Cloud Bastion Host (CBH)

User Guide

Issue 08

Date 2025-09-29

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property 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 Cloud 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 Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 Buying a CBH Instance

Overview

A Cloud Bastion Host (CBH) instance corresponds to an independently running CBH O&M management system. To perform real-time, remote, and efficient O&M on your resources, buy a CBH instance first, obtain an account on the CBH instance you got, log in to the CBH system mapped to the CBH instance, and configure the O&M system.

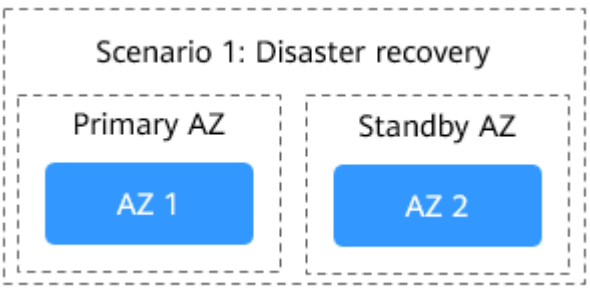
Scenarios

When purchasing a bastion host, which AZ you can select depends on the instance type (**Single-node** or **Primary/Standby**) you select.

- Single-node: As only one bastion host will be created after you buy a CBH instance, you can select any AZ.
- Primary/Standby: As two bastion hosts will be created after you buy a CBH instance, you need to select the primary AZ and standby AZ based on the disaster recovery (DR) or network latency requirements.
  - Scenario 1: If DR is required, deploy the primary and standby instances in different AZs.

    Example: Select **AZ1** for **Primary AZ** and **AZ2** for **Standby AZ**.

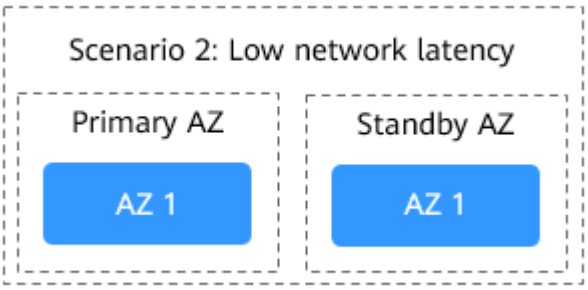
    Figure 1-1 AZ selection for DR capability requirements

  - Scenario 2: For lower network latency, deploy the primary and standby instances in the same AZ. Unlike DR scenarios, this configuration reduces latency significantly.

Example: Select **AZ1** for both **Primary AZ** and **Standby AZ**.

Figure 1-2 AZ selection for low network latency



Prerequisites

- You have obtained the information about the resources to be managed in the CBH system, and the resources are in the region where CBH is available.
- You have purchased at least one elastic IP address (EIP).

CAUTION

An EIP can be bound to only one cloud resource. A CBH instance cannot share an EIP with other cloud resources.

Procedure

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

Step 2 Click in the upper left corner on the displayed page and select a region.

Step 3 Click **Buy CBH Instance** to go to the **Buy CBH Instance** page.

Step 4 Select **CBH Instance** for **Service Type** and specify other parameters as required. For more information, see **Table 1-1**.

Table 1-1 CBH instance parameters

Parameter	Description
Billing Mode	The billing mode of the instance. Currently, only **Yearly/Monthly** is available. Yearly/Monthly is a prepaid billing mode in which a CBH instance is billed based on the service duration. This cost-effective mode is ideal when the duration of CBH instance usage is predictable.
Region	Select the region where you want to deploy the bastion host. For low network latency and quick resource access, select the region nearest to your workloads.

Parameter	Description
Project	Select the project the bastion host belongs to. For more information, see **Project Management**.
Instance Type	Select a single-node or primary/standby instance type based on your service requirements. • **Single-node**: Only one bastion host is available after the purchase. • **Primary/Standby**: After the purchase, two bastion hosts are delivered to form a two-node cluster. Once the primary bastion host is unavailable, the standby one takes over the job immediately. **NOTE** If you buy a primary/standby instance, do not disable HA, or logins will fail.
AZ	An AZ is the location where the bastion host instance you buy is deployed. For a primary/standby instance, you need to select the primary and standby AZs based on disaster recovery and network latency requirements. • For disaster recovery, different AZs are recommended. Example: Select **AZ2** for **Primary AZ** and **AZ3** for **Standby AZ**. • For lower network latency, one AZ is recommended. Example: Select **AZ2** for both **Primary AZ** and **Standby AZ**.
Instance Name	Name of the CBH instance.
Specifications	Specifications of your CBH instance. CBH provides standard and professional editions. Each edition has 50, 100, 200, 500, 1,000, 2,000, 5,000, and 10,000 asset specifications. Asset quantity indicates the maximum number of resources the instance you buy can manage and the maximum number of concurrent connections your instance can establish. The vCPUs and the size of data and system disks vary depending on the asset quantity. For example, if you select 100 assets, the number of resources your instance can manage and the maximum number of concurrent connections your instance can establish are both 100. **NOTE** Currently, primary/standby instances cannot manage public network resources using EIPs.
Storage Package	If you need more storage for a CBH instance, you can buy a storage package.

Parameter	Description
VPC	The Virtual Private Cloud (VPC) where your instance is located. Select a VPC in the current region. If no VPC is available in the current region, click **View VPC** and create one. **NOTE** • By default, networks in VPCs in different regions or even in the same region are not connected. The network communications on these different networks are isolated from each other. This is not the case for different AZs on the same VPC. Two networks on the same VPC should be able to communicate with each other even if they are in different AZs. • A CBH instance directly manages and allows access from resources, such as ECSs, in the same VPC in the same region. To manage resources such as ECSs in different VPCs in the same region, establish a VPC peering connection, use a VPN, or use other methods to connect networks. For details, see **Creating a VPC Peering Connection**. Managing ECSs across regions is not recommended. For more information, see **VPC Planning**.
Subnet	The subnet in the current VPC for your CBH instance. **NOTE** The selected subnet must be in the VPC network segment. For more information, see **Creating a VPC**.
Assign IPv4 Address	Select **Auto** or **Manual**. If you select **Manual**, you can view the used IP addresses.
Security Group	The security group for your CBH instance. The default security group is **Sys-default** in the current region. If no security group is available, click **Manage Security Groups** to create a security group or configure a new one. **NOTE** • A security group provides access rules for the CBH instances and resources that have the same security protection requirements and are mutually trusted in the same VPC. CBH instances are protected by these access rules after being added the security group. For details, see **Security Group Overview** • CBH instances and ECSs can be added to the same security groups. They do not affect each other when implementing security group rules. • For details about how to modify a security group, see **Changing Security Groups**. • Before creating HA instances, ensure that the security group allows inbound traffic from ports 22, 31036, 31679, and 31873. • During cross-version upgrade, ports 22, 31036, 31679, and 31873 are automatically enabled for the instance. After the upgrade, keep port 31679 enabled and disable other ports immediately if you do not need to use them. For more information about security groups, see **How Do I Configure a Security Group for a CBH Instance?**

Parameter	Description
EIP	(Optional) Select an EIP in the current region. If no EIP is available in the current region, click **Buy EIP** to create one. **NOTE** • If you select an EIP when purchasing an instance, but the EIP fails to be bound to the instance after the instance is in the running state, the EIP may have been bound to other servers while the instance is being created. In this case, bind another EIP to the instance by referring to **Binding an EIP to a CBH Instance**. • An EIP can be bound to only one cloud resource. A CBH instance cannot share an EIP with other cloud resources. After you created a CBH instance, you are required to bind an EIP to the instance for logging in to the CBH system. You need to create at least one EIP for a CBH instance. You can bind an EIP to the CBH instance now or later by referring to **Binding an EIP to a CBH Instance**. • To meet the requirements of the CBH system, set the EIP bandwidth to 5 Mbit/s or higher. • After the CBH instance is created, you can unbind the original EIP from the instance and bind a new EIP to it. For more information about EIPs, see **EIP Overview**.
Enterprise Project	Select the enterprise project the CBH instance you buy belongs to. The **default** enterprise project is selected by default.
Username	The default username **admin** is used. **admin** is the system administrator account. This account has the highest operation permissions. Keep the account information secure.
Password	User-defined password of the **admin** user. **NOTE** • The password must: – Contain 8 to 32 characters. – Contain at least three of the following types of characters: uppercase letters (A to Z), lowercase letters (a to z), digits (0 to 9), and following special characters: !@$%^-_=+[{}]:,./?~#* – Cannot contain the username or the username spelled backwards. – Cannot contain more than two consecutive identical characters. • Enter the same password in the **Password** and **Confirm Password** text boxes. • The CBH system cannot obtain the password of system administrator **admin**. Keep your account information secure. • When you log in to your CBH system as **admin** for the first time, change the password and configure mobile phone number as prompted. Otherwise, you cannot log in to the CBH system. • If you forget the password of user **admin** of the instance after you buy it, you can **reset the password**.
Required Duration	Required duration of the instance You can buy a CBH instance on a monthly or yearly basis.

Parameter	Description
Tag	**Tags**: It is recommended that you use the TMS predefined tag function to add the same tag to different cloud resources. For details, see **Resource Tag Overview**. If your organization has configured a tag policy for CBH, you need to add tags in compliance with the policy. If a tag does not comply with the tag policies, CBH instances may fail to be created. Contact your organization administrator to learn more about tag policies.

Step 5 Confirm details in the **Current Configuration** area and click **Next**.

NOTE

When receiving a network restriction notification, click **Enable** to eliminate the network restrictions so that the instance you buy can be issued.

You can view the rules in the security group and firewall ACL.

- Access to port 9443 is allowed in the outbound direction of the security group to which your CBH instance belongs.
- The subnet where the instance locates is not associated with the firewall ACL, or the ACL rule of the associated firewall allows the instance to access port 9443 in the outbound direction.

Step 6 On the **Confirm** page, confirm the details, read the privacy statement, select **Privacy Statement**, and click **Submit**.

Step 7 Complete the payment on the displayed page. Return to the CBH instance list and check the new CBH instance you buy.

The mapped CBH system is automatically created for you after you buy a CBH instance. It takes about 10 minutes for the creation to complete.

NOTE

Do not unbind an EIP from a CBH instance before the mapped CBH system is created. If you unbind an EIP from an instance before its status changes to **Running**, the mapped CBH system may fail to be created.

----End

Follow-up Procedure

- If the instance **Status** is **Running**, the CBH system is successfully created. Then, you can log in to the CBH system.
- If the instance **Status** is **Failed to create**, check the failure cause in the displayed dialog box. You can click **Service Tickets** in the upper right corner of the management console and submit a service ticket to contact technical support.
- If a CBH instance is about to expire or has expired, locate the row where the instance resides, click **More** > **Renew** in the **Operation** column, and complete required configuration to renew it. For details, see **Renewing a CBH Instance**.

- You need to configure and replace CBH system certificates in a timely manner. For details, see **Updating the CBH System Web Certificate**.

2 Authorizing Access to Cloud Assets

CBH has been interconnected with Key Management Service (KMS), Cloud Secret Management Service (CSMS), Elastic Cloud Server (ECS), and Relational Database Service (RDS), making it easier for you to use credentials managed by your bastion host.

Description

- If you complete the authorization for each asset module, CBH can have the following permissions for each service:
  - CSMS: CBH has the permissions needed to query your credential list in CSMS. You can select credentials as resource accounts on your CBH instance.

    NOTICE

    For secrets invoked through the bastion host, the account and password must comply with **Key** specifications. For details about how to create a secret, see **Data Encryption Workshop > Cloud Secret Management Service**.

    Example:

    username:root

    password:*****

  - KMS: CBH has the permissions needed to use KMS APIs to obtain credentials in CSMS. You can use obtained credentials to log in to the hosts managed by your CBH instance.
  - ECS: CBH will have the permissions to query your ECS list. You can synchronize your ECS list to the host list in CBH in just a few clicks.
  - RDS: CBH will have the permissions to query your RDS instance list. You can synchronize your RDS instance list to the host list in CBH in just a few clicks.
- After you authorize CBH to access KMS, CSMS, ECS, and RDS, it takes about 10 minutes for your bastion host to obtain the delegation tokens.

Procedure

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

Step 2 Click  in the upper left corner on the displayed page and select a region.

Step 3 Click **Cloud Asset Authorization** in the upper right corner.

Step 4 In the displayed dialog box, switch to  in the **Operation** column to enable the authorization.

Step 5 For details about how to add a resource account, see **Creating a Resource Account and Associating It with the Corresponding Resource**.

----End

3 Managing Instances

3.1 Checking Instance Details

Each CBH instance maps to an independently running CBH system.

You can manage CBH instances after obtaining an account with the CBH operation permission.

Checking CBH Instance Information

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

Step 2 Click  in the upper left corner on the displayed page and select a region.

Step 3 Click the instance name to go to its details page. On this page, you can check the basic information, billing mode, network configuration, and tags.

Table 3-1 Instance parameters

Parameter	Description
Instance Name	The name you specify for the instance. It cannot be modified once the instance is created.
Server ID	ID of the server housing the current instance. The ID of the server for the standby node is included.
Instance Type	Type of the instance.
Standby Instance Status	Status of the standby host. **NOTE** This parameter is displayed only when **Instance Type** is **Primary/Standby**.

Parameter	Description
Specifications	Asset specifications of the instance. You can change them if needed. **NOTE** • Changing specifications may fail due to running services. So, you are advised not to change specifications without any backups. • Make sure you have backed up the data before you start the change as specification change failure may affect the use of the bastion host.
Instance Version	Version of the instance.
Enterprise Project	Name of the enterprise project the instance belongs to.
Billing Mode	Billing mode of the current instance
Created	Time the instance is created.
Expiration	Time the instance expires. You can unsubscribe from or renew the instance before it expires.
Upon Expiration	Policy applied after an instance expires. **NOTE** If an instance expires, a grace period is provided based on the customer tier. During this period, you can still use the instance and renew it. After the grace period ends, the instance enters a retention period. During this period, the instance is frozen and cannot be accessed, but the data stored on it will be retained. After the retention period ends, the instance will be automatically released and the data will be automatically cleared.
VPC	VPC the instance in. You can switch the VPC for an instance. **NOTE** • Changing a VPC will interrupt the ECS network and change the subnet, IP address, and MAC address of the ECS. If you have active services, exercise caution when performing this operation. • During this process, do not perform any operations on the ECS or its EIP.
Subnet	Subnet of the VPC configured for the instance.
Virtual IP Address	Floating IP address of the instance.
Private IP Address	Private IP address of the instance, including the IP address of the standby node.
Security Group	Virtual network security rule.

Step 4 Click **Tag** to go to the tag page and view and edit the tag of the instance.

----End

3.2 Changing Specifications of a CBH Instance

If the specifications of your CBH instance cannot meet your requirements, you can upgrade the specifications of the instance. For example, you can select the **standard** or **professional** edition with higher specifications to expand the system data disk capacity, maximum number of concurrent requests, maximum number of assets, CPU, and memory. The default size of a CBH system disk is 100 GB. Changing specifications does not affect the system disk specifications and system software version.

Precautions

- Before specification change

  Data must be backed up before you change CBH specifications. For details, see **How Do I Back Up Data in a CBH System Before Upgrading the System Version?**

  Ensure that the current CBH system is version 3.2.16.0 or later if you want to change specifications to professional editions. Otherwise, the enhanced functions remain unavailable after specification change. If the CBH system version is earlier than 3.2.16.0, **upgrade the system version** first. For details about how to view the CBH system version, see **About System**.
- During specification change

  It takes about 30 minutes for the instance specifications to be changed. During this period, the CBH system is unavailable, but services running on the managed hosts are not affected. To avoid data loss, do not log in to the CBH instance for any operations during this period.
- After specification change

  Only the data disk specifications are changed. The system disk specifications are not affected. The CBH system changes the CPU, memory, and bandwidth for you, which does not affect the use of the original EIP.

For more details, see **CBH Instance Edition Upgrade**

Constraints

- CBH provides the standard and professional editions. Each edition has many types of asset specifications. For details about the edition specifications, see **CBH Editions**.
- Currently, specifications can be increased but cannot be decreased.
- In the current version, all instances cannot be changed without service interruption. During the change, services need to be suspended.

Prerequisites

- The CBH system data has been backed up.

  Before you change specifications, back up the CBH system data in case specification change fails. For details, see **Which Types of System Data Can Be Backed Up in the CBH System?**
- The CBH system has been updated to the latest version.

To change the edition to **Professional**, ensure that the bastion software version is 3.2.16.0 or later. To check the current CBH version, see "Instance Version" in **Checking Instance Details**.

Procedure

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

Step 2 Click  in the upper left corner on the displayed page and select a region.

Step 3 Locate the row that contains the target instance, and choose **More** > **Expand** > **Change Specifications** in the **Operation** column.

Step 4 Specify **New Specifications** and click **Next**.

Step 5 On the **Details** page, confirm the order details and click **Submit**.

NOTE

When receiving a network restriction notification, click **Enable** to eliminate the network restrictions so that specification change can be performed.

You can view the rules in the security group and firewall ACL and ensure that:

- Access to port 9443 is allowed in the outbound direction of the security group to which your CBH instance belongs.
- The subnet where the instance locates is not associated with the firewall ACL, or the ACL rule of the associated firewall allows the instance to access port 9443 in the outbound direction.

Step 6 Complete the payment.

Step 7 No manual actions are required. The specification change takes about 30 minutes. During the change, the status of the CBH instance changes from **Changing** to **Restarting**.

Step 8 When the CBH instance status changes to **Running**, the CBH system is available.

----End

3.3 Increasing Instance Storage

You can increase the storage space of a CBH instance without upgrading other specifications.

Constraints

The CBH system data has been backed up.

Before you expand capacity, back up the CBH system data in the event of expansion failures. For details, see **Which Types of System Data Can Be Backed Up in the CBH System?**

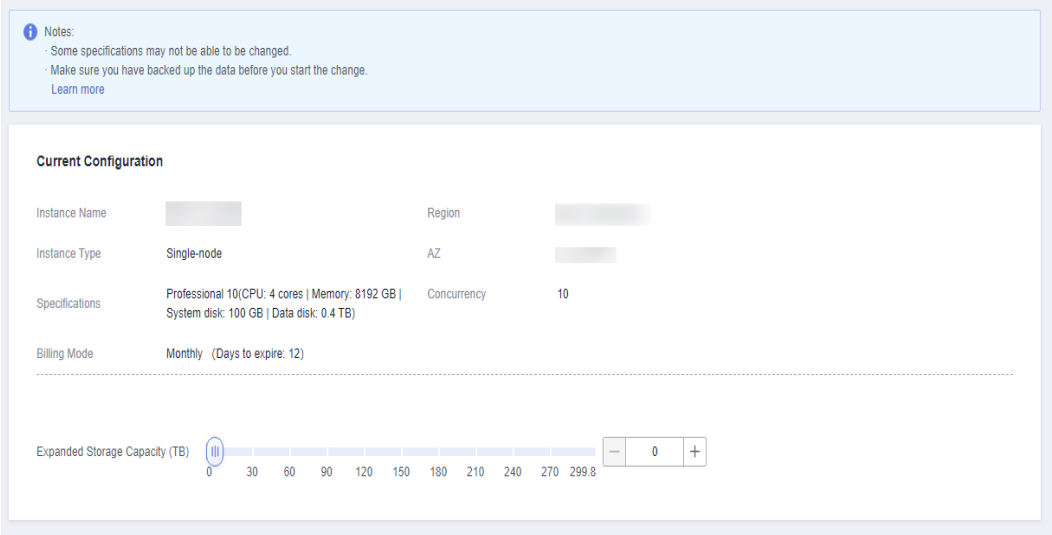
Procedure

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

Step 2 Click  in the upper left corner on the displayed page and select a region.

Step 3 Locate the row containing the instance you want to expand. In the **Operation** column, choose **More** > **Expand** > **Expand Storage**.

Figure 3-1 Expand storage



Step 4 Select the storage space you want to expand, confirm the billing mode and storage space, and then click **Next**.

Step 5 On the details page, confirm the storage of **Current Specifications** and **New Specifications** and the price for capacity expansion. Confirm the information and click **Pay Now**.

Step 6 Complete the payment.

Step 7 It takes about 30 minutes for the expansion to complete. During the expansion, no manual actions are required, and the status of the CBH instance will change from **Changing** to **Restarting**.

Step 8 When the CBH instance status changes to **Running**, the CBH system is available.

----End

3.4 Resetting the Login Method for User admin

This topic walks you through how to reset the login method for user **admin** in case the **admin** account failed one or more multifactor authentication factors.

Procedure

Step 1 Log in to the CBH console.

Step 2 Click  in the upper left corner on the displayed page and select a region.

Step 3 Locate the row containing the target instance. In the **Operation** column, choose **More** > **Reset** > **Reset Login Method for Admin**.

Step 4 In the displayed dialog box, click **OK** to reset the login method for user **admin**.

NOTE

After the login mode is reset, user **admin** must use the username and password to log in. To configure multi-factor authentication, see **Configuring Multifactor Verification**.

----End

3.5 Resetting the Password of User admin

This topic describes how to reset the password of user **admin** for a CBH system.

To reset passwords of other system users, see **How Can I Reset Passwords of CBH System Users?**

Procedure

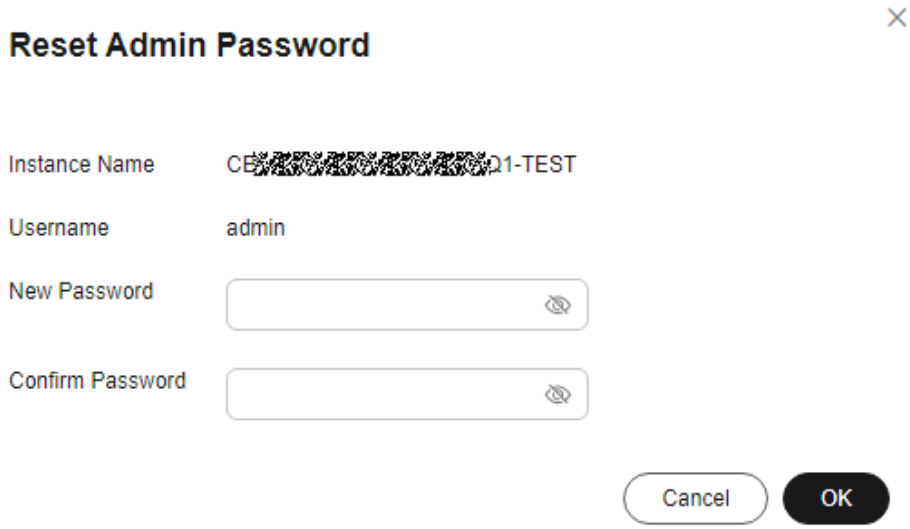
Step 1 **Log in to the CBH console**.

Step 2 Click in the upper left corner on the displayed page and select a region.

Step 3 Locate the row containing the target instance. In the **Operation** column, choose **More** > **Reset** > **Reset Admin Password**.

Step 4 In the dialog box displayed, reset the password of the admin account.

Figure 3-2 Resetting a password



Step 5 Confirm the configuration and click **OK**.

----End

3.6 Changing an Instance from Single-Node to Primary/Standby Deployment

This section describes how to change an instance from single-node to primary/standby node.

CAUTION

- Only CBH instances of the latest edition can be changed from single-node to primary/standby deployment. You can upgrade the instance edition if needed by referring to **Upgrading the Instance Version**.

Procedure

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

Step 2 Click  in the upper left corner on the displayed page and select a region.

Step 3 Locate the row containing the target instance. In the **Operation** column, choose **More** > **Change to Primary/Standby**.

Step 4 On the displayed page, specify **Standby Instance AZ** and click **Next**.

Step 5 Confirm the order details on the details page and click **Submit**.

NOTE

After the order is submitted, the **Status** of the instance changes to **Creating the standby instance** and then **Configuring HA**.

----End

3.7 Upgrading the Instance Version

CBH periodically upgrades the bastion host instance version to optimize functions or add new features. So the latest instance version is recommended.

- For the instance version update, see **What's New**.
- To view the version of the CBH instance in use, check **Device System** in **Viewing CBH Instance Information**.

Precautions

- Instance version description

  When upgrading versions of some CBH instances, two upgrades may be required. So, check the current version and the upgrade process before you start, as shown in **Table 3-2**.

Table 3-2 Process of upgrading a bastion host instance to the latest version

Version In Use	Applicable Process
3.3.37.0 or earlier	Two upgrades are required. • First upgrade: Upgrading the current version to 3.3.37.6. Rollback is not allowed during the upgrade. • Second upgrade: Upgrading the version from 3.3.37.6 to the latest version.

Version In Use	Applicable Process
3.3.38.0 to 3.3.50.0 (including 3.3.38.0 and 3.3.50.0)	Two upgrades are required. • First upgrade: Upgrading the current version to 3.3.50.4. Rollback is not allowed during the upgrade. • Second upgrade: Upgrading the version from 3.3.50.4 to the latest version.
3.3.52.0 or later (except the latest version)	Directly upgrade the current version to the latest version.

- Before the upgrade
  - Back up data to ensure a quick rollback in case of upgrade failure. For details, see **Which Types of System Data Can Be Backed Up in the CBH System?**
  - For instances with version 3.3.52.0 or later, the start time for a scheduled upgrade must be at least 24 hours later than the current time. You are advised to upgrade the service during idle hours. If a scheduled upgrade is set, you cannot shut down, restart, change, or expand the capacity of the bastion host. Before the upgrade starts, you can cancel the scheduled upgrade and reset the upgrade time.
- During the upgrade
  - The version upgrade takes about 30 minutes. Although the CBH system is unavailable during this period, there is no impacts on host resources managed on the instance. However, to prevent important data loss, do not log in to the CBH system during the version upgrade.
  - After the version upgrade is complete or during the cross-version upgrade, you can roll back the upgrade on the bastion host details page. After the rollback starts, the status of the bastion host will change to **Rolling back edition**.
- After the upgrade
  - The CBH instance automatically restarts after the upgrade completes. You can then use the mapped CBH system.
  - After the upgrade, you can use the configuration and storage data of the original CBH system. Version upgrading does not affect the original configuration and storage data of the CBH system.
  - After a cross-version upgrade is successful, the system enters a seven-day rollback retention period (during which the upgrade button is unavailable). If the rollback retention period expires, the rollback cannot be performed. Verify the CBH data after the upgrade.
  - The scale-out after the upgrade cannot be rolled back. If you plan a scale-out task after an upgrade, start the scale-out task 5 minutes later when the upgrade is finished.
  - After a successful cross-version upgrade, the instance ID, server ID, instance version, and creation time will change.

  - During cross-version upgrade, ports 80, 8080, 443, and 2222 are automatically enabled for the instance. If you do not need to use these ports, disable them immediately after the upgrade.
  - During cross-version upgrade, ports 22, 31036, 31679, and 31873 are automatically enabled for the instance. After the upgrade, keep port 31679 enabled and disable other ports immediately if you do not need to use them.
  - If a web certificate has been imported for an instance, import the certificate again after the cross-version upgrade for the instance.
- Version rollback

  After a rollback, the bastion host will restore to what it is before the upgrade. Data changes and new data will be lost as the bastion host will be interrupted during the rollback. Exercise caution when performing this operation.

Constraints

- In the new version of CBH, the application publish function is optimized. After the upgrade, to use the application O&M functions as usual, install the required plug-in on the application publish server as prompted. For details, see **Installing RemoteApp Program**.
- To upgrade version 3.3.40.0 and 3.3.41.0, synchronize the time of OBS buckets first.
- In the current version, all instances cannot be upgrade without service interruption. During the upgrade, services need to be suspended.

Prerequisites

The CBH system data has been backed up.

Before you upgrade, back up the CBH system data in the event of upgrade failures. For details, see **Which Types of System Data Can Be Backed Up in the CBH System?**

Procedure

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

Step 2 Click  in the upper left corner on the displayed page and select a region.

Step 3 In the row containing the target instance, choose **More** > **Plan Upgrade** > **Upgrade Schedule** in the **Operation** column.

NOTE

- Before the upgrade, click the target instance name to go to the details page and check the version in use on that page. Then, you can start the upgrade by referring to the applicable process in **Table 3-2**.
- If two upgrades are involved, start the second upgrade until the first one is complete.

Step 4 In the displayed instance upgrade dialog box, select the scheduled upgrade time and enter **YES** in the dialog box.

NOTE

Upgrade types:

- If two upgrades are required, it takes about 15 to 30 minutes to complete the first upgrade. During this period, the bastion host service will be interrupted.
- During the cross-version upgrade, a new CBH instance will be created, and the CBH instance you are using will be interrupted. It takes about 30 minutes to 2 hours to complete the upgrade. During the cross-version upgrade, the instance status changes to **Upgrading** first, and then to **Migrating data**, **Configuring HA**, and to **Running**.

Step 5 Wait for the upgrade to complete. It takes about 15 minutes to 2 hours for the upgrade to finish at the backend. The actual upgrade time varies depending on the upgrade type. Once the upgrade starts, the instance status changes to **Upgrading**.

Step 6 When the CBH instance status changes to **Running**, the CBH system is available.

After the upgrade is complete, click the instance name and check the instance version on the details page.

NOTE

- If the instance version does not change after the upgrade, the upgrade fails. Contact technical support.
- If two upgrades are needed, the second upgrade cannot be started until the first one is successful. You can check the new instance version on the instance details page.

----End

3.8 Starting a CBH Instance

The instance needs to be started in the following scenarios:

- After a CBH instance is stopped, its **Status** changes to **Stopped**. To log in to the mapped CBH system again, start the instance.
- If a CBH instance is abnormal, its **Status** changes to **Abnormal**. To log in to the mapped CBH system again, try starting the instance.

Procedure

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

Step 2 Click  in the upper left corner on the displayed page and select a region.

Step 3 Locate the row containing the instance you want to start. In the **Operation** column, click **Start**.

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

After the instance is started, its **Status** changes to **Running**.

----End

3.9 Stopping a CBH Instance

You can stop an instance in the **Running** status. After the instance is stopped, you cannot log in to the CBH system.

NOTE

Before stopping a bastion host instance, make sure no operations or O&M tasks are in progress. Once the bastion host instance is stopped, ongoing operations and O&M tasks will be forcibly logged out immediately.

Procedure

Step 1 Log in to the CBH console.

Step 2 Click in the upper left corner on the displayed page and select a region.

Step 3 Locate the row containing the instance you want to stop. In the **Operation** column, choose **More** > **Stop**.

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

After the CBH instance is stopped, its **Status** changes to **Stopped**.

A bastion host instance is still billed after it is stopped. So if you no longer need a bastion host instance, you need to delete it to stop the billing.

----End

3.10 Restarting a CBH Instance

To fix an abnormal instance, you can try restarting it.

NOTE

- Before restarting a bastion host instance, make sure no operations or O&M tasks are in progress. Once the bastion host instance is restarted, ongoing operations and O&M tasks will be forcibly logged out immediately.
- You can restart a bastion host instance in the **Running** status.
- Restarting a bastion host instance will interrupt services of the mapped system for about 5 minutes. During this period, the instance status is **Restarting**, so that the bastion system is unavailable.

Procedure

Step 1 Log in to the CBH console.

Step 2 Click in the upper left corner on the displayed page and select a region.

Step 3 Locate the row containing the instance you want to restart. In the **Operation** column, choose **More** > **Restart**.

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

> NOTE
>
> To forcibly restart a CBH instance, select the **Forcibly restart** check box. Forcibly restarting an instance may cause data loss. Make sure all data files have been saved before performing this operation, and no operations are performed in the mapped CBH system.

Step 5 The restart process usually takes about 5 minutes. During the restart, the instance status will change to **Restarting**.

The restart may take a longer time if both the CBH instance version upgrade and capacity expansion are performed.

> NOTE
>
> During the restart, an error might be reported indicating that the instance is abnormal and asking you to contact technical support. This is normal.

Step 6 Check the instance status. If it changes to **Running**, the bastion host system is available.

----End

3.11 Changing a VPC for a CBH Instance

This topic describes how to change the VPC your CBH instance belongs to on the CBH console. Provisioning your CBH instances and other projects in the same VPC will make communications between them more secure and stable.

Constraints

- The CBH instances must be in the **Running** status.
- Before changing the VPC, ensure that there are enough **Available IP Addresses** in the target VPC subnet. To check available IP addresses, go to the VPC console and select the target subnet.
  - Single-node instance: At least one IP address is required.
  - Primary/Standby instance: At least three IP addresses are required.
- The CBH instance version must be V3.3.52.0 or later.

Procedure

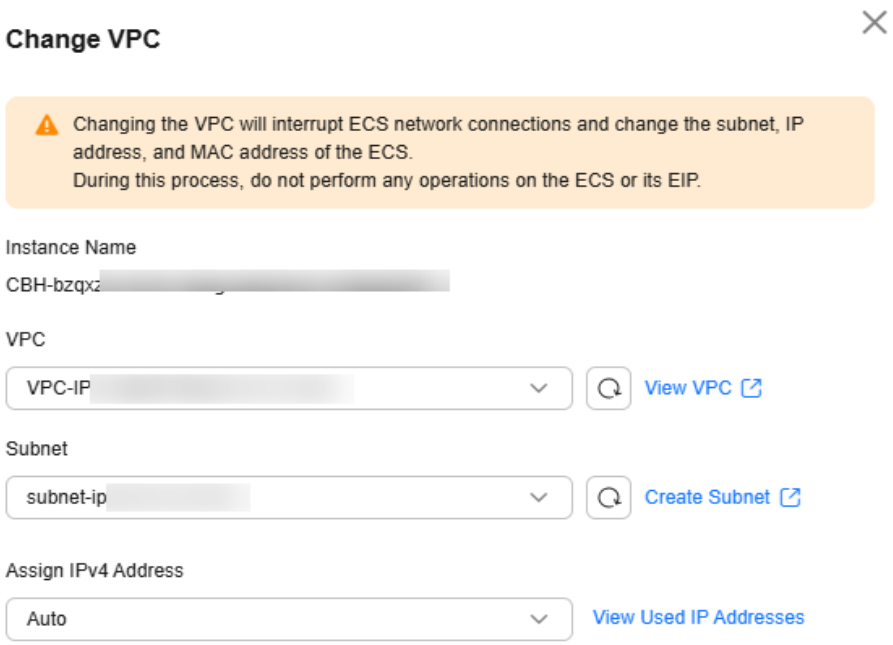
Step 1 **Log in to the CBH console**.

Step 2 Click  in the upper left corner on the displayed page and select a region.

Step 3 Locate the row that contains the target instance. In the **Operation** column, choose **More** > **Configure Network** > **Change VPC**.

Step 4 Select the target VPC and subnet from the **VPC** and **Subnet** drop-down lists.

Figure 3-3 Change VPC



NOTE

After changing the VPC, you need to remove the CBH instance from the original VPC subnet, or the subnet will still be used.

Step 5 Click **OK**.

----End

3.12 Changing Security Groups

A security group is a logical group. It provides access control policies for the ECSs and CBH instances that are trustful to each other and have the same security protection requirements in a VPC.

To ensure CBH instance security and reliability, configure security group rules to allow specific IP addresses and ports to access the resources. However, if you select an inapplicable security group when purchasing a bastion host, you cannot allow access from these IP addresses and ports by configuring security group rules. In this case, change the security group to meet your O&M requirements.

Constraints

- A CBH instance can be added to a maximum of five security groups.
- The CBH instances must be in the **Running** status.
- If a CBH instance is added to multiple security groups, rules of all security groups are applied to the instance.

Procedure

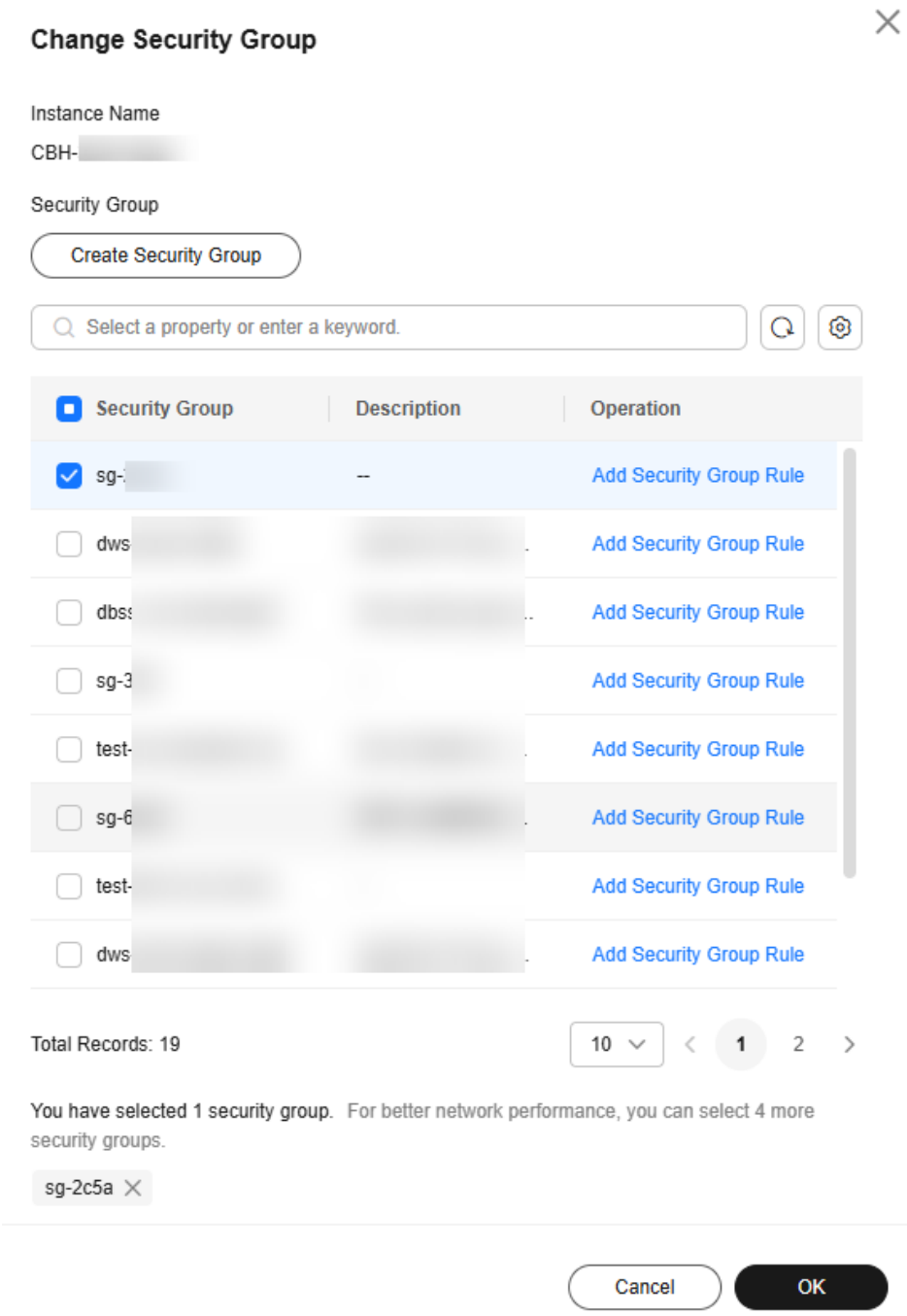
Step 1 Log in to the CBH console.

Step 2 Click in the upper left corner on the displayed page and select a region.

Step 3 Locate the row that contains the target instance. In the **Operation** column, choose **More** > **Configure Network** > **Change Security Group**.

Step 4 In the displayed dialog box, select the security group you want to configure for the instance.

Figure 3-4 Change Security Group



Step 5 Click **OK**. The security group is modified.

----End

3.13 Binding an EIP to a CBH Instance

An EIP must be bound to a bastion host instance if you want to perform any of the following operations (the minimum EIP bandwidth is 5 Mbit/s):

- Log in to your bastion host using a web browser. Login address: https://*<EIP-of-the-bastion-host-instance>*. for example, *https://10.10.10.10*.
- If the mobile SMS login is configured, you need to obtain the verification code through the mobile phone. If the EIP is not configured, you cannot receive SMS messages.
- Interconnect with LTS to send logs. For details, see **Configuring LTS**.
- In V3.3.2.0 and earlier versions, if no EIPs are bound to a bastion host instance, operations such as changing the version specifications, upgrading the version, and starting or restarting the instance will fail.

Constraints

When binding an EIP to a CBH instance, the operation can be done on the CBH console only. Otherwise, you cannot log in to the CBH instance using IAM.

Prerequisites

You have purchased at least one elastic IP address (EIP).

CAUTION

- An EIP can be bound to only one cloud resource. A CBH instance cannot share an EIP with other cloud resources.
- The same account must be used when you purchase CBH instances and EIPs to be bound to them. The instances and EIPs must be in the same region.

Procedure

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

Step 2 Click  in the upper left corner on the displayed page and select a region.

Step 3 Locate the row containing the instance to which you want to bind an EIP. In the **Operation** column, choose **More** > **Configure Network** > **Bind EIP**.

Step 4 In the displayed dialog box, select an EIP in the **Unbound** status and click **OK**.

If no EIPs are available, create one. For details, see **EIP Overview**.

After the EIP is bound, you can view it in the **EIP** column of the instance list. The **Login** button in the **Operation** column becomes available.

----End

3.14 Unbinding an EIP from a CBH Instance

To bind another EIP to a bastion host instance or release an EIP that has been bound to a bastion host instance, unbind the EIP from the instance first. After the EIP is unbound from the CBH instance, this EIP cannot be used to log in to the CBH system.

Procedure

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

Step 2 Click  in the upper left corner on the displayed page and select a region.

Step 3 Locate the row containing the instance from which you want to unbind an EIP. In the **Operation** column, choose **More** > **Configure Network** > **Unbind EIP**.

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

After the unbinding is successful, no IP address is displayed in the **EIP** column of the instance. The **Log in** button in the **Operation** column becomes unavailable.

----End

3.15 Managing Tags

You can use tags to manage resources in batches. For resources you want to manage them hierarchically, you can use keys and values. For common resources, you can use only keys.

Adding a Tag

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

Step 2 Click  in the upper left corner on the displayed page and select a region.

Step 3 Click the name of the target instance to go to its details page.

Step 4 In the **Tag** area, click **Add Tag**. In the dialog box displayed, enter a tag key and value.

NOTE

- A tag key cannot start with _sys_, and cannot start or end with a space. But UTF-8 letters, digits, spaces, and the following characters are allowed: _.:=+-@
- A tag value can contain only UTF-8 letters, digits, spaces, and the following characters: _.:=+-@
- It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. For details, see **Creating Predefined Tags**.

Step 5 Confirm the information and click **OK**. The tag is added.

----End

Editing a Tag

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

Step 2 Click  in the upper left corner on the displayed page and select a region.

Step 3 Click the name of the target instance to go to its details page.

Step 4 Click **Edit** in the **Operation** column of the target tag and edit the tag value.

Step 5 Confirm the information and click **OK**. The tag is modified.

----End

Deleting a Tag

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

Step 2 Click  in the upper left corner on the displayed page and select a region.

Step 3 Click the name of the target instance to go to its details page.

Step 4 Click **Delete** in the **Operation** column of the target tag.

Step 5 Confirm the deletion and click **OK**. The tag is deleted.

----End

3.16 Resource Management

CBH has been interconnected with LTS. You can view CBH resources on the **My Resources** page.

Procedure

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

Step 2 Click  in the upper left corner on the displayed page and select a region.

Step 3 In the navigation pane on the left, choose **Resource List**.

Step 4 Under **Service**, click **Cloud Bastion Host (CBH)** to filter all CBH resources.

Step 5 In the resource list, you can filter resource types by **Name**, **Resources ID**, and **Enterprise Project**.

Step 6 Click **Export Resource Info** to export resource details.

----End

3.17 Renewing a CBH Instance

To ensure that your CBH system is available, renew the CBH license before it expires or in a given period after it expires.

- If your CBH instance is about to expire, renew your subscription.

- If your CBH instance fails to be renewed before it expires, there is a retention period for you to renew it. During this period, you can still use the CBH instance. If the CBH instance fails to be renewed within the retention period, the CBH instance the will be frozen. The mapped CBH system becomes inaccessible. If your subscription is still not renewed within the retention period, your data stored in the CBH system will be deleted, and the resource will be released.
- You can select one-off renewal or auto-renewal.

Prerequisites

You have lifted network restrictions on the CBH instance.

NOTE

When receiving a network restriction notification, click **Enable** to eliminate the network restrictions so that the instance can be renewed.

You can view the rules in the security group and firewall ACL and ensure that:

- Access to port 9443 is allowed in the outbound direction of the security group to which your CBH instance belongs.
- The subnet where the instance locates is not associated with the firewall ACL, or the ACL rule of the associated firewall allows the instance to access port 9443 in the outbound direction.

Procedure

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

Step 2 Click  in the upper left corner on the displayed page and select a region.

Step 3 Locate the instance to be renewed, click **More > Renew** in the **Operation** column, and select a renewal method based on your needs.

- **Renew Once**: Select a fixed renewal period and set a fixed expiration date. After confirming the order, click **Pay Now**. Complete the payment on the payment page.
- **Auto Renew**: Select a renewal duration, select **Auto-renewals**, and specify the renew times. Confirm the information and click **Enable**.

Step 4 Return to the CBH instance list page and check the expiration time in the **Billing Mode** column. You can log in to the CBH system in about 5 minutes.

NOTE

After the renewal, the new license will be automatically delivered and deployed in about 5 minutes.

----End

3.18 Releasing an Instance

You can unsubscribe from a CBH instance if you no longer need it.

Prerequisites

You have stopped all operations in the CBH system and unbound the EIP from the instance you want to unsubscribe from.

Procedure

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

Step 2 Click  in the upper left corner on the displayed page and select a region.

Step 3 Locate the row containing the target instance and choose **More** > **Release** in the **Operation** column.

Step 4 Confirm the information and click **OK**.

Step 5 Complete the unsubscription.

NOTE

- You can only unbind an EIP from a CBH instance. To release an EIP, go to the EIP management page and manually release it.
- After the unsubscription request is submitted and approved, you will get a refund for the remaining required duration within a specified period. For more details, see **Unsubscription Rules**.
- It takes about one minute to complete the unsubscription.
- After you unsubscribe from a CBH instance, you cannot log in to the mapped CBH system and system data cannot be retrieved. Exercise caution when performing this operation.
- After you unsubscribe from a bastion host, the residual resources will be automatically cleared at 03:00 the next day. If you want to delete a security group, wait until the residual resources are cleared.

----End

3.19 Rolling Back the Upgrade

Bastion hosts can be rolled back to historical versions.

Prerequisites

- The bastion host instance to be rolled back must have been upgraded from an earlier version to the new version.
- Before the rollback, ensure that there are no on-going operations in the bastion host system.

Limitations and Constraints

- Only bastion hosts in the **Running** status can be rolled back.
- Bastion hosts that have been upgraded from **Single-node** to **Primary/Standby** as stated in **Changing an Instance from Single-Node to Primary/Standby Deployment** cannot be rolled back.

Procedure

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

Step 2 Click  in the upper left corner on the displayed page and select a region.

Step 3 In the row containing the target instance, choose **More** > **Plan Upgrade** > **Roll Back Version** in the **Operation** column.

Step 4 Check the instance version on the details page after the rollback. The rollback is automatically started and finished.

----End

3.20 Key CBH Instance Operations Recorded by CTS

3.20.1 CBH Operations Supported by CTS

Cloud Trace Service (CTS) records operations on cloud resources in your account. You can use the logs to perform security analysis, track resource changes, audit compliance, and locate faults.

After CTS is enabled, the system starts to record CBH operations. You can view operation records generated in the latest seven days on the CTS console. **Table 3-3** lists the CBH instance operations that can be recorded by CTS.

Table 3-3 Supported CBH instance operations

Operation	Resource Type	Trace Name
Starting a bastion host instance	cbh	StartInstance
Stopping a bastion host instance	cbh	StopInstance
Restarting a bastion host instance	cbh	RebootInstance
Upgrading a bastion host instance	cbh	UpgradeInstance
Rolling back a bastion host instance	cbh	RollbackInstance
Logging in to a bastion instance console as an IAM user	cbh	LoginInstance
Resetting the password of user admin for a bastion host instance	cbh	ResetInstancePassword

Operation	Resource Type	Trace Name
Resetting the login mode for user admin for a bastion host instance	cbh	ResetInstanceLoginMethod
Deleting a faulty bastion host instance	cbh	DeleteInstance
Changing a bastion host instance	cbh	ResizeInstance
Creating a bastion host instance	cbh	CreateInstance
Binding an EIP to a bastion host instance	cbh	InstallInstanceEip
Unbinding an EIP from a bastion host instance	cbh	UninstallInstanceEip
Changing the security group for a bastion host instance	cbh	UpdateInstanceSecurityGroup
Obtaining the CBH agency authorization of a specific user	cbh	ShowAuthorization
Creating or canceling an agency authorization for CBH	cbh	RegisterAuthorization
Counting the number of instances with a specified tag	cbh	CountInstancesByTag
Querying the tags of a bastion host instance	cbh	ShowInstanceTags
Creating tags for multiple instances	cbh	BatchCreateInstanceTag
Obtaining the O&M link	cbh	ShowOmUrl
Logging in to the console of a bastion host instance as user admin	cbh	LoginInstanceAdmin
Changing the type of a single-node bastion host instance	cbh	ChangeInstanceType
Changing the VPC for a bastion host instance	cbh	SwitchInstanceVpc

3.20.2 Viewing CTS Traces

After CTS is enabled, the system starts recording operations of CBH. Operation records for the last seven days can be viewed on the CTS console.

Procedure

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

Step 2 Click  in the upper left corner on the displayed page and select a region.

Step 3 On the left navigation pane, choose **Trace List**.

Step 4 Specify the filters used for querying traces. The following filters are available:

- **Trace Source**, **Resource Type**, and **Search By**
  - Select a search criteria from the drop-down list box. For example, choose **CBH** > **cbh** > **Trace Name** > **createInstance**, and click **Query** to query all instance creation operations.
  - **Trace Name**: Select a trace name, for example, **createInstance**.
  - **Resource ID**: Select or manually enter the ID of a CBH instance whose logs are to be viewed.
  - **Resource Name**: Select or manually enter the name of a CBH instance whose logs are to be viewed.
- **Operator**: Select a specific operator (a user rather than tenant).
- **Trace Status**: Available options include **All trace statuses**, **normal**, **warning**, and **incident**. You can only select one of them.
- You can specify start time and end time query traces during a time period.

Step 5 Click on the left of the trace to be queried to extend its details.

Step 6 Click **View Trace** in the **Operation** column for details.

----End

4 Logging In to a Bastion Host Instance

4.1 Logging In to an Instance

You can log in to a bastion host remotely, using a browser, or using a client.

During remote logins, you can select local, IAM, or admin login mode. In local or IAM login mode, use the accounts as required. In admin login mode, you can log in to a bastion host as user **admin** without entering passwords.

Accounts or keys are required for local logins, client logins, and browser logins.

If you have logged in to your bastion host using the current browser, you need to log out of the current account before logging in to the instance using another account.

Port Requirements

To use a bastion host for resource management, ensure that the communication between the bastion host and the managed resources is enabled. Before you start, check whether your network ACL configuration allows access to the bastion host and configure the security group for the bastion host by referring to **Table 4-1**.

⚠ CAUTION

- During cross-version upgrade, ports 80, 8080, 443, and 2222 are automatically enabled for the instance. If you do not need to use these ports, disable them immediately after the upgrade.
- During cross-version upgrade, ports 22, 31036, 31679, and 31873 are automatically enabled for the instance. After the upgrade, keep port 31679 enabled and disable other ports immediately if you do not need to use them.

Table 4-1 Inbound and outbound rule configuration reference

Scenario Description	Direction	Protocol/ Application	Port
Accessing a bastion host through a web browser (HTTP and HTTPS) **NOTE** • If HTTPS is used, configure port 443 only. • HTTP automatically redirects requests to HTTPS. If HTTP is used, configure both ports 80 and 443. Otherwise, the automatic redirection will not take effect.	Inbound	TCP	Ports 80 and 443
Accessing a bastion host through Microsoft Terminal Services Client (MSTSC)	Inbound	TCP	53389
Accessing a bastion host through an SSH client	Inbound	TCP	2222
Accessing a bastion host through an FTP client	Inbound	TCP	2121 and 20000 to 21000
Accessing a bastion host through an SFTP client	Inbound	TCP	2222
Remotely accessing Linux cloud servers managed by a bastion host over SSH clients	Outbound	TCP	22
Remotely accessing Windows cloud servers managed by a bastion host over the RDP protocol	Outbound	TCP	3389
Accessing Oracle databases through a bastion host	Inbound	TCP	1521
	Outbound	TCP	1521
Accessing MySQL databases through a bastion host	Inbound	TCP	33306
	Outbound	TCP	3306
Accessing SQL Server databases through a bastion host	Inbound	TCP	1433
	Outbound	TCP	1433
Accessing DB databases through a bastion host	Inbound	TCP	50000
	Outbound	TCP	50000
Accessing GaussDB databases through a bastion host	Inbound	TCP	18000

Scenario Description	Direction	Protocol/ Application	Port
	Outbound	TCP	8000 and 18000
License servers	Outbound	TCP	9443
Huawei Cloud services	Outbound	TCP	443
Accessing a bastion host system through an SSH client in the same security group	Outbound	TCP	2222
SMS service	Outbound	TCP	10743 and 443
Domain name resolution service	Outbound	UDP	53
Accessing PGSQL databases through a bastion host	Inbound	TCP	15432
	Outbound	TCP	5432
Accessing DM databases through a bastion host	Inbound	TCP	15236
	Outbound	TCP	5236
Accessing Redis databases through a bastion host	Inbound	TCP	16379
	Outbound	TCP	6379
Accessing databases through an SSH tunnel	Inbound	TCP	62222

Logon Type

Different login methods require different credentials. If multifactor verification is enabled, the static password login method becomes invalid.

Table 4-2 Login method description

Logon Type	Login Description
Password	Enter the username and password of your bastion host.
Mobile SMS Authentication	Enter the username and password of your bastion host, click **Send Code**, and enter the SMS verification code you will receive.

Logon Type	Login Description
Mobile OTP	Enter the username and password first, and then enter the mobile one-time password (OTP).
USBKey	Insert your USB key into your terminal device, select the issued USB key, and enter the corresponding personal identification number (PIN).
One-time Passwords (OTPs)	Enter the username and password first, and then enter the verification code displayed on your OTP token device.
Email	Enter the username, password, and email verification code. The email verification code is valid for 120 seconds.

Verification Type

You can use remote Active Directory (AD), Remote Authentication Dial In User Service (RADIUS), Lightweight Directory Access Protocol (LDAP), Security Assertion Markup Language (SAML), and Azure AD authentication methods. You can use existing user passwords on any of those remote servers for identity verification.

Table 4-3 Authentication methods

Verification Type	Authentication Description
Local Authentication	Static passwords configured for the system are used for identity verification. • Multifactor verification can be configured for users authenticated by static password. • You can reset or change the static passwords. If you forgot this password, you can find it back through email.
AD domain authentication	The passwords of users on the AD server are used for identity verification. • Multifactor verification can be configured for users authenticated by static password. • Passwords cannot be changed through the bastion host.
RADIUS Authentication	The passwords of users on the RADIUS server are used for identity verification. • Multifactor verification can be configured for users authenticated by static password. • Passwords cannot be changed through the bastion host.

Verification Type	Authentication Description
LDAP Authentication	The passwords of users on the LDAP server are used for identity verification. • Multifactor verification can be configured for users authenticated by static password. • Passwords cannot be changed through the bastion host.
Azure AD authentication	The passwords of Microsoft accounts are used for identity verification. The login page is redirected to the Microsoft Azure login page for you to provide credentials. • Multifactor verification cannot be configured for users authenticated by the Azure AD server. • Passwords cannot be changed through the bastion host.
SAML authentication	The passwords of users on the SAML server are used for identity verification. • Multifactor verification can be configured for users authenticated by static password. • Passwords cannot be changed through the bastion host.

4.2 Logging In to a Bastion Host Through the Service Console

You can select **Local Login**, **IAM Login** (available in V3.3.44.0 or later), or **Admin Login** (available in V3.3.52.1 or later, but not supported by Kunpeng bastion hosts). If you select **IAM Login** or **Admin Login**, no password is required.

If you have logged in to your bastion host using the current browser, you need to log out of the current account before logging in to the instance using another account.

Procedure

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

Step 2 Click  in the upper left corner on the displayed page and select a region.

Step 3 Locate the target instance and click **Remote Login** in the **Operation** column. In the displayed dialog box, select a login mode.

NOTE

- If you want to use a private IP address to log in a bastion host, make sure the instance and your local network are connected, or the login will fail.
- You can log in to the bastion host using **IAM Login** or **Admin Login** without entering a password. However, you must use an account or key to log in to the bastion host using **Local Login**.

Step 4 On the bastion host login page, select a verification mode, enter the login name, static password, and dynamic verification code as prompted, and click **Login**.

For details about the supported authentication methods and operations, see **Using a Web Browser to Log In to Your Bastion Host**.

----End

4.3 Using a Web Browser to Log In to Your Bastion Host

You can use mainstream browsers to log in to your bastion host for system management and resource O&M. Web browsers are recommended for system administrator **admin** or other administrators to manage the system and audit authorization.

NOTE

- First-time login users are required to bind a mobile number for password resetting.
- If you log in to a bastion host through the service console, you can select **Local Login**, **IAM Login** (available in V3.3.44.0 or later), or **Admin Login** (available in V3.3.52.1 or later, but not supported by Kunpeng bastion hosts). If you select **IAM Login** or **Admin Login**, no password is required.

Prerequisites

An EIP has been bound to your bastion host.

Procedure

Step 1 Enter the IP address of your bastion host in the address box of your browser to access the login page.

URL: https:// *EIP of your bastion host*, for example, *https://10.10.10.10*.

NOTE

Use supported browsers to access your bastion host. In an incompatible browser, the login verification message may fail to be sent to you, or exceptions may occur after you log in. For recommended browsers, see **Restrictions on Using CBH**.

Step 2 Select a login method on the login page.

Step 3 Enter credentials required by the login method you chose.

- **Using Static Passwords for Login Authentication**
- **Using SMS Messages for Login Authentication**
- **Using an Email Address for Login Authentication**
- **Using Mobile OTPs for Login Authentication**
- **Using a USB Key for Login Authentication**
- **Using an OTP Token for Login Authentication**
- **Using Azure AD for Login Authentication**

----End

Using Static Passwords for Login Authentication

Step 1 Select **Password**.

Step 2 Enter the username and password of your account.

Step 3 Click **Login**.

----End

Using SMS Messages for Login Authentication

Before you start, ensure that your mobile number can receive SMS messages.

Step 1 Select **SMS**.

Step 2 Enter the username and password of your bastion host account.

Step 3 Click **Send code** and enter the 6-digit OTP token in the received SMS message.

Step 4 Click **Login**.

----End

Using an Email Address for Login Authentication

Step 1 Select **Email**.

Step 2 Enter the username and password of your account.

Step 3 Obtain a verification code and enter the verification code.

Step 4 Click **Login**.

----End

Using Mobile OTPs for Login Authentication

Before your start, ensure that the time on your mobile phone must be the same as that in your bastion host, accurate to seconds.

NOTICE

The mobile phone token applet for your bastion host is stored in the applet cache. The applet cache may be cleared mistakenly in the background.

You can save the QR code image when applying for a mobile phone token. If the preceding situation occurs, scan the QR code again.

Step 1 Select **OTP**.

Step 2 Enter the username and password of your account.

Step 3 Start the token client on your mobile phone, obtain the 6-digit OTP, and enter it in the **OTP** text box.

Step 4 Click **Login**.

----End

Using a USB Key for Login Authentication

Step 1 Select **USBKey**.

Step 2 Insert your USB key. The bastion host automatically identifies the USB key.

Step 3 Enter the PIN code displayed on your USB key.

Step 4 Click **Login**.

----End

Using an OTP Token for Login Authentication

Step 1 Select **OTP token**.

Step 2 Enter the username and password of your account.

Step 3 Obtain the 6-digit OTP from the issued hardware token and enter it in the **OTP token** text box.

Step 4 Click **Login**.

----End

Using Azure AD for Login Authentication

Step 1 Click the Azure AD login link to go to the Microsoft Azure login page.

Step 2 Enter the username and password of your Microsoft Azure account as prompted.

NOTE

Your login name must contain the email address suffix, for example, zhang@example.com.

Step 3 Click **Log In**. After the verification is successful, you can log in to the system.

----End

4.4 Using a Client to Log In to Your Bastion Host

Your current client-based operation experience is still useful while using a bastion host for operations. Through your bastion host, you can use an SSH or Microsoft Terminal Services Client (MSTSC) client to directly log in to managed resources for operations.

- SSH client logins can be authenticated by static passwords, public keys, SMS messages, mobile OTPs, or OTP tokens.
- MSTSC client logins can only be authenticated by static passwords.
- SecureCRT 8.0 or later and Xshell 5 or later are recommended.

Using an SSH Client to Log In to Your Bastion Host

You can use an SSH client to log in to your authorized resources over your bastion host.

- Only host resources configured with the SSH, Telnet, or Rlogin protocols can be logged in through an SSH client.
- SecureCRT 8.0 or later and Xshell 5 or later are recommended.

Step 1 Start the local SSH client tool and choose **File** > **New** to create a user session.

Step 2 Configure session connections.

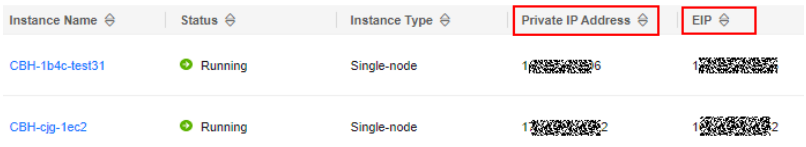
- Method 1

  In the displayed dialog box, select a protocol type, enter the EIP and port number (2222) of the bastion host instance, and click **OK**. Enter the login name of your CBH system account and click **Connect**.

- Method 2
  - In the newly opened blank session window, run a command in the following format: ***Protocol type User login name@System login IP address Port number***, for example, ssh admin@10.10.10.10 2222. After the login, select the target server.
  - In a newly opened blank session window, run a login command: ***{Protocol type} {Bastion host user login name}@{Host account username}@{Linux host IP address}@{Bastion host IP address} {Port}***. For example, you can run **ssh admin@10.10.10.10@10.10.10.101 2222** to log in to the target server.
- Method 3
  - In a newly opened blank session window, run a login command: ***{Protocol type} {User login name}@{System login IP address}*** **-p** ***{Port number}***, for example, **ssh admin@10.10.10.10 -p 2222**. After the login, select the target server.
  - In a newly opened blank session window, run a login command: ***{Protocol type} {Bastion host user login name}@{Host account username}@{Linux host IP address}@{Bastion host IP address}*** **-p** ***{Port}***. For example, you can run **ssh admin@10.10.10.10@10.10.10.101 -p 2222** to log in to the target server.

NOTE

system login IP address indicates the private IP address or EIP of your bastion host. Make sure the network connection between the local PC and the IP address is normal.



Step 3 Authenticate user identities.

Enter your identity credentials as prompted.

- If an SSH client is used, passwords, SMS messages, mobile OTPs, and OTP tokens can be used for login identity authentication. To enable **SMS**, **Mobile**

OTP, or **OTP token** authentication, you need to configure multi-factor authentication. For details, see **Configuring Multifactor Verification**.

- To configure an automatic logout timeout for inactive users and a verification-free duration for repeated SSH client logins, see **Configuring Client Login**.

Table 4-4 SSH client login authentication

Login Type	Login Description	Configuration Description
Password	Enter the username and password of your bastion host account.	Default login method. The login passwords in the **AD**, **RADIUS**, **LDAP**, or **Azure AD** authentication are the passwords of users on the remote server. For details, see **Remote Authentication Management**.
SSH Pubkey	Enter the private key and private key password for login authentication. After the login authentication is successful, next time the user can log in to the system over the SSH client without entering the password.	You need to generate a public and private key pair for login verification and add the SSH public key to the CBH system in the **Profile** center. For details, see **Adding an SSH Public Key**.
SMS	In **SMS** authentication, enter the **Password** or **SSH Pubkey** and the SMS verification code you will receive to complete the login authentication.	An available phone number has been configured for the account.
Mobile OTP	In **Mobile OTP** authentication, enter the **Password** or **SSH Pubkey** and the OTP token to complete the login authentication. **NOTE** Ensure that the CBH system time is the same as the mobile phone time (accurate to the second). Otherwise, a message indicating that the verification code is incorrect will be reported.	Bind your account to a mobile OTP and contact the administrator to configure multi-factor authentication. Otherwise, you cannot log in to the system. For details, see **Configuring Mobile OTP Login Verification**.
OTP token	After the **Password** or **SSH Pubkey** login is authenticated, select **OTP token** and enter the verification code.	A dynamic token must be issued to the user. For details, see **OTP Token Management**.

Step 4 After logging in to your bastion host, you can view system information and start O&M operations.

NOTE

You can also use APIs to log in to resources managed by a bastion host. To do so, you need to obtain the specific URL.

----End

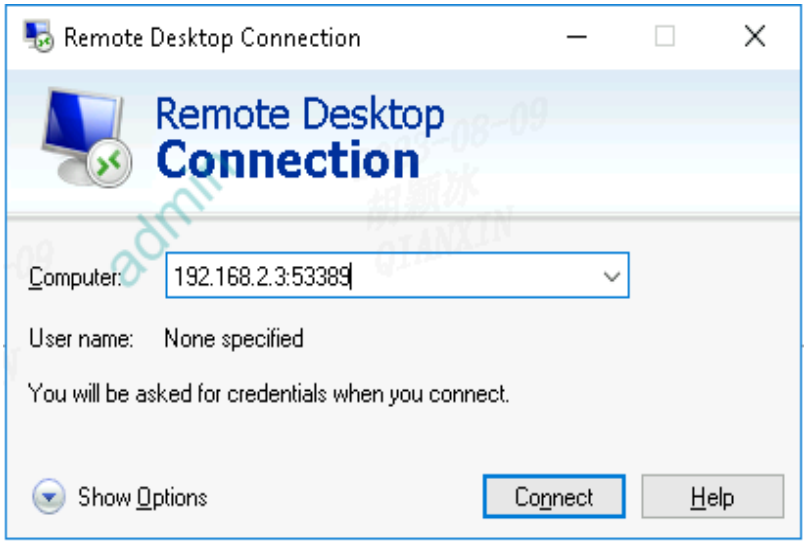
Using an MSTSC Client to Log In to Your Bastion Host

You can use a Microsoft Terminal Services Client (MSTSC) client to log in authorized resources over your bastion host.

Step 1 Open the MSTSC dialog box.

Step 2 In the displayed dialog box, enter your bastion host information in the **Computer** text box in the format of *Bastion host IP address*: **53389**.

Figure 4-1 Configuring the computer



Step 3 Click **Connect** and provide the following information to complete the login:

- Username: Enter *Login name of the bastion host user@Windows host resource account@Windows host resource IP address:Windows remote port* (3389 by default), for example, admin@Administrator@192.168.1.1:3389.

  NOTE

  The *Windows host resource account* must be a resource account that has been added to CBH and the login mode must be automatic login, or the resource account cannot be identified and O&M audit files cannot be generated. Real-time session O&M is not supported. For details, see **Creating a Resource Account and Associating It with the Corresponding Resource**.

- **Password**: Enter the password of the current bastion host user.

----End

5 User and Resource Account

5.1 Overview of Login Users, Roles, and Resource Accounts

You can manage instances by login users, roles, and resource account types to support your needs for different scenarios.

Login Users

You can centrally manage all system users. A system user you create for a bastion host is an account you can use for logging in to the bastion host.

The system administrator **admin** is the first account for users to log in to a bastion host for the first time. The **admin** user has the highest operation permissions and such permissions cannot be deleted or changed.

- System operation permissions of different users vary depending on their roles.
- Resource operation permissions can be assigned to users by user group.

Only **admin** or users with permissions for the **User** module can manage system users, including creating users, batch importing and exporting users, resetting user accounts and passwords, moving users to another department, changing user roles, adding users to user groups, configuring user login permissions, enabling and disabling users, and batch managing users.

User Groups

A user group includes multiple users. You can authorize users in batches by authorizing the corresponding user group. For details, see **Creating an ACL Rule and Associating It with Users and Resource Accounts**.

Only system administrator **admin** or the users with the permissions for the **User** module can manage user groups, including creating a user group, maintaining members in the user group, managing user group information, and deleting the user group.

A user group is associated with a department and does not belong to an individual user. By default, a user group created by the current login user belongs

to the department of the user. The department cannot be changed. Users who have the user group permissions can only view the information about all the user groups of their departments and lower-level departments.

NOTE

- The administrator of a superior department can add a user in the superior department to a user group in a lower-level department.
- If you have the permissions for the **User** module, you can view user group details. However, for the user groups in the superior department, you can view only the user list of the user group.
- If you have the permissions for the **User** module, you can remove a user of a superior department out of a user group. However, as a user in a lower-level department, you have no permissions to add those removed users back to the user group.
- A user can be added to multiple user groups.

User Roles

There are some preconfigured roles in CBH. You can use these roles to allocate permissions to view and use different module in a CBH system.

In a bastion host, only **admin** has the permission to customize roles and modify permissions for roles.

After a user is created, you can associate a role with the user to implement access control. A user can be associated with only one role.

By default, each instance has the following default roles: the department manager, policy manager, audit manager, and operation user. The default roles cannot be deleted, but their permissions can be modified.

You can also customize roles to configure the permission scope. However, only the **admin** user has the permission to create custom roles and edit the permission scope of default roles.

Table 5-1 Default roles

Parameter	Description
DepartmentManager	This role is the department operation manager and manages the bastion host system. This role has the configuration permissions for all other modules except **User** and **Role** modules.
PolicyManager	Specifies the user permission policy administrator. This role manages host operation permissions. It has the permissions for configuration of the user management, resource group management, and access policy management modules.
AuditManager	Specifies the O&M result audit administrator. This role queries and manages system audit data. This role has the configuration permissions for real-time session, historical session, and system logs modules.

Parameter	Description
User	This role specifies common users and operators who can access the system. This role has the permissions for O&M of resources, such as host and application resources, and service ticket authorization management.

Resource Accounts

A resource account is used to log in to resources managed in a bastion host instance. After logging in to a resource, you can perform operations.

A host or application resource may have multiple resource accounts configured. Each managed host or application account is considered as a resource account. You do not need to enter the username or password when you log in to a managed host using its managed resource accounts.

If no accounts are added for a host or application resource, the **Empty** account is generated by default. In this situation, when you log in to the host or application resource through your bastion host, a username and password is required.

Resource Account Groups

After you add multiple managed resource accounts to an account group, you can then authorize and authenticate accounts in batches by authorizing the corresponding account group.

Only system administrator **admin** or the user who has the account group management permission can manage account groups, including creating an account group, maintaining resources related to an account group, managing account group information, and deleting an account group.

An account group is associated with a department and does not belong to an individual. The account group created by the current login user belongs to the user's department by default. The department cannot be modified.

A user with the account group management permission can view information about all account groups of the same or lower-level departments.

NOTE

- The administrator of a superior department can add accounts of the superior department to the account group of a lower-level department. If you are a user in the lower-level department and have permissions for the **Account Group** module, you can view only the list but not the details of the accounts added from the superior department.
- You can also remove an account of superior department out of the account group. However, as a user in a low-level department, you have no permissions to add those removed accounts back to your current account group.
- A resource account can be added to multiple account groups.

5.2 Creating a Login User and Associating a Role with the User

A user in a CBH system represents a natural person who can log in to the CBH system. You can create users in your CBH system, batch import users from other platforms into your CBH system, and synchronize users from an Active Directory (AD) server to your CBH system. All those users then can log in to your CBH system.

The **admin** user has the highest permissions for the corresponding bastion host. It is also the first user who can log in to the bastion host. This means all other system users are created by user **admin**.

Constraints

To set **Department** to a superior department for a user, you must have management permissions for the **Department** module. For details about how to edit the role permissions of a user, see **Editing Role Information**.

Prerequisites

- You have obtained the permissions to create or import users on the **User** module.
- You have obtained the permissions to synchronize users from the AD domain server to the **System** module.

Creating a User

Step 1 Log in to your bastion host.

Step 2 In the navigation pane on the left, choose **User** > **User** to go to the user list page.

Step 3 In the upper right corner of the page, click **New**. In the displayed **New User** dialog box, complete required parameters.

Figure 5-1 New User

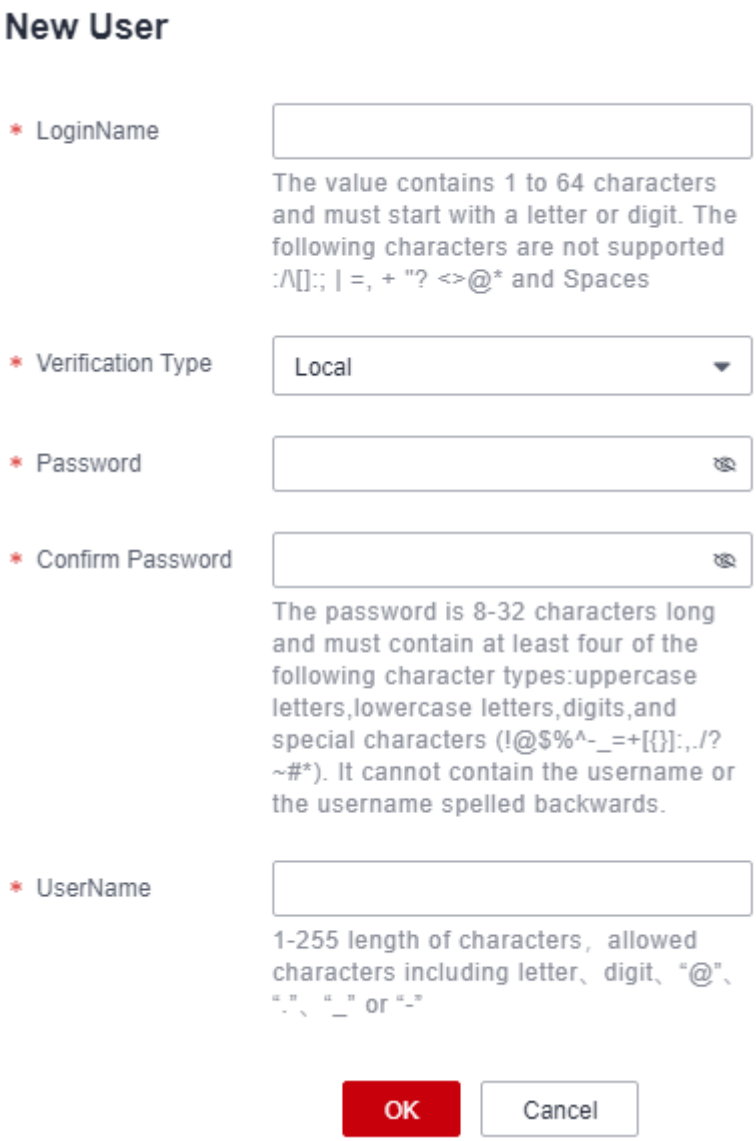


Table 5-2 Parameters for creating a user

Parameter	Description
LoginName	Specifies the username for logging in to the system. The **LoginName** must be unique in a system and cannot be changed once created.

Parameter	Description
Verification Type	Specifies how the user is verified for logging in to the bastion host. • **Local**: The user is verified against the account management system of the bastion host. This method is the default method. • **AD**: The user is verified against the Windows AD domain server. • **LDAP**: The user is verified against the third-party authentication server through the LDAP protocol. • **RADIUS**: The user is verified against the third-party authentication server through the RADIUS protocol. • **Azure AD**: The user is verified against the Azure platform based on Security Assertion Markup Language (SAML) configuration. **NOTE** If you want to verify the user against a remote AD domain, LDAP, or RADIUS servers or verify the user against the Azure AD service, configure the remote authentication server in the bastion host. For details, see **Authentication Configuration**.
Domain name	This parameter is mandatory if you select **Azure AD** for **Verification Type**. Provide the suffix you registered with the Azure platform.
Password/ Confirm Password	A password must be configured for the user to log in to the bastion host if you select **Local** for **Verification Type**.
UserName	Specifies the user-defined user name. This name indicates the name of the person who uses the account so that system users can be distinguished from each other.
Mobile	Specifies the mobile number of the user. This number is used for SMS authentication logins and password resetting.
Email	Specifies the email address of the user. The bastion host sends notifications to this email address.

Parameter	Description
Role	Specifies the role to be assigned to the user. Only one role can be assigned. By default, system roles include **DepartmentManager**, **PolicyManager**, **AuditManager**, and **User**. • **DepartmentManager**: responsible for managing departments. Except the **User** and **Role** modules, this role has the configuration permissions for all other modules. • **PolicyManager**: responsible for configuring policy permissions. This role has the configuration permissions for the **User Group**, **Account Group**, and **ACL Rules** modules. • **AuditManager**: responsible for auditing system and maintenance data. This role has the configuration permission for **Live Session**, **History Session**, and **System Log** modules. • **User**: common system users and resource operators. This role has the permissions for the **Host Operations**, **App Operations**, and **Ticket approval** modules. • User-defined role: Only the **admin** user can customize a new role or edit permissions of a default role.
Department Name	Specifies the department to which the user belongs. For details about how to create a department, see **Creating a Department**.
Remarks	(Optional) Provides supplementary information about the user.

Step 4 Click **OK**. You can then view the new system user on the user list page.

----End

Batch Importing Users

Step 1 Log in to your bastion host.

Step 2 In the navigation pane on the left, choose **User** > **User** to go to the user list page.

Step 3 Click  in the upper right corner.

Step 4 Click **Download** next to **Download template**.

Step 5 Enter the information of users according to the configuration requirements in the template.

Table 5-3 Template parameters

Parameter	Description
LoginName	(Mandatory) Specifies the username for the user to log in to the bastion host.

Parameter	Description
Verification Type	(Mandatory) Specifies the authentication method. Only one authentication method can be entered. You can select **Local**, **RADIUS**, **AD Domain**, **LDAP**, **Azure AD**, or **IAM**.
Password	(Mandatory) Specifies the user-defined login password. This parameter is required when **Verification Type** is set to **Local**.
Authentication server/ Domain name	(Mandatory) Specifies the authentication server. This parameter is required if **Verification Type** is set to **AD**, **LDAP**, or **Azure AD**. Note that the value must be entered in required format. • For AD domain authentication, the value must be in the format of *IP:PORT*, for example, *10.10.10.10:389*. • For LDAP authentication, the value must be in the format of *IP:'PORT/ou=test,dc=test,dc=com'*, for example, *10.10.10.10:'389/ou=test,dc=com'*. • For Azure AD authentication, provide the domain name.
UserName	Enter the name of a system user.
Mobile	Enter the mobile number of a system user.
Email	Enter the email address of the system user.
Role	(Mandatory) Enter the system role of the user. • Only one role type can be entered. • There are four default roles for your choice: **DepartmentManager**, **PolicyManager**, **AuditManager**, and **User**. • Only the **role** that has been created in the system can be entered.
Department Name	(Mandatory) Enter the department to which the user belongs. The department structure must be complete. • Only one department structure can be entered, and a user can belong to only one department. • By default, the department can be set to **HQ**. Use a comma (,) to separate a department and its lower-level department. • Only the **department** that has been created in the system can be entered.
Remarks	Provides supplementary information about the user account.
User Groups	Specifies the user group that a user belongs to. • A user account can belong to multiple user groups in the same department. Use a comma (,) to separate every two user groups. • Only the **user group** that has been created in the system can be entered.

Step 6 Click **Upload** and select the completed template file.

Step 7 (Optional) Select **Override existing user**.

- Selected: If an existing user account and the user account being imported have the same **LoginName**, the existing one will be overwritten. The user account information in the bastion host is updated accordingly.
- Deselected: If an existing user account and the user account being imported have the same **LoginName**, the existing one will be skipped and kept unchanged.

Step 8 Click **OK**. You can then view the new system user on the user list page.

----End

Synchronizing AD Domain Users

You can configure **Sync Mode** for the AD authentication to let the system synchronize existing user information on the AD domain server to your bastion host. When a user logs in to the bastion host, the AD domain server provides the identity authentication service.

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Authenticate**.

Step 3 Click **Add** in the **AD Settings** area.

Step 4 Set the AD domain authentication **Mode** to **Sync Mode**.

