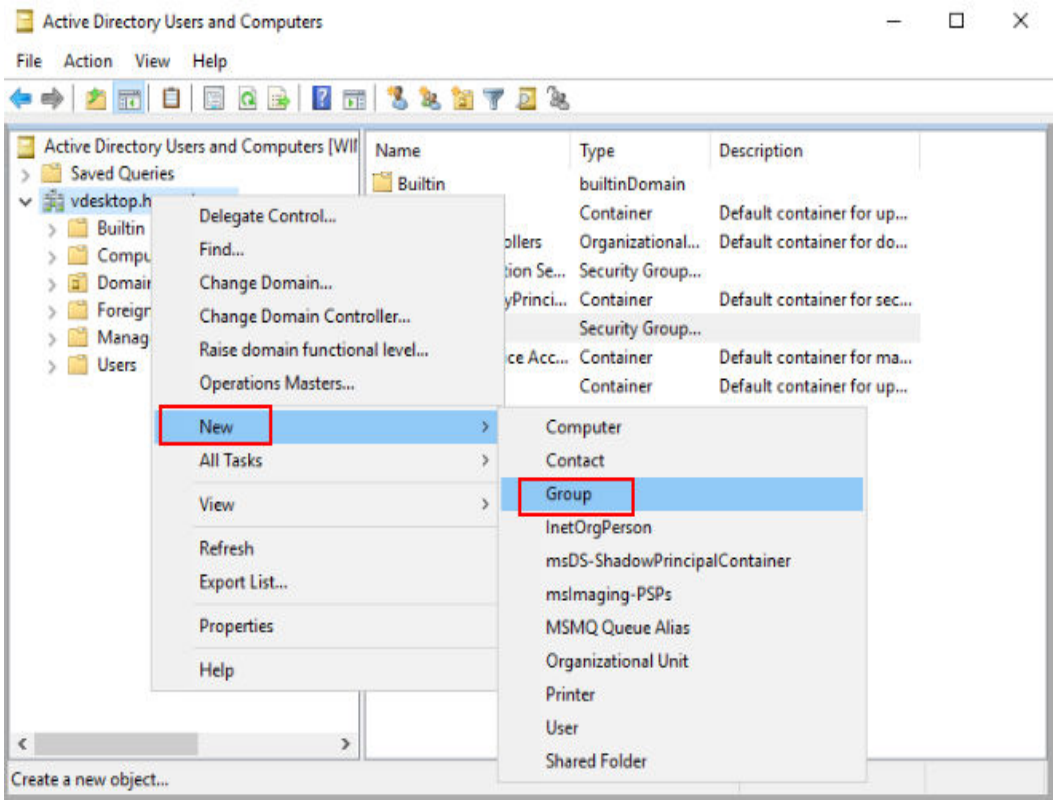
The AD domain administrator can specify a domain user as the local administrator of the PC. The domain user has some permissions of the AD domain administrator and can maintain the functions of the domain server of the Workspace Application Streaming service, for example, updating applications. As a dedicated domain administrator of Workspace Application Streaming, you can improve the security of domain servers and improve maintenance efficiency.

Creating a security group

Step 1 Log in to the AD server as the administrator and open **Server Manager**.

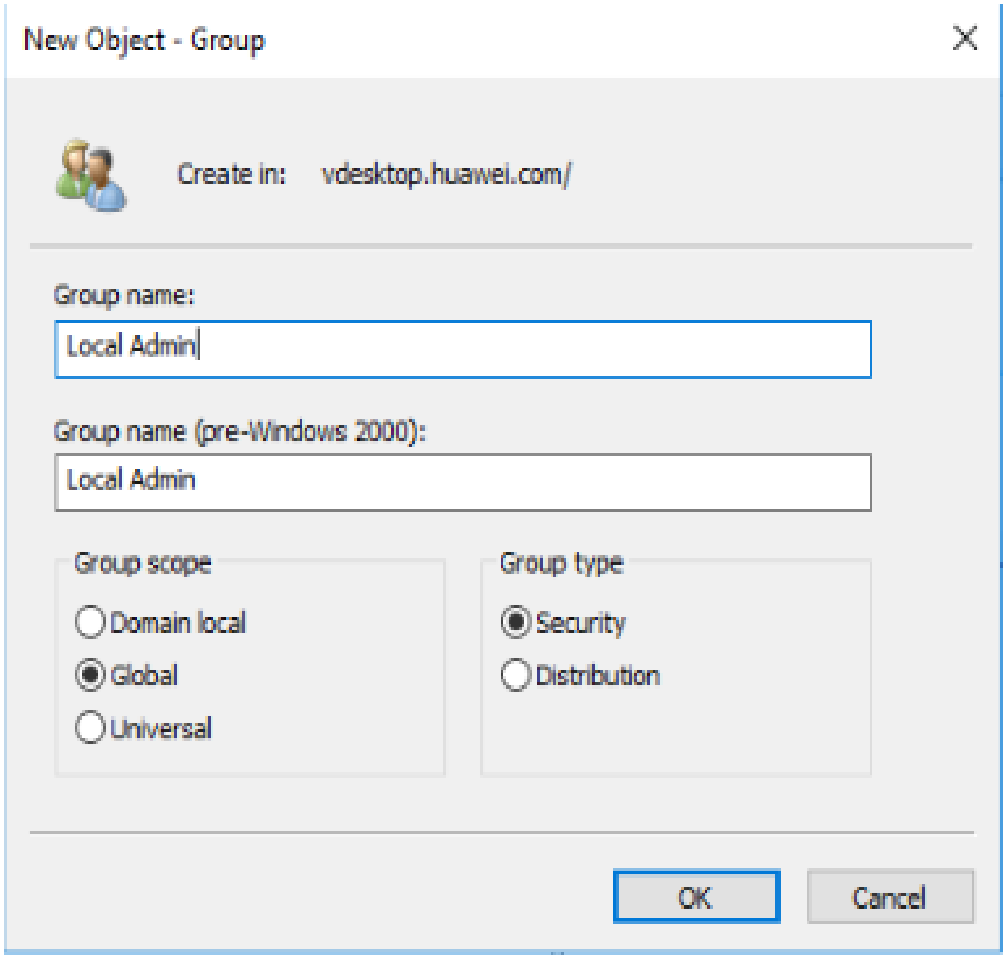
Step 2 Choose **Tools** > **Active Directory Users and Computers**.

Step 3 Right-click a domain and choose **New** > **Group** from the shortcut menu.



Step 4 Enter group information.

- Set **Group name** to **Local Admin**.
- Set **Group scope** to **Global**.
- Set **Group type** to **Security group**.



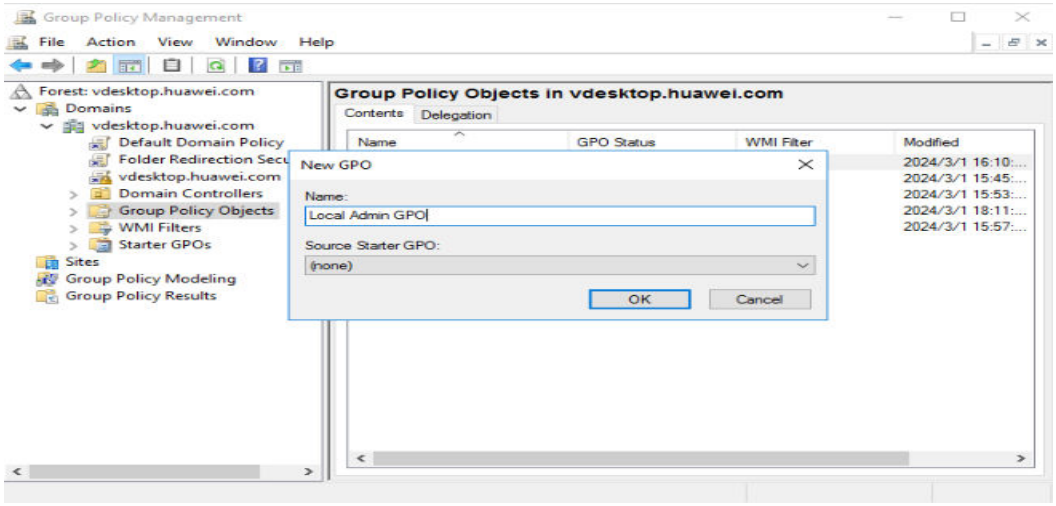
Step 5 Click **OK**.

Step 6 Right-click the **Local Admin** group and choose **Properties** from the shortcut menu. On the **Member** tab page, add a user (a domain user that needs to be used as the local administrator of the PC).

Step 7 Click **OK**.

Creating a GPO group policy

Step 8 Open the **Group Policy Management**, right-click **Group Policy Objects**, and create a GPO named **Local Admin GPO**.

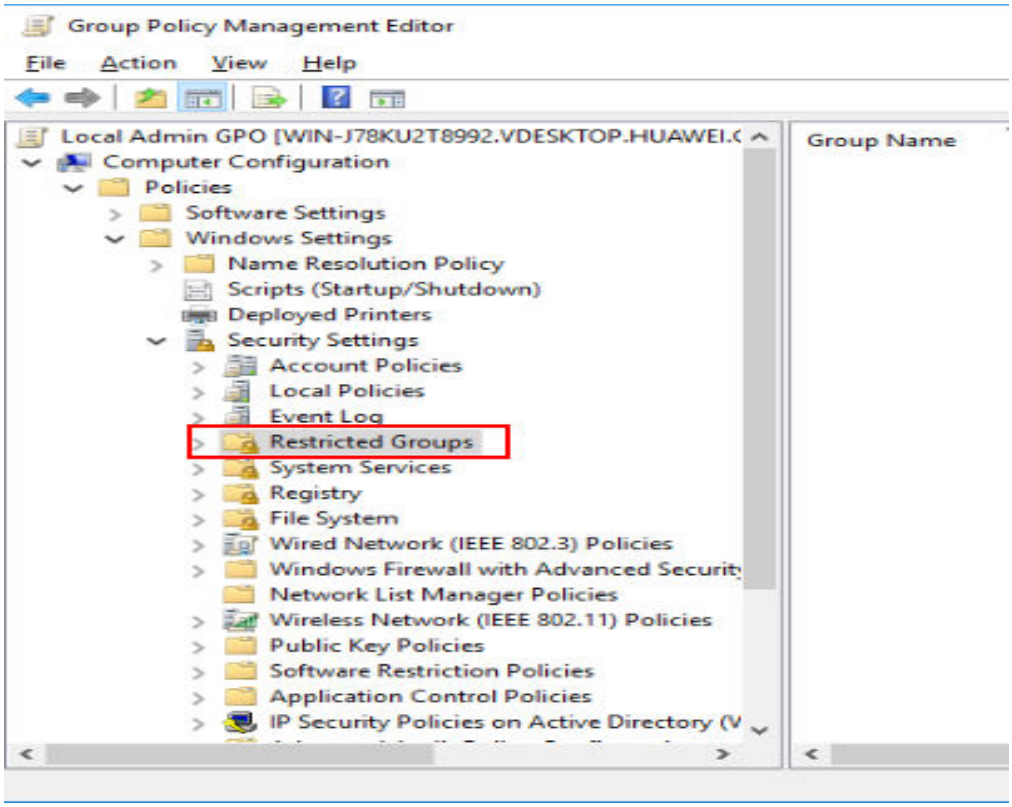


Step 9 Click **OK**.

Configuring the GPO policy

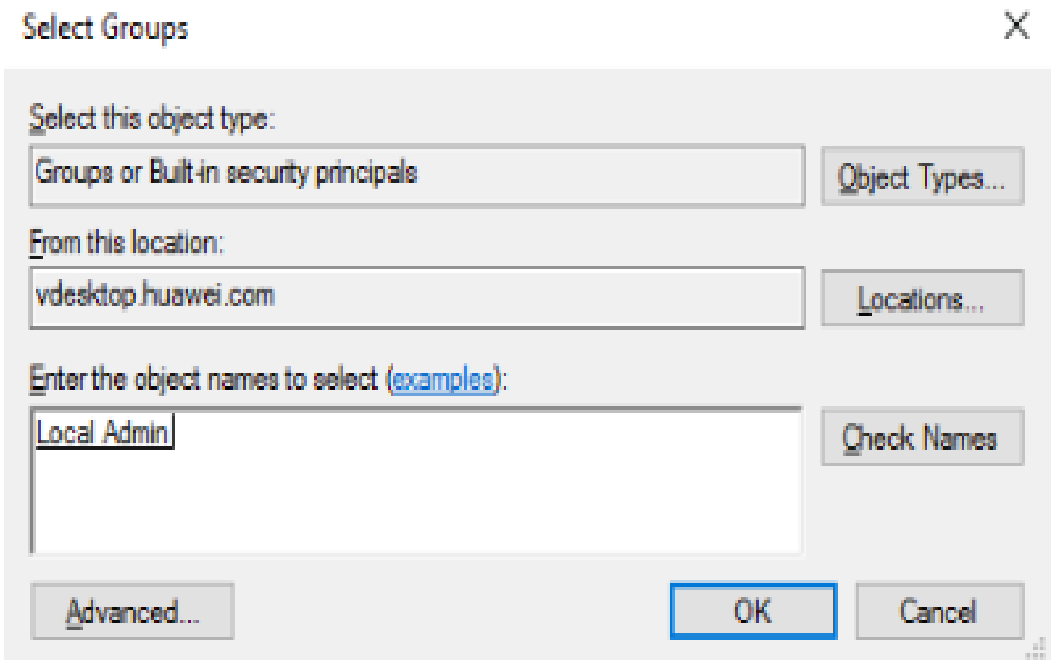
Step 10 Right-click the GPO created in **Step 8** and choose **Edit**. The **Local Group Policy Editor** window is displayed.

Step 11 In the navigation pane, choose **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings**. Right-click **Restricted Groups**.

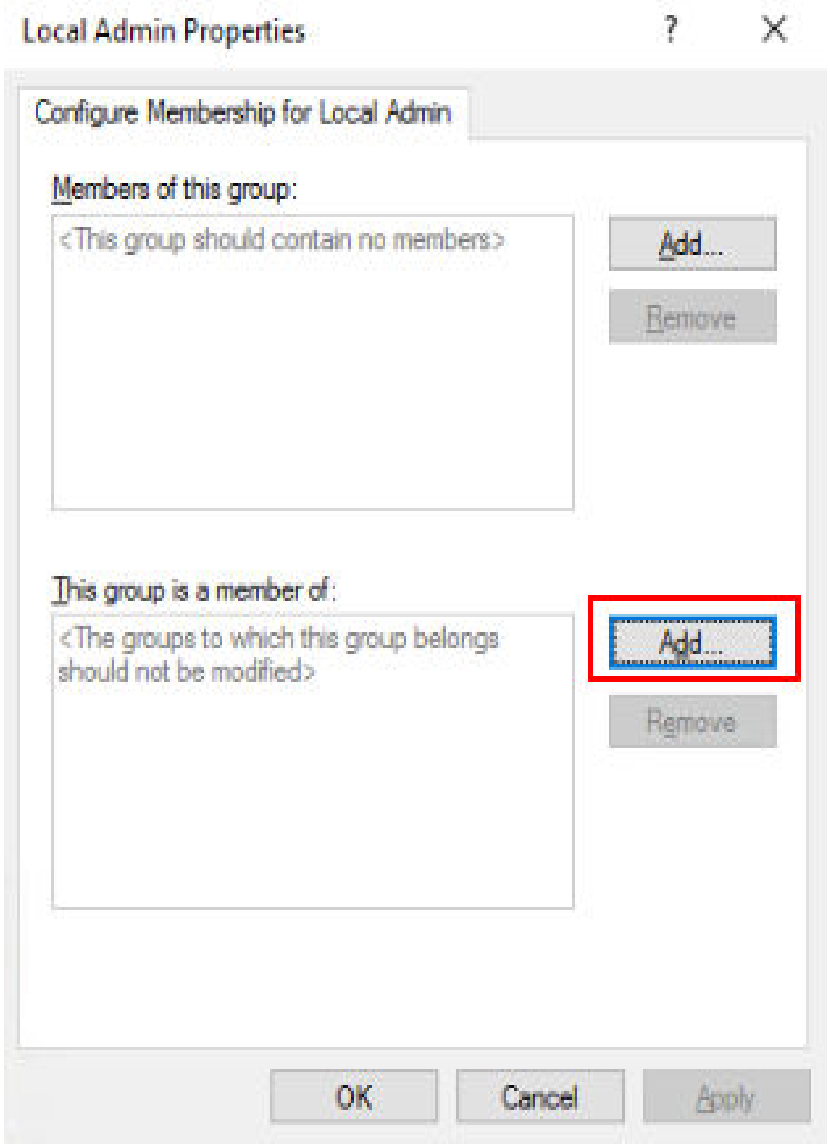


Step 12 Click **Add Group**.