Table 5-4 AD settings for synchronizing users

Parameter	Description
Server	Specifies the IP address of the AD domain server.
Status	Specifies whether to enable AD domain remote authentication. AD domain remote authentication is enabled by default. • Enabled: AD domain authentication is enabled. If the configuration information is valid, AD domain authentication is enabled or AD domain users are synchronized to the bastion host when the user performs a login. • Disabled: AD domain authentication is disabled.
SSL	Specifies whether to enable SSL encryption. SSL encryption is disabled by default. • Disabled: SSL encryption is disabled. • After SSL encryption is enabled, data transmitted by synchronized users or authenticated users is encrypted.
Mode	Specifies the working mode of AD domain. Select **Sync Mode**.
Port	Specifies the access port of the remote server of AD domain. The default port number is 389.

Parameter	Description
LoginName	Specifies the username of the account for logging in to the AD domain server.
Password	Specifies the password of the account for logging in to the AD domain server.
Domain	Specifies the domain of the AD service.
Base DN	Specifies the base DN for the remote AD domain server.
Dept Filter	Specifies the departments to be filtered out for the remote AD domain server.
User Filter	Specifies the users to be filtered out for the remote AD domain server.
Login Name Filter	Specifies the login name to be filtered out. Separate multiple login names with vertical bars (|).
UserName	Specifies the attribute name of user names on the remote AD domain server, for example, name.
Email	Specifies the attribute name of the user mailbox on the AD domain remote server, for example, mail.
Mobile	Specifies the attribute name of user's mobile phone on the AD domain remote server, for example, mobile.
Sync	Specifies the AD user synchronization method. The options include **Manual** and **Auto**. • **Manual**: After you complete required configurations, manually synchronize the user information from the AD server. • **Auto**: After you complete required configurations, user information is automatically synchronized. You are also required to configure **Start time of sync**, **Duration**, and **End time** for auto synchronization.
Department	Specifies the department to which the synchronized user account belongs.
Options	• **Override existing** – Selected: If an existing user account and the user account being imported have the same **LoginName**, the existing one will be overwritten. The user account information in the bastion host is updated accordingly. – Deselected: If an existing user account and the user account being imported have the same **LoginName**, the existing one will be skipped and kept unchanged. • **Sync user status**: If you select this, the current user status will be synchronized to the bastion host. This option is recommended.

Step 5 (Optional) If you want to synchronize users from the AD domain server, click **Next** to obtain the source department structure of the AD domain server.

- **Sync All Users** is enabled by default.
- If you select a superior department of the user source, all users in the lower-level department are included in the source.
- **Create new dept** is disabled by default. You can enable it to let system create departments based on the department structure in the AD domain and synchronize users from the AD domain departments.

Step 6 Click **OK**. You can then view AD authentication configurations in the AD server list.

Step 7 In the **AD Settings** area, locate the AD server row. In the **Operation** column, click **Start** to synchronize AD domain users to a bastion host. You can view the synchronized user information in the user list.

----End

5.3 User Management

5.3.1 Managing Basic User Information

When there are a large number of users in a bastion host, the quick search and advanced search modes are available for you.

You can query, view, and edit user information, including basic user and user group information, login restrictions, authorized resource accounts, multifactor verification methods, and the validity period of user accounts.

Prerequisites

You have the operation permissions for the **User** module.

Viewing and Editing User Information

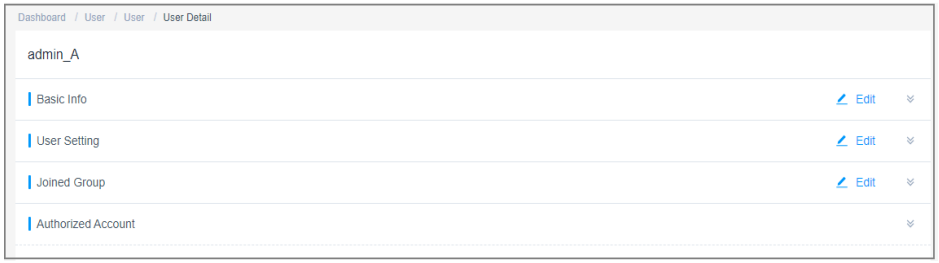
Step 1 Log in to your bastion host.

Step 2 Choose **User >User**. The user list page is displayed. You can query a user using the quick search or advanced search function.

- Quick search: Enter a keyword in the search box and search for a user by login name or username.
- Advanced search: Click **Advanced** next to text box and enter keywords in the corresponding attribute search boxes to search for users.

Step 3 In the user list, click the login name of the target user or click **Manage**. On the user details page, view the basic information in the **Basic Info** area and view the resource authorization information in the **Authorized Account** area.

Figure 5-2 User details



----End

Batch Editing User Information

Step 1 Log in to your bastion host.

Step 2 Choose **User >User**. The user list page is displayed. You can query a user using the quick search or advanced search function.

- Quick search: Enter a keyword in the search box and search for a user by login name or username.
- Advanced search: Click **Advanced** next to text box and enter keywords in the corresponding attribute search boxes to search for users.

Step 3 In the user list, select the target login user.

- In the lower left corner, choose **More** > **Delete NetDisk Data**. In the dialog box displayed, confirm the deletion information and click **OK**.
- In the lower left corner, choose **More** > **Edit Dept**. In the dialog box displayed, select the target department and click **OK**.
- In the lower left corner, choose **More** > **Edit Role**. In the dialog box displayed, select target roles and click **OK**.

----End

5.3.2 Adding Users to a User Group

You can add one or more users to a user group. Then you can authorize users by user group. A user can be added to multiple user groups.

Constraints

- The administrator of a superior department can add a user in the superior department to a user group in a lower-level department.
- If you have the permissions for the **User** module, you can remove a user of a superior department out of a user group. However, as a user in a lower-level department, you have no permissions to add those removed users back to the user group.

Prerequisites

You have the operation permissions for the **User** module.

Adding a User to a User Group

Step 1 Log in to your bastion host.

Step 2 Choose **User >User**. The user list page is displayed. You can query a user using the quick search or advanced search function.

- Quick search: Enter a keyword in the search box and search for a user by login name or username.
- Advanced search: Click **Advanced** next to text box and enter keywords in the corresponding attribute search boxes to search for users.

Step 3 In the **Operation** column of the user you want, click **Join**.

Step 4 In the displayed **Edit UserGroup** dialog box, select one or more user groups and add the user to selected user groups.

Step 5 Click **OK**. Go to the user details page, click the login name of the target user. In the **Joined Group** area, view the user groups the user has been added to.

NOTE

For details about how to batch add users to a user group, see **Editing the Members of a User Group**.

----End

5.3.3 Enabling or Disabling a User

You can batch **Enable** or **Disable** other users and change the user account status in just a few clicks.

The system administrator **admin** is **Enabled** by default and cannot be disabled.

- Enable

  The default user status is **Enabled**. Enabled users can use the bastion host within the permission scope.
- Disable

  The user account status is changed to **Disabled**. Disabled users cannot log in to the bastion host. A logged-in user will be forcibly logged out when the mapped user account is disabled.

Prerequisites

You have the operation permissions for the **User** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **User >User**. The user list page is displayed. You can query a user using the quick search or advanced search function.

- Quick search: Enter a keyword in the search box and search for a user by login name or username.
- Advanced search: Click **Advanced** next to text box and enter keywords in the corresponding attribute search boxes to search for users.

Step 3 Select the users whose status you want to change and click **Enable** or **Disable** in the lower left corner. This operation takes effect immediately.

----End

5.3.4 Deleting a User

You can delete users one by one or in batches from a bastion host.

The system administrator **admin** cannot be deleted.

NOTE

- A logged-in user will be logged out forcibly immediately after the account deletion. Exercise caution when performing this operation.
- If a user account is deleted, all permissions associated with the user account become invalid, and files in the user's personal net disk are cleared and cannot be restored. So, ensure that related data has been backed up before deleting the user account.

Prerequisites

You have the operation permissions for the **User** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **User >User**. The user list page is displayed. You can query a user using the quick search or advanced search function.

- Quick search: Enter a keyword in the search box and search for a user by login name or username.
- Advanced search: Click **Advanced** next to text box and enter keywords in the corresponding attribute search boxes to search for users.

Step 3 To delete one user, click **Delete** in the **Operation** column of the user.

Step 4 To delete multiple users at a time, select the ones you want to delete and click **Delete** at the bottom of the user list.

----End

5.3.5 Configuring User Login Restrictions

Overview

To effectively reduce security risks caused by user account leakage, you can enable or disable multifactor verification, set the account validity period, and configure login limit by time range, IP address, and MAC address.

- Multifactor verification: authenticates user login by SMS, OTP token, or USB key as well as password.
- Period of validity: determines the validity period of a user account for logging in to a bastion host.
- Login limit by time: allows or forbids a user account to log in to a bastion host at the specified duration.

- Login limit by IP address: allows or forbids only users from specified IP addresses to log in to a bastion host.
- Login limit by MAC address: allows or forbids only users with specified MAC addresses on a LAN to log in to a bastion host.

Constraints

- To use the **Mobile OTP** authentication, ensure that the system time and the mobile phone system time are synchronized, accurate to the seconds. Otherwise, the mobile OTP authentication will fail.
- The built-in SMS gateway has restrictions on the frequency and number of SMS messages that can be sent. To avoid these restrictions, use a third-party SMS gateway. For more details, see **Configuring SMS Message Outgoing**.
- MAC addresses belong to the data link layer and are used for LAN addressing. The parameter **MAC Limit** takes effect only on the LAN.
- If multifactor verification is configured for the **admin** user, the first time login will fail. Submit a service ticket for technical support to deselect all multifactor verification options.

Prerequisites

- You have the operation permissions for the **User** module.
- To enable **Mobile OTP** in multifactor verification, **bind a mobile OTP** to the user account in **Profile**. Otherwise, the user account cannot be used to log in to the system.

Configuring Login Restrictions for a User

Step 1 Log in to your bastion host.

Step 2 Choose **User >User**. The user list page is displayed. You can query a user using the quick search or advanced search function.

- Quick search: Enter a keyword in the search box and search for a user by login name or username.
- Advanced search: Click **Advanced** next to text box and enter keywords in the corresponding attribute search boxes to search for users.

Step 3 Click the login name of the user whose information you want to change, or click **Manage** in the row of the user in the **Operation** column.

Step 4 Click **Edit** in the **User Setting** area.

Table 5-5 User login limit parameters

Parameter	Description
Multifactor Verification	Specifies the authentication methods for users to log in to the bastion host. The options are **Mobile SMS**, **Mobile OTP**, **USBKey**, and **OTP token**. • By default, all options are deselected. If no options are selected, only the local password is used for identity authentication. • **Mobile SMS**: Mobile SMS can be enabled in multifactor verification only after a mobile number is bound to the user account for receiving SMS messages. • **Mobile OTP**: To make the mobile OTP authentication take effect, **bind a mobile OTP** to the user account in **Profile** first. • **USBKey**: To make the USBKey multifactor verification take effect, relate the user account to an issued USB Key. For details, see **Issuing a USB Key**. • **OTP token**: To make the OTP token authentication take effect, relate the user account to an OTP token. For details, see **Issuing an OTP Token**.
IAM Login	If you enable this, you can directly log in to the bastion host from IAM.
Period of validity	Specifies the validity period of the user account.
Logon Time Limit	Specifies the allowed or forbidden login time range. The time limit is set by the day and the hour.
Edit IP limit	Specifies the IP address or IP address range to be blacklisted or whitelisted. • **Blacklist**: forbids all user logins from the specified IP address or IP address range. • **Whitelist**: allows only user logins from the specified IP address or IP address range. • **Blacklist-Multifactor Verification for within the List**: allows you to configure the IP address or IP address range for the blacklist. Users whose IP addresses or IP address ranges are in the blacklist are allowed to log in to the bastion host only when multifactor verification is configured for them. • **Blacklist-Multifactor Verification for beyond the List**: allows you to configure the IP address or IP address range for the whitelist. Users whose IP addresses or IP address ranges are not in the whitelist are allowed to log in to the bastion host only when multifactor verification is configured for them. • If no IP address is specified, there is no IP-based login limit.

Parameter	Description
MAC Limit	Specifies the MAC address or address range to be blacklisted or whitelisted. • **Blacklist**: forbids all users from configured MAC addresses to log in to the bastion host. • **Whitelist**: allows only users from configured MAC addresses to log in to the bastion host. • If no MAC address is specified, there is no login limit by MAC address.

Step 5 Click **OK**. You can view the user login configurations on the user details page.

----End

Configuring Login Restrictions for a Batch of Users

Step 1 Log in to your bastion host.

Step 2 Choose **User >User**. The user list page is displayed. You can query a user using the quick search or advanced search function.

- Quick search: Enter a keyword in the search box and search for a user by login name or username.
- Advanced search: Click **Advanced** next to text box and enter keywords in the corresponding attribute search boxes to search for users.

Step 3 Select the target login user accounts.

- Edit multifactor verification.
  a. In the lower left corner, choose **More** > **Edit multifactor**. In the dialog box displayed, select the verification methods as needed for the target user.
     - You can select multiple different verification methods.
     - You can also select **Modify All** to edit the multifactor verification settings for all users in the current department and its subordinate department.
  b. Confirm the information and click **OK**.
- Edit the validity period.
  a. In the lower left corner, choose **More** > **Edit validity period**. In the dialog box displayed, select the start and end time for the target user.
     - After the setting, the target account can log in to the bastion host only within the valid period.
     - You can set either the start time, or the end time, or both.
  b. Confirm the information and click **OK**.
- Edit the login time limit.
  a. In the lower left corner, choose **More** > **Edit time limit**. In the dialog box displayed, select the login period.

- Select the time when the target user can log in to the system by the hour.
- You can select **Permit** or **Forbid**, and then set the time duration.

b. Confirm the information and click **OK**.

- Edit IP address login limit.
  a. In the lower left corner, choose **More** > **Edit IP limit**. In the dialog box displayed, select the login IP address restriction type.

     You can select:

     - **Blacklist**: The entered addresses are not allowed to log in to the system.
     - **Whitelist**: Only entered addresses are allowed to log in to the system.
     - **Blacklist-Multifactor Verification for within the list**: Users from the specified IP address or IP address range can log in to the system through multifactor verification only.
     - **Whitelist-Multifactor Verification for beyond the list**: Users not from the specified IP address or IP address ranges can log in to the system through multifactor verification only.

  b. Enter IP addresses in the text box.

     Enter multiple addresses with line breaks. Ensure that each line contains only one address or address range. The subnet mask is supported, for example, you can enter 192.168.1.10-192.168.1.100 or 192.168.1.10/24.

  c. Confirm the information and click **OK**.
- Edit the MAC address limit.
  a. In the lower left corner, choose **More** > **Edit MAC limit**. In the dialog box displayed, select the login MAC address restriction type.

     Select **Blacklist** or **Whitelist**.

  b. Enter MAC addresses in the text box.

     If there are multiple addresses, enter them in different lines. Make sure each line contains only one address.

  c. Confirm the information and click **OK**.

----End

5.3.6 Resetting a User Login Password

Forgotten, lost, or expired passwords may cause login security accidents. To reduce password login risks, you can change user login passwords in batches.

Constraints

- You are not allowed to change the password of system administrator **admin**. It can only be changed in the **Profile** module as user **admin**.
- If your password is changed by batch resetting, change the password when the first time you log in to the bastion host after password resetting. This is

because the same password is generated for all selected users during password batch resetting.

- After you log in to a bastion host, only the passwords of other users can be batch reset.
- Plaintext passwords cannot be viewed or exported.
- For users with remote authentication enabled, their passwords can be changed only on the remote authentication server.

Prerequisites

You have the operation permissions for the **User** module.

Procedure

Step 1 Log in to your bastion host.

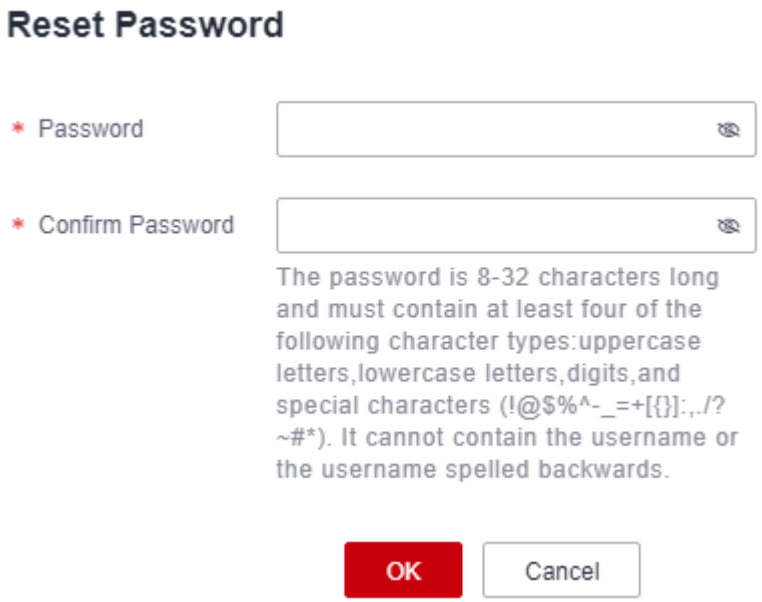
Step 2 Choose **User >User**. The user list page is displayed. You can query a user using the quick search or advanced search function.

- Quick search: Enter a keyword in the search box and search for a user by login name or username.
- Advanced search: Click **Advanced** next to text box and enter keywords in the corresponding attribute search boxes to search for users.

Step 3 Select the target login user and choose **More** > **Reset Password** in the lower left corner.

Step 4 In the dialog box displayed, enter a new password.

Figure 5-3 Reset Password



Step 5 Confirm the information and click **OK**.

Be sure that involved users are notified of new passwords in a timely manner.

----End

5.3.7 Exporting User Information

You can export user information in batches so that you can have a local backup and edit basic user information easily.

Constraints

- You can export user information about login name, authentication method, authentication server, username, mobile number, email address, role, department, and user group.
- To ensure user account security, passwords cannot be exported.

Prerequisites

You have the operation permissions for the **User** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **User >User**. The user list page is displayed. You can query a user using the quick search or advanced search function.

- Quick search: Enter a keyword in the search box and search for a user by login name or username.
- Advanced search: Click **Advanced** next to text box and enter keywords in the corresponding attribute search boxes to search for users.

Step 3 Select users you want to export. If no users are selected, all users will be exported by default.

Step 4 Click  in the upper right corner. Confirm the export in the displayed dialog box.

- Set an encryption password to encrypt the exported file.
- Enter your password.

  When you use an IAM, SAML, or Azure AD account to log in to a bastion host, if the system displays a message indicating that the local password is not set, set the local password in the **Profile** center or contact the administrator. For details, see **Changing Your Password/Setting a Local Password**.
- Select the CSV or Excel format.

Step 5 Click **OK**. After the task is created, click **Go to Download Center**. If the export progress reaches 100%, click **Download** in the **Operation** column. Then you can view the exported user accounts in the downloaded file.

----End

5.4 User Role Management

5.4.1 Creating a User Role

In a bastion host, default roles include **DepartmentManager**, **PolicyManager**, **AuditManager**, and **User**. This topic walks you through how to create a custom role.

Constraints

- Only system administrator **admin** can create a system role.
- To obtain permissions for the user group and account group modules, configure the **User** and **Account** modules.

Creating a Role

Step 1 Log in to your bastion host.

Step 2 In the navigation pane on the left, choose **User** > **Role** to go to the role list page.

Step 3 On the displayed page, click **New** in the upper right corner of the page. In the displayed **New Role** dialog box, complete required parameters

Table 5-6 Parameters for creating a role

Parameter	Description
Role	Specifies the role name. The value of **Role** must be unique in a bastion host and cannot be changed after it is created.
Managing Permission	Specifies whether to enable permission management for the role. Users assigned with management permissions can select a superior department when they create a resource or user. • **Enable**: The role has the management permissions and users with this role granted can view the data of their departments and lower-level departments. • **Disable**: The role has no management permissions.
Remarks	(Optional) Provides supplementary information about the role.

Step 4 Click **Next**. In the displayed dialog box, configure system module permissions for the role.

- Select a system module and specific actions: the role has permissions for the module and selected actions.
- Select only a system module: The role has only the permission to view the module.

Step 5 Click **OK**. You can then view the created role in the role list.

----End

5.4.2 Deleting a Role

This topic describes how to delete a role.

Constraints

- Only system administrator **admin** can delete a system role.
- Default system roles cannot be deleted.

Procedure

Step 1 Log in to your bastion host.

Step 2 In the navigation pane on the left, choose **User** > **Role** to go to the role list page.

Step 3 To delete a single role, click **Delete** in the **Operation** column.

Step 4 To delete multiple roles at a time, select the ones you want to delete and click **Delete** at the bottom of the role list.

----End

5.4.3 Querying and Editing Role Information

You can log in to your bastion host as user **admin** to view or role change details, including basic role information, role permissions, and module information.

Constraints

- Only system administrator **admin** can view and edit a system role.
- Management permissions of a default system role cannot be edited.
- If you change the permissions of a system default role, you can restore default permissions in just a few clicks.

Procedure

Step 1 Log in to your bastion host.

Step 2 In the navigation pane on the left, choose **User** > **Role** to go to the role list page.

Step 3 Query a role.

Enter a keyword in the search box and search for a role by name.

Step 4 Click the name of a desired role and click **Manage** in the **Operation** column.

Step 5 In the **Basic Info** area, view the detailed information about the role.

Click **Edit** and modify the basic information.

Step 6 In the **Permissions** area, view the system operation permissions of the role.

- Click **Edit**. In the displayed dialog box, modify the system operation permissions of the role.
- Click **Remove** of a module to revoke permissions for the module of the role.

----End

5.5 User Group Management

5.5.1 Creating a User Group

This section describes how to create a user group.

Prerequisites

You have the operation permissions for the **User** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 In the navigation pane on the left, choose **User** > **User Group** to go to the user group list page.

Step 3 Click **New**. In the **New UserGroup** dialog box displayed, configure basic information about the group.

Table 5-7 Creating a User Group

Parameter	Description
User Groups	Specifies user-defined user group name, which must be unique in a bastion host.
Remarks	(Optional) Provides supplementary information about the user group.

Step 4 Enter a user group name and descriptions in the **Group** and **Remarks** fields, respectively. The user group name in a bastion host must be unique.

Step 5 Click **OK**. You can then view the newly created user group in the user group list and add members to it. For details, see **Adding Users to a User Group**.

----End

5.5.2 Deleting a User Group

You can delete user groups from a bastion host. After a user group is deleted, the resource permissions the group members have been granted through the user group become invalid.

Prerequisites

You have the operation permissions for the **User** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **User** > **User Group** in the navigation pane.

Step 3 To delete a single user group, click **Delete** in the **Operation** column of the user group.

Step 4 To delete multiple user groups at a time, select the ones you want and click **Delete** at the bottom of the user group list.

----End

5.5.3 Querying and Editing User Group Information

You can view and edit basic information and members of a user group.

Constraints

- If you have the permissions for the **User** module, you can view user group details. However, for the user groups in the superior department, you can view only the user list of the user group.
- If you have the permissions for the **User** module, you can remove a user of a superior department out of a user group. However, as a user in a lower-level department, you have no permissions to add those removed users back to the user group.

Prerequisites

You have the operation permissions for the **User** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **User** > **User Group** in the navigation pane.

Step 3 Query a user group.

Enter a keyword in the search box and search for a user group by name.

Step 4 Click the name of the user group you want to edit or click **Manage** in the row of the user group in the **Operation** column.

Step 5 In the **Basic Info** area, view the detailed information about the user group.

Click **Edit** in the area to modify the name and remarks of the user group.

Step 6 In the **Members** area, view information about all members in the user group.

- Click **View** to go to the details page.
- In the row of a specific member, click **Remove** in the **Operation** column to remove the user from the user group.

----End

5.5.4 Editing the Members of a User Group

This section describes how to add members to or remove members from a user group.

Constraints

- If you have the permissions for the **User** module, you can view user group details. However, for the user groups in the superior department, you can view only the user list of the user group.
- If you have the permissions for the **User** module, you can remove a user of a superior department out of a user group. However, as a user in a lower-level department, you have no permissions to add those removed users back to the user group.

Prerequisites

You have the operation permissions for the **User** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **User** > **User Group** in the navigation pane.

Step 3 In the **Operation** column of the user group you want to edit, click **Member**.

Figure 5-4 Editing the members of a user group

Step 4 In the displayed dialog box, select **Add By User** or **Add By Department**.

Step 5 After selecting a user or department, click **OK**.

----End

5.6 Creating a Resource Account and Associating It with the Corresponding Resource

A host or application resource may have multiple accounts configured. Each account of a managed host or application resource is considered as a managed resource account. You do not need to enter the username or password when you log in to a managed host using its managed resource accounts.

If no accounts are added for a host or application resource, the **Empty** account is generated by default. In this situation, when you log in to the host or application resource through your bastion host, a username and password are required.

Constraints

- Automatic login accounts cannot be configured for Microsoft Edge application resources.
- If the AD domain service is installed on the managed resources, the account to be added is *Domain name*|*Host account username*, for example, *ad*|*administrator*.

Prerequisites

- You have the operation permissions for the **Account** module.
- You have added host or application resources.

Adding an Account for a Resource

Step 1 Log in to your bastion host.

Step 2 Choose **Resource** > **Account** in the navigation pane.

Step 3 Click **New**. In the dialog box displayed, configure resource account attributes.

Figure 5-5 New Account

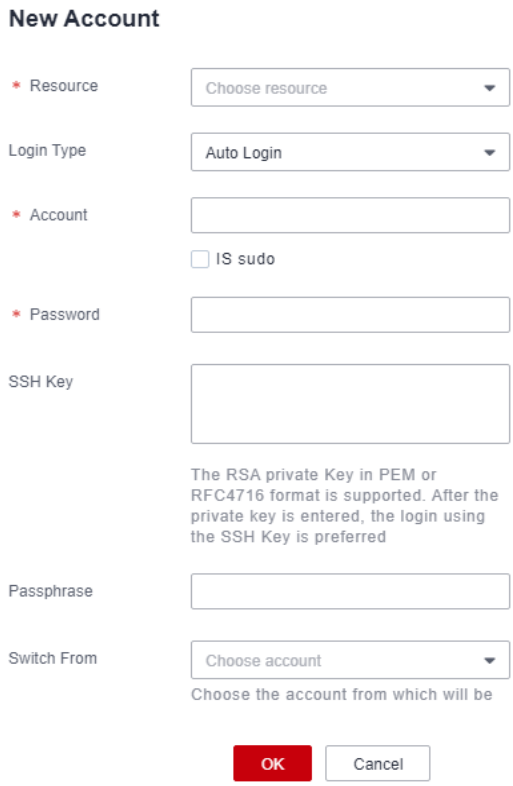


Table 5-8 Parameters for new managed resource accounts

Parameter	Description
Resource	Host or application resource to be related to the account.

Parameter	Description
Logon Type	Login method. You can select **Auto Login**, **Manual Login**, **Sudo Login**, or **CSMS Credentials Login**. • If you select **Auto Login**, **Account** and **Password** are mandatory. • If you select **Manual Login**, you can configure **Account**. • If you select **CSMS Credentials Login**, you can configure **CSMS Credentials** and **Remarks**. • If you select **Sudo Login**, a password is mandatory. • **Sudo Login** is valid only for SSH hosts. If **Sudo Login** is selected, **Switch From** and **Switch Command** are mandatory.
Accounts	Account name of the managed resource. The value of **Account** must be unique in a bastion host and cannot be changed after it is created. If you select **IS sudo**, the account is identified as a sudo account for managing resources and has the password change permission.
Password	Password of the account being added By default, **Verify** is selected. After the account is added, the system automatically verifies the status of the account. • After the account is verified, the resource information is saved. • If the verification fails, modify the configuration as prompted. If the system prompts that the account verification times out, modify the resource configuration. If the system prompts that the account password is incorrect, return to the configuration window and change the account password.
SSH Key	Authentication method that can be configured for host resources using the SSH protocol. After the configuration, an SSH key is preferentially used to log in to a related host resource.
Passphrase	Private key corresponding to the SSH key configured for an SSH host.
CSMS Credentials	(This parameter is available only when login mode is CSMS credential login.) Select the CSMS credential to be managed.
Switch From	For an SSH host, select a configured account and set it to a sudo account.
Switch command	Switchover command for an SSH host, for example, **su root**.
Description	Brief description of the account.

Step 4 Click **OK**. The newly created account will be displayed in the account list.

----End

Batch Importing Accounts of Managed Resources into Your Bastion Host

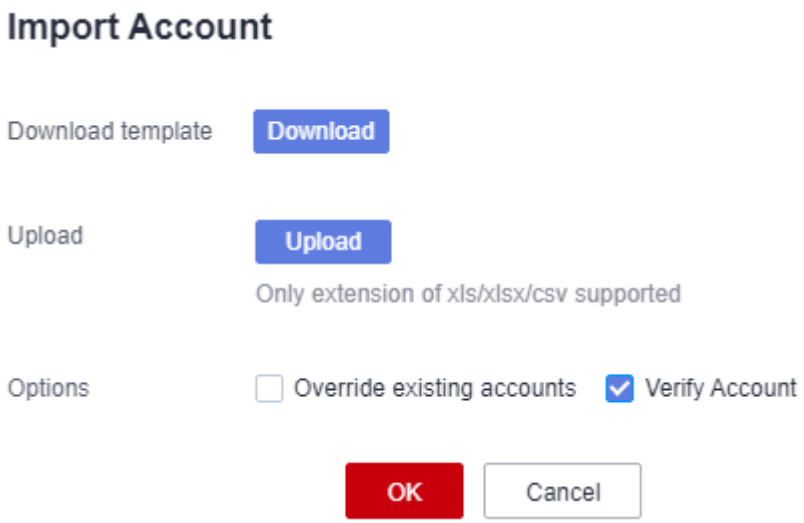
To import application server from a file, the file must be in .csv, .xls, or .xlsx format.

Step 1 Log in to your bastion host.

Step 2 Choose **Resource** > **Account** in the navigation pane.

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

Figure 5-6 Import Account



Step 4 Click **Download** to download the template if no template is available locally.

Step 5 Enter the information of accounts according to the configuration requirements in the template file.

Table 5-9 Template parameters

Parameter	Description
Account	(Mandatory) Enter the username of the managed resource account.
Logon Type	Method to log in to the resource. • This parameter can be set to **Auto Login**, **Manual Login**, or **Sudo Login**.
IS Sudo	Whether to set the account as a sudo account. • This parameter can be set to **Yes** or **No**.
Password	Password of the account for logging in to the resource.

Parameter	Description
SSH Key	Authentication method that can be configured for SSH hosts. After the configuration, an SSH key is preferentially used to log in to a related host resource. **NOTE** If the target resource account to be imported uses only the password for logins, leave this parameter empty.
Passphrase	Private key sequence mapped to the SSH key.
Oracle Param	This parameter is mandatory for Oracle hosts. • This parameter can be set to **SERVICE_NAME** or **SID**. • Separate multiple parameter values with commas (,).
SERVICE_NAME or SID	This parameter is mandatory for Oracle hosts. • Separate multiple parameter values with commas (,).
Login Role	This parameter is mandatory for Oracle hosts. • This parameter can be set to **normal**, **sysdba**, or **sysoper**. • Separate multiple parameter values with commas (,).
Database Name	This parameter is mandatory for the DB2 databases. • Select the database name or instance name. • Separate multiple parameter values with commas (,).
Instance Name	This parameter is mandatory for the DB2 databases. • Select the database name or instance name. • Separate multiple parameter values with commas (,).
Switch From	Sudo account of the host resource.
Switch command	The command to switch over between accounts.
AD Domain	For Radmin application resources, enter the AD domain address.
Description	Brief description of the managed resource account.
Resource	Enter the name of the resource that has been added to the host list or application list.
IP address/ domain name	For associated host resources, enter the IP address or domain name of the host resource.

Parameter	Description
Type	(Mandatory) Enter the protocol type of the host resource or the application type of the application resource. • Supported host protocols: SSH, RDP, Telnet, FTP, SFTP, VNC, DB2, MySQL, SQL Server, Oracle, SCP, PostgreSQL, and GaussDB. • Supported application types: Microsoft Internet Explorer, Mozilla Firefox for Windows, Google Chrome, VNC Client, SecBrowser, vSphere Client, Radmin, dbisql, MySQL Tool, SQL Server Tool, Oracle Tool, Rlogin, Mozilla Firefox for Linux, DM Tool, KingbaseES Tool, GBaseDataStudio for GBase8a, X11, and **Other**.
Port	This parameter is mandatory for host resources. Enter the IP address or domain name of the host resource.
Account Group	The account group to which the managed resource account belongs. • A managed resource account can belong to multiple account groups in the same department. Use a comma (,) to separate every two account groups. • Only the **account group** that has been created in the system can be entered.

Step 6 Click **Upload** and select the completed template.

Step 7 (Optional) Configure **Override existing accounts**, which is deselected by default.

- Selected: A managed resource account will be overwritten by the one being imported if both accounts have the same name.
- Deselected: A managed resource account will be skipped when the one being imported and the managed resource account have the same name.

Step 8 (Optional) Configure **Verify Account**, which is selected by default.

- Selected: The account status is verified when it is imported.
- Deselected, the account status will not be verified when it is imported.

Step 9 Click **OK**. The resource account list page is displayed. You can check the new account on the displayed page.

----End

Batch Creating Resource Accounts

You can create resource accounts for multiple hosts at the same time.

Step 1 Log in to your bastion host.

Step 2 Choose **Resource** > **Host** in the navigation pane on the left.

Step 3 Select the hosts for which you want to create accounts and choose **More** > **Add Account**.

NOTE

Only hosts with the same protocol type are supported.

Step 4 Enter the account information to be added, as shown in **Table 5-10**.

Table 5-10 Parameters for creating resource accounts in batches

Parameter	Description
Login Type	Select the login mode of the created accounts. • **Auto Login** • **Manual Login** • **CSMS Credentials Login** • **Sudo Login**
Account	Name of the account. You can specify one. If the login mode is set to automatic login, this parameter is mandatory.
Password	Password of the account.
SSH Key	This parameter is mandatory if the current account needs to log in to the system using an SSH key. The RSA private key in PEM or RFC4716 format is supported. After the RSA private key is entered, the SSH key is preferentially used for login.
passphrase	Password of the SSH key. You need to enter the SSH key first. If the SSH key is password-free, you do not need to set this parameter.
CSMS Credentials	This parameter is mandatory only when **Login Mode** is set to **CSMS Credentials Login**.
Description	Description of the current account. A maximum of 128 characters can be entered.
Options	Select an option. • **Overwrite existing account**: You can select this to overwrite the existing accounts that have the same usernames as that of accounts you are creating. • **Verify Account**: Check whether the added account can be used to log in to the system. This option can be selected only when the automatic login mode is used.

Step 5 Confirm the information and click **OK**.

----End

5.7 Resource Account Management

You can edit basic information of resource accounts, verify resource accounts, add resource accounts to resource account groups, and associate resource accounts with users. You can also delete and export resource accounts.

Constraints

- Accounts for application resources cannot be verified online.
- The administrator of a superior department can add an account in the superior department to an account group in a lower-level department.
- If you have permissions for the **Account Group** module, you can remove an account of superior department out of the account group. However, as a user in a low-level department, you have no permissions to add those removed accounts back to your current account group.
- A resource account can be added to multiple account groups.

Prerequisites

You have the operation permissions for the **Host**, **AppServer**, **Application**, and **Account** modules.

Viewing the Resource Account List

Step 1 Log in to your bastion host.

Step 2 Choose **Resource > Account**. On the displayed account list page, you can search for the target account through a quick search or an advanced search.

- Quick search: Select a search field and enter a keyword in the search box. You can select the following search fields: resource account, associated resource, host address, sudo account, SSH key account, or passphrase.
- Advanced search: Click **Advanced** next to text box and enter keywords in the corresponding attribute search boxes to search for resource accounts.

----End

Viewing and Editing Basic Information About a Resource Account

Step 1 In the resource account list, click the target resource account or click **Manage** in the **Operation** column. The resource account details page is displayed.

Step 2 In the **Basic Info** area, view the resource account information and click **Edit** on the right of the **Basic Info** area.

Step 3 In the displayed dialog box, modify the account information. For details about parameters, see **Table 5-8**.

Step 4 Confirm the information and click **OK**.

----End

Adding a Resource Account to an Account Group

You can add resource accounts to groups. Then you can manage resource accounts by group.

Method 1

Step 1 In the resource account list, click the target resource account or click **Manage** in the **Operation** column. The resource account details page is displayed.

Step 2 In the **Joined Group** area, view account groups the current resource account have been added to.

Step 3 Click **Edit** on the right of the **Joined Group** area. In the displayed dialog box, add the account to or remove the account from the group.

- Click the name of the target account group or **View** in the **Operation** column to view all information about the account group.
- Click **Remove** in the **Operation** column of the target account group to remove the current account from the group.

----End

Method 2

Step 1 On the **Account** page, locate the row containing the target account and click **Join** in the **Operation** column.

Step 2 In the displayed dialog box, add or remove the resource account to or from a group.

----End

Editing Authorized Users Associated with a Resource Account

After a user is associated with a resource account, the user can view the corresponding resources after log in to the system.

Step 1 In the resource account list, click the target resource account or click **Manage** in the **Operation** column. The resource account details page is displayed.

Step 2 In the **Authorized User** area, view associated users.

Step 3 Click a username to view the user details.

----End

Verifying Managed Resource Accounts

The status of a managed resource account is used to identify whether the password of the account is valid. The password cannot be manually changed and can only be updated through account verification.

The managed resource accounts can be manually verified when they are added or automatically verified based on preset schedule.

NOTE

Account verification is to verify connectivity by logging in to resources in the background. This process will not be recorded in history sessions.

Automatic verification

The system automatically verifies managed host accounts at 01:00 on the fifth, fifteenth, and twenty-fifth days of each month. After the verification is complete, the **admin** system administrator will receive a verification result message. No task will be generated. The message is displayed on the **Messages** page.

Real-time verification

Step 1 On the **Account** page, select the target account and click **Test and verify** below the account list.

Step 2 Configure **Connect Timeout** and **Done notification**.

- The default **Connect Timeout** interval is **10** seconds. If the network condition is poor, increase the **Connection Timeout** interval.
- By default, no task completion notifications will be sent.
- To receive notifications, select **Email**. Additionally, you can view the verification results on the **Tasks** page.

Step 3 Click **OK**. Refresh the **Account** page and view the verification results in the **Status** column.

To verify all resource accounts in an account group, see **Managing Resource Account Groups**.

Table 5-11 Resource account status description

Status	Description
Normal	If the system verifies that the username and password of the resource account are correct and can be used to log in to the managed resource, the account is in the **Normal** status.
Abnormal	If the account username or password is incorrect, the resource account cannot be used to log in to the system. The account is in the **Abnormal** status.
N/A	If a resource account is not verified after it is added, the account is in the **N/A** status.

----End

Exporting Resource Accounts

You can export resource information in batches from your bastion host so that you can have a local backup and edit basic resource information easily.

- To enhance information security of resources, you can encrypt resource information you export.

- The exported host resource file contains basic information, accounts, and plaintext passwords of managed hosts.
- The exported application server file contains basic information, path, account, and plaintext passwords of application servers.
- The exported application file contains basic information and account information, including plaintext passwords, of managed application resources.
- The exported account file contains basic account information, plaintext passwords, related resources, and related resource addresses.

Procedure

Step 1 On the **Account** page, select the accounts you want to export.

If no accounts are selected, information about all accounts is exported by default.

Step 2 Click  in the upper right corner. Confirm the export in the displayed dialog box.

- Set an encryption password to encrypt the exported file.
- Enter your password.

  When you use an IAM, SAML, or Azure AD account to log in to a bastion host, if the system displays a message indicating that the local password is not set, set the local password in the **Profile** center or contact the administrator. For details, see **Changing Your Password/Setting a Local Password**.
- Select the CSV or Excel format.

Step 3 Click **OK**. After the task is created, click **Go to Download Center**. If the export progress reaches 100%, click **Download** in the **Operation** column. Then you can view the exported account information in the downloaded file.

----End

Deleting One or More Resource Accounts

Step 1 On the resource account list page, locate the row where the target account resides and click **Delete** in the **Operation** column.

Step 2 In the dialog box displayed, confirm the information and click **OK**.

To batch delete resource accounts, select all target accounts and click **Delete** below the account list.

NOTE

- If a resource has only one account configured in your bastion host, the resource cannot be accessed through the bastion host once the account is deleted. Exercise caution when performing this operation.
- Before deleting a target resource account, make sure no tasks are in progress or operated on the corresponding resources. The deletion takes effect immediately, and the ongoing operations or sessions will be interrupted immediately. Exercise caution when performing this operation.

----End

5.8 Managing Resource Account Groups

After you add multiple managed resource accounts to an account group, you can then authorize and authenticate accounts in batches by authorizing the corresponding account group.

Only system administrator **admin** or the user who has the account group management permission can manage account groups, including creating an account group, maintaining resources related to an account group, managing account group information, and deleting an account group.

An account group is associated with a department and does not belong to an individual. The account group created by the current login user belongs to the user's department by default. The department cannot be modified. A user with the account group management permission can view information about all account groups of the same or lower-level departments.

NOTE

- The administrator of a superior department can add accounts of the superior department to the account group of a lower-level department. If you are a user in the lower-level department and have permissions for the **Account Group** module, you can view only the list but not the details of the accounts added from the superior department.
- You can also remove an account of superior department out of the account group. However, as a user in a low-level department, you have no permissions to add those removed accounts back to your current account group.
- A resource account can be added to multiple account groups.

Constraints

- As a system user who has permissions for the **Account** module, when you view account group, you can view accounts of your department and the superior department. However, for the accounts of the superior department, you can view only the account list but not the account details.
- If you have permissions for the **Account Group** module, you can remove an account of superior department out of the account group. However, as a user in a low-level department, you have no permissions to add those removed accounts back to your current account group.

Prerequisites

You have the operation permissions for the **Account** module.

Viewing the Resource Account Group List

Step 1 Log in to your bastion host.

Step 2 Choose **Resource > Account Group**. On the displayed account group list page, you can quickly search for the target resource account group.

Quick search: Select a search field and enter a keyword in the search box.

----End

Creating a Resource Account Group

Step 1 On the **Account Group** page, click **New** on the right. In the displayed **New Account Group** dialog box, configure basic information about the account group.

Table 5-12 Parameters for creating an account group

Parameter	Description
Account Group	The name you specify for the group. This name must be unique in a bastion host.
Remarks	(Optional) Provides supplementary information about the account group.

Step 2 Click **OK**. You can then view the newly created account group in the account group list and add account to it. For more details, see **Adding Accounts to an Account Group**.

----End

Editing Basic Information About a Resource Account Group

Step 1 On the **Account Group** page, click an account group name or click **Manage** in the **Operation** column to go to the account group details page.

Step 2 Click **Edit** on the right of the basic information area. In the dialog box displayed, edit the account group name and description.

Step 3 Confirm the information and click **OK**.

----End

Editing Resource Accounts in an Account Group

Method 1

Step 1 On the **Account Group** page, click an account group name or click **Manage** in the **Operation** column to go to the account group details page.

Step 2 Click **Add** on the right of the account group member area. In the displayed dialog box, select the account you want to add to the group.

You can search for the target resource account by resource account, associated resource, host address, or application address.

Step 3 Confirm the information and click **OK**.

Step 4 Click the name of the target resource account or **View** in the **Operation** column to view the detailed information about the resource account.

Step 5 Click the name of an associated resource to view the resource details.

Step 6 To remove a resource account from the current account group, locate the target account and click **Remove** in the **Operation** column.

----End

Method 2: **Adding resource accounts to an account group**

Step 1 In the account group list, locate the target account group and click **Add Account** in the **Operation** column.

Step 2 In the displayed dialog box, select the resource account to be added to the group.

You can search for the target resource account by resource account, associated resource, host address, or application address.

Step 3 Confirm the information and click **OK**.

----End

Removing a Resource Account from an Account Group

Method 1: Removing resource accounts from an account group by referring to method 1 in **Editing Resource Accounts in an Account Group**

Method 2

Step 1 In the account group list, click **Remove Account** in the **Operation** column of the target account group.

Step 2 In the displayed dialog box, select the resource account you want to remove from the group.

You can search for the target resource account by resource account, associated resource, host address, or application address.

Step 3 Confirm the information and Click **OK**.

----End

Batch Verifying Resource Accounts in an Account Group

You can verify managed resource accounts by account group in just a few clicks.

Step 1 On the **Account Group** page, select the target account group and click **Test and verify** below the account group list.

Step 2 Configure **Connect Timeout** and **Done notification**.

- The default **Connect Timeout** interval is **10** seconds. If the network condition is poor, increase the **Connection Timeout** interval.
- By default, no task completion notifications will be sent.
- To receive notifications, select **Email**. Additionally, you can view the verification results on the **Tasks** page.

Step 3 Click **OK**. Go to the **Account** page and view the verification results in the **Status** column.

----End

Deleting a Resource Account Group

Step 1 On the **Account Group** page, locate the row containing the target account and click **Delete** in the **Operation** column.

Step 2 In the dialog box displayed, confirm the information and click **OK**.

NOTE

After an account group is deleted, the resource accounts associated with the account group are removed from the group. Deleting an account group does not affect the original configurations of the resource accounts in the group.

----End

6 Resource

6.1 Resource Management Overview

A bastion host enables centralized resource management, making it easier for you to manage entire lifecycle of managed resources and their accounts in a more secure way. You can easily switch over between resource management and maintenance through single sign-on (SSO) without affecting business running on resources.

Resource Management Scenario

You can use a bastion host instance to manage hosts, applications, cloud servers (containers), and databases.

NOTE

- Host, database, and application resources can be batch imported and exported.
- Before managing application and container resources, you need to create a server on your bastion host instance to establish connections between the bastion host and managed resources. After doing this, you can add resources to the bastion host for centralized management.
- In addition to managing Huawei Cloud resources, CBH can also manage non-Huawei Cloud and on-premises resources by creating a proxy server as long as the protocol is supported by CBH.

Table 6-1 Types of resources a bastion host can manage

Resource Type	Management Method
Host resources	• Public network resources: You can create, import, and automatically discover public network resources on the bastion host instance for management. • Resources in different network environments or dedicated network environments: You can create a proxy server in the bastion host instance to manage resources. Currently, only SOCKS5 server proxies are supported.

Resource Type	Management Method
Application resources	You can create an application server in the bastion host instance to interconnect the application client with the bastion host instance, so that you can create and manage application resources with the bastion host instance.
Database resources	You can create, import, and automatically discover public network resources on the bastion host instance for management.
Container resources	You can create a Kubernetes server in your bastion host instance to establish connections between the Kubernetes worker nodes where the pods are running with the bastion host instance, so that you can create and manage container resources with the bastion host instance.

Types of Managed Resources

You can use a bastion host to manage a wide range of resource types, including Windows and Linux servers, Windows applications, databases, such as MySQL and Oracle, and Kubernetes servers. A host may map to multiple host resources. This means if you configure different protocols for the same host, the host resources are counted based on the protocols you configure for this host. This is similar to application resources. The following lists supported resource types:

- Host resources of the client-server architecture, including hosts configured with the Secure Shell (SSH), Remote Desktop Protocol (RDP), Virtual Network Computing (VNC), Telnet, File Transfer Protocol (FTP), SSH File Transfer Protocol (SFTP), DB2, MySQL, SQL Server, Oracle, Secure Copy Protocol (SCP), or Rlogin protocol.
- Application resources of the browser-server architecture or the client-server architecture, including more than 12 types of browser- and client-server architecture Windows applications, such as Microsoft Edge, Google Chrome, and Oracle tools.

Table 6-2 Types of resources a bastion host can manage

Resource Type	OS and Protocol Types Supported
Host resources	Supported protocols: SSH, RDP, VNC, Telnet, FTP, SFTP, SCP, and Rlogin Supported OS types: Linux, Windows, Cisco, Huawei, H3C, DPtech, Ruijie, Sugon, Digital China sm-s-g 10-600, Digital China sm-d-d 10-600, ZTE, ZTE5950-52tm, Surfilter, and ChangAn

Resource Type	OS and Protocol Types Supported
Application resources	• Supported Windows application types: MySQL Tool, Microsoft Edge, Mozilla Firefox for Windows, Oracle Tool, Google Chrome, VNC Client, SQL Server Tool, SecBrowser, vSphere Client, Radmin, dbisql, Navicat for MySQL, Navicat for PostgreSQL, Internet Explorer, and **Other**. • Supported Linux application types: DM Tool, KingbaseES Tool, Mozilla Firefox for Linux, and GBaseDataStudio for GBase8a.
Database resources	Supported protocols: GaussDB, PostgreSQL, DB2, MySQL, SQL Server, Oracle, and DM.
Container resources	Currently, only Kubernetes servers are supported.

6.2 Host or Database Resources

6.2.1 Managing Host or Database Resources with a Bastion Host

A bastion host can manage hosts through a wide range of protocols, such as SSH, RDP, VNC, Telnet, FTP, SFTP, DB2, MySQL, SQL Server, Oracle, Redis, SCP, and Rlogin, covering Windows hosts, Linux hosts, and databases.

This topic describes how to use a bastion host to centrally manage your host resources. We will introduce how to add a host resource, import host resources from a file, import host resources from a cloud platform, automatically discover host resources, and clone host resources.

Constraints

- The total number of host and application resources to be added cannot exceed the **number of assets**.
- The combination of **Protocol**, **Host Address**, and **Port** must be unique in a bastion host system. This means the host resources to be managed must be unique. Otherwise, when you create a host resource with the same configuration, an error message will be displayed, indicating that the host resource already exists.
- To set **Department** to a superior department for a host resource, you must have management permissions for the **Department** module. For details about how to edit the role permissions of a user, see **Editing Role Information**.

Prerequisites

You have the operation permissions for the **Host** module.

Adding a Host or Database Resource

Step 1 Log in to your bastion host.

Step 2 Choose **Resource** > **Host** in the navigation pane on the left.

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

Enter the required network information and basic information of the host resource you want to add.

Figure 6-1 New Host

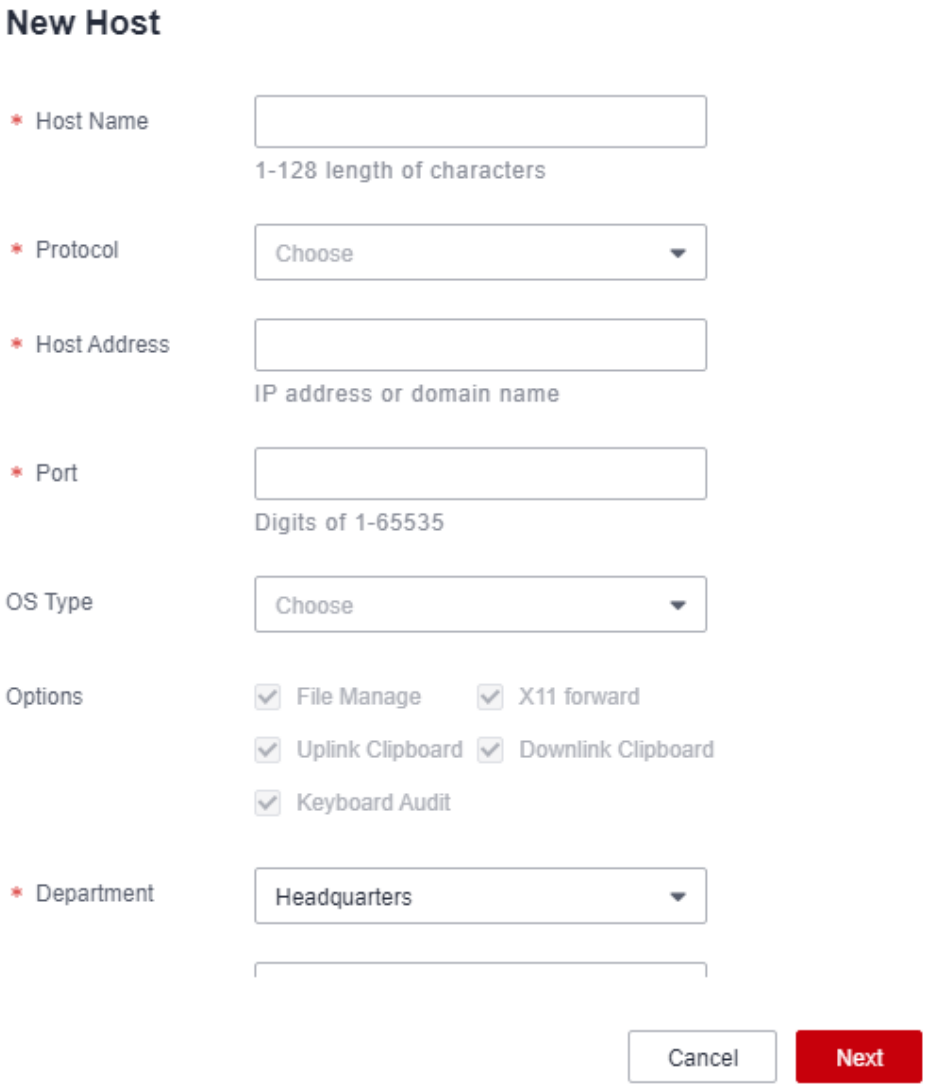


Table 6-3 Parameters for adding a resource

Parameter	Description
Host Name	Custom name of the host resource. A host name must be unique in a bastion host.

Parameter	Description
Protocol	Type of the protocol configured for the host. • In professional editions, you can configure SSH, RDP, VNC, Telnet, FTP, SFTP, DB2, MySQL, SQL Server, Oracle, SCP, Rlogin, Redis, and DM for a host. • In CBH standard editions, you can configure SSH, RDP, VNC, Telnet, FTP, SFTP, SCP, and Rlogin for a host.
Host Address	Host IP address that can be used to establish connection with your bastion host. • Select the EIP or private IP address of the host. Private IP addresses are recommended. • By default, the IPv4 address of the host is used. After an IPv6 address is enabled for a host, select either the IPv4 address or IPv6 address. **NOTE** A private IP address on the same VPC network recommended. The network stability and proximity will affect the O&M activities through a bastion host. The external access port of the private IP address is not restricted by the network security (security group and ACL) policies. While the port for external access over an EIP is restricted by network security policies. So a managed host resource may become inaccessible over an EIP through the bastion host. So we recommend private IP addresses.
Port	Port number of the host.
OS Type	(Optional) Type of the host OS or device OS. • The default value is empty. You need to select an OS type based on the type of the added resources. • Multiple default OS types are provided. The system administrator **admin** can customize OS types. For details, see **OS Types**.
Terminal Speed	If you select **Rlogin** for **Protocol**, you can select different terminal speed.
Encode	If you select **SSH** or **TELNET** for **Protocol**, you can use Chinese O&M page. The options are **UTF-8**, **Big5**, and **GB18030**.
Terminal Type	If you select **SSH** or **TELNET** for **Protocol**, you can specify the O&M terminal you want. You can select **Linux**, **Xterm-256color** (default), or **Xterm**.

Parameter	Description
Options	(Optional) Select **File Manage**, **X11 forward**, **Uplink Clipboard**, **Keyboard Audit**, and/or **Downlink Clipboard**. • **File Manage**: This option is supported only by SSH, RDP, and VNC hosts. • **Clipboard**: This option is supported only by SSH, RDP, and Telnet hosts. • **X11 forward**: This option is supported only by SSH hosts. • **Keyboard Audit**: Only RDP, VNC, and protocol hosts can be configured.
Department Name	Department to which the host resource belongs.
Label	(Optional) You can customize a label or select an existing one.
Remarks	(Optional) Provides the description of the host resource.

Step 4 Click **Next** and start to add resource accounts.

Table 6-4 Parameters of managed host accounts

Parameter	Description
Add Account	When to add the account. The options are **Rightnow** and **Afterward**. • If you select **Rightnow**, continue the configuration on the page to add the account immediately. • If you select **Afterward**, no further configuration is required on the page. You can add the account information later in the resource list or on the resource details page.
Login Type	Login method. You can select **Auto Login**, **Manual Login**, **Sudo Login**, or **CSMS Credentials Login**. • If you select **Auto Login**, **Account** and **Password** are mandatory. • If you select **Manual Login**, **Account** and **Password** are optional. • If you select **CSMS Credentials Login**, make sure you have available credentials. • If you select **Sudo Login**, a password is mandatory. **NOTE** If you select the key pair automatic login mode, select **Allow to change the SSH Key** when creating a password rule, or manual password change may fail.

Parameter	Description
Account	Account username of the managed host. **NOTE** If the AD domain service is installed on the host, the added account is *Domain name*|*Host account name*, for example, ad\administrator.
Password	Password of the account being added. By default, **Verify** is selected. After the account is added, the system automatically verifies the status of the account. **NOTE** • Verification succeeded. After the account is verified, the host resource information is saved. • Verification failed – If the system prompts that the account verification times out, return to the configuration window and modify the resource information. If the **root** account is used, ensure that the root login permission has been enabled on the host. – If the system prompts that the account password is incorrect, return to the configuration window and change the account password.
SSH Key	Authentication method that can be configured for host resources using the SSH protocol. After the configuration, an SSH key is preferentially used to log in to a related host resource.
Passphrase	Private key sequence corresponding to the SSH key. This parameter is optional. • You do not need to enter the password for logging in to the host when no private key password is generated. • You need to enter the private key password each time you log in to the host when the private key password is generated.
Parameter	If the selected protocol type is PostgreSQL, GaussDB, DB2, or Oracle, you can add parameters for the corresponding protocol. A maximum of 20 parameters can be added.
Login Role	If the selected protocol type is Oracle, you can select a role for logging in to the host resource.
Description	Brief description of the account.

NOTE

If no accounts are configured for the managed hosts, account **[Empty]** is generated by default. When you log in to the managed host through a bastion host for operations, select **[Empty]** and enter the username and password of an account of the host.

Step 5 Click **OK**. After the account is verified, you can then view the new host resource under the **Host** tab.

----End

Importing Host or Database Resources from a File

To import application server from a file, the file must be in .csv, .xls, or .xlsx format.

Step 1 Log in to your bastion host.

Step 2 Choose **Resource** > **Host** in the navigation pane on the left.

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

Step 4 Select **From file** for **Import**.

Step 5 Click **Download** next to **Download template**.

Step 6 Enter the information of host resources according to the configuration requirements in the template file.

NOTE

The table content must be in text format.

Table 6-5 Template parameters

Parameter	Description
Name	(Mandatory) a user-defined host resource name.
IP address/ domain name	(Mandatory) IP address or domain name of a host.
Protocol	(Mandatory) Select the protocol type of the host resource. Only one protocol type can be selected for a certain type of host resource. • In professional editions, you can configure SSH, RDP, VNC, Telnet, FTP, SFTP, DB2, MySQL, SQL Server, Oracle, SCP, Rlogin, Redis, and DM for a host. • In CBH standard editions, you can configure SSH, RDP, VNC, Telnet, FTP, SFTP, SCP, and Rlogin for a host.
Port	(Mandatory) Enter the host port number.
OS Type	Enter the operating system type of the host.
Department Name	(Mandatory) the department to which the host resource belongs. The department structure must be complete. • Only one department structure can be entered, and a resource can belong to only one department. • By default, the department can be set to **HQ**. Use a comma (,) to separate a department and its lower-level department. • Only the **department** that has been created in the system can be entered.

Parameter	Description
Label	Label of the host resource. • You can enter multiple labels and separate them with commas (,).
Remarks	Provides supplementary information about the host resource.
Account	Account of the host resource. • If this parameter is left blank, no **Empty** account will be generated.
Logon Type	Method to log in to the host resource. • This parameter can be set to **Auto Login**, **Manual Login**, or **Sudo Login**.
IS Sudo	Whether to set the account as a sudo account. • This parameter can be set to **Yes** or **No**.
Password	Password of the account for logging in to the resource.
SSH Key	Authentication method that can be configured for SSH hosts. After the configuration, an SSH key is preferentially used to log in to a related host resource.
passphrase	Private key sequence mapped to the SSH key. You need to enter the private key password each time you log in to the host when the private key password is generated. For details, see **How Do I Configure an SSH Key for Logging In to a Managed Host?**
Oracle Param	This parameter is mandatory for Oracle hosts. • This parameter can be set to **SERVICE_NAME** or **SID**. • Separate multiple parameter values with commas (,).
SERVICE_NAME or SID	This parameter is mandatory for Oracle hosts. • Separate multiple parameter values with commas (,).
Login Role	This parameter is mandatory for Oracle hosts. • This parameter can be set to **normal**, **sysdba**, or **sysoper**. • Separate multiple parameter values with commas (,).
Database Name	This parameter is mandatory for the DB2 databases. • Select the database name or instance name. • Separate multiple parameter values with commas (,).
Instance Name	This parameter is mandatory for the DB2 databases. • Select the database name or instance name. • Separate multiple parameter values with commas (,).

Parameter	Description
Switch From	For a host resource using the SSH protocol, enter its account username and set it to a sudo account.
Switch command	The command to switch over between accounts.
Description	Brief description of the managed resource account.
Account Group	The account group to which the managed resource account belongs. • A managed resource account can belong to multiple account groups in the same department. Use a comma (,) to separate every two account groups. • Only the **account group** that has been created in the system can be entered.

Step 7 Click **Upload** and select the completed template.

Step 8 (Optional) Configure **Override existing hosts**, which is not selected by default.

- Selected: An existing host resource will be overwritten when the existing host resource and the one being imported have the same *protocol type@host address:port* information.
- Deselected: An existing host resource will be skipped when the existing host resource and the one being imported have the same *protocol type@host address:port* information.

Step 9 Click **OK**. You can return to the host list and check the newly added host.

NOTE

- When you import host information by file, provide the host information based on configuration requirements in the .xlsx template file.
- SSH private keys can be used for logging in to hosts over SSH. When you set **SSH Key** and **Passphrase** parameters, enter the correct private key and password. After the SSH key public key and passphrase password are configured, the SSH key private key is preferentially used to verify login.
- The SSH key private key and passphrase are optional. You are advised to manage only the host accounts and passwords for managed hosts whose information is imported in batches.

----End

Importing Host or Database Resources

You can search for resources in your account in all regions and add them all to your bastion host in just a few clicks.

Step 1 Log in to your bastion host.

Step 2 Choose **Resource** > **Host** in the navigation pane on the left.

Step 3 Click **Import Cloud Resources** in the upper right corner of the page.

Table 6-6 Parameter description

Parameter	Description
Resource Type	You can select the cloud host or cloud database type. **NOTE** Currently, only MySQL, PostgreSQL, and SQL Server databases are supported.
Authentication Type	You can select AK/SK or a cloud service agency. **NOTE** Currently, Platform Bastion Host (PBH) supports only the AK/SK authentication.
Access Key ID	This parameter is mandatory when **Authentication Type** is set to **AK/SK**. To get the access key ID, click the information icon on the right of the text box.
Access Key Secret	This parameter is mandatory when **Authentication Type** is set to **AK/SK**. To get access key secret, click the information icon on the right of the text box of **Access Key ID**.
Priority of IP imported	You can select **Public** or **Internal**.
Options	(Optional) Configure **Override existing hosts**, which is not selected by default. • Selected: An existing host resource will be overwritten when the existing host resource and the one being imported have the same *protocol type@host address:port* information. • Deselected: An existing host resource will be skipped when the existing host resource and the one being imported have the same *protocol type@host address:port* information.
Department Name	Department to which the imported host resources belong.
Label	Label attached to the imported host resources.

Step 4 Check the information and click **Next**. On the region selection page, select the region where resources are to be imported.

NOTE

You can select only one region at a time.

Step 5 Confirm the information and click **Next**. The system automatically completes the import. After the import is finished, check the host list.

----End

Automatically Discovering Host or Database Resources

With the **Auto Discover** function, you can use Nmap to scan for hosts in a specific IP address or IP address range.

NOTE

Host resources can be automatically discovered only when the hosts and your bastion host are in the same VPC and the network connection is normal.

Step 1 Log in to your bastion host.

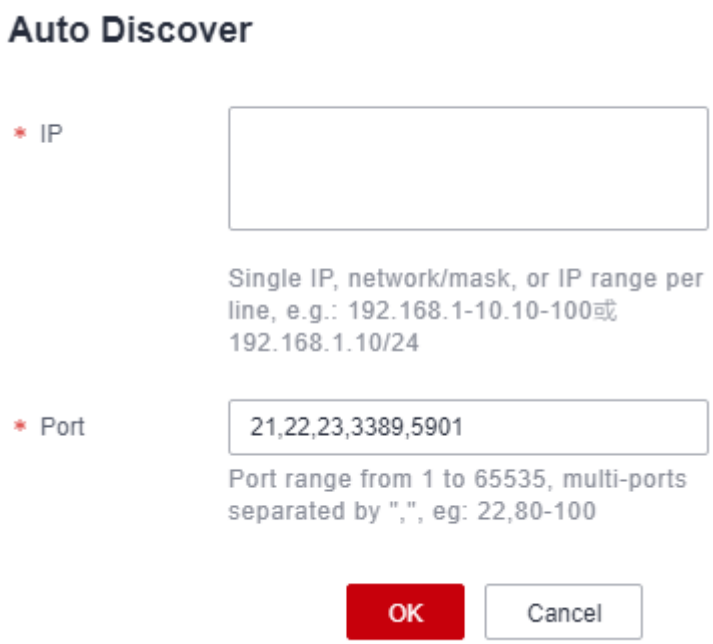
Step 2 Choose **Resource** > **Host** in the navigation pane on the left.

Step 3 Click **Auto Discover** in the upper right corner of the page.

Step 4 Enter the IP address and port number of host resources to be imported.

The default ports are **21**, **22**, **23**, **3389**, and **5901**. You can also add other ports or port ranges.

Figure 6-2 Auto Discover



Step 5 Click **OK** to start the auto discovery.

Step 6 Select the host resources to be imported.

- Enter a host name. If you do not enter the host name, the default host name is the IP address of the host.
- A protocol type is set automatically for the host based on default port. If the host does not match the default port, manually select a protocol type.

Step 7 Select the discovered hosts and click **Add**.

Click **Return** or **Close** to return to the host resource list page and view the newly added host resources.

----End

Cloning Host or Database Resources

If you want to add a host as many types of resources to your bastion host, you can add other types of host resources by just modifying configurations of a certain type you have added to CBH.

Step 1 Log in to your bastion host.

Step 2 Choose **Resource** > **Host** in the navigation pane on the left.

Step 3 In the **Operation** column of an added host resource, choose **More** > **Clone**.

Step 4 Modify information of the host resource and add accounts for the new host resource.

To complete the host clone, modify at least one of the following parameters of the host resource you select: **Protocol**, **Host Address**, and **Port**.

Step 5 Click **OK**. The host list page is displayed. You can check the new host resource on the displayed page.

----End

6.2.2 Managing Proxy Servers

In addition to managing resources in the public network environment, the bastion host can also manage resources in different network environments or dedicated network environments. To this end, you need to create a proxy server first.

Prerequisites

- You have the operation permissions for the **Host** module.
- Currently, only SSH and RDP host resources are supported.

Creating a Proxy Server

Step 1 Log in to your bastion host.

Step 2 Choose **Resource** > **Host** in the navigation pane on the left.

Step 3 Click the **Proxy Server** tab and then **New**. In the displayed dialog box, edit the proxy server information.

Table 6-7 Proxy server parameters

Parameter	Description
Server Name	Name of the proxy server. You can enter 1 to 128 characters.
Proxy Type	Select a proxy type. Currently, only SOCKS5 is supported.
Server Address	The private or public IP address of the server that is created as the proxy server. The IP address must be able to communicate with the bastion host.

Parameter	Description
Port	Port for the proxy server to access. The default port for SOCKS5 is 1080. If a fixed port is set, enter the fixed port number.
Department	Select a department. If no department is available, create one.
Server Account	Username for the account for logging in to the proxy server.
Password	Password of the account for logging in to the proxy server.
Test connectivity	When creating a server, you can test its connectivity. You are advised to select this option. If this option is not selected, the connectivity of the proxy server cannot be ensured, so the server may fail to manage or maintain resources.

Step 4 Confirm the information and click **OK**.

----End

Edit Proxy Server Information

Step 1 In the bastion host system, choose **Resource > Host** > **Proxy Server**.

Step 2 Click the name of the target server or click **Manage** in the **Operation** column. On the displayed proxy server details page, click **Edit** on the right of the **Basic Info** area.

Step 3 In the displayed dialog box, edit the basic information about the proxy server. For details about the parameters, see **Table 6-7**.

Step 4 Confirm the information and click **OK**.

----End

Deleting a Proxy Server

Step 1 In the bastion host system, choose **Resource > Host** > **Proxy Server**.

Step 2 Click the name of the target proxy server or **Delete** in the **Operation** column. In the dialog box displayed, confirm the information and click **OK**.

NOTE

If you delete a proxy server, resources that are using the proxy server will be disconnected from the bastion host immediately. No more operations can be performed for the resources. Exercise caution when performing this operation.

----End

6.2.3 Managing Host or Database Resources

You can view and edit the basic information, login users, resource accounts, O&M tasks for a specific host managed in your bastion host. You can also view and edit the basic information about proxy servers on the bastion host.

Viewing the Host or Database Resource List

Step 1 Log in to your bastion host.

Step 2 Choose **Resource** > **Host** in the navigation pane on the left.

Step 3 Click the **Host List** tab. On the page displayed, you can perform a quick search or an advanced search to search for the target resource.

- Quick search: Enter a keyword in the search box and search for a user by login name or username.
- Advanced search: Click **Advanced** next to text box and enter keywords in the corresponding attribute search boxes to search for resources.

----End

Editing Basic Information About a Resource

Step 1 Click the name of the target resource or **Manage** in the **Operation** column. The resource details page is displayed.

Step 2 In the **Basic Info** area, view all information about the current resource.

Step 3 Click **Edit** on the right of the area. In the displayed dialog box, edit the basic information about the current resource. For details about the parameters, see **Table 6-3**.

Step 4 Edit the content as needed, confirm the information, and click **OK**.

----End

Edit or Add Resource Accounts for a Resource

A resource account verifies your identity when you log in to a resource managed in your bastion host for O&M. You can associate multiple resource accounts with a resource.

Method 1: Edit and add resource accounts.

Step 1 Click the name of the target resource or **Manage** in the **Operation** column. The resource details page is displayed.

Step 2 In the **Account** area, view the accounts associated with the current resource.

Step 3 Click **Add** on the right of the area. In the displayed dialog box, create a resource account. For details about the parameters, see **Table 5-8**.

Step 4 Confirm the information and click **OK**. The resource account is created and associated with the current resource. Return to the resource account list to view the new resource account. If the new resource account is listed, the resource account has been added.

Step 5 Locate the target resource account and click **Remove** in the **Operation** column to disassociate the target resource account from the current resource. The removed resource account will not be deleted.

Step 6 Click the resource account name or **View** in the **Operation** column. On the displayed account details page, edit the basic information, joined group, and authorized users of the account.

----End

Method 2: Add resource accounts only.

Step 1 Locate the target resource and click **More** > **Add Account** in the **Operation** column to add a resource account.

Step 2 In the displayed dialog box, create a resource account for the current resource. For details about the parameters, see **Table 5-8**.

Step 3 Confirm the information and click **OK**. The resource account is created and associated with the current resource.

----End

Editing the Authorized Login User of a Resource

The login user associated with a resource can view the resource details after logging in to the bastion host instance. Unauthorized users cannot view the resource details.

Step 1 Click the name of the target resource or **Manage** in the **Operation** column. The resource details page is displayed.

Step 2 In the **Authorized User** area, view the authorized login users of the current resource.

Step 3 Click the username to view the details about the user. You can also edit the login restriction and user group of the user. For details, see **User Management**.

----End

Editing an Operation Task for a Resource

Step 1 Click the name of the target resource or **Manage** in the **Operation** column. The resource details page is displayed.

Step 2 In the **OPS Task** area, view the operation task details of the current resource.

----End

Deleting a Managed Resource

Locate the target managed resource and choose **More** > **Delete** in the **Operation** column to delete the resource.

NOTE

After a resource is deleted, all data of the resource is cleared. The resource account associated with the resource is cleared. The data of the resource account associated with the policy and ticket is also deleted.

Batch Editing OS Type for Resources

The OS type of a resource is identified by label. You can use labels to filter resources of the same OS type and manage them or edit their settings centrally.

You can also quickly locate the resources of the same OS type and change their passwords together.

Step 1 On the **Host List** tab, select all target resources and choose **More** > **Edit OS Type** in the lower left corner of the list.

NOTE

Make sure only the same type of resource is selected. Once the modification is complete, the OS type of all the selected resources will be changed.

Step 2 In the dialog box displayed, select the OS type as needed.

Step 3 Confirm the information and click **OK**.

----End

Batch Editing Resource Encoding

You can switch the encoding format of resources managed by your bastion host. In this way, you can easily view resources in different encoding formats.

Step 1 On the **Host List** tab, select all target resources and choose **More** > **Edit Host Encoding** in the lower left corner of the list.

Step 2 In the dialog box displayed, select an encoding format as needed.

Currently, only UTF-8, Big5, and GB 18030 are supported.

Step 3 Confirm the information and click **OK**.

----End

Batch Editing Operation Options for Hosts

The operation options include the actions and audits a user can perform during resource operation.

Step 1 On the **Host List** tab, select all target resources and choose **More** > **Edit Option** in the lower left corner of the list.

NOTE

Make sure the right resources are selected. Once the modification is complete, the supported operation options will be changed for all the selected resources.

Step 2 In the dialog box displayed, select operation options as needed.

Options you can select: **File Manage**, **X11 forward**, **Uplink Clipboard**, **Downlink Clipboard**, and **Keyboard Audit**.

Step 3 Confirm the information and click **OK**.

----End

Batch Editing the Connection Mode

You can batch edit the connection mode of host resources. Your bastion host will connect to target hosts using the connection mode you select.

Step 1 On the **Host List** tab, select all target resources and choose **More** > **Edit Host ConnectType** in the lower left corner of the list.

NOTE

Make sure the right resources are selected. Once the modification is complete, the connection type will be changed for all the selected resources.

Step 2 In the dialog box displayed, select a connection mode as needed.

NOTE

Currently, the direct connection and proxy modes are supported. If you select the proxy mode, you need to select a proxy server. If no proxy servers are available, create a proxy server by referring to **Managing Proxy Servers**.

Step 3 Confirm the information and click **OK**.

----End

Batch Editing Departments for Resources

Step 1 On the **Host List** tab, select all target resources and choose **More** > **Edit Dept** in the lower left corner of the list.

NOTE

Make sure the right resources are selected. Once the modification is complete, the department for all the selected resources will be changed accordingly.

Step 2 In the dialog box displayed, select a department as needed.

Step 3 Confirm the information and click **OK**.

----End

Batch Adding Resource Accounts

You can add one resource account for multiple resources at a time. In doing this, the resource account will be associated with all selected resources.

Step 1 On the **Host List** tab, select all target resources and choose **More** > **Add Account** in the lower left corner of the list.

NOTE

Make sure the right resources are selected. Once the task is finished, the same account will be added for all the selected resources.

Step 2 In the displayed dialog box, enter the information about the resource account you want to add. For details about the parameters, see the corresponding parameters in **Table 5-8**.

Step 3 Confirm the information and click **OK**.

----End

Batch Exporting Host Resources

Step 1 On the **Host** page, select the host resources to be exported.

NOTE

If no resources are selected, information about all resources is exported by default.

Step 2 Click  in the upper right corner. Confirm the export in the displayed dialog box.

- Set an encryption password to encrypt the exported file.
- Enter your password.
- Select the CSV or Excel format.

Step 3 Click **OK**. After the task is created, click **Go to Download Center**. If the export progress reaches 100%, click **Download** in the **Operation** column. Then you can view the exported host resource information in the downloaded file.

----End

6.3 Application Resources

6.3.1 Managing Application Resources Using a Bastion Host

You can use a bastion host to manage application resources and application accounts on Windows or Linux servers that support remote desktops. To do so, you only need to install clients and browsers on those servers.

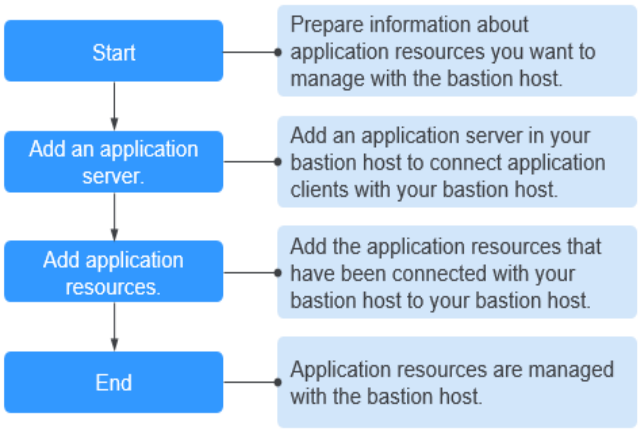
After you obtain the permission for application resources, you can access client-based application resources and browser-based application resources via your bastion host. You do not have to manually enter usernames and passwords as the credentials are automatically filled in. A bastion host also records all operations by video. In this way, remote application accounts security is under control, and remote application operations can be auditable.

You can use a bastion host to manage a wide range of application resources, such as Google Chrome, Microsoft Edge, Mozilla Firefox, SecBrowser, Oracle Tool, MySQL, SQL Server Tool, dbisql, VNC Client, vSphere Client and Radmin.

Procedure for Managing Application Resources

You can create an application server in the bastion host instance to interconnect the application client with the bastion host instance, so that you can create and manage application resources in the bastion host instance.

Figure 6-3 Managing application resources



Constraints

- The total number of host and application resources to be added cannot exceed the **number of assets**.
- For Windows servers, only applications running on Windows Server 2008 R2 or later can be managed.
- For Linux servers, only applications running on Linux CentOS 7.9 servers can be managed.
- Port 2376 and ports 35000 to 40000 must be enabled between a Linux server and the bastion host. The port cannot be changed once it is enabled.
- Before you add an application resource, ensure that an application server has been added.
- Automatic login accounts cannot be configured for Microsoft Edge application resources.
- If multiple bastion host instances share one application server, the versions of the bastion host instances must be the same. Otherwise, the application server may be unavailable for the bastion host instances of an earlier version.

Prerequisites

- You have all resources ready, such as Windows servers, Linux servers, images, enterprise authorization codes, and client licenses, for deploying an application publishing server.
- You have installed the application server. For more details, see **Installing Application Publish Server**.
- You have obtained the permission to manage the **AppServer** and **Application** tabs under the **Application Publish** module.

Adding an Application Server

Step 1 Log in to your bastion host.

Step 2 Choose **Resource** > **Application** > **AppServer**.

Step 3 Click **New**. In the displayed **New AppServer** dialog box, complete required parameters.

- Creating a Windows application server

Table 6-8 Windows application server parameters

Parameter	Description
Server Type	Windows
Server Name	Specifies the name of the application server. The server name must be unique in a bastion host.
Server	Specifies the IP address or domain name of the application server.
Type	Specifies the type of the browser or client tool used to access the application. By default, 14 types are supported, including MySQL Tool, Microsoft Edge, Mozilla Firefox (for Windows servers), Oracle Tool, Google Chrome, VNC Client, SQL Server Tool, SecBrowser, vSphere Client, Radmin, dbisql, Navicat for MySQL, Navicat for PostgreSQL, and Other. By default, each application resource type corresponds to an application program. You can obtain the application name from the default **Program Path**.
Port	Specifies the port number for accessing the application publish server. The default port 3389 is used for a Windows server.
Account	Specifies the server account used to access the application. If AD domain is configured, the server account is in the format of *AD domain name**account name*, for example, *ad|administrator*.
Password	Specifies the password used to access the application resource.
Department Name	Specifies the department of the application server.
Program Path	Specifies the path of the application resource on the application server. – Each program type has a default startup path. You can also customize a startup path. For example, to allow a system user to access only Google Chrome from the application server, set **Program Path** to **C:\DevOpsTools\Chrome\chrome.exe**. – If you select **Other**, manually configure the corresponding program path.

Parameter	Description
Remarks	(Optional) Provides the description of the application server.

- Creating a Linux application server

  Table 6-9 Linux application server parameters

Parameter	Description
Server type	Linux
Server Name	Specifies the name of the application server. The server name must be unique in a bastion host.
Server	Specifies the IP address or domain name of the application server.
Type	Specifies the type of the browser or client tool used to access the application. Supported types: DM Tool, KingbaseES Tool, Mozilla Firefox for Linux, and GBaseDataStudio for GBase8a.
Port	Enter the port for accessing the application publish server. The default port 2376 is used for a Linux server.
Password	Contact Huawei Cloud technical support to obtain the password.
Department	Specifies the department the application server belongs to.
Remarks	(Optional) Provides the description of the application server.

Step 4 Click **OK**. You can return to the application server list and check the newly added server.

----End

Importing Application Servers from a File

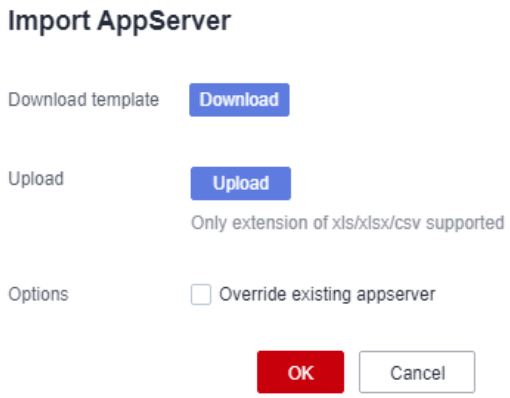
To import application server from a file, the file must be in .csv, .xls, or .xlsx format.

Step 1 Log in to your bastion host.

Step 2 Choose **Resource** > **Application** > **AppServer**.

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

Figure 6-4 Import App Server



Step 4 Click **Download** to download the template if no template is available locally.

Step 5 Enter the configuration information of application servers to be imported according to the configuration requirements in the template file.

Step 6 Click **Upload** and select the completed template.

Step 7 (Optional) Configure **Override existing appservers**. This option is deselected by default.

- If you select this option, an existing application server information will be overwritten by the one being imported when both application servers have the same name.
- If you deselect this option, an existing application server information will be skipped when the one being imported and the existing one have the same name.

Step 8 Click **OK**. You can go to the application server list and check the newly imported servers.

----End

Adding an Application Resource

Step 1 Log in to your bastion host.

Step 2 Choose **Resource** > **Application** > **Application**.

Step 3 Click **New**. In the displayed **New application** dialog box, complete required parameters.

Table 6-10 Parameters for adding an application resource

Parameter	Description
App Name	Specifies the name of an application resource to be added. The **App Name** of an application resource must be unique in a bastion host. **NOTE** The application name must be unique in a bastion host. This means it cannot be the same as the name of any managed hosts or other application resources.

Parameter	Description
AppServer	Select a created application publishing server.
Department Name	Specifies the department of the application.
App Address	(Optional) Specifies the address of the application. The value can be an IP address or domain name. • If the application is released as a browser, enter the URL of the web page. If the address has a corresponding port, enter the address in the format of *URL:Port number*. • If the application is released as a database or client, enter the address of the database server.
APP Port	(Optional) Enter the application access port. • If the application is released as a database or client, enter the database access port. • Leave this parameter blank if the application is released in other formats except databases.
Param	(Optional) Set application parameters. • Enter the database instance name if the application is released as a database. • Leave this parameter blank if the application is released in other formats except databases.
Custom Params	(Optional) Set custom application parameters. • **Fill Node**: Enter the selector path of the input box to be filled. For example, **#accountNamed > input**. For details about how to obtain the selector path, see **Obtaining the Selector Path**. • **Fill Content**: Enter the text to be filled in. You can use **{account}** or **{password}** to replace the application account and password.
Checkbox Recognition	(Optional) If you enable **Checkbox Recognition**, the system automatically identifies and selects check boxes. This parameter determines whether to identify all check boxes that can be identified on the login page, for example, the user privacy agreement check box of the browser. This parameter is available only when **App Server** is set to **Chrome**, **Firefox-Windows**, or **Firefox-Linux**.

Parameter	Description
Checkbox Selector	(Optional) If you enable **Checkbox Recognition**, you can set **Checkbox Selector**, which is the selector path of the selected check box. Example: User privacy agreement: **.agreement input[type="checkbox"]** For details about how to obtain the selector path, see **Obtaining the Selector Path**. This parameter is available only when **App Server** is set to **Chrome**, **Firefox-Windows**, or **Firefox-Linux**.
Automatic Logon	(Optional) After this function is enabled, when you log in to a web resource using a browser, you can automatically log in to the resource without manually clicking the login button. This parameter is available only when **App Server** is set to **Chrome**, **Firefox-Windows**, or **Firefox-Linux**.
Login Button Selector	If you enable **Automatic Logon**, you must set the selector path of the automatic login button. Example: **#login-button** For details about how to obtain the selector path, see **Obtaining the Selector Path**. This parameter is available only when **App Server** is set to **Chrome**, **Firefox-Windows**, or **Firefox-Linux**.
Options	(Optional) Configure the session window functions that can be used during the O&M. • **File Manage**: This function allows you to manage file or folder permissions, including the permissions to view, delete, and edit files and folders. • **Uplink Clipboard**: This function allows you to copy text through the O&M session RDP clipboard. • **Downlink Clipboard**: This function allows you to paste text through the O&M session RDP clipboard. • **Keyboard Audit**: This function records the information entered through the keyboard. • **Kiosk**: For applications that can be managed through a browser, you can use this function to hide the address bar and disable F12, right-click, and the browser toolbar. You can use F12 instead of Ctrl to implement combined key operations. **Kiosk** is supported only when **App Server** is set to **Chrome**, **Firefox-Windows**, or **Firefox-Linux**.
Label	(Optional) You can customize a label or select an existing one.
Remarks	(Optional) Provides the description of the application resource.

Step 4 Click **Next**.

Table 6-11 Parameters for adding an application resource account

Parameter	Description
Add Account	• If you select **Rightnow**, configure **Logon Type** and then **Account**. • If you select **Afterward**, no further configuration is required on the page. You can add the account information later in the resource list or on the resource details page. In this situation, when you click **OK**, account **[Empty]** is automatically created. Only one **[Empty]** account is created for an application resource.
Logon Type	• If you select **Auto Login**, **Account** and **Password** must be provided. • If you select **Manual Login**, **Account** and **Password** are optional. If no application account is set, the **[Empty]** account is automatically created.
Account	Account to access the application
Password	Password of the application account
AD Domain	For Radmin application resources, enter the AD domain server address.
Description	Brief description of the account.

NOTE

When logging in to a managed host using **[Empty]**, manually enter the application account username and password.

Step 5 Click **OK**. The application publish list page is displayed. You can check the created application publishing service.

----End

Importing Application Resources from a File

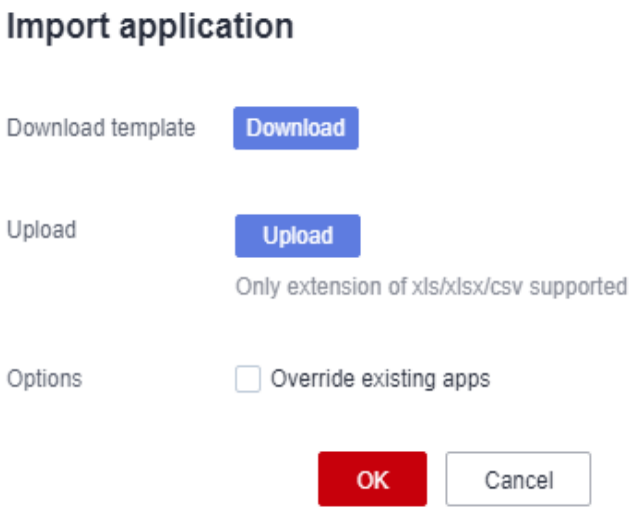
To import application server from a file, the file must be in .csv, .xls, or .xlsx format.

Step 1 Log in to your bastion host.

Step 2 Choose **Resource** > **Application** > **Application**.

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

Figure 6-5 Import application



Step 4 Click **Download** next to **Download template**.

Step 5 Enter the configuration information of application resources to be imported according to the configuration requirements in the template file.

Step 6 Click **Upload** and select the completed template.

Step 7 (Optional) Configure **Override existing apps**. This option is deselected by default.

- Selected: A managed application resource will be overwritten by the one being imported if both application resources have the same name.
- Deselected: A managed application resource will be skipped when the managed one and the one being imported have the same name.

Step 8 Click **OK**. You can go to the new application in the application release service list.

----End

Obtaining the Selector Path

The following describes how to obtain the selector path required in the login button on the bastion host login page.

Step 1 On the bastion host login page, press F12 to open the browser developer tool.

Step 2 Click  and then click **Login**.

Figure 6-6 Querying the login button element

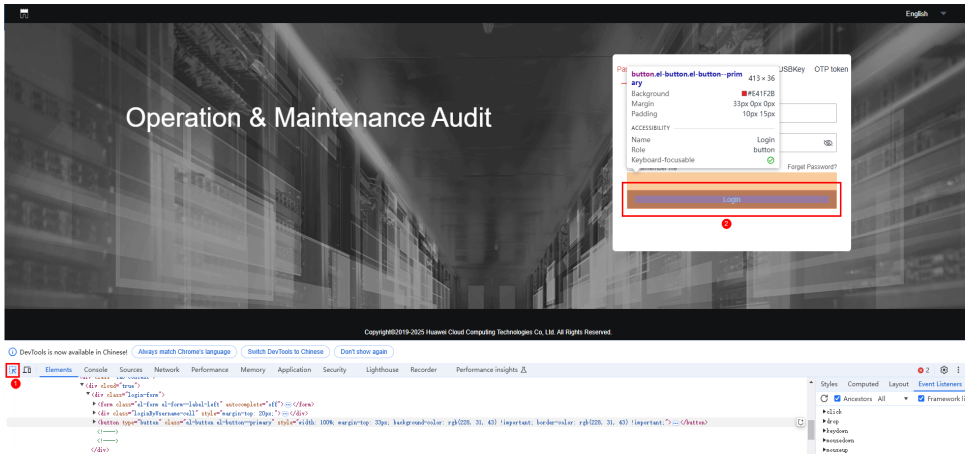
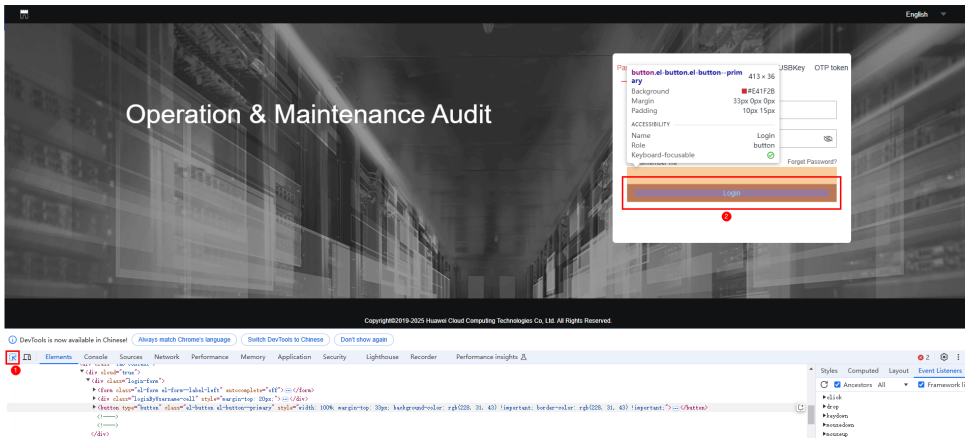


Figure 6-7 EN



Step 3 On the **Elements** tab, right-click the button line and choose **Copy** > **Copy selector** from the shortcut menu.

The copied path is the selector path required in the login button.

Figure 6-8 Querying the selector path

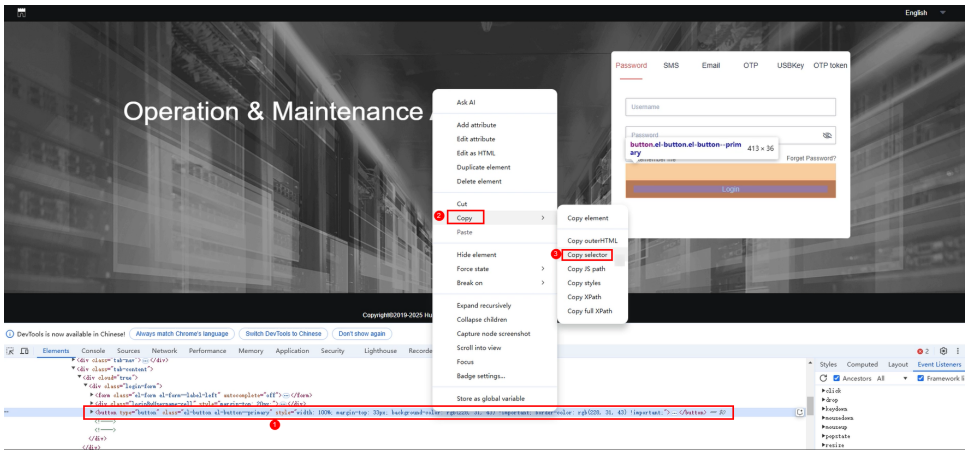
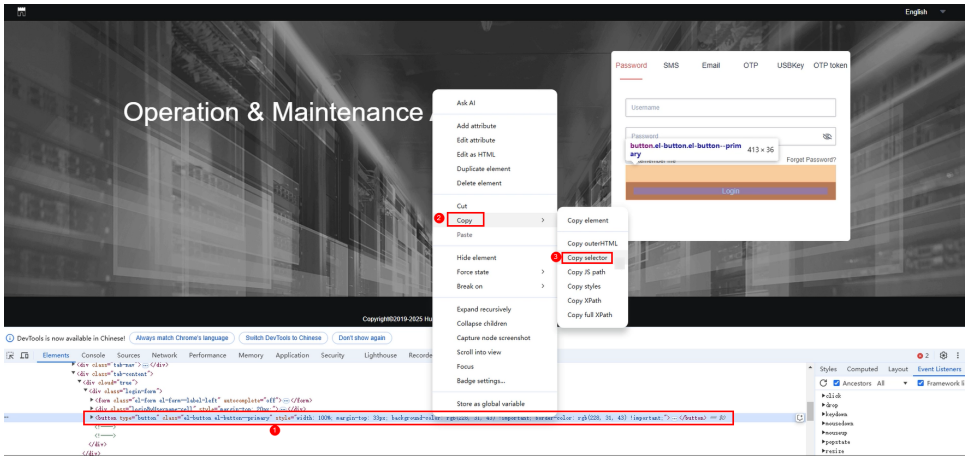


Figure 6-9 EN



----End

6.3.2 Managing Application Servers

You can use the bastion host instance to edit, delete, and export application servers to ensure that the application server information is updated in a timely manner.

Editing Application Server Information

Step 1 Log in to your bastion host.

Step 2 Choose **Resource** > **Application** > **AppServer**.

Step 3 Click the name of the target application server or **Manage** in the **Operation** column. The application server details page is displayed.

Step 4 In the **Basic Info** area, view the details about the application server and click **Edit** on the right.

Step 5 In the displayed dialog box, edit the basic information about the application server. For details about the parameters, see **Table 6-8**.

NOTE

The OS type for application servers cannot be edited.

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

----End

Deleting One or More Application Servers

Step 1 Log in to your bastion host.

Step 2 Choose **Resource** > **Application** > **AppServer**.

Step 3 Click the name of the target application server or **Delete** in the **Operation** column. In the dialog box displayed, confirm the information and click **OK**.

NOTE

If you delete an application server, resources that are using the server will be disconnected from the bastion host immediately. No more operations can be performed for the resources. Exercise caution when performing this operation.

----End

Batch Exporting Application Servers

Step 1 Choose **Application** > **AppServer** and select the application server resources to be exported.

If no application servers are selected, information about all application servers is exported by default.

Step 2 Click  in the upper right corner. Confirm the export in the displayed dialog box.

- Set an encryption password to encrypt the exported file.
- Enter your password.
- Select the CSV or Excel format.

Step 3 Click **OK**. After the task is created, click **Go to Download Center**. If the export progress reaches 100%, click **Download** in the **Operation** column. Then you can view the exported application server resource information in the downloaded file.

----End

Changing the Department an Application Server Belongs To

Step 1 Log in to your bastion host.

Step 2 Choose **Resource** > **Application** > **AppServer**.

Step 3 Select all target application servers and choose **More** > **Edit Dept** in the lower left corner of the list. In the dialog box displayed, select the target department, confirm the information, and click **OK**.

NOTE

The department for all the selected servers will be edited. The batch operation cannot be canceled. Exercise caution when performing this operation.

----End

6.3.3 Managing Application Resources

You can edit the information about the application resources managed in your bastion host. You can edit basic information, resource accounts associated with the resources, and authorized login users. You can also add resource accounts and labels for application resources.

Viewing the Application Resource List

Step 1 Log in to your bastion host.

Step 2 Choose **Resources > Application > Application**. On the application list page, you can view all managed application resources.

----End

Editing Basic Application Resource Information

Step 1 Click the name of the target application resource or **Manage** in the **Operation** column. The application resource details page is displayed.

Step 2 In the **Basic Info** area, view basic information. Click **Edit** on the right. In the displayed dialog box, edit basic information about the application resource. For details about the parameters, see **Table 6-10**.

Step 3 Confirm the information and click **OK**.

----End

Managing Resource Accounts for an Application Resource

Step 1 Click the name of the target application resource or **Manage** in the **Operation** column. The application resource details page is displayed.

Step 2 In the **Account** area, view the accounts associated with the current application resource.

- Click the name of the target resource account or **View** in the **Operation** column to view the detailed information about the resource account.
- Click **Remove** in the **Operation** column of the target resource account to disassociate the resource account from the current application resource.

Step 3 Click **Add** on the right. In the dialog box displayed, enter the account information to add an account for the current application resource. For details about the parameters, see **Table 6-11**.

Step 4 Confirm the information and click **OK**.

----End

Managing Authorized Users for an Application Resource

Step 1 Click the name of the target application resource or **Manage** in the **Operation** column. The application resource details page is displayed.

Step 2 In the **Account** area, view the login users associated with the current application resource.

----End

Batch Editing Operation Options for Application Resources

Step 1 In the application list, select target application resources and choose **More** > **Edit Option** in the lower left corner of the list.

Step 2 In the dialog box displayed, select the options you want to edit.

NOTE

Batch editing actions cannot be rolled back. Exercise caution when performing this operation.

Step 3 Confirm the information and click **OK**.

----End

Editing the Department for an Application Resource

Step 1 In the application list, select the target application resources and choose **More** > **Edit Dept** in the lower left corner of the list.

Step 2 In the dialog box displayed, select the department as needed.

NOTE

Batch editing actions cannot be rolled back. Exercise caution when performing this operation.

Step 3 Confirm the information and click **OK**.

----End

Batch Adding Resource Accounts for Application Resources

Step 1 In the application list, select the target application resources and choose **More** > **Add Account** in the lower left corner of the list.

Step 2 In the dialog box displayed, enter the account information. For details about the parameters, see **Table 6-11**.

Step 3 Confirm the information and Click **OK**.

----End

Deleting an Application Resource

Step 1 In the application list, locate the target application resource and choose **More** > **Delete** in the **Operation** column.

Step 2 In the dialog box displayed, confirm the information and click **OK**.

NOTE

No operations can be performed on deleted resources. Exercise caution when performing this operation.

----End

Exporting the Application Resource List

Step 1 On the **Application** page, select the application resources to be exported.

NOTE

If no resources are selected, information about all resources is exported by default.

Step 2 Click  in the upper right corner. Confirm the export in the displayed dialog box.

- Set an encryption password to encrypt the exported file.
- Enter your password.
- Select the CSV or Excel format.

Step 3 Click **OK**. After the task is created, click **Go to Download Center**. If the export progress reaches 100%, click **Download** in the **Operation** column. Then you can view the exported application resource information in the downloaded file.

----End

6.4 Cloud Servers (Using a Bastion Host to Manage Container Resources)

6.4.1 Creating a Kubernetes Server

You can add Kubernetes servers to your bastion host for management. This section describes how to add a Kubernetes server to a bastion host.

Constraints

- The number of managed Kubernetes servers is restricted by the bastion host license you hold.
- You must have the permission to create a **Kubernetes server**.
- Only the professional editions can manage Kubernetes services.
- To use this function, the bastion host version must be V3.3.48.0 or later.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **Resource** > **Cloud Service**. The **Cloud Service** is displayed.

Step 3 Click **Kubernetes Server**. The **Kubernetes Server** page is displayed.

Step 4 Click **New** in the upper left corner. Configure parameters in the dialog box that is displayed.

Figure 6-10 Creating a Kubernetes server

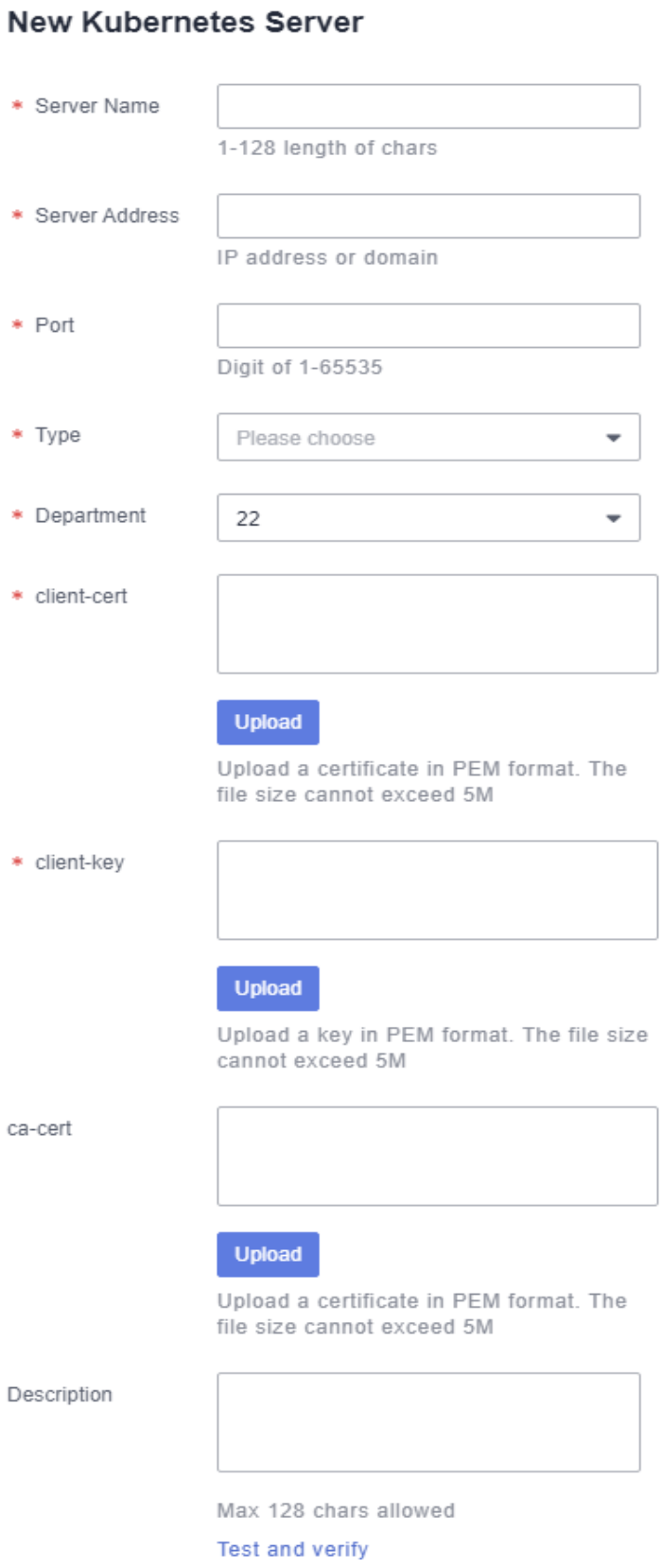


Table 6-12 Parameters

Parameter	Description
Server Name	Customize a service name.
Server	Enter your Kubernetes server address.
Port	Enter your Kubernetes server port number.
Type	For V3.3.54.0, only **Kubernetes** can be selected.
Department Name	Select the department of the Kubernetes server. The default value is **Headquarters**.
client-cert	Obtain the value of **client-certificate-data** from the debugging information, and enter the decoded value by using the way of **Base64**.
client-key	Obtain the value of **client-certificate-data** from the debugging information, and enter the corresponding **Base64** value.
ca-cert	Obtain the value of **certificate-authority-data** from the debugging information, and enter the decoded value by using the way of **Base64**.
Remarks	(Optional) Enter the description of the server.

Step 5 Click **OK**. The Kubernetes server is created.

----End

6.4.2 Operations About Kubernetes Servers

After Kubernetes servers are managed by a bastion host, you can delete managed servers or modify information at any time.

Constraints

- The number of managed Kubernetes servers is restricted by the bastion host license you hold.
- You must have the permission to perform operations on the **Kubernetes Server**.
- To use this function, the bastion host version must be V3.3.48.0 or later.

Modifying Kubernetes Server Information

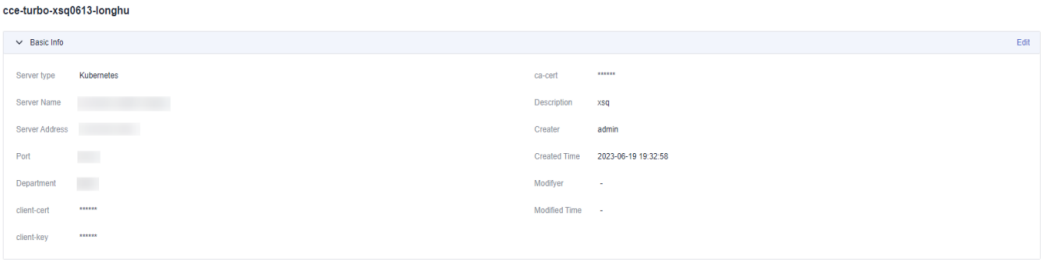
Step 1 Log in to your bastion host.

Step 2 Choose **Resource** > **Cloud Service**. The **Cloud Service** is displayed.

Step 3 Click **Kubernetes Server**. The **Kubernetes Server** page is displayed.

Step 4 In the **Operation** column of the server whose information is to be modified, click **Manage**.

Figure 6-11 Editing a Kubernetes server



Step 5 Click **Edit** in the upper left corner to modify the Kubernetes server information. For details about the parameters, see **Table 6-12**.

Step 6 Click **OK**. The Kubernetes server information is modified.

----End

Deleting a Kubernetes Server

Step 1 Log in to your bastion host.

Step 2 Choose **Resource** > **Cloud Service**. The **Cloud Service** is displayed.

Step 3 Click **Kubernetes Server**. The **Kubernetes Server** page is displayed.

Step 4 In the **Operation** column of the server to be deleted, click **Delete**.

Step 5 Click **OK**. The Kubernetes server information is deleted.

----End

6.4.3 Creating a Container

You can add Kubernetes containers to your bastion host for management. This section describes how to add a container to a bastion host.

Constraints

- You must have the permission on the **container** to perform operations.
- The Kubernetes server where the container is located has been added to the bastion host for management. For details, see **Creating a Kubernetes Server**.
- To use this function, the bastion host version must be V3.3.48.0 or later.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **Resource** > **Cloud Service**. The **Cloud Service** is displayed.

Step 3 Click **New** in the upper left corner. Configure parameters in the dialog box that is displayed.

Figure 6-12 Creating a Container

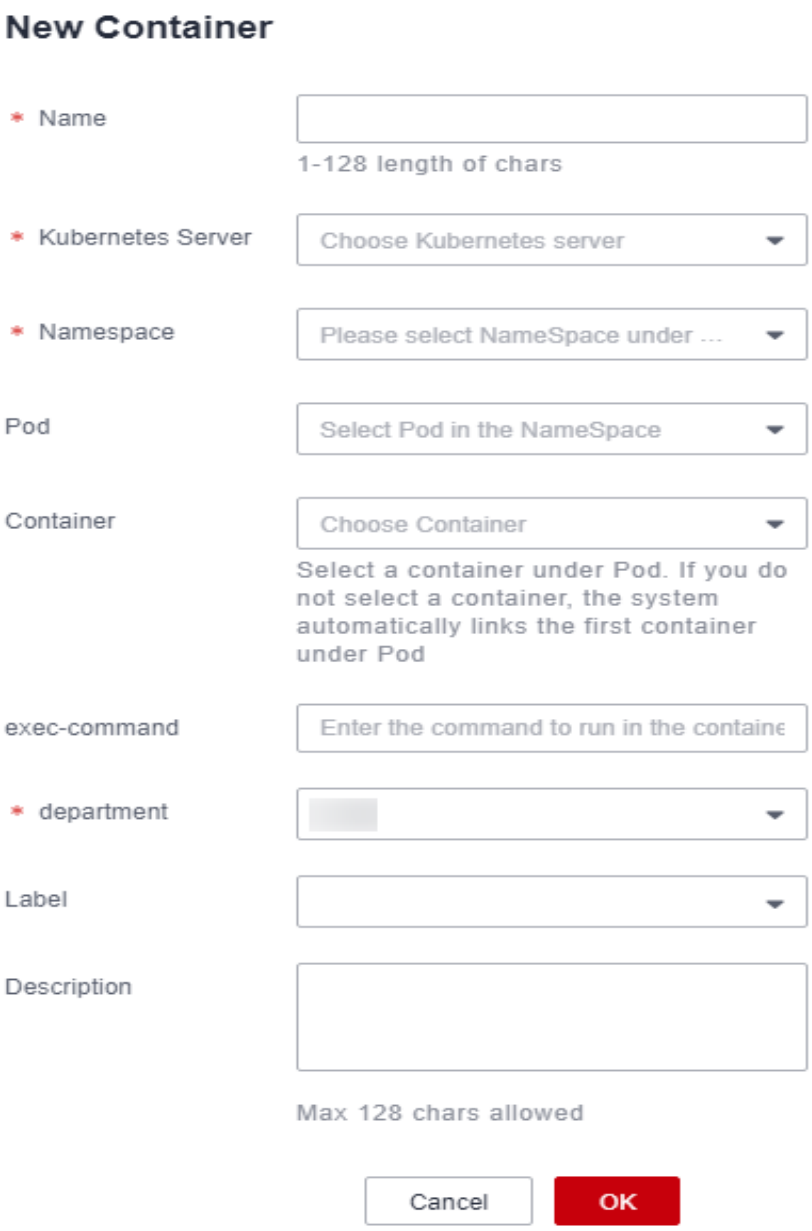


Table 6-13 Parameters for creating a container

Parameter	Description
Container Name	Enter a container name.
Kubernetes Server	Select the Kubernetes server that you added in **Creating a Kubernetes Server**.
Namespace	Namespace where the container to be managed is located.

Parameter	Description
Pod	(Optional) Select the pod where the container to be managed is located. If there are only containers to be managed in the pod, you do not need to select pods.
Container	(Optional) Select the container to be managed. If there are multiple containers in the pod and none of them are selected, the system automatically connects to the first container in the pod by default.
exec-command	(Optional) Enter the pre-running command in the container. If you do not set this parameter, then no command will be executed, and the input/output is attached to the main process of the container. **NOTE** If you set this parameter, the connection is similar to **kubectl exec**. If you do not set this parameter, the connection is similar to **kubectl attach**.
Department Name	Select the department of the container to be managed.
Label	Add a label for the container to be managed.
Container Description	Description about the container

Step 4 Click **OK**. The container has been managed.

----End

6.4.4 Container Resource Management

After a container is managed by a bastion host, you can delete the container or modify the container information at any time.

Constraints

- You must have the permission on the **container** module.
- To use this function, the bastion host version must be V3.3.48.0 or later.

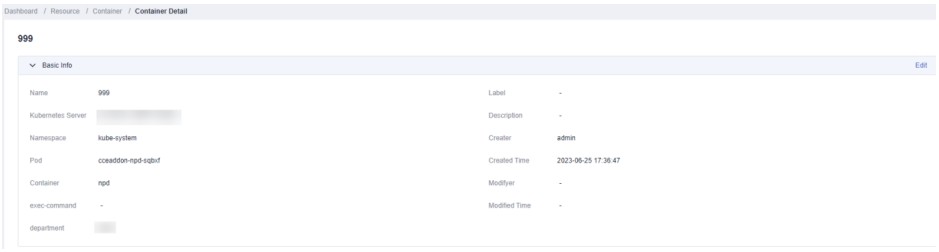
Editing a Container

Step 1 Log in to your bastion host.

Step 2 Choose **Resource** > **Cloud Service**. The **Cloud Service** is displayed.

Step 3 Click **Manage** in the **Operation** column of the container whose information is to be modified. The **Container Detail** page is displayed.

Figure 6-13 Container detail



Step 4 Click **Edit** on the right of the **Basic Info** row. In the dialog box that is displayed, modify the container information. For details about the parameter rules, see **Table 6-13**.

Step 5 After modifying the parameters, click **OK**. The container information is modified.

----End

Delete Containers

Step 1 Log in to your bastion host.

Step 2 Choose **Resource** > **Cloud Service**. The **Cloud Service** is displayed.

Step 3 Click **Delete** in the **Operation** column of the container to be deleted.

Step 4 In the dialog box that is displayed, click **OK**. The container is deleted.

----End

6.5 Resource Labels

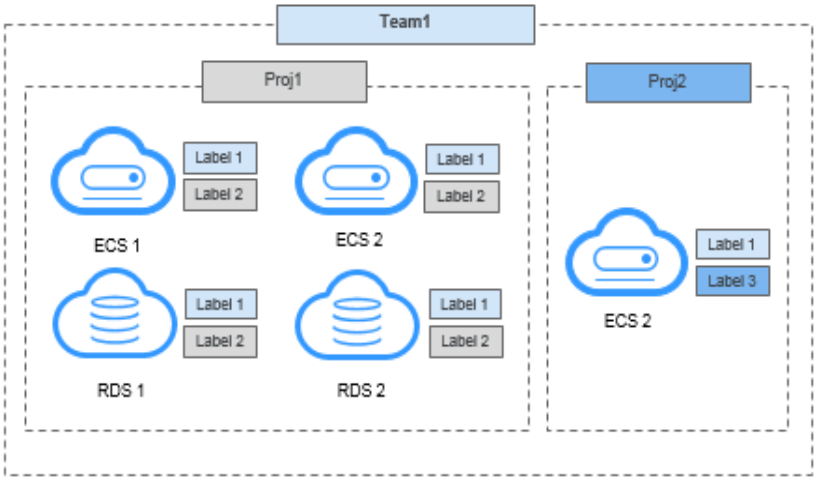
6.5.1 Overview

You can set labels to identify and group host and application resources managed in a bastion host. In this way, you can identify all resources related to a managed host or application resource.

After a label is added to a host or application, all managed resources related to the host or application will be labeled. In this way, you can search for resources by label. A host or application can have a maximum of 10 labels.

Each managed resource, such as ECSs and RDS instances, is tagged with two labels. **Label 1** is identified by team, and **Label 2** and **Label 3** are identified by project. You can search for resources by label.

Figure 6-14 Examples of labels



After you add labels to resources, you can search for managed resources by label and manage labels. For more details, see **Table 6-14**.

Table 6-14 Label usage in CBH

Navigation Path	Operation
Dashboard > Recently Logged Host	Search for resources.
Dashboard > Recently Logged Application	Search for resources.
Dashboard > My Hosts	Search for resources.
Dashboard > My APPs	Search for resources.
Resource > Host	Add, delete, or edit labels and search for resources by label.
Resource > Application	Add, delete, or edit labels and search for resources by label.
Operation > Host Operations.	Add or delete labels and search for resources by label.
Operation > App Operations	Add or delete labels and search for resources by label.

6.5.2 Adding a Label for a Resource

You can define resource labels for your exclusive use. Labels cannot be shared among system users.

You can add labels to host or application resources when or after you add host or application resources. A host or application can have a maximum of 10 labels by default.

You can configure labels when you **add host resources** or **add application resources**. This topic describes how to add labels after host and application resources are added to your bastion host. Labels can be added through the resource management or operation modules. As an example, the following content walks you through how to add labels to a host resource in the **Host** module.

Prerequisites

You have the obtained the operation permissions for the **Host**, **Application Publish**, **Host Operations**, and **App Operations** modules.

Adding Labels for Host Resources

Step 1 Log in to your bastion host.

Step 2 Choose **Resource** > **Host** in the navigation pane on the left.

Step 3 Select the host you want to add a label and click **Add Label** at the bottom of the host list. The **Add Label** dialog box is displayed.

Step 4 Enter the custom label content, confirm the content, and click **OK**. Return to the **Host** or **Host Operations** page to view the new label of the host.

Step 5 Search for resources by label. Go to the resource list page in the **Resource** module, select a label from the drop-down list in the **Label** column to search for resources.

----End

Adding Labels for Application Resources

Step 1 Log in to your bastion host.

Step 2 Choose **Resource** > **Application** to go to the application publish list page.

Step 3 Select the application resource you want to add a label and click **Add Label** at the bottom of the resource list. The **Add Label** dialog box is displayed.

Step 4 Enter the custom label content, confirm the content, and click **OK**. Return to the **Application** page under **Resource** and view the label of the application resource.

----End

Adding Labels for Container Resources

Step 1 Log in to your bastion host.

Step 2 Choose **Resource** > **Cloud Service**. The **Cloud Service Management** page is displayed.

Step 3 Select the container resource you want to add a label and click **Add Label** at the bottom of the resource list. The **Add Label** dialog box is displayed.

Step 4 Enter the custom label content, confirm the content, and click **OK**. Return to the **Container** tab and view the label of the container resource.

----End

6.5.3 Deleting a Resource Label

This topic describes how to delete a resource label.

Constraints

- After you confirm the deletion, all labels of the selected resource are deleted.
- If a label is not used by any resources, the system will delete it.

Prerequisites

You have the obtained the operation permissions for the **Host**, **Application Publish**, **Host Operations**, and **App Operations** modules.

Deleting a Host Resource Label

You can delete labels from resources.

Step 1 Log in to your bastion host.

Step 2 Choose **Resource** > **Host** in the navigation pane on the left.

Step 3 Select the target host and click **Delete Label** at the bottom of the host list. In the displayed **Delete Label** dialog box, click **Confirm**. All labels added to the host are then deleted.

Step 4 Go to the **Host** page in the **Resource** module or the **Host Operations** page in the **Operation** module to verify that labels are deleted.

NOTE

Additionally, you can go to the resource list page and click **Manage** in the host or application row. On the displayed page, delete the label of a managed host or application resource.

----End

Deleting an Application Resource Label

Step 1 Log in to your bastion host.

Step 2 Choose **Resource** > **Application** to go to the application publish list page.

Step 3 Select the target application resource and click **Delete Label** below the resource list.

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

----End

Deleting a Container Resource Label

Step 1 Log in to your bastion host.

Step 2 Choose **Resource** > **Cloud Service**. The **Cloud Service Management** page is displayed.

Step 3 Select the target application resource and click **Delete Label** below the resource list.

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

----End

6.6 Resource OS Types

A bastion host can manage resource OS types and allows you to define custom operating system (OS) types.

You can add tags to OS types and then group and manage resources by those tags. With OS type tags, you can change server passwords, store password change parameters, and run password rules for resources of a certain OS type at the same time.

A bastion host can manage 14 OS types by default, including Linux, Windows, Cisco, Huawei, H3C, DPtech, Ruijie, Sugon, Digital China sm-s-g 10-600, Digital China sm-d-d 10-600, ZTE, ZTE5950-52tm, Surfilter, and ChangAn.

Constraints

- Only system administrator **admin** can modify the OS type configuration.
- The default OS type cannot be deleted or modified. Only the customized OS types can be deleted or modified.

Customizing OS Types

Step 1 Log in to your bastion host.

Step 2 Choose **Resource** > **OS Type** to switch to the OS type list page.

Step 3 Click **New** to switch to the **New OS Type** dialog box and configure parameters.

Table 6-15 Parameters for creating an OS type

Parameter	Description
OS Type	Specifies the name of the custom OS type.

Parameter	Description
Chpw Param	Specifies the command of changing the account password and its return value. A maximum of 16 commands can be added. • **password** indicates the old password. • **new_password** indicates the new password. • **change_user** indicates the account whose password needs to be changed. • Brackets are not allowed.
Chpw Param for Sudo Login	Specifies the command of obtaining the permission for changing the account password and its success return. A maximum of 16 commands can be added. • **password** indicates the old password. • **new_password** indicates the new password. • Brackets are not allowed.
Remarks	Provides brief introduction about the OS type.

Step 4 Click **OK**. The newly created OS type will be displayed in the OS type list.

Step 5 Manage customized OS types.

----End

Other Operations

Step 1 Log in to your bastion host.

Step 2 Choose **Resource** > **OS Type** to switch to the OS type list page.

Step 3 Delete a customized OS type.

- To delete an OS type, click **Delete** in the **Operation** column of the row where the OS type locates.
- To delete multiple OS types, select the ones you want to delete and click **Delete** at the bottom of the OS type list to delete them together.

Step 4 View and edit the customized OS type configurations.

1. Click the name of the OS type you want to edit or click **Manage** in the row of the OS type in the **Operation** column.
2. Click **Edit** in the **Basic Info** area to edit the basic information of the OS type.

----End

7 Policy

7.1 Policy Overview

With a bastion host, you can configure some policies for operations to make operation faster.

You can configure access control, command control, database control, password change, and account synchronization policies for operation tasks in advance.

Table 7-1 Policies supported by bastion hosts

Policy Type	Policy Description
ACL rules	ACL rules are used to control users' permissions to access resources.
Command rules	Command rules are used to control permissions for critical O&M operations on managed resources, implementing fine-grained control over the execution of commands on Linux hosts.
Database rules	Database rules are used to intercept sensitive database session operations, implementing fine-grained control over database operations. When an authorized system user logs in to a database related to a database rule, their sensitive operations will be intercepted once the database rule is triggered.

Policy Type	Policy Description
Password rules	With password rules, you can let the bastion host periodically change the passwords of multiple managed host resources at a time, enhancing the managed resource account security. With password rules, you can: • Change passwords of managed resource accounts manually, periodically, or at a scheduled time. • Change the passwords of multiple managed resource accounts to different passwords randomly generated by the system, the same password generated by the system, or to the same password you specify.
Account synchronization rules	Synchronization rules are used to automatically synchronize managed host accounts, making it easier for you to manage accounts of managed hosts, delete zombie accounts, and discover accounts that are not managed in a timely manner. This further strengthens management of resources.

7.2 ACL Rules

7.2.1 Creating an ACL Rule and Associating It with Users and Resource Accounts

ACL Rules are used to control users' permissions for accessing resources.

With ACL rules, you can:

- Batch import and export rules.
- Sort command rules by priority. The rule in the upper position has the higher priority than the ones in a lower position.
- Control access to managed resources from a wide range of dimensions, including the validity period, login period, user IP address, file transfer permission, file management permission, RDP clipboard function, keyboard audit, demonstration mode, and operator watermark display function. ACL Rules are used to control users' permissions for resources.
  - Specify the validity period of the policy.
  - Restrict the time period during which the access is allowed or forbidden.
  - IP limit: The policy allows or forbids users with specified IP addresses to access resources. You can configure the IP address whitelist or blacklist.
    - Whitelist: This policy allows only specified IP addresses to access resources.
    - Blacklist: This policy does not allow specified IP addresses to access resources.

- Enable permissions for file transfer. This means you can enable or disable the function to upload files to managed resources or download files from managed resources.
- Enable permissions for file management. This means you can enable or disable the function to view, delete, and edit files on the managed resources.
- Grant permissions to use the RDP clipboard. This means you can enable or disable the RDP clipboard function.
- Keyboard audit: You can enable this function to let the bastion host record all keyboard input information.
- Enable or disable watermarks on the web operation background. The watermark content is the login name of the current system user.
- **Kiosk**: For applications that can be managed through a browser, you can use this function to hide the address bar and disable F12, right-click, and the browser toolbar. You can use F12 instead of Ctrl to implement combined key operations.

Constraints

- To grant the file upload/download permission, enable **File Transmission** and **File Manage**.
- Keyboard audit supports only RDP and VNC protocols.

Prerequisites

You have the operation permissions for the **ACL Rules** module.

Access Control Policy Description

For some types of managed resources, some O&M operations may not be supported in some O&M channels.

For Linux application O&M, version 3.3.40.0 and later support file upload, file download, uplink clipboard, and downlink clipboard.

Feature	Validity Period	File Transfer	Options					Logon Time Limit		IP Limit		Two-person Authorization
	Effective/ Expiration Time	Upload/ Download	File management	Uplink/ Downlink clipboard	Watermarking	Keyboard audit	Kiosk	Permit	Forbid	Blacklist	Whitelist	

SSH H5 O&M	√	√	√	√	√	×	×	√	√	√	√	√
SSH client O&M	√	×	×	×	×	×	×	√	√	√	√	×
RDP H5 O&M	√	√	√	√	√	√	×	√	√	√	√	√
RDP client O&M	√	×	×	×	×	√	×	√	√	√	√	×
Telnet H5 O&M	√	√	√	√	√	×	×	√	√	√	√	√
Telnet client O&M	√	×	×	×	×	×	×	√	√	√	√	×
VNC	√	×	×	×	√	√	×	√	√	√	√	√
FTP	√	√	√	×	×	×	×	√	√	√	√	√
SFTP	√	√	√	×	×	×	×	√	√	√	√	√
SCP	√	×	×	×	×	×	×	√	√	√	√	√
PostgreSQL	√	×	×	×	×	×	×	√	√	√	√	√
GaussDB	√	×	×	×	×	×	×	√	√	√	√	√
DB2	√	×	×	×	×	×	×	√	√	√	√	√
MySQL	√	×	×	×	×	×	×	√	√	√	√	√

SQL Server	√	×	×	×	×	×	×	√	√	√	√	√
Oracle	√	×	×	×	×	×	×	√	√	√	√	√
Rlogin H5 O&M	√	√	√	√	√	×	×	√	√	√	√	√
Rlogin client O&M	√	×	×	×	×	×	×	√	√	√	√	×
Windows application O&M	√	√	√	√	√	√	√	√	√	√	√	√
Linux application O&M	√	√	√	√	√	√	√	√	√	√	√	√

Creating an ACL Rule

Step 1 Log in to your bastion host.

Step 2 Choose **Policy** > **ACL Rules** to enter the ACL rule list page.

Step 3 On the displayed page, click **New** in the upper right corner of the page.

NOTE

You can also select a rule and choose **More** > **Insert** to create an ACL rule. After the configuration is complete, a new rule is created.

Step 4 Configure the basic information.

Table 7-2 Basic information about an ACL rule

Parameter	Description
Rule Name	Name of a user-defined ACL rule. The rule name must be unique in a bastion host.
Period of validity	Effective time and expiration time of an ACL rule
File Transmission	Permission to upload and download files during O&M. If **Upload** or **Download** is selected, **File Manage** must be selected in **Options** for the permission to take effect. • If **Upload** and/or **Download** are selected, files can be uploaded and/or downloaded. • If **Upload** and **Download** are deselected, files cannot be uploaded or downloaded.
Options	Options of the session window function during O&M. After selecting a function, you also need to select the same function for the associated resources to let the selected function work. • **File Manage**: This function allows you to manage file or folder permissions, including the permissions to view, delete, and edit files and folders. **NOTE** – The file management function is available for managed hosts logged using SSH or RDP. – The file management function is unavailable for managed hosts using VNC. To manage files on such host resources, publish certain applications. – The file management function is unavailable for managed hosts using Telnet. • **Uplink clipboard**: This function allows you to copy text through the O&M session RDP clipboard. • **Downlink clipboard**: This function allows you to paste text through the O&M session RDP clipboard. • **Watermark**: This function displays the user login name watermark in the operation session window. • **Keyboard Audit**: This function records the information entered through the keyboard.
Logon Time Limit	Time period during which managed resources can or cannot be accessed.

Parameter	Description
IP Limit	Source IP addresses by which users are allowed or forbidden to access resources. • Select **Blacklist** and configure the IP addresses or IP address range to restrict users from these IP addresses from logging in to the resources. • Select **Whitelist** and configure the IP addresses or IP address range to allow users from these IP addresses to log in to the resources. • If no IP addresses are entered in the field, there is no login restriction on the managed host.

Step 5 Click **Next** and start to relate the command rule to one or more users or user groups.

- You can relate the ACL rule to multiple users or user groups at a time.
- After a user group is related to a command rule, users automatically obtain the permissions of the command rule the instant they are added to the user group.

Step 6 Click **Next** and start to relate the ACL rule to one or more accounts or account groups.

- You can relate an ACL rule to multiple managed resource accounts or account groups at a time.
- After an account group is related to an ACL rule, accounts automatically obtain the permissions of the ACL rule the instant they are added to the account group.

Step 7 Click **OK**. The system switches to the **ACL Rules** list, and you can then view the new ACL rule.

After you relate an ACL rule to users, the authorized users can view and access resources through the **Host Operations** and **App Operations** module.

NOTE

Users in the **Relate User** and **Relate User Group** must have been assigned a role that has the permissions for the **Host Operations** or **App Operations** module. Otherwise, the users cannot view the resource operation modules or access managed resources for operations.

----End

Batch Importing ACL Rules

You can take the following steps to batch import ACL rules:

Step 1 Click  in the upper right corner to download the batch import template and enter the access control policy information.

Step 2 In the dialog box displayed, click **Upload** to upload the completed access control list.

To overwrite the existing rules, select **Override existing opsStrategy**.

NOTE

Only XLS, XLSX, and CSV files can be uploaded.

Step 3 Click **OK**.

----End

Batch Exporting ACL Rules

Click  in the upper right corner of the list to export all data in the list.

Follow-up Operations

In your bastion host, you can manage all ACL rules on the rule list page. For example, you can manage related users and resources, delete, enable, clone, and disable ACL rules, and sort ACL rules by priority.

- To quickly relate a command rule to more users, user groups, accounts, or account groups, select the rule and click **Relate** in the **Operation** column.
- To clone a rule, select the rule and choose **More** > **Clone** in the **Operation** column. Then, you can edit the cloned rule to quickly generate a new rule.
- To delete a command rule, select the rule and click **Delete** in the **Operation** column.
- To disable command rules, select the target rules that have been enabled and click **Disable** at the bottom of the list. When the status of those rules changes to **Disabled**, they become invalid.
- To change the priority of a command rule, select the rule and drag and drop it to an upper or lower position.

7.2.2 Setting Two-person Authorization

Two-person authorization, also known as two-person approval, adds an additional layer of resource security during O&M. After two-person authorization is configured, O&M personnel can access core resources only after being authorized and authenticated by the administrator onsite. Even if the O&M personnel account is lost, the information of business-critical resources will not be disclosed, reducing O&M risks and ensuring the security of critical assets.

Constraints

Only department administrators of the current and superior departments, including the system administrator **admin**, can be selected as the approvers for two-person authorization.

Prerequisites

- You have the operation permissions for the **ACL Rules** module.
- The ACL rule has been related to the system user and managed accounts.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **Policy** > **ACL Rules** to enter the ACL rule list page.

Step 3 Select an ACL rule you want to enable two-person approval, and choose **More** > **Approver** in the **Operation** column. The **Edit Approvers** dialog box is displayed.

Step 4 Select one or more department administrators and set them as approvers of two-person authorization.

Step 5 Click **OK**.

----End

Follow-up Operations

After two-person authorization is successfully configured, double authorization is required when the user related to this rule accesses the resource.

The user needs to select an approver and enter the account password of the approver. The user then can access the resource only after the verification is successful.

7.2.3 Querying and Editing an ACL Rule

You can edit ACL rules to meet your changed O&M needs. For example, if your O&M personnel or resource permissions are changed, you can query involved ACL rules and edit their configurations, including basic permissions, related users, user groups, accounts, and account groups, and approvers of two-person authorization.

- A modified database rule takes effect the instant its status changes to **Enabled**.
- If related users have logged in to resources before the modification, those users need to log out and log in again for the modified database rule to take effect.

Prerequisites

You have the operation permissions for the **ACL Rules** module.

Querying and Editing Database Rule Configurations

Step 1 Log in to your bastion host.

Step 2 Choose **Policy** > **ACL Rules** to enter the ACL rule list page.

Step 3 Query ACL rules.

- Quick search

  Enter a keyword in the search box to quickly query ACL rules by rule name, user, resource name, host IP address, resource account, time limit, or IP address limit.

- Advanced search

Enter keywords in the corresponding attribute search boxes to search for database rules in exact mode.

Step 4 Click the name of the database rule that you want to edit or click **Manage** in the row of the rule in the **Operation** column. The details page of the rule is displayed.

Step 5 View and edit basic information.

In the **Basic Info** area, click **Edit**. In the displayed dialog box, edit the database rule details.

You can modify configurations of **Rule Name**, **Period of validity**, **File Transmission**, **Options**, **Logon Time Limit**, and **IP Limit**.

Step 6 View and edit users related to the rule.

- To relate a user to the rule or remove a related user, click **Edit** in the **Users** area and complete modifications in the displayed dialog box.
- To only remove a related user, click **Remove** in the row of the related user.

Step 7 View and edit user groups related to the rule.

- To relate a user group to the rule or remove a related user group, click **Edit** in the **User Group** area and complete modifications in the displayed dialog box.
- To only remove a related user group, click **Remove** in the row of the related user group.

Step 8 View and edit accounts related to the database rule.

- To relate an account to the rule or remove a related account, click **Edit** in the **Account** area and complete modifications in the displayed dialog box.
- To only remove a related account, click **Remove** in the row of the related account.

Step 9 View and edit account groups related to the rule.

- To relate an account group to the rule or remove a related account group, click **Edit** in the **Account Group** area and complete modifications in the displayed dialog box.
- To only remove a related account group, click **Remove** in the row of the related account group.

Step 10 View and edit two-person authorization.

- To add or remove an approver, click **Edit** in the **Approver** area and complete modifications in the displayed dialog box.
- To only remove an approver, click **Remove** in the row of the approver.

----End

Exporting ACL Rules

Step 1 Log in to your bastion host.

Step 2 Choose **Policy** > **ACL Rules** to go to the ACL rule list page. Select the rules to be exported.

If no ACL rules are selected, all ACL rules will be exported by default.

Step 3 Click  . After the task is created, click **Go to Download Center**. If the export progress reaches 100%, click **Download** in the **Operation** column. Then you can view the exported rules in the downloaded file.

----End

7.3 Command Rules

7.3.1 Creating a Command Rule

Command rules are used to control permissions for critical O&M operations on managed resources, implementing fine-grained control over the execution of commands on Linux hosts.

For hosts using SSH and Telnet protocols, a bastion host can record O&M session operations, trigger dynamic authorization, and disconnect connection to an operation session. A bastion host uses the guacd proxy to audit and filter the commands executed during operations based on the rule configured by the administrator. The proxy will return the audited commands, filtering results, and command output content for session operation recording, dynamic authorization, and disconnection.

With command rules, you can:

- Sort command rules by priority. The rule in the upper position has the higher priority than the ones in a lower position.
- Configure four command execution actions, including permitting, rejecting, requiring dynamic approval, and disconnecting the connection.
  - **Permit**: When a command rule is triggered, the system continues to execute the command. By default, all operations are allowed.
  - **Reject command**: After a command rule is triggered, the system rejects to execute the command and displays a message indicating that the command has been intercepted.
  - **Disconnect**: After a command rule is triggered, the system rejects to execute the command and disconnects the O&M session. The system displays a message indicating that the connection is forcibly disconnected by the administrator.
  - **Dynamic approval**: After a command rule is triggered, the system rejects to execute the command. The system displays a message indicating that the command has been intercepted and asking you to submit a command approval ticket. A command approval ticket is automatically generated. The command can be executed only after the ticket is submitted and approved.

Constraints

Command rules apply only to Linux hosts using the SSH or Telnet protocol for fine-grained permission control.

Prerequisites

You have obtained the permissions to manage the **Cmd Rules** module.

Creating a Command Rule

Step 1 Log in to your bastion host.

Step 2 Choose **Policy** > **Cmd Rules** > **Cmd Rules** to go to the command rule list page.

Step 3 Click **New** in the upper right corner of the page to switch to the **New Command Rule** dialog box.

NOTE

You can also select a command rule and choose **More** > **Insert** to create a command rule. After the configuration is complete, a new rule is created.

Step 4 Configure the basic information.

Table 7-3 Basic information parameters

Parameter	Description
Rule Name	Name of a command rule. The rule name must be unique in a bastion host.
Action	Action executed by the command rule. The options are **Disconnect**, **Reject command**, **Dynamic approval**, and **Permit**. • **Disconnect**: When a session runs the command to bring the rule into effect, the session is disconnected. • **Reject command**: When a session runs the command to bring the rule into effect, the command is rejected directly. • **Dynamic approval**: When a session runs the command to bring the rule into effect, the command is rejected directly. The command must be submitted to the administrator for approval to be executed. • **Permit**: When a session runs the command to bring the rule into effect, the system runs the command.
Period of validity	Effective time and expiration time of the rule
Time Limit	Validity period of a rule

Step 5 Click **Next** and start to relate the command rule to one or more commands or command sets.

- **Relate Command**: Enter one command in each line. You can enter multiple commands. For more details, see **User-defined Commands That Can be Related to a Command Rule**.
- **Relate Command Set**: Relate the command rule to a created command set. For details about command sets, see **Managing Command Sets**.

Step 6 Click **Next** and start to relate the command rule to one or more users or user groups.

- After a user group is related to a command rule, users automatically obtain the permissions of the command rule the instant they are added to the user group.

Step 7 Select a created account or account group.

- After a command rule is related to an account group, accounts automatically obtain the permissions of the rule the instant they are added to the account group.

Step 8 Click **OK**. You can then view the created command rule in the rule list.

During O&M, when a command rule is triggered, the system executes configured actions accordingly.

NOTE

Users in the **Relate User** and **Relate User Group** must have been assigned a role that has ticket approval permissions. Otherwise, users cannot view the command approval ticket module or submit a ticket to obtain required permissions.

----End

Follow-up Operations

In your bastion host, you can manage all command rules on the rule list page, including managing related users or resources, deleting, enabling, or disabling one or more command rules, and sorting command rules by priority.

- To quickly relate a command rule to more users, user groups, accounts, or account groups, select the rule and click **Relate** in the **Operation** column.
- To delete a command rule, select the rule and click **Delete** in the **Operation** column.
- To disable command rules, select the ones you want to disable and click **Disable** at the bottom of the list. When the status of those rules changes to **Disabled**, they become invalid.
- To change the priority of a command rule, select the rule and drag and drop it to an upper or lower position.

7.3.2 Querying and Editing a Command Rule

This topic describes how to view and edit a command rule. You can view and edit the rule configurations, including the basic settings, related passwords, and related command sets. You can also edit the users, user groups, accounts, account groups related to the rule.

- A modified database rule takes effect the instant its status changes to **Enabled**.
- If related users have logged in to resources before the modification, those users need to log out and log in again for the modified database rule to take effect.

Prerequisites

You have obtained the permissions to manage the **Cmd Rules** module.

Querying and Editing Database Rule Configurations

Step 1 Log in to your bastion host.

Step 2 Choose **Policy** > **Cmd Rules** > **Cmd Rules**.

Step 3 Query command rules.

- Quick search

  Enter a keyword in the search box to quickly query command rules by rule name, user, resource name, host IP address, resource account, command set, command, or parameter.

- Advanced search

  Enter keywords in the corresponding attribute search boxes to search for database rules in exact mode.

Step 4 Click the name of the database rule that you want to edit or click **Manage** in the row of the rule in the **Operation** column. The details page of the rule is displayed.

Step 5 View and edit basic information.

In the **Basic Info** area, click **Edit**. In the displayed dialog box, edit the database rule details.

You can edit **Rule Name**, **Period of validity**, **Action**, and **Time Limit**.

Step 6 View and edit commands related to the rule.

- To edit related commands or parameters, click **Edit** in the **Command** area and complete modifications in the displayed dialog box.
- To only delete a related command, click **Remove** in the row of the related command.

Step 7 View and edit command sets related to the command rule.

- To relate a command set to the rule or remove a related command set, click **Edit** in the **Command Set** area and complete modifications in the displayed dialog box.
- To only delete a related command set, click **Remove** in the row of the related command set.

Step 8 View and edit users related to the rule.

- To relate a user to the rule or remove a related user, click **Edit** in the **Users** area and complete modifications in the displayed dialog box.
- To only remove a related user, click **Remove** in the row of the related user.

Step 9 View and edit user groups related to the rule.

- To relate a user group to the rule or remove a related user group, click **Edit** in the **User Group** area and complete modifications in the displayed dialog box.
- To only remove a related user group, click **Remove** in the row of the related user group.

Step 10 View and edit accounts related to the database rule.

- To relate an account to the rule or remove a related account, click **Edit** in the **Account** area and complete modifications in the displayed dialog box.
- To only remove a related account, click **Remove** in the row of the related account.

Step 11 View and edit account groups related to the rule.

- To relate an account group to the rule or remove a related account group, click **Edit** in the **Account Group** area and complete modifications in the displayed dialog box.
- To only remove a related account group, click **Remove** in the row of the related account group.

----End

7.3.3 Managing Command Sets

To relieve you from complicated and repetitive workloads on adding a large number of commands to command rules, a bastion host provides command sets, which include common commands and parameters used for Linux hosts and network devices.

This topic walks you through how to create, view, modify, delete, and batch import command sets.

Prerequisites

You have obtained the permissions to manage the **Cmd Rules** module.

Creating a Command Set

Step 1 Log in to your bastion host.

Step 2 Choose **Policy** > **Cmd Rules** > **CmdSet** to go to the command set list page.

Step 3 Create a command set.

1. Click **New** in the upper right corner of the page to switch to the **New Command Set** dialog box.
2. Configure the command set name.

   The command set name must be unique in a bastion host.
3. Click **OK**. You can then view the new command set on the **CmdSet** tab.

Step 4 Add commands to the command set.

1. In the row of the command set you want to add commands, click **Command** in the **Operation** column. The **Command** dialog box is displayed.
2. Select command sets or a single command.
3. Click **OK**.

----End

Querying and Editing a Command Set

Step 1 Log in to your bastion host.

Step 2 Choose **Policy** > **Cmd Rules** > **CmdSet** to go to the command set list page.

Step 3 Query a command set.

Quick search: Enter a keyword in the search box to quickly query command sets by command set name, command, and/or parameter.

Step 4 Click the command set name or click **Manage** in the row of the command set in the **Operation** column.

Step 5 View and edit basic information.

In the **Basic Info** area, click **Edit**. In the displayed dialog box, edit the basic information.

You can edit **CommandSet Name**. The **Department** cannot be changed.

Step 6 View and edit commands and parameters in the **Command** area.

- To add preset commands or parameters, click **Add** in the **Command** area and select preset commands in the displayed dialog box.
- To delete a command or parameter, locate the row containing the command or parameter you want to delete and click **Remove**.

----End

Deleting a Command Set

Step 1 Log in to your bastion host.

Step 2 Choose **Policy** > **Cmd Rules** > **CmdSet** to go to the command set list page.

Step 3 To delete one command set, click **Delete** in the **Operation** column of the row where the command set locates.

Step 4 To delete multiple command sets at a time, select the ones you want to delete and click **Delete** at the bottom of the list to delete all selected command sets together.

----End

Batch Importing Command Sets

Step 1 Log in to your bastion host.

Step 2 Choose **Policy** > **Cmd Rules** > **CmdSet** to go to the command set list page.

Step 3 Click  in the upper right corner. In the displayed dialog box, download the template.

Step 4 Complete the template. Click **Upload** to import.

You can choose to overwrite existing command sets.

NOTE

Only XLS, XLSX, and CSV files can be uploaded.

Step 5 Confirm the information and click **OK**.

----End

7.3.4 Defining Custom Related Commands

After a custom command is related to a command rule, the bastion host determines whether to execute the command based on the command rule.

Custom related commands are case-sensitive. If the command to execute is inconsistent with the configured one, the command rule will fail to be triggered. The following examples are for your reference:

- Single command format

  If you want to configure a rule to deny the **ls** command, set the related command of the rule to **ls**. The rule is triggered when the single command **ls** is executed.

- Single command and path format

  If you want to configure a rule to dynamically authorize the log query actions, set the related command of the rule to **ls /var/log/**. The rule is triggered when the command **ls /var/log/** is executed. If the **ls /var/log** command is executed, the rule fails to be triggered.

- Commands that contain the wildcard character (*), which indicates one or more characters.

  If you want to configure a rule to deny all deletion commands, set the related command of the rule to **rm ***. The rule is triggered when the command **rm -rf** is executed; while the rule will fail to be triggered if the **rm** command is executed.

- Commands that contain the question mark (?), which indicates any single character. The number of entered question marks indicates the number of unknown characters.

  If you want to configure a rule to deny commands that will delete files or file directories containing two certain characters, set the related command to **rm -rf ??**. The rule is triggered when the command **rm -rf ts** is executed. The rule will fail to be triggered if the **rm -rf test** command is executed.

- Commands that contain a string or any characters enclosed in square brackets ([]) or negated ones in square brackets (using a vertical bar (|) or caret (^) to negate)

  If you want to configure a rule to dynamically approve commands that will delete files or file directories containing any characters in the string "abcd", set the related command of the rule to **rm -rf [abcd]**. The rule is triggered when the command **rm -rf cloud** is executed. The rule will fail to be triggered if the **rm -rf test** or **rm -rf ABCD** command is executed.

7.4 Database Rules

7.4.1 Creating a Database Rule

Database rules are used to intercept sensitive database session operations, implementing fine-grained control over database operations. When an authorized system user logs in to a database related to a database rule, their sensitive operations will be intercepted once the database rule is triggered.

With database rules, you can:

- Sort command rules by priority. The rule in the upper position has the higher priority than the ones in a lower position.
- Configure four command execution actions, including permitting, rejecting, requiring dynamic approval, and disconnecting the connection.
  - Permit: By default, all operations are allowed. After a database rule is triggered, operations in the related regulation set are allowed.
  - Reject: After a database rule is triggered, the system rejects to execute the operation and displays a message indicating that the operation has been intercepted.
  - Disconnect: After a database rule is triggered, the system rejects to execute the operation and disconnects the O&M session. The system displays a message indicating that the connection is forcibly disconnected by the administrator.
  - Dynamic approval: After a database rule is triggered, the system rejects to execute the operation. The system displays a message indicating that the operation has been intercepted and asking you to submit a database approval ticket. A database approval ticket is automatically generated. The command can be executed only after the ticket is submitted and approved.

Constraints

- The database operation audit is available only in professional editions.
- Database rules apply only to MySQL, Oracle, PostgreSQL, and GaussDB databases for fine-grained permission control.

Prerequisites

You have the operation permissions for the **DB Rules** module.

Creating a Database Rule

Step 1 Log in to your bastion host.

Step 2 Choose **Policy** > **DB Rules** > **DB Rules**.

Step 3 In the upper right corner of the page, click **New**.

NOTE

You can also select a database rule and choose **More** > **Insert** to create a database rule. After the configuration is complete, a new rule is created.

Step 4 Configure the basic information.

Table 7-4 Basic information parameters

Parameter	Description
Rule Name	Name of the database rule. The rule name must be unique in a bastion host.
Action	Action executed by the rule. The options are **Disconnect**, **Reject command**, **Dynamic approval**, and **Permit**. • **Disconnect**: When a database rule is triggered, the system automatically disconnects the session. • **Reject command**: When a database rule is triggered, the system directly rejects the command. • **Dynamic approval**: When a database rule is triggered, the system directly rejects the command and requires an approval from the administrator. To continue the execution of the command, the system user needs to submit a ticket to the administrator for approval. • **Permit**: When a database rule is triggered, the system allows the database operation commands to be executed.
Period of validity	Effective time and expiration time of the rule
Time Limit	Validity period of a rule

Step 5 Click **Next** and start to relate the command rule to a rule set.

Select a rule set. For details about command sets, see **Managing Database Rule Sets**.

Step 6 Click **Next** and start to relate the database rule to one or more users or user groups.

After a user group is related to a command rule, users automatically obtain the permissions of the command rule the instant they are added to the user group.

Step 7 Click **Next** and start to relate the database rule to one or more accounts or account groups.

After a database rule is related to an account group, accounts automatically obtain the permissions of the database rule the instant they are added to the account group.

Step 8 Click **OK**. You can then view the created rule in the rule list.

During O&M, when a command rule is triggered, the system executes configured actions accordingly.

NOTE

Users in the **Relate User** and **Relate User Group** panes must have a role that has database ticket approval permissions assigned to them. Otherwise, users cannot view the database approval ticket module or submit a ticket to obtain required permissions.

----End

Follow-up Operations

In your bastion host, you can manage all database rules on the rule list page, including managing related users or resources, deleting, enabling, or disabling one or more command rules, and sorting command rules by priority.

- To quickly relate a command rule to more users, user groups, accounts, or account groups, select the rule and click **Relate** in the **Operation** column.
- To delete a command rule, select the rule and click **Delete** in the **Operation** column.
- To disable command rules, select the ones you want to disable and click **Disable** at the bottom of the list. When the status of those rules changes to **Disabled**, they become invalid.
- To change the priority of a command rule, select the rule and drag and drop it to an upper or lower position.

7.4.2 Querying and Editing a Database Rule

This topic describes how to view and edit a database rule. You can view and edit rule configurations, including basic settings, related regulation sets, users, user groups, accounts, and account groups.

- A modified database rule takes effect the instant its status changes to **Enabled**.
- If related users have logged in to resources before the modification, those users need to log out and log in again for the modified database rule to take effect.

Prerequisites

You have the operation permissions for the **DB Rules** module.

Querying and Editing Database Rule Configurations

Step 1 Log in to your bastion host.

Step 2 Choose **Policy** > **DB Rules** to go to the **DB Rules** page.

Step 3 Query database rules.

- Quick search

  Enter a keyword in the search box to quickly query database rules by rule name, user, resource name, host IP address, resource account, and regulation set name.

- Advanced search

Enter keywords in the corresponding attribute search boxes to search for database rules in exact mode.

Step 4 Click the name of the database rule that you want to edit or click **Manage** in the row of the rule in the **Operation** column. The details page of the rule is displayed.

Step 5 View and edit basic information.

In the **Basic Info** area, click **Edit**. In the displayed dialog box, edit the database rule details.

You can edit **Rule Name**, **Period of validity**, **Action**, and **Time Limit**.

Step 6 View and edit regulation sets related to the rule.

- To relate a regulation set to the rule or remove a related regulation set, click **Edit** in the **RegSet** area and complete modifications in the displayed dialog box.
- To only delete a related regulation set, click **Remove** in the row of the related regulation set.

Step 7 View and edit users related to the rule.

- To relate a user to the rule or remove a related user, click **Edit** in the **Users** area and complete modifications in the displayed dialog box.
- To only remove a related user, click **Remove** in the row of the related user.

Step 8 View and edit user groups related to the rule.

- To relate a user group to the rule or remove a related user group, click **Edit** in the **User Group** area and complete modifications in the displayed dialog box.
- To only remove a related user group, click **Remove** in the row of the related user group.

Step 9 View and edit accounts related to the database rule.

- To relate an account to the rule or remove a related account, click **Edit** in the **Account** area and complete modifications in the displayed dialog box.
- To only remove a related account, click **Remove** in the row of the related account.

Step 10 View and edit account groups related to the rule.

- To relate an account group to the rule or remove a related account group, click **Edit** in the **Account Group** area and complete modifications in the displayed dialog box.
- To only remove a related account group, click **Remove** in the row of the related account group.

----End

7.4.3 Managing Regulation Sets

You can create regulation sets for quickly adding a large number of database rules, relieving you from complicated and repetitive workloads.

There are 29 preconfigured common database operation commands, including **ALTER**, **TRUNCATE**, **EXECUTE**, **INSERT**, **DELETE**, **UPDATE**, **SELECT**, **GRANT**, **REVOKE**, **HANDLER**, **DEALLOCATE**, **SET**, **COMMIT**, **ROLLBACK**, **PREPARE**,

CREATEINDEX, **DROPINDEX**, **CREATEFUNCTION**, **DROPFUNCTION**, **CREATEVIEW**, **DROPVIEW**, **CREATEDATABASE**, **DROPDATABASE**, **CREATEPROCEDURE**, **DROPPROCEDURE**, **CREATETABLE**, **DROPTABLE**, **CALL**, and **ACCESS**.

This topic walks you through how to create, view, modify, and delete a regulation set.

Prerequisites

You have the operation permissions for the **DB Rules** module.

Creating a Regulation Set

Step 1 Log in to your bastion host.

Step 2 Choose **Policy** > **Database Rules** > **RegSet** to go to the DB rule list.

Step 3 Create a regulation set.

1. In the upper right corner of the page, click **New**.
2. Configure the **RegSet name** and specify a protocol.
   - The **RegSet Name** must be unique in a bastion host.
   - Currently, MySQL, Oracle, PostgreSQL, GaussDB, and DM are supported. The protocol type cannot be changed after being configured.
3. Click **OK**. You can then view new regulation set on the list page.

Step 4 Add database rules.

1. In the row of the command set you want to add rules, click **Add regulation** in the **Operation** column.
2. Add libraries, tables, and commands for the regulation set.

Table 7-5 Parameters for adding regulation

Parameter	Description
Lib	This parameter is optional. It can be set to a regular expression to match the library name. By default, all SQL statements that use this command are intercepted.
Table	This parameter is optional. It can be set to a regular expression to match the table name. By default, all SQL statements that use this command are intercepted.
Cmd	This parameter is mandatory. Select at least one preset command. Currently, 29 commands are available. You can select multiple commands.

3. Click **OK**.

----End

Querying and Editing a Regulation Set

Step 1 Log in to your bastion host.

Step 2 Choose **Policy** > **Database Rules** > **RegSet** to go to the DB rule list.

Step 3 Query the regulation sets.

Quick search: Enter a keyword in the search box and search for regulation sets by regulation set name.

Step 4 Click the name of a regulation set you want to edit or click **Manage** in the row of the regulation set in the **Operation** column.

Step 5 View and edit basic information.

In the **Basic Info** area, click **Edit**. In the displayed dialog box, edit the basic information.

You can edit **RegSet name**. The **Protocol** and **Department** cannot be changed.

Step 6 Query and edit a regulation set in the **Regulation** area.

- To add a library, table, or command to a regulation set, click **Add** and then complete modifications in the displayed dialog box.
- To delete a regulation set, locate the row and click **Remove**.

----End

Deleting a Regulation Set

Step 1 Log in to your bastion host.

Step 2 Choose **Policy** > **Database Rules** > **RegSet** to go to the DB rule list.

Step 3 To delete one regulation set, click **Delete** in the **Operation** column of the row where the regulation set locates to delete it.

Step 4 To delete several regulation sets together, select the ones you want to delete and click **Delete** at the bottom of the list to delete all selected regulation sets together.

----End

7.5 Password Rules

7.5.1 Creating a Password Rule

With password rules, you can let the bastion host periodically change the passwords of multiple managed host resources at a time, improving the managed resource account security.

With password rules, you can:

- Change passwords of managed resource accounts manually, periodically, or at a scheduled time.
- Change the passwords of multiple managed resource accounts to different passwords randomly generated by the system, the same password generated by the system, or the same password you specify.

Constraints

- Password rules apply only to hosts configured with SSH, MySQL, SQL Server, Oracle, RDP, or Telnet protocols.
- To enable a password change rule for Windows hosts, enable the SMB service and open port 445 in the security group.
- Windows 10 does not support password change in SMB mode. Before associating a Windows 10 resource account, you need to configure WinRM and create a password rule. For details about how to configure server parameters, see **Setting Parameters of Windows 10 Servers**.

Prerequisites

- You have the operation permissions for the **Password Rules** module.
- The configured OS type of the resource whose account password you want to change must be the same as the actual OS type of the resource.
- The login mode for resource accounts in a password rule must be automatic login or privilege escalation login. Otherwise, the corresponding account cannot be selected during policy creation.

Creating a Password Change Rule

Step 1 Log in to your bastion host.

Step 2 Choose **Policy** > **Password Rules** > **Password Rule**.

Step 3 Click **New** in the upper right corner of the page to switch to the **New ChangePassword Rule** dialog box.

Step 4 Configure the basic information.

Table 7-6 Parameter for password rules

Parameter	Description
Rule Name	Name of a password rule. The rule name must be unique in a bastion host.

Parameter	Description
Timing	The options are **Manual**, **Fixed-Time**, and **Cycle**. • **Manual**: Manually trigger the password rule to change the password of the managed resource account. • **Fixed-Time**: The password change rule is triggered by the bastion host to change the password of the managed resource account at a fixed time. This type of rule is executed only once. • **Cycle**: The password rule is periodically triggered by the bastion host to change the passwords of the managed resource accounts. This type of password change rule is triggered periodically.
Execute Time	Date when the password rule is executed. The default execution time is at 00:00 every day.
Cycle	The cycle for password changes. Then, you can preview when the latest five password changes happened in **Time Preview**. **NOTE** • The unit is day. If a positive integer containing more than eight digits is entered, the execution time cannot be previewed. • You need to set the **End Time** for this type of rules. Otherwise, the rule will be executed indefinitely.
Method	How the password is changed. The options are **Generate different passwords**, **Generate the same password**, and **Specify the same password**. • Generating a different password: The system randomly generates different passwords for managed resource accounts in compliance with password requirements. • Generating the same password: Randomly generate the same password for managed resource accounts in compliance with password requirements. • Specifying the same password: You need to manually enter a preset password. Enter the password as prompted. **NOTE** A password randomly generated by a bastion host contains 20 characters, including uppercase letters, lowercase letters, digits, and the following special characters %, -, _, and? A random password must contain at least an uppercase letter, a lowercase letter, and a special character.

Parameter	Description
Options	The following options are supported: • **Allow to change the sudo account password**: To change the password of sudo account, select this option, or the password of the sudo account cannot be changed. This option is not selected by default. • **Priority use of the sudo account to change password**: To let the system automatically search for the corresponding sudo account and use it to change the account password, select this option. If no sudo account is available, the password can be changed using the current account. This option is selected by default. • **Allow to change the SSH Key**: To let the system automatically change SSH public keys, select this option. **NOTE** • The **Allow to change the SSH Key** option is supported in version 3.3.36.0 and later only. To use this function, upgrade your bastion host instance to the latest version by referring to **Upgrading the Instance Version**. • If you select the key pair automatic login mode when managing host resources, enable **Allow to change the SSH Key**, or manual password change may fail.

Step 5 Click **Next** and start to relate the ACL rule to one or more accounts or account groups.

- After a password rule is related to an account group, accounts automatically obtain the permissions of the rule the instant they are added to the account group.
- If a password change rule is related to multiple managed resource accounts, batch changing passwords is available.

Step 6 Click **OK**. You can then view the new password rule in the rule list.

To obtain the new password of the managed resource accounts, export host resource details by referring to **Batch Exporting Host Resources**.

Step 7 Click **Execute** in the **Operation** column. In the dialog box displayed, confirm the execution. The policy updates passwords immediately.

----End

Setting Parameters of Windows 10 Servers

Step 1 Log in to a Windows 10 server.

Step 2 Start the Windows Remote Management (WinRM) service.

1. Search for **Windows Components**.
2. In the navigation pane on the left, choose the local service. In the window displayed on the right, locate **Windows Remote Management(WS-Management)**.

3. Right-click **Windows Remote Management(WS-Management)** and choose **Start** from the shortcut menu.

Step 3 Configure WinRM.

1. Run the **cmd** command as the administrator and run the following command:
```
winrm qc
```
2. Perform twice. After the command output is displayed, enter **y** as prompted.
3. Run the following commands:
```
winrm set winrm/config/service '@{AllowUnencrypted="true"}'
```
4. Run the following commands:
```
winrm set winrm/config/service/auth '@{Basic="true"}'
```

Step 4 (Skip this step if you are already an administrator.) Run the following command to add a user to the user group:

For example, run the following command to add **appuser01** to the user group:

```
net localgroup "Remote Management Users"  appuser01  /add
```

Step 5 In the power shell dialog box, run the following command to add a firewall:

```
New-NetFirewallRule -DisplayName "WinRM-5985" -Direction Inbound -LocalPort 5985 -Protocol TCP -Action Allow
```

----End

Follow-up Operations

You can manage all password rules on the rule list page, including managing related resources, deleting, enabling, or disabling one or more password change rules, and immediate execution of a password change rule.

- To quickly relate a synchronization rule to more accounts or account groups, select the rule and click **Relate** in the **Operation** column.
- To delete a command rule, select the rule and click **Delete** in the **Operation** column.
- To disable password rules, select the ones you want to disable and click **Disable** at the bottom of the list. When the status of those rules changes to **Disabled**, they become invalid.
- To change the password of a managed account immediately, click **Execute** in the **Operation** column.

7.5.2 Querying and Editing a Password Rule

You can edit password rules to meet your changed O&M requirements. For example, you can edit when and how a password rule is executed and which accounts, account groups, and resources a password rule is used for.

A modified database rule takes effect the instant its status changes to **Enabled**.

Prerequisites

You have the operation permissions for the **Password Rules** module.