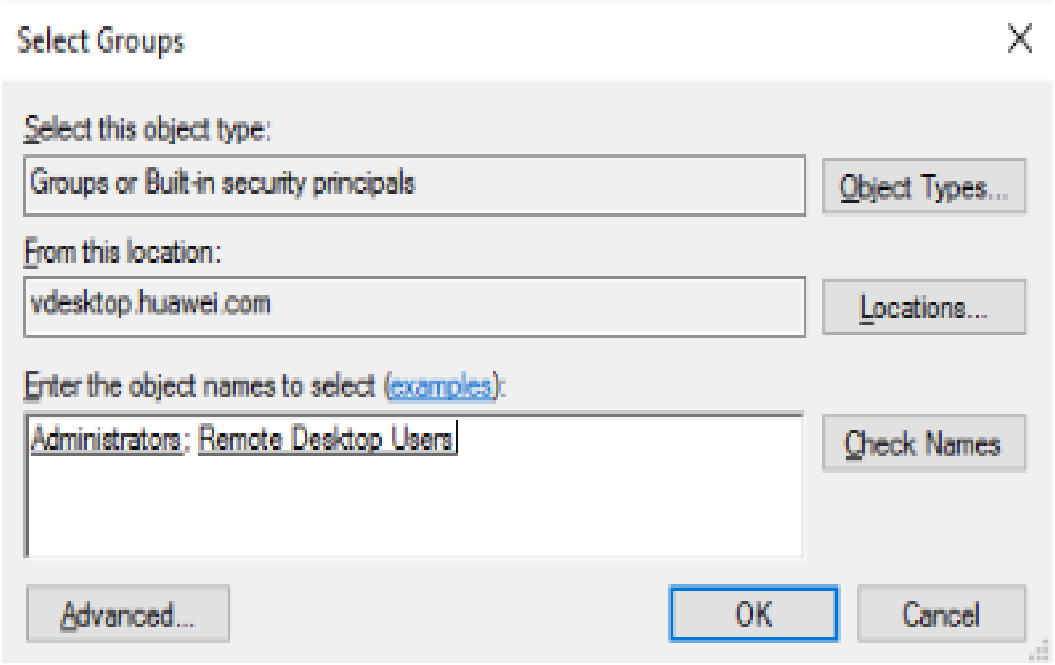
Step 13 Add the **Local Admin** group created in **Step 7** to the restricted group list.



Step 14 Expand the restricted group list, right-click the added **Local Admin** group, and choose **Properties** from the shortcut menu.



Step 15 In the **This group belongs to** area, click **Add**.

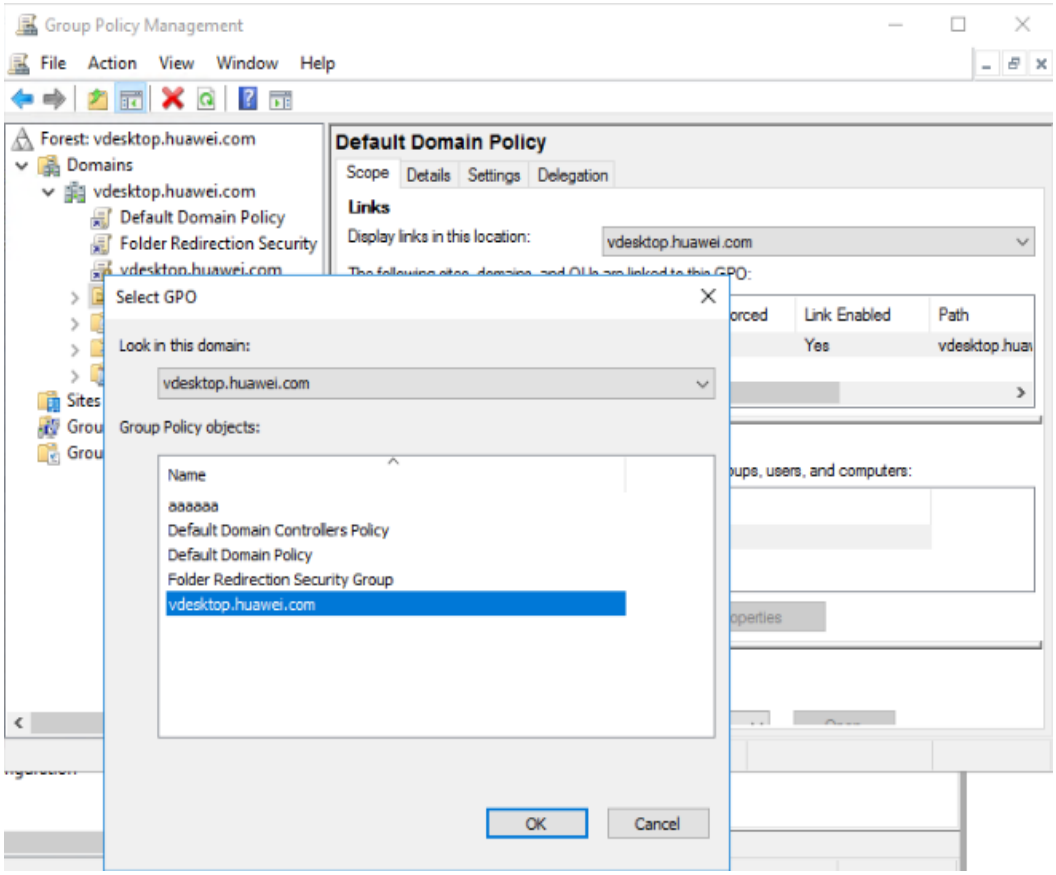


Step 16 Add the **Local Admin** group to the **Administrators** and **Remote Desktop Users** user groups, and click **OK**.

Connecting the Local Admin GPO group policy to a specified OU

Step 17 Open the group policy manager, right-click the OU to which you want to apply the group policy, and choose **Connect existing GPOs** from the shortcut menu.

Step 18 On the GPO list page, select **Local Admin GPO** and click **OK**.



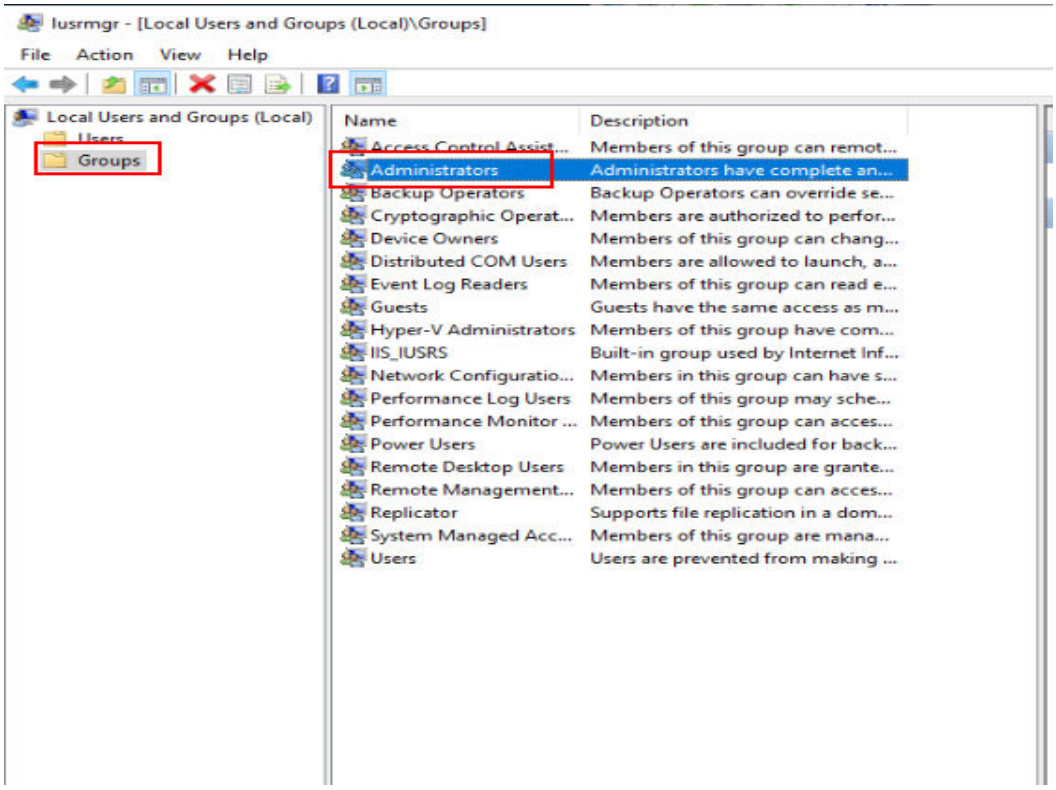
Verifying whether the group policy is configured successfully

Step 19 Add a local PC to the domain where Workspace Application Streaming resides and add the PC to the OU to which the group policy has been applied (for example, **aps OUS** in **Step 18**). For details, see **2.23.19 How Do I Add an ECS to the Domain of an APS?**.

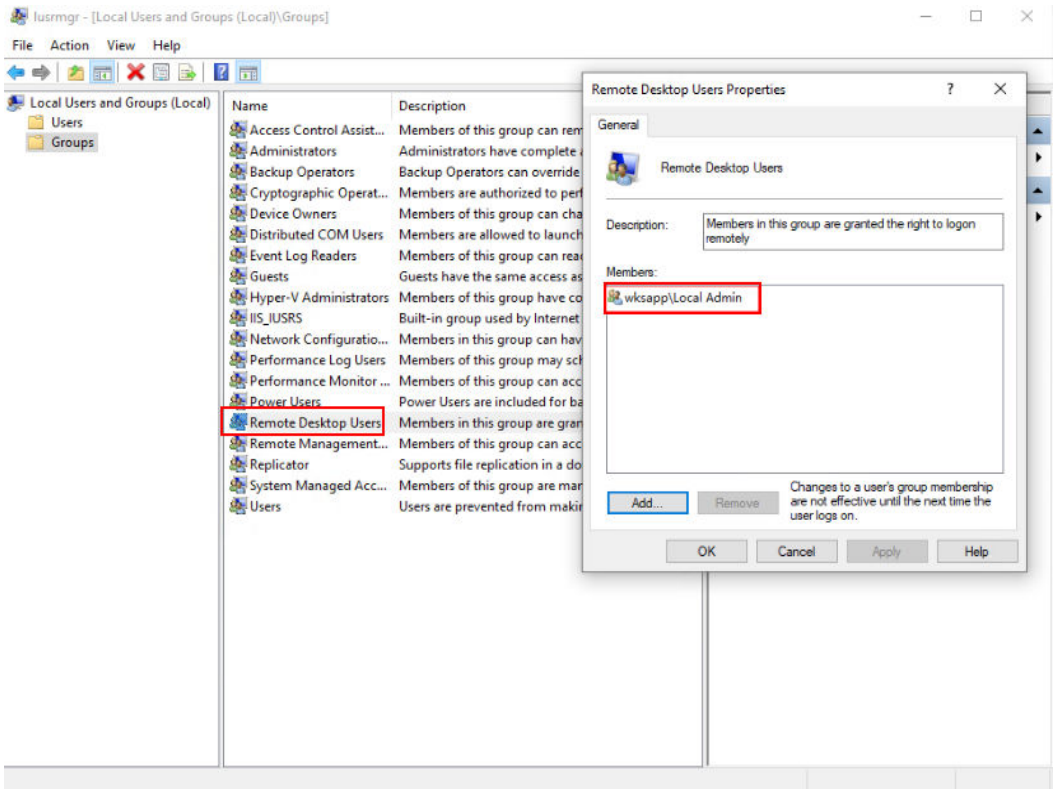
Step 20 Run the following command to open the **Local Users and Groups** page:

lusrmgr.msc

Step 21 Click **Groups**, right-click the **Administrators** user group, and choose **Properties** from the shortcut menu to check whether the **Local Admin** group member is included.



Step 22 Right-click the **Remote Desktop Users** user group and choose **Properties** from the shortcut menu to check whether the **Local Admin** group member is included.



Step 23 Restart and log in to the PC, open the cmd CLI, and run the following command to perform forcible update:

gpupdate /force

----End

2.23.21 How Do I Install Sandbox Software?

Scenarios

This section describes how to install the sandbox software.

Prerequisites

- You have created an APS.
- **Click here** to obtain the sandbox software package.

Procedure

Step 1 Log in to the **Workspace Application Streaming console** as an administrator.

Step 2 In the navigation pane, choose **Server Groups**.

Step 3 Click the name of the server group where the sandbox software is to be installed.

Step 4 Upload the Sandboxie software to the APS in any of the following ways:

Method 1: Use the image repository to synchronize the download link to the server for download. For details, see **2.5.2 Image Creation**.

Method 2: Enable policy management and copy the software from the local PC to the server. For details, see **2.9.1 Creating a Policy Group**.

Method 3: Enable the Internet access function and download the software from the website. For details, see **2.21.1 Allowing Workspace Application Streaming to Access the Internet**.

Step 5 Double-click the sandbox software package to install it, select the installation language as required, and click **OK**. The **License Agreement** page is displayed.

Step 6 Read the agreement and click **I Accept**. On the displayed **Select Installation Location** page, select an installation location as required and click **Install**.

Step 7 After the installation is complete, click **Next** to go to the driver installation page.

Step 8 Click **Next** to complete the sandbox software installation.

NOTE

After the software is installed, a software compatibility check dialog box is displayed. You can select a check item as required.

----End

Introduction to the Sandbox

Sandboxie runs your applications in an isolated abstract area called sandbox. Under the supervision of Sandboxie, applications can run properly at full speed, but do not cause permanent changes to your computer. Instead, the changes take effect only in the sandbox.

Getting Started

Find the **Sandboxie Control** program from the **Start** menu of Windows and click it to open the **Sandboxie Control** console. Click **Help** and select **Getting Started**. You can view the basic usage principles of Sandboxie according to the tutorial.

Application Scenarios

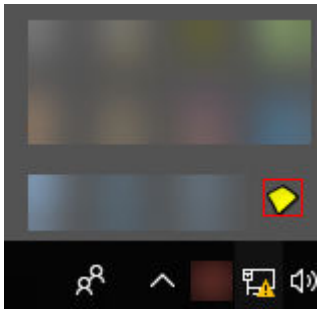
You can install Sandboxie on the APS to use the same application when there are multiple applications and sessions.