Querying and Editing Rule Configurations

Step 1 Log in to your bastion host.

Step 2 Choose **Policy** > **Password Rules** > **Password Rule**.

Step 3 Query password rules.

- Quick search

  Enter a keyword in the search box to quickly query password rules by rule name, resource name, and account.

- Advanced search

  Enter keywords in the corresponding attribute search boxes to search for database rules in exact mode.

Step 4 Click the name of the rule that you want to edit or click **Manage** in the row of the rule in the **Operation** column. The details page of the rule is displayed.

Step 5 View and edit basic information.

In the **Basic Info** area, click **Edit**. In the displayed dialog box, edit the database rule details.

- You can edit **Rule Name**, **Timing**, **Method**, and **Options**.
- The **Department** cannot be modified.

Step 6 View and edit accounts related to the database rule.

- To relate an account to the rule or remove a related account, click **Edit** in the **Account** area and complete modifications in the displayed dialog box.
- To only remove a related account, click **Remove** in the row of the related account. The rule becomes invalid for the deleted account.

Step 7 View and edit account groups related to the rule.

- To relate an account group to the rule or remove a related account group, click **Edit** in the **Account Group** area and complete modifications in the displayed dialog box.
- To only remove a related account group, click **Remove** in the row of the related account group. The rule becomes invalid for all accounts in the deleted account group.

----End

7.5.3 Managing Password Logs

After a password rule is executed, logs are generated accordingly. You can view the password change details in password logs.

Prerequisites

You have the operation permissions for the **Password Rules** module.

Viewing Log Details

Step 1 Log in to your bastion host.

Step 2 Choose **Policy** > **Password Rules** > **Password Log** to view and manage password logs.

Step 3 Query password logs.

Quick search: Enter a keyword in the search box and search for password change logs by rule name.

Step 4 Select the password log and click **Detail**.

You can view the log content, including the basic information and password change result.

Figure 7-1 Viewing password log details

----End

Downloading Password Logs

Step 1 Log in to your bastion host.

Step 2 Choose **Policy** > **Password Rules** > **Password Log** to view and manage password logs.

Step 3 Click **Download**.

Step 4 Confirm downloading information.

1. **Set encryption password**: This parameter is optional. If this parameter is not set, the downloaded password log is an unencrypted CSV file. If you set a password, the downloaded password change log is an encrypted .zip file.
2. **User Password**: This parameter is mandatory. You need to enter the login password of the current user and then the password change log can be downloaded only after the verification is successful. This ensures password security of managed host accounts.
3. Click **OK** to download the file locally.

----End

Deleting Execution Logs

Step 1 Log in to your bastion host.

Step 2 Choose **Policy** > **Password Rules** > **Password Log**.

Step 3 To delete one execution log, select the one you want and click **Delete** in the **Operation** column to delete it.

Step 4 To delete multiple execution logs at a time, select the ones you want and click **Delete** at the bottom of the list to delete all selected logs together.

----End

7.6 Account Synchronization Rules

7.6.1 Creating a Synchronization Rule

Synchronization rules are used to automatically synchronize managed host accounts, making it easier for you to manage accounts of managed hosts, delete zombie accounts, and discover accounts that are not managed in a timely manner. This further strengthens management of resources.

With synchronization rules, you can:

- Synchronize accounts from managed hosts manually, periodically, or at a scheduled time.
- Pull accounts from managed hosts, check the validity of pulled accounts, and update the managed resource account status.
- Update the password of a host account, create a host account, or delete invalid host accounts by pushing managed resource account information to the corresponding hosts.

Constraints

- The account synchronization is supported only in professional editions.
- Account synchronization rules apply only to hosts using the SSH protocol.
- Only one managed resource account is allowed to log in to a managed host and pull its account information.

Prerequisites

You have the operation permissions for the **Sync Rules** module.

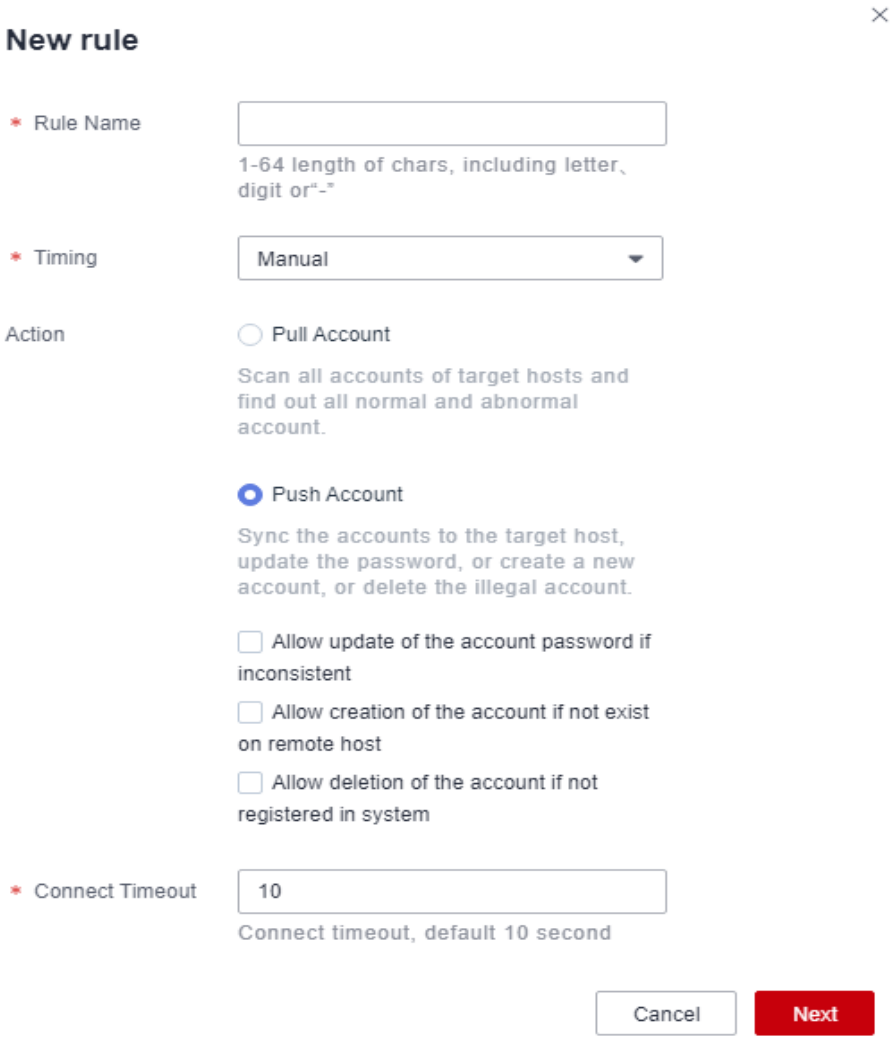
Creating a Synchronization Rule

Step 1 Log in to your bastion host.

Step 2 Choose **Policy** > **Sync Rules** > **Sync Rules**.

Step 3 Click **New** in the upper right corner of the **Sync Rule** area to switch to the **New rule** dialog box.

Figure 7-2 New rule



Step 4 Configure the basic information.

Table 7-7 Parameters for configuring an account synchronization rule

Parameter	Description
Rule Name	Name of an account synchronization rule. The rule name must be unique in a bastion host.

Parameter	Description
Timing	The options are **Manual**, **Fixed-Time**, and **Cycle**. You need to configure the execution time if **Fixed-Time** or **Cycle** is selected. • **Manual**: Manually trigger the rule to change the password of the managed resource accounts. • **Fixed-Time**: The rule is triggered by the bastion host to change the password of the managed resource account at a fixed time. This type of rule is executed only once. • **Cycle**: The rule is periodically triggered by the bastion host to change the password of the managed resource account. This type of rule is triggered periodically.
Execute Time	Date when a policy is periodically executed. The default execution time is at 00:00 every day.
Cycle Frequency	Account synchronization frequency. • The options are every minute, every hour, every day, every week, and every month. • You need to set the **End Time** for this type of synchronization rules. Otherwise, the rule will be executed indefinitely.
Action	Synchronization mode. By default, **Pull Account** is selected. • **Pull Account**: Scans all accounts of a host and collects statistics on all normal and abnormal accounts. • **Push Account**: Pushes accounts to a host to automatically update account passwords, create accounts, or delete invalid accounts of the host. **NOTE** When the synchronization mode is set to push account, the following three options are available: – If the account and password are inconsistent, the password can be updated. – If the account does not exist, the account can be created. – If a non-managed account exists on the host, the account can be deleted.
Connect Timeout	Timeout interval for connecting to a managed host. If the connection times out, the account synchronization task is interrupted. The default value is 10 seconds.

Step 5 Click **Next** and start to relate the synchronization rule to one or more accounts or account groups.

Only one account can be configured for each host to execute synchronization tasks.

Step 6 Click **OK**. You can then view the new synchronization rule in the rule list.

To obtain the account synchronization details, **download the synchronization logs** after the synchronization.

----End

Follow-up Operations

You can manage all synchronization rules on the rule list page, including managing related resources, deleting, enabling, or disabling one or more synchronization rules, and immediately executing a synchronization rule.

- To quickly relate a synchronization rule to more accounts or account groups, select the rule and click **Relate** in the **Operation** column.
- To delete a command rule, select the rule and click **Delete** in the **Operation** column.
- To disable synchronization rules, select the ones you want to disable and click **Disable** at the bottom of the list. When the status of those rules changes to **Disabled**, they become invalid.
- To execute a synchronization rule immediately, click **Execute** in the **Operation** column.

7.6.2 Querying and Editing a Synchronization Rule

You can edit a synchronization rule to meet your changed requirements. For example, you can edit when and how a synchronization rule is executed and which accounts, account groups, and resources a synchronization rule is used for.

A modified rule takes effect the instant its status changes to **Enabled**.

Prerequisites

You have the operation permissions for the **Sync Rules** module.

Querying and Editing Rule Configurations

Step 1 Log in to your bastion host.

Step 2 Choose **Policy** > **Sync Rules** > **Sync Rules**.

Step 3 Query account synchronization rules.

- Quick search

  Enter a keyword in the search box to quickly query rules by rule name, resource name, and account,

- Advanced search

  Enter keywords in the corresponding attribute search boxes to search for rules in exact mode.

Step 4 Click the name of the rule that you want to edit or click **Manage** in the row of the rule in the **Operation** column. The details page of the rule is displayed.

Step 5 View and edit basic information.

In the **Basic Info** area, click **Edit**. In the displayed dialog box, edit the rule details.

- You can edit **Rule Name**, **Timing**, and **Action**.
- The **Department** cannot be modified.

Step 6 View and edit accounts related to the rule.

- To relate an account to the rule or remove a related account, click **Edit** in the **Execute Account** area and complete modifications in the displayed dialog box.
- To only remove a related account, click **Remove** in the row of the related account. The removed account then cannot be used for synchronizing accounts of the corresponding host.

Step 7 View and edit account groups related to the rule.

- To relate an account group to the rule or remove a related account group, click **Edit** in the **Account Group** area and complete modifications in the displayed dialog box.
- To only remove a related account group, click **Remove** in the row of the related account group. Each account in the removed account group cannot be used for synchronizing accounts of the corresponding host.

----End

7.6.3 Managing Synchronization Execution Logs

After a synchronization rule is executed, execution logs are generated accordingly. You can view the account synchronization result in the execution logs, including the synchronized account information, new account information, and deleted account information.

Prerequisites

You have the operation permissions for the **Sync Rules** module.

Viewing Log Details

Step 1 Log in to your bastion host.

Step 2 Choose **Policy** > **Sync Rules** > **Sync Log**.

Step 3 Query OM task execution logs.

Quick search: Enter a keyword in the search box and search for execution logs by rule name.

Step 4 Select the execution log and click **Detail**.

You can view the basic information, host details, account list for synchronizing passwords, and account list for synchronizing SSH keys.

Figure 7-3 Viewing the basic information

----End

Downloading OM Task Execution Logs

Step 1 Log in to your bastion host.

Step 2 Choose **Policy** > **Sync Rules** > **Sync Log**.

Step 3 Select the execution log and click **Download** to download the log in CSV format.

----End

Deleting Execution Logs

Step 1 Log in to your bastion host.

Step 2 Choose **Policy** > **Sync Rules** > **Sync Log**.

Step 3 Select an execution log and click **Delete** in the row to delete it.

Step 4 To delete multiple execution logs at a time, select the ones you want and click **Delete** at the bottom of the list to delete all selected logs together.

----End

8 Resource Operation

8.1 Host Resource Operation

8.1.1 Configuring Host Resource Operations

After obtaining the access permissions for host resources, you can view authorized host resources in the host operation list and set labels and operation method for host resources.

You can configure operation methods such as H5 pages, clients, and primary/secondary accounts based on protocols you configure for specific host resources.

- H5 page operations: Browser pages are used for resource operations.
- Client operations: A client is automatically enabled by your bastion host for resource operations.
- Primary/secondary account operations: Resource accounts and passwords are managed by bastion hosts. You need to manually start the client and log in to the target resources with the accounts and passwords to perform resource operations.

Constraints

- Labels cannot be shared with others. You can define your own resource labels for your exclusive use.
- Downloading login configuration is supported by only resources managed over SSH.

Prerequisites

- You have the management permissions for the **Host Operations** module.
- You have obtained the access permissions for the resources.

Viewing the Host Resource List

Step 1 Log in to your bastion host.

Step 2 Choose **Operation** > **Host Operations** to go to the **Host Operations** page.

Quick search: You can quickly search for a specific resource by automatic recognition, host name, or host address.

----End

Configuring a Resource Label

You can use custom labels to group host resources for quick operations.

Step 1 In the host resource list, select the target resource and click in the **Label** column.

To add labels for a batch of resources, select target resources and click **Add Label** in the lower left corner of the list.

Step 2 Enter a label type and press **Enter** or select an existing label type.

Step 3 Click **OK**. You can check the added label on the **Host Operations** page.

To delete a resource label, select one or more resources and click **Delete Label** in the lower left corner of the list. In the displayed dialog box, confirm the information and click **OK**.

----End

Configuring Web Operations

On the host operations page, you can set the operation method to RDP, SSH, or FTP/SFTP.

Step 1 Go to the **Host Operations** page and click **Web OPS Settings** in the upper right corner.

Step 2 In the dialog box displayed, select a protocol and then select an operation method.

- Currently, the supported protocols include RDP, SSH, and FTP/SFTP.
  - RDP and SSH: support H5 page and client operations.
  - FTP/SFTP: support primary/secondary account and client operations.
- You can configure operation methods such as H5 pages, clients, and primary/secondary accounts based on protocols you configure for specific host resources.
  - H5 page operations: Browser pages are used for resource operations.
  - Client operations: A client is automatically enabled by your bastion host for resource operations.
  - Primary/secondary account operations: Resource accounts and passwords are managed by bastion hosts. You need to manually start the client and log in to the target resources with the accounts and passwords to perform resource operations.
- If you select the RDP protocol, you can specify the connection type. For details, see **Enabling Forcible RDP Connections**.

Step 3 Check the information and click **OK**.

----End

Downloading the Host Configuration File

If you use the SecureCRT or XShell client to operate SSH resources, download the configuration file by referring to this section.

Step 1 Go to the **Host Operations** page and click **Export Host Configuration** in the upper right corner.

Step 2 In the dialog box displayed, select the login configuration download item and the corresponding encoding format.

- Login configuration download: Only the SecureCRT and XShell clients can be selected.
- File encoding format: Select the encoding format of the file to be downloaded. You are advised to select the encoding format used by the local client.

Step 3 Confirm the information and click **OK** to start the download.

----End

8.1.2 Using a Web Browser to Log In to Resources for O&M

After you log in to a host resource using a web browser, the cooperation, file management, file transfer, and command preset functions are available for you. A bastion host can log all activities performed on a host resource. The logs can be used for audits.

- Cooperation: This function allows the session initiator to invite other system users to participate the current session by sharing the session link with them, implementing O&M collaboration.
- File management: If you participate in a session and have operation permissions for this function, on the pane on the right of the session, you can manage files or folders on managed hosts and net disks on them. You can:
  - Create new folders.
  - Change the name of a file or folder.
  - Delete files or folders in batches.
- File transfer: This function allows session participants to download or upload files or folders on the host or host net disk after they obtain the operation permissions. They can:
  - Upload and download files.
  - Upload folders.
  - Upload multiple files on a local server or net disk to a host or download multiple files from a host to a local server or net disk, if **Host Files** is selected as the destination address.
  - Upload multiple files or a folder to a host net disk or download multiple files from a host net disk to a local host, if **Netdisk** is selected as the destination address.

This topic describes how to log in to a host using a web browser and how to perform operations in the session window of the hosts using character or image protocols.

Notes

During O&M, bastion hosts automatically record videos for audit. To prevent sensitive information leakage, do not enter sensitive information that is displayed in plaintext during O&M.

Constraints

- Only hosts using character protocols (SSH and Telnet) or image protocols (RDP and VNC) can be logged in using a web browser.
- The file transfer and management functions are unavailable for hosts using the Telnet protocol.
- Although using a web browser for O&M allows you to copy and paste a large number of characters without garbled characters, a maximum of 80,000 characters can be copied from the local to the remote, and a maximum of 1000,000 of bytes can be copied from the remote to the local.
- If you log in to a bastion host as a non-admin user and want to manage Windows host resources, deselect the admin console. To do so, go to the **Operation** > **Host Operations** page, click **Web OPS Settings** in the upper right corner, then deselect **admin console**.
- File management

  Files and folders cannot be edited in batches.
- File Transmission
  - By default, the system supports the upload of a single file with a maximum size of 100 GB. However, the size of a single file to be uploaded is limited by the **Personal Netdisk** space and browser type.

    NOTE

    If the disk space is insufficient, the upload will fail. In this case, you need to clear the disk or expand the disk capacity.
  - Folders cannot be downloaded.
  - For the hosts using the RDP protocol, only **Netdisk** can be select as the destination address.

Prerequisites

- You have the management permissions for the **Host Operations** module.
- You have obtained the access permissions for the resources.
- The network connection between the managed host and the system is normal, and the account username and password for logging in to the managed host are correct.

Procedure

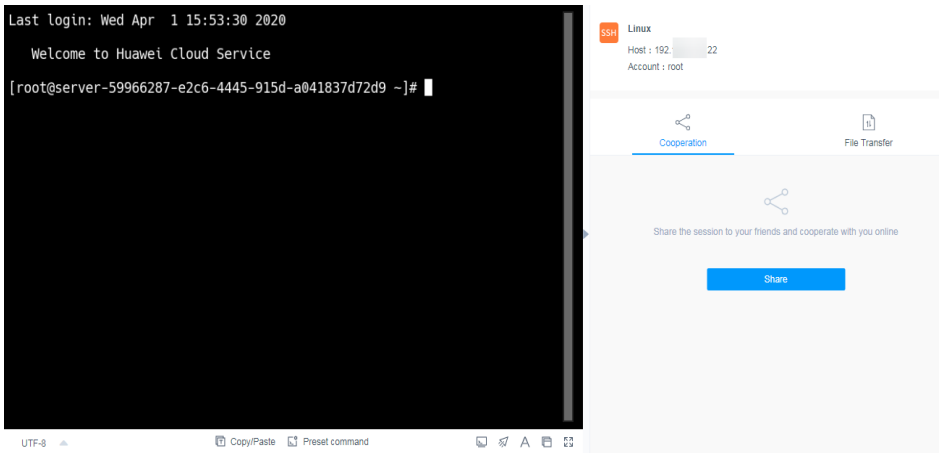
Step 1 Log in to your bastion host.

Step 2 Choose **Operation** > **Host Operations** to go to the **Host Operations** page.

Step 3 Select the host you want and click **Login** in the **Operation** column to open the session.

- **Session Window of Hosts Using the RDP or VNC Protocol**
- **Session Window of Hosts Using the SSH or Telnet Protocol**

Figure 8-1 Session window of hosts using the SSH protocol



Step 4 Invite other system users to participate in the current session. For details, see **Cooperation**.

1. Click **Cooperation**. The collaborative session window is displayed.
2. Click **Share**. Complete the information in the displayed **Invite friends** dialog box.

   NOTE

   - The URL link can be copied and sent to multiple users.
   - Only users with the access permission can access the bastion host. Otherwise, a connection error will be reported, indicating that the connection has been disconnected because the server does not respond for a long time. Check your network settings and try again (Code: T_514).
3. Copy the link and send it to the users whom you want to invite. The users must have the access permission assigned. Once they receive the link, they can log in to the bastion host, open a web browser, and enter the link to open it in the web browser.
4. If you are invited, click **Enter** to join the session.

Table 8-1 Parameters for session operation

Parameter	Description
Apply for control	The invited user can apply for control from the invitation sender. Once approved, the invited user can control the current session.
Exit session	Exit the current session.

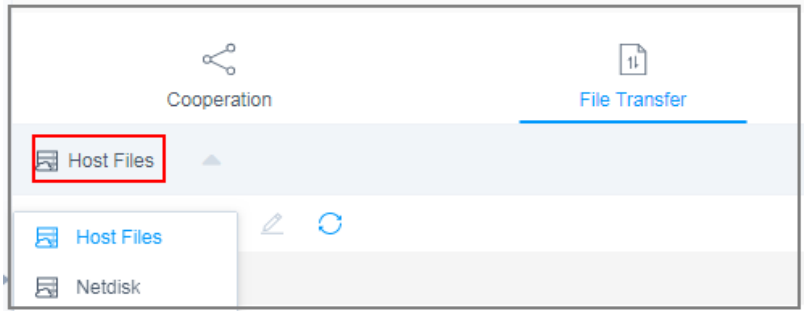
Step 5 Upload files to or download files from the host or host net disk. For details, see **File Transfer**.

1. Click **File Transfer**. The **File Transfer** window is displayed.

Figure 8-2 File Transmission

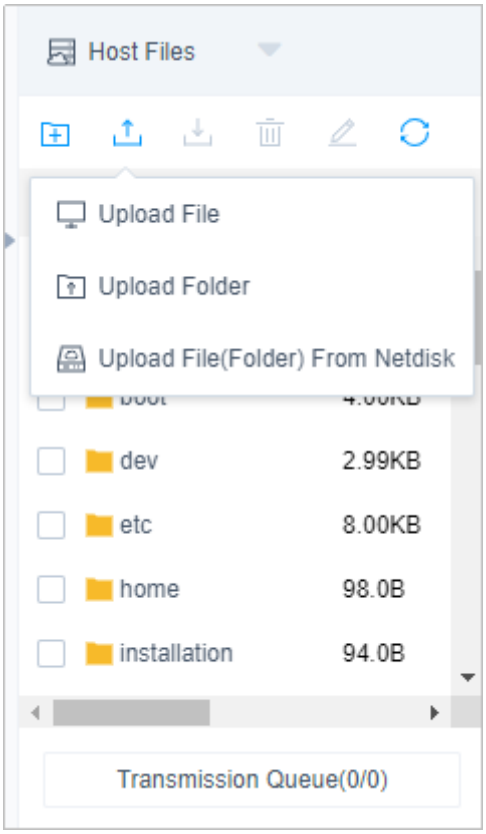
2. **Host Files** is selected by default. You can click **Host Files** to switch the destination address to **Netdisk**.

Figure 8-3 Switchover of destination address



3. Click  to upload a file.
4. Select a file and click  to download a file.

Figure 8-4 Uploading files



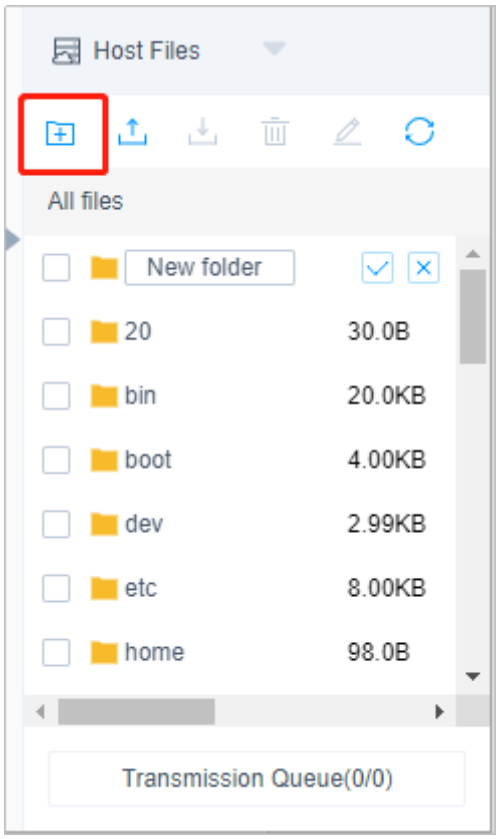
NOTE

- **Netdisk** is dedicated for your exclusive use. It cannot be accessed by other users. You can transfer files from **Netdisk** to multiple hosts without worries of data leakage.
- The default file storage path of Windows servers is drive G, and that of Linux servers is the root directory.
- To upload or download files on a Windows server, open the disk directory of the server and copy and paste the file to drive **G** of the Netdisk.

Step 6 In the file management area, manage files or folders on the host or host net disk.

1. Click **File Transfer**. The **File Transfer** window is displayed.
2. Click to create a folder.

Figure 8-5 New folder



3. Select one or more files or folders and click to delete them.
4. Select a file or folder and click to edit its name.
5. Click to refresh all file directories.

----End

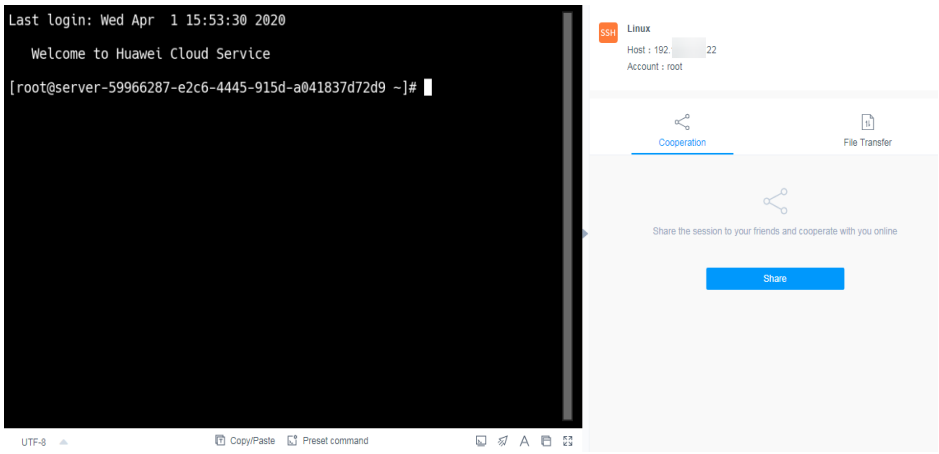
Session Window of Hosts Using the SSH or Telnet Protocol

Table 8-2 Linux host operations

Parameter	Description
Encode	The character protocol supports multiple encoding formats.
Copy/ Paste	Select the characters, press **Ctrl+C** to copy it, and press **Ctrl+V** to paste it.
Preset command	You can preset commands that are long and frequently used.
Terminal Type	The character protocol supports terminal type switching, including Linux and Xterm.

Parameter	Description
Mass sending	When the group sending function is enabled, you can run commands in multiple sessions at the same time.
Font size	There are three types of font sizes: large, medium, and small.
Copy window	You can copy the current session window.
Full screen	Displays the window in full screen.

Figure 8-6 Session window of hosts using the SSH protocol



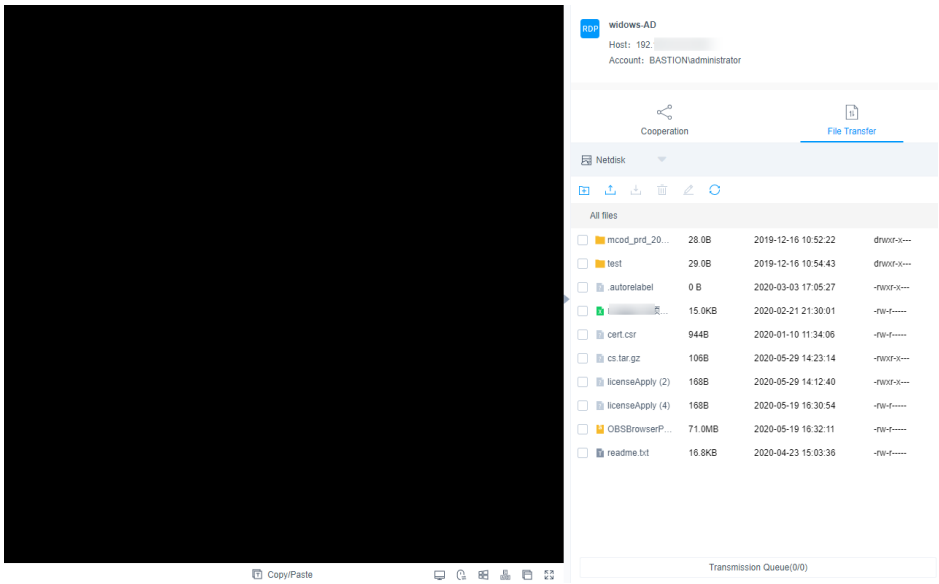
Session Window of Hosts Using the RDP or VNC Protocol

Table 8-3 Windows host operations

Parameter	Description
Copy/ Paste	Remote text: Select the character you want, press **Ctrl+C** twice to copy the character, and press **Ctrl+V** to paste the character. Remote machine files: Select a text or image, press **Ctrl+B** to copy it, and press **Ctrl+G** to paste it. **NOTE** Although using a web browser for O&M allows you to copy and paste a large number of characters without garbled characters, a maximum of 80,000 characters can be copied from the local to the remote, and a maximum of 1000,000 of bytes can be copied from the remote to the local.
Resolution	You can switch the resolution of the current operation interface. During the switching, a new connection is created.

Parameter	Description
Switch to remote mouse	You can switch over between the local mouse and remote mouse.
Windows	This Windows icon can be used for easy access to Windows system functions.
Ctrl+Alt+Delete	Lock the screen.
Copy window	You can copy the current session window.
Full screen	Displays the window in full screen.

Figure 8-7 Session window of hosts using the RDP protocol



8.1.3 Using an SSH Client to Log In to Resources for O&M

You can use an SSH client to log in to managed resources via a bastion host. You do not have to change your habits of using an SSH client. Through SSH client, the command rules and operation audit function are still available.

This topic uses Xshell as an example to describe how to use an SSH client to log in to a resource for O&M and how to download the configuration file of the resource.

Notes

During O&M, bastion hosts automatically record videos for audit. To prevent sensitive information leakage, do not enter sensitive information that is displayed in plaintext during O&M.

Constraints

- Logging using an SSH client is used only for hosts using the SSH, Telnet, or Rlogin protocol. For hosts using the Rlogin protocol, only an SSH client can be used for logins.
- Supported SSH clients include SecureCRT 8.0 or later, Xshell 5 or later, PuTTY, and MAC Terminal 2.0 or later.
- The following table lists the servers supported by different algorithm types in different scenarios.

Table 8-4 Servers supporting SSH O&M

Algorithm Type	HTML5 (H5) O&M	SSH Client
Key exchange	• diffie-hellman-group-exchange-sha256 • diffie-hellman-group-exchange-sha1 • diffie-hellman-group14-sha1 • diffie-hellman-group1-sha1 • ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521 • curve25519-sha256 • curve25519-sha256@libssh.org • diffie-hellman-group14-sha256	• diffie-hellman-group-exchange-sha256 • diffie-hellman-group-exchange-sha1 • diffie-hellman-group14-sha1 • diffie-hellman-group1-sha1 • ecdh-sha2-nistp521 • ecdh-sha2-nistp384 • ecdh-sha2-nistp256

Algorithm Type	HTML5 (H5) O&M	SSH Client
Encryption	• aes128-ctr • aes192-ctr • aes256-ctr • aes128-cbc • aes192-cbc • aes256-cbc • 3des-cbc • blowfish-cbc • arcfour128 • arcfour • cast128-cbc • 3des-cbc • rijndael-cbc@lysator.liu.se	• aes128-ctr • aes192-ctr • aes256-ctr • aes128-cbc • aes192-cbc • aes256-cbc • 3des-cbc • blowfish-cbc • arcfour128 • arcfour256
HMAC	• hmac-md5 • hmac-md5-96 • hmac-sha1 • hmac-sha1-96 • hmac-sha2-256 • hmac-sha2-512 • hmac-ripemd160 • hmac-ripemd160@openssh.com	• hmac-md5 • hmac-md5-96 • hmac-sha1 • hmac-sha1-96 • hmac-sha2-256 • hmac-sha2-512
Host Key	• ssh-rsa • ssh-dss • ecdsa-sha2-nistp256 • ecdsa-sha2-nistp384 • ecdsa-sha2-nistp521 • ssh-ed25519	• ssh-rsa • ssh-dss • rsa-sha2-256 • rsa-sha2-512 • ecdsa-sha2-nistp256 • ecdsa-sha2-nistp384 • ecdsa-sha2-nistp521

Prerequisites

- You have the management permissions for the **Host Operations** module.
- You have obtained the access permissions for the resources.
- You have installed the client tool.
- The network connection between the managed host and the system is normal, and the account username and password for logging in to the managed host are correct.

Procedure

Step 1 Start the local client tool Xshell and choose **File** > **New** to create a user session.

Step 2 Configure session connections.

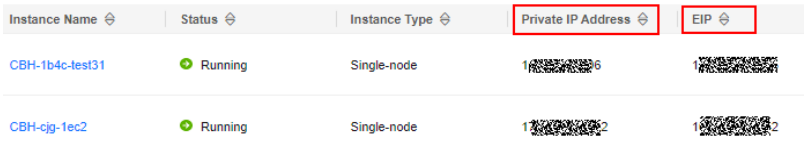
- Method 1
  a. Set **Protocol Type** to **SSH**, enter the elastic IP address of your bastion host, set **Port** to **2222**, and click **OK**.
  b. Enter the username of your bastion host and click **Connect**.
- Method 2:

  In the newly opened blank session window, run a command in the following format: ***Protocol type User login name@System login IP address Port number***, for example, ssh admin@10.10.10.10 2222.
- Method 3

  In the live session window of a Linux host, run a command in the following format: ***Protocol type User login name@System login IP address*-p *Port number***, for example, ssh admin@10.10.10.10 -p 2222.

NOTE

system login IP address indicates the private IP address or EIP of your bastion host. Make sure the network connection between the local PC and the IP address is normal.



Step 3 Verify user identity.

- Select **Password**, enter your password, and click **OK**.
- Select **Public Key**, upload the private key file that matches the **SSH public key** added to the bastion host in the user key area, select the target private key, and click **OK**.

  After the authentication is successful, the user can use the SSH client to log in to the bastion host without having to enter a password.

Step 4 Log in to your bastion host.

If an SSH client is used, password, SMS message, mobile token, and OTP can be used for login identity authentication. To use mobile SMS message, mobile OTP, and OTP authentication methods, configure multifactor verification. For details, see **Configuring User Login Restrictions**.

- Mobile SMS: After logging in to the system using the local password, select **Mobile SMS** for **Multifactor Verification**, and enter the SMS verification code.
- Mobile OTP: After logging in to the system using the local password, select **Mobile OTP** and enter the dynamic password of the mobile phone token.
- One-Time password: After logging in to the bastion host using the local password, select **OTP** and enter the dynamic token verification code.

Step 5 Import accounts of a managed host.

Decompress the configuration file package, open the **readme.txt** file, and import the resource account. For details about how to download the package, see **Downloading Host Configuration File**.

Step 6 Log in to the managed host using an account.

Select the account to be used for logging, enter the password of the system user, and log in to the host for O&M.

----End

Downloading Host Configuration File

To import host resources in batches using the SSH client, download the configuration files of the hosts to be imported.

Step 1 Log in to your bastion host using a web browser.

Step 2 Choose **Operation** > **Host Operations** to go to the **Host Operations** page.

Step 3 Click **Export Host Configuration**.

Step 4 Select the configuration file of the client and click **OK** to download the configuration file.

----End

8.1.4 Using an FTP or SFTP Client to Log In to File Transfer Resources

You can use file transfer clients to transfer files between authorized managed hosts. This means you can transfer files the way you are used to. A bastion host can log all activities performed on a host resource. The logs can be used for audits.

This topic describes how to obtain client login information and log in to resources that use a file transfer protocol.

Constraints

- If the primary/secondary account operation method is selected for the FTP/SFTP protocol, only resource accounts with **Login Type** set to **Auto Login** can be used. The **Empty** resource account cannot be used.
- Transferring file over SFTP is not supported for host resources with MFA enabled. For details, see **Configuring Multifactor Verification**.
- Only hosts with **Protocol** set to **FTP** or **SFTP** can be logged in to using a web browser. Client tools must meet the requirements in the following table.

Table 8-5 Tools supported

Host Protocol	Client Tool Required
SFTP	Xftp 6 or later, WinSCP 5.14.4 or later, and FlashFXP 5.4 or later

Host Protocol	Client Tool Required
FTP Protocol	Xftp 6 or later, WinSCP 5.14.4 or later, FlashFXP 5.4 or later, and FileZilla 3.46.3 or later

Table 8-6 Supported clients

Algorithm Type	SSH Client
Key exchange	• diffie-hellman-group-exchange-sha256 • diffie-hellman-group-exchange-sha1 • diffie-hellman-group14-sha1 • diffie-hellman-group1-sha1 • ecdh-sha2-nistp521 • ecdh-sha2-nistp384 • ecdh-sha2-nistp256
Encryption	• aes128-ctr • aes192-ctr • aes256-ctr • aes128-cbc • aes192-cbc • aes256-cbc • 3des-cbc • blowfish-cbc • arcfour128 • arcfour256
HMAC	• hmac-md5 • hmac-md5-96 • hmac-sha1 • hmac-sha1-96 • hmac-sha2-256 • hmac-sha2-512
Host Key	• ssh-rsa • ssh-dss • rsa-sha2-256 • rsa-sha2-512 • ecdsa-sha2-nistp256 • ecdsa-sha2-nistp384 • ecdsa-sha2-nistp521

Prerequisites

- You have the management permissions for the **Host Operations** module.
- You have obtained the access permissions for the resources.
- You have installed the client tool.
- The network connection between the managed host and the system is normal, and the account username and password for logging in to the managed host are correct.
- You have enabled FTP and opened ports 2222 (for SFTP) and 2121 (for FTP). For details, see **Configuring the Operation Ports**.
- You have **configured an SSO client** on the local PC if you want to select the client operation method for the FTP or SFTP protocol.

Procedure

Step 1 Obtain the login information.

1. Log in to your bastion host.
2. Choose **Operation** > **Host Operations** to go to the **Host Operations** page.
3. Select an FTP or SFTP host resource, and click **Login**.

Step 2 Log in to the host using a client tool.

1. Start the local FTP or SFTP client tool.
2. Enter the host address, port number, user name, and login password.

   NOTE

   You can use APIs to log in to host resources using the FTP or SFTP protocol.

Table 8-7 Parameter description

Parameter	Description
Host Addr	IP address for logging in to the bastion host.
Port	Port number. The default port number is 2222.
UserName	Username in the configuration information in the format of login name@resource account name@host address, for example, admin@root@192.168.1.1.
Password	Password for the user to log in to the bastion host.

----End

8.1.5 Using an SSO Client to Log In to Database Resources for O&M

You can use single sign-on (SSO) tools to invoke the database client tool for database resource O&M and operation audit. Before your start, install the SSO and database client tools and then configure the path of the database client tool.

This topic describes how to configure the SSO client and how to use the SSO tool to log in to database resources.

NOTE

There are four options for the single sign-on (SSO) tool:

- Mysql cmd
- MySQL Administrator
- Navicat
- DBeaver (supported by bastion host V3.3.48.0 and later versions)

Notes

During O&M, bastion hosts automatically record videos for audit. To prevent sensitive information leakage, do not enter sensitive information that is displayed in plaintext during O&M.

Constraints

- The database operation audit is available only in professional editions.
- Only MySQL, SQL Server, Oracle, DB2, PostgreSQL, and GaussDB databases can be managed.

  NOTE

  A bastion host cannot verify the database with SSL enabled. When connecting to GaussDB databases, you need to disable SSL (**sslmode**) on DBeaver.
- The client tool can be invoked only through SsoDBSettings.
- Only SecureCRT and XShell host resource operation clients can be used.
- Only some database clients can be invoked through an SSO tool. For details, see the following table.

Table 8-8 Supported database protocols, versions, and clients

Database Type	Version	Supported Client
MySQL	MySQL 5.5, 5.6, 5.7, and 8.0	Navicat 11, 12, 15, and 16 MySQL Administrator 1.2.17 MySQL CMD
Microsoft SQL Server	2014, 2016, 2017, 2019, and 2022	Navicat 11, 12, 15, and 16 SSMS 17.6
Oracle	10g, 11g, 12c, 19c, and 21c	Toad for Oracle 11.0, 12.1, 12.8, and 13.2 Navicat 11, 12, 15, and 16 PL/SQL Developer 11.0.5.1790
DB2	DB2 Express-C	DB2 CMD command line 11.1.0

Database Type	Version	Supported Client
PostgreSQL	11, 12, 13, 14, and 15	DBeaver 22 and 23
GaussDB	2 and 3	DBeaver 22 and 23

NOTE

- You need to download the database versions supported.
- If you want to use an SSO tool to perform O&M on GaussDB databases, download the JDBC driver package of V2.0-3.*x* by referring to **Using JDBC to Connect a Database** first. Then delete all files from the **Library** in **Database > Driver Manager**, and add the downloaded JDBC driver package.
- If you need to use an SSO tool to perform O&M on PostgreSQL and GaussDB databases, add the **sslmode** attribute to the connection attributes in **Database > Driver Manager** and save the value as **disable**.
- The SsoTool.msi remote tool can be installed only in the default path **C:\sso\SsoTool**. If you install it in other paths, the tool may fail to be started.

Prerequisites

- You have the management permissions for the **Host Operations** module.
- You have obtained the access permissions for the resources.
- You have installed the client tool.
- The network connection between the managed host and the system is normal, and the account username and password for logging in to the managed host are correct.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **Operation** > **Host Operations** to go to the **Host Operations** page.

Step 3 Select the host with protocol set to database, and click **Login**.

The client tool selection window is displayed.

NOTE

- When you first time log in to the database, you will see the SsoDBSettings download window.
- The download tool varies depending on the bastion host version you are using.

  For example, if you are using version 3.3.44.0, SSO tool Windows and UOS (Arm) are provided. You can select either of them from the drop-down list.

Step 4 Select the client tool that has been installed and click **OK**.

The system automatically calls the local database client tool to log in to the database.

----End

Configuring the SSO Client

The following uses the **Navicat** client as an example to describe how to configure the client path.

Step 1 Start local SSO tool SsoDBSettings.

Step 2 Click the path configuration icon next to **Navicat Path**.

Step 3 Find the absolute path where the Navicat client is installed, select the .exe file, and click **Open**.

Step 4 Go to the SsoDBSettings SSO tool configuration page and view the selected Navicat client path.

Step 5 Click **Save** to return to the **Host Operations** page in your bastion host. Then, you can log in to the database.

----End

8.1.6 Logging In to and Maintaining Database Resources Using a Local Client

You can use a local client tool to log in to and maintain MySQL and PostgreSQL databases on macOS to audit database O&M. This section uses Navicat as an example to describe how to log in to MySQL and PostgreSQL databases on macOS for O&M.

Notes

During O&M, bastion hosts automatically record videos for audit. To prevent sensitive information leakage, do not enter sensitive information that is displayed in plaintext during O&M.

Constraints

- The database operation audit is available only in professional editions.
- You can log in to MySQL and PostgreSQL databases on macOS only by using the method described in this section.
- To prevent network faults or network configuration problems from affecting the login to the system, enable the ports bound to the security group of the CBH system by referring to **Table 8-9**. For more details, see **How Do I Configure a Security Group for a CBH Instance?**.

Table 8-9 Port configuration requirements

Database Type	Port
MySQL	• Inbound: 33306 and 62222 • Outbound: 3306
PostgreSQL	• Inbound: 15432 and 62222 • Outbound: 5432

- Only some database clients are supported. For details, see **Table 8-10**.

Table 8-10 Supported database types, versions, and clients

Database Type	Version	Supported Client
MySQL	MySQL 5.5, 5.6, 5.7, and 8.0	• Navicat 17 or later • DBeaver 25 or later
PostgreSQL	11, 12, 13, 14, and 15	

NOTE

If you need to use a client tool to perform O&M for PostgreSQL databases, add the **sslmode** attribute to the connection attributes in **Database > Driver Manager** and save the value as **disable**.

Prerequisites

- You have the management permissions for the **Host Operations** module.
- You have obtained the access permissions for the resources.
- You have installed the client tool.
- The network connection between the managed host and the system is normal, and the account username and password for logging in to the managed host are correct.

Procedure

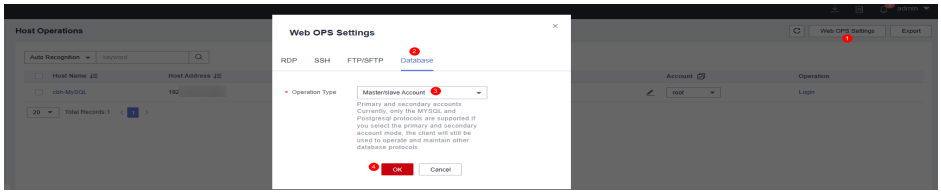
Step 1 Log in to your bastion host.

Step 2 Choose **Operation** > **Host Operations** to go to the **Host Operations** page.

Step 3 Set **Operation Type** to **Master/slave Account**.

1. In the upper right corner on the **Host Operations** page, click **Web OPS Settings**.
2. Click the **Database** tab.
3. Set **Operation Type** to **Master/slave Account** and click **OK**.

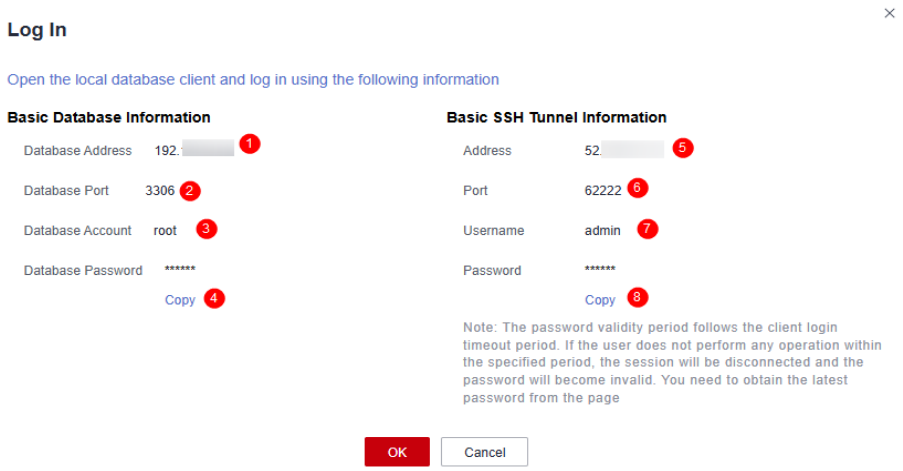
Figure 8-8 Configuring operation type



Step 4 Select a host with protocol type set to MySQL or PostgreSQL and click **Login** in the **Operation** column.

Complete **Step 5** based on the information in the displayed window.

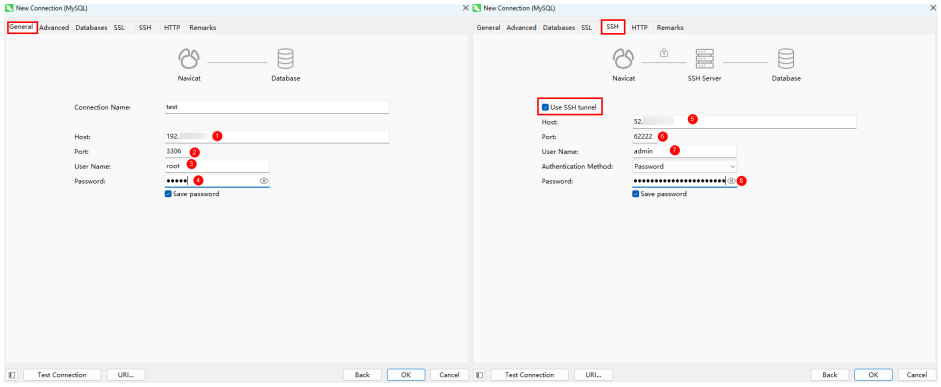
Figure 8-9 Login information



Step 5 Open the local client tool, configure login information, and log in to the database.

Take the Navicat client as an example. Create a connection, configure the connection on the **General** and **SSH** tabs based on the login information in **Step 4**, and then connect to the database.

Figure 8-10 Configuration example



----End

8.1.7 Batch Logging In to Host Resources for O&M

You can batch log in to host resources through your bastion host for operations, including file transfer, file management, and command presetting. A bastion host can log all activities performed on a host resource. The logs can be used for audits.

Constraints

- Batch login is unavailable for hosts configured with the FTP, SFTP, DB2, MySQL, Oracle, SQL Server, or SCP protocol.
- Manual login and two-person approval accounts cannot be used for batch logging.
- The cooperation session function is unavailable for hosts logged in through batch logging.

NOTE

During batch logins, if invalid usernames or passwords, or both, are used for a server, the session for the server will not displayed, and no error messages are reported. You need to log in this server separately to check the error message.

Prerequisites

- You have the management permissions for the **Host Operations** module.
- You have obtained the access permissions for the resources.

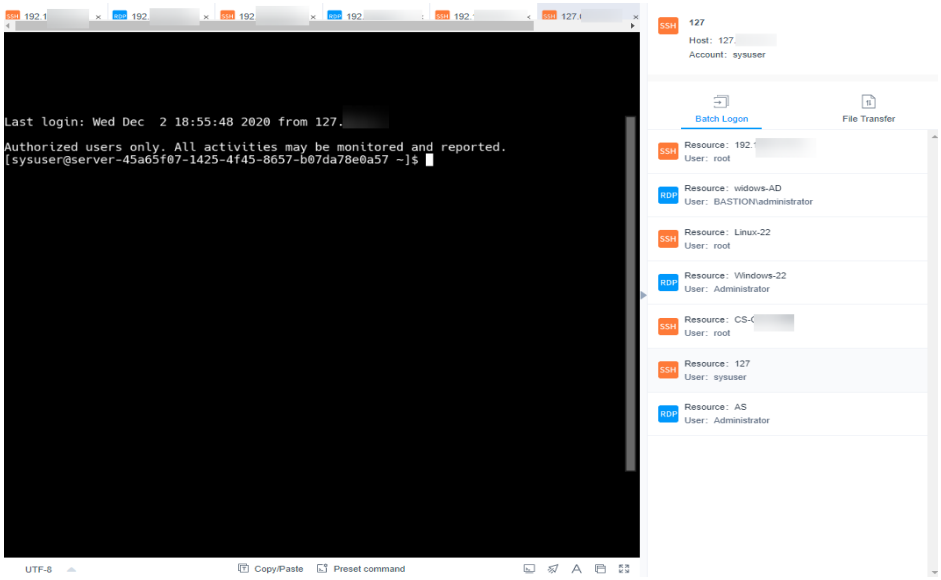
Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **Operation** > **Host Operations** to go to the **Host Operations** page.

Step 3 Select multiple resources and click **Batch Logon**.

Figure 8-11 Batch logon session windows



Step 4 Switch over session windows.

Click the resource name in the batch logon list to switch to the corresponding session window.

Step 5 For details about the operations in the session window, see the following description.

- **Session Window of Hosts Using the RDP or VNC Protocol**
- **Session Window of Hosts Using the SSH or Telnet Protocol**

Step 6 Upload files to or download files from the host or host net disk. For details, see **File Transfer**.

Step 7 In the file management area, manage files or folders on the host or host net disk. For details, see **Using a Web Browser for Logins**.

----End

8.1.8 File Transfer

When you manage resources through a web browser, you can upload or download files on the **File Transfer** tab. This feature enables file transfer between a local computer and managed host and between different managed hosts. The CBH system records the entire file transfer process in detail, making it easier to audit file upload and download operations.

Netdisk is a personal net disk in a system, which is preset for each system user. A user can temporarily store files on it for file transfer between managed hosts. The file content in the personal net disk is visible only to users who creates the file.

Netdisk is directly associated with each system user. If a user is deleted, the files on the personal net disk are cleared and the personal net disk space is released.

Constraints

- Currently, when you use a web browser for O&M, files can be uploaded or downloaded only on the hosts using the SSH or RDP protocol.
- During web-based O&M, users cannot upload files to or download files from managed hosts by running the **rz** or **sz** command but only through **File transfer**.

  NOTE

  For Linux hosts, users can transfer files by running commands on the SSH client. For example, users can run the **rz** or **sz** command on the SSH client to upload or download files. However, the CBH system cannot record such file upload and download data, and the purpose of security audit cannot be met.
- Web-based O&M allows you to download one or more files but not folders.
- Resumable download is not supported. Do not stop or pause the file upload or download process.
- For a file larger than 1 GB, you can split the file into several small files and then upload or download them in batches or **use the FTP client to transfer the file**.

  NOTE

  If the disk space is insufficient, the upload will fail. In this case, you need to clear the disk or expand the disk capacity.

Prerequisites

- You have the permissions to upload and download host resource files.
- You have the host operation permissions and can log in to the managed host using a web browser.

Uploading Files to and Downloading Files from a Managed Linux Host

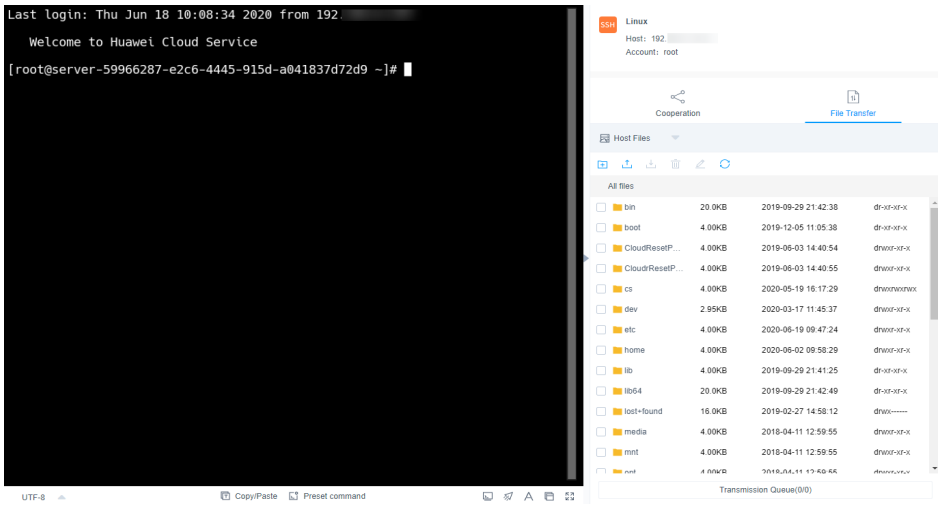
Files can be directly transferred between a Linux host and a local computer without having to use the personal net disk. A personal net disk can be used to transfer files from other managed hosts.

Step 1 Log in to your bastion host.

Step 2 Choose **Operation** > **Host Operations**, select the target Linux host resource, and click **Login** to go to its operation page.

Step 3 On the right of the operation page, choose **File Transfer** to view the Linux host file list.

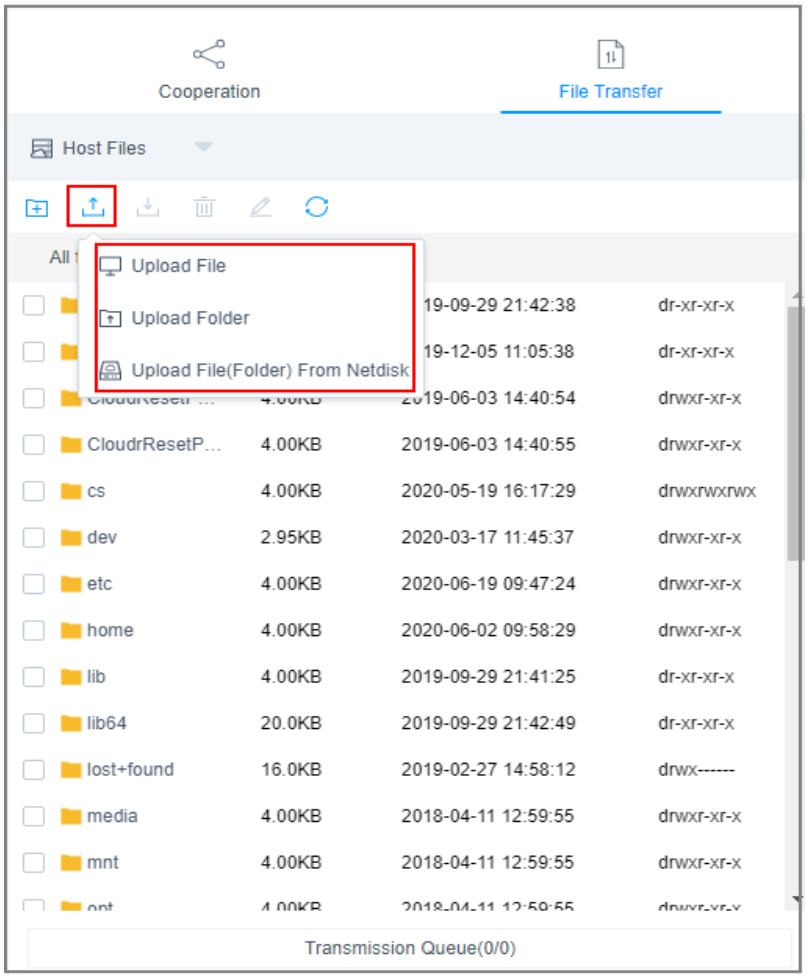
Figure 8-12 Viewing the file list of a Linux host



Step 4 Upload files to the Linux host.

You can click the upload icon and choose **Upload File**, **Upload Folder**, or **Upload File (Folder) from Netdisk** to upload one or more local files, local folders, or net disk files or folders to the Linux host.

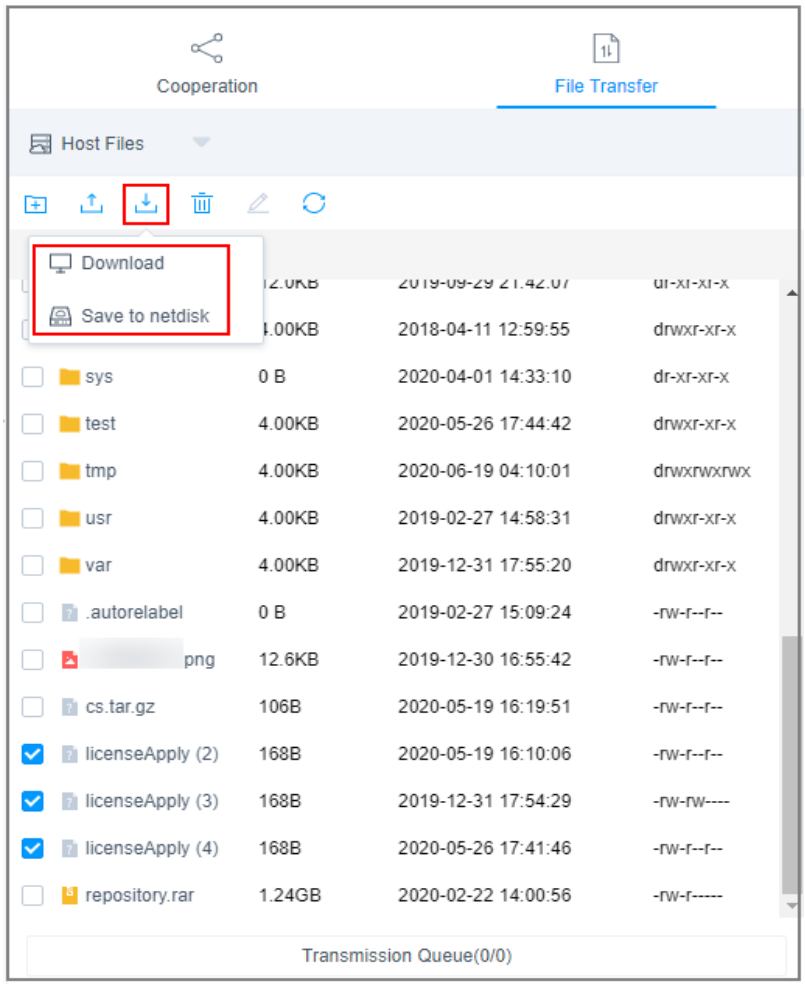
Figure 8-13 Uploading files to a Linux host



Step 5 Download files from the Linux host.

1. Select one or more files to be downloaded.
2. Click **Download** or **Save to netdisk** to download selected files to the local computer or the personal net disk, respectively.

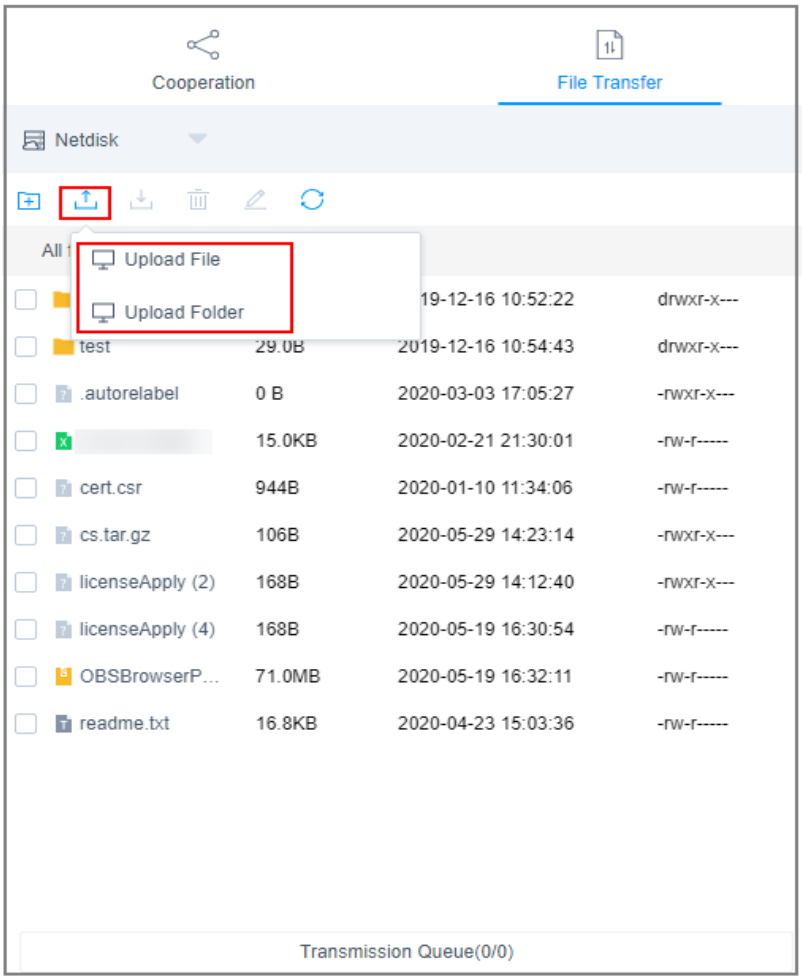
Figure 8-14 Downloading files from a Linux host



Step 6 Upload files to the personal net disk

1. Click **Host File** and select **Netdisk** to switch to the personal net disk file list.
2. Click **Upload File** or **Upload Folder** to upload one or more local files or folders.

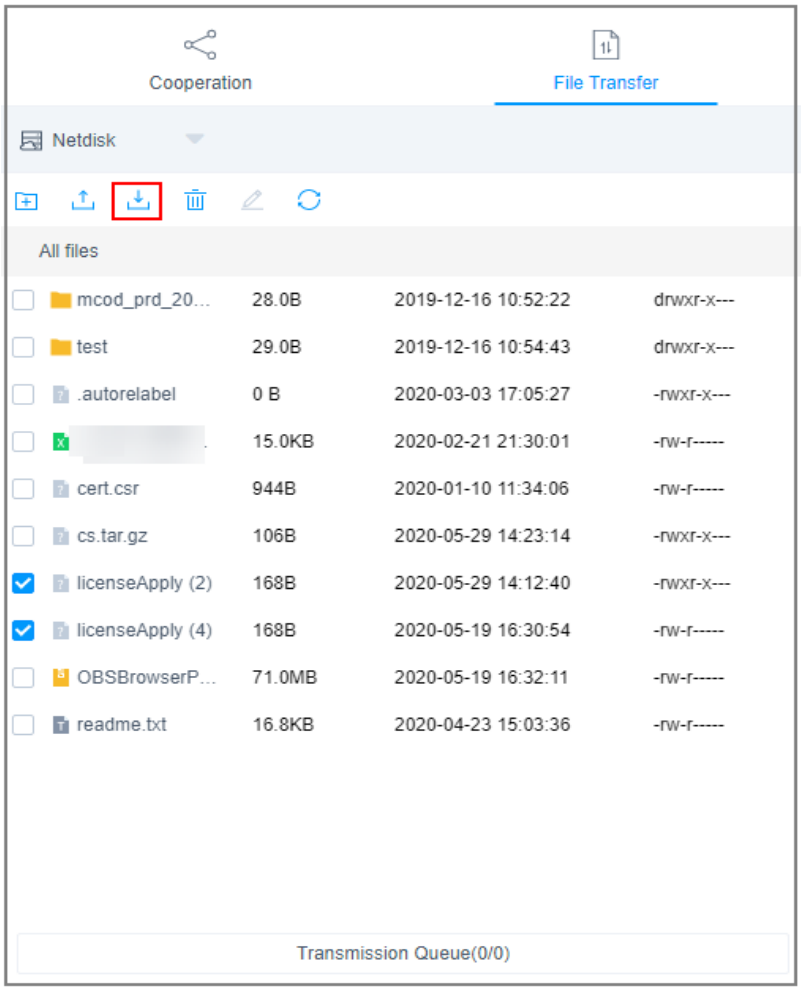
Figure 8-15 Uploading files to the personal net disk



Step 7 Download files from the personal net disk.

1. Select one or more files to be downloaded.
2. Click the download icon to download one or more files to the local computer.

Figure 8-16 Downloading files from the personal net disk



----End

Uploading Files to and Downloading Files from a Managed Windows Host

For Windows hosts managed in a CBH system, the default path for storing files is **NetDisk G**. This disk is your personal net disk.

Files on a Windows host cannot be directly transferred between the lost and a local computer. They can be transferred only through the personal net disk.

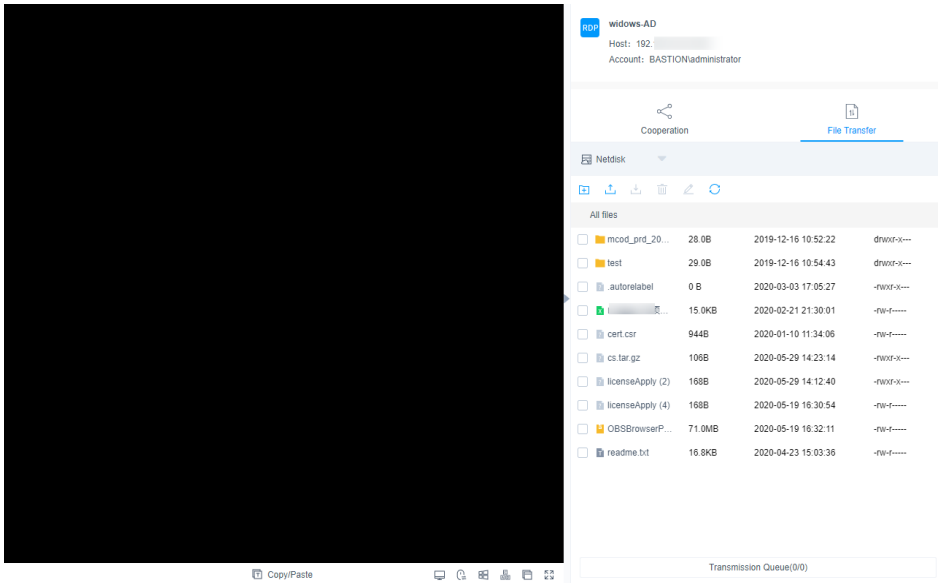
Step 1 Log in to your bastion host.

Step 2 Choose **Operation** > **Host Operations** and locate the target Windows host.

Step 3 Click **Login** to open the Windows host operation session.

Step 4 Click **File Transfer** to list of host files on the personal net disk.

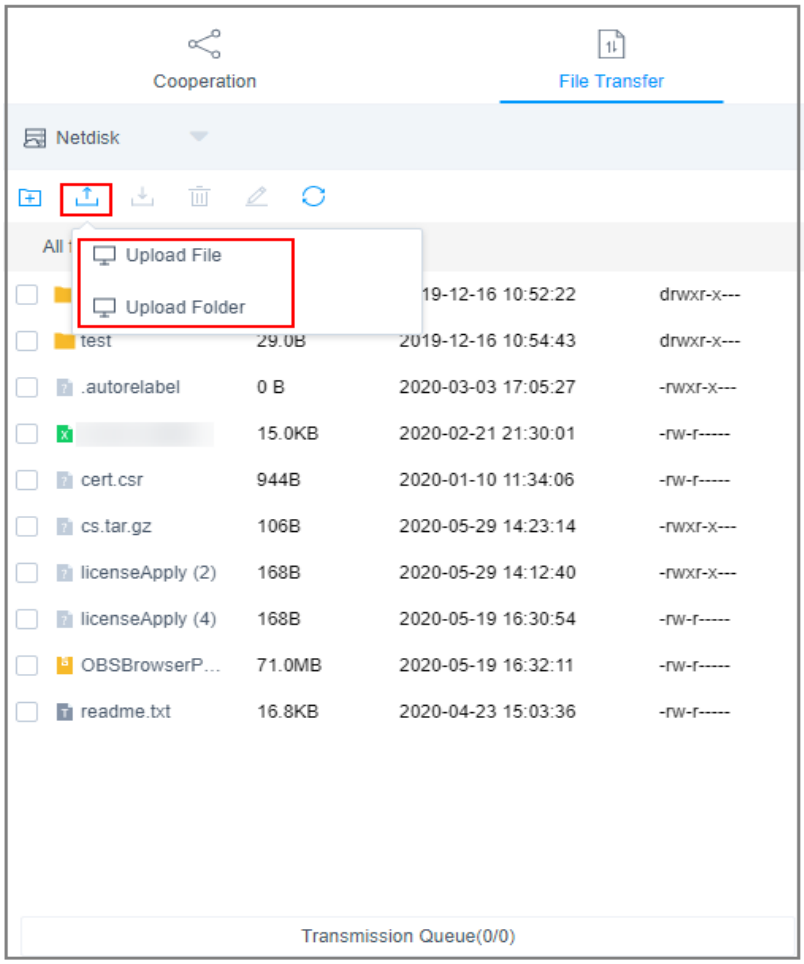
Figure 8-17 Windows host file transfer



Step 5 Upload files to the Windows host.

1. Click **Upload File** or **Upload Folder** to upload one or more local files or folders.
2. Open the disk directory of the Windows host and search for **NetDisk** on drive G.
3. Open **NetDisk**, right-click the file or folder to be uploaded, copy and paste it to the target directory on the Windows host.

Figure 8-18 Uploading files to the personal net disk



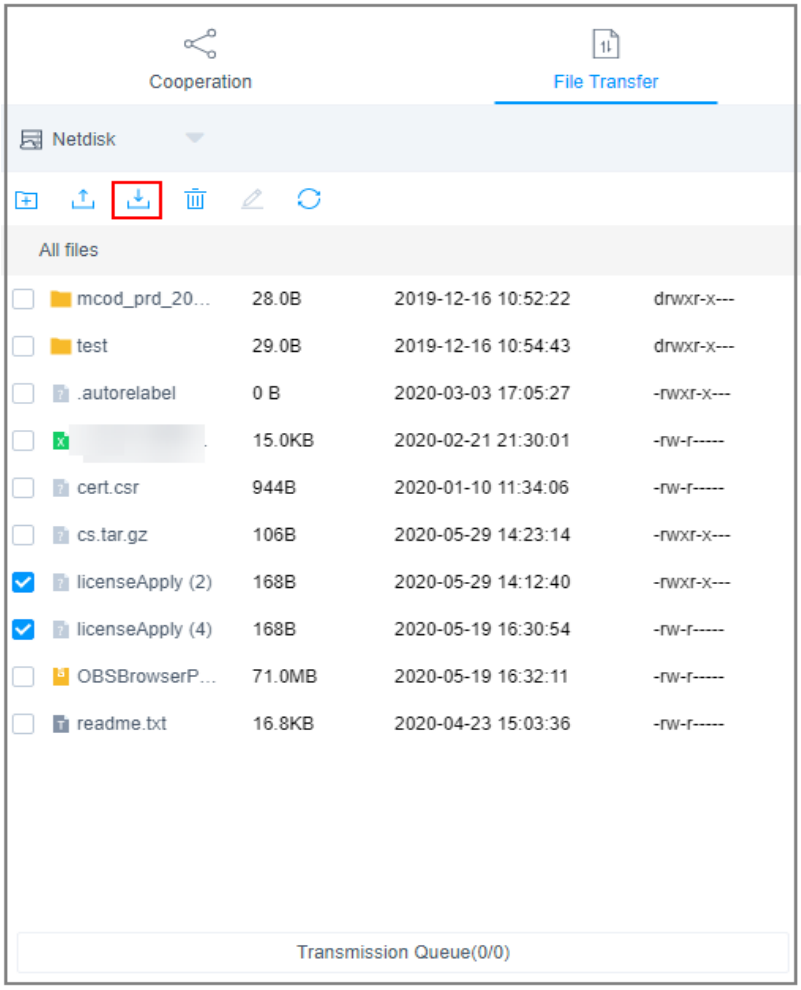
Step 6 Download files from the Windows host.

1. Open the Windows host disk directory, right-click the file or folder to be download, and copy it.
2. Open the **NetDisk** disk directory, right-click and paste the file or folder to the personal net disk.

Step 7 Download files from the personal net disk.

1. Select one or more files to be downloaded.
2. Click the download icon to download one or more files to the local computer.

Figure 8-19 Downloading files from the personal net disk



----End

8.1.9 Cooperation

A bastion host supports collaborative operations. A session creator can invite other system users through a URL to join the on-going session. Participants can perform operations on the session after being approved by the session creator. This function can be used in scenarios such as remote demonstration and consultation of difficult O&M problems.

Constraints

- Before sharing an operation session, ensure that the network connection between the bastion host and the managed host is normal. Otherwise, the invited user cannot join the session, and the connection error (code: T_514) is reported on the session window of the creator. The error code T_514 indicates that the server does not respond for a long time and the connection is disconnected, and you need to check your network and try again.
- The invitation URL can be copied and sent to multiple users. Only users with the account permissions of the managed resource can open the invitation URL.

- The invited user can join the session only before the URL expires or the session ends.

Prerequisites

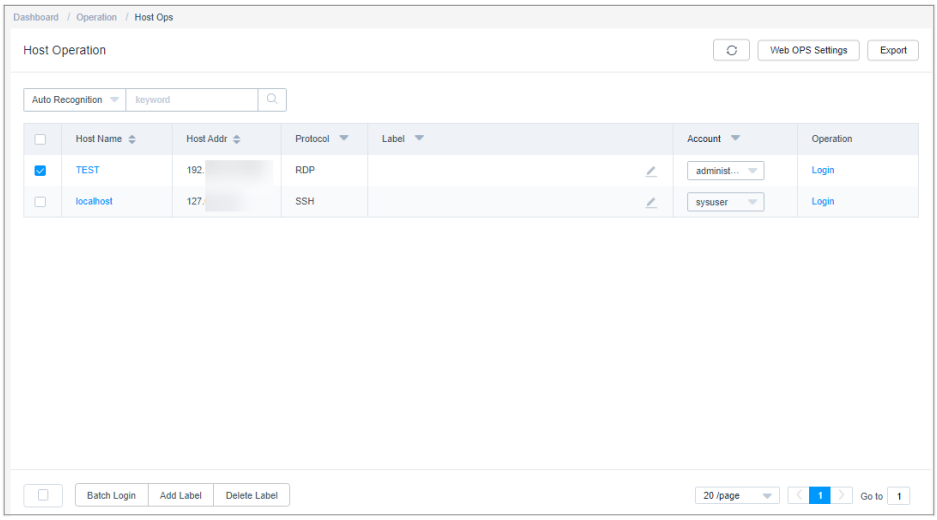
- You have the operation permissions for the host resources.
- You have logged in to the host using a web browser.

Procedure

Step 1 Log in to your bastion host.

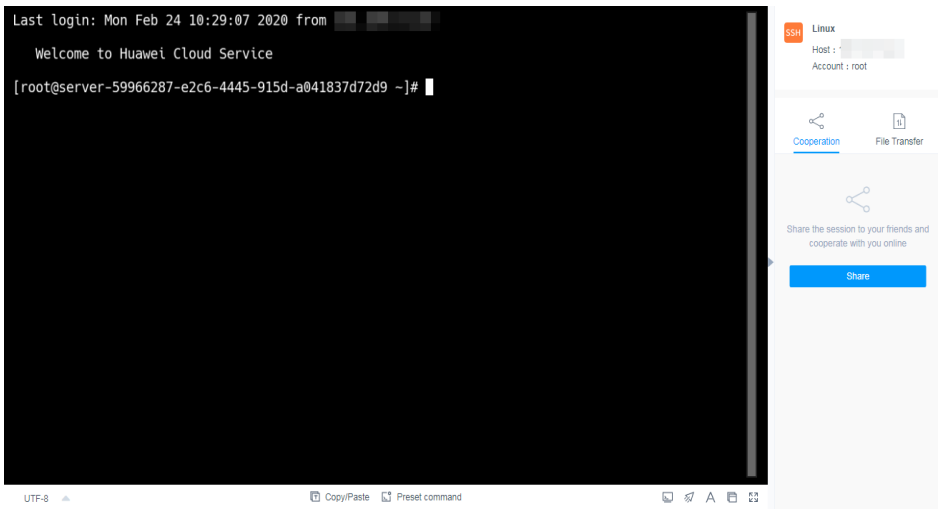
Step 2 Choose **Operation** > **Host Operations** to go to the **Host Operations** page.

Figure 8-20 Host Operation



Step 3 Select the host resource you want to operate and click **Login**.

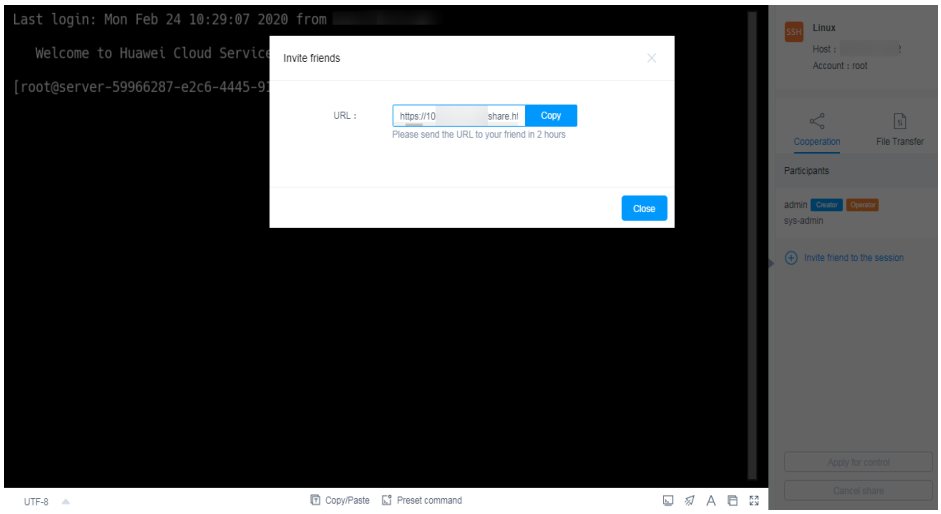
Figure 8-21 Host resource operation page



Step 4 Click **Share** on the right of the dialog box to invite other users to join the session.

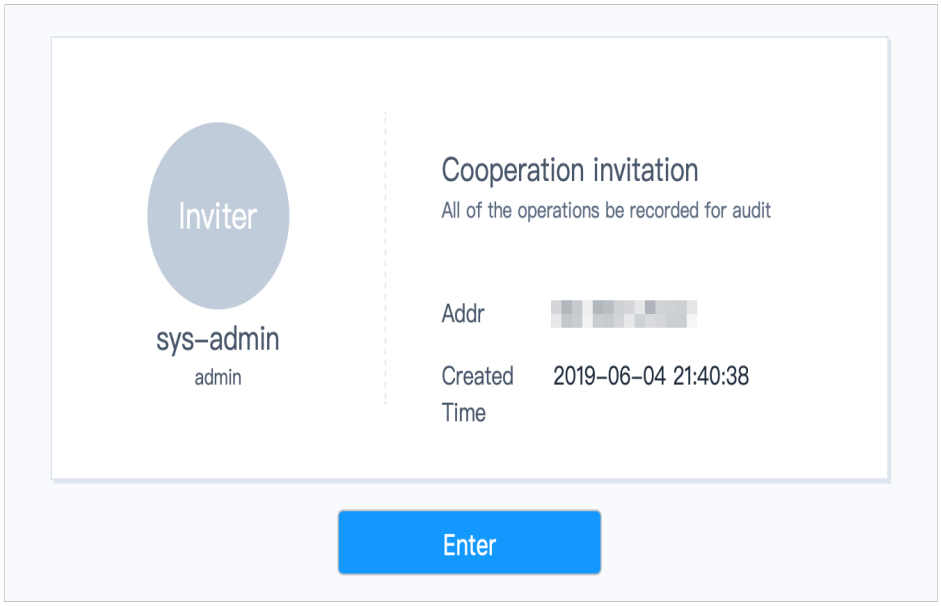
Step 5 Click **Invite friends** to obtain the invitation URL. Copy the URL and send it to the user who has permissions for account of the managed resource.

Figure 8-22 Obtaining the invitation URL



Step 6 The invited user then can log in to the bastion host, open the invitation URL, and view the invitation information.

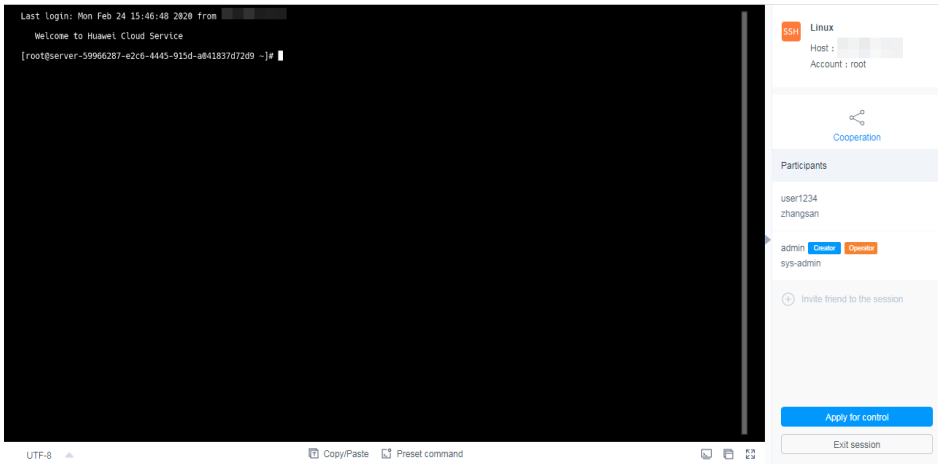
Figure 8-23 Invitation information displayed for the invited users



Step 7 As an invited user, click **Enter** to join the session.

- Click **Apply for control** to send a request to the current controller to apply for the control permission.
- Click **Release control** or **Exit session** to hand the session control back to the creator.
- Click **Exit session** to exit the current session. After exiting the session, the invited user can join the session again as long as the invitation URL does not expire and the session remains in progress.

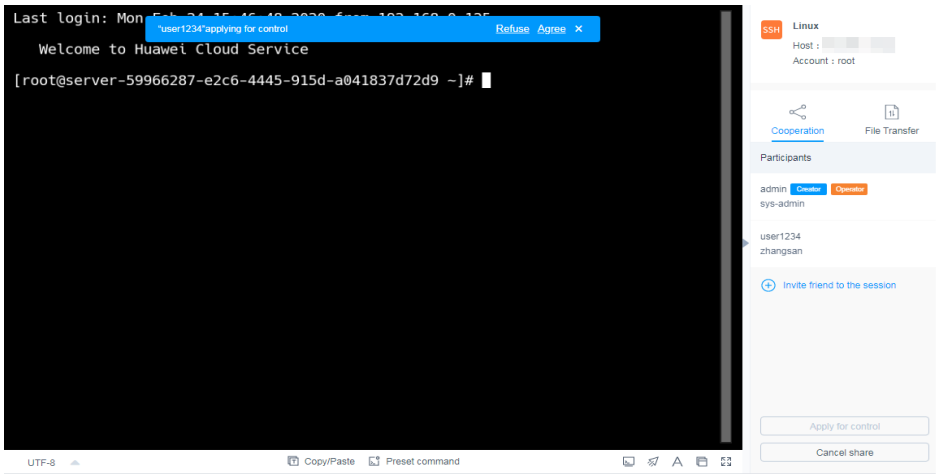
Figure 8-24 Cooperation session page of invited users



Step 8 The creator or the invited user can manage the session.

- If the creator clicks **Cancel share** or exits the session, the cooperation session ends. The invited user is forced to exit the session and cannot access the session again through the URL.
- When an invited user applies for the session control permission, the session creator can click **Agree** to hand over the session control permission or click **Refuse** to reject the application.

Figure 8-25 Cooperation session page of the inviter



----End

8.1.10 Enabling Forcible RDP Connections

When the number of Windows remote desktop connections exceeds the upper limit, no more remote connections with the host resources can be established. In this case, you can enable the **admin console** in the bastion host to implement force logins. This means you can force the bastion host to establish login connections by forcibly logging out other logged-in users.

This topic describes how to enable the **admin console** configuration for enabling force RDP connections.

Constraints

- This function is available only for hosts using the RDP protocol.
- This function is available to user **admin** only.

Prerequisites

You have the management permissions for the **Host Operations** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **Operation** > **Host Operations** to go to the **Host Operations** page.

Step 3 Click **Web OPS Settings**. The configuration window is displayed.

Step 4 Select the **admin console** connection mode.

Step 5 Click **OK** to return to the **Host Operations** page.

After the configuration is successful, when a user attempts to log in to an RDP host, even if the number of connections exceeds the upper limit, logins of this user will be successful at the cost of forcible logouts of other users.

----End

8.2 Application Resource Operation

8.2.1 Viewing the Application Resource List and Setting Resource Labels

After obtaining the access permissions for application resources, you can view authorized application resources and set labels for them.

This topic describes how to view authorized resources and set resource labels.

Constraints

Labels cannot be shared with others. You can define your own resource labels for your exclusive use.

Prerequisites

- You have the management permissions for the **App Operations** module.
- You have obtained the access permissions for the resources.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **Operation** > **App Operations** to go to the **App Operations** page.

Step 3 Query application resources.

Quick search: Enter a keyword in the search box to quickly query application resources by auto recognition, application name, and application IP address.

Step 4 Add a label to an application resource.

1. Select an application resource you want and click in the **Label** column.
2. Enter a label type and press **Enter** or select an existing label type.
3. Click **OK**. You can then view the added label on the **App Operations** page.

Step 5 Add a label for multiple application resources at a time.

1. Select multiple resources and click **Add Label** in the lower left corner of the list.
2. Enter a label type and press **Enter** or select an existing label type.
3. Click **OK**. You can then view the added label on the **App Operations** page.

Step 6 Delete an application resource label.

1. Select multiple resources and click **Delete Label** in the lower left corner of the list.
2. In the displayed dialog box, confirm the deletion and click **OK**.

----End

8.2.2 Using a Web Browser to Log In to Application Resources for O&M

After you log in to an application resource using a web browser, the cooperation, file management, and file transfer functions are available for you. A bastion host can log all activities performed on an application resource. The logs can be used for audits.

- Cooperation: This function allows the session initiator to invite other system users to participate the current session by sharing the session link with them, implementing O&M collaboration.
- File management: This function allows all session participants to manage files or folders on hosts and host net disk after they obtain the operation permissions. In addition, they can:
  - Create new folders.
  - Change the name of a file or folder.
  - Delete files or folders in batches.
- File transfer: This function allows session participants to download or upload files or folders on the host or host net disk after they obtain the operation permissions. They can:
  - Upload and download files.
  - Upload folders.
  - Upload multiple files or a folder to a host net disk or download multiple files from a host net disk to a local host, if **Netdisk** is selected as the destination address.

This topic describes how to log in to application resources and perform operations through a web browser.

Notes

During O&M, bastion hosts automatically record videos for audit. To prevent sensitive information leakage, do not enter sensitive information that is displayed in plaintext during O&M.

Constraints

- Only web browsers can be used to log in to application resources for O&M.
- Although using a web browser for O&M allows you to copy and paste a large number of characters without garbled characters, a maximum of 80,000 characters can be copied from the local to the remote, and a maximum of 1000,000 of bytes can be copied from the remote to the local.
- File management

  Files and folders cannot be edited in batches.
- File Transmission
  - By default, the system supports the upload of a single file with a maximum size of 100 GB. However, the size of a single file to be uploaded is limited by the **Personal Netdisk** space and browser type.

    NOTE

    If the disk space is insufficient, the upload will fail. In this case, you need to clear the disk or expand the disk capacity.
  - Folders cannot be downloaded.
  - For application resources, only **Netdisk** can be select as the destination address.

Prerequisites

- You have the management permissions for the **App Operation** module.
- You have obtained the access permissions for the resources.
- The network connection between the application server and the system is normal, and the account username and password for logging in to the application server are correct.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **Operation** > **App Operations** to go to the **App Operations** page.

Step 3 On the displayed page, select the application resource you want and click **Login** in the **Operation** column to open the session.

Figure 8-26 Windows application operation session

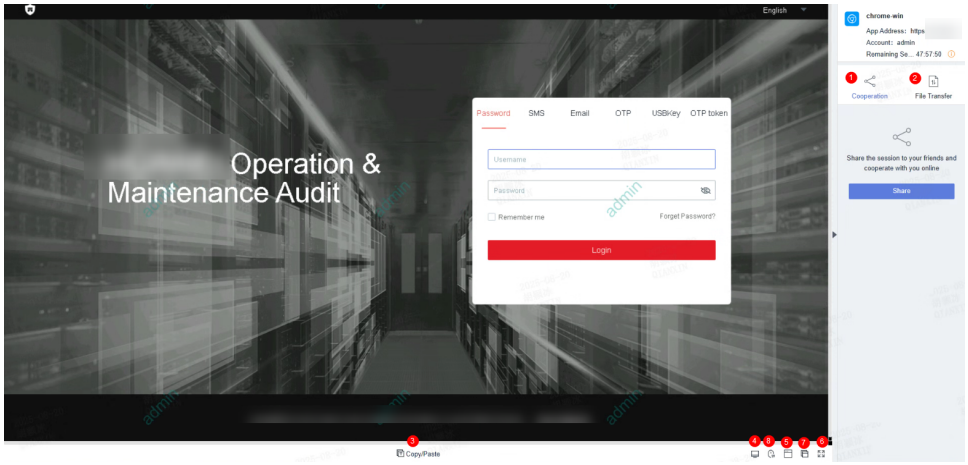


Figure 8-27 Linux application operation session

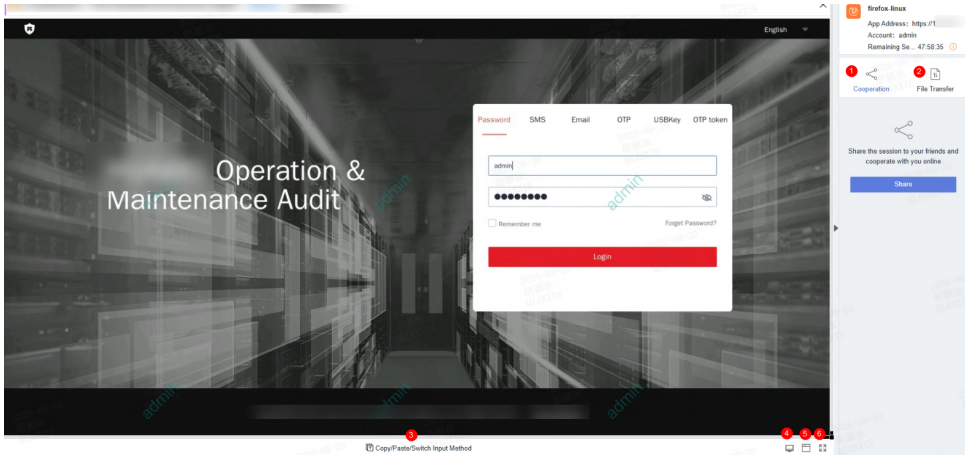


Table 8-11 Parameters for session operation

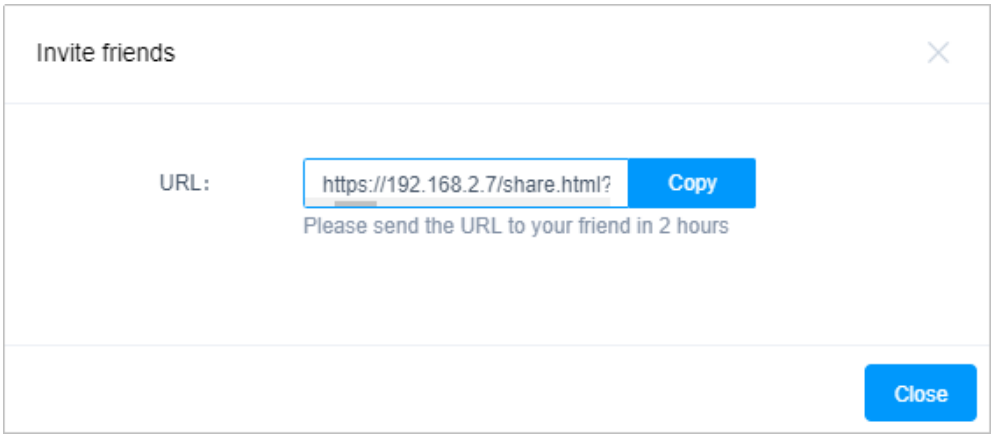
No.	Parameter	Description
①	Cooperation	You can invite colleagues to participate in the session and perform operations together. For details, see **Step 4**.
②	File Transfer	You can upload or download files to or from the host web disk, and manage files and folders. For details, see **Step 5** and **Step 6**.

No.	Parameter	Description
③	Copy/ Paste/ Switch Input Method	• **Copy**: Use **Ctrl+C** to copy. • **Paste**: Use **Ctrl+V** to paste pure text to the remote host, and **Ctrl+G** to paste internal text or files within the asset. • **Switch Input Method**: Only Linux application operation supports input method switch. – **Ctrl+Shift+Space**: Switch the input method in the sequence of English > Pinyin. **NOTE** Although using a web browser for O&M allows you to copy and paste a large number of characters without garbled characters, a maximum of 80,000 characters can be copied from the local to the remote, and a maximum of 1000,000 of bytes can be copied from the remote to the local.
④	Resolution	You can switch the resolution of the current operation interface. During the switching, a new connection is created.
⑤	Demonstration	In demonstration mode, you can switch to the previous page, next page, or close the current page.
⑥	Full screen	Displays the window in full screen.
⑦	Copy window	You can copy the current session window.
⑧	Switch to remote mouse	You can switch over between the local mouse and remote mouse.

Step 4 Invite other system users to participate in the current session. For details, see **Cooperation**.

1. On the **Cooperation** tab, click **Share**.
2. Click **Share**. Complete the information in the displayed **Invite friends** dialog box.

Figure 8-28 Collaboration session page of the inviter

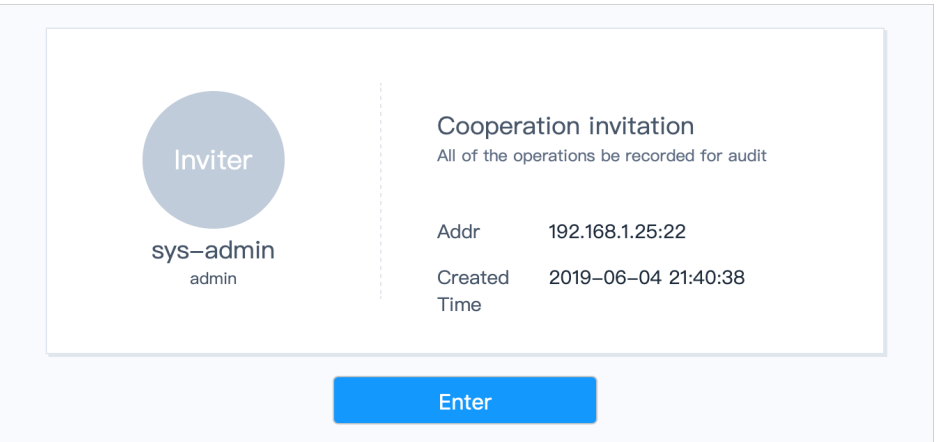


NOTE

The link can be copied and sent to multiple users.

3. Copy the URL and send it to the user who has permissions for accounts managed in the bastion host.
4. Log in to the bastion host as the invited user, open a new browser window, and paste the session link.

Figure 8-29 Collaborative session information



5. If you are invited, click **Enter** to join the session.

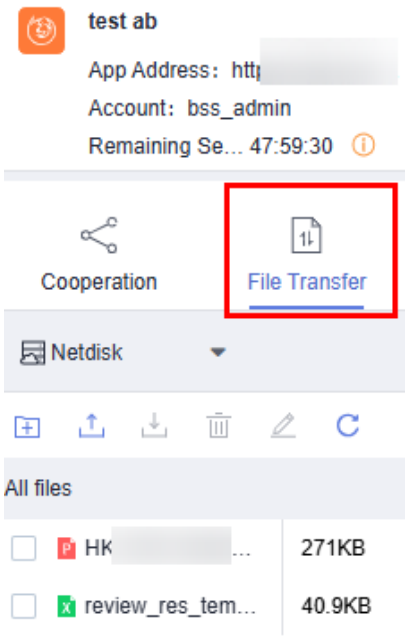
Table 8-12 Parameters for session operation

Parameter	Description
Apply for control	The invited user can apply for control from the invitation sender. Once approved, the invited user can control the current session.
Exit session	Exit the current session.

Step 5 Upload files to or download files from the host or host net disk. For details, see **File Transfer**.

On the **File Transfer** tab of the operation window, you can manage files or folders on the system personal net disk.

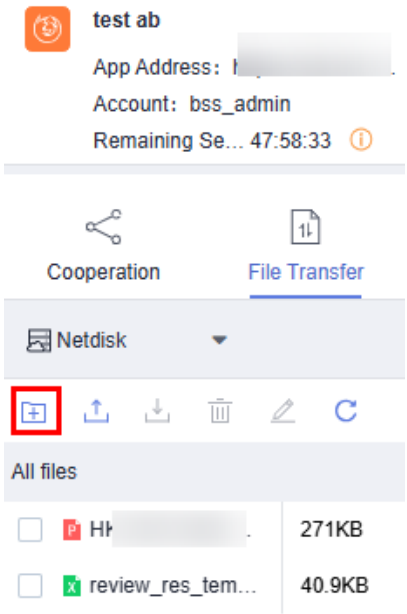
Figure 8-30 File Transmission



Step 6 In the file management area, manage files or folders on the host or host net disk.

1. On the **File Transfer** tab of the operation window, click to create a folder.

   Figure 8-31 New folder



2. Select one or more files or folders and click to delete them.

3. Select a file or folder and click to edit its name.
4. Click to refresh all file directories.

----End

8.3 Cloud Service Operation

8.3.1 Viewing the Host Resource List and Setting Resource Labels

After obtaining the access permissions for cloud service resources, you can view authorized resources in the cloud service O&M list and set labels for cloud service resources.

This topic describes how to view authorized resources and set resource labels.

Constraints

Labels cannot be shared with others. You can define your own resource labels for your exclusive use.

Prerequisites

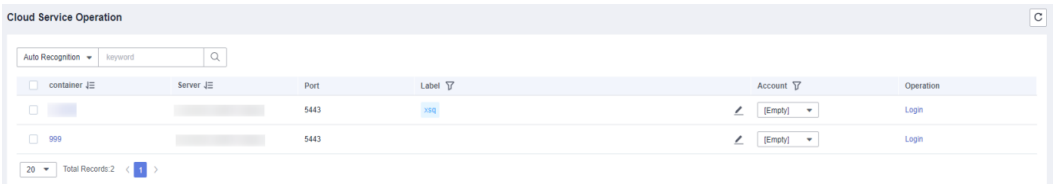
- You have the management permission for the **Cloud Service Operations** module.
- You have obtained the access permissions for the resources.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **Operation > Cloud Service Operations**. The host operation page is displayed.

Figure 8-32 Cloud service operation



Step 3 Display container resources

Quick search: Enter a keyword in the search box to quickly query host resources by auto recognition, host name, and host IP address.

Step 4 Add a label to an application resource.

1. Select an application resource you want and click in the **Label** column.
2. Enter a label type and press **Enter** or select an existing label type.

3. Click **OK**. You can then view the added label on the cloud service operation page.

Step 5 Add a label for multiple application resources at a time.

1. Select multiple resources and click **Add Label** in the lower left corner of the list.
2. Enter a label type and press **Enter** or select an existing label type.
3. Click **OK**. You can then view the added label on the cloud service operation page.

Step 6 Delete an application resource label.

1. Select multiple resources and click **Delete Label** in the lower left corner of the list.
2. After confirming that the information is correct, click **OK** to return to the cloud service operation page. The label has been deleted.

----End

8.3.2 Logging In to Managed Resources Using a Web Browser for O&M Container

When you use a web browser for O&M, you can use collaborative operation. A bastion host can log all activities performed on a host resource. The logs can be used for audits.

NOTE

Currently, **File Transfer** is not supported when O&M using a web browser.

Cooperation: This function allows the session initiator to invite other system users to participate the current session by sharing the session link with them, implementing O&M collaboration.

This section describes how to use a web browser to log in to a managed container.

Notes

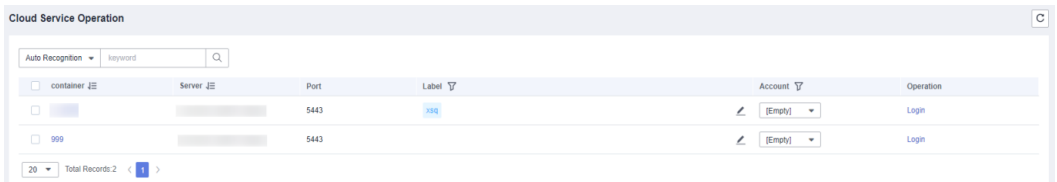
During O&M, bastion hosts automatically record videos for audit. To prevent sensitive information leakage, do not enter sensitive information that is displayed in plaintext during O&M.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **Operation** > **Cloud Service Operations**. The host operation page is displayed.

Figure 8-33 Cloud service operation



Step 3 Click **Login** in the **Operation** column of the target container to log in to the session.

Step 4 Invite other system users to participate in the current session. For details, see **Cooperation**.

1. Click **Cooperation**. The collaborative session window is displayed.
2. Click **Share**. Complete the information in the displayed **Invite friends** dialog box.

   NOTE

   - The URL link can be copied and sent to multiple users.
   - Only users with the access permission can access the bastion host. Otherwise, a connection error will be reported, indicating that the connection has been disconnected because the server does not respond for a long time. Check your network settings and try again (Code: T_514).
3. Copy the link and send it to the users whom you want to invite. The users must have the access permission assigned. Once they receive the link, they can log in to the bastion host, open a web browser, and enter the link to open it in the web browser.
4. If you are invited, click **Enter** to join the session.

Table 8-13 Parameters for session operation

Parameter	Description
Apply for control	The invited user can apply for control from the invitation sender. Once approved, the invited user can control the current session.
Exit session	Exit the current session.

----End

8.4 Operation Script Management

8.4.1 Creating a Script

You can use a bastion host to manage scripts. You can execute scripts to perform complicated or repetitive operation tasks, improving O&M efficiency. You can compile scripts online or import scripts by file.

NOTE

The **HSS-Agent.sh** automatic download and installation script has been built in the bastion host.

Constraints

- Script management is supported by professional editions only.
- Currently, Python and Shell script can be managed.

- Your scripts can be managed by yourself, administrator, or department administrator.

Prerequisites

You have the management permissions for the **Script** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **Operation** > **Script** to go to the script management page.

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

Step 4 In the displayed **New Script** dialog box, configure the basic information about the script.

Table 8-14 Script information parameters

Parameter	Description
Source	The script content source. This parameter can be set to **Edit online** or **From file**. • **Edit online**: indicates that you can edit the script information online to form your script. • **From file**: You can import offline scripts. Only Shell and Python scripts can be uploaded. The file size cannot exceed 5 MB.
Department Name	Department to which the host resource belongs.
Name	Name of the script. For a user-defined script rule, the script name must be unique in the system. **NOTE** For the script imported by file, the name is automatically filled based on the name of the imported file.
Remarks	Brief description of the script. A maximum of 128 characters are allowed.

Step 5 Click **OK**. The system returns to the script list page, and you can view the information about the new script.

----End

Follow-up Operations

After creating an online edited script, you can edit the script online on the script details page. For more details, see **Viewing and Modifying Script Information**.

8.4.2 Viewing and Editing Script Information

This topic describes how to view and modify script online.

Constraints

- If a script exceeds 128 KB, you cannot view the script online. You can download the script to your local PC by referring to **Downloading a Script**.
- The built-in script **HSS-Agent.sh** cannot be modified.

Prerequisites

You have the management permissions for the **Script** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **Operation** > **Script** to go to the script management page.

Step 3 Query a script.

- Quick search

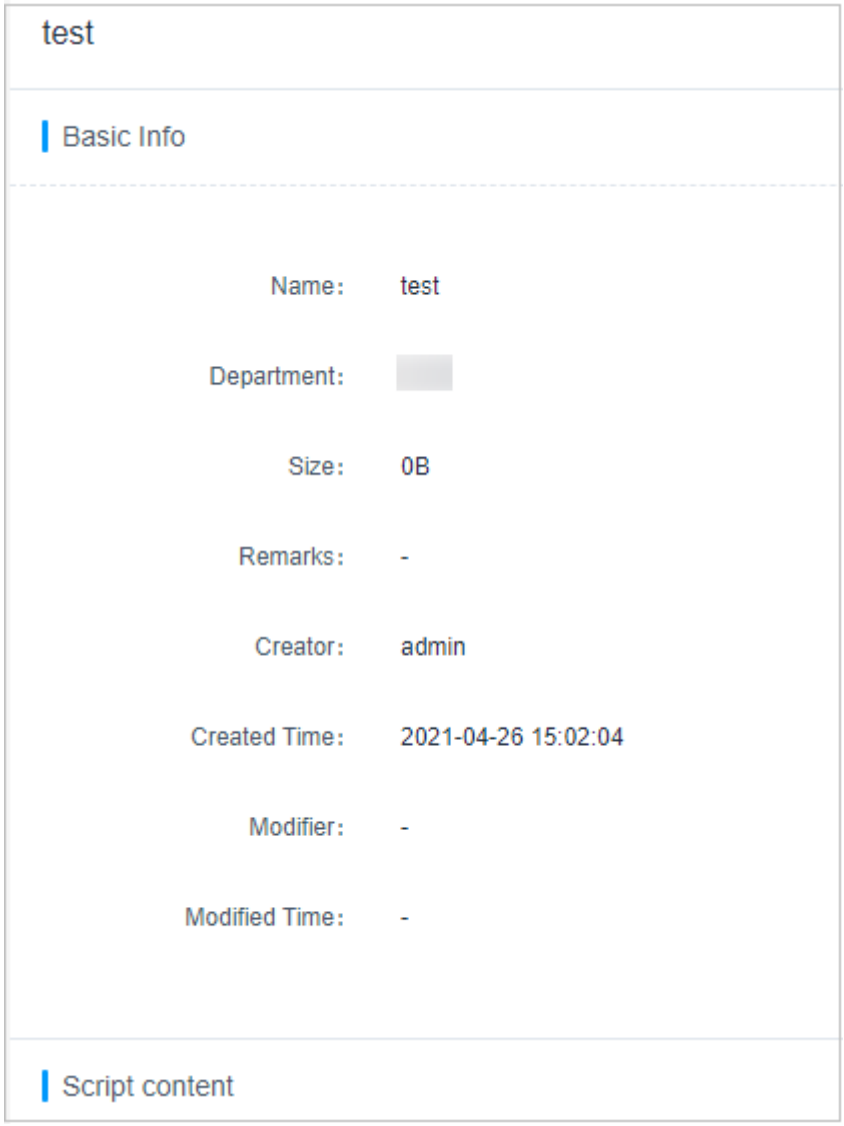
  Enter a keyword in the search box and search for scripts by name.

- Advanced search

  Enter keywords in the corresponding attribute search boxes to search for scripts in exact mode.

Step 4 Click the name of the script you want to modify or locate the row where the script locates and click **Manage** in the **Operation** column.

Figure 8-34 Script details page



Step 5 On the displayed script details page, view and edit basic information of the script.

In the **Basic Info** area, click **Edit**. In the displayed dialog box, edit the script details.

You can edit the script **Name** and **Remarks**.

Step 6 View and modify script content.

In the **Script content** area, click **Edit**. In the displayed dialog box, edit the script content.

----End

8.4.3 Downloading a Script

This topic describes how to download a script for local query and management.

Prerequisites

You have the management permissions for the **Script** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **Operation** > **Script** to go to the script management page.

Step 3 Select the script you want to download and click **Download** in the **Operation** column to download the script.

----End

8.4.4 Deleting a Script

This topic describes how to delete an online script and manage the scripts.

Prerequisites

You have the management permissions for the **Script** module.

Constraints

The built-in script **HSS-Agent.sh** cannot be deleted.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **Operation** > **Script** to go to the script management page.

Step 3 Delete a department.

1. Select the script you want to delete and click **Delete** in the **Operation** column.
2. In the displayed dialog box, click **OK**.

Step 4 Delete departments in batches.

Select multiple scripts at a time and click **Delete** at the bottom of the script list to delete all selected scripts together.

----End

8.5 Fast Operation

8.5.1 Managing Command Operation Tasks

A bastion host supports fast operations. You can manage many resources concurrently by executing commands. You can execute the same command on multiple host resources that use the SSH protocol through one task, and the corresponding execution results are returned accordingly.

This topic describes how to manage command tasks, including creating, executing, and stopping command tasks, and viewing task execution results.

Constraints

- Fast operation is supported by professional editions only.
- Fast operation tasks apply only to Linux hosts using the SSH protocol.
- Currently, Fast operation tasks cannot be performed on Windows host, database, or application resources.

Prerequisites

- You have the management permissions for the **Fast Operation** module.
- You have obtained the access permissions for the resources.
- The network connections between the managed hosts and the bastion host are normal.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **Operation** > **Fast Operation** > **CMD Console** to go to the quick command OM page.

Step 3 Configure fast command operation information.

Table 8-15 Fast command operation parameters

Parameter	Description
CMD	Enter the command to be executed for host resources.
execute account	• You can click the **select** link and select a created SSH account or account group. • You can also click the **Reset** link and reset the selected account or account group. **NOTE** You can select a maximum of one account for each resource.
Options	(Optional) If you have no permissions for the selected accounts, select **Sudo** to escalate your privilege and execute the task under the sudoers file.

Step 4 Execute the command task.

Click **Execute** next to the **CMD** text box to execute the command operation task.

Step 5 Stop the command operation task.

Click **Stop** to stop the task.

NOTE

Stopping a task cannot stop the corresponding job that is being executed on a certain resource.

Step 6 View the execution results.

After the command operation task is executed, check the execution results. To view execution results of historical operation tasks, see **Viewing Execution Logs**

1. In the execution result area, enter a keyword in the search box to quickly query the task execution result by resource name, execution result, host address, or execution account.
2. Click **Expand** to view the execution results of the corresponding task.
3. Click **Export** to download the corresponding execution logs in CSV format.

----End

8.5.2 Managing Script Operation Tasks

You can manage multiple resources concurrently by executing scripts. This helps improve operation efficiency. You can execute the same script on multiple host resources that use the SSH protocol through one task, and the corresponding execution results are returned accordingly.

This topic describes how to manage script operation tasks, including creating, executing, and stopping script operation tasks, and viewing task execution results.

Constraints

- Fast operation is supported by professional editions only.
- Fast operation tasks apply only to Linux hosts using the SSH protocol.
- Currently, Fast operation tasks cannot be performed on Windows host, database, or application resources.

Prerequisites

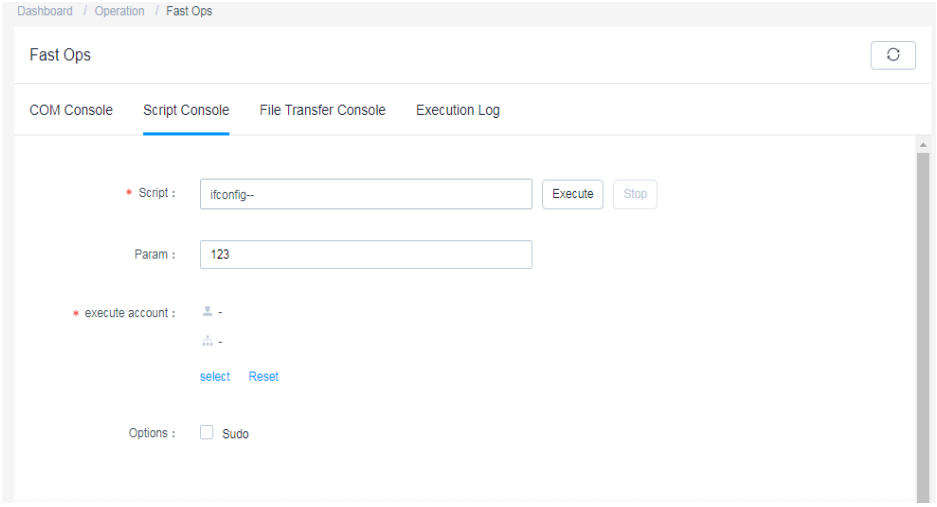
- You have the management permissions for the **Fast Operation** module.
- You have obtained the access permissions for the resources.
- The network between the managed hosts and the bastion host is connected.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **Operation** > **Fast Operation** > **Script Console** to go to the quick script operation page.

Figure 8-35 Script Console



Step 3 Configure fast script operation information.

Table 8-16 Fast script operation parameters

Parameter	Description
Script	The script to be executed for the host resources. • You can select the script content in the script management module or upload a new local script file.
Param	(Optional) user-defined script parameter.
execute account	• You can click the **select** link and select a created SSH account or account group. • You can also click the **Reset** link and reset the selected account or account group. **NOTE** You can select a maximum of one account for each resource.
Options	(Optional) If you have no permissions for the selected accounts, select **Sudo** to escalate your privilege and execute the task under the sudoers file.

Step 4 Execute the script operation task.

Click **Execute** next to the **Script** text box to execute the script operation task.

Step 5 Stop the script operation task.

Click **Stop** to stop the task.

NOTE

Stopping a task cannot stop the corresponding job that is being executed on a certain resource.

Step 6 View the execution results.

After the script operation task is executed, check the execution results. To view execution results of historical operation tasks, see **Viewing Execution Logs**

1. In the execution result area, enter a keyword in the search box to quickly query the task execution result by resource name, execution result, host address, or execution account.
2. Click **Expand** to view the execution results of the corresponding task.
3. Click **Export** to download the corresponding execution logs in CSV format.

----End

8.5.3 Managing File Transfer Tasks

A bastion host supports fast operations. You can quickly upload system disk files or local files to paths of many managed hosts at a time. You can upload one or more files to multiple hosts with just one file transfer task and the system returns the execution results.

This topic describes how to manage file transfer tasks, including creating, executing, and stopping file transfer tasks, and viewing task execution results.

Constraints

- Fast operation is supported by professional editions only.
- Fast operation tasks apply only to Linux hosts using the SSH protocol.
- Currently, Fast operation tasks cannot be performed on Windows host, database, or application resources.

Prerequisites

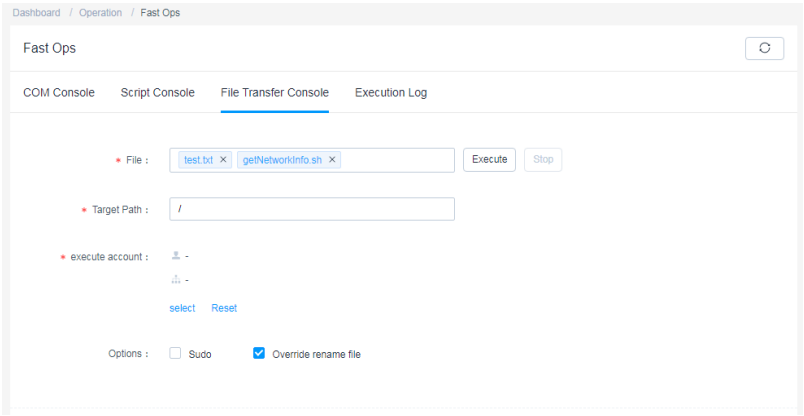
- You have the management permissions for the **Fast Operation** module.
- You have obtained the access permissions for the resources.
- The network between the managed hosts and the bastion host is connected.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **Operation** > **Fast Operation** > **File Transfer Console** to go to the **File Transfer Console** tab.

Figure 8-36 File Transfer Console



Step 3 Configure fast file transfer information.

Table 8-17 Parameters for fast file transfer

Parameter	Description
File	Files to be transferred. The system disk file is selected by default. You can also upload the local file to the personal net disk and then select the file. A maximum of 10 files can be selected.
Target Path	Absolute path on the host to which files are transferred
execute account	• The managed resource account allowed to execute the script. You can **select** a created SSH account or account group. • You can also **Reset** the selected account or account group. **NOTE** You can select a maximum of one account for each resource.
Options	(Optional) • (Optional) If you have no permissions for the selected accounts, select **Sudo** to escalate your privilege and execute the task under the sudoers file. • **Override rename file**: If a file with the same name as the file to be uploaded exists in the target path of the destination host, the existing file will be overwritten by the newly uploaded file.

Step 4 Execute the file transfer task.

Click **Execute** next to the **File** text box to execute the file transfer task.

Step 5 Stop the file transfer task.

Click **Stop** to stop the task.

NOTE

Stopping a task cannot stop the job that is being executed until the job is done.

Step 6 View the execution results.

After the file transfer task is executed, check the execution results. To view execution results of historical operation tasks, see **Viewing Execution Logs**

1. In the execution result area, enter a keyword in the search box to quickly query the task execution result by resource name, execution result, host address, or execution account.
2. Click **Expand** to view the execution results of the corresponding task.
3. Click **Export** to download the corresponding execution logs in CSV format.

----End

8.5.4 Managing Fast Operation Task Execution Logs

This topic describes how to manage execution logs after fast operation tasks are executed. You can view task details, export execution logs, and delete execution logs.

Prerequisites

- You have the management permissions for the **Fast Operation** module.
- Fast operation tasks (including fast command tasks, script tasks, and file transfer tasks) have been executed.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **Operation** > **Fast Operation** > **Execution Log** to go to the **Execution Log** tab.

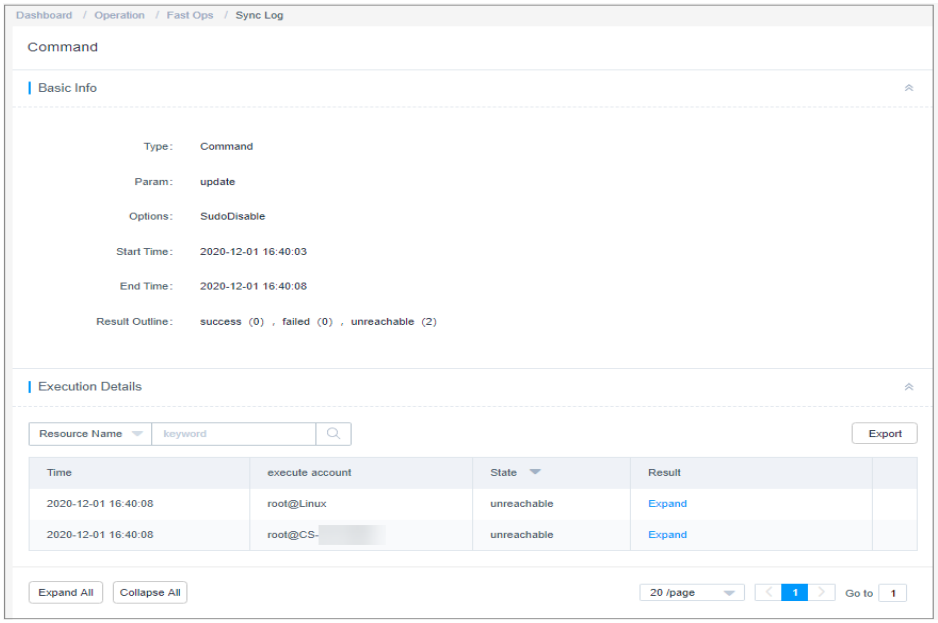
Step 3 Query logs.

Enter a keyword in the search box and search for execution logs by execution parameter.

Step 4 View execution log details.

1. Select the execution log you want to view and click **Detail**.

Figure 8-37 Execution log details



2. In the **Basic Info** area, view the basic information and brief result of the operation task.
3. In the **Execution Details** area, view the detailed execution result of the operation task.
4. In the **Execution Details** area, click **Export** to export the detailed execution result of the operation task.

Step 5 Download execution logs.

Select the execution log and click **Download** in the **Operation** column to download the log in CSV format.

Step 6 Delete execution logs.

- To delete one execution log, select the one you want and click **Delete** in the **Operation** column of the corresponding row to delete it.
- To delete multiple execution logs at a time, select the ones you want and click **Delete** at the bottom of the list to delete the selected logs together.

----End

8.6 OM Task

8.6.1 Creating an OM Task

You can create auto OM tasks to let the bastion host automatically execute the task according to task steps, task types, resources, and execution mode you configure. For example, you can create an OM task to upload system disk files or local files to many designation hosts. With the fast operation, a bastion host automatically executes OM tasks based on your configured execution period and time. In addition, it can automatically execute multiple types of tasks concurrently on multiple devices, improving the OM efficiency.

- Multiple OM tasks can be concurrently performed step by step on multiple resources that use the SSH protocol, including command, script, and file transfer OM tasks.
- After an operation task is submitted, the system automatically performs operations in sequence and returns the execution result.

Constraints

- Fast operation is supported by professional editions only.
- Automated operation tasks can be executed only on Linux host resources that use the SSH protocol.
- Currently, automated operation tasks cannot be performed on Windows host, database, or application resources.
- Operation tasks created by you can be managed only by yourself and cannot be managed by other system users.

Prerequisites

- You have the management permissions for the **OM Task** module.
- You have obtained the access permissions for the resources.
- The network between the managed hosts and the bastion host is connected.

Creating an Automated Operation Task

Step 1 Log in to your bastion host.

Step 2 Choose **Operation** > **OM Task** > **Task**.

Step 3 Click **New** in the upper right of the **OM Task** area.

Step 4 Configure basic information about the task.

Table 8-18 Basic task information parameters

Parameter	Description
Task Name	Name of the task. The value of **Task Name** must be unique in the system.
Timing	Execution mode of the operation task. The options are **Manual**, **Scheduled**, and **Cycle**. You need to configure the execution time if **Fixed-Time** or **Cycle** is selected. • **Manual**: indicates that you need to manually start the task. • **Fixed-Time**: indicates that the task will start at the specified time. This type of rule is executed only once. • **Cycle**: indicates that the task will start periodically at the specified interval. This type of password rule is triggered periodically.
Execute Time	Date when the task is periodically executed. The default execution time is at 00:00 every day.

Parameter	Description
Cycle Frequency	Task execution frequency. • The options are every minute, every hour, every day, every week, and every month. • Set the **End Time** for this type of tasks. Otherwise, the tasks will be executed periodically forever.
Options	(Optional) If you have no permissions for the selected accounts, select **Sudo** to escalate your privilege and execute the task under the sudoers file.
Remarks	Brief description of the operation task.

Step 5 Click **Next** and start to configure execution accounts or account groups.

Step 6 Click **Next** and set task steps.

1. Click **Add Step** and select **Command**, **Script**, or **Transfer File**.
2. Select one or more task types and set task parameters.

   NOTE

   Multiple steps can be added to an operation task.

Step 7 Click **OK**. The system returns to the task list page, and you can view the information about the new operation task.

You can **download the execution logs** to obtain the task execution results.

----End

Follow-up Operations

On the **OM Task** page, you can manage all created OM tasks, including managing related execution accounts and deleting, enabling, or disabling OM tasks.

- To quickly relate an OM task to more accounts, select the task and click **Relate** in the **Operation** column.
- To delete an OM task, select the task and click **Delete** in the **Operation** column.
- To disable a periodic OM task, select the enabled ones and click **Disable** at the bottom of the list. When the status of those tasks changes to **Disabled**, they are hibernated.
- To execute an OM task, click **Execute** in the **Operation** column.

  NOTE

  During the task execution, task steps are performed in sequence. When a task step is interrupted or the selected resource is unreachable, the subsequent task steps will be stopped.

8.6.2 Querying and Modifying OM Tasks

You can edit steps in an OM task anytime you want to meet your changed requirements. You can view and edit task configuration, including the basic task

settings, task steps, as well as execution date, period, and account or account group.

Prerequisites

- You have the management permissions for the **OM Task** module.
- You have obtained the access permissions for the resources.

Querying and Editing Task Configurations

Step 1 Log in to your bastion host.

Step 2 Choose **Operation** > **OM Task** > **Task**.

Step 3 Query OM tasks.

- Quick search

  Enter a keyword in the search box to quickly query tasks by task name, resource name, and execution account.

- Advanced search

  Enter keywords in the corresponding attribute search boxes to search for tasks in exact mode.

Step 4 Click the name of the task or click **Manage** in the **Operation** column of the task row.

Step 5 On the displayed OM task details page, view and edit basic information.

In the **Basic Info** area, click **Edit**. In the displayed dialog box, edit the details.

- You can edit **Task Name** and **Timing**.

Step 6 On the displayed OM task details page, view and edit basic information of the execution account.

- To add or delete an execution account, click **Edit** in the **Execute Account** area and complete modifications in the displayed dialog box.
- To only remove an execution account, click **Remove** in the row of the execution account. The removed account then cannot be to execute the OM tasks on the corresponding host.

Step 7 In the displayed dialog box, view and edit basic information of the execution account.

- To add or delete an execution account group, click **Edit** in the **Execute Account Group** area and complete modifications in the displayed dialog box.
- To only remove an execution account group, click **Remove** in the row of the execution account group. Each account in the removed account group cannot be used for executing OM tasks on the corresponding host.

Step 8 In the displayed OM task dialog box, view and edit task steps.

- In the **Task Step** area, click **Add**. In the displayed **Add Step** dialog box, add one or more task steps as needed.
- To modify an added task step, click **Edit** in the row of the corresponding step and complete modifications in the then displayed dialog box.

- To only remove a task step, click **Remove** in the row of the task step. The removed task step will no longer be executed in the OM task.

Step 9 View the execution history of an OM task in the **History** area.

- To view the execution details of an OM task, click **View** in the **Operation** column of the corresponding row of the OM task.
- To download execution details, click **Export** in the **Operation** column of the corresponding row of the OM task.

----End

8.6.3 Managing OM Task Execution Logs

After an OM task is executed, an execution log is generated. You can view the task execution result in the log, including the execution results and details.

This topic describes how to manage execution logs, including viewing, downloading, and deleting execution logs.

Prerequisites

You have the management permissions for the **OM Task** module.

Viewing Log Details

Step 1 Log in to your bastion host.

Step 2 Choose **Operation** > **OM Task** > **Execution Log** to go to the task list page.

Step 3 Query OM task execution logs.

Quick search: Enter a keyword in the search box and search for O&M tasks by task name.

Step 4 Select the task you want and click **Detail** in the **Operation** column.

- In the **Basic Info** area, view the basic information and brief result of the operation task.
- In the **Execution Details** area, view and export the detailed execution result of the OM task.

----End

Downloading OM Task Execution Logs

Step 1 Log in to your bastion host.

Step 2 Choose **Operation** > **OM Task** > **Execution Log** to go to the task list page.

Step 3 Select the task you want and click **Download** in the **Operation** column to download execution logs in CSV format.

Step 4 Click **View** to go to the task details page.

You can view the basic information and brief execution result of an operation task. In the execution details area, you can view and export the detailed execution result of an operation task.

Step 5 Click **Export** to download the current execution log file in CSV format to the local computer.

Step 6 To delete one execution log, select the one you want and click **Delete** in the **Operation** column to delete it.

To delete multiple execution logs at a time, select the ones you want and click **Delete** at the bottom of the list to delete the selected logs together.

----End

Deleting Execution Logs

Step 1 Log in to your bastion host.

Step 2 Choose **Operation** > **OM Task** > **Execution Log** to go to the task list page.

Step 3 To delete on task logs, select the one you want and click **Delete** in the **Operation** column to delete it.

Step 4 To delete multiple execution logs at a time, select the ones you want and click **Delete** at the bottom of the list to delete all selected logs together.

----End

9 Ticket

9.1 Ticket Configuration Management

9.1.1 Configuring the System Ticket Modes

A ticket mode consists a series of ticket settings which restrict the resource scope that can be applied for through an access control ticket and the method a ticket is submitted. There are two modes of ticket settings:

- **Basic Settings**: In this mode, you can restrict the access scope of resources that can be applied for through an access control ticket and specify the way to submit a command control ticket.
- **Advanced Settings**: In this mode, you can restrict the access scope of resources that can be applied for through access control ticket from multiple dimensions, such as the user department, user role, and resource department.
  - After a **User Department** is configured, users in the department form a user pool. Only users in the user pool can apply for resources in the resource pool.
  - If no **User Role** is configured, all users in the user pool can apply for resources in the resource pool.
  - If **User Role** is configured, only users of specified roles in the user pool can apply for resources in the resource pool.
- A user pool is a group of users specified by the user department and user role. After a department or role is associated, users of the department or role can apply for resources in the resource pool.
- A resource pool is a group of resources specified by the resource department. After a department is associated, the resources of the department can be applied for by users in the user pool.

Prerequisites

You have the management permissions for the **System** module.

Configuring the Basic Ticket Settings

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Ticket**.

Step 3 In the **Basic Settings** area, click **Edit**.

Set the **Application scope** of resources that can be viewed by the user and the **Submission mode** of command approval ticket.

Table 9-1 Parameter description

Parameter	Description
Application scope	Specifies the scope of resources that can be applied for with the access control ticket. • The default value is the current department. • **This Department**: When applying for access control tickets, you can apply for the access control permission on the resources of the current department, excluding the resources of lower-level departments. • **This Dept and lower level**: When applying for access control tickets, you can apply for access control permissions for resources of the current department and lower-level departments. • **All**: You can apply for access control permissions for all system resources.
Submission mode	Specifies the way to submit a ticket. The options are **Manual** and **Auto**. • By default, **Manual** is selected. • **Manual**: After a command control ticket is generated, submit the ticket to the administrator for approval. • **Auto**: After a command control ticket is generated, it is automatically submitted to the administrator for approval.

Step 4 Click **OK**. You can then view the configured ticket settings.

----End

Configuring the Advanced Ticket Settings

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Ticket**.

Step 3 In the **Advanced Settings** area, click **Edit**.

Step 4 Configure the user pool.

Select user department or user role.

Step 5 Click **Next** and configure resource department.

Step 6 Click **OK**. You can then view the configured ticket settings.

----End

Follow-up Operations

- To modify the resource pool and user pool in a certain piece of advanced settings, click **Edit** in the corresponding row. In the displayed dialog box, select other user and/or resource departments.
- To delete the restrictions of a certain piece of advanced settings, click **Delete** in the corresponding row. Deleted authentication information cannot be recovered. Exercise caution when performing this operation.

9.1.2 Configuring the Ticket Approval Process

The ticket approval process is the policy that specifies how to approve a system ticket. You can customize the approval process in terms of the approval process mode, approval form, approval node, approval series, and final approval node to enhance the management of the ticket approval process. The following are some major factors in an approval process:

- Approval process type

  There are two types of application processes, the hierarchical process and fixed process. The hierarchical process is applicable to the approval within a department, and the fixed process is applicable to approval across departments.

- Approval form

  Approval form is used to specify how a ticket is approved when multiple approvers are involved in the approval process. There are two forms, multiplayer approval and countersign approval. In multiplayer approval form, a ticket is approved as long as it is approved by any of the approvers. In countersign approval form, a ticket is approved only after it is approved by all approvers.

- Approval node

  Approval node is used to specify attributes of the approver in the approval process, including the department and role attributes. The department administrator who meets the department and role requirements has the approval permission.

- Approval series

  Approval series refers to the number of approval levels. If you select the hierarchical approval process, the approval series must be specified.

- Final approval node

  After approvals at other levels complete, **admin** performs the final approval.

This topic describes how to customize a ticket approval process.

Prerequisites

You have the management permissions for the **System** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Ticket**.

Step 3 In the **Approval process** area, click **Edit**.

In the displayed **Approval process** dialog box, specify required parameters.

Table 9-2 Parameters for configuring ticket approval processes

Parameter	Description
Approval process type	Approval process. The options are **Classification** for hierarchical process and **Regular** for fixed process. After the ticket approval process is configured, the ticket goes to each approver in sequence for approval. If there is no qualified approver at one stage, the ticket is approved at this stage by default. Then the ticket is routed to the next stage. • Hierarchical process (default): Approval is performed level by level based on the approval level. • Fixed process: Approval is performed based on the fixed approval node. **NOTE** You can send an email to notify the approver of the ticket status in the following ways: – Set an outgoing email address by referring to **Configuring the Outgoing Mail Server** and ensure that emails can be sent properly. – On the **Ticket** tab, set the alarm level to **High**. For details, see **Configuring Alarm Levels**.
Approval form	How the approval is performed. The options are **Multiplayer** and **Countersign**. • The multiplayer approval mode is used by default. • **Multiplayer**: indicates that an approval from only one approver at each level is required. After the ticket is approved at a certain level, it becomes invisible to other approvers at the same level. If a ticket is rejected by any approver at the same level, the ticket is rejected. • **Countersign**: A ticket will not be transferred to the next level for approval until all approvers at the same level approve the ticket. If any approvers reject the ticket, the ticket is rejected. • During the approval process, the admin account can review all tickets on any node, and the review result is the final result.

Parameter	Description
Approval node	Set the approver attribute of the node. The department attribute and role attribute must be set. After the setting is complete, the users who meet the department and role requirements automatically become the approvers of the node. If no users meet the department and role requirements, the system automatically searches for qualified users in the superior department until **HQ** is reached. • Department attribute: includes **User department** and **Resource department**. • **Role attribute**: The role must have the administrator and ticket approval permissions. The default role is the department administrator. For example, if you select **User department**, the administrator of the department to which the ticket applicant belongs is select as the approver. If you select **Resource department**, the administrator of the department to which the resource belongs is selected as the approver.
Approval series	Number of approval levels. If you select **Classification** for approval process, this parameter is mandatory. • A maximum of five levels of approval series can be set. • The default value is **1**, indicating that an approval level is required.
Final approval node	Whether to enable final approval by **admin**. Final approval is enabled by default ( ). • : indicates that final approval by **admin** is disabled. • : indicates that final approval by **admin** is enabled. This means the ticket cannot be approved until all approvers in other levels approve it and the **admin** user approves it. **NOTE** If no qualified approvers at all approval levels, the approval from the **admin** user is required no matter whether the final approval is enabled.

Step 4 Click **OK**. You can then view the configured ticket approval process.

----End

9.2 Creating an ACL Ticket

If you have no permissions to access some resources, you can submit a ticket to apply for the required permissions.

Prerequisites

You have the management permissions for the **ACL Ticket** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **Tickets** > **ACL Ticket** to go to the ACL ticket page.

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

In the displayed **New ACL ticket** page, configure basic information.

Table 9-3 Parameters for configuring an ACL ticket

Parameter	Description
Operation Time	Specifies the time period for accessing the resource. The start time and end time must be set.
File Transfer	File transfer permissions, including uploading and downloading files.
Options	Whether to enable the functions in the session window when a web browser is used for O&M. • **File Manage**: Permissions to manage files or folders. If **Upload** or **Download** is selected for **File transfer**, **File Manage** must be enabled. • **uplink clipboard** and **downlink clipboard**: Permissions to use the clipboard function on hosts with **Protocol** set to **RDP**. • **Watermark**: Permissions to display the watermark of the user login name in the operation session window. • **Keyboard Audit**: This function records the information entered through the keyboard. • **Kiosk**: For applications that can be managed through a browser, you can use this function to hide the address bar and disable F12, right-click, and the browser toolbar. You can use F12 instead of Ctrl to implement shortcut key operations.
Remarks	(Optional) Briefly describe the reason for applying for the resource access control permission or other information.

Step 4 Click **Next** and select an account for which the permissions are applied.

Step 5 Click **OK** to submit the ticket.

After the administrator approves the ticket, you obtain the access permission for the resources.

----End

Follow-up Operations

- After a ticket is submitted, the administrator will receive a notification in the message center. They can view the ticket details. The ticket will also display in the ticket approval page. The administrator can choose to approve or reject the ticket.

- To modify a submitted ticket, click **Withdraw** to cancel the ticket. Then, the ticket status changes to **Revoked**.
- To view or modify the ticket information after the ticket is created, click **Manage** to go to the ticket details page.

  NOTE

  For tickets in the **approving** status, you can only view the details but cannot modify the content. Only the ticket in the **Revoked** or **Not submitted** state can be modified.
- If a submitted ticket has expired, click **Delete** to delete it. You can also select multiple tickets and click **Delete** in the lower left corner to delete them in batches.

CAUTION

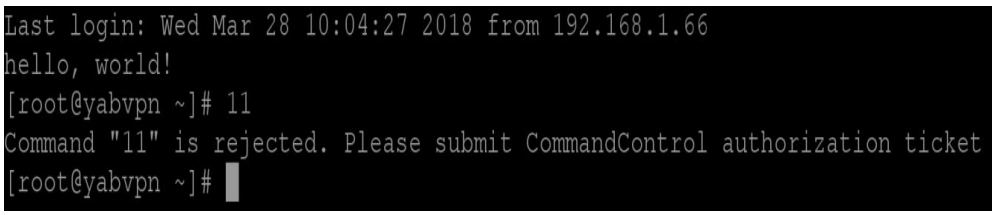
Deleted tickets cannot be recovered. Exercise caution when performing this operation.

9.3 Managing Command Approval Tickets

You can enable dynamic authorization of operations on Linux server. This enhances the restriction of critical operations.

During O&M on Linux hosts, if an operation command triggers the command rules for dynamical approval, the system automatically intercepts the operation command and generates a command approval ticket. The command approval ticket is sent to the administrator. After it is approved by the administrator, you obtain the permission to run the operation command on the Linux host.

Figure 9-1 Example of command interception



This topic describes how to manage command approval tickets.

Constraints

A bastion host can intercept sensitive operation commands and generate tickets only for Linux hosts using the SSH or Telnet protocol.

Prerequisites

- You have the management permissions for the **Command Approval Ticket** module.
- Command interception has been triggered, and a command approval ticket has been generated.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **Tickets** > **Command Approval Ticket**.

Figure 9-2 Command Approval Ticket

Step 3 Submit a ticket.

Command approval tickets can be submitted automatically or manually. For details, see **Configuring Basic Ticket Settings**.

- If the automatic submission mode is selected, the system automatically submits the ticket to the administrator for approval.
- If the manual submission mode is selected, click **submit** to send it to the administrator for approval in the **Operation** column on the **Command Approval Ticket** list page.
- If the ticket is rejected by the administrator, you can modify the ticket information and submit it again.

Figure 9-3 Submitted ticket

Step 4 Withdraw a ticket.

Click **Withdraw** in the **Operation** column of the ticket you want to cancel. The ticket status then changes to **Revoked**.

Step 5 Modify ticket information.

- Click **Manage** to go to the details page.
- Click **Edit** on the details page and modify the authorized operation duration.

NOTE

For tickets in the **approving** status, you can only view the details but cannot modify the content. Only the ticket in the **Revoked** or **Not submitted** state can be modified.

Step 6 Delete a ticket.

- To delete one ticket, in the row of the ticket you want to delete, click **Delete** in the **Operation** column.
- To delete multiple tickets, select the ones you want to delete and click **Delete** at the bottom of the ticket list to delete all selected tickets together.

CAUTION

Deleted tickets cannot be recovered. Exercise caution when performing this operation.

----End

Follow-up Operations

- After a ticket is submitted, the administrator will receive a notification in the message center. They can view the ticket details. The ticket will also display in the ticket approval page. The administrator can choose to approve or reject the ticket.
- After the administrator approves the ticket, you then obtain the command operation permissions within the authorization scope and period.
- After the permission in the ticket is revoked by the administrator, the operation commands will be intercepted again.

9.4 Managing Database Approval Tickets

You can enable dynamic approval of database operations. This enhances a more strict management of critical database operations.

During O&M on databases, if an operation command triggers the database rules for dynamical approval, the system automatically intercepts the operation command and generates a database approval ticket. The command approval ticket is sent to the administrator. After the administrator approves the ticket, you obtain the permission to run the operation command.

This topic describes how to manage database approval tickets.

Constraints

- The database operation audit is available only in professional editions.
- A bastion host can intercept sensitive operation commands and generate tickets only for MySQL and Oracle databases.
- A database approval ticket cannot be manually created. It is automatically generated when a user attempts to run a command which triggers a database rule.

Prerequisites

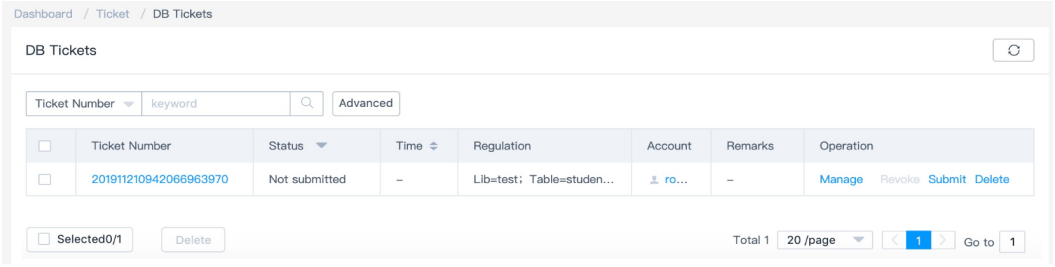
- You have the management permissions for the **DB Tickets** module.
- Operation interception has been triggered, and a database approval ticket has been generated.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **Tickets** > **DB Tickets**.

Figure 9-4 Database approval ticket list



Step 3 Submit a ticket.

- In the row of the ticket you want to submit, click **Submit** in the **Operation** column to submit the ticket to the administrator for approval.
- If the ticket is rejected by the administrator, you can modify the ticket information and submit it again.

Step 4 Withdraw a ticket.

Click **Withdraw** in the **Operation** column of the ticket you want to cancel. The ticket status then changes to **Revoked**.

Step 5 Modify ticket information.

- Click **Manage** to go to the details page.
- Click **Edit** on the details page and modify the authorized operation duration.

NOTE

For tickets in the **approving** status, you can only view the details but cannot modify the content. Only the ticket in the **Revoked** or **Not submitted** state can be modified.

Step 6 Delete a ticket.

- To delete one ticket, in the row of the ticket you want to delete, click **Delete** in the **Operation** column.
- To delete multiple tickets, select the ones you want to delete and click **Delete** at the bottom of the ticket list to delete all selected tickets together.

CAUTION

Deleted tickets cannot be recovered. Exercise caution when performing this operation.

----End

Follow-up Operations

- After a ticket is submitted, the administrator will receive a notification in the message center. They can view the ticket details. The ticket will also display in the ticket approval page. The administrator can choose to approve or reject the ticket.
- After the administrator approves the ticket, you then obtain the operation permissions within the authorization scope and period.

- After the permission in the ticket is revoked by the administrator, the operation commands will be intercepted again.

9.5 Ticket Approval

After a ticket is created by a system user or generated by the system, the ticket goes to the specified approvers. The approvers receive a ticket approval notification in the message center. They can view tickets to be approved on the **Ticket approval** page.

This topic describes how to manage tickets submitted by others. You can view ticket details as well as approve, reject, and revoke a ticket approval.

Prerequisites

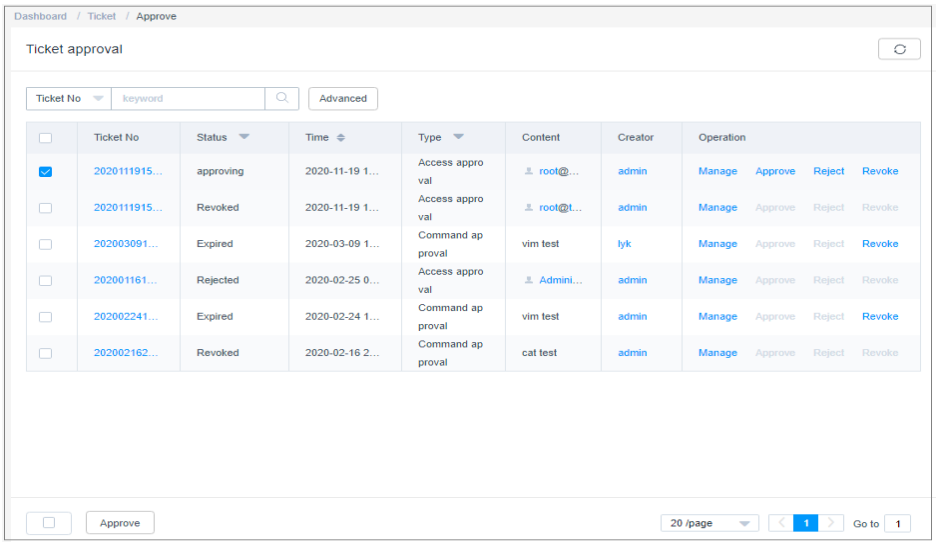
You have the management permissions for the **Ticket approval** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **Ticket** > **Ticket approval**.

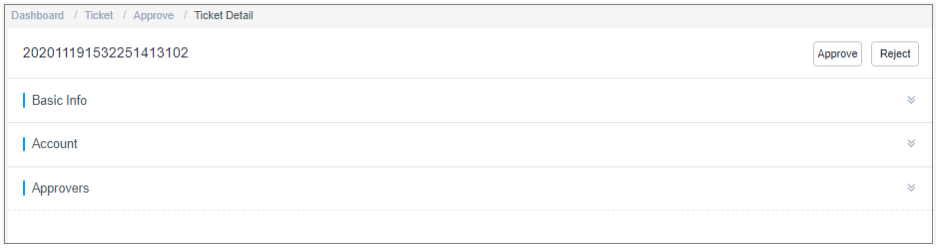
Figure 9-5 Ticket approval



Step 3 Views details about tickets.

In the row of a ticket you want to manage, click **Manage** in the **Operation** column. On the displayed ticket details page, view the basic information, account list, and approver list of the ticket.

Figure 9-6 Ticket details



Step 4 Approve the ticket.

- To approve one ticket, click **Approve** in the **Operation** column of the corresponding row.
- To approve multiple tickets at a time, select the ones you want and click **Approve** in the lower left corner of the list to approve them together.

Step 5 Reject a ticket.

In the row of the ticket you want to reject, click **Reject** in the **Operation** column.

Step 6 Cancel a ticket.

In the row of the ticket you want to cancel the authorization, click **Cancel** in the **Operation** column.

----End

9.6 Ticket Application Examples

Case 1: Creating a Classification Approval Ticket to Control Resource Requests Based on User Departments

Prerequisites

- You have configured required parameters, including departments, users, roles, and resources. For more details, see **Department**, **User**, and **Resource**.
- The ticket approval process is configured as shown in **Table 9-4**. For more details about ticket approval process, see **Configuring the Ticket Approval Process**.

Table 9-4 Parameters for configuring a ticket approval process

Parameter	Value
Approval process type	Classification
Approval form	Multiplayer
Approval node	User department – Department Manager
Approval series	3

Approval Process

A user submits a ticket to apply for access permissions for resources based on the department that the user belongs to.

Both user A and user B (lower-level administrators) have the approval right. If either one of them approves, the ticket is approved. If either one of them rejects, the ticket is rejected. After one of the lower-level administrators approves the ticket, the workflow goes to the next stage for user C (middle-level administrator) to review. The rest can be deduced by analogy. After user D (higher-level administrator) approves the ticket, the user obtains the requested permissions. If the ticket is rejected at any stage during the approval, it fails to be approved and the user cannot obtain the permissions.

NOTE

An account with permissions of the admin administrator can approve or reject any ticket on any node, and the result is the final result.

Case 2: Creating a Classification Approval Ticket to Control Resource Requests Based on Resource Departments

Prerequisites

- You have configured required parameters, including departments, users, roles, and resources. For more details, see **Department**, **User**, and **Resource**.
- The ticket approval process is configured as shown in **Table 9-5**. For more details about ticket approval process, see **Configuring the Ticket Approval Process**.

Table 9-5 Parameters for configuring a ticket approval process

Parameter	Value
Approval process type	Classification
Approval form	Multiplayer
Approval node	User department – Department Manager
Approval series	3

Approval Process

A user submits a ticket to apply for access permissions for resources based on the department that the resource belongs to.

If user D (lower-level administrator) approves the ticket, the workflow goes to the next stage for user E (middle-level administrator) to review. If user D rejects the ticket, the ticket is rejected. The rest can be deduced by analogy. After user F (higher-level administrator) approves the ticket, the user obtains the requested permissions. If the ticket is rejected at any stage during the approval, it fails to be approved and the user cannot obtain the permissions.

NOTE

An account with permissions of the admin administrator can approve or reject any ticket on any node, and the result is the final result.

Case 3: Creating a Ticket with Fixed Approval Process and Countersign Form

Prerequisites

- You have configured required parameters, including departments, users, roles, and resources. For more details, see **Department**, **User**, and **Resource**.
- The ticket approval process is configured as shown in **Table 9-6**. For more details about ticket approval process, see **Configuring the Ticket Approval Process**.

Table 9-6 Parameters for configuring a ticket approval process

Parameter	Value
Approval process type	Regular
Approval form	Countersign
Approval node	3

Approval Process

A user submits a ticket to apply for access to resources of a department that the user does not belong to.

Both user B and user C have the approval right. If both of them approve, the ticket is approved. If either one of them rejects, the ticket is rejected. After the engineering department administrators approve the ticket, the workflow goes to the next stage for user D (finance department administrator) to review. The rest can be deduced by analogy. After user E (finance department administrator) approves the ticket, the user obtains the requested permissions. If the ticket is rejected at any stage during the approval, it fails to be approved and the user cannot obtain the permissions.

NOTE

An account with permissions of the admin administrator can approve or reject any ticket on any node, and the result is the final result.

10 Audit

10.1 Live Session

10.1.1 Viewing Live Sessions

After a system user logs in to a managed resource via a bastion host, the audit administrator will receive session records in real time. The audit administrator can view and audit live operation sessions to prevent losses caused by violations.

Prerequisites

- You have the management permissions for the **Live Session** module.
- There is at least one live session.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **Audit** > **Live Session**.

Step 3 Query live sessions.

- Quick search

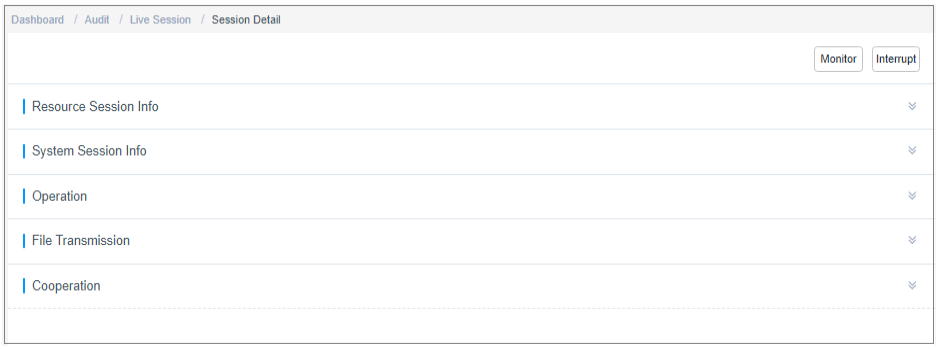
  Enter a keyword in the search box to quickly query live sessions by resource name, account, user, or source IP.

- Advanced search

  Enter keywords in the corresponding attribute search boxes to search for live sessions in exact mode.

Step 4 Click **Detail** in the **Operation** column of the live session you want to view.

Figure 10-1 Viewing Live Sessions



Step 5 View resource session information, system session information, operation records, file transmission records, and collaborative session records.

----End

10.1.2 Monitoring Live Sessions

After a system user logs in to a managed resource through a bastion host, the audit administrator will receive session records in real time. The audit administrator can monitor live sessions to audit real-time operations of other system users.

Prerequisites

- You have the management permissions for the **Live Session** module.
- There is at least one live session.
- Currently, only H5 O&M sessions and SSH client sessions are supported.

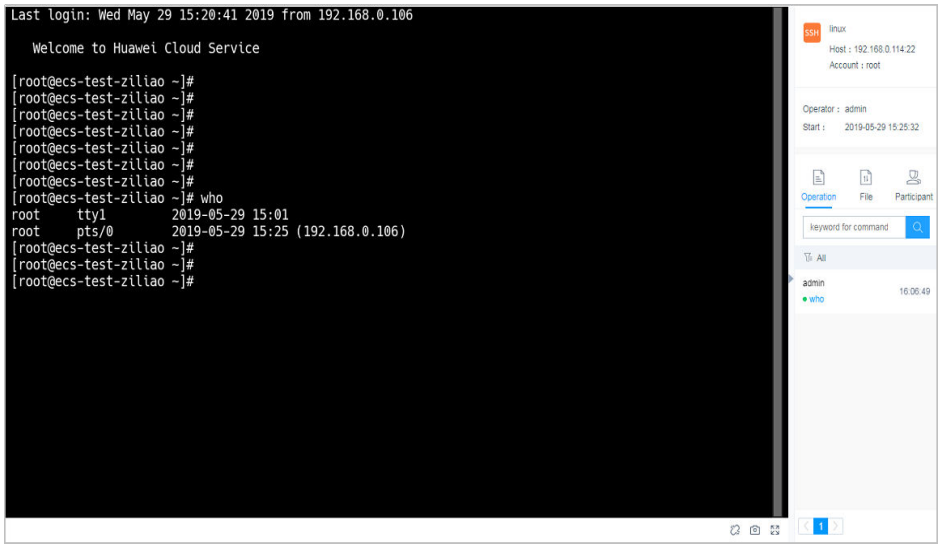
Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **Audit** > **Live Session**.

Step 3 Click **Monitor** in the **Operation** column of the live session you want to monitor. The OM session window is visible to you.

Figure 10-2 Monitoring Live Sessions



Step 4 In the displayed session window, view real-time operations, historical OM operations, file transmission records, and participant records of the session.

----End

10.1.3 Interrupting a Live Session

After a system user logs in to a managed resource through a bastion host, the audit administrator will receive session records in real time. When discovering violations or high-risk operations, the audit administrator can interrupt the session to prevent the system user from performing further operations.

Prerequisites

- You have the management permissions for the **Live Session** module.
- There is at least one live session.

Procedure

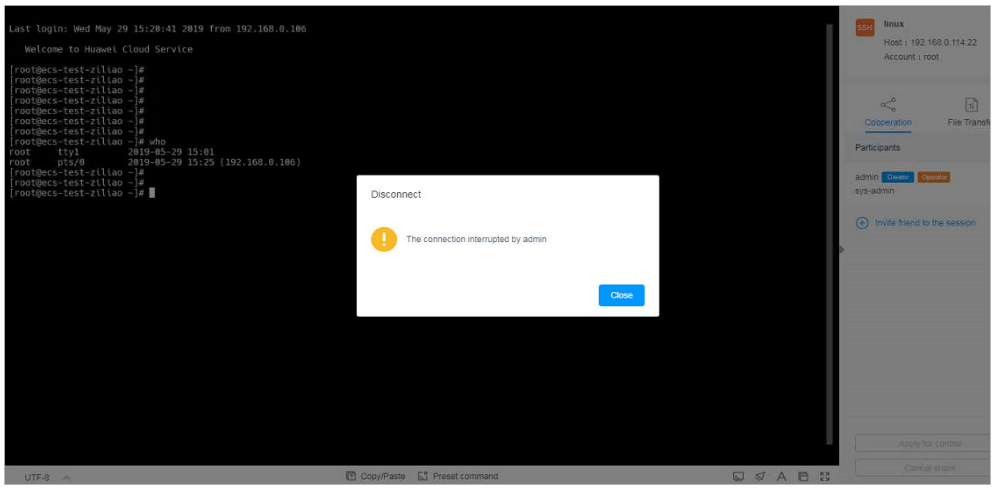
Step 1 Log in to your bastion host.

Step 2 Choose **Audit** > **Live Session**.

Step 3 Click **Interrupt** in the **Operation** column of the session to forcibly disconnect the session.

After the session is interrupted, the session window is immediately disconnected and the system user receives a message indicating that the session is interrupted.

Figure 10-3 Session interrupted



----End

10.2 History Session

10.2.1 Viewing History Sessions

After an operation is finished, the audit administrator will receive a history session record as well. The audit administrator can query operation record details and audit historical sessions online.

CAUTION

Sensitive data may exist in the video files to be audited. Exercise caution when checking these files to prevent information leaks.

Constraints

- Text and video audit are available for operations performed through a web browser.
- For O&M operations, file transfer, and database operations through an SSH client, video audit is unavailable.
- Details about account verification for accessing managed resources will not be recorded.
- Only valid session logs can be played. Valid session logs start when you initiate a session and end when the last operation is completed.

Prerequisites

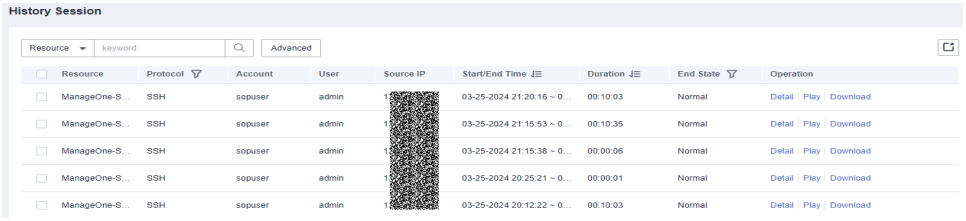
- You have the management permissions for the **History Session** module.
- The OM session has finished.

Viewing History Sessions

Step 1 Log in to your bastion host.

Step 2 Choose **Audit** > **History Session**.

Figure 10-4 History Session



NOTE

The **More** operation in the **Details** column is removed from version 3.3.42.0 or later versions.

Step 3 Query history sessions.

- Quick search

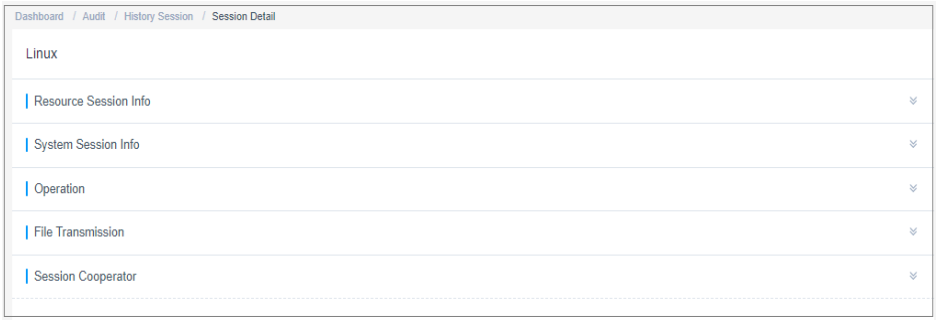
  Enter a keyword in the search box to quickly query history sessions by resource name, account, user, or source IP.

- Advanced search

  Enter keywords in the corresponding attribute search boxes to search for history sessions in exact mode.

Step 4 Click **Detail** in the **Operation** column of the history session you want to view.

Figure 10-5 Viewing History Sessions



Step 5 View resource session information, system session information, operation records, file transmission records, and collaborative session records.

For a history session, you can view the resource name, type, host IP address, account, start and end time, session duration, session size, operation user, source IP address and MAC address of the operation user, login mode, operation records, file transfer records, and session collaboration records.