Software Configuration

Sandbox control

- Sandboxie runs through Sandboxie Control. The program adds the yellow Sandboxie icon to the notification area of the taskbar, as shown in **Figure 2-55**.

Figure 2-55 Icon



- If **Sandboxie Control** is not activated, you can find and start it from the Sandboxie program group in the Windows **Start** menu, as shown in **Figure 2-56**.

Figure 2-56 Starting the program

- Once activated, you can use the Sandboxie tray icon to hide and display the main window of Sandboxie Control. Double-click the icon or you can right-click the icon and select the first command, which alternates between the hidden window and the displayed window.

2.23.22 How Do I Do If There Is No Sound or the Screen Is Frozen While There Is Sound When Using Google Chrome or Bilibili Player for Video Playback?

Scenarios

End users encounter no sound or frozen screen in video playback using Google Chrome or Bilibili player.

Procedure

Example of using Google Chrome:

In application mode:

Step 1 Log in to the **Workspace Application Streaming console** as an administrator.

Step 2 In the navigation pane, choose **Application Groups**.

Step 3 Click the application group containing the Google Chrome application.

Step 4 Locate the row that contains the Google Chrome application, click **Modify**, and enter **--no-sandbox --force-wave-audio** for **Command Parameter**, and click **OK**.

Step 5 Refresh the client and try again.

In shared desktop mode:

Step 6 Log in to the shared desktop, right-click the Google Chrome shortcut, and choose **Properties**.

Step 7 Append **--no-sandbox --force-wave-audio** to the value of Target (T).

Step 8 Restart Google Chrome.

----End

2.23.23 How Do I Do If the Window Cannot Be Dragged When the Sandbox Application Is Started?

Procedure

Step 1 Log in to the APS where the application is published as the administrator.

Step 2 Click  and enter **Regedit** to open the registry editor.

Step 3 Check whether the **TransparentWindows** registry exists in **Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Huawei\HDPServer\Rail**.

- If no, go to **Step 4**.
- If yes, go to **Step 6**.

Step 4 Right-click in the blank area on the right and choose **New** > **Multi-String Value**.

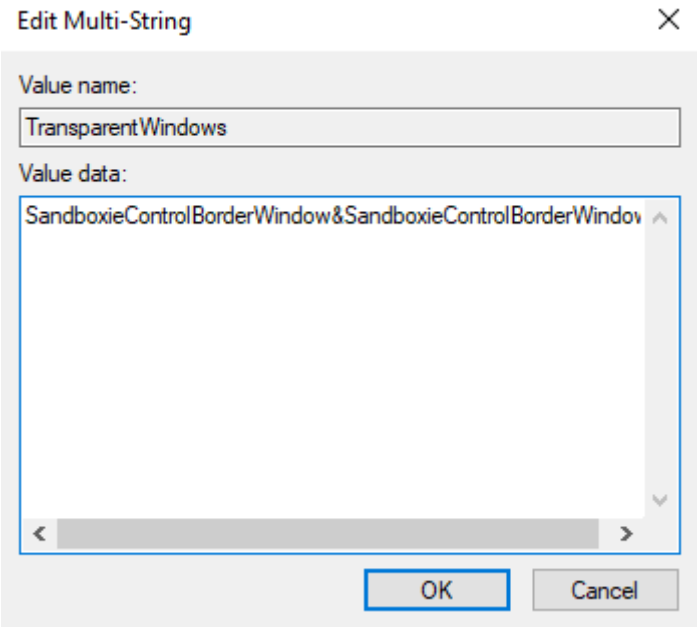
Step 5 Name the registry **TransparentWindows**.

Step 6 Double-click **TransparentWindows**. The page for editing multiple strings is displayed.

Step 7 Enter **SandboxieControlBorderWindow&SandboxieControlBorderWindow** in **Value data** based on whether the value data exists in the value data list.

- If the **TransparentWindows** registry does not contain other values, add **SandboxieControlBorderWindow&SandboxieControlBorderWindow**, as shown in **Figure 2-57**.

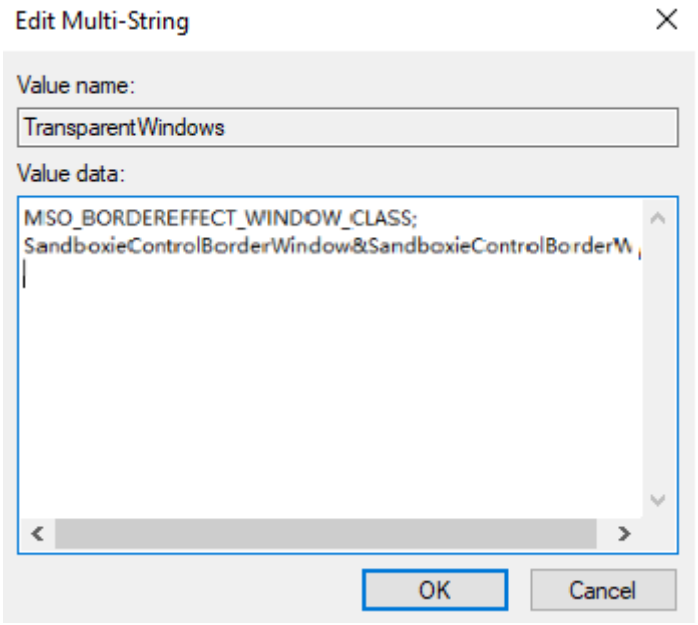
  Figure 2-57 Example of registry containing no other values

- If other value data already exists in the **TransparentWindows** registry, add **SandboxieControlBorderWindow&SandboxieControlBorderWindow** to the end of the value data.

  Figure 2-58 shows an example.

Figure 2-58 Example of registry containing other values



Step 8 Click **OK** and close the registry editor.

Configuring the path access permission in the sandbox

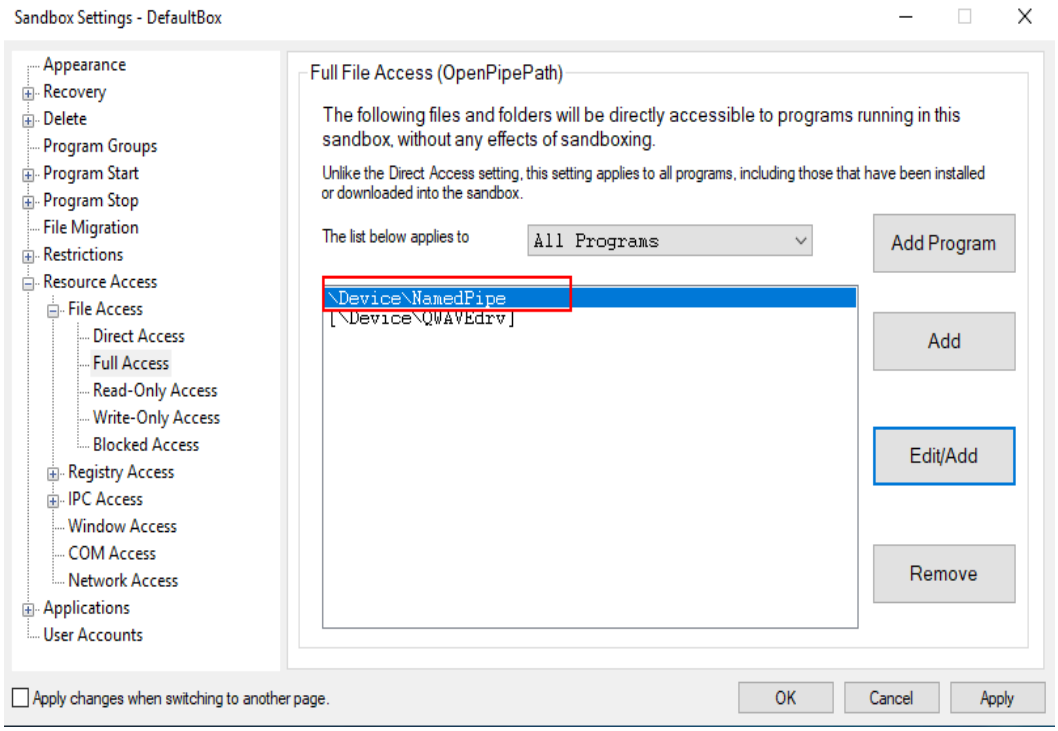
Step 9 On the APS, right-click the **Sandboxie Control** tray icon to go to the console.

Step 10 Right-click **Sandbox** and choose **Sandbox Settings** from the shortcut menu.

Step 11 Choose **Resource Access** > **File Access** > **Full Access**.

Step 12 Click **Edit/Add**. In the displayed dialog box, enter **\Device\NamedPipe** and click **OK**, as shown in **Figure 2-59**.

Figure 2-59 Adding the access permission



----End

2.23.24 RD License Server Fails to Be Added to the AD domain

Scenarios

When a cloned system is used, a Windows Server 2016 server fails to be added to the domain because the SID of the domain is the same as that of the PC.

Procedure

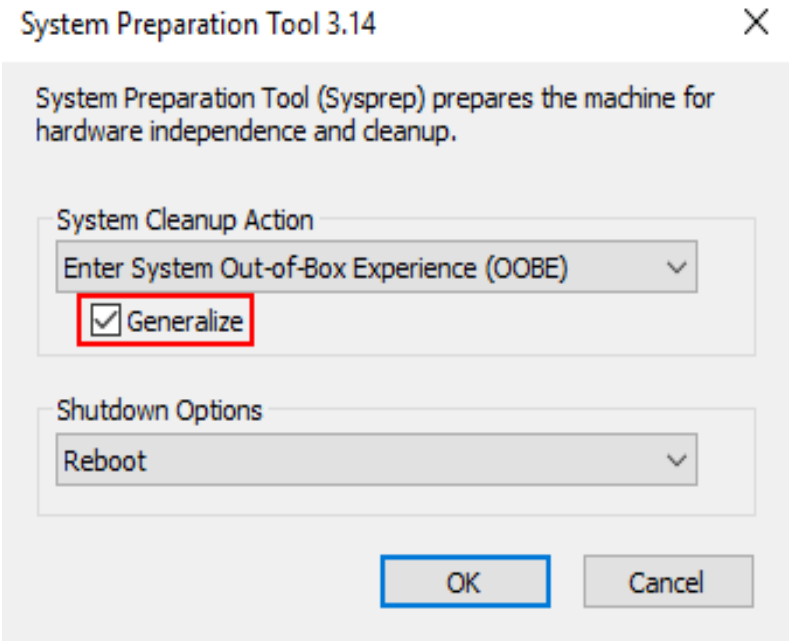
Step 1 Log in to the RD License server.

Step 2 Go to the **windows/System32/Sysprep** directory.

Step 3 Double-click **Sysprep.exe** and the **System Preparation Tool** window is displayed.

Step 4 Select **Generalize** for **System Cleanup Action**, as shown in **Figure 2-60**.

Figure 2-60 System preparation tool



Step 5 Click **OK**.

----End

2.23.25 Error Code 6030/6047 Reported When Accessing a Shared Desktop Application

Scenarios

Error code 6030 or 6047 is reported when accessing a shared desktop application.

The administrator checks whether the server is in the **Ready** status and whether the user has active sessions after logging in to the server using the VNC/RDP.

Procedure

Step 1 Use the problematic account to log in to the server through the VNC or RDP and log out of the session, or restart the server.

Step 2 Log in to the server again.

----End

2.23.26 File Resources on the APS Cannot Be Automatically Refreshed During Workspace Application Streaming Operations

Scenarios

File resources on the APS need to be manually refreshed after being opened or operated by Workspace Application Streaming.

Procedure

Step 1 Log in to the APS where the application is published as the administrator.

Step 2 Click  and enter **Regedit** to open the registry editor.

Step 3 The following uses Notepad as an example:

In the **Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows \CurrentVersion\App Paths** directory, check whether **notepad.exe** exists. (For applications with the above issue, specify the actual name.)

- If no, go to **Step 4**.
- If yes, go to **Step 5**.

Step 4 Right-click **App Paths** and choose **New** > **Item** > **notepad.exe** from the shortcut menu.

Step 5 In the **Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows \CurrentVersion\App Paths\notepad.exe** directory, check whether the **DontUseDesktopChangeRouter** key exists.

- If no, go to **Step 6**.
- If yes, go to **Step 7**.

Step 6 Right-click **notepad.exe** and choose **New** > **DWORD** and name **DontUseDesktopChangeRouter**.

Step 7 Double-click the **DontUseDesktopChangeRouter** key, change the value to **1**, and click **OK**.

----End

2.23.27 How Do I Update or Add an Application?

Scenarios

When using remote applications and remote desktops, you may encounter the following situations:

- New applications need to be added.
- The software version of an application has been upgraded, and the existing application software version needs to be updated.

Prerequisites

You have obtained the .exe or .msi file of the application to be updated from the official channel.

Creating an Image

- For details, see **2.5.2 Image Creation**.

NOTE

Use the image of the server in the server group where the application is to be added or updated is. If the image does not exist, you can use another image. However, you need to reinstall the application that has been published in the application group.

Upgrading the Server Image

Step 1 Log in to the Workspace Application Streaming **console** and go to the **Server Groups** page. Locate the row that contains the server group to be updated and choose **More** > **Modify** on the right. Select the new image generated in the previous step, and click **OK**.

Step 2 Click the server group name. The server list page is displayed.

Step 3 Select the first server and choose **More** > **Rebuild/Upgrade Image** on the right.

Step 4 Select an image, select a server group, and enter **upgrade** in the confirmation text box as prompted.

Step 5 Click **Upgrade Image**.

Step 6 Repeat **Step 4** to **Step 5** to upgrade the images of other servers in the server group.

----End

Publishing an Application

Step 1 Enter the **Application Groups** page. Click the application group whose applications need to be updated. The application group details page is displayed.

NOTE

Go to **2** only when you need to publish applications.

Step 2 Click **Add App**. The **Publish Application** page is displayed. Select the applications, and click **OK**.

----End

2.23.28 How Do I Authorize an IAM User to Use Workspace Application Streaming?

Scenarios

An IAM user account created by the administrator needs to be assigned permissions before using Workspace Application Streaming.

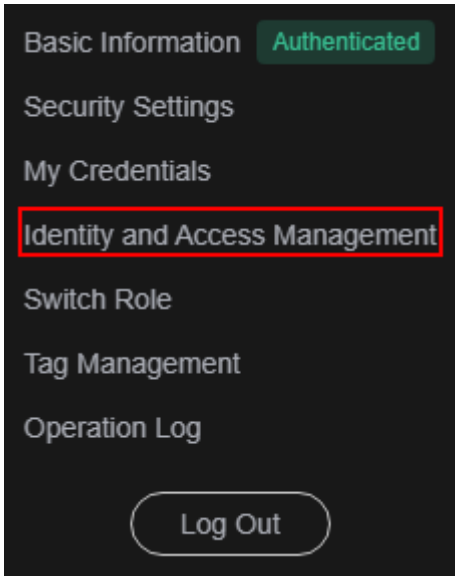
Procedure

Method 1

Step 1 Log in to the Workspace Application Streaming **console** using a Huawei Cloud account.

Step 2 Click **Identity and Access Management** under the account to go to the IAM page.