----End

Online Playback of History Session

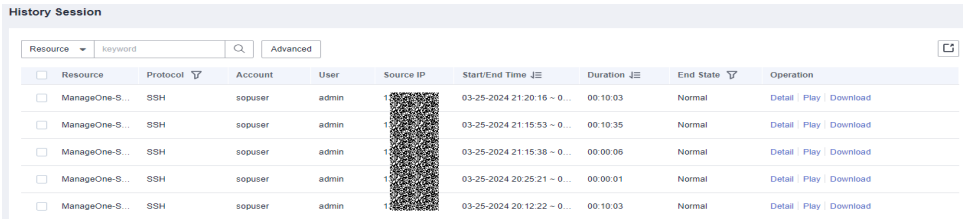
The total duration and playable duration of a downloaded video file may be different because the logout time and last operation time are different.

- The total duration starts from the time when a system user logs in to a resource to the time they log out of the resource.
- The playable duration starts from the time a system user logs in to a resource to the time the last session is complete.

Step 1 Log in to your bastion host.

Step 2 Choose **Audit** > **History Session**.

Figure 10-6 History Session

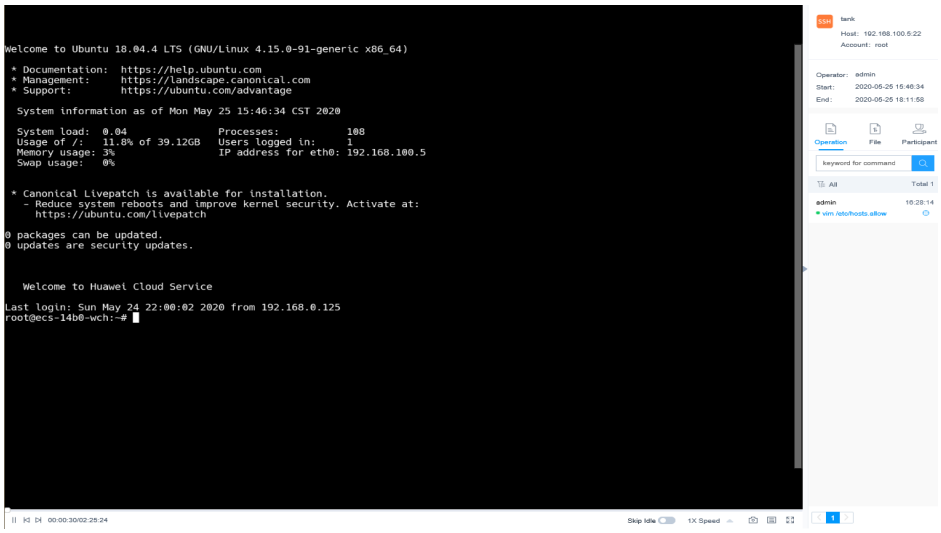


NOTE

The **More** operation in the **Details** column is removed from version 3.3.42.0 or later versions.

Step 3 Click **Play** in the **Operation** column of the historical session you want to audit.

Figure 10-7 History session video playback



Step 4 Play the video recording the entire session operation process.

- In the session window, check the total duration and drag the playback progress bar as needed.
- In the right pane of the session window, you can view information such as operation instructions, file transfer records, participants of the session, and join a live session to monitor the participants.

Step 5 Skip idle playback.

- If **Skip Idle** is enabled, only the content containing the session operations is played.
- This function is disabled by default.

Step 6 Control playback speed as needed.

Click **1X** and select a playback speed. You can select **1X**, **2X**, **4X**, **8X**, or **16X**.

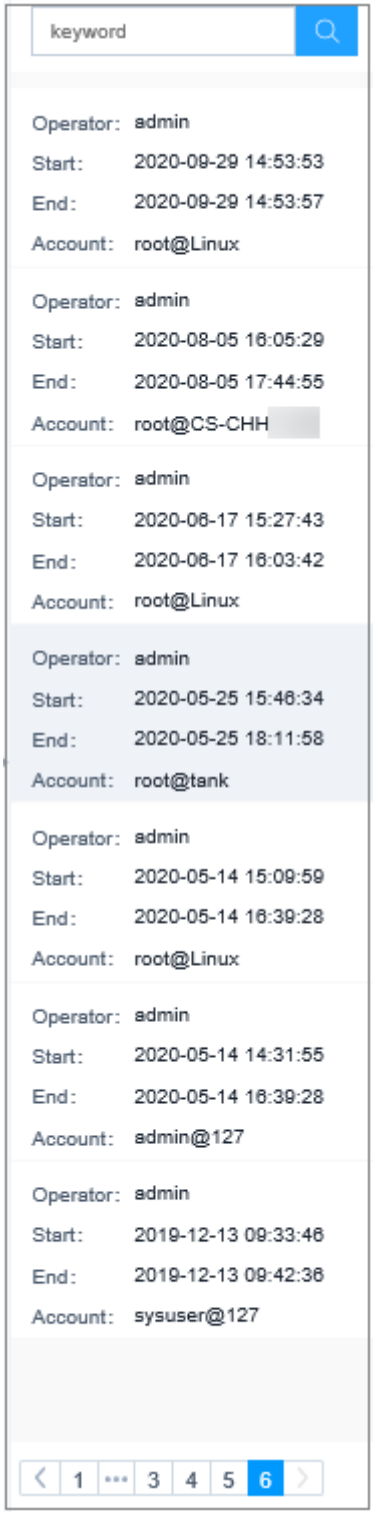
Step 7 Take a quick screenshot of the session.

Click to generate a screenshot in .png format.

Step 8 Query the playlist.

1. Click to expand the playlist on the right of the session window. Then you can select a history session to play its video.
2. Enter a login name or account name in the search box to search for a historical session.
3. Click the target session to play its video immediately.

Figure 10-8 History session playback list



----End

10.2.2 Exporting History Session Records

You can export all history session records for offline audits.

CAUTION

Sensitive data may exist in the video files to be audited. Exercise caution when exporting these files to prevent information leaks.

Prerequisites

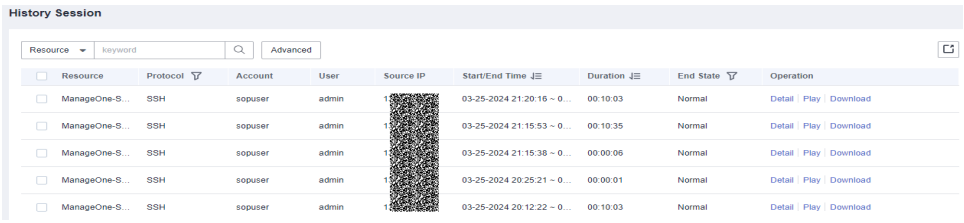
- You have the management permissions for the **History Session** module.
- The OM session has finished.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **Audit** > **History Session**.

Figure 10-9 History Session



NOTE

The **More** operation in the **Details** column is removed from version 3.3.42.0 or later versions.

Step 3 (Optional) Select one or more history session logs.

If no log is selected, all historical session logs are exported by default.

Step 4 Click  in the upper right corner. After the task is created, click **Go to Download Center**. If the export progress reaches 100%, click **Download** in the **Operation** column. Then you can view the exported historical sessions in the downloaded file.

NOTE

A maximum of two concurrent historical session export tasks are supported.

----End

10.2.3 Managing Session Videos

After an operation is finished, the audit administrator will receive a history session record as well. As an audit administrator, you can audit operation commands on Linux hosts and operations on Windows hosts. You can also generate, download, or delete operation videos for different audit purposes.

CAUTION

Sensitive data may exist in the video files to be audited. Exercise caution when downloading these files to prevent information leaks.

Constraints

- Text and video audit are available for operations performed through a web browser.
- For O&M operations, file transfer, and database operations through an SSH client, video audit is unavailable.
- Only valid session records can be played back with videos. Valid session records start when you initiate a session and end when the last operation is completed.
- Log videos are cached in your CBH system and use memory space. You are advised to save them to a local PC and clear the disk space in a timely manner. Alternatively, you can expand the system disk space by referring to **Changing Specifications of a CBH Instance**. For details about the specifications of different assets, see **Edition Differences**.

Prerequisites

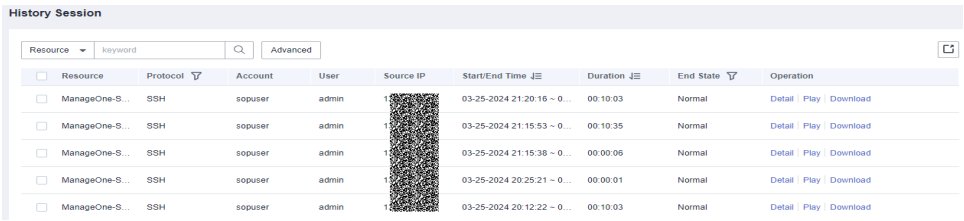
- You have the management permissions for the **History Session** module.
- The OM session has finished.

Generating Session Videos

Step 1 Log in to your bastion host.

Step 2 Choose **Audit** > **History Session**.

Figure 10-10 History Session



NOTE

The **More** operation in the **Details** column is removed from version 3.3.42.0 and later versions.

Step 3 In the **Operation** column of a history session, choose **More** > **Generate Video**. The system starts generating a video for the session.

The task center displays a message indicating that a task is being executed. After the task is finished, a notification is sent to you through the message center indicating that the session video is generated.

NOTE

- If the bastion host has abundant storage space, the video duration and size are not limited.
- If the system storage space is insufficient, the video may fail to be generated. You are advised to expand the system disk capacity in a timely manner.
- Session videos can be backed up to OBS buckets. For details, see **Configuring OBS Buckets for Remote Log Backup**.

----End

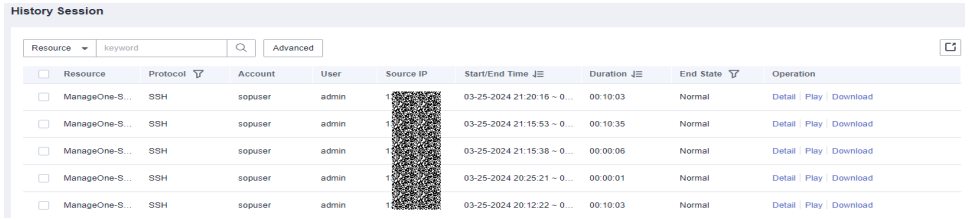
Downloading a Session Video

After a video is generated, it is cached in the system and occupies the system storage space. To save system storage space, download videos and save them locally.

Step 1 Log in to your bastion host.

Step 2 Choose **Audit** > **History Session**.

Figure 10-11 History Session



NOTE

The **More** operation in the **Details** column is removed from version 3.3.42.0 and later versions.

Step 3 In the **Operation** column of the history session recording you want to download, click **Download** to download it.

After the video is downloaded, a notification is sent to you through the message center.

NOTE

To play back a session recording in a compressed package, take the following steps:

1. Download the **local player tool** by referring to **Download Center**.
2. Open the local player tool and drag the downloaded package to the playback window.

----End

10.3 System Log

10.3.1 Querying System Logs

System logs include system login logs and system operation logs. System login logs record all login activities. System operation logs record all operations

performed on the bastion host console after login, including but not limited to adding, deleting, and modifying resource accounts or system users, as well as logins.

For example, after a system user logs in to a bastion host and performs operations such as permission configuration and audit management, you, the audit administrator, will receive system log records. You can query login and operation log details to audit system logs online.

Prerequisites

You have the management permissions for the **System Logon** or **System Operation** module under **System Log**.

Querying System Logon Logs

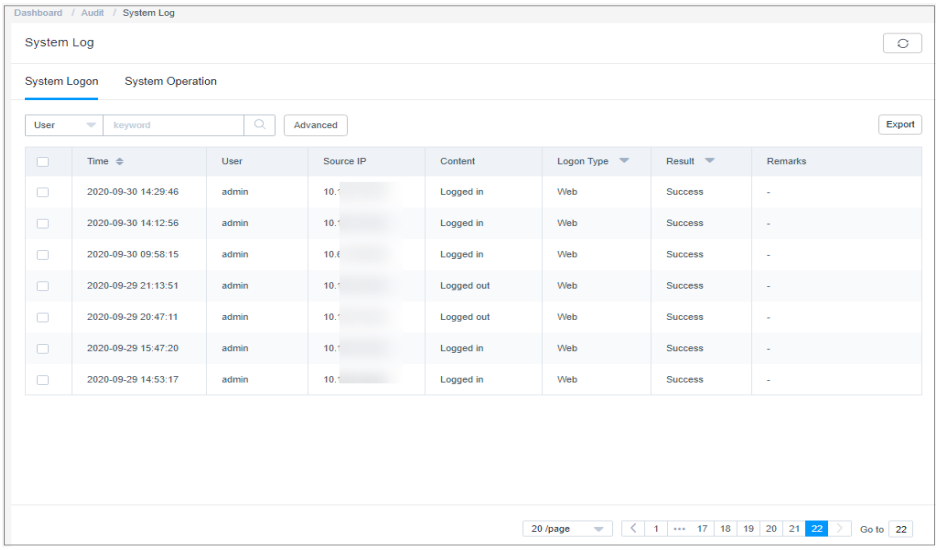
Step 1 Log in to your bastion host.

Step 2 Choose **Audit** > **System Log** > **System Logon** to switch to the system log page.

NOTE

In system operation logs, O&M task results record whether O&M tasks are complete. System logs do not include the execution results of specific commands or scripts in an O&M task.

Figure 10-12 System logon logs



Step 3 Query login logs.

- Quick search

  Enter a keyword in the search box to quickly query system logon logs by user, source IP address, start time, end time, and log content.

- Advanced search

  Enter keywords in the corresponding attribute search boxes to search for system login logs in exact mode.

Step 4 View the login logs in the search result.

----End

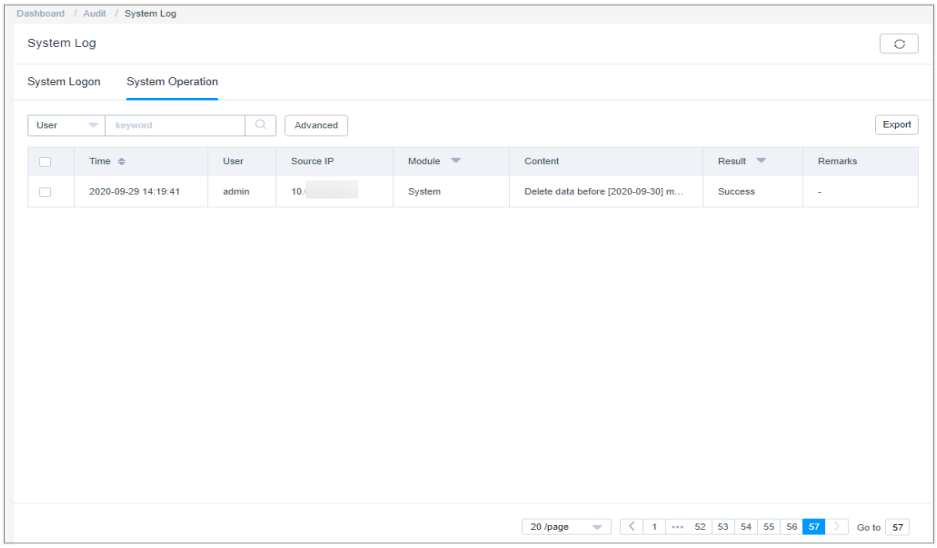
Viewing System Operation Logs

Step 1 Log in to your bastion host.

Step 2 Choose **Audit** > **System Log** to go to the system log page.

Step 3 Click the **System Operation** tab.

Figure 10-13 System operation logs



Step 4 Query operation logs.

- Quick search

  Enter a keyword in the search box to quickly query operation logs by user, source IP address, start time, end time, and log content.

- Advanced search

  Enter keywords in the corresponding attribute search boxes to search for operation logs in exact mode.

Step 5 View the operation logs in the search result.

----End

10.3.2 Exporting System Logs

After a system user logs in to a bastion host and performs operations such as permission configuration and audit management, you, the audit administrator, will receive system log records. You can query login and operation record details in a bastion host and audit system logs online. System logs include system login logs and system operation logs.

Prerequisites

You have the management permissions for the **System Logon** or **System Operation** module under **System Log**.

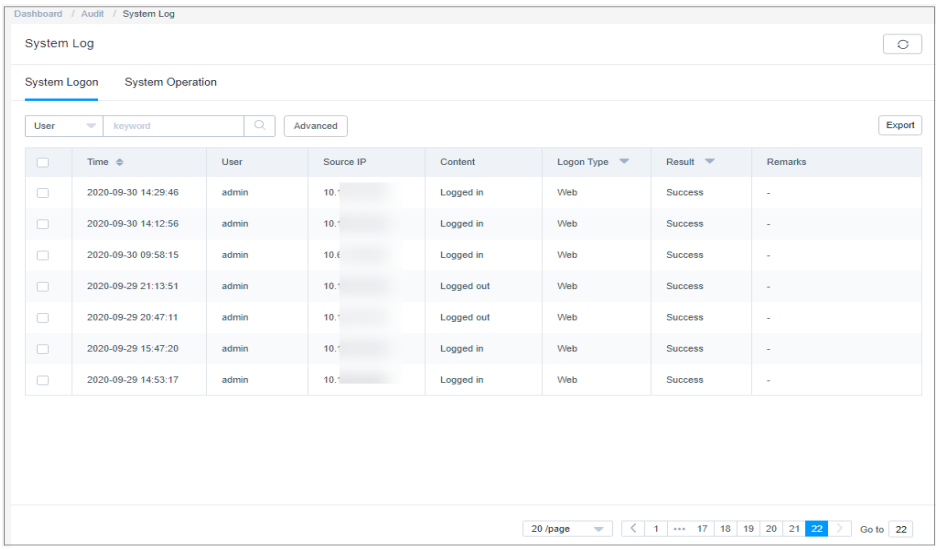
Exporting System Logon Logs

Step 1 Log in to your bastion host.

Step 2 Choose **Audit** > **System Log** to go to the system log page.

Step 3 In the **System Logon** tab, click **Export** in the upper right corner to export system logon logs.

Figure 10-14 System logon logs



Step 4 (Optional) Select one or more login logs.

If no log is selected, all login logs are exported by default.

Step 5 Click  in the upper right corner. After the task is created, click **Go to Download Center**. If the export progress reaches 100%, click **Download** in the **Operation** column. Then you can view the exported system login logs in the downloaded file.

----End

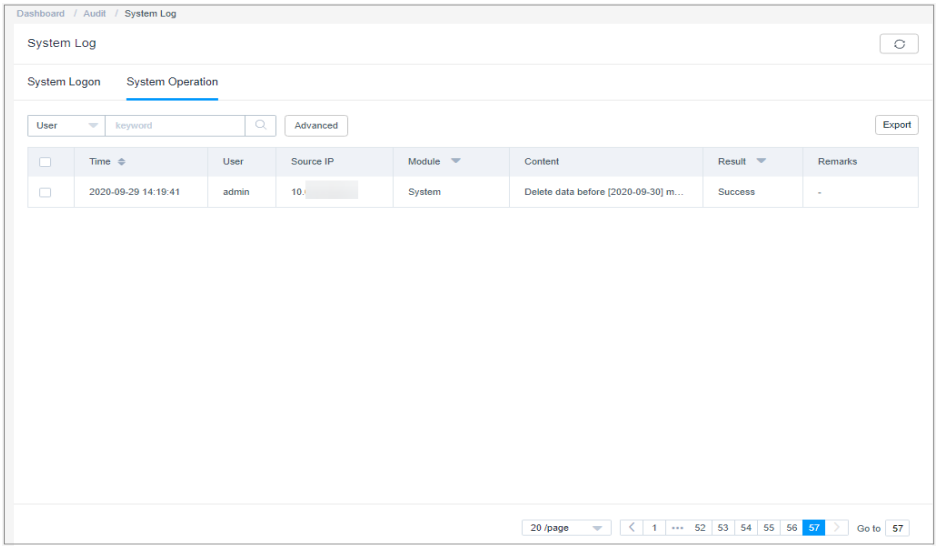
Exporting System Operation Logs

Step 1 Log in to your bastion host.

Step 2 Choose **Audit** > **System Log** to go to the system log page.

Step 3 Click the **System Operation** tab.

Figure 10-15 System operation logs



Step 4 (Optional) Select one or more operation logs.

If no log is selected, all operation logs are exported by default.

Step 5 Click  in the upper right corner. After the task is created, click **Go to Download Center**. If the export progress reaches 100%, click **Download** in the **Operation** column. Then you can view the exported system operation logs in the downloaded file.

NOTE

Two records are generated for in system operation logs. One is for the creation task triggered when the export button is clicked, and the other is for the export task, which records the export result, success or failure.

----End

10.4 Operation Report

10.4.1 Viewing Operation Reports

As the audit administrator, you can view and export operation details reports. An operation report includes the **Operation Stat**, **Logon Stat**, **Duration Stat**, **SrcIP Stat**, **Cooperation Stat**, **Approval Stat**, **Interception Stat**, **Command Stat**, and **File Stat** graphs.

Constraints

- Operation statistics for a maximum of 180 consecutive days can be viewed.
  - By default, the operation data of the current day is displayed by the hour.
  - If the time range you select falls into a week of a month, the operation data is displayed by the day.
  - If the time range you select falls into a week spanning different months, the operation data can be displayed by the day or by the month.

  - If the time range you select spans different weeks of a month, the operation data can be displayed by the day or by the week.
  - If the time range you select spans different weeks of different months, the operation data can be displayed by the day, by the week, or by the month.
- You can view operation statistics in line, bar, or pie charts.
  -  : indicates statistics will be displayed in a line chart.
  -  : indicates that statistics will be displayed in a bar chart.
  - Only the command interception trend chart can be displayed in a pie chart.
- By default, the **Operation Stat** trend chart is displayed. It allows you to:
  - View operation statistics trend chart by user. A maximum of five users can be selected.
  - View operation statistics trend chart by resource. A maximum of five resources can be selected.

Prerequisites

You have the management permissions for the **Operation Report** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **Audit** > **Operation Report**.

Step 3 Click each statistics tab and view the details.

The following describes details about each tab.

----End

Operation Stat

Displays the distribution of accessed resources by user or by resource. By default, the statistics of the current day is displayed by the hour.

In the detailed data area, view the session start and end time, user login name, resource name, protocol type, and account.

Logon Stat

Displays the number of historical sessions by user or by resource. By default, the statistics of the current day is displayed by the hour.

In the detailed data area, view the session start and end time, user login name, resource name, protocol type, and account.

Duration Stat

Displays the duration of history sessions by user or by resource. By default, the statistics of the current day is displayed by the hour.

In the detailed data area, view the session start and end time, user login name, resource name, protocol type, account, and session duration.

SrcIP Stat

Displays the number of source IP addresses from which sessions are established by user or by resource. By default, the statistics of the current day is displayed by the hour.

In the detailed data area, view the session start and end time, user login name, resource name, protocol type, account, and source IP address.

Cooperation Stat

Displays the number of users participating in a cooperation session by user or by resource. By default, the statistics of the current day is displayed by the hour.

In the detailed data area, view the session start and end time, user login name, resource name, protocol type, account, and login names of session participants.

Two-person authorization

Displays the number of sessions requiring two-person approval by user or by resource. By default, the statistics of the current day is displayed by the hour.

In the detailed data area, view the approval time, user login name, resource name, protocol type, account, and login names of approvers.

Interception Stat

Displays the number of intercepted commands by user or by resource. By default, the statistics of the current day is displayed by the hour.

Intercepting a command includes three actions, disconnecting the session, rejecting the session, or asking dynamical approval.

In the detailed data area, view the operation time, user login name, resource name, protocol type, account, and action.

Command Stat

Displays the number of executed commands by user or resource. By default, the statistics of the current day is displayed by the hour.

In the detailed data area, view the operation time, user login name, resource name, protocol type, account, and operation instructions.

File Stat

Displays the number of files uploaded and downloaded by user or by resource. By default, the statistics of the current day is displayed by the hour.

In the detailed data area, view the file operation time, user login name, resource name, protocol type, account, operation type, and file name.

10.4.2 Pushing Operation Reports

For your convenience of audit, you can manually export the operation reports or enable the auto send function to let the bastion host push operation reports to you through emails at the interval you select.

- Operation reports can be automatically sent by the day, week, and month.
- The report format can be PDF, DOC, XLS, or HTML.
- An operation report for a maximum of 180 consecutive days can be pushed each time.

Prerequisites

- You have the management permissions for the **Operation Report** module.
- You have completed **Configuring the Outgoing Mail Server**.

Manually Exporting an Operation Report

Step 1 Log in to your bastion host.

Step 2 Choose **Audit** > **Operation Report**.

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

Step 4 In the displayed **Export** dialog box, configure the method and time to export the report and the report format.

Table 10-1 Parameters for exporting operation reports

Parameter	Description
Granularity	Time granularity for displaying the trend chart of the operation report. The options are **Hourly**, **Daily**, **Weekly**, and **Monthly**.
Time	Start time and end time to generate the operation report to be exported. • Start time and end time are mandatory. • A maximum of 180 consecutive days are allowed.
Report Type	Type of operation statistics to be included in the operation report.
File format	Format of the report. You can select only one format. • DOC is selected by default. • You can download a report in PDF, DOC, XLS, or HTML.

Step 5 Click **OK** to export the operation report immediately.

----End

Automatically Pushing a System Report

Step 1 Log in to your bastion host.

Step 2 Choose **Audit** > **Operation Report**.

Step 3 On the displayed page, click **Auto Send** in the upper right corner.

Step 4 In the displayed **Auto Send** dialog box, configure the method and time to push the report and the report format.

Table 10-2 Auto Send

Parameter	Description
Status	Whether to enable the auto send function. This function is disabled by default ( ). • : indicates that auto send function is disabled. • : indicates that the auto send function is enabled. The operation report of the previous period will be sent to you through emails.
Send cycle	Interval at which a report is sent. • By default, the report is sent at 00:00 on the specified date. • Reports can be sent by the day, week, or month. • Statistics in the daily reports are displayed by the hour. • Statistics in the weekly reports are displayed by the day. • Statistics in the monthly reports are displayed by the week.
File format	Format of the report. You can select only one format. • DOC is selected by default. • You can download a report in PDF, DOC, XLS, or HTML.

Step 5 Click **OK**.

----End

10.5 System Report

10.5.1 Viewing System Reports

As an audit administrator, you can view operation details in a system report. A system report usually includes the **UserControl Stat**, **User&Resource Stat**, **SrcIP Stat**, **Logon Stat**, **Exception Stat**, **Supervision Stat**, and **User Status** trend charts.

Constraints

- Each trend chart displays the statistics for a maximum of 180 consecutive days.

  - By default, the operation data of the current day is displayed by the hour.
  - Operation data over 30 days can only be viewed by the week or month.
  - Operation data within 30 days can be viewed by the day, week, or month.
- The trend chart can only be a bar chart.

Prerequisites

You have the management permissions for the **System Report** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **Audit** > **System Report**.

Step 3 Click each statistics tab and view the details.

----End

UserControl Stat

This area displays the number of disabling and enabling users. By default, the statistics of the current day is displayed.

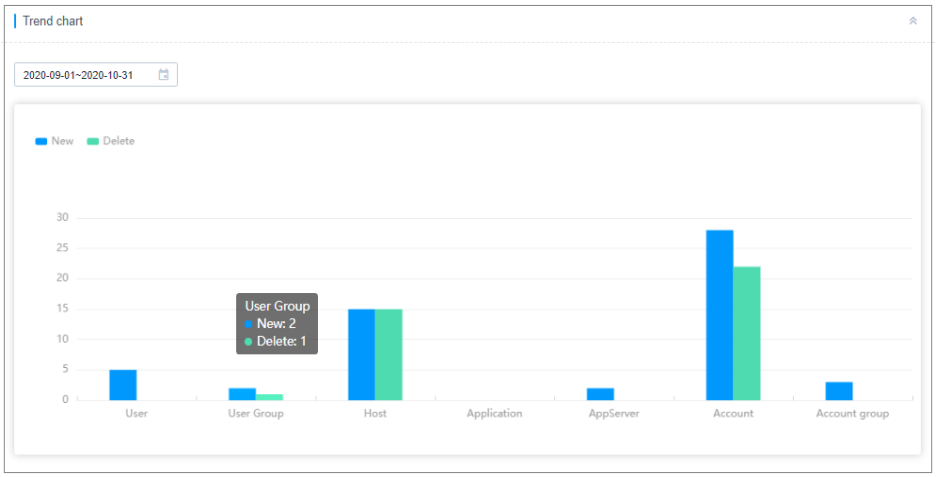
In the detailed data area, view the operation time, user login name, source IP address, operation, and operation results.

User&Resource Stat

This area displays statistics of how many users, user groups, hosts, application resources, application servers, accounts, and account groups are created and deleted. By default, the statistics of the current day is displayed.

In the detailed data area, view the operation time, user login name, source IP address, operation, and operation results.

Figure 10-16 Trend chart of User&Resource Stat



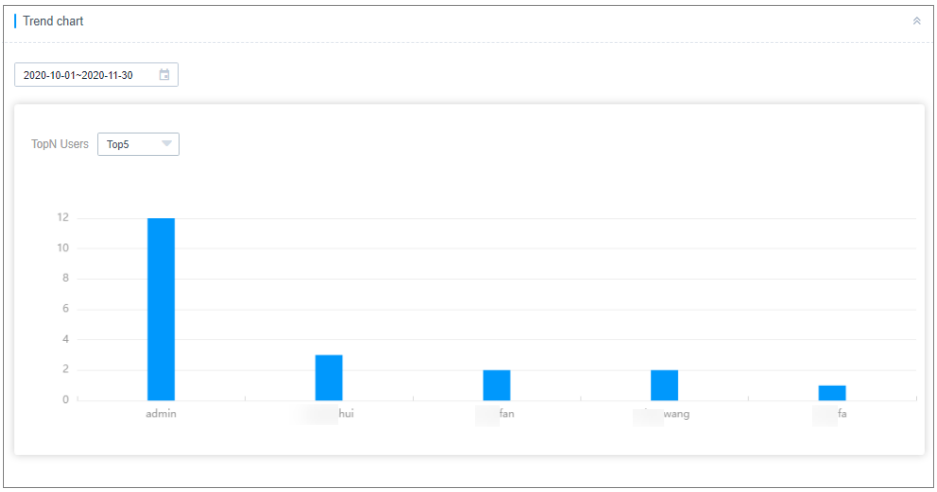
SrcIP Stat

This area displays the number of IP addresses from which users log in to the system. By default, the statistics of the current day is displayed.

You can view top 5, top 10, and top 20 source IP addresses.

In the detailed data area, view the logon time, source IP address, operation, and operation results.

Figure 10-17 Trend chart of SrcIP Stat



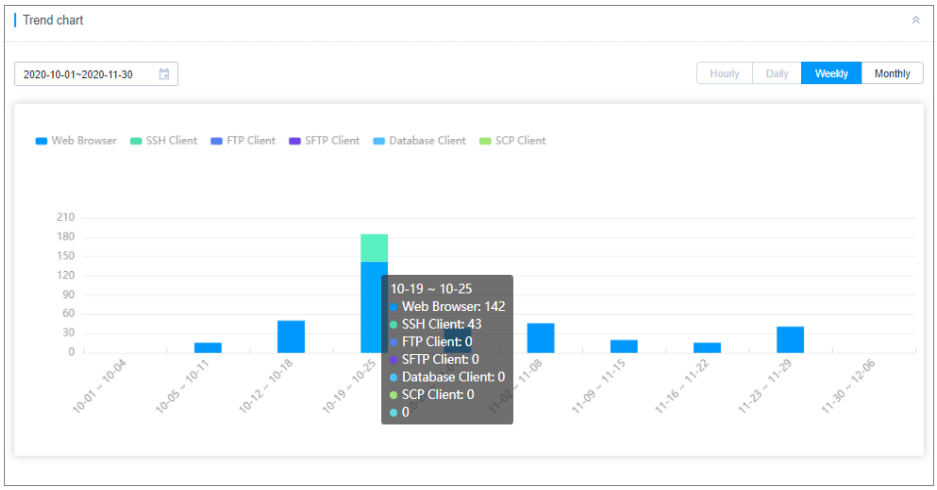
Logon Stat

This area displays the number of logins by login method. By default, the statistics of the current day is displayed.

You can view logins by web browsers and SSH, FTP, and SFTP clients.

In the detailed data area, view the logon time, source IP address, operation, and operation results.

Figure 10-18 Trend chart of Logon Stat



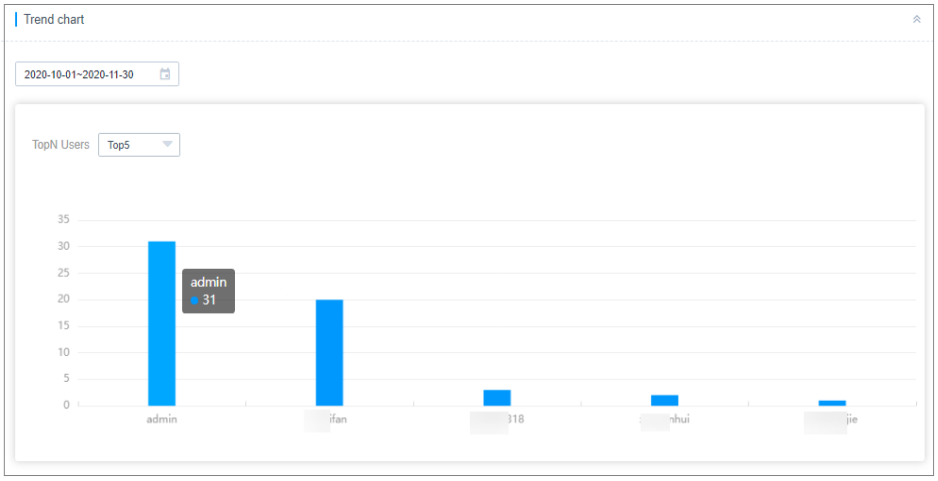
Exception Stat

This area displays the number of login exceptions. By default, the statistics of the current day is displayed.

You can view top 5, top 10, and top 20 login exceptions.

In the detailed data area, view the logon time, source IP address, operation, and operation results.

Figure 10-19 Trend chart of Exception Stat



Supervision Stat

This area displays the number of interrupted sessions and monitored sessions. By default, the statistics of the current day is displayed.

In the detailed data area, view the logon time, source IP address, operation, and operation results.

User Status

This area displays the number of zombie users and the number of users by password strength.

- Zombie users are valid users who have not logged in for more than 14 days. Zombie accounts are counted by the number of days during which they have not logged in.

  By default, information about top 5 zombie accounts is displayed. You can view top 5, top 10, and top 20 zombie users.

  In the detailed data area, view the time of the last successful login, source IP address, operation, and operation results.

- Password strength is classified into three levels: high, medium, and low.

  In the detailed data area, you can view the login name of the user who completes the last password change, password strength, and last password change time, which are displayed in ascending order by password strength.

NOTE

Password strength classification criteria:

High: The password contains eight or more characters that include uppercase letters, lowercase letters, digits, and special characters.

Medium: The password contains eight or more characters that include two or three types of the following characters: uppercase letters, lowercase letters, digits, and special characters.

Low: The password contains fewer than eight characters or contains eight or more characters that include one type of the following characters: uppercase letters, lowercase letters, digits, or special character.

10.5.2 Pushing System Reports

For your convenience of audit, you can manually export the system reports or enable the auto send function to let the bastion host push system reports to you through emails at the interval you select.

- System reports can be automatically sent by the day, week, and month.
- The report format can be PDF, DOC, XLS, or HTML.
- A system report for a maximum of 180 consecutive days can be pushed each time.

Prerequisites

- You have the management permissions for the **System Report** module.
- You have configured an available email address to receive reports.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **Audit** > **System Report**.

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

Step 4 In the displayed **Export** dialog box, configure the method and time to export the report and the report format.

Table 10-3 Parameters for exporting system reports

Parameter	Description
Granularity	Time granularity for displaying the trend chart of the system report. The options are **Hourly**, **Daily**, **Weekly**, and **Monthly**.
Time	Start time and end time to generate the report to be exported. • Start time and end time are mandatory. • A maximum of 180 consecutive days are allowed.
Report Type	Type of statistics to be included in the report.

Parameter	Description
File format	Format of the report. You can select only one format. • DOC is selected by default. • You can download a report in PDF, DOC, XLS, or HTML.

Step 5 Click **OK** to export the system report immediately.

Step 6 Go to your email address to check the system report after you receive the notification in the message center.

----End

Automatically Pushing a System Report

Step 1 Log in to your bastion host.

Step 2 Choose **Audit** > **System Report**.

Step 3 On the displayed page, click **Auto Send** in the upper right corner.

Step 4 In the displayed **Auto Send** dialog box, configure the method and time to push the report and the report format.

Table 10-4 Parameters for auto-send function

Parameter	Description
Status	Whether to enable the auto send function. This function is disabled by default ( ). • : indicates that auto send function is disabled. • : indicates that the auto send function is enabled. The operation report of the previous period will be sent to you through emails.
Send cycle	Interval at which a report is sent. • By default, the report is sent at 00:00 on the specified date. • Reports can be sent by the day, week, or month. • Statistics in the daily reports are displayed by the hour. • Statistics in the weekly reports are displayed by the day. • Statistics in the monthly reports are displayed by the week.
File format	Format of the report. You can select only one format. • DOC is selected by default. • You can download a report in PDF, DOC, XLS, or HTML.

Step 5 Click **OK**.

----End

11 Authentication Configuration

11.1 Multifactor Verification Management

11.1.1 USB Key Management

USB keys can only be issued to user accounts with USB key authentication enabled in multifactor verification.

Before using a USB key for second authentication, prepare USB keys and install the USB key driver on the local computer.

USB keys from different vendors cannot identify each other for login authentication. You need to **configure the USB key vendor** based on the USB keys in use.

Prerequisites

- You have obtained a USB key.
- You have the management permissions for the **User** module.
- You have the management permissions for the **USBKey** module.

Procedure

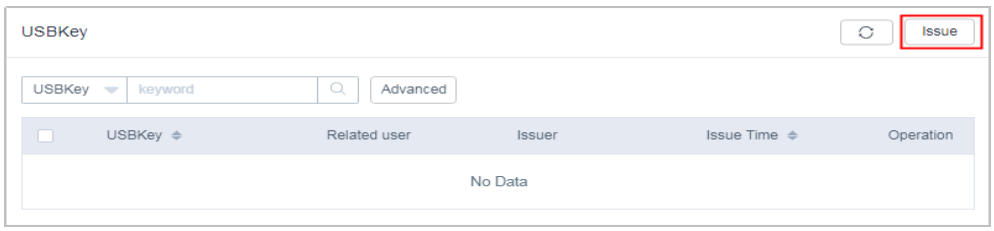
One USB key can be issued to one user only.

Step 1 Log in to your bastion host.

Step 2 Choose **User** > **USBKey** in the navigation pane.

Step 3 Click **Issue** to issue a USB key.

Figure 11-1 USBKey



Step 4 Select a user with the USB key multifactor verification enabled as the related user.

Figure 11-2 Issuing a USB key

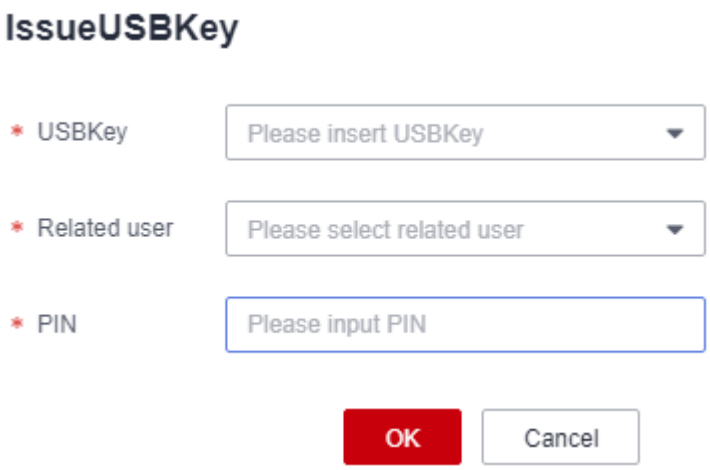


Table 11-1 Parameters for issuing a USB key

Parameter	Description
USBKey	Specifies the USB key ID.
Relate User	Specifies the user to which the USB key is related. USB key in multifactor verification must be enabled for such users.
PIN	Specifies the personal identification number (PIN) uniquely corresponding to the USB key. It is provided by the USB key vendor.

Step 5 Click **OK**. You can then view the newly issued USB key in the USB key list.

When you log in to a bastion host as a related user, insert the issued USB key to the local host. The bastion host automatically identifies the USB key. So you can select the corresponding USB key on the login page and enter the PIN number to finish the authentication.

----End

Revoking a USB Key

Step 1 Log in to your bastion host.

Step 2 Choose **User** > **USBKey** in the navigation pane.

Step 3 In the **Operation** column of the row containing the USB key to be revoked, click **Revoke**.

Step 4 To revoke multiple USB keys at a time, select the ones you want and click **Revoke** at the bottom of the USB key list to revoke the selected USB keys together.

----End

11.1.2 OTP Token Management

OTP tokens can be issued only to users with **OTP Token** enabled in multifactor verification.

You need to prepare OTP token devices in advance. Currently, CBH supports Jansh ETZ201/203 and Feitian tokens.

Prerequisites

- You have obtained a hardware token.
- You have the management permissions for the **User** module.
- You have the management permissions for the **OTP** module.

Issuing an OTP Token

One OTP token can be issued only to one user.

Step 1 Log in to your bastion host.

Step 2 Choose **User** > **OTP token** in the navigation pane.

Step 3 Click **Issue** to issue an OTP token.

Step 4 Enter the required token information.

Figure 11-3 Issue Token ID

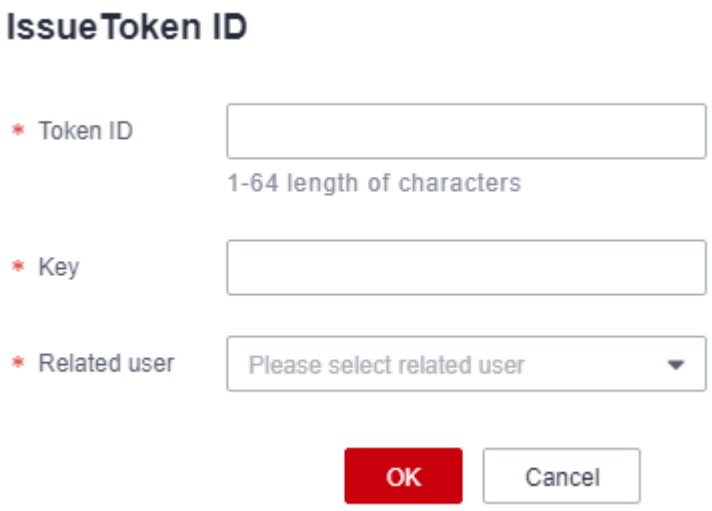


Table 11-2 Parameters for issuing an OTP token

Parameter	Description
Token ID	Specifies the OTP token ID.
Key	Specifies the key uniquely corresponding to the OTP token. It is provided by the OTP token vendor.

Parameter	Description
Relate User	Specifies the user to whom the OTP token is related. OTP token must be enabled in multifactor verification for such users.

Step 5 Click **OK**. You can view the newly issued OTP token in the OTP token list.

For users with OTP token enabled, they need to enter the username, password, and the dynamic password issued by the OTP token for logins.

----End

Importing an OTP Token

Step 1 Log in to your bastion host.

Step 2 Choose **User** > **OTP token** in the navigation pane.

Step 3 Click **Import** to batch import OTP tokens.

Step 4 Click **Download** next to **Download template**.

Step 5 Enter the configuration information of the OTP tokens to be imported according to the configuration requirements of the template.

Step 6 Click **Upload** and select the complete template.

- You can upload files in CSV, XLS, or XLSX format.
- **Override existing OTP token**
  - Selected: The token ID will be overwritten if two tokens have the same key and related user configured, and the information of the existing token will be updated but the token is not deleted.
  - Not selected: The system skips the tokens with duplicate keys and related users.

Step 7 Click **OK**. You can then view the imported OTP tokens in the token list.

----End

Exporting an OTP Token

Step 1 Log in to your bastion host.

Step 2 Choose **User> OTP Token**. On the OTP token list page displayed, select the OTP tokens you want to export.

If no tokens are selected, all tokens are exported by default.

Step 3 Click  in the upper right corner. On the dialog box displayed, confirm the export.

- Set an encryption password to encrypt the exported file.
- Enter your password.

- Select the CSV or Excel format.

Step 4 Click **OK**. After the task is created, click **Go to Download Center**. If the export progress reaches 100%, click **Download** in the **Operation** column. Then you can view the exported OTP tokens in the downloaded file.

----End

Revoking an OTP Token

After an OTP token is deleted, the related user cannot log in to the bastion host through the OTP token.

Step 1 Log in to your bastion host.

Step 2 Choose **User** > **OTP token** in the navigation pane.

Step 3 In the **Operation** column of the row containing the OTP token to be revoked, click **Revoke**.

Step 4 In the OTP token list, you can select multiple OTP tokens and click **Revoke** at the bottom of the list to revoke the selected tokens together.

----End

11.1.3 Mobile OTPs

A mobile OTP application is a software token application used to generate a dynamic password on a bound mobile phone. You can configure mobile one-time password (OTP) verification to implement MFA for your bastion host. After mobile OTP verification is configured, in addition to the username and password, a 6-digit mobile OTP verification code is required for each login. For details, see **Configuring Mobile OTP Login Authentication**.

Currently, built-in mobile OTPs and Remote Authentication Dial In User Service (RADIUS) mobile OTPs are supported.

- Built-in mobile OTPs support Time-based One-Time Password (TOTP). You need to bind a mobile OTP to a user in the **Profile** module in your bastion host system. You can bind a mobile OTP through a WeChat applet or other similar programs, such as Google Authenticator and FreeOTP Authenticator, that support TOTP.
- RADIUS mobile OTPs also support TOTP. You need to connect to the RADIUS server you have created and bind the mobile OTP on the RADIUS server. You can bind the mobile OTP through a WeChat applet or similar programs, such as Google Authenticator and FreeOTP Authenticator, that support TOTP.

NOTICE

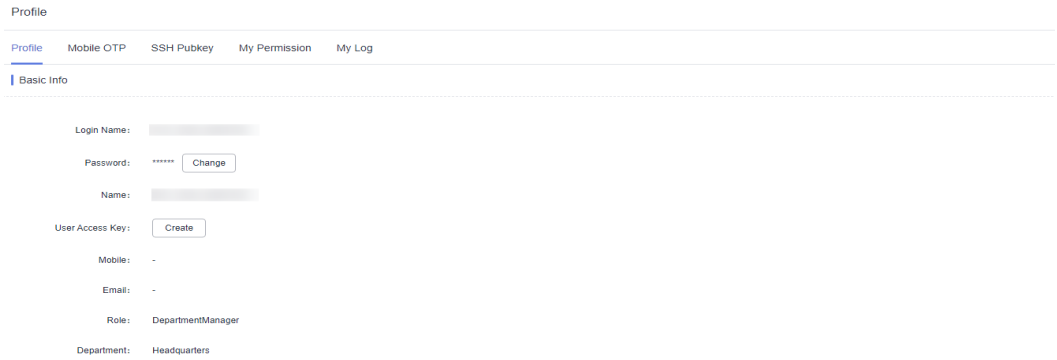
- Ensure that your bastion host and mobile phone have the same system time, accurate to seconds. Otherwise, the mobile OTP application may fail to be bound to the user account.
- If the mobile OTP fails to be bound, change the system time to be the same as the mobile phone time. After this, refresh the page to generate a new quick response (QR) code for binding.

Binding a Mobile OTP application to a User

Step 1 Log in to your bastion host.

Step 2 On the **Dashboard** page, click the username in the upper right corner and choose **Profile**.

Figure 11-4 Profile



Step 3 Click the **Mobile OTP** tab.

Step 4 In the displayed **Mobile OTP** dialog box, bind a mobile OTP application as prompted.

NOTE

Before binding, make sure the time of the bastion host is consistent with that of the mobile phone.

1. WeChat applet access token

   Start WeChat on the mobile phone, obtain the dynamic password for binding according to the operation guide, and enter the 6-digit dynamic password. After the verification, the mobile OTP application is bound.

2. App-based mobile OTP

   Start the installed mobile OTP application, scan the QR code in step 2 to obtain a dynamic password, and enter the 6-digit dynamic password. After the verification, the mobile OTP application is bound to you.

Step 5 Refresh the page.

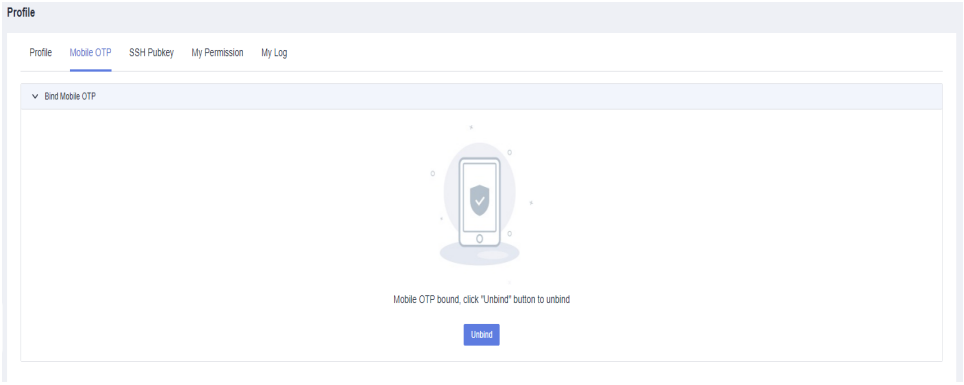
----End

Unbinding a Mobile OTP Application

Click **Unbind** on the **Mobile OTP** tab to unbind the mobile OTP application.

After the unbinding, refresh the page.

Figure 11-5 Unbinding a mobile OTP application



11.1.4 SSH Pubkey

Your SSH public key is used for **passwordless login over the SSH client**.

You can generate an SSH key pair (including the public key and private key) on your local PC, add the public key to the bastion host system, export the private key to the local PC, and import the private key to the SSH client tool. In this way, you can log in to the bastion host system using the SSH client without entering a password.

You can run the following commands to generate an SSH key pair:

- RSA algorithm: **ssh-keygen -t rsa**
- Ed25519 algorithm: **ssh-keygen -t ed25519**

Constraints

Only OpenSSH public keys are supported.

Prerequisites

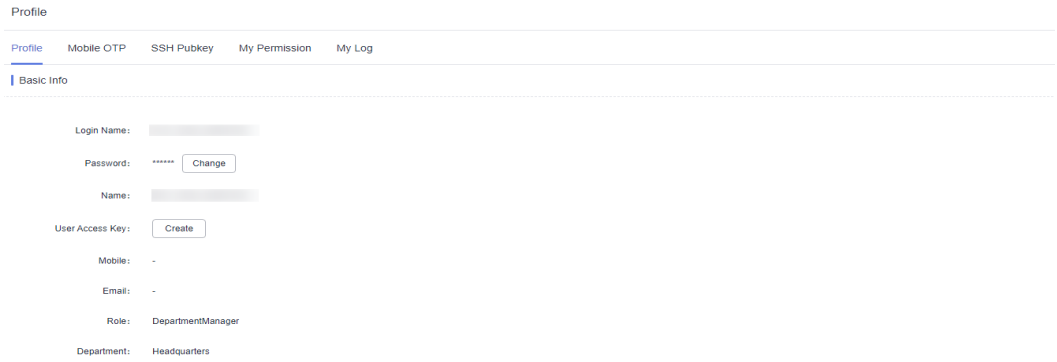
You have generated an SSH key pair on your local PC.

Adding an SSH Public Key

Step 1 Log in to your bastion host.

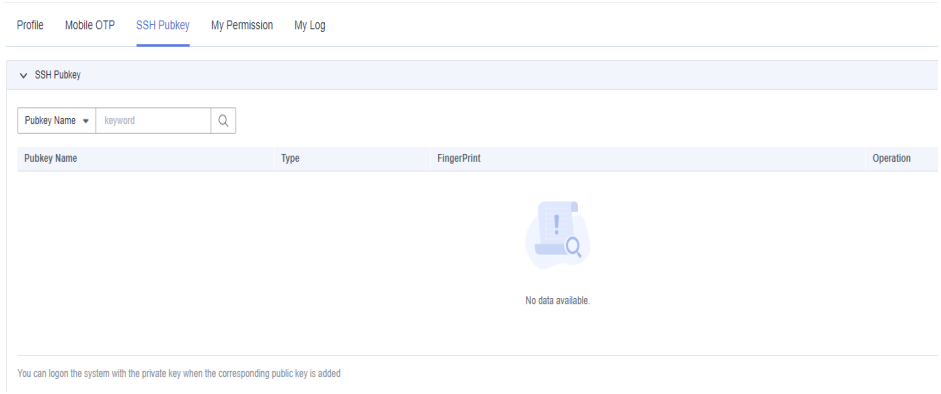
Step 2 On the **Dashboard** page, click the user name in the upper right corner and choose **Profile**.

Figure 11-6 Profile



Step 3 Click the **SSH Pubkey** tab.

Figure 11-7 SSH Pubkey



Step 4 Click **Add** in the **SSH Pubkey** area.

Step 5 In the displayed **Add SSH Pubkey** dialog, specify the public key name and enter the SSH public key.

Step 6 Click **OK**. You can view the added SSH public key.

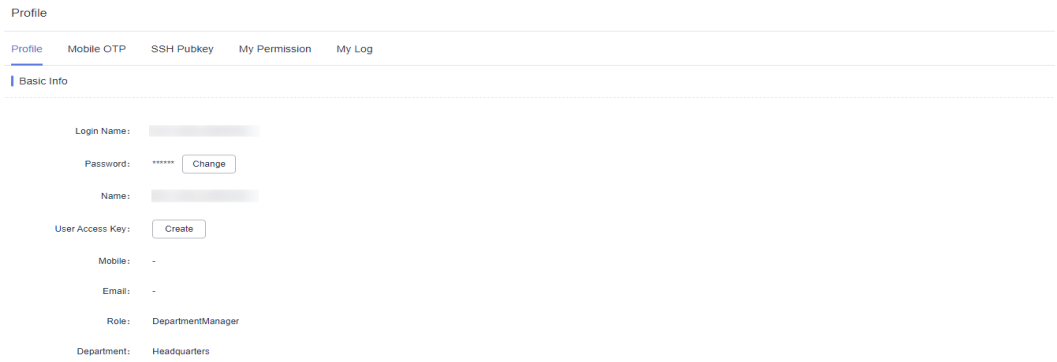
----End

Deleting an SSH Public Key

Step 1 Log in to your bastion host.

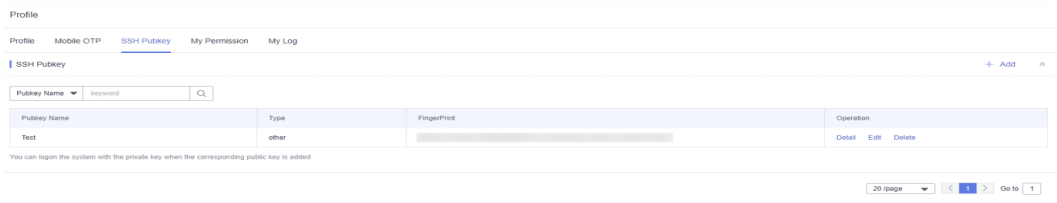
Step 2 On the **Dashboard** page, click the user name in the upper right corner and choose **Profile**.

Figure 11-8 Profile



Step 3 Click the **SSH Pubkey** tab.

Figure 11-9 SSH Pubkey



Step 4 In the **Operation** column of the SSH public key you want to delete, click **Delete**.

Step 5 In the displayed confirmation dialog box, click **OK**. You can check the deletion on the displayed SSH public key list.

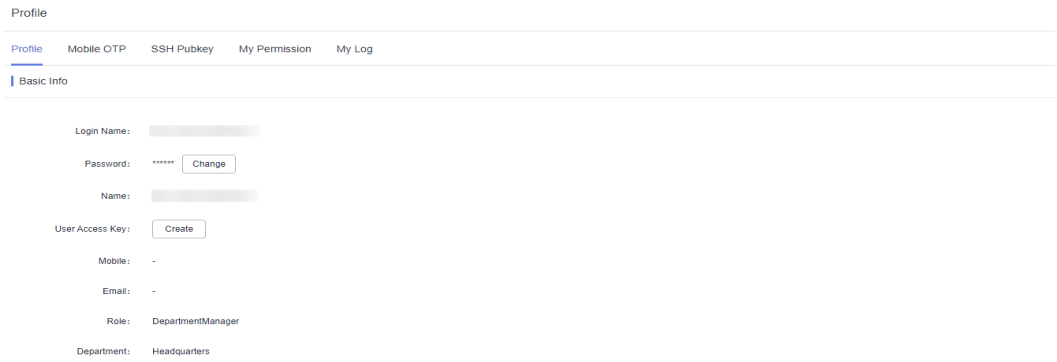
----End

Editing an SSH Public Key

Step 1 Log in to your bastion host.

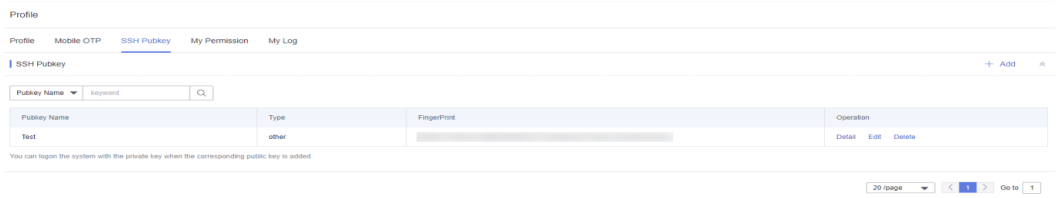
Step 2 On the **Dashboard** page, click the user name in the upper right corner and choose **Profile**.

Figure 11-10 Profile



Step 3 Click the **SSH Pubkey** tab to go to the SSH public key management page.

Figure 11-11 SSH Pubkey



Step 4 In the **Operation** column of the SSH public key you want to modify, click **Edit**.

Step 5 In the displayed **Edit SSH pubkey** dialog box, edit the public key name and the public key.

Step 6 Click **OK**. You can view the modified SSH public key.

----End

11.2 Configuring Multifactor Verification

11.2.1 Configuring SMS Login Verification

You can configure a mobile phone to receive a 6-digit code for login identity verification. In SMS authentication method, both the static login password and a 6-digit SMS verification code are required for login.

The mobile number you configure must be valid. If the mobile number is changed later, reset the login method for user **admin**. For details, see **Resetting Login Method for User admin**.

Constraints

- Only one phone number can be bound to a system user account.
- You have enabled the SMS gateway IP address and port 10743 and port 443 for the security group of the bastion host instance, and the bastion host system can access the SMS gateway.

Step 1: Bind a Phone Number

The phone number bound to a user account must be valid and can receive SMS messages.

Method 1: Binding a phone number as an individual system user

Step 1 Log in to your bastion host using your static password.

Step 2 On the **Dashboard** page, click the user name in the upper right corner and choose **Profile**.

Step 3 In the displayed **Profile** management page, click **Edit**.

Step 4 In the displayed **Edit Basic Info** dialog box, enter a valid phone number in the **Mobile** text box.

NOTE

The country code is required for phone numbers. The format is as follows: + *country code phone number*, for example, *+86 1xxxxxxxxx*.

Step 5 Click **OK**.

----End

Method 2: Changing a user's phone number as the administrator

Step 1 Log in to your bastion host as the administrator.

Step 2 Choose **User** > **User** to go to the **User** management page.

Step 3 Select a user and click its **LoginName**.

Step 4 On the displayed page, click **Edit** in the **Basic Info** area.

Step 5 Enter a valid phone number in the **Mobile** text box.

Step 6 Click **OK**.

----End

Step 2: Configure SMS Authentication as the Administrator

Step 1 Log in to your bastion host as the administrator.

Step 2 Choose **User** > **User** to go to the **User** management page.

Step 3 Select a user and click its **LoginName**.

Step 4 In the **User Setting** area, click **Edit**.

Step 5 In the displayed **Edit user setting** dialog box, select **Mobile SMS** for **Multifactor Verification**.

Step 6 Click **OK**.

The next time the user logs in to the system, they will have to provide an SMS code.

----End

11.2.2 Configuring Mobile OTP Login Verification

A mobile OTP is a mobile application that can generate a dynamic password for identity verification.

In mobile OTP verification method, both your static login password and a 6-digit one-time password are required for login.

After mobile OTP authentication, the bastion host can be used in a non-public network environment as long as the bastion host time is the same as the mobile phone time.

NOTICE

If you want to enable MFA for the **admin** account, you need to configure the mobile phone token first, or the **admin** account cannot log in to the system in MFA mode.

If the mobile OTP expires and the login fails, reset the login method for user **admin**. For details, see **Resetting Login Method for User admin**.

Currently, built-in mobile OTPs and Remote Authentication Dial In User Service (RADIUS) mobile OTPs are supported.

- Built-in mobile OTPs support Time-based One-Time Password (TOTP). You need to bind a mobile OTP to a user in the **Profile** module in your bastion host system. You can bind a mobile OTP through a WeChat applet or other similar programs, such as Google Authenticator and FreeOTP Authenticator, that support TOTP.
- RADIUS mobile OTPs also support TOTP. You need to connect to the RADIUS server you have created and bind the mobile OTP on the RADIUS server. You can bind the mobile OTP through a WeChat applet or similar programs, such as Google Authenticator and FreeOTP Authenticator, that support TOTP.

Constraints

Ensure that your bastion host and mobile phone have the same system time, accurate to the seconds. Otherwise, the system may prompt that the mobile OTP fails to be bound.

Synchronize the bastion host system time to the mobile phone time. Refresh the page, scan the new QR code, and try again.

Step 1: Configure the Mobile OTP Type

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Security**.

Step 3 In the **Mobile Token Settings** area, click **Edit**.

Step 4 In the displayed **Mobile Token Settings** dialog box, select a mobile OTP type.

You can select **Built-in** or **RADIUS**. If you select **RADIUS**, the parameters are described as follows:

Table 11-3 RADIUS mobile OTP parameters

Parameter	Description
Server	Enter the IP address of the RADIUS server.
Port	Enter the port number of the RADIUS server.
Protocol	The options are **PAP** and **CHAP**.

Parameter	Description
Password	Enter the shared key for RADIUS server authentication.
Timeout	Configure an authentication timeout. The value ranges from 5 to 30, in seconds. A maximum of three authentication attempts are allowed, and each attempt must be within the configured authentication timeout.

Step 5 Click **OK**. You can then check the mobile token settings of the current system user on the **Security** tab.

----End

Step 2: Bind a Mobile OTP as a Common User

Built-in Mobile OTP

Step 1 Log in to your bastion host using your static password.

Step 2 On the **Dashboard** page, click the user name in the upper right corner and choose **Profile**.

Step 3 On the displayed **Profile** page, click the **Mobile OTP** tab.

On the displayed page, follow the instructions to bind a mobile OTP.

NOTE

If you do not have the WeChat app, use the Google verification code program to scan the second QR code.

Step 4 (Optional) To unbind the mobile OTP, click **Unbind** on the **Mobile OTP** tab.

----End

RADIUS Mobile OTP

Step 1 Create a user on the RADIUS server and bind a mobile OTP for the user as prompted.

----End

Step 3: Enable Mobile OTP Authentication for a User as the Administrator

Built-in Mobile OTP

Step 1 Log in to your bastion host as the administrator.

Step 2 Choose **User** > **User** to go to the **User** management page.

Step 3 Select a user having mobile OTP bound and click its **LoginName**.

Step 4 In the **User Setting** area, click **Edit**.

Step 5 In the displayed **Edit user settings** dialog box, select **Mobile OTP** for **Multifactor Verification**.

Step 6 Click **OK**.

The next time the user logs in to the system, they will have to provide a mobile OTP.

----End

RADIUS Mobile OTP

Step 1 Create a user in the bastion host system. The login name of the user must be the same as that of the user created on the RADIUS server in **Step 1**.

1. Log in to your bastion host as the administrator.
2. Choose **User** > **User** to go to the **User** management page.
3. Click **New**. In the displayed **New User** dialog box, complete required parameters.

Table 11-4 Parameters for creating a user

Parameter	Description
LoginName	The login name must be the same as the name of the user created on the RADIUS server. The **LoginName** must be unique in a system and cannot be changed once created.
Authentication Type	Select **Local**. **Local**: The user is verified against the account management system of the bastion host. This method is the default method.
Password/ Confirm Password	You need to specify a custom password for logging in to the system.
UserName	User-defined username. This name indicates the name of the person who uses the account so that system users can be distinguished from each other.
Mobile	Enter the mobile phone number. This number is used for SMS authentication logins and password resetting.
Email	Enter an email address. The bastion host sends notifications to this email address.

Parameter	Description
Role	Specifies the role to be assigned to the user. Only one role can be assigned. By default, system roles include **DepartmentManager**, **PolicyManager**, **AuditManager**, and **User**. – **DepartmentManager**: responsible for managing departments. Except the **User** and **Role** modules, this role has the configuration permissions for all other modules. – **PolicyManager**: responsible for configuring policy permissions. This role has the configuration permissions for the **User Group**, **Account Group**, and **ACL Rules** modules. – **AuditManager**: responsible for auditing system and maintenance data. This role has the configuration permission for **Live Session**, **History Session**, and **System Log** modules. – **User**: common system users and resource operators. This role has the permissions for the **Host Operations**, **App Operations**, and **Ticket approval** modules. – User-defined role: Only the **admin** user can customize a new role or edit permissions of a default role.
Department	Select the department that the user belongs to. For details about how to create a department, see **Creating a Department**.
Remarks	Brief description of the user.

4. Click **OK**.

   On the **User** page, you can view the created user.

Step 2 Configure mobile OTP authentication for the same user in the bastion host system.

1. Go to the **User** page.
2. Select the same user and click its **LoginName**.
3. In the **User Setting** area, click **Edit**.
4. In the displayed **Edit user settings** dialog box, select **Mobile OTP** for **Multifactor Verification**.
5. Click **OK**.

   The next time the same user logs in to the system, they will have to provide a mobile OTP.

----End

11.2.3 Configuring USB Key Login Verification

USB token is a one-time password technology implemented based on USB keys. In USB key authentication method, you will need to insert the USB key into your

local host for login. The system login page then automatically identifies the inserted USB key and requires you to enter the corresponding PIN to pass identity authentication.

If the USB key driver is accidentally uninstalled, reset the login method for user **admin**. For details, see **Resetting Login Method for User admin**.

Constraints

- Currently, USB keys of Century Longmai (GM3000), Century Longmai - SM series algorithms (GM3000), JIT, Century Longmai - Certificates, Feitian - Certificates, and Feitian (ePass3000GM) are supported. USB keys from different vendors cannot identify each other for login authentication. Configure your vendor before enabling this authentication method. For details, see **Configuring USB Keys**.
- A USB key can be issued to one user only.

Prerequisites

You have obtained a USB key and installed the USB key driver locally.

Step 1 Configure USB Key Authentication

Step 1 Log in to your bastion host as the administrator.

Step 2 Choose **User** > **User** to go to the **User** management page.

Step 3 Select a user and click its **LoginName**.

Step 4 In the **User Setting** area, click **Edit**.

Step 5 In the displayed **Edit user setting** dialog box, select **USBKey** for **Multifactor Verification**.

Step 6 Click **OK**.

----End

Step 2: Issue the USBKey

Step 1 Log in to your bastion host as the administrator.

Step 2 Choose **User** > **USBKey** in the navigation pane.

Step 3 Click **Issue** to issue a USB key.

Step 4 Select a user with the USB key multifactor verification enabled as the related user.

Table 11-5 Parameters for issuing a USB key

Parameter	Description
USBKey	Specifies the USB key ID.

Parameter	Description
Relate User	Specifies the user to which the USB key is related. USB key in multifactor verification must be enabled for such users.
PIN	Specifies the personal identification number (PIN) uniquely corresponding to the USB key. It is provided by the USB key vendor.

Step 5 Click **OK**. You can then view the newly issued USB key in the USB key list.

When logging in to a bastion host with a USB key, insert your USB key into your local host, select the USB key on the login page, and enter the PIN as prompted. The USB key is identified automatically when it is inserted.

----End

11.2.4 Configuring OTP Token Login Verification

An OTP token is a security hardware device that generates one-time passwords. You can use event-based OTP tokens. In OTP token authentication method, both your static login password and a 6-digit one-time password generated by your hardware are required for login.

Constraints

- Currently, bastion hosts support only Jansh ETZ201/ETZ203 and Feitian OTP tokens.
- A hardware OTP token can be issued only to one user.

Prerequisites

You have obtained a hardware token.

Step 1: Configure OTP Token Authentication

Step 1 Log in to your bastion host as the administrator.

Step 2 Choose **User** > **User** to go to the **User** management page.

Step 3 Select a user and click its **LoginName**.

Step 4 In the **User Setting** area, click **Edit**.

Step 5 In the displayed **Edit user setting** dialog box, select **OTP token** for **Multifactor Verification**.

Step 6 Click **OK**.

----End

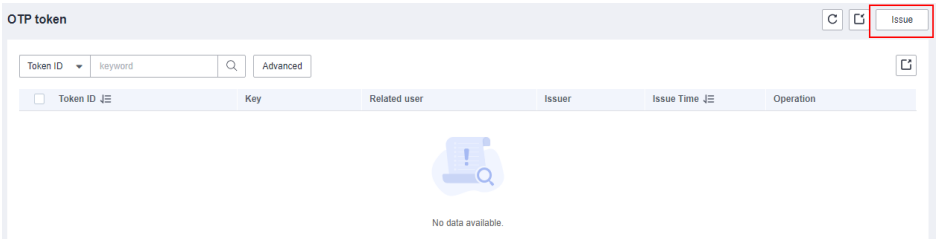
Step 2: Issue an OTP Token

Step 1 Log in to your bastion host as the administrator.

Step 2 Choose **User** > **OTP token** in the navigation pane.

Step 3 Click **Issue** to issue an OTP token.

Figure 11-12 Issuing an OTP token



Step 4 Enter the required token information.

Figure 11-13 Issue Token ID

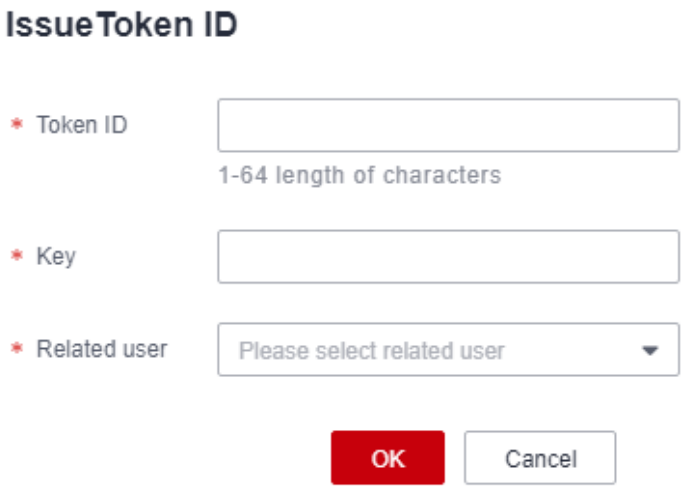


Table 11-6 Parameters for issuing an OTP token

Parameter	Description
Token ID	Specifies the OTP token ID.
Key	Specifies the key uniquely corresponding to the OTP token. It is provided by the OTP token vendor.
Relate User	User who the OTP token is related to.

Step 5 Click **OK**. You can view the newly issued OTP token in the OTP token list.

In the OTP token authentication method, the login page requires the login name, static password, and the dynamic OTP issued by your hardware token.

----End

11.2.5 Configuring Email Address Login Verification

For logins to bastion host instance, you can also enable email verification for users. Then, after a user enters a password, an email verification code is required for a login. In addition, email verification supports logins over SSH clients.

Prerequisites

- You have configured **an email address** and tested it successfully.
- You have added users. For details, see **Adding a User**.

Constraints

- This method is not supported for first-time logins. You need to configure email address login verification after the first login.
- The bastion host version must be 3.3.62.0 or later.

Adding an Email Address for an Account

Step 1 Log in to your bastion host instance in **Admin Login** mode and choose **User** > **User**.

Step 2 In the user list, select one or more accounts for which you want to add email addresses and choose **More** > **Edit multifactor** below the list.

Step 3 In the dialog box displayed, select the email verification mode.

NOTE

- If you have configured other login verification methods and still want to use them, select them all together in this step.
- If you want to enable email verification for all accounts in the department that the target account belongs to or all accounts in its subordinate departments, select **Modify All**.

Step 4 Click **OK**. Then, you can choose **User** > **User** and click the target account username to view the added email address and multifactor verification settings.

----End

11.3 Remote Authentication Management

11.3.1 Configuring Remote AD Authentication

You can interconnect your bastion host with the AD server to authenticate user logins. You can enable authentication mode or synchronization mode for the AD domain service.

- Auth Mode

  If this mode is selected, your bastion host does not synchronize user information from the AD domain server. You need to log in to the bastion host as the administrator and create system users manually. When a user logs in to your bastion host, its identity is authenticated by the AD domain server.

- Sync Mode

  If this mode is selected, your bastion host synchronizes user information from the AD domain server. So, there is no need to create system users additionally. When a user logs in to your bastion host, its identity is authenticated by the AD domain server. For details, see **Synchronizing AD Domain Users**.

Prerequisites

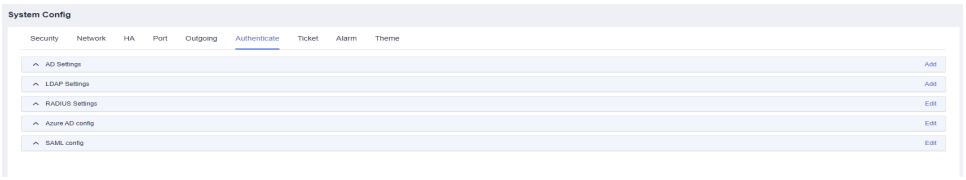
- You have the management permissions for the **System** module.
- You have obtained the information about the AD domain server.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Authenticate** to go to the authentication configuration page.

Figure 11-14 Configuring remote authentication



Step 3 Click **Add** in the **AD Settings** area.

Step 4 Select **Auth** for **Auth Mode** and configure other parameters as shown in **Table 11-7**.

Figure 11-15 AD Settings

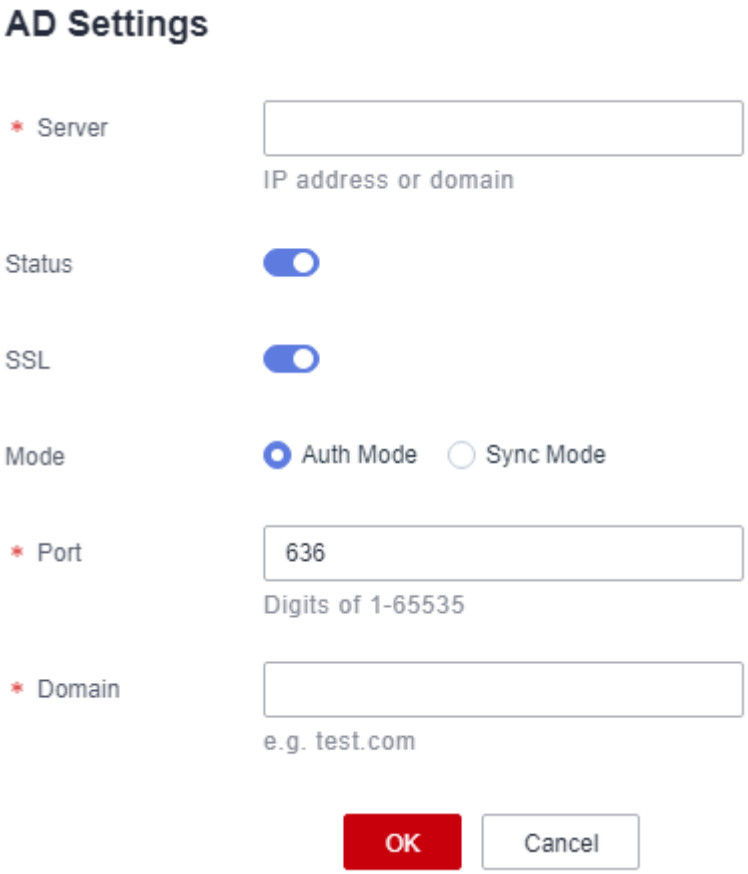


Table 11-7 AD authentication parameters

Parameter	Description
Server	Specifies the IP address of the AD domain server.
Status	Specifies the status of remote AD authentication (default: ). •  : AD domain authentication is enabled. If the configuration information is valid, AD domain authentication is enabled or AD domain users are synchronized to the bastion host when the user starts a login. • : AD authentication is disabled.
SSL	Specifies the status of SSL encryption (default:). • : SSL encryption is disabled. •  : SSL encryption is enabled. After SSL encryption is enabled, data transmitted by synchronized users or authenticated users is encrypted.
Mode	Specifies the working mode of AD domain. Select **Auth Mode**.

Parameter	Description
Port	Specifies the access port of the remote server of AD domain. The default port number is 389.
Domain	Specifies the domain of the AD service.

Step 5 Click **OK**. You can then view AD authentication configurations in the AD server list.

----End

Follow-up Operations

- To view details of the configured AD authentication, click **Details** in the **Operation** column.
- To modify or disable AD authentication, or change the authentication mode, click **Edit** in the **Operation** column and reconfigure the AD authentication in the displayed dialog box.
- If the AD authentication is no longer required, click **Delete** in the **Operation** column to delete it. Deleted authentication information cannot be recovered. Exercise caution when performing this operation.

11.3.2 Configuring Remote LDAP Authentication

You can interconnect your bastion host with the LDAP server to authenticate logins to the bastion host.

Constraints

- Identical configurations of two LDAP authentication servers are not allowed. Each LDAP server has unique combination of IP address, port number, and user OU.
- Querying authentication method is included in version 3.3.36.0 and later only. To use this function, upgrade your bastion host instance to the latest version by referring to **Upgrading the Instance Version**.

Prerequisites

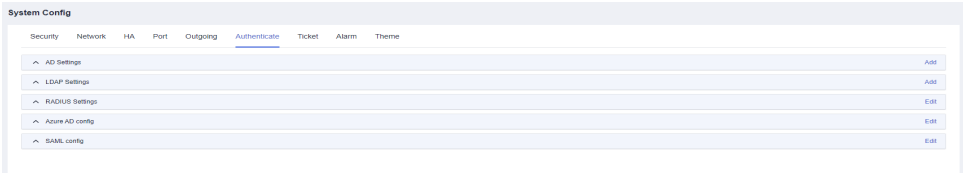
- You have the management permissions for the **System** module.
- You have obtained the information about the LDAP server.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Authenticate** to go to the authentication configuration page.

Figure 11-16 Configuring remote authentication



Step 3 Click **Add** in the **LDAP Settings** area.

LDAP supports the two authentication modes:

- If you select **Auth** for **Auth Mode**, configure the parameters by referring to **Table 11-8**.

Figure 11-17 Configuring LDAP authentication

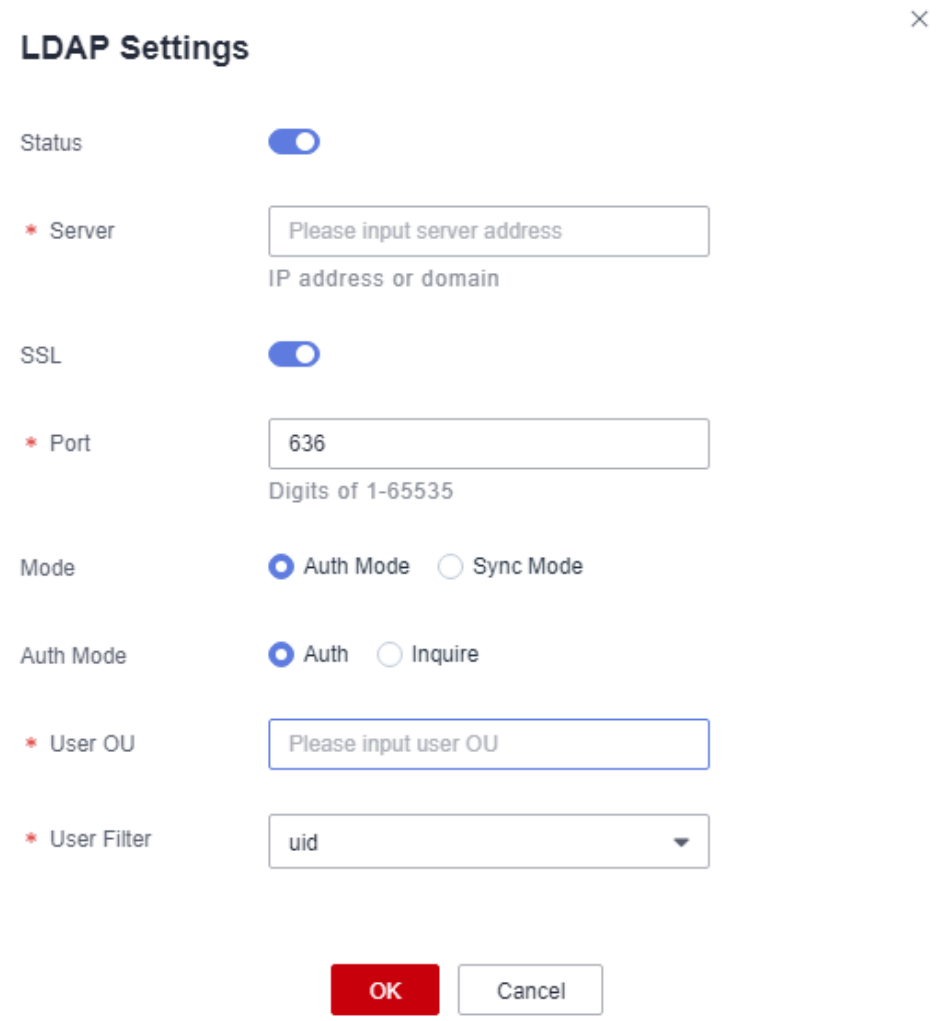


Table 11-8 LDAP authentication parameters

Parameter	Description
Server	Specifies the IP address of the LDAP server.