Figure 2-61 Identity and Access Management

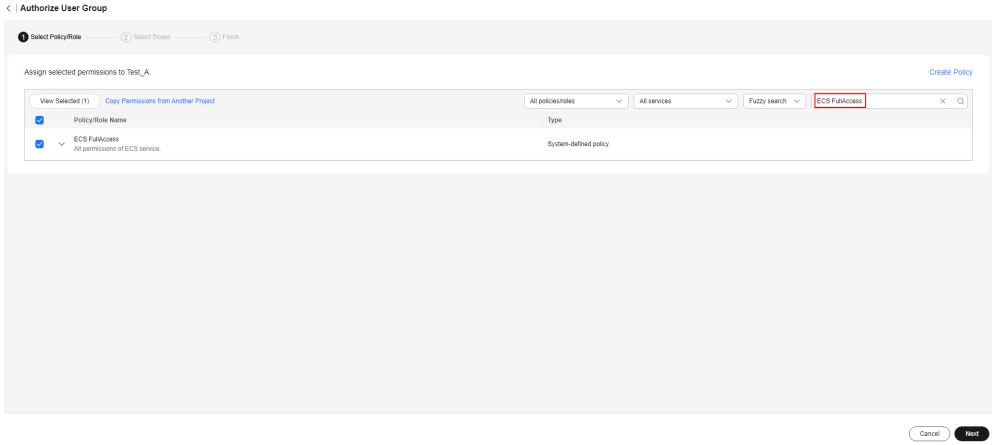


Step 3 In the navigation pane on the left, choose **User Groups**.

Step 4 Click **Authorize** in the **Operation** column of the desired user group. On the displayed page, assign the following permissions, as shown in **Figure 2-62**.

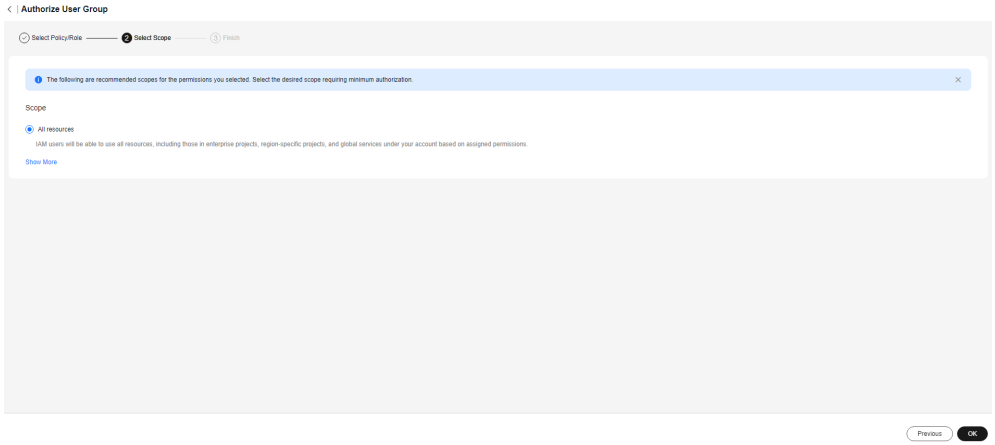
- IAM ReadOnlyAccess
- Tenant Administrator
- IMS Administrator
- ECS FullAccess

Figure 2-62 Assigning permissions



Step 5 Click **Next** and select the authorization scope, as shown in **Figure 2-63**.

Figure 2-63 Selecting the authorization scope

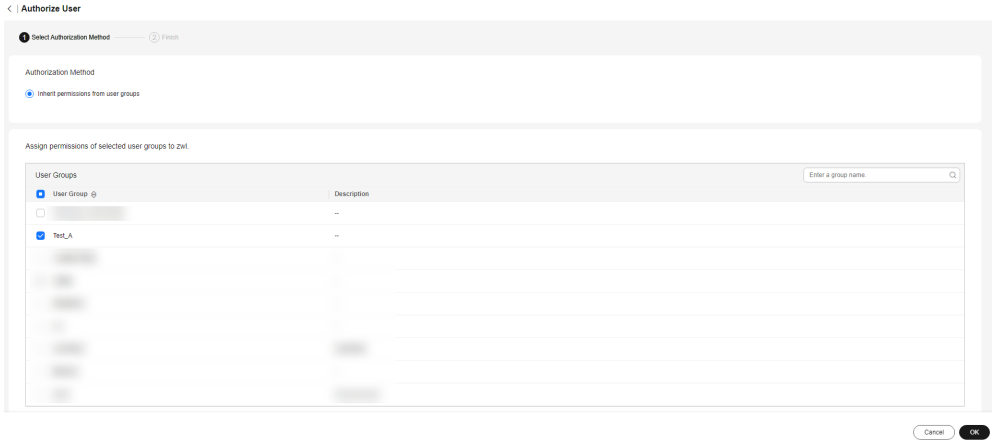


Step 6 Click **OK**.

Step 7 In the navigation pane on the left, choose **Users**.

Step 8 Click **Authorize** in the **Operation** column of the desired user. On the displayed page, select the user group whose permissions are to be assigned to the user, as shown in **Figure 2-64**.

Figure 2-64 Authorization methods



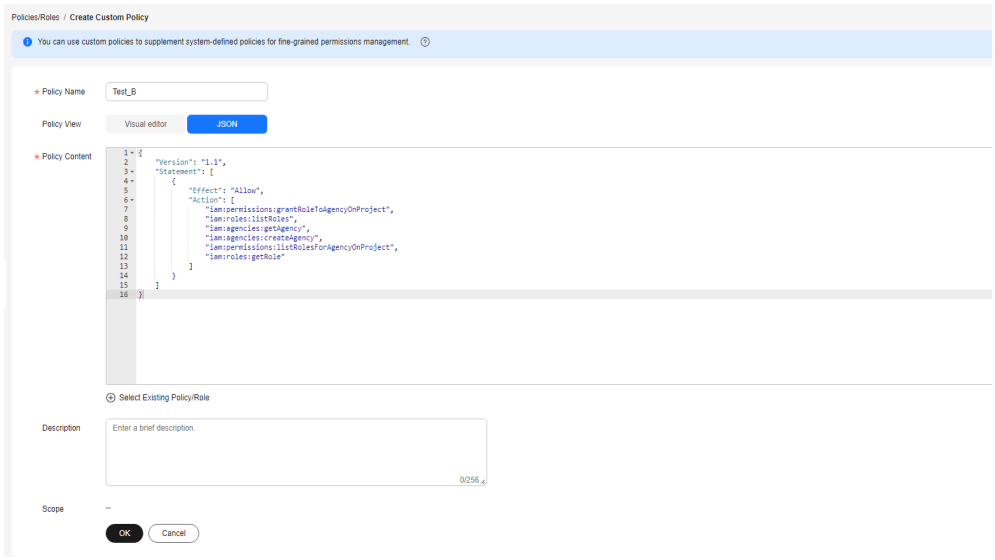
Method 2

Step 9 In the navigation pane on the left, choose **Permissions** > **Policies/Roles**.

Step 10 Click **Create Custom Policy** in the upper right corner.

Step 11 Enter a policy name, set **Policy View** to **JSON**, and configure the policy content, as shown in **Figure 2-65**.

Figure 2-65 Creating a custom policy

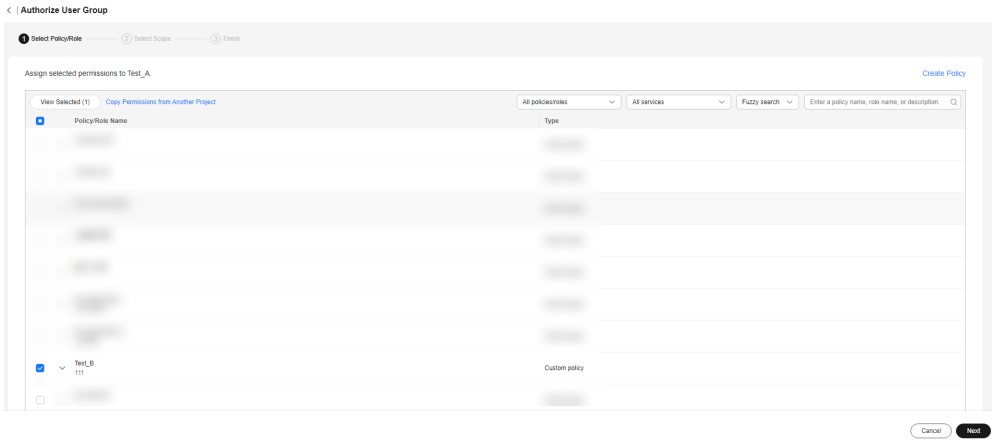


Step 12 Click **OK**.

Step 13 In the navigation pane on the left, choose **User Groups**.

Step 14 Click **Authorize** in the **Operation** column of the desired user group. On the displayed page, assign the user group using the created custom policy, as shown in **Figure 2-66**.

Figure 2-66 Authorizing a user group using the created custom policy

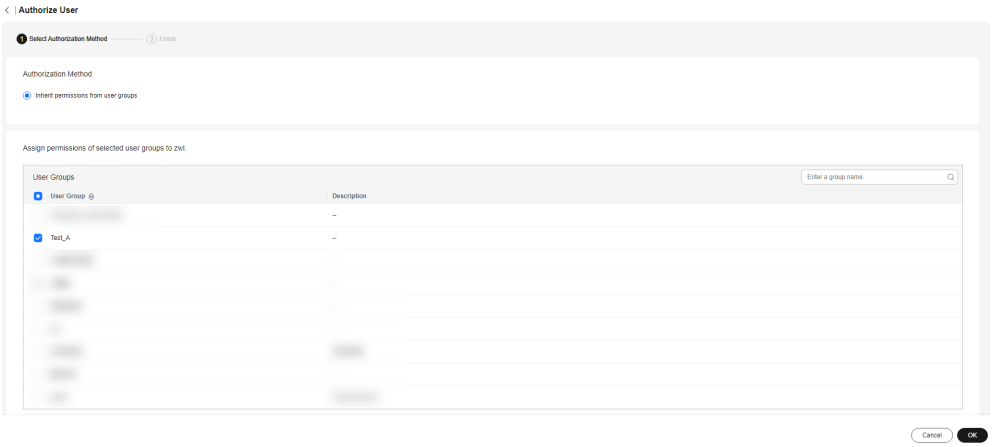


Step 15 Click **Next**, select the authorization scope, and then click **OK**.

Step 16 In the navigation pane on the left, choose **Users**.

Step 17 Click **Authorize** in the **Operation** column of the desired user. On the displayed page, select the user group whose permissions are to be assigned to the user, as shown in **Figure 2-67**.

Figure 2-67 Authorization methods



----End

2.23.29 How Do I Calculate the Number of Concurrent Sessions of a Cloud Application?

Scenarios

In multi-session mode, before creating a server group, the administrator calculates the maximum number of sessions of the corresponding specifications.

Prerequisites

- You have created an image by referring to **2.5.2 Image Creation**.
- You have obtained the minimum system requirements for the software.

Procedure

Step 1 Log in to the Workspace Application Streaming **console** as an administrator.

Step 2 Create a server group by referring to **2.6.1.1 Creating a Server Group**.

NOTE

When creating a server group, set the total number of sessions to 2 to 5. Select the package type and specifications ID based on the actual specifications to be calculated.

Step 3 Create an application group by referring to **2.7.1.1 Creating an Application Group** and associate it with the server group created in **Step 2**.

Step 4 Click the name of the application group created in **Step 3**. On the displayed application group details page, add the desired application (such as Google Chrome) and the task manager application by referring to **2.7.2.1.1 Adding Applications**.

Step 5 Click the **User Authorization** tab and select the users to be authorized (recommended: two to five users) by referring to **2.7.2.2.1 Authorizing Users or User Groups**.

Step 6 On the **Server Groups** page, click the name of a server group. The **Basic Information** page of the server group is displayed.

Step 7 In the server list in the lower part of the displayed page, click  in the **Monitoring** column. The server monitoring information is displayed. Record the CPU, memory, and GPU usage when the server is unloaded.

Step 8 Log in to the Huawei Cloud client using the user account (user A) added in **Step 5** and click the desired application (such as Google Chrome) and the task manager application. Perform operations on this application and observe and record the resource usage (such as CPU, memory, and GPU) on the user panel of the task manager.

Step 9 Repeat **Step 8** to log in using two to five accounts. Perform operations on the desired application without opening the task manager application. User A observes and records the resource usage of each session.

NOTE

- The bottleneck metric is the metric with the highest usage of each session recorded in **Step 9**. For example, if the CPU usage, memory usage, and GPU usage of each session are 10%, 5%, and 4%, respectively, the bottleneck metric is CPU usage.
- Recommended maximum number of sessions = (85% – Bottleneck metric usage when the server is unloaded)/Bottleneck metric usage of each session
- After the calculation is complete, if the resources are no longer used, delete or unsubscribe from the servers, server groups, and application groups purchased in **Step 2** in a timely manner. Otherwise, unexpected fees will be incurred.

----End

2.23.30 What If I Can't Open a Cloud Application?

Scenarios

End users cannot open a cloud application on the client (a message is displayed indicating that a file is missing or the path is incorrect). However, the cloud application can be opened using VNC or on the APS. The administrator needs to modify the application path in **Command Parameter** of the application on the console.

NOTE

- The administrator modifies **Command Parameter** of the application that cannot be opened, and integrates the files or parameters that are needed to start the application on the APS into **Command Parameter** of the application on the console.

  Example: SPECviewperf 13.0.

  Right-click the software and choose **Properties** from the shortcut menu to view **Target location** and **Start in** of the software.

  Target location: **C:\SPEC\SPECgpc\SPECviewperf13\gui\nw.exe vp13bench**

  Start in: **C:\SPEC\SPECgpc\SPECviewperf13**

  The command parameter to be added for the cloud application is the parameter following the *Start in* + *Target location*. An example is **C:\SPEC\SPECgpc\SPECviewperf13\vp13bench**.
- The configuration parameters vary with software products.

Procedure

Step 1 Log in to the Workspace Application Streaming **console** as an administrator.

Step 2 In the navigation pane, choose **Application Groups**. The **Application Groups** is displayed.

Step 3 Click an application group name. The application group details page is displayed.

Step 4 Click **Edit** in the **Operation** column of the application that cannot be opened. The **Modify Application** page is displayed.

Step 5 Integrate the files or parameters that are needed to start the application into **Command Parameter** of the application on the console.

Step 6 Click **OK**.

----End

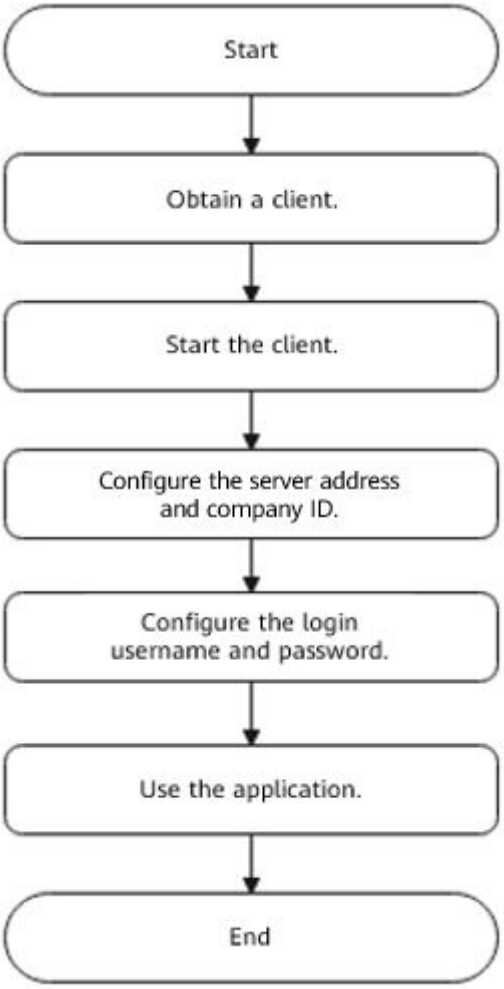
3 Terminal User Operation Guide

3.1 Process
3.2 Using an Application on a Soft Client
3.3 Using an Application on a Thin Client
3.4 FAQs

3.1 Process

Figure 3-1 shows you how to use Workspace Application Streaming.