Parameter	Description
Status	Specifies whether to enable remote LDAP authentication. Remote LDAP authentication is enabled by default ( ). – : LDAP authentication is enabled. Remote LDAP authentication is enabled when a user starts a login. – : LDAP authentication is disabled.
SSL	Specifies whether to enable SSL encryption. SSL encryption is disabled by default ( ). – : SSL encryption is disabled. – : SSL encryption is enabled. After SSL encryption is enabled, data transmitted by synchronized users or authenticated users is encrypted.
Port	Specifies the access port of the remote LDAP server. The default port number is 389.
Mode	Select **Auth Mode** or **Sync Mode**. – **Auth Mode**: The bastion host is interconnected with the AD server. To add a domain user, you need to manually select LDAP authentication on the user management page. – **Sync Mode**: After the bastion host is connected to the AD server, you can choose **Systemconfig > Authenticate** and synchronize users under the corresponding OU to the bastion host.
User OU	Specifies the user organization unit (OU) on the LDAP server.
User Filter	Specifies the users to be filtered out on the LDAP server.

- Select **Auth** for **Auth Mode** and configure the parameters by referring to **Table 11-9**.

  NOTE

  Querying authentication methods is supported in version 3.3.36.0 and later only. To use this function, upgrade your bastion host to the latest version by referring to **Upgrading the Instance Version**.

Figure 11-18 Inquire

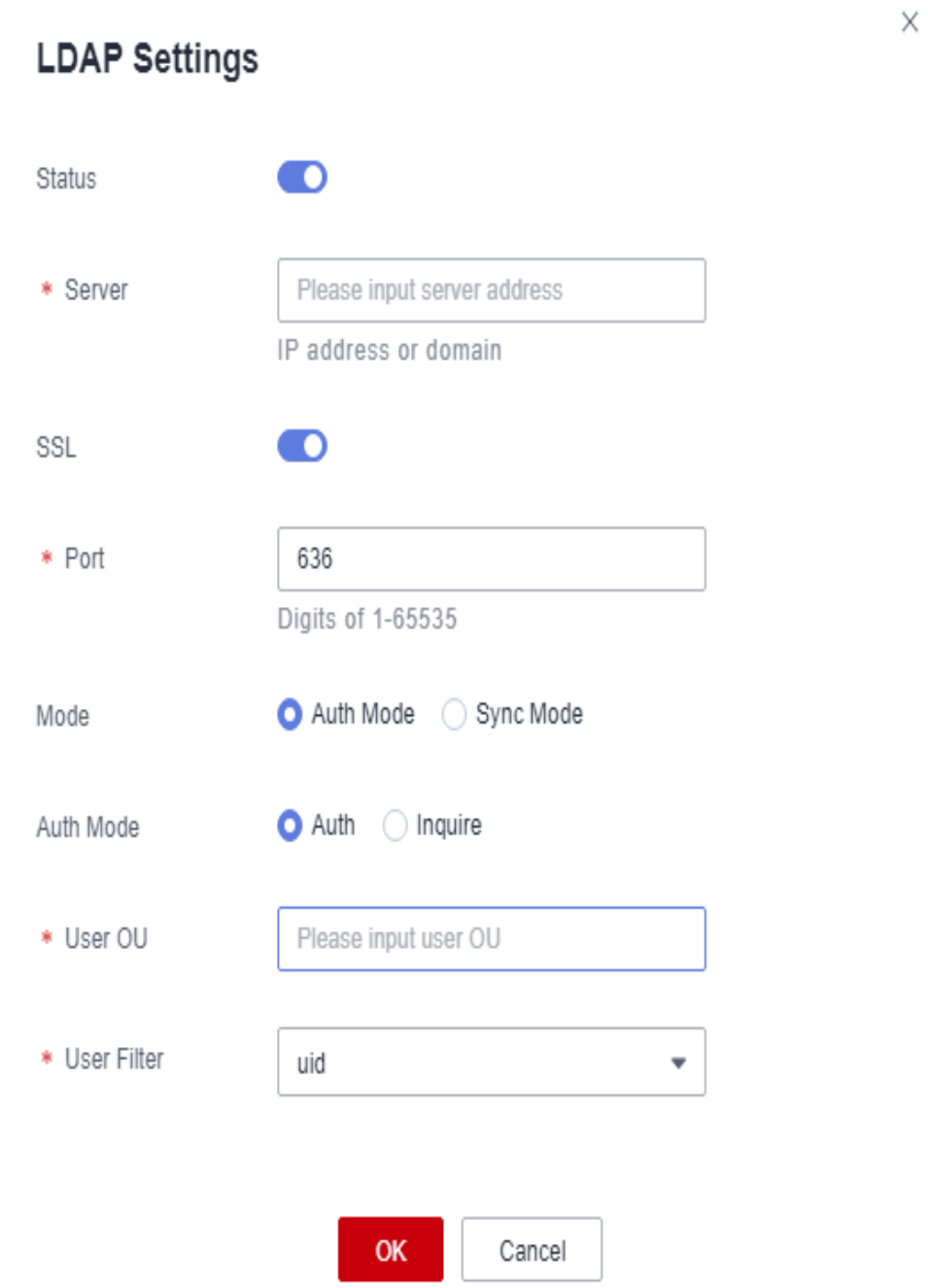


Table 11-9 LDAP inquiring mode parameters

Parameter	Description
Server	Specifies the IP address of the LDAP server.

Parameter	Description
Status	Specifies whether to enable remote LDAP authentication. Remote LDAP authentication is enabled by default ( ). – : LDAP authentication is enabled. Remote LDAP authentication is enabled when a user starts a login. – : LDAP authentication is disabled.
SSL	Specifies whether to enable SSL encryption. SSL encryption is disabled by default ( ). – : SSL encryption is disabled. – : SSL encryption is enabled. After SSL encryption is enabled, data transmitted by synchronized users or authenticated users is encrypted.
Port	Specifies the access port of the remote LDAP server. The default port number is 389.
Mode	Select **Auth Mode** or **Sync Mode**. – The bastion host is interconnected with the AD server. To add a domain user, you need to manually select LDAP authentication on the user management page. – After the CBH instance is connected to the AD server, you can choose **Systemconfig** > **Authenticate** and synchronize users under the corresponding OU to the bastion host.
Base DN	Base DN of the LDAP server.
Administrator DN	Administrator DN.
Administrator Password	Password of the administrator.
User OU	Specifies the user organization unit (OU) on the LDAP server.
User Filter	Specifies the users to be filtered out on the LDAP server.

Step 4 Click **OK**. You can then view LDAP authentication configurations in the LDAP server list.

----End

Follow-up Operations

- To view details of the configured LDAP authentication, click **Details** in the **Operation** column.
- To modify or disable LDAP authentication, click **Edit** in the **Operation** column and reconfigure LDAP authentication in the displayed dialog box.

- If the LDAP authentication is no longer required, click **Delete** in the **Operation** column to delete it. Deleted authentication information cannot be recovered. Exercise caution when performing this operation.

11.3.3 Configuring Remote RADIUS Authentication

You can interconnect your bastion host with the RADIUS server to authenticate logins to your bastion host.

This topic describes how to configure the RADIUS authentication and how to test the user validity of the configured RADIUS authentication.

Prerequisites

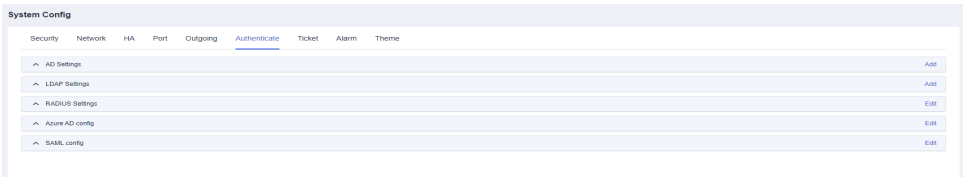
- You have the management permissions for the **System** module.
- You have obtained the information about the RADIUS server.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Authenticate** to go to the authentication configuration page.

Figure 11-19 Configuring remote authentication



Step 3 Click **Edit** in the **RADIUS Settings** area.

Figure 11-20 RADIUS Settings

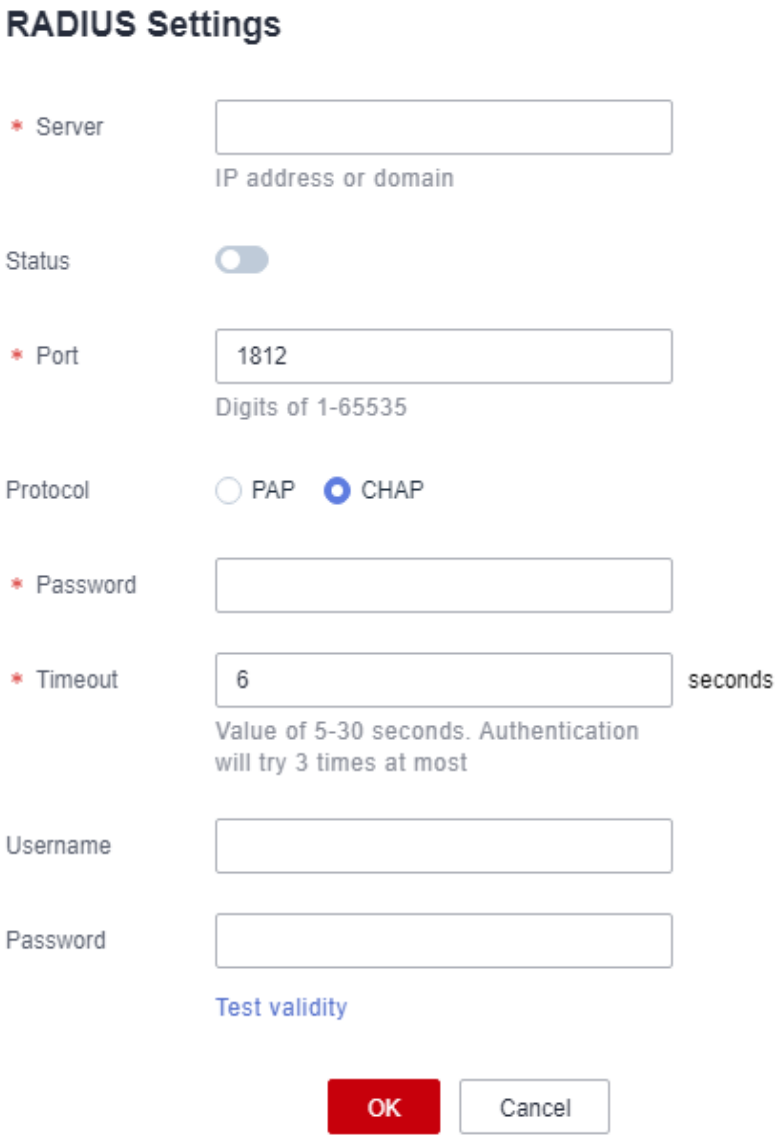


Table 11-10 RADIUS authentication parameters

Parameter	Description
Server	Specifies the IP address of the RADIUS server.
Status	Specifies the status of remote RADIUS authentication (default:). • : RADIUS authentication is enabled. Remote RADIUS authentication is enabled when the user starts a login. • : RADIUS authentication is disabled.
Port	Specifies the access port of the remote RADIUS server. The default port number is 1812.

Parameter	Description
Protocol	Specifies the remote authentication protocol. This parameter can be set to **PAP** or **CHAP**. **NOTE** The value must be the same as the authenticated resource protocol.
Password	Specifies the authentication key of the remote RADIUS server.
Timeout	Specifies the timeout for remote RADIUS authentication.
Username	Specifies the username on the RADIUS server to test whether the RADIUS server information is correct.
Password	Specifies the password of username on the RADIUS server to test whether the RADIUS server information is correct.
Test validity	You can click **Test validity** to test whether the RADIUS server is configured properly.

Step 4 Click **OK**. You can then view RADIUS authentication configurations in the RADIUS server list.

----End

Follow-up Operations

To modify or disable RADIUS authentication, click **Edit** in the **Operation** column and reconfigure RADIUS authentication in the displayed dialog box.

11.3.4 Configuring Remote Azure AD Authentication

You can interconnect your bastion host with the Azure AD platform to authenticate logins to your bastion host.

Prerequisites

- You have the management permissions for the **System** module.
- You have created users and added enterprise application resources on Azure AD, and obtained information about the Azure AD platform configuration.

  NOTE

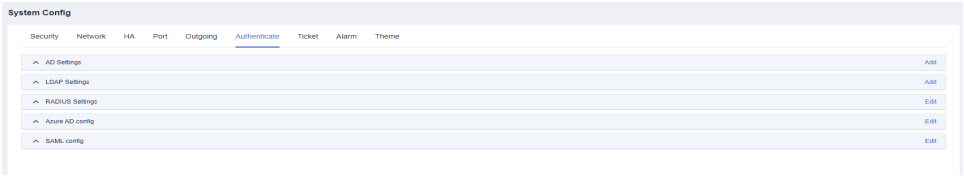
  Azure AD-related operations and configurations need to be performed on the Azure page. For details, see related documents on the Azure official website or contact Azure engineers.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Authenticate** to go to the authentication configuration page.

Figure 11-21 Configuring remote authentication



Step 3 Click **Edit** in the **Azure AD config** area.

Figure 11-22 Azure AD Config

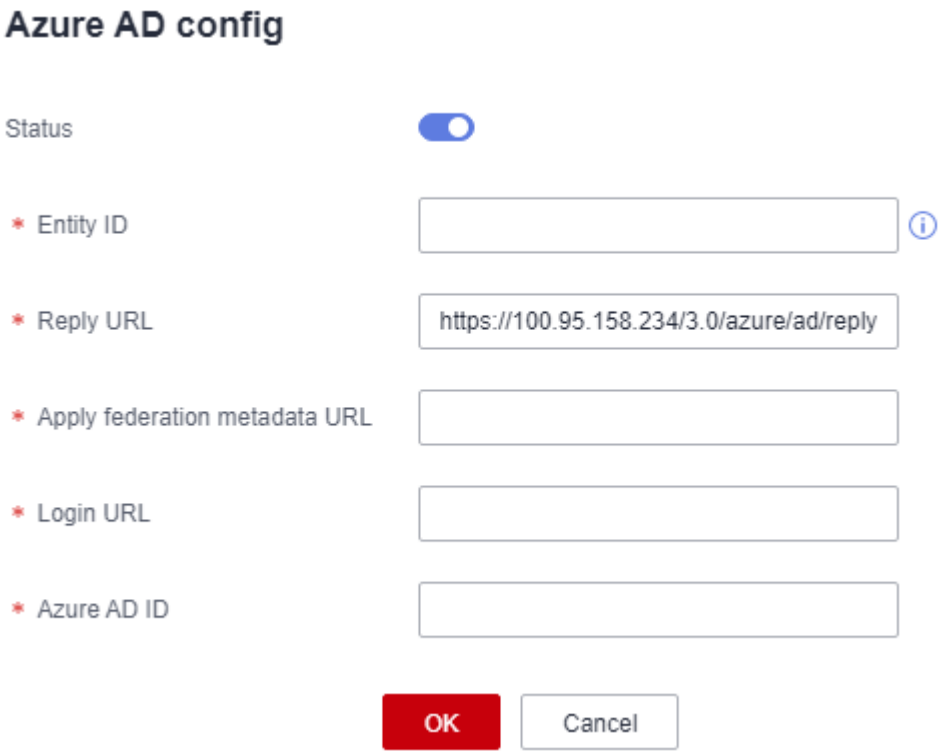


Table 11-11 Azure AD authentication parameters

Parameter	Description
Status	Specifies the status of remote Azure AD authentication (default:). • : Azure AD authentication is enabled. Remote Azure AD authentication is enabled when a user starts a login. • : Azure AD authentication is disabled.
Entity ID	Specifies the enterprise name or URL.
Reply URL	Specifies the reply URL. This parameter is automatically set to the URL of the current bastion host. If the IP address or domain name of the bastion host is changed, change the IP address or domain name in the URL.

Parameter	Description
Apply federation metadata URL	Specifies the application federation metadata URL generated after SAML signature certificate is configured in Microsoft Azure.
Logon URL	Specifies the login URL generated after SAML single sign-on is configured in Microsoft Azure.
Azure AD ID	Specifies the Azure AD ID generated after SAML single sign-on is configured in Microsoft Azure.

Step 4 Click **OK**. You can then view Azure AD authentication configurations in the Azure AD server list.

NOTICE

If the Azure AD certificate is updated, you need to delete the old certificate on the Azure AD portal before logins.

----End

Follow-up Operations

- To modify or disable Azure AD authentication, click **Edit** in the **Operation** column and reconfigure Azure AD authentication in the displayed dialog box.
- After Azure AD authentication is configured, you are required to create a user who has been added to the enterprise application or created on the Azure platform. For details, see **Creating a User**.

11.3.5 Configuring Remote SAML Authentication

You can interconnect your bastion host with the SAML platform to authenticate logins to your bastion host.

This topic describes how to configure the SAML authentication mode.

Prerequisites

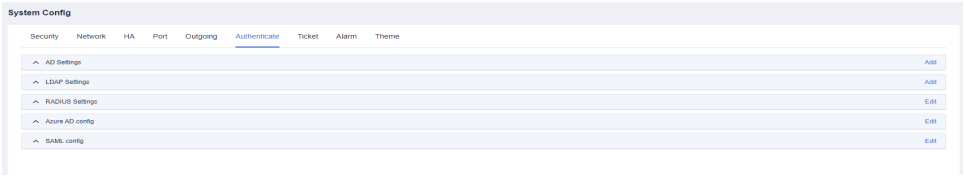
- You have obtained the permission to manage the **System** module in the bastion host.
- You have created a user on the SAML platform and obtained related configurations on the SAML platform.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Authenticate** to go to the authentication configuration page.

Figure 11-23 Configuring remote authentication



Step 3 Click **Edit** in the **SAML Settings** area.

Figure 11-24 Configuring SAML authentication

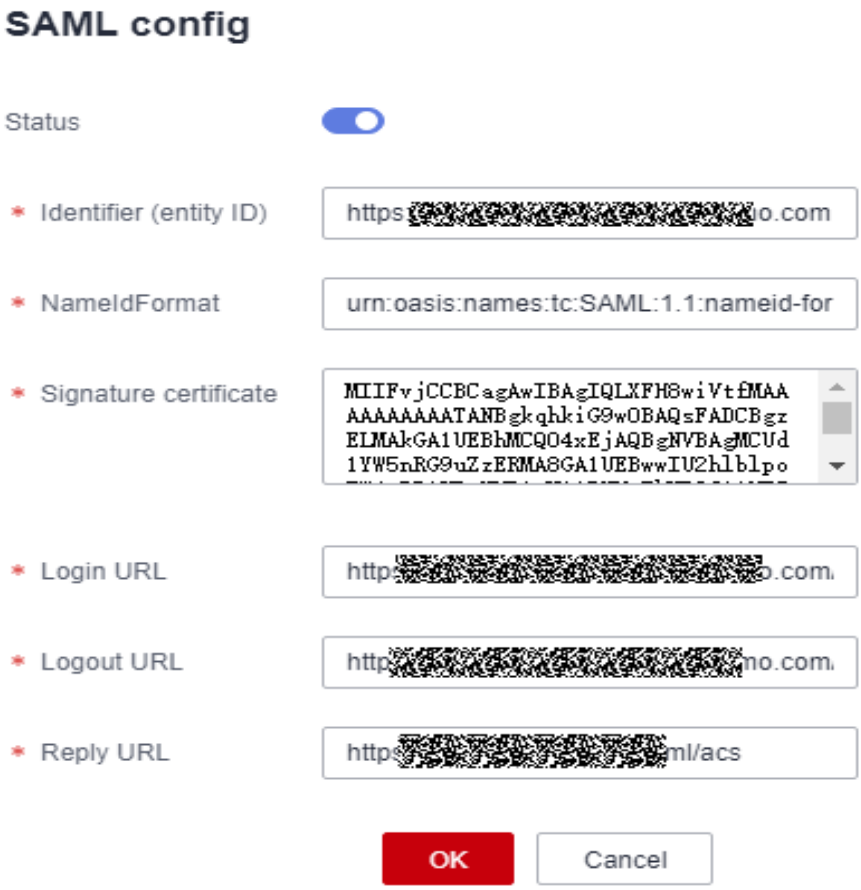


Table 11-12 SAML authentication parameters

Parameter	Description
Status	Specifies the status of remote SAML authentication (default:). • : SAML-based authentication is enabled. Remote SAML authentication is enabled when the user starts a login. • : SAML-based authentication is disabled.

Parameter	Description
Cover Existing Users	Whether to enable the SAML overwriting function. The default value is . •  : If an account with the same username already exists, the existing account will be overwritten. • : If an account with the same name already exists, the SAML user fails to be created in the system.
Entity ID	Obtain the metadata from IdP (Shibboleth IDP, which is configured in the **C:\Program Files (x86)\Shibboleth\IdP\metadata** directory by default). Identifier: Enter the following part of **EntityID**.
NameIdFormat	Obtain the metadata from IdP (Shibboleth IDP, which is configured in the **C:\Program Files (x86)\Shibboleth\IdP\metadata** directory by default). NameIdFormat: The value **urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified** is recommended.
Signature certificate	Enter the signing certificate of **FrontChannel** displayed in the IdP.
Logon URL	Enter the location address of **SingleSignOnService** displayed in the **HTTP-Redirect**.
Logout URL	Enter the location address of **SingleSLogoutService** displayed in the **HTTP-Redirect**.
Reply URL	The default value of **Host** is the IP address of **Localhost**. Set this parameter based on the site requirements, for example, the domain name.

Step 4 Click **OK** to submit the configuration data. You can view and manage SAML authentication configurations.

----End

12 Login Security Configuration

12.1 Configuring User Login Lockout

To harden login security, the source IP address, or the combination of the user account and source IP address, or user account will be locked out if the number of consecutive invalid password attempts exceeds the configured threshold.

This topic describes how to configure the user login lockout, including changing the lockout method, lockout duration, and maximum login attempts.

Prerequisites

You have the management permissions for the **System** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Security**.

Step 3 In the **UserLock Config** area, click **Edit**.

Complete configurations as prompted.

Figure 12-1 UserLock Config

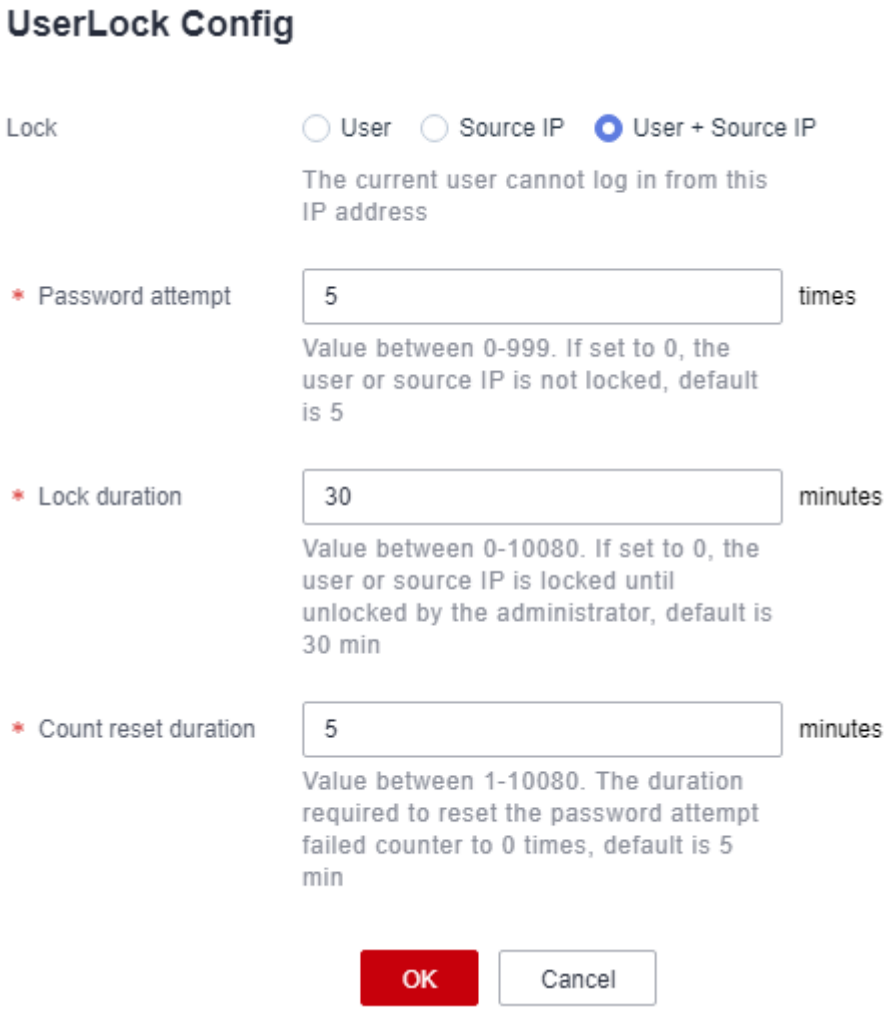


Table 12-1 Parameters for configuring user lockout

Parameter	Description
Lock	Select the user lockout method. • **User**: If the number of consecutive failed password attempts exceeded the upper limit, the user is blocked by the system. • **Source IP**: If the number of consecutive failed password attempts exceeded the upper limit, the source IP address is blocked by the system. • **User + Source IP**: If the number of consecutive failed password attempts exceeded the upper limit, the login name and source IP address are blocked by the system.

Parameter	Description
Password attempt	Allowed maximum number of consecutive failed password attempts. • Default value: **5** • Value range: **0** to **999** • If this parameter is set to **0**, the user account will not be locked out even if the password is incorrect.
Lock duration	Lockout duration • Default value: **30** minutes • Value range: **0** to **10080**, in minutes • If this parameter is set to **0**, the user account or source IP address will be locked out unless the administrator unlocks it.
Count reset duration	Duration after which the number of login failures is reset to **0**. • Default value: **5** minutes • Value range: **1** to **10080**, in minutes

Step 4 Click **OK**. You can then check the lockout configuration of the current system user on the **Security** tab.

----End

12.2 Configuring the Login Password Rules

This topic describes how to configure the user password policies, including the password strength, number of password verification times, and password change period.

Prerequisites

You have the management permissions for the **System** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Security**.

Step 3 In the **Password Config** area, click **Edit**.

Complete configurations as prompted.

Figure 12-2 Password Config

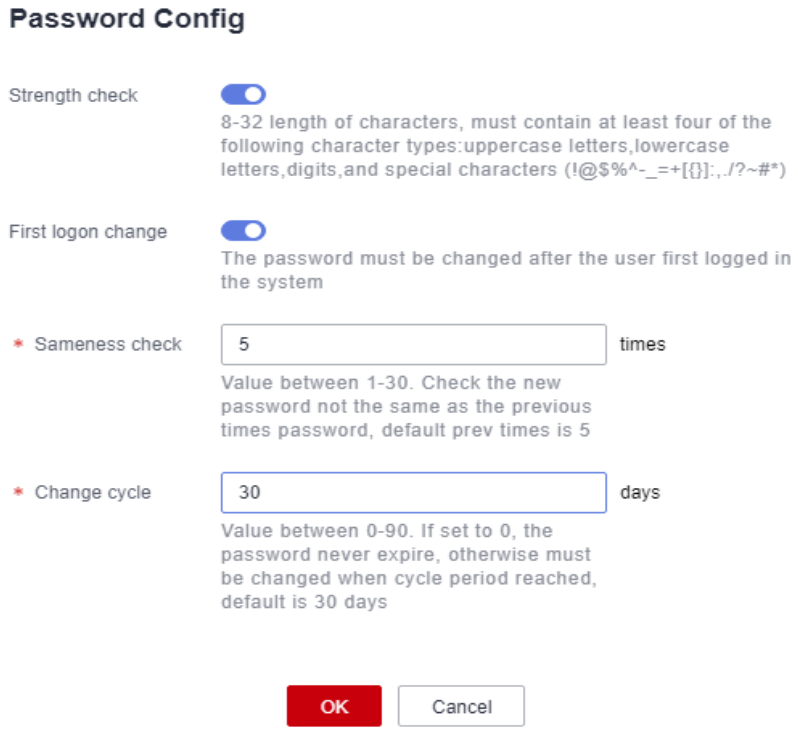


Table 12-2 Parameters for configuring a password rule

Parameter	Description
Strength check	Checks password strength. It is enabled ( ) by default. • : disabled • : The password can contain 8 to 32 characters and must contain at least three types of the following characters: uppercase letters, lowercase letters, digits, and special characters !@$%^-_=+[{}]:,./?~#*.
First logon change	Forces a user to change password upon first login to the system. It is enabled ( ) by default. • : disabled. • : enabled.
Sameness check	Prohibits the reuse of the latest *N* passwords. • The password used for initial login is not counted. • Default value: **5** • Value range: **1** to **30**

Parameter	Description
Change cycle	Password validity period. Users will be forced to change their passwords upon expiry. • Default value: **30** days • Value range: **0** to **90**, in days • If the value is **0**, the password never expires.

Step 4 Click **OK**. You can then check the password rule of the current system user on the **Security** tab.

----End

12.3 Configuring Web Login Timeout and Authentication

This topic describes how to configure the timeout and authentication settings for logins through web browsers, including login timeout duration, SMS verification code validity period, graphic verification code, SSH public key login, and SSH password login.

Prerequisites

You have the management permissions for the **System** module.

Configuring Web Login Requirements

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Security**.

Step 3 In the **Web Login Config** area, click **Edit**.

Complete configurations as prompted.

Table 12-3 Parameters for configuring web login

Parameter	Description
Idle timeout	Duration to wait before an inactive user is logged out. After a system user logs in to a bastion host through a web browser, if they have no operations for a period longer than the configured idle timeout, they will be logged out. • Default value: **30** minutes • Value range: **1** to **1,440**, in minutes

Parameter	Description
SMS duration	SMS verification code validity period. • Default value: **60** seconds • Value range: **60** to **3,600**, in seconds • If the value is **0**, the SMS verification code never expires.
Captcha	Whether to use the CAPTCHA technology for graphic verification. The options are **Enable**, **Disable**, and **Auto**. • **Enable**: A graphic verification code is required for every login. • **Disable**: No graphic verification code is required for logins. • **Auto**: A graphic verification code is required when the number of consecutive failed password attempts exceeds the configured login attempts.
Login attempts	If the number of consecutive failed password attempts exceeds the login attempts, the graphic verification is automatically enabled. • This parameter is mandatory if **Captcha** is set to **Auto**. • Default value: **3** • Value range: **1** to **30**
Captcha duration	Validity period of a CAPTCHA. • Default value: **60** seconds • Value range: **15** to **3600**, in seconds • If the value is **0**, the graphic verification code never expires.
Domain Check	Whether to check domain. This option is disabled by default ( ). • : enabled. If you select the AD domain authentication, you are required to download an SSO client and use the same login name as that registered with the AD domain server for logins. • : disabled

Parameter	Description
Source IP Check	Whether to check source IP address. The default status is . •  : The **Source IP Check** is enabled. If this function is enabled, your bastion host obtains the source IP address of the access request from the TCP connection details. When the system finds that the source IP address changes, it disconnects the current session and requires the user to log in again. • : The **Source IP Check** is disabled. If this function is disabled, the session is not disconnected when the source IP address changes. **NOTE** – A bastion host will record every source IP address no matter whether **Source IP Check** is enabled. – If you are logged out over and over again due to IP address changes after enabling **Source IP Check**, you can disable it. There are no impacts on your using of the bastion host. – Only V3.3.44.0-S and later versions support this function.
Not Allow Multipoint Login	After this function is enabled, the same bastion host does not allow login from multiple addresses or devices.
Keep Client Session	To enable or disable this function, you need to enable **Not Allow Multipoint Login** first. • Disabled: When system users access the bastion host through the web page, the sessions of the logged-in clients are forcibly disconnected. If they log in to the bastion host through the same client, the sessions of the logged-in clients cannot be forcibly disconnected. • Enabled: After this function is enabled, when system users access the bastion host through the web page, the client session that has been logged in to is not forcibly disconnected. The client session is retained, and logins through web page is disabled.
Enforce Multifactor Login	If this function is enabled, the system forcibly uses multi-factor authentication for logins. If multi-factor authentication is not configured for the account, contact the administrator to configure it. Otherwise, disable this function.

Step 4 Click **OK**. You can then check the web login configuration of the current system on the **Security** tab.

----End

Configuring Login Using a Client

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Security**.

Step 3 In the **Client Login Config** area, click **Edit**.

Complete configurations as prompted.

Table 12-4 Parameters for configuring client login

Parameter	Description
Idle timeout	Duration to wait before an inactive user is logged out of the bastion host SSH client. • Default value: **30** minutes • Value range: **1** to **43200**, in minutes
Logon with SSH key	Whether to enable SSH key login authentication (Default:). • : enabled. If you have configured an SSH public key, you can log in to the system using the SSH client without providing passwords. • : disabled.
Logon with password	Whether to enable SSH password login authentication (Default:). • : enabled • : disabled • If both **Logon with SSH key** and **Logon with password** are enabled, the SSH key login authentication is preferentially performed.

Step 4 Click **OK**. You can then check the client login configuration of the current system on the **Security** tab.

----End

12.4 Updating a System Web Certificate

A web certificate for a bastion host is a Secure Sockets Layer (SSL) server digital certificate issued by a trusted root certificate authority (CA). The certificate is used to verify the website identity and secure connections.

A secure self-issued certificate is configured for each bastion host by default, but this certificate takes effect only within certain scope and period. You can replace it with your own certificate.

This topic describes how to update the system certificate if it expires or fails a security check.

NOTE

If the browser still says the system is insecure after you update an SSL certificate, fix the issue by referring to **Why Does the Browser Still Consider the Website Insecure While the Website Has an SSL Certificate Deployed?**

Prerequisites

- You have purchased and downloaded an SSL certificate.
- The domain name the uploaded certificate is used for has been resolved to the EIP bound to the bastion host. For details, see **Adding Record Sets for a Public Zone**.
- You have the management permissions for the **System** module.

Constraints

- Currently, only the Java Keystore certificate file of Tomcat, that is, the certificate file in .jks is supported.
- Currently, the bastion host system supports the following certificate cryptographic algorithms: RSA and ECDSA.
- A certificate file cannot exceed 20 KB and must contain a certificate password. When you upload an SSL certificate, provide its password for verification, or the upload will fail.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Security**.

Step 3 In the **Web Certificate** configuration area, click **Edit**. The **Web Certificate** upload dialog box is displayed.

Step 4 Upload the certificate file downloaded in your computer.

Step 5 After the certificate file is uploaded, enter the Keystore password to verify the certificate.

Step 6 Click **OK**. You can then check the web certificate configuration of the current system user on the **Security** tab.

Step 7 Restart the bastion host for the updated certificate to take effect.

You can use either of the following methods to restart the bastion host:

- Restart a bastion host instance on the Huawei Cloud management console. For details, see **Restarting a Bastion Host Instance**.
- Use the system tool in a bastion host to restart. For details, see **Managing System Tools**.

Figure 12-3 System web certificate information

----End

12.5 Configuring the Mobile OTP Type

A mobile OTP application is a software token application used to generate a dynamic password on a bound mobile phone. In mobile OTP verification method, a password and a 6-digit mobile OTP verification code are required for logging in to a bastion host.

This topic describes how to set the mobile OTP type.

Constraints

- Currently, only the following OTP types are supported:
  - Built-in mobile OTPs support Time-based One-Time Password (TOTP). You need to bind a mobile OTP to a user in the **Profile** module in your bastion host system. You can bind a mobile OTP through a WeChat applet or other similar programs, such as Google Authenticator and FreeOTP Authenticator, that support TOTP.
  - RADIUS mobile OTPs also support TOTP. You need to connect to the RADIUS server you have created and bind the mobile OTP on the RADIUS server. You can bind the mobile OTP through a WeChat applet or similar programs, such as Google Authenticator and FreeOTP Authenticator, that support TOTP.
- For the mobile token to take effect, ensure that the mobile token types configured in the system and on your mobile phone are the same.

Prerequisites

You have the management permissions for the **System** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Security**.

Step 3 In the **Mobile Token Settings** area, click **Edit**.

Step 4 In the displayed **Mobile Token Settings** dialog box, select a mobile OTP type.

You can select **Built-in** or **RADIUS**. If you select **RADIUS**, the parameters are described as follows:

Table 12-5 RADIUS mobile OTP parameters

Parameter	Description
Server	Enter the IP address of the RADIUS server.
Port	Enter the port number of the RADIUS server.
Protocol	The options are **PAP** and **CHAP**.
Password	Enter the shared key for RADIUS server authentication.
Timeout	Configure an authentication timeout. The value ranges from 5 to 30, in seconds. A maximum of three authentication attempts are allowed, and each attempt must be within the configured authentication timeout.

Step 5 Click **OK**. You can then check the mobile token settings of the current system user on the **Security** tab.

----End

12.6 Configuring the USB Key Vendor

This topic describes how to configure the USB key vendor.

Constraints

- Currently, the bastion host supports USB keys of Century Longmai (GM3000), JIT, Century Longmai-SM series algorithms (GM3000), and ePass3000GM.
- If you change the vendor of a USB key, the issued USB key cannot be identified by the system.
- For details about the USB key vendor configuration, see **Configuring USB Key Login Verification**.

Prerequisites

You have the management permissions for the **System** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Security**.

Step 3 In the **USB Key Settings** area, click **Edit**.

Step 4 In the displayed dialog box, select a vendor.

Step 5 Click **OK**. You can then check the USB key settings of the current system on the **Security** tab.

----End

12.7 Configuring Policies to Disable Certain Users (Available in V3.3.30.0 and Later)

The zombie user policy function allows you to identify zombie users and customize a threshold time range. If a user does not log in to the system within the configured threshold time range, the system marks the user as zombie and disables the user. Only the administrator can enable the zombie user. The default threshold is 30 days. If the threshold is set to 0, all users are disabled immediately.

Prerequisites

You have the management permissions for the **System** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Security**.

Step 3 In the **UserDisabled Config** area, click **Edit**.

- **Disable zombie users**: By default, this function is disabled. After this function is enabled, the status is  .
- **Determines the zombie user time**: The value ranges from 0 to 10,080. The default value is 30 days. If the value is set to 0, all users are disabled immediately until the administrator cancels the disabling. For details about how to enable users, see **Enabling or Disabling a User**.

Step 4 Click **OK**.

----End

12.8 Configuring the RDP Resource Client Proxy (Available in 3.3.26.0 and Later Versions)

If a server that uses the RDP protocol to establish connections through the bastion host over RDP, the security layer verification is used. You can select a security layer verification mode.

Prerequisites

You have the management permissions for the **System** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Security**.

Step 3 In the **RDP resource client proxy Configuration** area, click **Edit**.

Step 4 In the **Security layer** drop-down list, select a client proxy and click **OK**.

You can select **RDP**, **TLS**, or **Negotiate**.

----End

12.9 Enabling API Configuration (Included in V3.3.34.0 and Later Versions Only).

After you enable the API configuration, you can use your bastion host by calling APIs.

Prerequisites

You have the management permissions for the **System** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Security**.

Step 3 In the **API Config** area, click **Edit**.

Step 4 Click .

Step 5 Click **OK**.

----End

12.10 Configuring Automatic Inspection (Available in V3.3.36.0 and Later)

After automatic inspection is enabled, the system automatically verifies accounts of managed resources at 01:00 on the 5th, 15th, and 25th days of each month.

Prerequisites

You have the management permissions for the **System** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Security**.

Step 3 In the **Auto Inspect Config** area, click **Edit**.

Step 4 By default, automatic inspection is enabled. You can click  to disable it.

Step 5 Click **OK**.

----End

12.11 Configuring a Resource Account

If you enable this function, account **Empty** is automatically added. You can modify the account name. You can also disable this function. If it is disabled, a custom account name is required when creating a resource account.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Security**.

Step 3 On the right of resource account configuration, click **Edit** to go to the configuration page.

Step 4 The **Empty** account is automatically added and enabled by default (). You can disable it if needed.

Step 5 Click **OK**.

----End

12.12 Configuring Client Login

You can configure an automatic logout timeout for inactive users. In addition, you can configure a verification-free duration for repeated SSH client logins.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Security**.

Step 3 On the right of the **Client Login Config** bar, click **Edit**. The **Client Login Config** dialog box is displayed.

Step 4 Set the client login parameters by referring to **Table 12-6**.

Table 12-6 Configuring Client Login

Parameter	Description	Example Value
Idle timeout	If no operation is performed within the specified period after a successful login, the user is automatically logged out. The user needs to log in again. The value ranges from 1 to 43,200, in minutes. The default value is **30**.	30
Logon with SSH key	Whether to enable SSH key login authentication for users who have been logged out after idle timeout. This function is enabled by default.	
Logon with password	Whether to enable SSH password authentication for users who have been logged out after idle timeout. This function is enabled by default.	
Captcha Validation Free Time	After multifactor authentication is enabled, you can configure a grace period for authenticated SSH sessions, allowing users to reconnect without entering credentials repeatedly during this period. The default value is 0, which means that you must enter the verification code for each login. The value ranges from 0 to 168, in hours. The default value is **0**. **NOTE** If the validation-free time is changed, you need to enter the verification code again when logging in over the SSH client. The configured validation-free time will be counted from the start again.	0

Step 5 Click **OK**.

----End

12.13 Configuring a User Expiration Reminder

You can configure a user validity period reminder. Then, the system will send an email reminder every day 5 days before the user validity period actually expires.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Security**.

Step 3 On the right of **User Expiration Countdown Settings**, click **Edit** to go to the configuration page.

Step 4 Set **User Password** and enable **User Expiration Countdown** ( ).

Step 5 Click **OK**.

----End

12.14 Configuring Session Limit

If you configure the session limit settings, new sessions cannot be created when the CPU usage, disk space, or memory usage triggers the configured limit. Any ongoing session that triggers the timeout limit configured will be disconnected.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Security**.

Step 3 Click **Edit** on the right of **Session Limit Settings** to go to the configuration page.

Step 4 Enable **Session Limit** (enabled status:) and set the CPU and memory usage, disk space threshold, and session timeout. When any of the limits is reached, new sessions will be stopped. Any ongoing session that triggers the session timeout will be disconnected.

NOTE

If you configure a session timeout, a countdown timer is displayed on the right of the session window. To set a longer timeout, contact the administrator to increase the session timeout. The countdown timer will turn red if there are only 15 minutes left.

Step 5 Click **OK**.

----End

12.15 Configuring Insecure Protocols

You can enable and disable insecure protocols as needed.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Security**.

Step 3 On the right of the **Protocol Config** area, click **Edit**. In the displayed dialog box, enable this function.

After this function is enabled, FTP, Telnet, and Rlogin can be used. Note that using insecure protocols may put your data at risk. Do not enter sensitive information.

Step 4 Confirm the information and click **OK**.

----End

12.16 Configuring Insecure Algorithms

You can enable and disable insecure algorithms as needed.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Security**.

Step 3 On the right of the **Algorithm Config** area, click **Edit**. In the displayed dialog box, enable this function.

After this function is enabled, SSH allows the use of insecure algorithms for interoperability with third-party systems or compatibility with other scenarios. If insecure algorithms are used, your data may be at risk. Do not enter sensitive information.

Step 4 Confirm the information and click **OK**.

----End

13 Instance Configuration

13.1 Instance Configuration Overview

System configuration includes security, network, port, outgoing, authentication, ticket, alarm, audit, and HA backup. By default, only the system administrator **admin** has permissions to modify system configurations and manage the overall system running status.

- Security configuration: See **Login Security Management**.
- Network configuration: See **Network**.
- HA configuration: See **HA**.
- Port configuration: See **Port**.
- Outgoing configuration: See **Outgoing**.

  NOTE

  User Expiration Countdown Settings: If you configure this, you will receive an email five days before a user expires.
- Authentication configuration: See **Remote Authentication Management**.
- Ticket configuration: See **Ticket Configuration Management**.
- Alarm configuration: See **Alarm**.
- System theme: See **Theme**.

13.2 Network

13.2.1 Viewing Network Configurations

This topic describes how to view the system network interface, DNS address, default gateway address, and static routes.

Prerequisites

You have the management permissions for the **System** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Network**.

Step 3 In the **Network interfaces** area, view the network interface information of the bastion host.

By default, the network interfaces cannot be modified.

Step 4 In the **DNS** configuration area, view the primary and secondary DNS addresses of the bastion host.

By default, the DNS address cannot be changed.

Figure 13-1 System DNS address

Step 5 In the **Gateway** area, view the default gateway of the bastion host.

By default, the DHCP gateway address is identified as the system gateway. The default gateway cannot be changed.

Figure 13-2 System default gateway

Step 6 In the **Static Route** configuration area, view accessible servers in other network segments.

----End

13.2.2 Adding a Static Route to Your Bastion Host

After a bastion host restarts, non-static routes may be lost, affecting network availability. To prevent this issue, add static routes to the system.

Prerequisites

You have the management permissions for the **System** module.

CAUTION

Each static route must be correct. If the information is incorrect, you cannot log in to your bastion host.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Network**.

Step 3 In the **Static Route** configuration area, click **Add**.

In the displayed **Add static route** dialog box, configure other parameters.

Step 4 Click **OK**. You can then go to the **Security** configuration page and view the configured static route.

----End

Follow-up Operations

To delete a static route, click **Delete** in the **Operation** column in the corresponding row.

13.3 HA

13.3.1 Enabling HA

A bastion host supports dual-node high availability (HA). After HA is enabled, the secondary node will take over the service if the primary node breaks down.

Constraints

- The primary node must be configured first. After the primary node is configured and the configuration takes effect, configure the secondary node and ensure that the primary and secondary nodes use the internal network for HA synchronization configuration.
- After the HA configuration on the secondary node is complete, the historical data is cleared regardless of whether there is configuration data on the secondary node, and the configuration data of the primary node is synchronized to the secondary node.

Prerequisites

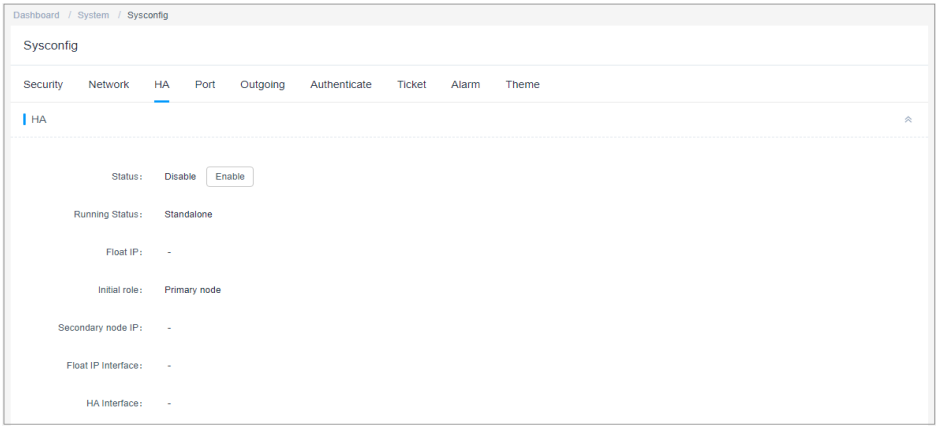
- You have the management permissions for the **System** module.
- You have prepared two bastion hosts, and both of them use the same license.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **HA**.

Figure 13-3 HA



Step 3 View the HA status. By default, the HA status is **Disabled**.

CAUTION

Do not disable HA for a primary/standby instance you buy, or logins will fail.

Step 4 Click **Enable** next to **Status**.

In the displayed **Enable HA** dialog box, configure the network information for the primary and secondary nodes.

Table 13-1 Parameters for enabling the HA function

Parameter	Description
Initial role	The working status of the node. This parameter can be set to **Primary node** or **Secondary node**. You need to configure the bastion host that functions as the primary node first.
HA cluster authcode	The value is automatically generated by the system and is used for mutual verification between the primary and secondary nodes. • When configuring HA parameters for the primary node, record the verification key of the HA group and configure the parameters for the secondary node accordingly. • The value is a string consisting of 8 to 20 digits or letters.
Secondary node IP	When configuring HA parameters for the primary node, enter the IP address of the bastion host that functions as the secondary node.
Primary node IP	When configuring HA parameters for the secondary node, enter the IP address of the bastion host that functions as the primary node.

Parameter	Description
HA Key	When configuring HA parameters on the primary node, enter the key for mutual authentication between the primary and secondary nodes.
Float IP	Enter an unused IP address that is in the same network range as the fixed IP address of the current bastion host. A mask must be added to the end of the floating IP address. A floating IP address is the logical IP address of the two bastion hosts. When you access this IP address, you will automatically log in to one of the bastion hosts, usually the primary node.
Float IP Interface	Select the network interface where the fixed IP address of the bastion host is located.
HA Interface	This interface is the same as that of the floating IP interface.

Step 5 Click **OK** and then restart the system for the configuration to take effect.

----End

Effective Conditions

Restart the primary and secondary nodes for the HA configuration to take effect.

- Before the restart, the **Running Status** is **Standalone**, indicating that the configuration does not take effect.
- After the restart, the HA backup cannot take effect until the primary node discovers the IP address of the secondary node and the **Running Status** of the secondary node changes to **Online**.

Follow-up Operations

To disable the dual-node HA function, click **Disable** next to **Status** in each system.

Save the settings and restart the two bastion hosts. HA is disabled after the restart.

13.4 Port

13.4.1 Configuring the Operation Ports

The operation port is required for accessing managed resources, such as SSH, SFTP, or FTP resources, and logging in to a bastion host through SSH client. Different operation ports may be required for different types of resources. The default operation port is 2222.

If you change the default port, modify the security group configuration of the instance accordingly.

This topic describes how to configure an operation port.

Prerequisites

You have the management permissions for the **System** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Port**.

Step 3 In the **Operation Port** area, click **Edit**.

- Configure port for SSH/SFTP resources. The default port number is 2222.
- The FTP agent service is disabled by default. Enable the FTP agent service. The default port is 2121.

Step 4 Click **OK** and then restart the system for the configuration to take effect.

----End

13.4.2 Configuring the Web Console Port

The web console port is used for logging in to your bastion host through a web browser. The default port is 443.

If you change the default port, modify the port configured in the security group of the instance accordingly.

This topic describes how to configure a web console port.

Prerequisites

You have the management permissions for the **System** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Port**.

Step 3 In the **Web Console** area, click **Edit**.

In the displayed **Web Console** dialog box, configure the port for accessing the web browser. The default port is 443.

Step 4 Click **OK** and then restart the system for the configuration to take effect.

----End

13.4.3 Configuring the SSH Console Port

The SSH console port is required for logging in to your bastion host through an SSH client. The default port is 22.

If you change the default port, modify the port configured in the security group of the instance accordingly.

This topic describes how to configure an SSH console port.

Prerequisites

You have the management permissions for the **System** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Port**.

Step 3 In the **SSH Console** area, click **Edit**.

In the displayed **SSH Console** dialog box, configure the port for accessing the SSH client. The default port is 22.

Step 4 Click **OK** and then restart the system for the configuration to take effect.

----End

13.5 Outgoing

13.5.1 Configuring the Outgoing Mail Server

To send email notifications, such as password change plans and alarm messages, configure an outgoing mail server.

- You can set a private mailbox server or public mailbox server as required and test whether the entered server information is valid.
- Currently, two protocols are supported: SMTP and Exchange (only Exchange 2010).

Prerequisites

You have the management permissions for the **System** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Outgoing**.

Step 3 In the **Email** area, click **Edit**. In the displayed dialog box, configure the email sending method as prompted.

Table 13-2 Parameters for configuring outgoing emails

Parameter	Description
Protocol	The SMTP and Exchange modes are supported. • **SMTP**: SMTP is used as the mail transfer protocol. • **Exchange**: Exchange is used as the mail processing component.
Server	Address of the server where the email address that is being added is located. You can obtain the address from the official website or the unified administrator of the enterprise that the email address belongs to.
Encrypt	Set this parameter when **SMTP** is selected. Select the encryption mode of the original email address. You can select **SSL** or **TLS**. If the email address is not encrypted, select **Null**. You can obtain the encryption mode from the official website or the unified administrator of the enterprise that the email address belongs to.
Port	Set this parameter when **SMTP** is selected. Enter the port opened for the original email address on the server. You can obtain the port number from the official website or the unified administrator of the enterprise that the email address belongs to.
Version	Set this parameter when **Exchange** is selected. Select the Exchange version supported. Currently, only Exchange 2010 is supported.
Domain	Set this parameter when **Exchange** is selected. Enter the domain the original email address belongs to. You can obtain the domain from the official website or the unified administrator of the enterprise that the email address belongs to.
Sender	Enter the account for sending emails. The email account must be valid.
Password of sender	Enter the password of the account for sending emails. The password of the valid email account you enter.
Receiver	Recipient of an email.

After the configuration is complete, click **Send test email** to check whether the email can be sent properly.

Step 4 Click **OK**. You can then view email configuration on the **Outgoing** tab.

----End

13.5.2 Configuring the Outgoing SMS Gateway

SMS messages are mainly used to:

- Receive the mobile phone verification code for login authentication.
- Reset the password.
- Receive alarm messages. For details about the alarm scope, see **Alarm**.

Currently, you can select **Built-in** or **Third-party** SMS gateways. If you select **Third-party**, general **SMS Gateway** and cloud SMS gateway are available.

- If you do not need to push system alarms or send and receive SMS messages to mobile numbers outside the Chinese mainland, you can configure the SMS gateway by referring to **Built-in SMS gateway**.
- If you need to receive system alarms or send and receive SMS messages to mobile numbers outside the Chinese mainland, configure the SMS gateway by referring to **General Third-party SMS Gateway**.
- If you have enabled Huawei Cloud **Message & SMS** (MSGSMS) service, configure the SMS gateway by referring to **Third-Party Message & SMS Service**.

  NOTE

  - MSGSMS cannot push system alarms.
  - If your cloud MSGSMS gateway becomes invalid, the system gateway automatically takes over the job.

Prerequisites

You have the management permissions for the **System** module.

Built-in SMS gateway

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Outgoing**.

Step 3 In the **SMS API** area, click **Edit**.

Step 4 Select **Built-in** and enter a mobile number to verify the connectivity of the built-in SMS gateway.

Step 5 Click **OK**. You can then view SMS gateway configuration on the **Outgoing** tab.

CAUTION

- The built-in SMS gateway cannot push system alarm notifications.
- If you want to receive SMS messages using a mobile number outside the Chinese mainland, enter the mobile phone number on the profile page.

----End

General Third-party SMS Gateway

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Outgoing**.

Step 3 In the **SMS API** area, click **Edit**.

Step 4 Select **Third-party** and then select **SMS Gateway** from the **SMS Conf** drop-down list.

In the displayed parameter list, specify other parameters as prompted.

Step 5 Click **OK**. You can then view SMS gateway configuration on the **Outgoing** tab.

Table 13-3 SMS API parameters

Parameter	Description
Method	Request method. The options are **POST** and **GET**.
URL	URL of SMS API. You can enter a universal URL or a URL containing parameters. Do not enter MD5-encrypted URLs.
HTTP Header	HTTP request header. Use colons (:) to separate the name and value of the HTTP request header. Only HTTP and HTTPS gateways are supported.
API Params	API parameters of the SMS gateway. Replace keywords *$MOBILE* and *$TEXT* with the phone number and SMS content.
Encode	Encode method. You can select **UTF-8**, **Big5**, or **GB18030**.
Mobile	Phone number for receiving the SMS messages. Enter an available phone number and verify the SMS message content.

----End

Third-Party Message & SMS Service

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Outgoing**.

Step 3 In the **SMS API** area, click **Edit**.

Step 4 Select **Third-party** and then configure MSGSMS for SMS gateway.

Select the Chinese SMS gateway or international SMS gateway as required.

Step 5 Click **OK**. You can then view SMS gateway configuration on the **Outgoing** tab.

Table 13-4 Cloud SMS gateway parameters

Parameter	Description
APP_Key	The key of the SMS application.
APP_Secret	The secret of the SMS application.
Application Access URL.	Access URL of the SMS application.
Sender	Channel number before the SMS message. To get this number, apply for your SMS signature first.
Template ID	ID of requested SMS template. **NOTE** The template should be read like this "Your CBH verification code: *XXX* (valid within *XXX* minutes). To ensure account security, do not provide this verification code to anyone." For details, see **Applying for an SMS Template**.
Mobile	Phone number for receiving the SMS messages. Enter an available phone number and verify the SMS message content.

----End

13.5.3 Configuring LTS

You can use Log Tank Service (LTS) to manage operation logs in the bastion host.

Prerequisites

- You have the management permissions for the **System** module.
- You have enabled Log Tank Service (LTS).
- An EIP has been bound to the bastion host.

Constraints

- An EIP must be bound to the bastion host.
- LTS must be enabled before you configure LTS in your bastion host.

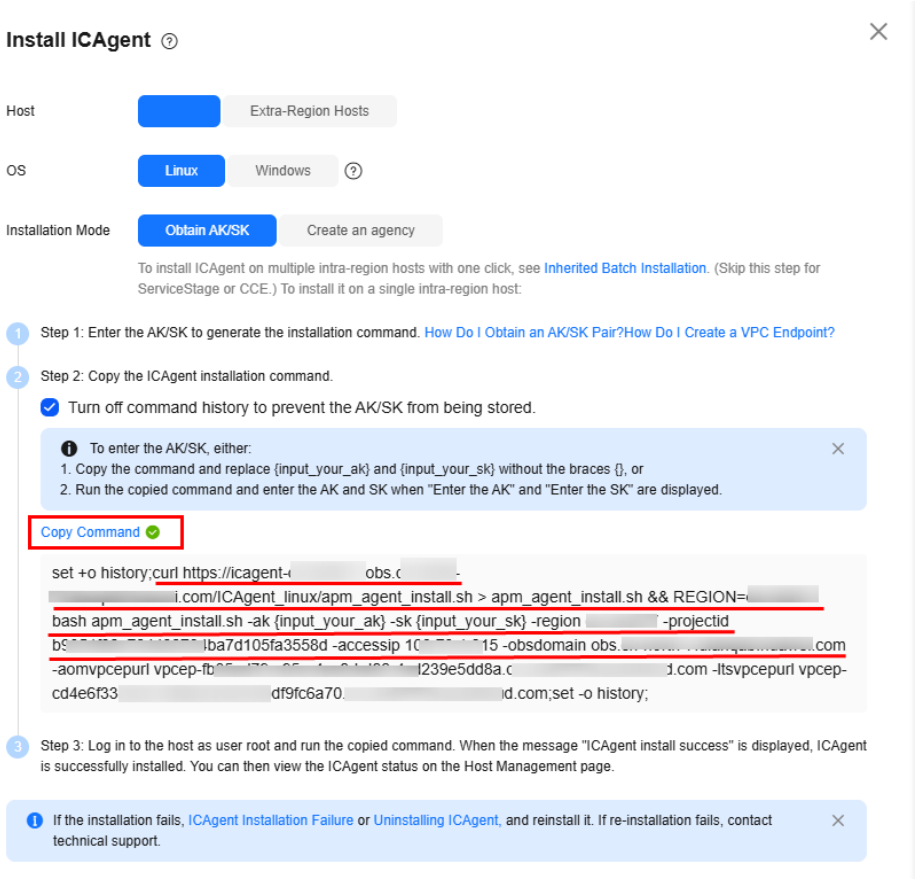
Procedure

Step 1 Obtain the ICAgent installation command from LTS.

For details, see **Installing ICAgent (Intra-Region Hosts)**. You can click **Copy Command** as shown in **Figure 13-4** to copy the installation command. The command structure is as follows:

```
set +o history;curl https://icagent-{region}.{obsdomain}/ICAgent_linux/apm_agent_install.sh > apm_agent_install.sh && REGION=[region] bash apm_agent_install.sh -ak {input_your_ak} -sk {input_your_sk} -region [region] -projectid [projectid] -accessip [accessip] -obsdomain [obsdomain] -aomvpcepurl [aomvpcepurl] -ltsvpcepurl [ltsvpcepurl];set -o history;
```


Figure 13-4 Install ICAgent



Step 2 Process the command obtained in **Step 1** according to the following rules:

- Replace **{input_your_ak}** and **{input_your_sk}** in the command with the actual AK and SK you have.
- Delete the **set +o history;** field from the command start and end lines.
- Delete the **-aomvpcepurl [aomvpcepurl] -ltsvpcepurl [ltsvpcepurl];** field from the latter part of the command.
- If the bastion host is earlier than V3.3.54.0, change **https** to **http**. HTTPS is supported by bastion hosts V3.3.54.0 and later.

The processed command formats are as follows:

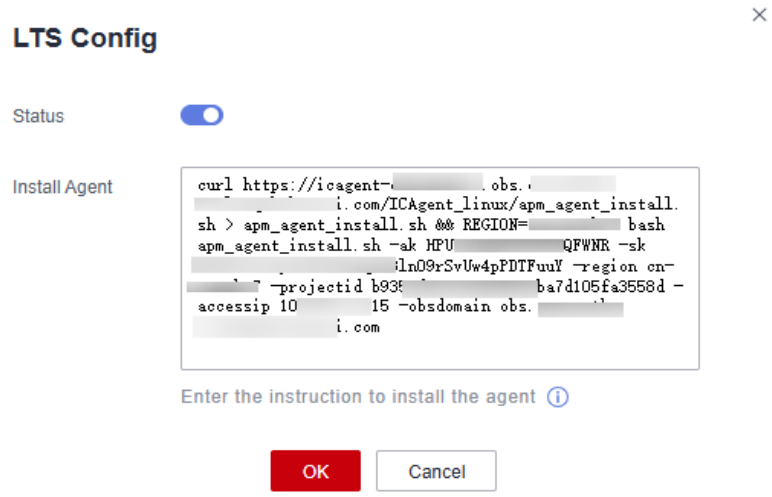
- Versions earlier than V3.3.54.0
  curl **http**://icagent-{region}.{obsdomain}/ICAgent_linux/apm_agent_install.sh > apm_agent_install.sh && REGION=[region] bash apm_agent_install.sh -ak {input_your_ak} -sk {input_your_sk} -region [region] -projectid [projectid] -accessip [accessip] -obsdomain [obsdomain]
- V3.3.54.0 and later
  curl **https**://icagent-{region}.{obsdomain}/ICAgent_linux/apm_agent_install.sh > apm_agent_install.sh && REGION=[region] bash apm_agent_install.sh -ak {input_your_ak} -sk {input_your_sk} -region [region] -projectid [projectid] -accessip [accessip] -obsdomain [obsdomain]

Step 3 Install the ICAgent in the bastion host system.

1. Log in to your bastion host.
2. Choose **System** > **System Config** > **Outgoing**.
3. On the displayed page, locate the **LTS Config** area and click **Edit**.

4. Click to enable the LTS service, and enter the command processed in **Step 2** in the **Install Agent** text box.

   Figure 13-5 Example for V3.3.54.0 and later



5. Click **OK**.

   You can click **Go to the task center** in the displayed dialog box to view the task progress and status in the task center.

----End

13.6 Alarm

13.6.1 Configuring Alarm Channels

You can enable alarm notification on messages of a certain severity level. There are five types of alarm messages, including system messages, service messages, task messages, command alarms, and ticket messages. All messages are classified into high, medium, and low severity levels.

- Alarm notifications can be sent through message center, emails, or SMS message.
- Whether to report an alarm for a message and which alarm channel is used vary depending on severity level of the message. By default:
  - For messages of low severity, no alarms are sent.
  - For messages of medium severity, alarms are sent through the message center.
  - For messages of high severity, alarms are sent through the message center and emails.

This topic describes how to configure the alarm channels.

Constraints

Alarm notifications can be pushed through SMS messages only after you enable the SMS APIs.

Prerequisites

You have the management permissions for the **System** module.

Alarm

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Alarm**.

Figure 13-6 Alarm

Step 3 In the **Alarm Channel** area, click **Edit**.

In the displayed **Alarm Channel** dialog box, set alarm channels for different message types.

Step 4 Click **OK**. You can then view alarm level configuration on the **Alarm** tab.

----End

13.6.2 Configuring Alarm Levels

You can configure the alarm levels, alarm mode, and alarm sending scope.

Prerequisites

You have the management permissions for the **System** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Alarm**.

Figure 13-7 Alarm configuration

Step 3 In the **Alarm Level** area, click **Edit**.

- In the displayed **Alarm Level** dialog box, configure alarm severity levels for different types of messages in each tab.

- The alarm level can be high, medium, or low.

Step 4 Click **OK**. You can then view alarm level configuration on the **Alarm** tab.

----End

13.6.3 Configuring Alarm Sending

This section describes how to configure the alarm sending scope.

Prerequisites

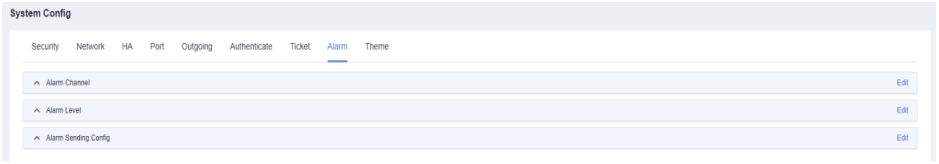
You have the management permissions for the **System** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Alarm**.

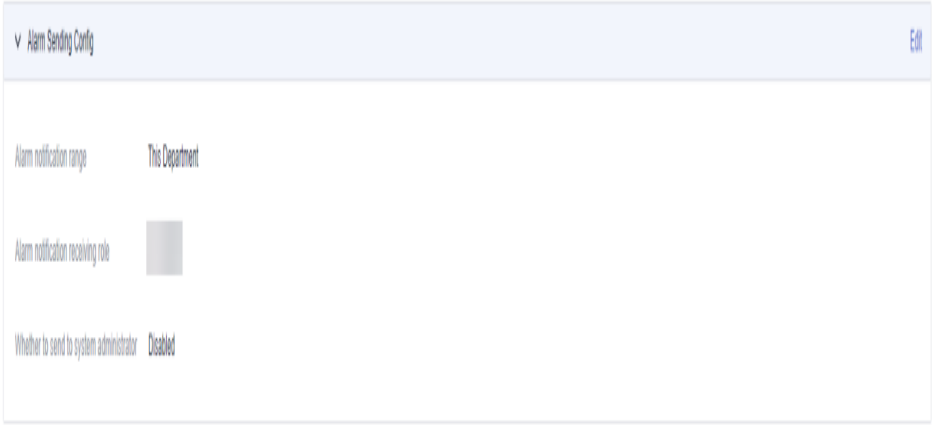
Figure 13-8 Alarm



Step 3 In the **Alarm Sending Configuration** area, click **Edit**.

- Select **This Department** or **The department and all superior departments** to which the alarm notification is sent based on the alarm notification range.
- Alarm notifications can be sent to system administrators. You can determine whether to send alarm notifications as needed.

Figure 13-9 Alarm sending configurations



Step 4 Click **OK**. You can then view alarm sending configuration on the **Alarm** tab.

Figure 13-10 View the alarm sending configurations.

----End

13.7 Theme

13.7.1 Changing the System Theme

On the theme tab, you can customize the page language and system and company logos you want to display for your bastion host.

Prerequisites

You have the management permissions for the **System** module.

Theme

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Config** > **Theme**.

Step 3 Switch over the system language.

1. On the displayed page, in the **Language settings** area, click **Edit**.
2. Select a language. You can select simplified Chinese or English.
3. Click **OK**.

   Then, log out the system, clear cookies, and log in to it again for the specified language to take effect.

   NOTE

   Changing language in the upper right corner on the login page takes effect immediately.

Step 4 Change the system logo.

1. In the **Logo settings** area, click **Edit**.
2. Click logos under **System logo** and **Company logo**, respectively, open the local path, and select a logo you want to use.
3. Click **OK**. Then you can check the system logo and company logo on the **Theme** tab.

----End

14 Basic Instance Information Management

14.1 Instance Dashboard

In a bastion host system, the **Dashboard** page presents the O&M information, system user actions, and host and application operations. The **Dashboard** module consists of a basic statistic area and 17 graph panels, including **Focus Resources**, **Online User**, **Tickets To Approve**, **Host Statistics**, **Application Statistics**, **Alive Sessions**, **Today Spawned Sessions**, **Logon Statistics**, **Operation Statistics**, **Top 5 of Operation User**, **Top 5 of Operation Host**, **System Status**, **System Info**, **Recently Logged Hosts**, **Recently Logged Apps**, **My Hosts**, and **My Apps**.

These panels are visible for you based on your roles. This topic uses the system administrator **admin** as an example to describe how to get information on the **Dashboard** page.

Procedure

Step 1 Log in to your bastion host.

Step 2 In the navigation tree on the left, choose Desktop. The Desktop Dashboard page is displayed.

Step 3 View different panels based on your needs. For details about the functions of each panel, see the following topics.

----End

Focus Resources

Displays statistics about users, hosts, applications, and application servers that can be managed by the current user, and the number of unprocessed alerts.

To view basic statistics, obtain the management permissions for **User**, **Host**, **Application**, and **Application Server** modules and the role management permissions. Otherwise, this panel will be invisible for you. In the basic statistics area, you can view:

- User information

  Displays the number of user accounts that can be managed. You can click this module to go to the user list page and manage the users.

- Hosts

  Displays the number of host resources that can be managed. You can click this module to go to the host list page and manage the host resources.

- **Application**

  Displays the number of application resources that can be managed. You can click this module to go to the application resource list page and manage the application resources.

- **AppServer**

  Displays the number of application servers that can be managed. You can click this module to go to the application server list page and manage the application servers.

- **Alert**

  Displays the number of unprocessed alarms. You can click this module to go to the message center page and manage messages.

Online User

Displays the online users and historical login users you can manage.

To view the statistics of online users, obtain the management permission of the **User** module and the role management permission.

Click a username in the list to go to the user details page. On this page, you can view and manage user information.

Tickets to Approve

Displays the tickets to be approved.

To view the tickets to be approved, obtain the management permission of the **Ticket Approval** module and the role management permission.

Click a ticket in the list to go to the ticket details page. On this page, you can view the ticket information and approve it with just one click.

Host Statistics

Displays the statistics on hosts you can manage.

To view the statistics of hosts, obtain the management permission of the **Host** module and the role management permission.

- Different color represents different host type. Move your cursor over a color block in the circle to view the number of hosts of a certain type.
- Click a color block to go to the corresponding host list page.

Application Statistics

Displays the statistics on application types you can manage.

To view the statistics of application resources, obtain the management permission of the **Application** module and the role management permission.

- Different color represents different host type. Move your cursor over a color block in the circle to view the number of application resources of a certain type.
- Click a color block to go to the corresponding application list page.

Alive Sessions

Displays the statistics on sessions you can manage.

To view the statistics of live sessions, obtain the management permission of the **Live Session** module and the role management permission.

You can click a live session type to go to the corresponding live session list page and monitor the session in real time.

Today Spawned Sessions

Displays the statistics on historical sessions you can manage.

To view the statistics of historical sessions, obtain the management permission of the **History Session** module and the role management permission.

You can click a history session type to go to the corresponding historical session list page and view historical sessions.

Logon Statistics

Displays the trend chart of the number of logins to the system by system users under your management. You can view the trend charts of the current week and month.

To view the statistics on logins, obtain the management permission of the **User** module and the role management permission.

- To view how many times the system is logged in within a certain day, move your cursor over the corresponding date.

Operation Statistics

Displays the trend chart of the number of logins to managed resources by system users under your management. You can view the trend charts of the current week and month.

To view the statistics on logins to resources, obtain the management permission of the **History Session** module and the role management permission.

To view how many times authorized resources are accessed through the bastion host within a certain day, move your cursor over the corresponding date.

Top 5 of Operation User

Displays top 5 system users with most login times to managed resources. You can view the trend charts of the current week and month.

To view the statistics on user login times to the managed resources, obtain the management permission of the **History Session** module and the role management permission.

Click a user in the list to go to the user details page. On this page, you can view and manage user information.

Top 5 of Operation Host

Displays top 5 mostly accessed resources. You can view the trend charts of the current week and month.

To view the statistics on managed resources, obtain the management permission of the **History Session** module and the role management permission.

Click a host resource in the list to go to the details page. On this page, you can view and manage resource information.

System Status

Displays the CPU, memory, and disk usage of the current system.

To view the statistics on system status, obtain the management permission of the **System** module and the role management permission.

System Info

You can view the basic information about the current system and the specifications of the licensed instance version.

To view information about your bastion host, obtain the management permission of the **System** module and the role management permission.

Figure 14-1 System Info

Recently Logged Host

Lists the host resources you have logged in recently.

To view recently logged in hosts, obtain the management permissions for the **Host Operations** module.

- To view details about a host, click the host name in the list to go to the details page.
- To quickly log in to a host resource, click **Login** in the host row.

Recently Logged Application

Lists the application resources you have logged in recently.

To view recently logged in application resources, obtain the management permissions for the **App Operations** module.

- To view details about an application, click the application name in the list to go to the details page.
- To quickly log in to an application resource, click **Login** in the application row.

My Hosts

Displays host resources you are authorized to log in.

To view hosts that you can log in for operations, obtain the management permissions for the **Host Operations** module.

- To view details about a host, click the host name in the list to go to the details page.
- To quickly log in to a host resource, click **Login** in the host row.

My APPs

Displays the application resources that you are authorized to log in to.

To view application resources that you can log in for operations, obtain the management permissions for the **App Operations** module.

- To view details about an application, click the application name in the list to go to the details page.
- To quickly log in to an application resource, click **Login** in the application row.

14.2 Viewing CBH Instance Information

This topic walks you through how to view basic system information.

Prerequisites

You have the management permissions for the **System** module.

Procedure

Step 1 Log in to your bastion host.

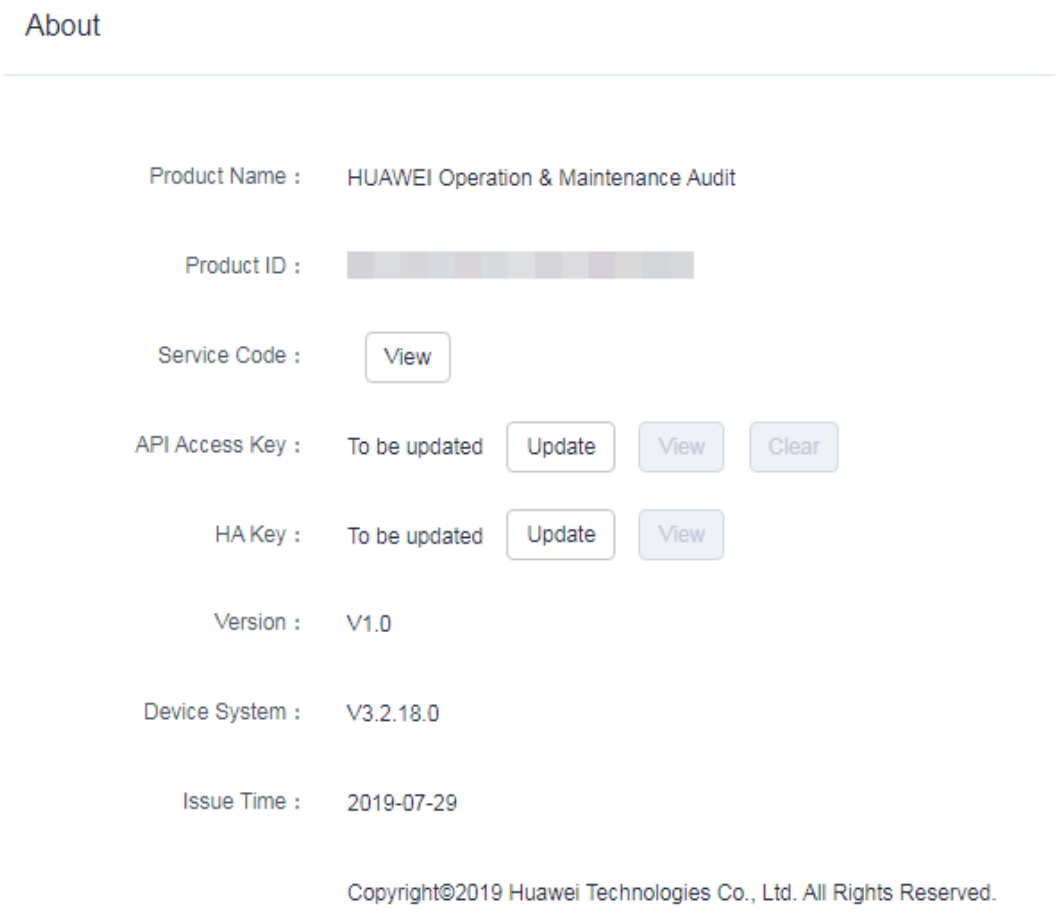
Step 2 On the left navigation pane, choose **System** > **About**.

Step 3 View basic system information.

Table 14-1 System parameters

Parameter	Description
Product Name	Bastion host
Product ID	Unique authentication code of a product
Service Code	This code is used by technical personnel to log in to the system background and manage the background. Click **View** to obtain the code. After obtaining the service code, keep it secure. Do not send it to the public information platforms. **NOTE** When technical personnel use the service code to log in to the system backend, a piece of root account login record will be added to the bastion host login log.
API Access Key	Used for node authentication on the unified management platform • **View**: To view the information, enter the password of the system administrator **admin**, access key secret, and access key ID. • **Update** and **Clear**: To update or clear the API credentials, enter the password of the system administrator **admin**. After the password is updated or cleared, the node managed by the unified management platform becomes invalid.
HA Key	Used to configure the HA When configuring the standby node for HA on the web interface, connect the programs on the standby node to the specified active one, perform the validity check based on configuration information, and then modify the configuration on the active node after the validity check is passed.
Version	Version of the instance.
Device System	Version of the current system software
Issue Time	Release date of the instance.

Figure 14-2 About



----End

14.3 Profile

14.3.1 Viewing Your Profile

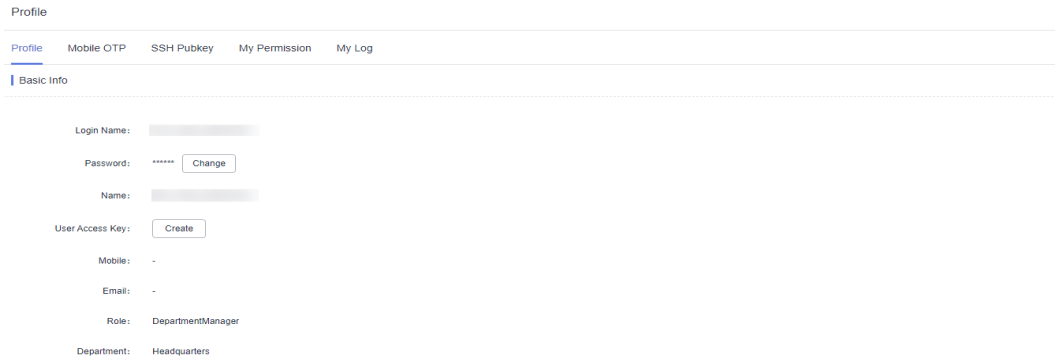
On the **Profile** page, tabs **Profile**, **Mobile OTP**, **SSH Pubkey**, **My Permission**, and **My Log** are available for you to configure basic user information, user permissions, system usage logs, mobile one-time passwords (OTPs), and SSH public keys.