Figure 3-1 How to use Workspace Application Streaming



NOTE

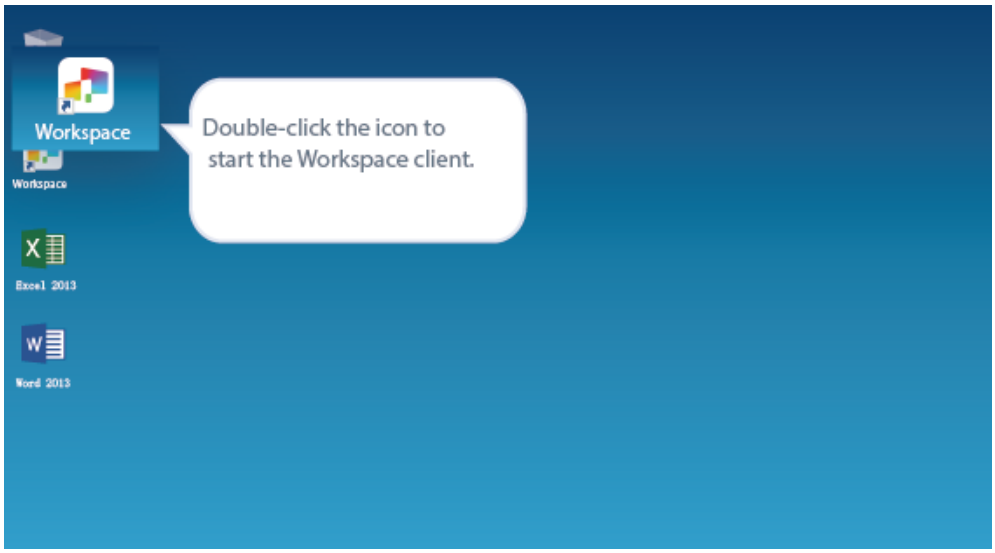
The required Workspace client is built in the TC. After the TC is started, start the client.

3.2 Using an Application on a Soft Client

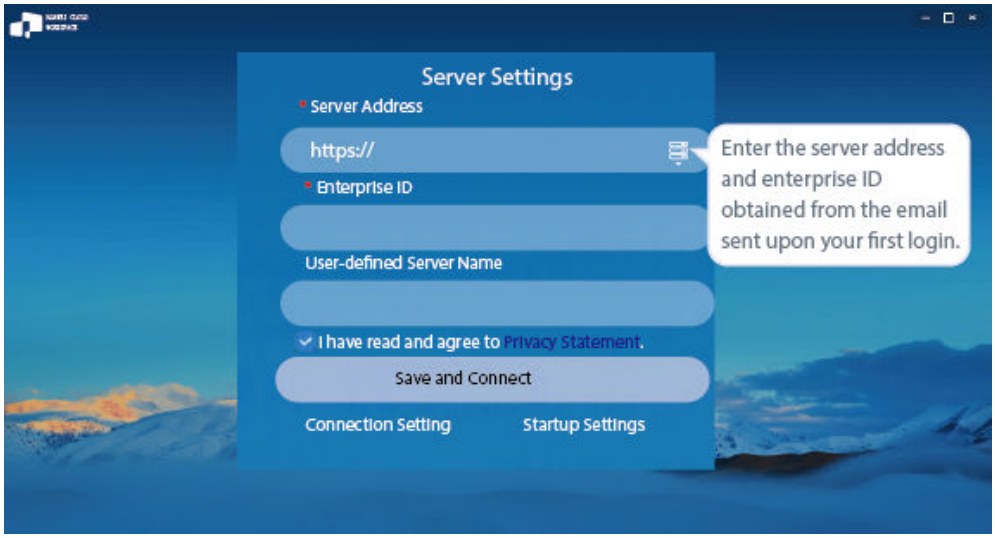
Step 1: Downloading and Installing the Workspace Client

Download the Workspace client for Windows and install it.

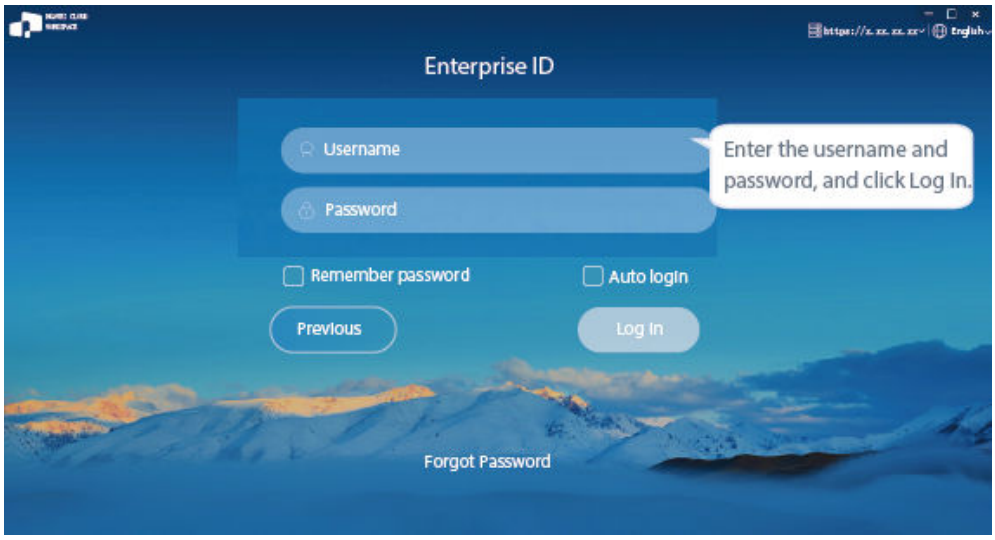
Step 2: Starting the Client



Step 3: Configuring a Server Access Address and Company ID

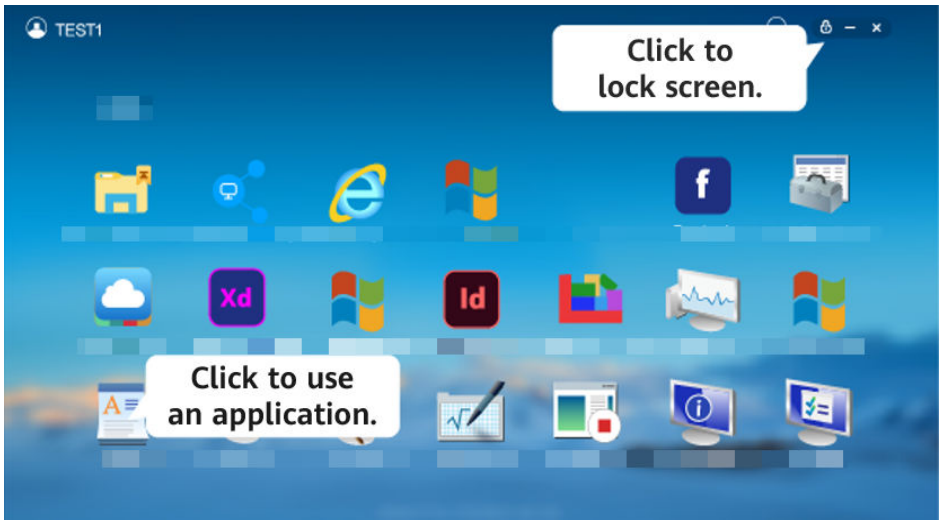


Step 4: Entering a Username and Password for Login

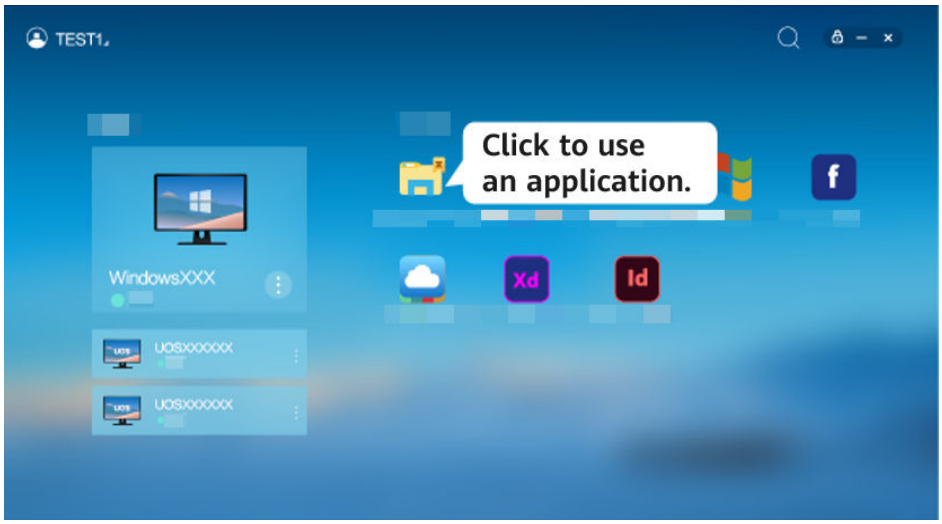


Step 5: Using Applications or Cloud Storage Remotely

- **Use applications remotely on the homepage.**
  - The current user has only Workspace Application Streaming.



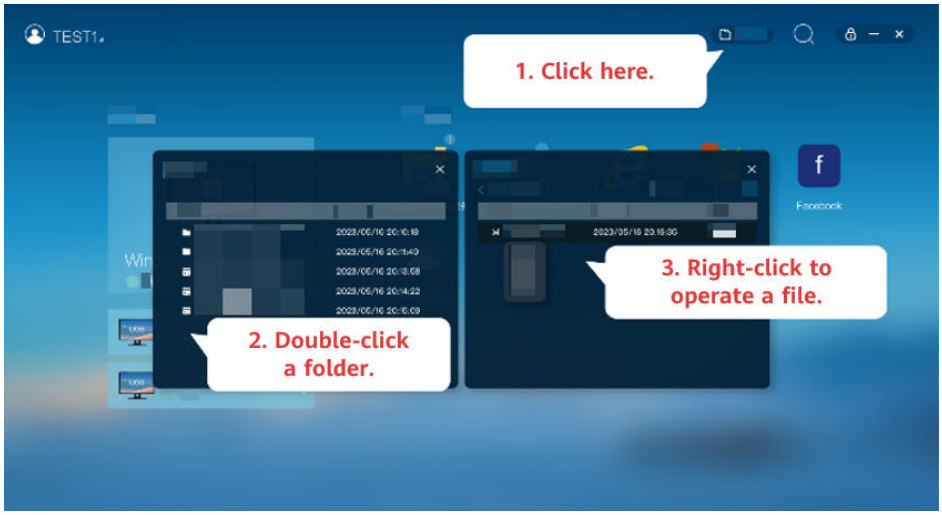
  - The current user has both Workspace Application Streaming and Workspace.



- **Use cloud storage remotely on the homepage.**

  Open cloud storage.

  Double-click to enter the folder, and upload files or create folders.

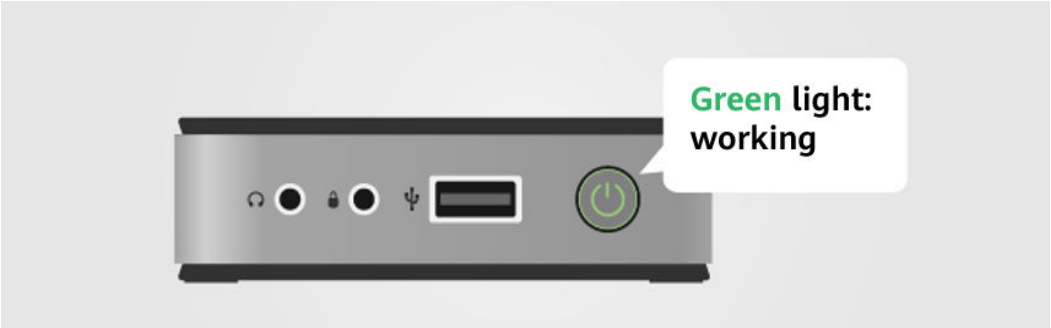


NOTE

After the user has logged in to the application, open the **C:\Users*username*** directory on the APS.

3.3 Using an Application on a Thin Client

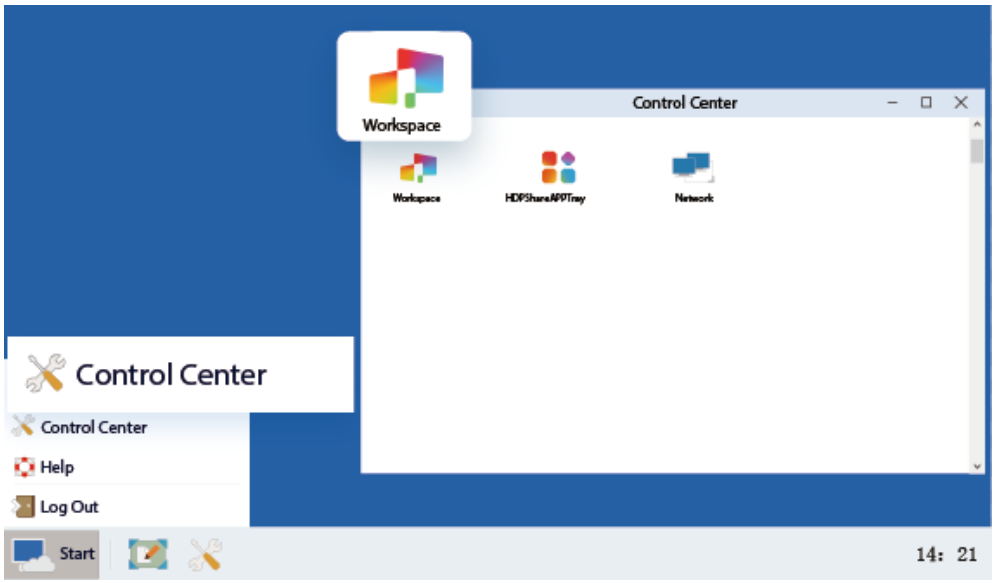
Step 1: Connecting Cables and Powering on the Thin Client



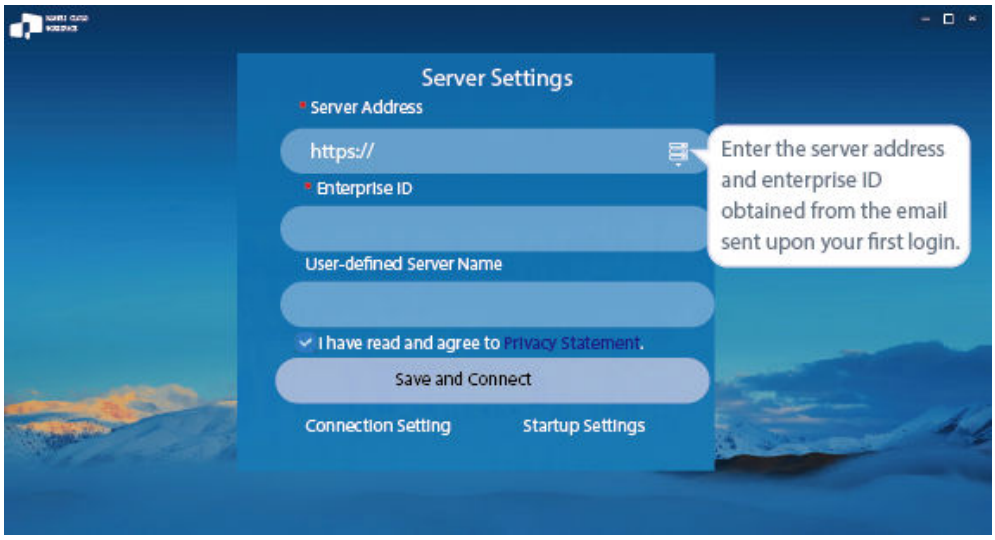
Step 2: Starting the Client

NOTE

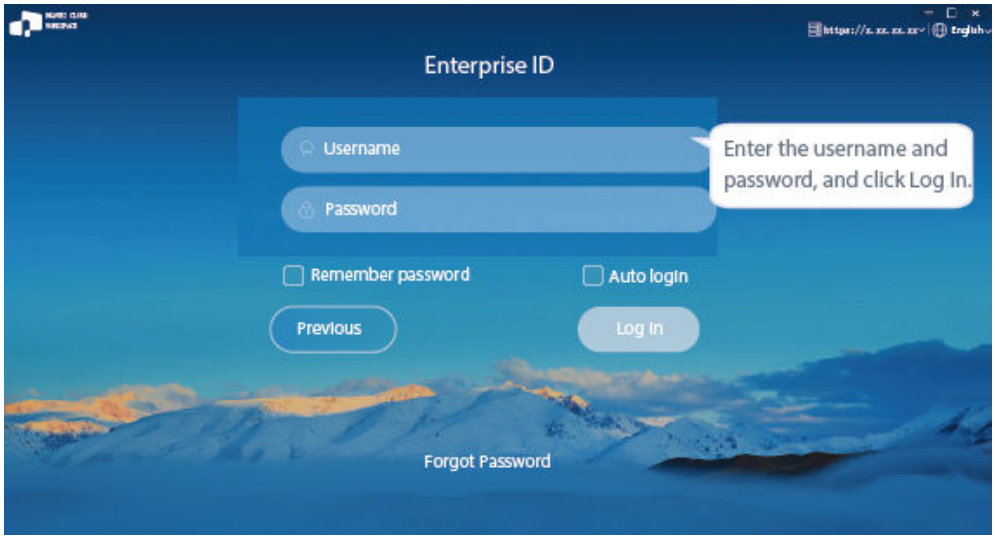
If you log in to the TC for the first time, start the Workspace client in the TC control center.



Step 3: Configuring a Server Access Address and Company ID

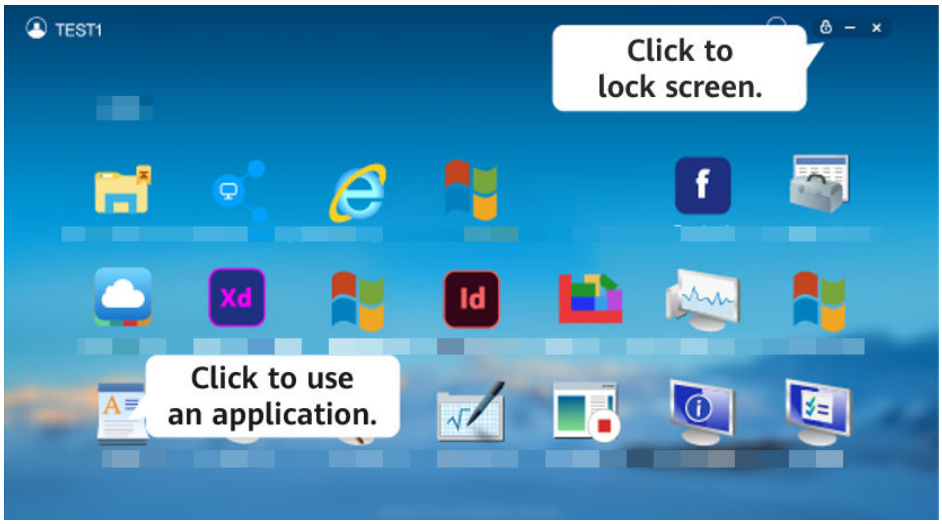


Step 4: Entering a Username and Password for Login

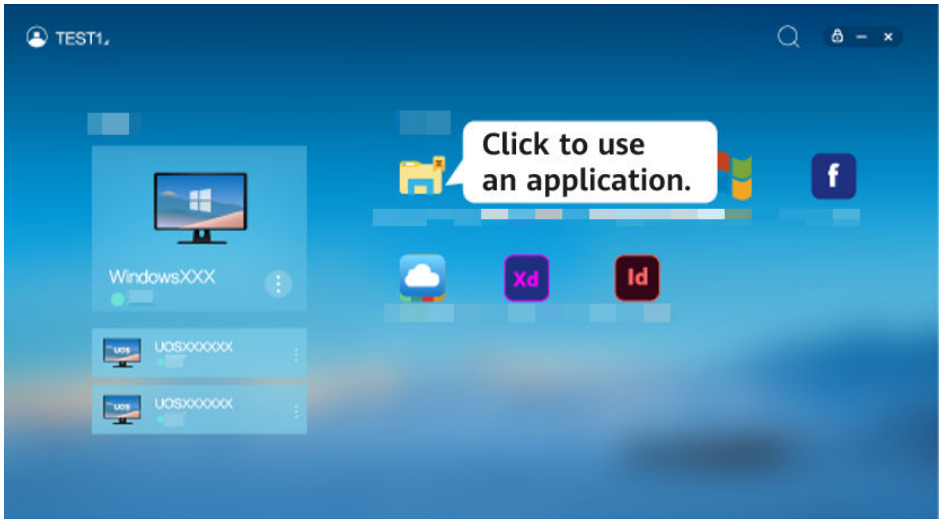


Step 5: Using Applications or Cloud Storage Remotely

- **Use applications remotely on the homepage.**
  - The current user has only Workspace Application Streaming.



- The current user has both Workspace Application Streaming and Workspace.



- **Use cloud storage remotely on the homepage.**

  Open cloud storage.

  Double-click to enter the folder, and upload files or create folders.

NOTE

After the user has logged in to the application, open the **C:\Users*username*** directory on the APS.

3.4 FAQs

3.4.1 How Do I Do If the Cloud Application Cannot Be Used?

Contact the administrator.

3.4.2 How Do I Do If I Cannot View Cloud Applications on Desktops?

Contact the administrator.

3.4.3 How Do I Do If I Forget the Password?

If you lose or forget the login password, contact the administrator. The administrator resets the password for the user on the AD server by referring to **2.23.17 How Do I Reset a User Password?** and notifies the user of the new password.

3.4.4 How Do I Do If the Account is Locked?

If your account is locked because you enter incorrect passwords for five consecutive times, you can contact the administrator to rectify the fault and enter the correct password to log in again.

3.4.5 How Do I Do If I Fail to Log In to the Client?

Users can rectify the fault based on the displayed information. The possible causes and corresponding handling procedures are listed for reference, as shown in **Table 3-1**. If the login still fails, contact the administrator.

Table 3-1 Example

Login Failure Prompt	Possible Cause	Handling Method
6005: Your VM is not ready. Please try again later or restart the TC.	An internal copy error occurs on the client.	• Method 1: Try to log in again. • Method 2: Restart the TC and log in again.

Login Failure Prompt	Possible Cause	Handling Method
6008: Your VM is not ready. Try again later.	The client program is running abnormally because of incorrect memory allocation.	• Method 1: Try to log in again. • Method 2: Restart the TC and log in again.
6008: Your client version is incompatible. Update the client version.	The client version is incompatible .	Update the client version.
6010: Your VM is not ready. Try again later or contact the administrator.	The configuration on the client is not synchronized with that on the server.	• Method 1: Try to log in again. • Method 2: Restart the client and log in again. • Method 3: Restart the APS and log in again.
6050: Network errors exist. Try again later.	The network connection between the client and the server is abnormal.	• Method 1: Check whether the network connection between the client and the server is normal. • Method 2: Restart the APS and log in again.

3.4.6 How Do I Enable a Local Storage Device to Copy Files to an APS?

Administrators can configure the following policies to copy application files from a local storage device to an APS. You only need to configure one of the following policies.

Clipboard Redirection

Step 1 Log in to the Workspace Application Streaming **console** as an administrator.

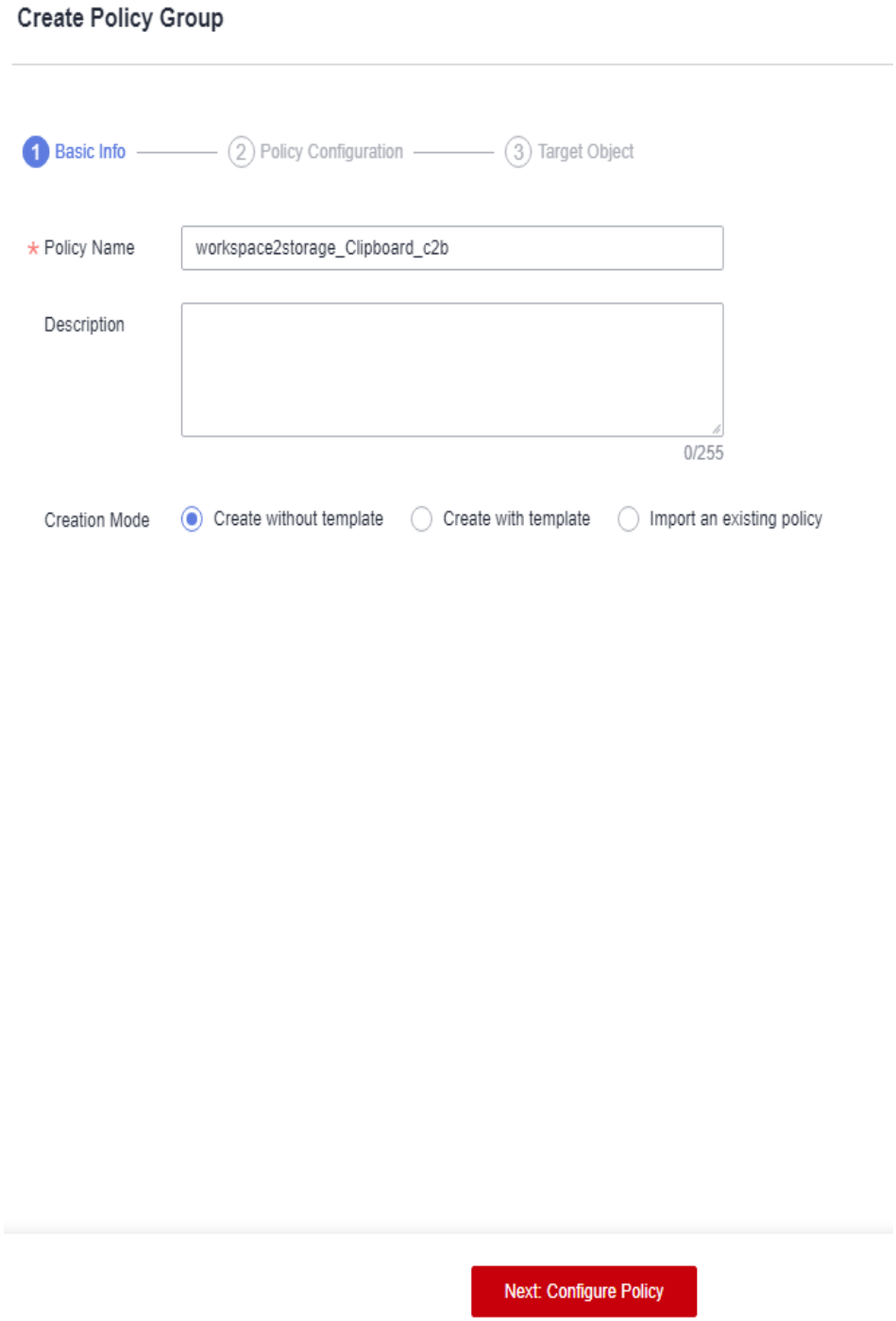
Step 2 In the navigation pane, click **Policy Groups**. The **Policy Groups** page is displayed.

Step 3 Click **Create Policy Group** in the upper right corner. The **Create Policy Group** page is displayed.

Step 4 Configure the **Policy Name**, **Description**, and **Creation Mode**, and click **Next: Configure Policy**.

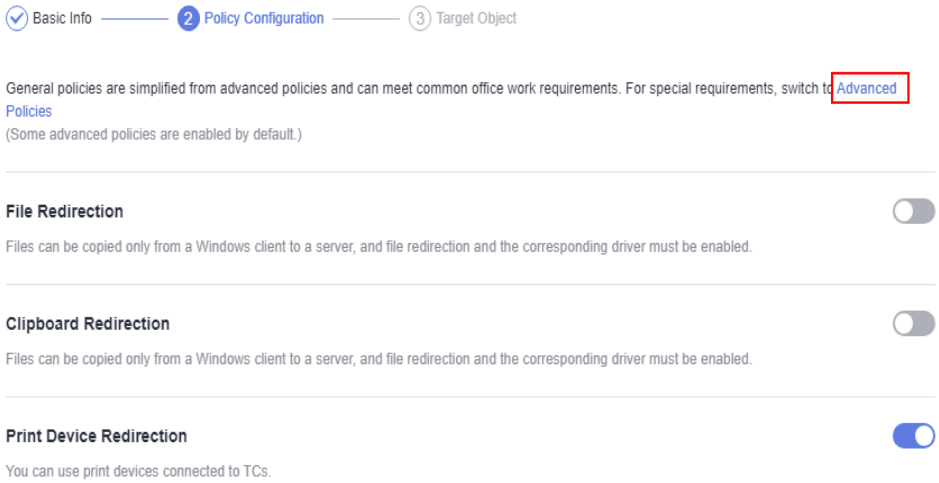
- The **Policy Name** must contain digits, letters, and underscores (_), and cannot contain more than 55 characters, for example, **workspace2storage_Clipboard_c2b**.
- The description contains up to 255 characters. For example, clipboard redirection is used when an external device copies a file to an APS.
- Retain the default creation mode.

Figure 3-2 Creating a policy group



Step 5 Click **Advanced Policies**.

Figure 3-3 Switching to advanced policies



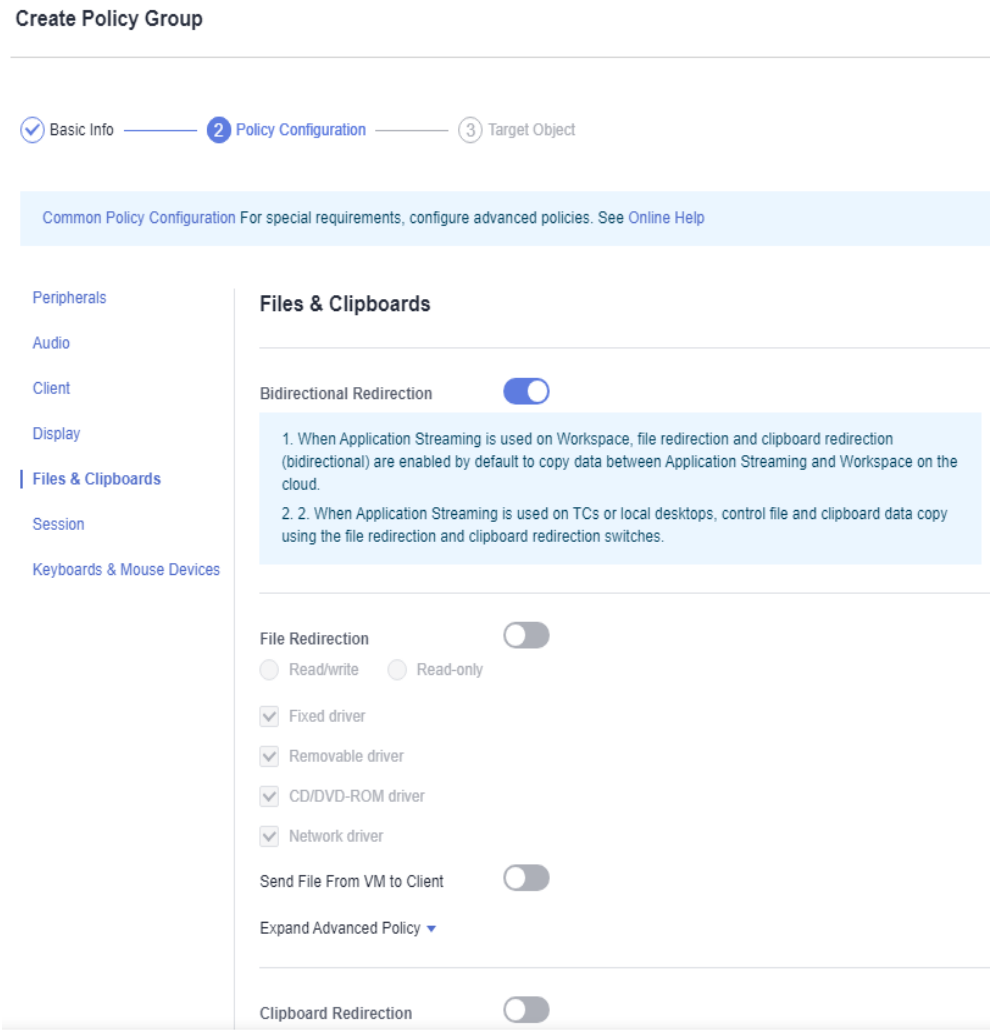
Step 6 On the displayed page, click **Files & Clipboards**.

Step 7 Enable the **Clipboard Redirection** policy, and select **Client to server**, as shown in **Figure 3-4**.

NOTE

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

Figure 3-4 Client to server

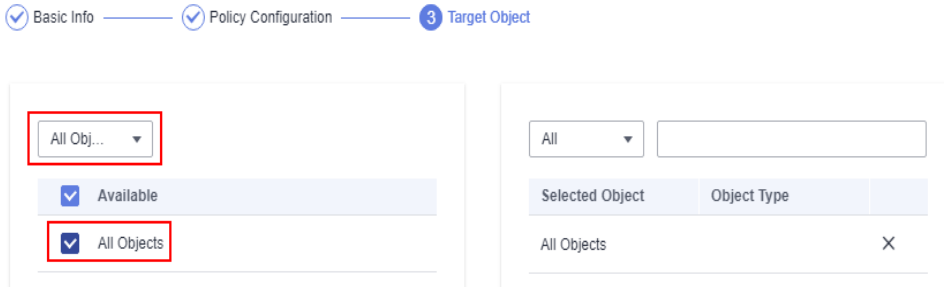


Step 8 Click **Next: Select Object**.

Step 9 Select an object as required.

For example, if you select **All Objects** and select all objects, the policy applies to all users and application groups in the current project.

Figure 3-5 Selecting an object



Step 10 Click **Next: Finish**.

----End

File Redirection

Step 1 Log in to the Workspace Application Streaming **console** as an administrator.

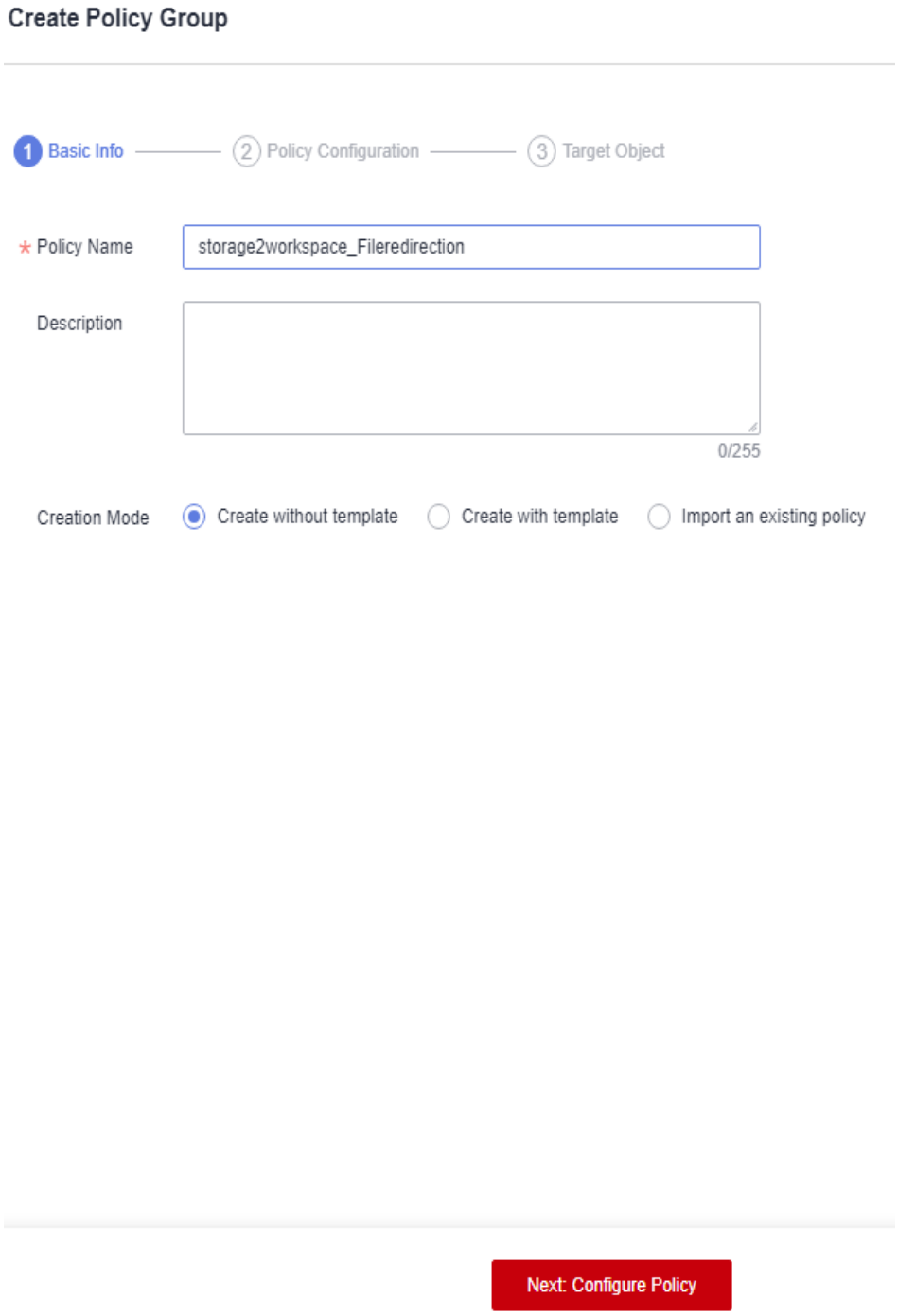
Step 2 In the navigation pane, click **Policy Groups**. The **Policy Groups** page is displayed.

Step 3 Click **Create Policy Group** in the upper right corner. The **Create Policy Group** page is displayed.

Step 4 Configure the **Policy Name**, **Description**, and **Creation Mode**, and click **Next: Configure Policy**.

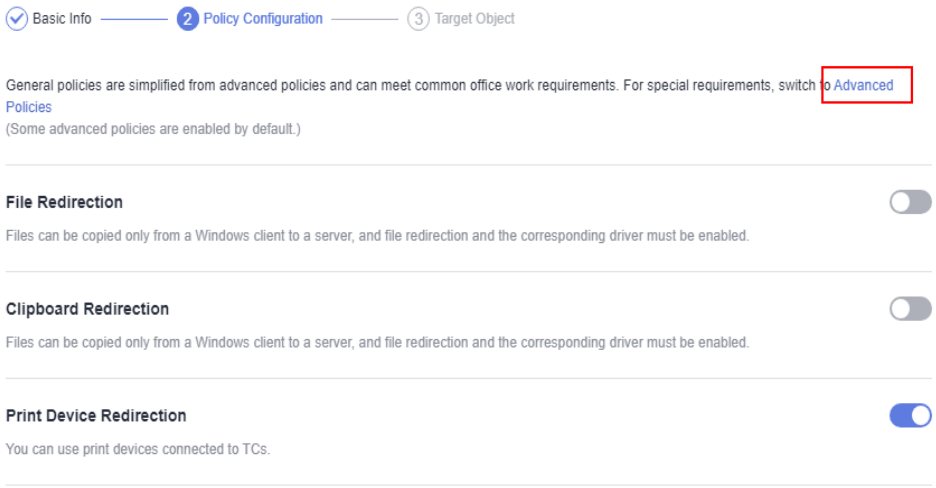
- The **Policy Name** must contain digits, letters, and underscores (_), and cannot contain more than 55 characters, for example, **storage2workspace_Fileredirection**.
- The description contains up to 255 characters. For example, file redirection is used when an external device copies a file to a Workspace Application Streaming server.
- Retain the default creation mode.

Figure 3-6 Creating a policy group



Step 5 Click **Advanced Policies**.

Figure 3-7 Switching to advanced policies



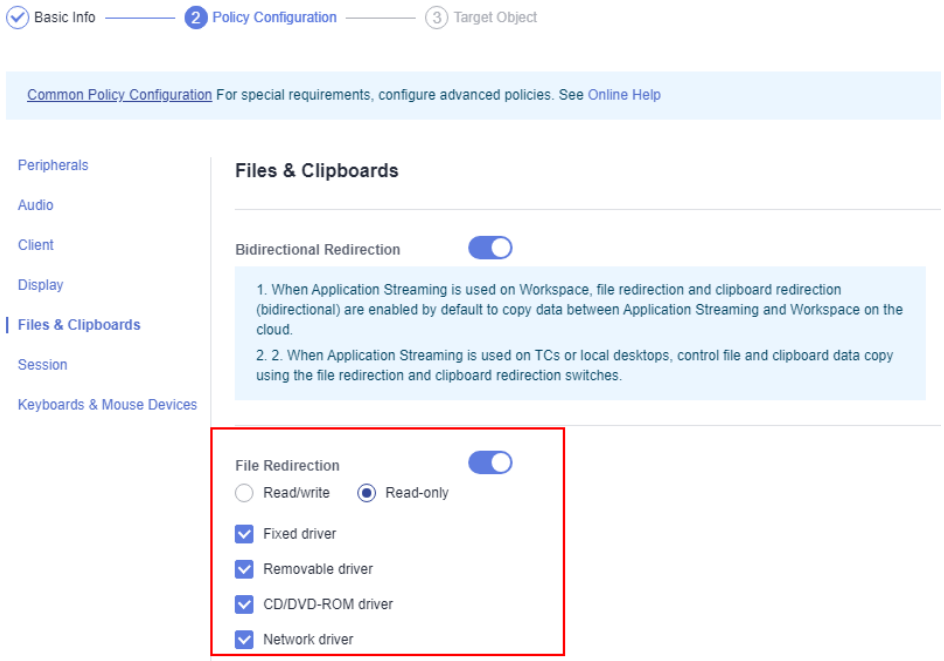
Step 6 On the displayed page, click **Files & Clipboards**.

Step 7 Enable the **File Redirection** policy and select **Read-only**, as shown in **Figure 3-8**.

NOTE

You do not need to set other advanced policy parameters under **Files & Clipboards**. If you have strict requirements on the traffic and file size, set the parameters by referring to **2.9.3 Configuring an Advanced Policy**.

Figure 3-8 Read-only of file redirection

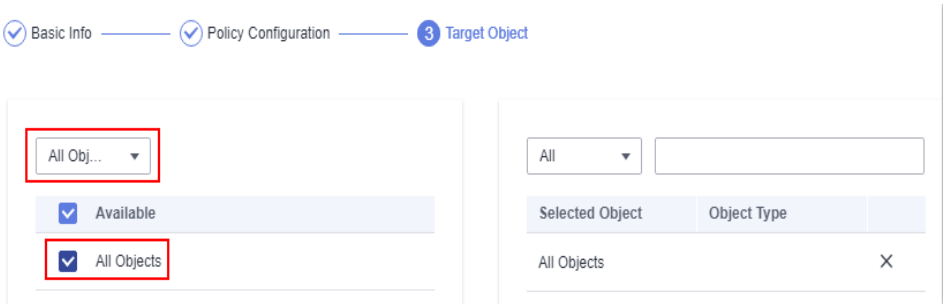


Step 8 Click **Next: Select Object**.

Step 9 Select an object as required.

For example, if you select **All Objects** and select all objects, the policy applies to all users and application groups in the current project.

Figure 3-9 Selecting an object



Step 10 Click **Next: Finish**.

----End

File Sending

Step 1 Log in to the Workspace Application Streaming **console** as an administrator.

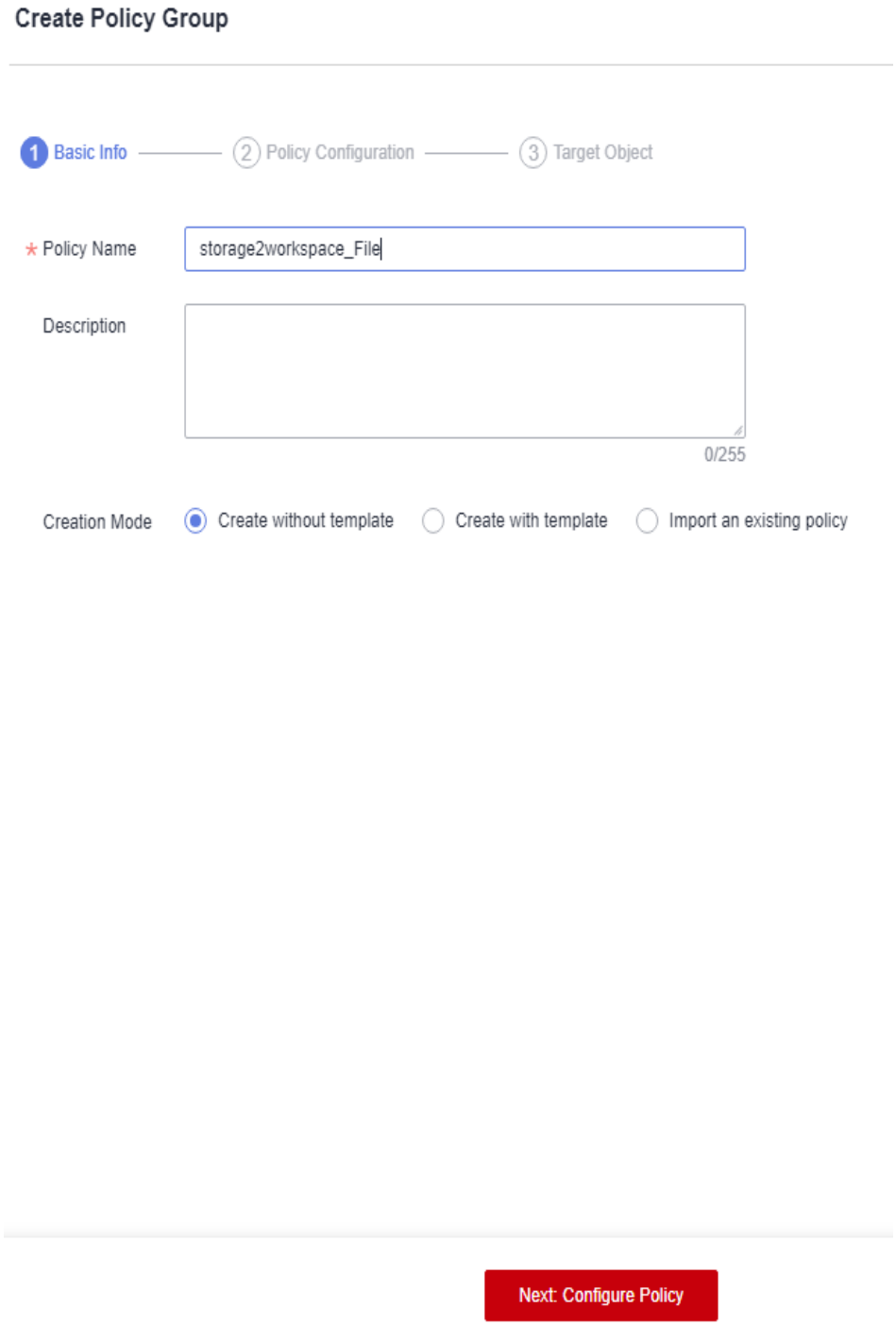
Step 2 In the navigation pane, click **Policy Groups**. The **Policy Groups** page is displayed.

Step 3 Click **Create Policy Group** in the upper right corner. The **Create Policy Group** page is displayed.

Step 4 Configure the **Policy Name**, **Description**, and **Creation Mode**, and click **Next: Configure Policy**.

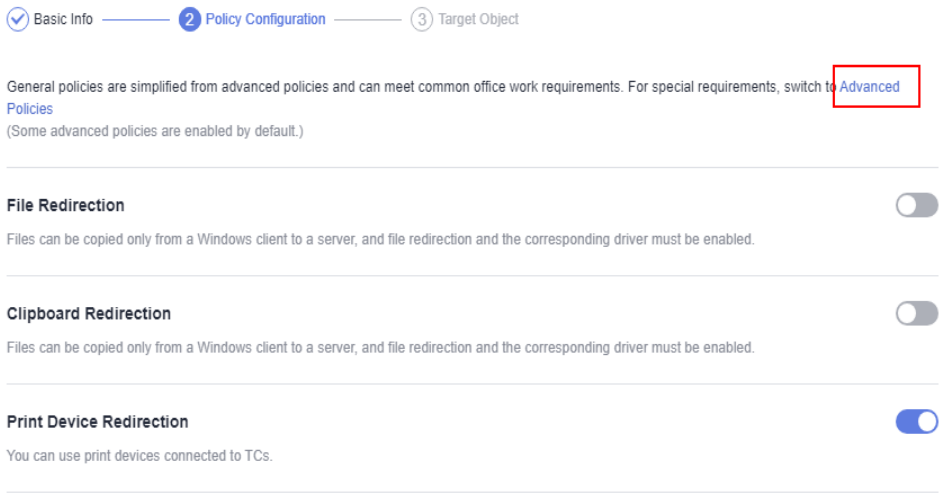
- The **Policy Name** must contain digits, letters, and underscores (_), and cannot contain more than 55 characters, for example, **storage2workspace_File**.
- The description contains up to 255 characters. For example, file sending is used when an external device copies a file to an APS.
- Retain the default creation mode.

Figure 3-10 Creating a policy group



Step 5 Click **Advanced Policies**.

Figure 3-11 Switching to advanced policies



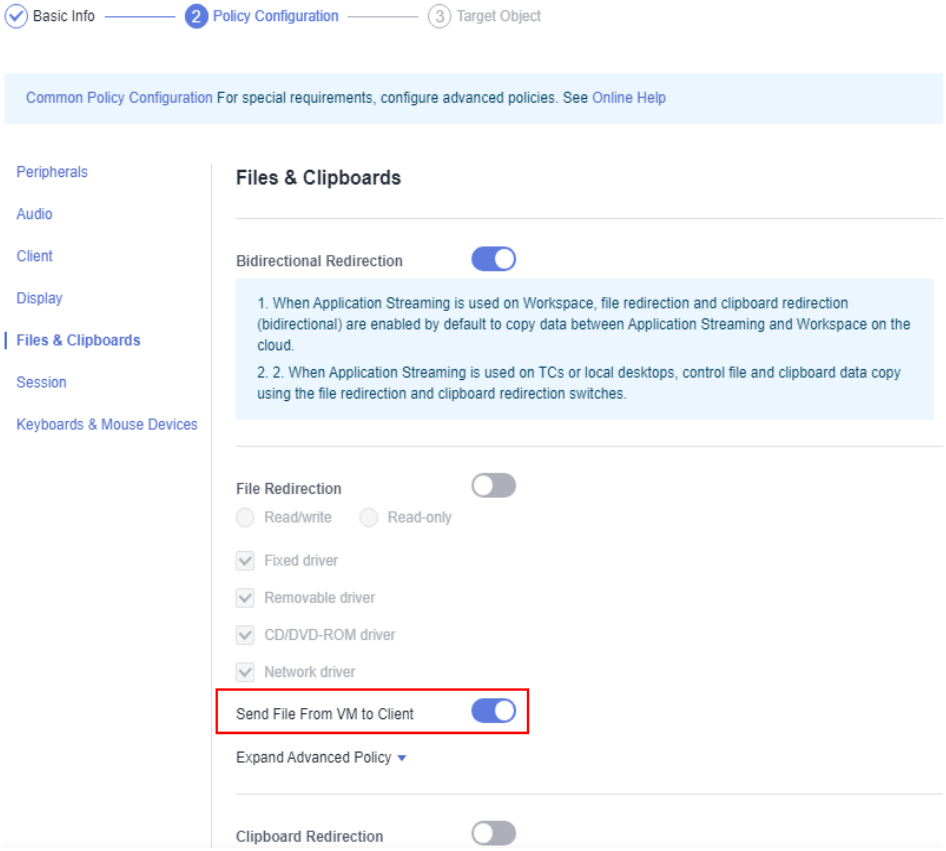
Step 6 On the displayed page, click **Files & Clipboards**.

Step 7 Enable the **Send File From VM to Client** policy, as shown in **Figure 3-12**.

NOTE

If **Send File From VM to Client** is enabled, you can send files from an external storage device to the APS only when both the client (TC/SC) and the server run Windows.

Figure 3-12 Configuring a file sending policy

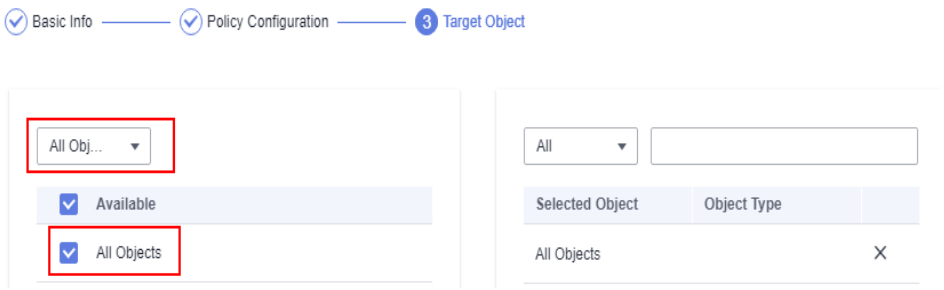


Step 8 Click **Next: Select Object**.

Step 9 Select an object as required.

For example, if you select **All Objects** and select all objects, the policy applies to all users and application groups in the current project.

Figure 3-13 Selecting an object



Step 10 Click **Next: Finish**.

----End

3.4.7 How Do I Recover Important Files and Documents from the Sandbox to the Local Computer?

Prerequisites

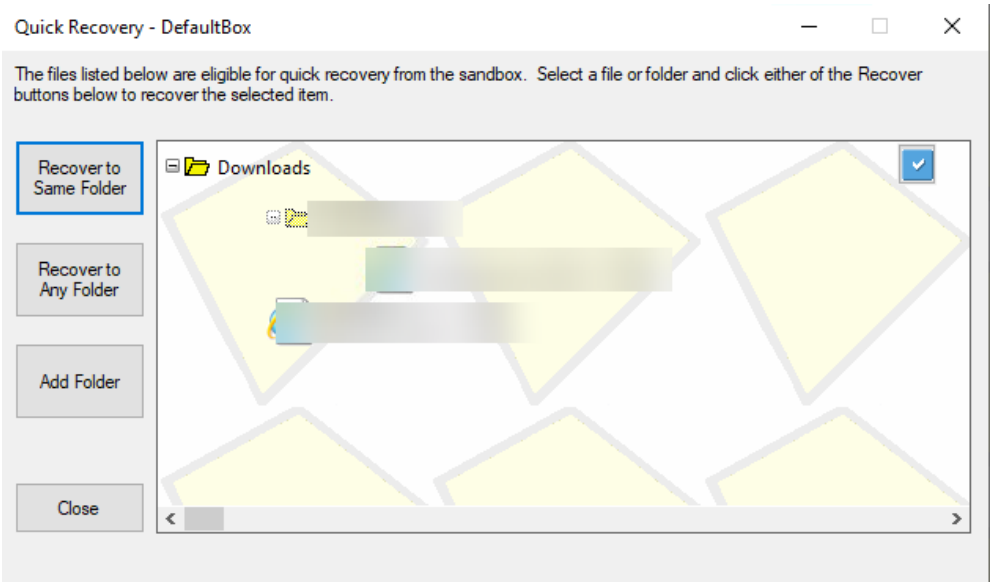
The administrator has published the sandbox console application to the application group.

Step 1 Log in to the client and click **Sandboxie Control** on the application list page. The **Sandboxie Control** console is displayed.

Step 2 On the console, right-click the sandbox to be recovered and choose **Quick Recovery** from the shortcut menu.

The **Quick Recovery** page is displayed, as shown in **Figure 3-14**.

Figure 3-14 Quick recovery



Step 3 You can choose **Recover to Same Folder** or **Recover to Any Folder**.

Step 4 View the recovered folder on the APS.

----End

3.4.8 How Do I Delete a Sandbox?

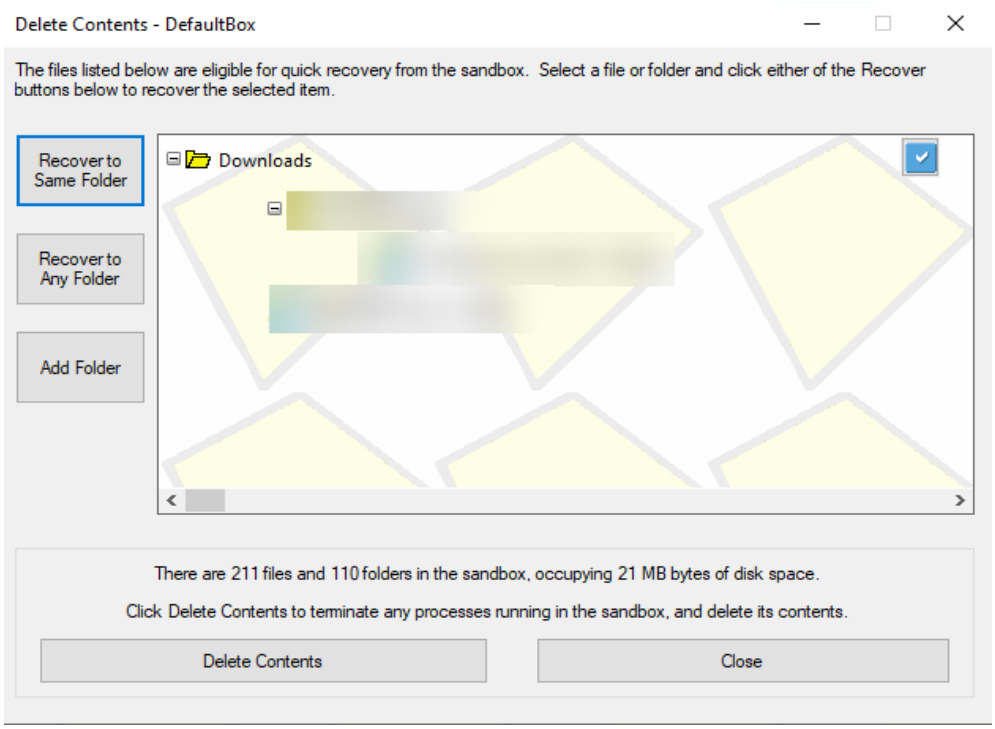
Prerequisites

- The administrator has published the sandbox console application to the application group.
- When you stop using applications in Sandboxie and have restored downloaded files, documents, and other required work items, you can delete the content from the sandbox.

Step 1 Log in to the client and click **Sandboxie Control** on the application list page. The **Sandboxie Control** console is displayed.

Step 2 On the console, select the sandbox from which you want to delete files, right-click the sandbox name, and choose **Delete Contents** from the shortcut menu. The **Delete Contents** page is displayed, as shown in **Figure 3-15**.

Figure 3-15 Deleting a sandbox



Step 3 Click **Delete Contents**.

----End

3.4.9 How Do I Remove the Yellow Border of an Application After the Sandbox Application Is Started?

Prerequisites

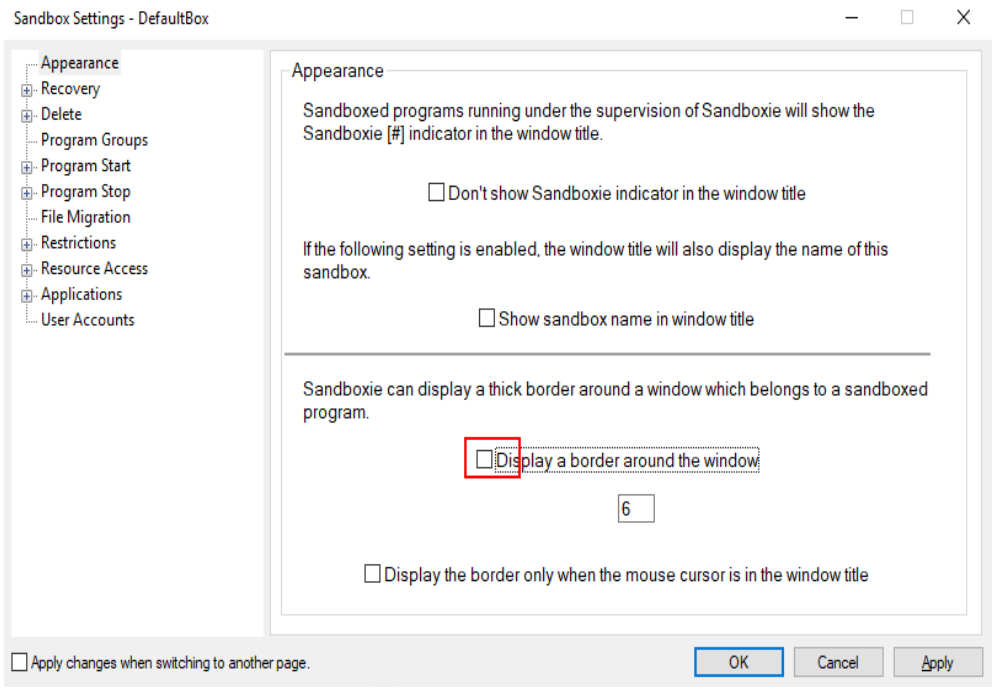
The administrator has published the sandbox console application to the application group.

Step 1 Log in to the client and click **Sandboxie Control** on the application list page. The **Sandboxie Control** console is displayed.

Step 2 On the console, right-click the desired sandbox and choose **Sandbox Settings** from the shortcut menu, and click **Appearance**.

Step 3 Deselect **Display a border around the window** and click **OK**, as shown in **Figure 3-16**.

Figure 3-16 Sandbox settings



----End