Procedure

Step 1 Log in to your bastion host.

Step 2 On the **Dashboard** page, click the user name in the upper right corner and choose **Profile**.

Figure 14-3 Profile



Step 3 Click each tab to view the corresponding information.

You can view profile, mobile OTP, SSH public key, permission, and log information.

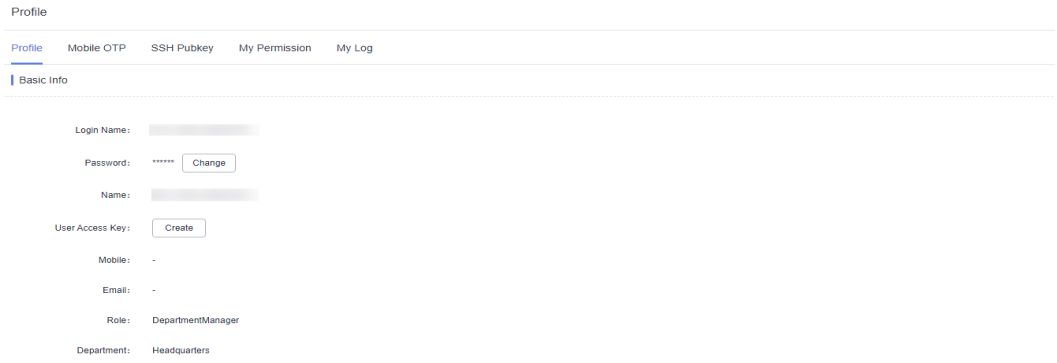
----End

Basic Info

Click the **Profile** tab to view basic user information, including the login name, ciphertext password, name, mobile number, email address, role, and department.

To change the mobile number, email address, and password, see **Editing Basic Information in Profile**.

Figure 14-4 Profile

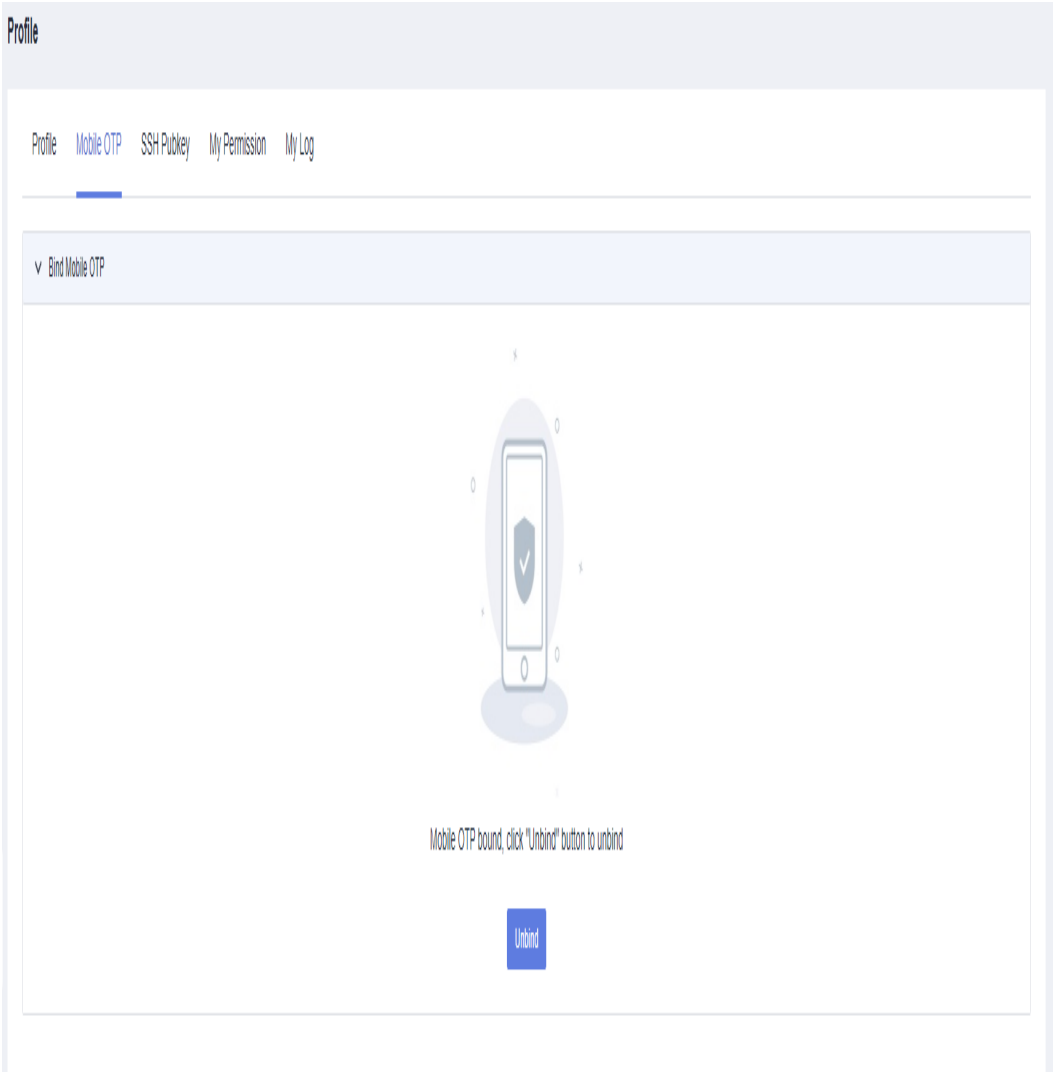


Mobile OTP

To view the mobile phone token bound to your current account, click the **Mobile OTP** tab.

To bind or unbind a mobile phone token, see **Managing Mobile OTPs**.

Figure 14-5 Mobile OTP

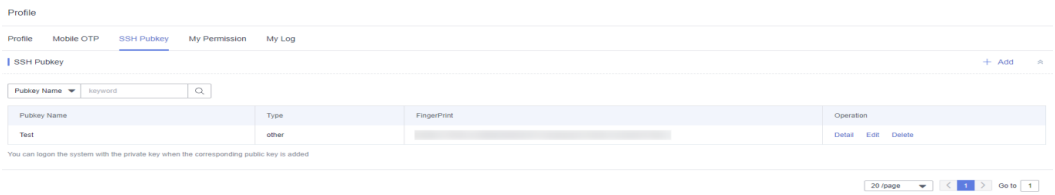


SSH Public Key

To view SSH public keys and their basic information, click the **SSH Pubkey** tab.

To add, modify, and delete a public key, see **Managing SSH Public Keys**.

Figure 14-6 SSH Pubkey

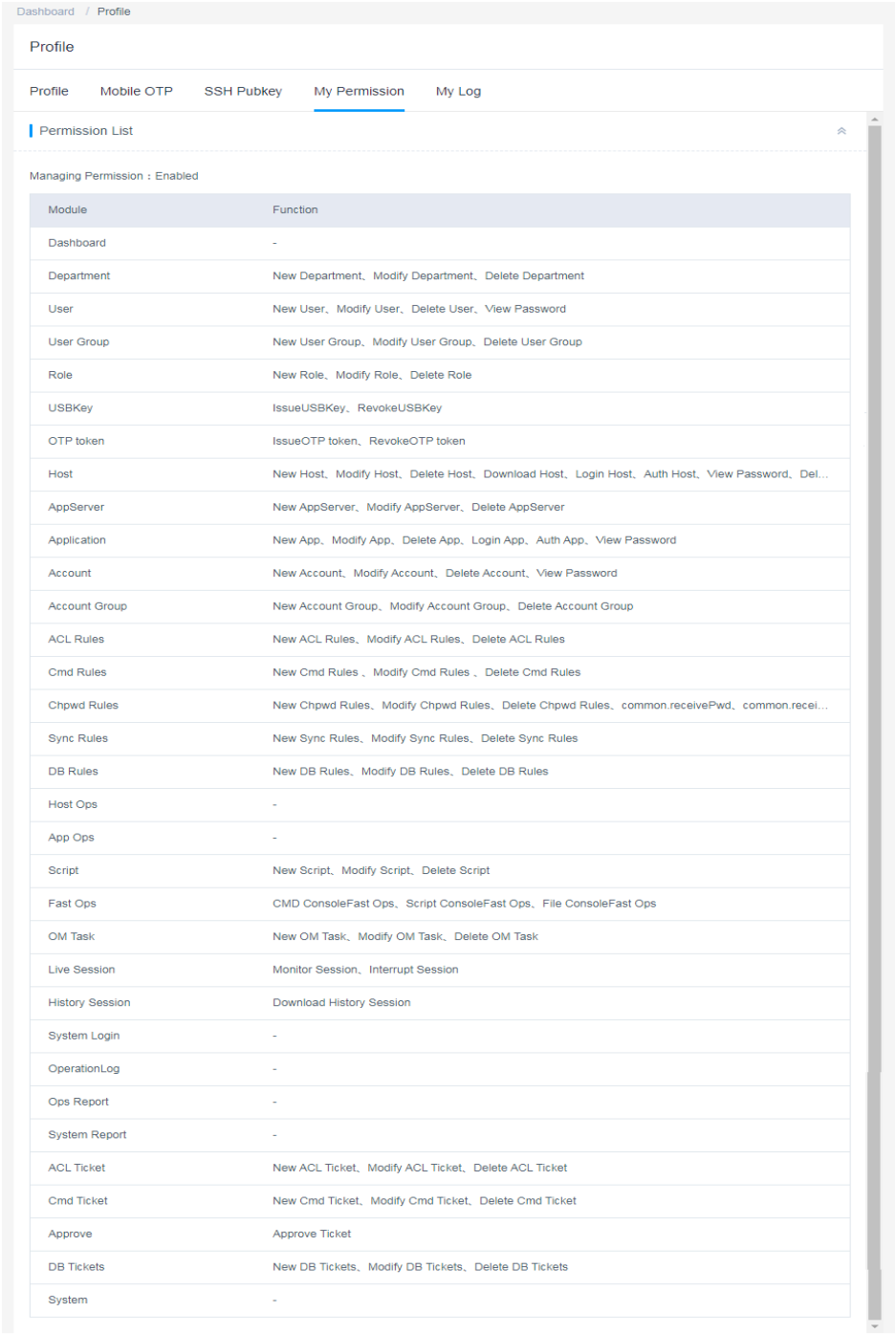


My Permission

To view the personal system permissions and check whether the administrator permission is enabled, click the **My Permission** tab.

Log in to your bastion host as system administrator **admin**.

Figure 14-7 Permissions of user **admin**



My Log

To view logs, click the **My Log** tab. You can then view **System Logon**, **System Operation**, and **Resource Logon** logs.

NOTE

Logs can be managed only by users with the system management permission. Individual users cannot clear their logs. For details, see **Data Maintenance**.

- System logon logs

  A system logon log includes the login time, source IP address of the login user, login method, and login result.

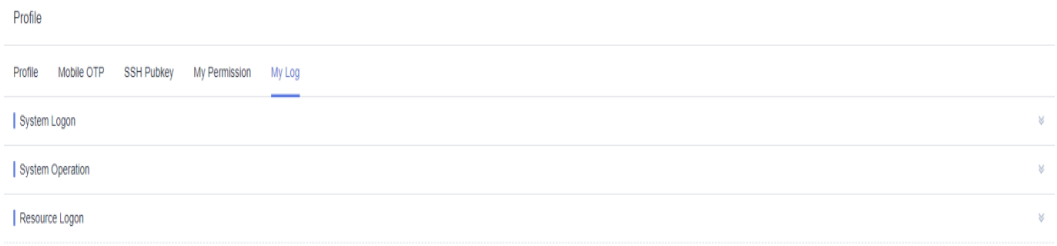
- System operation logs

  A system operation log includes the operation time, source IP address of the operation user, operation module, operation content, and operation result.

- Resource logon logs

  A resource logon log includes the resource name, protocol type, account, source IP address of the login user, login start and end time, and session duration.

Figure 14-8 My Log



14.3.2 Editing Basic Information in Profile

Basic information of a user profile includes the login name, ciphertext password, name, mobile number, email address, role, and department.

- In the Profile area, you can change your password, name, mobile number, and email address.
- The value of **Login Name** must be unique in a bastion host and cannot be changed once it is created.
- Role and department information can be managed only by users with the user management permission and cannot be modified by common individual users. For more details, see **Querying and Modifying User Information**.

This topic describes how to change your password and modify basic information in the **Profile** area.

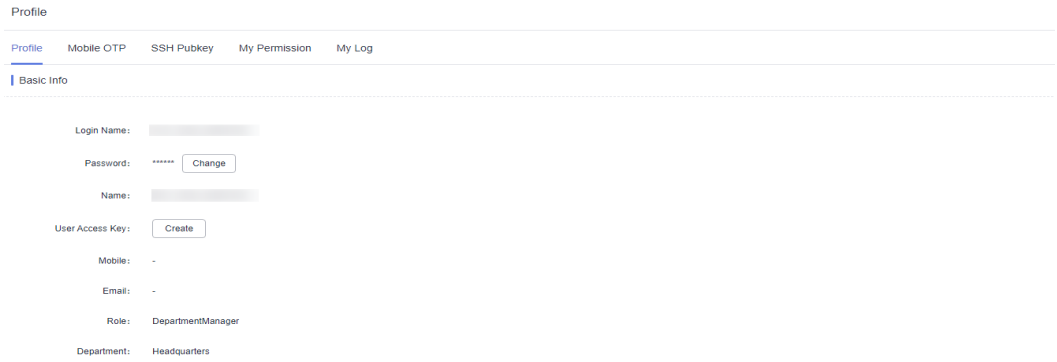
Changing Your Password/Setting a Local Password

If you use an IAM, SAML, or Azure AD account to log in to the bastion host, you need to set a local password for resource O&M. In other scenarios, you can change the user password on the bastion host.

Step 1 Log in to your bastion host.

Step 2 On the **Dashboard** page, click the user name in the upper right corner and choose **Profile**.

Figure 14-9 Profile

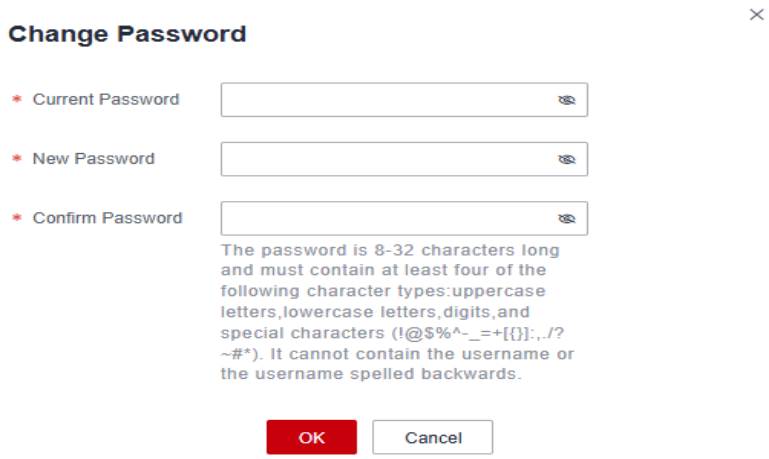


Step 3 On the **Basic Info** tab, click **Change** next to **Password**.

Step 4 Configure parameters depending on the login account.

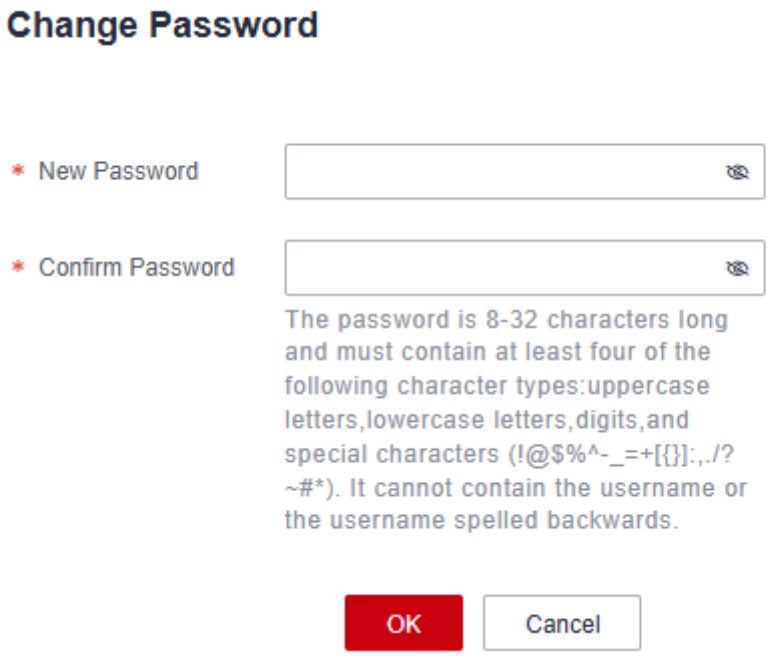
- Setting a local password: Enter a new password.

  Figure 14-10 Setting a local password

- Changing your password: Enter the current password and specify a new password.

Figure 14-11 Changing your password



The new password:

- Can contain 8 to 32 characters.
- Contain at least three of the following types of characters: uppercase letters (A to Z), lowercase letters (a to z), digits (0 to 9), and following special characters: !@$%^-_=+[{}]:,./?~#*
- Cannot contain the username or the username spelled backwards.

Step 5 Check the settings and click **OK**. The profile page is displayed.

Log out of the system. The new password takes effect after you log in to the system again.

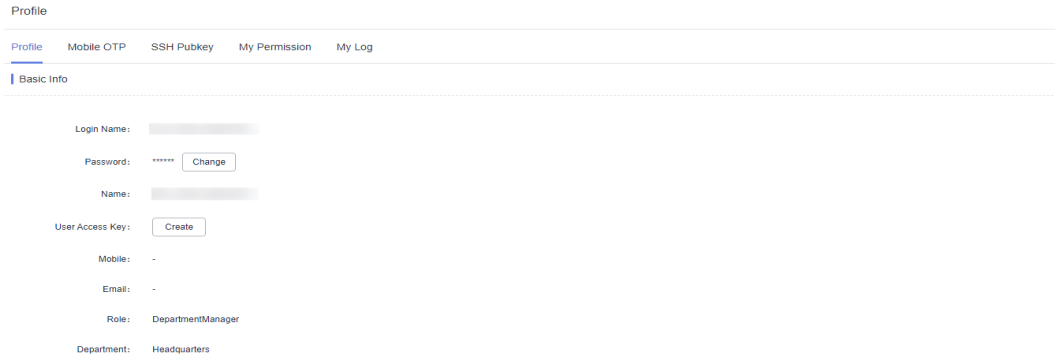
----End

Modifying Basic Information

Step 1 Log in to your bastion host.

Step 2 On the **Dashboard** page, click the user name in the upper right corner and choose **Profile**.

Figure 14-12 Profile



Step 3 Click **Edit** in the **Basic Info** area.

Step 4 In the displayed dialog box, enter the user name, mobile number, or email address into the **Name**, **Mobile**, and **Email** text boxes, respectively.

Step 5 Click **OK**.

The new user name, mobile number, and email address take effect upon the completion of editing.

----End

14.4 Tasks

The task center is the task management center that displays the task receiving status.

- Task types: importing a user, host, cloud server, application, application server, and an account, changing the password of an account, synchronizing users from the AD Domain server, system maintenance (including upgrade and restoration), generating an O&M video, account synchronization, account verification, configuring backup mechanism, automatic O&M, importing dynamical OTPs, and installing Agent.
- The task status can be **Executing**, **Finished**, or **Stop**.

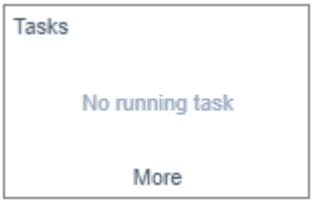
Procedure

Step 1 Log in to your bastion host.

Step 2 Click  in the upper right corner of the page to show the small task center window.

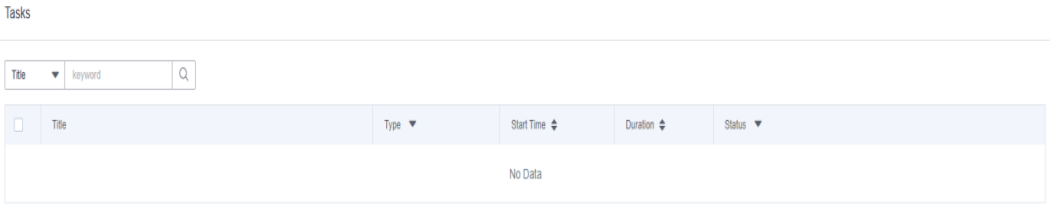
You can view the latest three tasks that are being executed.

Figure 14-13 Small task center window



Step 3 Click **More** to go to the **Tasks** page.

Figure 14-14 Viewing a task list



Step 4 Query tasks.

Enter a keyword in the search box and search for tasks by title.

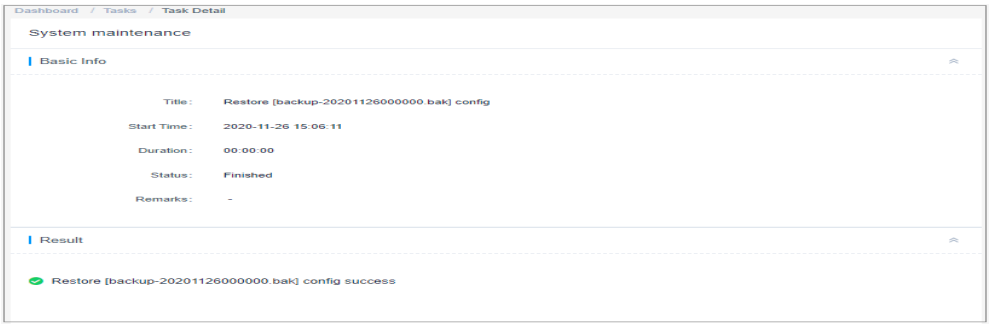
Step 5 View the tasks.

On the **Tasks** page, you can view all running tasks, finished tasks, and stopped tasks.

Step 6 View task details.

1. Click the name of a task.
2. View the basic information and execution result of the task.

Figure 14-15 View task details.



----End

14.5 Messages

14.5.1 Managing Messages

The message center receives system messages. The latest three unread messages are displayed in the small message center window. After a task is complete, you can view messages about all tasks in the task center.

- There are five types of messages, including system messages, service messages, task messages, command alarms, and ticket messages.
- All messages are classified in to three levels by importance, **High**, **Medium**, or **Low**.

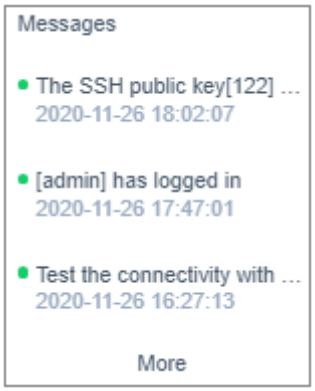
Viewing Messages

Step 1 Log in to your bastion host.

Step 2 Click in the upper right corner to view the latest three unread messages.

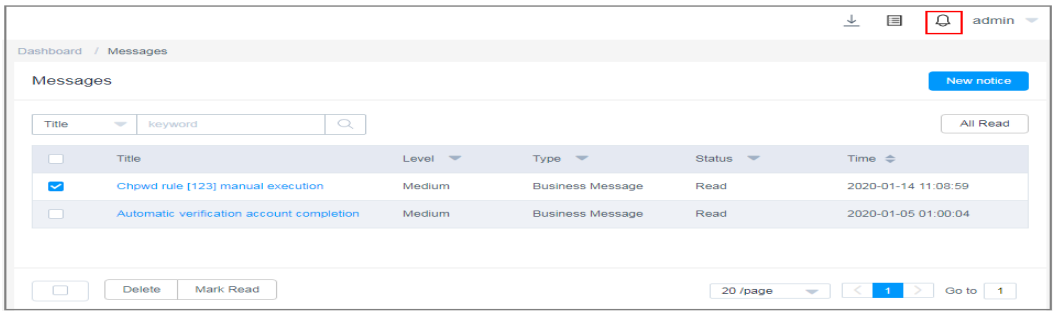
The following figure shows an example.

Figure 14-16 Small message center window



Step 3 Click **More** to go to the **Messages** page.

Figure 14-17 Message list



Step 4 Query messages.

Enter a keyword in the search box and search for messages by message title.

Step 5 View the search results.

Messages are sorted in descending order by time. You can view all read and unread messages.

Step 6 Viewing message details.

1. Click the name of the message to go to the details page.
2. View basic information of the message.

Figure 14-18 Message details

----End

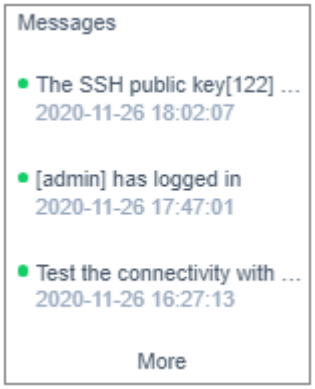
Deleting a Message

Step 1 Log in to your bastion host.

Step 2 Click in the upper right corner to expand the message center window.

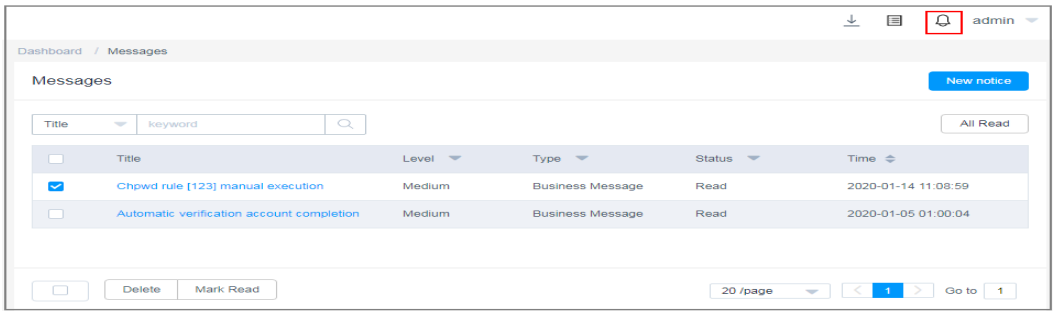
You can view the latest three unread messages.

Figure 14-19 Small message center window



Step 3 Click **More** to go to the **Messages** page.

Figure 14-20 Message list



Step 4 Select one or more messages and click **Delete** in the lower left corner.

Step 5 In the confirmation dialog box, click **OK** to delete the selected messages immediately.

CAUTION

Deleted messages cannot be restored. Exercise caution when performing this operation.

----End

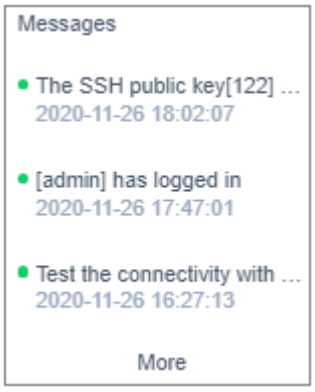
Marking a Message

Step 1 Log in to your bastion host.

Step 2 Click in the upper right corner to expand the message center window.

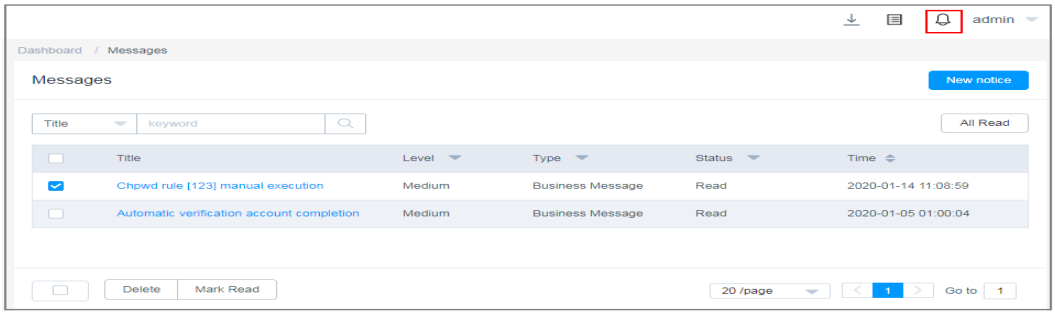
You can view the latest three unread messages.

Figure 14-21 Small message center window



Step 3 Click **More** to go to the **Messages** page.

Figure 14-22 Message list



Step 4 Marks one or more messages.

1. Select one or more messages and click **Mark Read** in the lower left corner.
2. In the displayed confirmation dialog box, click **OK**. The status of the target message changes to **Read**.

Step 5 Mark all messages.

1. Click **All Read**.

2. In the displayed confirmation dialog box, click **OK**. The status of the all messages changes to **Read**.

----End

14.5.2 Creating a System Notice

A system notice is used to notify system users of major changes in the system. After a system notice is created, the notice content is displayed on the top of page for each system user.

As an individual system user, to let the system notice not show again, click **Read** on the left of the notice.

Constraints

- Only system administrator **admin** can create system notices.
- A system notice is intended for all users in the system. It cannot be customized.
- Only one system notice can be shown each time.

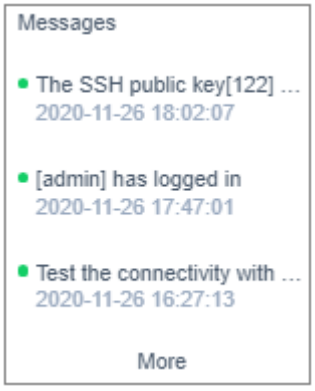
Procedure

Step 1 Log in to your bastion host.

Step 2 Click in the upper right corner to expand the message center window.

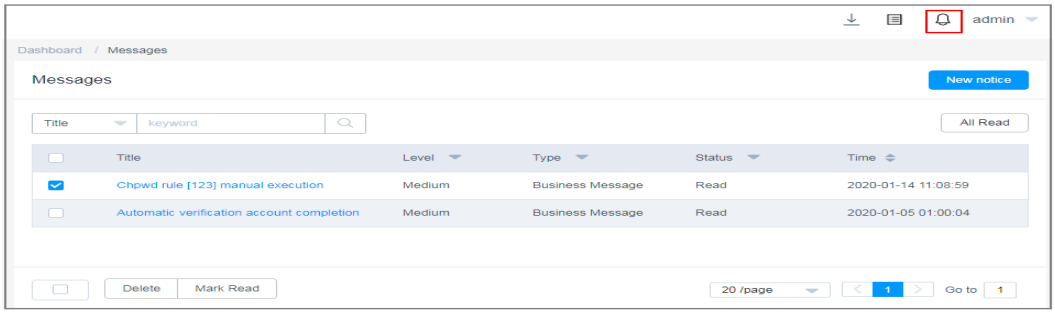
You can view the latest three unread messages.

Figure 14-23 Small message center window



Step 3 Click **More** to go to the **Messages** page.

Figure 14-24 Message list



Step 4 Click **New notice**.

Step 5 In the displayed **New notice** dialog box, enter the content.

Step 6 Click **OK**. You can view the unread system notice.

Figure 14-25 Example notice

----End

14.6 Download Center

The download center provides links for downloading client tools, including tool packages such as the database client. In the download center, you can also view download or export tasks.

The download center is visible only to the current user, and the generated files can be downloaded only by the current user as well.

Procedure

Step 1 Log in to your bastion host.

Step 2 Click  in the upper right corner to go to **Download Center**. Then select the **Common Tools** tab.

Step 3 Click  next to a client tool to go to the third-party tool page and download the tool as required.

Step 4 Click the **Download Tasks** tab to view the download details.

- A maximum of 15 concurrent download tasks are supported. If that number is reached, no more new download tasks can be created until an ongoing task is finished.
- A maximum of two historical session download tasks can be executed concurrently.
- Download tasks cannot be manually deleted. They are automatically deleted after the download deadline arrives.

----End

15 Department Management

15.1 Overview

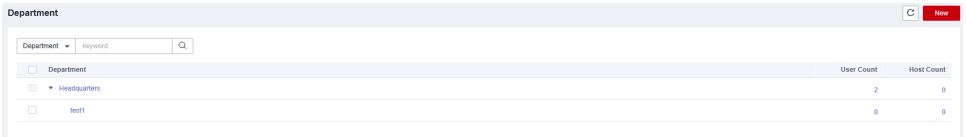
The **Department** module works as an organization that is used to group organization structure and identify users and resources. A CBH system has a default department named **HQ**. The **HQ** department cannot be deleted. Other departments can be created only under the **HQ** department.

Users in lower-level departments cannot view superior department information, including the organization structure, users, host resources, application resources, application publish servers, resource accounts, and policies and operation audit data configured by superior departments.

For users in different departments, they can be managed by administrators of their own department and superior department only.

Only system administrator **admin** or users with the management permissions for the **Department** module can manage the department organization structure, including creating, editing, deleting, and querying a department, querying users in a certain department, and querying resources in a certain department.

Figure 15-1 Department management



15.2 Creating a Department

The default department **HQ** is the top department in a bastion host. You can create departments only under **HQ**.

Prerequisites

You have the operation permissions for the **Department** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 In the navigation pane on the left, select **Department**.

Step 3 On the displayed page, click **New** in the upper right corner of the page to open the **New Department** dialog box.

Step 4 Select a superior department for **Superior Dept**, enter a name of the department to be created in the **Department** field, and enter the description in the **Remarks** area if necessary.

NOTE

- The department name defined in a bastion host must be unique.
- The superior department can be selected only from the existing department directory tree.

Step 5 Click **OK**. You can then view the new department on the department management page.

----End

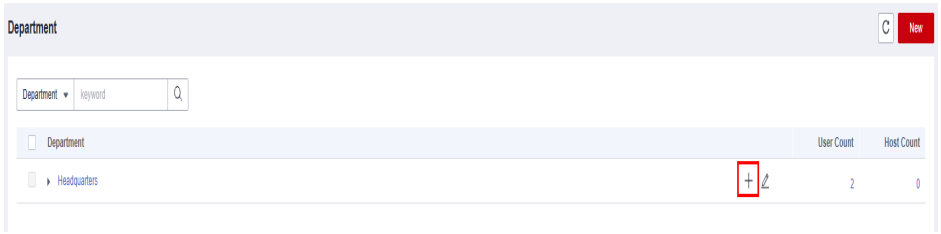
How to Create a Department Quickly

Step 1 Log in to your bastion host.

Step 2 Select **Department** in the navigation pane on the left.

Step 3 Move the cursor to the superior department column and click + to quickly create a lower-level department.

Figure 15-2 Quickly creating a lower-level department



Step 4 Change the department name.

----End

15.3 Deleting a Department

The default department **HQ** is the top department in a bastion host and cannot be deleted. When a superior department is deleted, all its lower-level departments are deleted automatically.

Prerequisites

You have the operation permissions for the **Department** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Select **Department** in the navigation pane on the left.

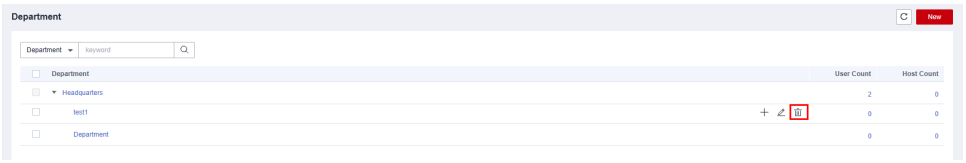
Step 3 Delete a department.

Move the cursor over the row where the department to be deleted locates to let the operation icons appear. Click then the deletion icon to delete the department.

NOTE

Deleting a department will delete all its lower-level departments, users, and resources under the department and all its lower-level departments.

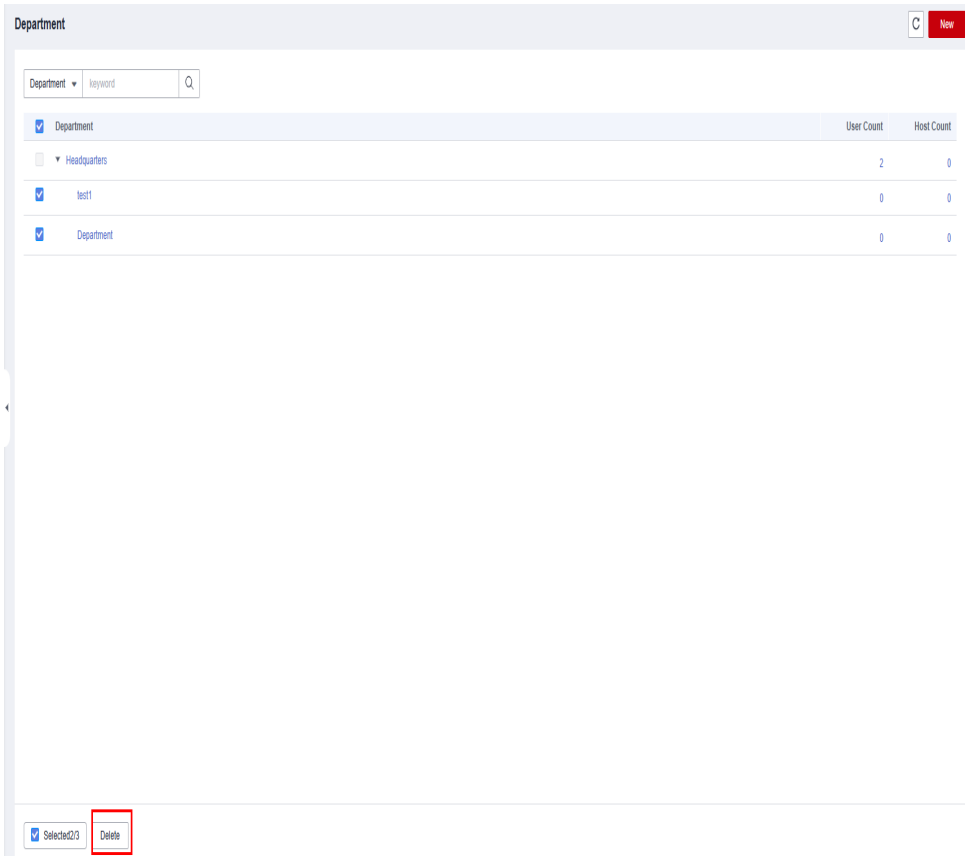
Figure 15-3 Deleting a department



Step 4 Delete departments in batches.

Select the ones you want and click **Delete** at the bottom of the list to delete all selected departments together.

Figure 15-4 Batch deleting departments



----End

15.4 Viewing and Editing Department Information

You can change department name and superior department a department belongs to.

After a department is moved from one superior department to another, resources and users in the department are automatically moved accordingly.

Prerequisites

You have the operation permissions for the **Department** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Select **Department** in the navigation pane on the left.

Step 3 Click the name of the department to be edited.

Step 4 In the **Basic Info** area, view the detailed information about the department.

Click **Edit** and edit basic information.

----End

15.5 Querying Configurations of a Department

A bastion host can collect statistics on the number of users and hosts under each department. You can query the user and host asset configurations of a department on the department management page. Application resources and application publish servers are not included in the statistics.

Prerequisites

You have the operation permissions for the **Department** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Select **Department** in the navigation pane on the left.

Step 3 Enter a department name in the search box to query the superior department tree to which the department belongs.

Step 4 View the number of users or hosts in the **User Count** or **Host Count** column in each department in the department tree.

Step 5 Click a specific number to go to the **User** or **Host** page, respectively, and then view the department configuration.

----End

16 Maintenance Management

16.1 Data Maintenance

16.1.1 Viewing System Memory

The storage space of a bastion host consists of system partitions and data partitions. If the idle space of the data partition is insufficient, delete historical system data.

Prerequisites

You have the management permissions for the **System** module.

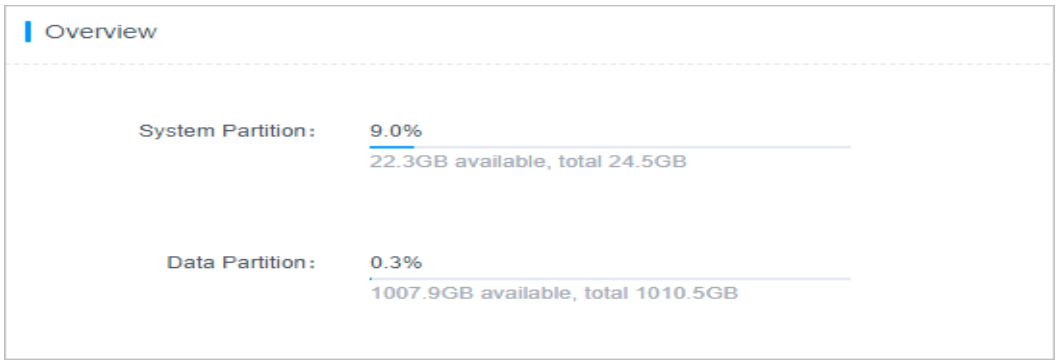
Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **Data Maintain** > **Storage Mgmt**.

Step 3 In the **Overview** area, view the space usage of the system partition and data partition.

Figure 16-1 Storage space overview



----End

Configuring a Download Task

Step 1 On the storage configuration page, click **Edit** on the right of **Download Task**.

Step 2 In the dialog box displayed, configure the size of a single download task.

NOTE

The default value is 4. After the configuration, files larger than the value cannot be downloaded from the bastion host. The value ranges from 1 to 1024.

----End

16.1.2 Configuring the Netdisk Capacity

The **Netdisk** is used to temporarily store files from managed hosts or the local server for the purpose of file transfer. The **Netdisk** is a personal net disk in a bastion host.

This topic describes how to set the net disk capacity.

Constraints

- The maximum available space of the net disk is the available space of the system data disk.
- After **Personal Netdisk** is set, the bastion host allocates the same personal net disk capacity for each user in the system.
- Files on the **Netdisk** can only be manually deleted. Periodic clearance of personal net disk space is not supported.

Prerequisites

You have the management permissions for the **System** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **Data Maintain** > **Storage Mgmt** to go to the storage configuration page.

Step 3 In the **Netdisk** area, click **Edit**. In the displayed dialog box, set the disk size.

Table 16-1 Netdisk parameters

Parameter	Description
Personal Netdisk	A private disk exclusively used by the current user • The default value is **100 MB**. • To use the personal net disk unlimitedly when the system data disk capacity is allowed, set **Personal Netdisk** to **0**.

Parameter	Description
Total Netdisk	Total netdisk capacity. • The default value is **5120 MB**. • To use all space of the total net disk unlimitedly when the system data disk capacity is allowed, set **Total Netdisk** to **0**.

Step 4 Click **OK**. You can then view capacity of the configured **Personal Netdisk** and **Total Netdisk** on the **Storage Mgmt** tab.

Step 5 Click **Detail** and view details about the net disk.

Step 6 In the row containing the net disk, click **Delete NetDisk Data** in the **Operation** column.

NOTE

You can also select all net disks from which you want to delete data and click **Delete NetDisk Data** to clear the disks together.

----End

16.1.3 Deleting System Data

If the system data disk usage is higher than 95%, the system may become unavailable. To ensure that the system data disk can be used properly, you can configure automatic or manual deletion of system data by referring to this section.

The system data that is automatically or manually deleted is mainly the files temporarily stored on the data disk, including large historical session video files, local backup log files, and local backup system configuration files.

NOTICE

Deleted system data cannot be restored. Exercise caution when performing this operation.

Constraints

Data of a specific day cannot be deleted through **Manual Deletion**. You can delete the data before the date you select.

Prerequisites

You have the management permissions for the **System** module.

Configuring Auto Deletion

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **Data Maintain** > **Storage Mgmt** to go to the storage configuration page.

Step 3 In the **Auto Deletion** area, click **Edit**. In the displayed dialog box, set related parameters.

Table 16-2 Configuring Auto Deletion

Parameter	Description
Auto Deletion	Status of auto deletion (default: ). •  : Auto deletion is enabled. The system automatically starts the data deletion job when the data storage duration and data disk usage exceeds the limit. • : Auto deletion is disabled.
Data life (days)	Data storage duration. The data is automatically deleted when its storage duration exceeds the specified value. • Default value: **180** days. • Value range: **1** to **10000**, in days.
Overwrite when full	If you enable this, data on the disk will be automatically deleted once the data disk usage exceeds 90%. This function is recommended. Whether to enable this function (default: ). • : This function is disabled •  : This function is enabled. • Auto deletion policies: – The system checks the data disk usage every 30 minutes. When the usage is lower than 90%, the auto deletion stops. – By default, the system deletes data generated 180 days earlier than the current day. – If the data disk usage is still higher than 90%, the rest data is deleted day by day backwards from the day before the current day until the space usage is lower than 90% – Data of the current day cannot be automatically deleted.
Download Task Validity Time	The validity period for the task. When the validity period reaches its end, the files in unfinished tasks are automatically deleted. The default value is 60. The value ranges from 1 to 10,000.
Delete Content	The options are as follows: • System Log • Session Log

Step 4 Click **OK**. You can check the configured automatic deletion information on the storage configuration management page.

----End

Manual Deletion

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **Data Maintain** > **Storage Mgmt** to go to the storage configuration page.

Step 3 In the **Manual Deletion** area, select a date.

NOTE

Data generated over the last 30 days cannot be deleted. So only dates from 30 days earlier can be selected.

Step 4 Click **Delete**. Data generated before the selected date is deleted.

----End

16.1.4 Creating a Local Data Backup

To enhance data disaster recovery management and improve audit data security and system scalability, you can back up configuration logs for your bastion host.

This topic walks you through how to create a backup locally.

Constraints

- Supported logs: System login logs, resource login logs, command operation logs, file operation logs, and two-person authorization logs
- After a local backup is created, a log file is generated on the system data disk.

Prerequisites

You have the management permissions for the **System** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **Data Maintain** > **Log Backup**.

Step 3 In the **Data Backup Locally** area, click **Add**. In the displayed dialog box, configure backup content and date range.

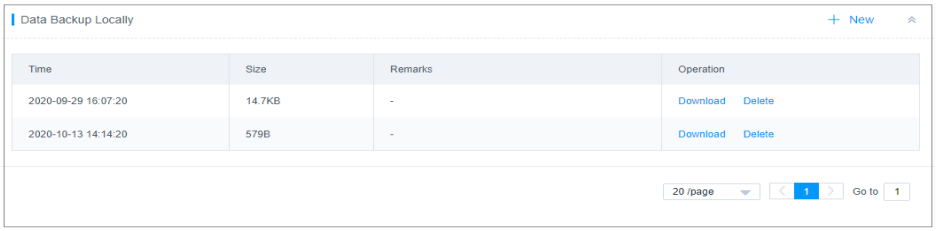
Table 16-3 Creating a Local Backup

Parameter	Description
Log content	Type of logs to be backed up • The options are **System Login**, **Resource Logon**, **Command log**, **File log**, and **Double auth log**. • Select at least one log type.
Date Range	Date range to generate logs to be backed up • Select at least one day.

Parameter	Description
Remarks	Brief description. • A maximum of 128 characters can be entered.

Step 4 Click **OK**. You can then view the backup information on the **Log Backup** tab.

Figure 16-2 Data Backup Locally



----End

Follow-up Operations

- To download a local backup to your local server, click **Download** in the **Operation** column of the corresponding row.
- To delete a local backup, click **Delete** in the **Operation** column of the corresponding row.

16.1.5 Configuring the Syslog Server for Remote Backup

To enhance data disaster recovery management and improve audit data security and system scalability, you can back up configuration logs for your bastion host.

Constraints

- After remote backup is enabled, the system backs up system data in real time by default.
- Logs are automatically backed up on a daily basis and uploaded to the corresponding folder on the Syslog server.
- Supported logs: System login logs, resource login logs, command operation logs, file operation logs, and two-person authorization logs

Prerequisites

You have the management permissions for the **System** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **Data Maintain** > **Log Backup**.

Step 3 In the **Backup to the syslog server** area, click **Edit**. In the displayed dialog box, complete required parameters.

Table 16-4 Parameters for configuring the Syslog server

Parameter	Description
Status	Whether to back up data to the Syslog server (default:). •  : This function is enabled. The system automatically starts backup at 00:00 every day. • : This function is disabled.
Sender Identifier	Identifier for connecting your bastion host to the Syslog server. The identifier is used to identify the bastion host from which the logs are received on the Syslog server.
Server IP	IP address of the Syslog server.
Port	Port number of the Syslog server.
Protocol	Protocol of the Syslog server. • The options are **TCP** or **UDP**. • If **TCP** is selected, click **Test connectivity** to check whether the server is reachable.
Backup Content	Select at least one type of logs to be backed up. • System login logs: record all logins to the instance. • Resource login logs: record all operations for resources managed by the current instance. • Command operation logs: record all commands executed in the current instance. • File operation logs: record all file operations, including uploading and downloading files, in the instance. • Two-person authorization logs: record all two-person authorization operations in the instance.

Step 4 Click **OK**. You can then view the backup information on the **Log Backup** tab.

After the configuration is complete, the system backs up the data of the previous day at 00:00 every day and uploads the data to the remote Syslog server.

----End

Follow-up Operations

- To disable the Syslog server backup, click **Edit**. In the displayed dialog box, set **Status** to **Disabled**.
- To view or download logs backed up to the Syslog server, log in to the Syslog server.

16.1.6 Configuring an FTP/SFTP Server for Remote Log Backup

To enhance data disaster recovery management and improve audit data security and system scalability, you can back up configuration logs for your bastion host.

This topic walks you through how to configure the FTP or SFTP server for remote log backup.

Constraints

- After remote backup is enabled, the system backs up the system data of the previous day at 00:00 every day by default.
- Logs are automatically backed up on a daily basis and uploaded to the corresponding folder on the FTP or SFTP server.
- Logs of the same day cannot be backed up repeatedly in the same server path.
- System configuration and session playback logs can be remotely backed up to the FTP or SFTP server.

Prerequisites

You have the management permissions for the **System** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **Data Maintain** > **Log Backup**.

Step 3 In the **Backup to the FTP/SFTP server** area, click **Edit**. In the displayed dialog box, complete required parameters.

Table 16-5 Parameters for configuring the FTP or SFTP server

Parameter	Description
Status	Whether to back up data to the FTP or SFTP server (default:). •  : Remotely backing up logs to an FTP or SFTP server is enabled. The system automatically starts backup at 00:00 every day. • : Remotely backing up logs to an FTP or SFTP server is disabled. **NOTE** After this function is enabled, the system backs up the data of the previous day at 00:30 every day. Password logs are backed up in real time. The system will send backup to the remote FTP/SFTP server.
Protocol	Protocol over which logs are transferred for backing up • The options are **FTP** and **SFTP**.
Server IP	IP address of the FTP or SFTP server.
Port	Port number of the FTP or SFTP server.
Username	Username on the FTP or SFTP server to test whether the FTP or SFTP server is reachable.

Parameter	Description
Password	Password of the username on the FTP or SFTP server to test whether the FTP or SFTP server is reachable.
Storage Path	Path where the logs are stored. • The path must start with a period (.). For example, if the path is **./test/abc**, the absolute path is **/home/*username*/test/abc**. • If this parameter is left empty, the backup content is stored in the home directory of the FTP or SFTP server user, for example, absolute path /home/*username*.
Test connectivity	Tests whether the configured FTP or SFTP server is reachable. • It checks only the network status between the bastion host and the FTP or SFTP server. The user account of the server is not verified.
Backup Content	Select at least one type of logs to be backed up. • System configuration • Session recording playback log • System logon log • Resource logon log • Command operation log • File operation log • Two-person authorization log

Step 4 Click **OK**. You can then view the backup information on the **Log Backup** tab.

After the configuration is complete, the system backs up the data of the previous day at 00:00 every day and uploads the data to the remote FTP or SFTP server.

----End

Follow-up Operations

- To back up the logs of a certain day immediately, start the remote backup immediately.

  In the **Backup to FTP/SFTP server** area, select the date of the logs to be backed up and click **Backup**.
- To disable the FTP or SFTP server backup, click **Edit**. In the displayed dialog box, set **Status** to **Disabled**.
- To view or download logs backed up to the FTP or SFTP server, log in to the FTP or SFTP server.

16.1.7 Configuring OBS Buckets for Remote Log Backup

To enhance data disaster recovery management and improve audit data security and system scalability, you can back up configuration logs for your bastion host.

This topic walks you through how to set OBS buckets to remotely back up logs.

Constraints

- After remote backup is enabled, the system backs up the system data of the previous day at 00:00 every day by default.
- Logs are automatically backed up on a daily basis and uploaded to the corresponding folder in the OBS bucket.
- Logs of the same day cannot be backed up repeatedly in the same server path.
- System configuration and session playback logs can be remotely backed up to OBS buckets.

Prerequisites

- You have the management permissions for the **System** module.
- You have created an OBS bucket, and the network between the OBS bucket and your bastion host is normal.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **Data Maintain** > **Log Backup**.

Step 3 In the **Remote Backup To OBS** area, click **Edit**. In the displayed dialog box, set bucket parameters.

Table 16-6 Parameters for remote backup to OBS

Parameter	Description
Status	Whether to back up logs to an OBS bucket (default:). • : Backing up logs to OBS buckets is enabled. The system automatically starts backup at 00:00 every day. • : Backing up logs to OBS buckets is disabled.
Access Key ID	Specifies the access key ID, which is used to verify the identity of the request sender for accessing the OBS bucket. An access key ID is a unique identifier associated with a secret access key and is used together with the secret access key to sign requests cryptographically. Obtain **Access Keys**.
Secret Access Key	Specifies the secret access key used together with the access key ID. A secret access key works as a cryptographic signature to identify the sender of a request and prevent the request from being tampered with.

Parameter	Description
EndPoint	Region where the bucket is located. **View bucket information** to obtain the endpoint of OBS in the region.
bucket	Bucket name.
Storage Path	Bucket path or bucket folder path. The path cannot contain three or more consecutive slashes (/). If the OBS bucket does not have the corresponding path, a folder is automatically generated in the bucket. Example: cbh/bastion/.../...
Test connectivity	Tests whether the network between your bastion host and the configured OBS bucket is reachable. The connectivity test checks only the network status between the bastion host and the OBS bucket.
Backup Content	Select at least one type of logs to be backed up. • System configuration • Session recording playback log • System logon log • Resource logon log • Command operation log • File operation log • Two-person authorization log
Backup file encryption password	Enter the encryption password of the backup file. **NOTE** The password can contain 8 to 32 characters and must contain at least three types of the following characters: uppercase letters, lowercase letters, digits, and special characters !@$%^-_=+[{}]:,./?~#*.

Step 4 Click **OK**. You can then view the backup information on the **Log Backup** tab.

After the configuration is complete, the system backs up the data of the previous day at 00:00 every day and uploads the data to the OBS bucket.

----End

Follow-up Operations

- To back up the logs of a certain day immediately, start the remote backup immediately.

  In the **Remote Backup To OBS** area, select the date of the logs to be backed up and click **Backup**.
- To disable the remote OBS bucket backup, click **Edit**. In the displayed dialog box, set **Status** to **Disabled**.

- To view or download logs backed up to the OBS bucket, **log in to the OBS console** and perform operations in the corresponding bucket folder.

16.2 System Maintenance

16.2.1 Viewing System Status

To keep your bastion host stay healthy, you can keep an eye on the CPU, memory, disk, and network bandwidth usage in a timely manner.

This topic describes how to check the system CPU, disk, and network bandwidth usage.

Prerequisites

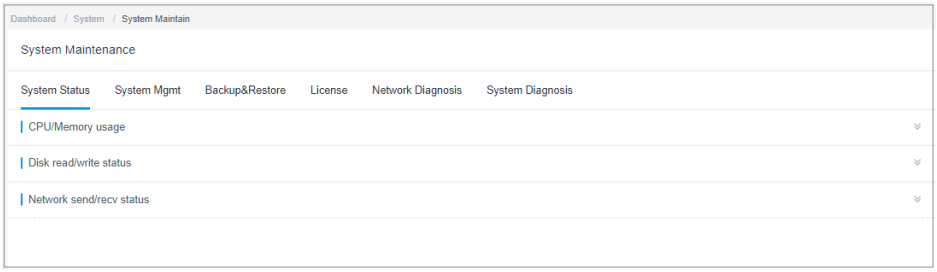
You have the management permissions for the **System** module.

Viewing System CPU and Memory Usage

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Maintain** > **System Status**.

Figure 16-3 Viewing System Status



Step 3 Expand the **CPU/Memory usage** area and view the CPU or memory usage.

- View CPU or memory usage statistics over the past 5 minutes, 15 minutes, or 1 hour.
- To view CPU or memory usage at a certain moment, move your cursor over the time point.

----End

View Disk Read/write Status

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Maintain** > **System Status**.

Step 3 Expand the **Disk read/write status** area and view the read/write usage of the system disk.

- View disk read/write statistics over the past 5 minutes, 15 minutes, or 1 hour.

- To view disk read/write speed at a certain moment, move your cursor over the time point.

----End

Viewing Network Sending and Receiving Status

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Maintain** > **System Status**.

Step 3 Expand the **Network send/recv status** area and view the system network receiving or sending status.

- View network packet receiving and sending speed over the past 5 minutes, 15 minutes, 1 hour, or 24 hours.
- View the sending and receiving status on the **eth0** and **eth1** network interfaces.
- To view network sending or receiving speed at a certain moment, move your cursor over the time point.

Figure 16-4 Network sending and receiving status

----End

16.2.2 System Mgmt

This topic describes how to update the system IP address, system time, instance version, as well as how to restart, shut down, and restore the system, and how to manage the basic system information and status.

Prerequisites

You have the management permissions for the **System** module.

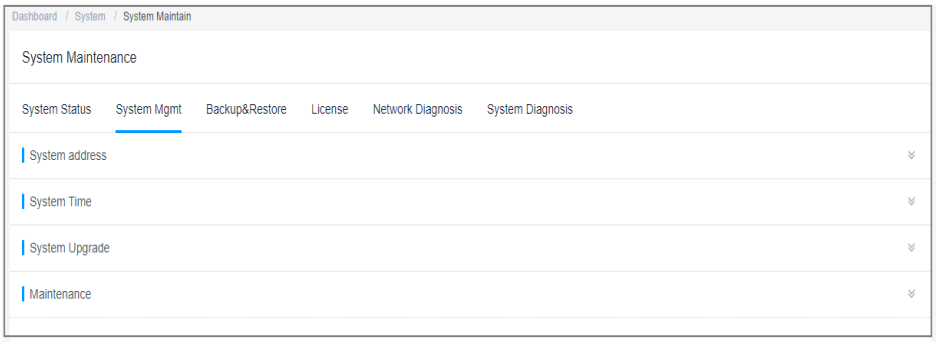
Managing System Addresses

If the system is behind a NAT device or firewall, set this parameter to the external NAT address. Otherwise, applications such as FTP cannot be connected.

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Maintain** > **System Mgmt**.

Figure 16-5 System Mgmt

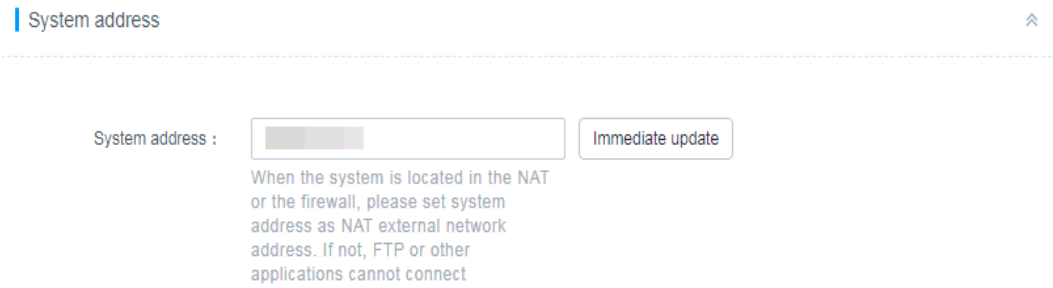


Step 3 Expand the **System address** area.

Step 4 Update the system IP address.

- After the EIP bound to the mapped bastion host is changed, update the system IP address accordingly.
- The system IP address must be the NAT external network address. Otherwise, application resources such as FTP cannot be connected.

Figure 16-6 System address



----End

Managing System Time

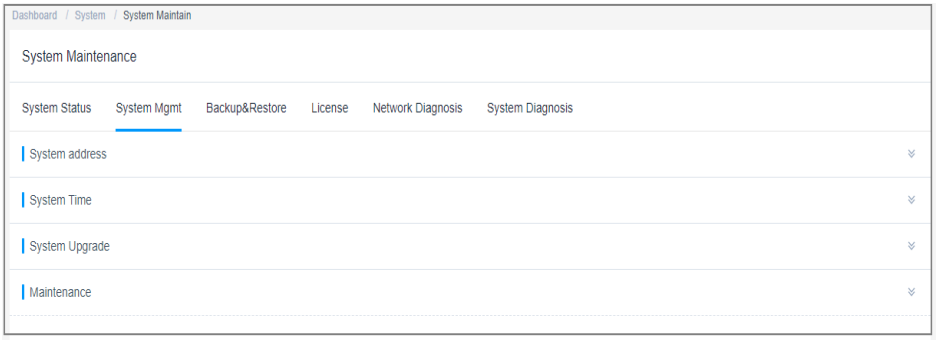
NOTE

Incorrect system time will make policies and tickets ineffective and causes failures in the authentication of the mobile OTP and dynamic OTP token when they bound to the bastion host.

Step 1 Log in to your bastion host.

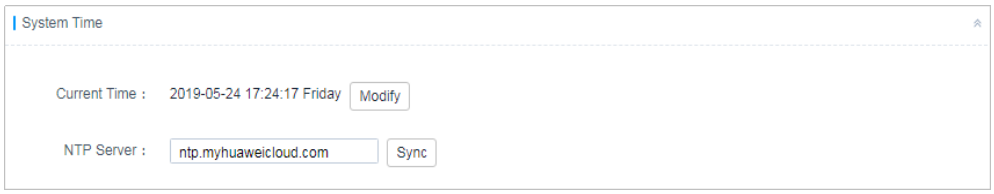
Step 2 Choose **System** > **System Maintain** > **System Mgmt**.

Figure 16-7 System Mgmt



Step 3 Expand the **System Time** area.

Figure 16-8 System Time



Step 4 Update the system time manually.

1. Click **Modify** next to the **Current Time**.
2. In the displayed **Edit System Time** dialog box, specify the date and time.
3. Click **OK**. You can check the update on the system management page displayed.

Step 5 Synchronize time from the NTP server.

The current system time is synchronized by default.

1. Select the built-in NTP server or enter the IP address of the NTP server.
2. Click **Sync**.

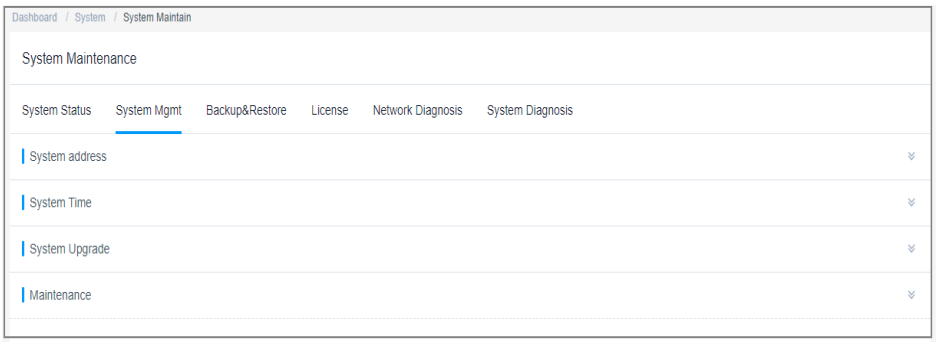
----End

Managing System Version

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Maintain** > **System Mgmt**.

Figure 16-9 System Mgmt



Step 3 Expand the **System Upgrade** area.

Figure 16-10 System Upgrade

Step 4 Upgrade the instance version.

NOTE

To upgrade the instance version, upgrading the mapped bastion host is recommended. For details, see **Upgrading the System Version**.

1. Before the upgrade, you need to verify the SHA 256 value of the upgrade package provided by Huawei.
2. Click **Upgrade**, open the local directory, and select and upload the upgrade package.
3. After the package is uploaded, its version number is displayed. Click **OK** to start the upgrade.
4. Wait for the system to automatically restart, which takes about 5 minutes. After the system is restarted, the upgrade is complete.
5. Log in to the system again and choose **System** > **About System** to check the device version.

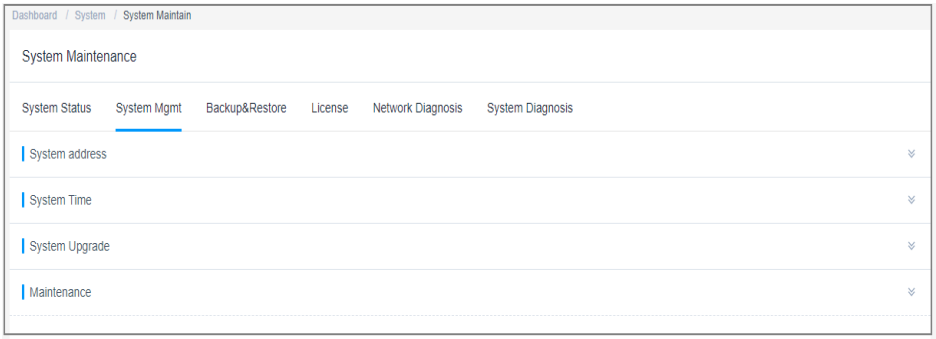
----End

Managing System Tools

Step 1 Log in to your bastion host.

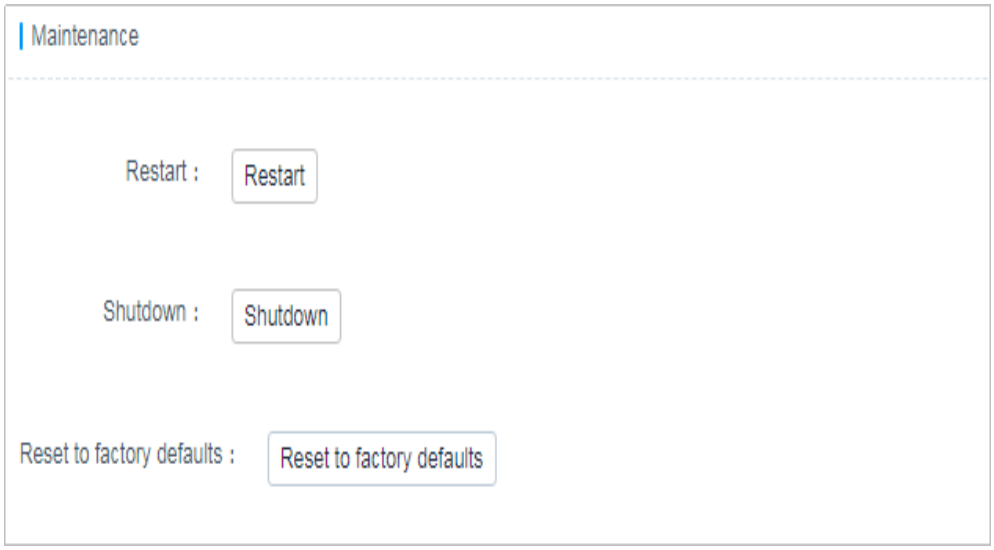
Step 2 Choose **System** > **System Maintain** > **System Mgmt**.

Figure 16-11 System Mgmt



Step 3 Expand the **Maintenance** area. In this area, you can restart and upgrade the system and restore the system to factory settings.

Figure 16-12 Maintenance



- Restarting the system

  NOTE

  To restart a bastion host, restarting it on the management console is recommended. For details, see **Restarting a Bastion Host Instance**.

  a. Click **Restart**. A confirmation dialog box is displayed.
  b. Click **OK**. The administrator confirmation dialog box is displayed.
  c. Enter the password of system administrator **admin**.
  d. Click **OK**. After the verification is successful, you can log in to the system.

- Restart the operation service.

  a. Click **Restart**. A confirmation dialog box is displayed.
  b. Click **OK**. The administrator confirmation dialog box is displayed.
  c. Enter the password of system administrator **admin**.
  d. Click **OK**. After the verification is successful, you can restart the operation service.

- Restoring factory settings

  a. Click **Reset to factory defaults**. A confirmation dialog box is displayed.
  b. Click **OK**. The administrator confirmation dialog box is displayed.
  c. Enter the password of system administrator **admin**.
  d. Click **OK**. After the verification is successful, the system is restored to the initial settings, and all system data is cleared.

  WARNING

  Do not restore factory settings unless in emergencies. Otherwise, all system data will be lost.

----End

16.2.3 System Configuration Backup and Restoration (Backup&Restore)

To ensure that the system configuration data is not lost, enable the automatic backup function or periodically back up the system configuration data.

This section describes how to back up and restore system configurations and how to manage the backup files

The backup files are stored on your bastion host. So they will use some of space. You can check the backup file size by date in the backup list.

Constraints

- A system configuration backup file can only be used for the bastion host that generates it.
- Only system configuration parameters can be backed up. System data generated during O&M cannot be backed up. For details about system data backup, see **Data Maintenance**

Prerequisites

You have the management permissions for the **System** module.

Backing Up System Configuration Data

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Maintain** > **Backup&Restore**.

Step 3 Enable auto backup.

In the **Config Backup** area, enable **Auto**. The system will automatically back up the configuration at 00:00 every day.

Step 4 Start a backup job immediately.

1. In the **Config Backup** area, click **New**.
2. In the displayed dialog box, enter remarks to distinguish backup files.
3. Click **OK** to start the backup. After the backup is complete, you can view the backup file in the backup list.

----End

Restoring System Configurations

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Maintain** > **Backup&Restore**.

Step 3 Restore the system configuration. Select any of the following methods:

- One-click system configuration restoration

  Before your start, ensure that a system configuration backup file is ready.

  a. In the **Config Backup** area, select the backup file you want to use.

b. In the **Operation** column, click **Restore**.

- Using a local backup file to restore system configurations
  a. In the **Config Restore** area, click **Upload**.
  b. In the displayed dialog box, select a backup configuration file that has been downloaded.
  c. After the backup file is uploaded, click **OK** to start the restoration.

Step 4 Refresh the page. After the system is restored, you are required to log in to the system again.

----End

Managing Backup Files

You can download and delete system configuration backup files to save more storage space.

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Maintain** > **System Status**.

Step 3 Download a backup file.

1. In the **Config Backup** area, select the backup file you want to use.
2. In the **Operation** column, click **Download** to download the backup file.

Step 4 Delete a backup file.

1. In the **Config Backup** area, select the backup file you want to use.
2. In the **Operation** column, click **Delete** to delete the backup file to release storage space.

----End

16.2.4 License

When the system license is about to expire or the system specifications are upgraded, the system administrator can renew the instance, obtain a new license file, and update the license.

In 3.3.62.0 and later versions, primary and standby instances can be authorized separately without having to disabling HA.

Prerequisites

You have the management permissions for the **System** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Maintain** > **License** and view the current license information.

Table 16-7 License parameters

Parameter	Description
Customer Info	Region and AZ where the system is used
Authorization Type	By default, **Official Version** is set for **Authorization Type**.
Status	**Activated**: The license can be used normally. • Click **Update License**, download the license application file as prompted, and contact the vendor to apply for a license. Import the new license to update the license. • Click **Backup License** to download the current system license to your PC. **NOTE** When the numbers of assets, users, and concurrent requests increase, you can update the license to upgrade the system specifications. In this case, adjust the CPU, memory, and bandwidth configurations of your bastion host.
Initial Host Status	This parameter is available for primary/standby instances. **Activated**: The license can be used normally. • Click **Update License**, download the license application file as prompted, and contact the vendor to apply for a license. Import the new license to update the license. • Click **Backup License** to download the current system license to your PC. **NOTE** When the numbers of assets, users, and concurrent requests increase, you can update the license to upgrade the system specifications. In this case, adjust the CPU, memory, and bandwidth configurations of your bastion host.
Initial Standby Status	This parameter is available for primary/standby instances. **Activated**: The license can be used normally. • Click **Update License**, download the license application file as prompted, and contact the vendor to apply for a license. Import the license file authorized by the vendor to update the license. • Click **Backup License** to download the current system license to your PC. **NOTE** When the numbers of assets, users, and concurrent requests increase, you can update the license to upgrade the system specifications. In this case, adjust the CPU, memory, and bandwidth configurations of your bastion host.
Product ID	Product ID of the current system

Parameter	Description
Authorized Modules	Supported function modules. The function modules available depend on the edition you are using. We provided standard editions and professional editions. • Standard editions: include only basic modules. • Professional editions: include basic modules, **automatic O&M**, and **database audit**. – Automatic O&M includes the **Sync Rules**, **Script**, **Fast Operation**, and **OM Task** modules, as well as the configuration backup function. – Database audit allows you to audit database logs and operation commands. To this end, add databases to your bastion host and install local database tools for the bastion host to access databases.
Max Resources	Maximum number of resources that can be added to a bastion host (including host and application resources)
Max Concurrent Conns	Maximum number of connections established to host and application resources at the same time over different protocols. This number is the result of the number of logged users multiply by the number of logged in resources.

----End

16.2.5 Network Diagnosis

If a managed host fails to be logged in, you can quickly check the network between the bastion host and the managed host resource with network diagnosis built in the bastion host. You can use any of the following methods to check the connectivity:

- Ping the host IP address to check whether the bastion host communicates with the host resource over the ICMP protocol.
- Perform route tracing on the host address to check whether the route between the bastion host and the host resource is reachable.
- Perform the TCP port test on the host IP address to check the host resource is reachable over the TCP port from the bastion host.

NOTE

- If the network is unreachable, rectify the fault.
- If the network connectivity is normal, check whether the username, password, and port number of the host added to the system are correct.

This topic describes how to test the network connectivity.

Prerequisites

You have the management permissions for the **System** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Maintain** > **Network Diagnosis**.

Step 3 Ping the IP address of the host to check the network connectivity.

1. Set **Infotype** to **ping**.
2. Enter the host IP address and click **Test** to view the connectivity test result.
3. Check whether the system can communicate with the host using the ICMP protocol.

Step 4 Traceroute the host IP address and check the network connectivity.

1. Set **Infotype** to **traceroute**.
2. Enter the host IP address and click **Test** to view the connectivity test result.
3. Check whether there is a reachable route between the system and the host.

Step 5 Test network connectivity through the TCP port.

1. Set **Infotype** to **TCP port**.
2. Enter the host IP address and port number and click **Test** to view the connectivity test result.
3. Check whether the TCP port between the system and the host is reachable.

----End

16.2.6 System Diagnosis

On the system diagnosis page, you can easily check the status and details about the bastion host, including overall information and details about system load, kernel, memory, network interface card (NIC), disk usage, routes, and ARP.

Prerequisites

You have the management permissions for the **System** module.

Procedure

Step 1 Log in to your bastion host.

Step 2 Choose **System** > **System Maintain** > **System Diagnosis**.

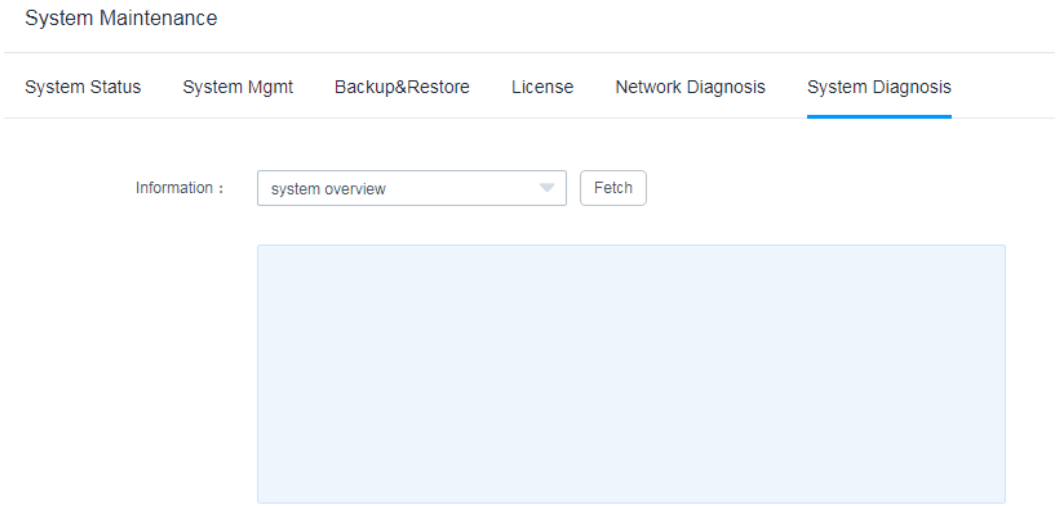
Step 3 Select an information type and then click **Fetch** to view the details.

Table 16-8 System diagnosis parameters

Parameter	Description
system overview	Obtains overview information about the bastion host, including memory, I/O, and CPU.
system load	Obtains information about the bastion host load.

Parameter	Description
system kernel	Obtains information about the system kernel.
memory summary	Obtains information about the system memory.
network interfaces	Obtains information about the system NIC.
disk usage	Obtains information about the disk usage of the system.
route table	Obtains route information about the system.
ARP table	Obtains ARP information about the system.

Figure 16-13 System Diagnosis



----End

17 Installing an Application Server

17.1 Overview

For Windows and special Linux OSs, resource O&M cannot be directly performed on the bastion host console. You need to create an application publishing server to implement resource O&M.

Specification Selection

To ensure that all resources can be operated and maintained properly, the memory specifications of the Windows publishing server need to support the number of resources to be managed. For details, see the following table.

Table 17-1 Recommended specifications and number of assets for a Windows application publishing server

Memory Specifications	Idle Memory Usage	Available Memory	Concurrent Assets Supported
4GiB	About 800 MiB	About 3.2 GiB	About 16
8GiB	About 800 MiB	About 7.2 GiB	About 36
16GiB	About 800 MiB	About 15.2 GiB	About 76
32GiB	About 800 MiB	About 31.2 GiB	About 156
64GiB	About 800 MiB	About 63.2 GiB	About 316
128GiB	About 800 MiB	About 127.2 GiB	About 636

17.2 Installing a Windows Server 2019 Application Server

17.2.1 Installing a Server

Prerequisites

You have obtained the account and its password of the server administrator.

Procedure

Step 1 Log in to the server as the administrator.

Step 2 Start **Server Manager** and click **Dashboard**.

Step 3 Click **Add Roles and Features**. In the displayed **Add Roles and Features Wizard** dialog box, complete settings as prompted, and click **Next**.

Step 4 On the **Installation Type** page, select **Role-based or feature-based installation**.

Step 5 Select a destination server.

Step 6 In the **Server Roles** window, select **Active Directory Domain Services**, **DNS Server**, and **Remote Desktop Service**.

Step 7 (Optional) Select features required for the server or click **Next** to skip this step.

Step 8 Choose **Remote Desktop Service** > **Role Service**.

Select **Remote Desktop Session Host**, **Remote Desktop Connection Broker**, **Remote Desktop Licensing**, **Remote Desktop Gateway**, and **Remote Desktop Web Access**.

Step 9 (Optional) Choose **Web Server (IIS)** > **Role Services**. In the displayed window, accept the default settings.

Step 10 (Optional) Choose **Network Policies and Access Services**. Accept the default selection.

Step 11 Confirm the installation settings and click **Install**.

Step 12 When the installation completes, click **Finish** and restart the application server.

----End

17.2.2 Licensing and Activating the Remote Desktop Service

Prerequisites

- You have obtained the enterprise license number and related information.
- You have obtained the account and its password of the server administrator.

Procedure

Step 1 Log in to the server as the administrator.

Step 2 Choose **Start** > **Administrative Tools** > **Remote Desktop Services** > **Remote Desktop Licensing Manager**.

Step 3 In the displayed window, right-click the target server name, and then choose **Activate Server** from the shortcut menu.

Step 4 Open the **Activate Server Wizard** and perform operations as prompted.

Step 5 Select the automatic connection method.

Step 6 Enter the information about your company and user name.

Step 7 (Optional) Enter the detailed contact information about the company.

Step 8 Confirm the installation and start the license installation wizard.

Step 9 Select **Enterprise Agreement** for **License program**.

Step 10 Enter the enterprise agreement number.

NOTE

The enterprise agreement number must be purchased from the third-party platform in advance to obtain the official remote desktop authorization license.

Step 11 Select **Windows Server 2019** for **Product version**, select **RDS Per User CAL** for **License type**, and set **Quantity** to **100**.

Step 12 After the license is installed, activate the server and return to the **Remote Desktop Licensing Manager** console and check whether the server is activated.

----End

17.2.3 Modifying the Group Policy

Prerequisites

You have obtained the account and its password of the server administrator.

Starting Local Group Policy Editor

Open the command line interface and enter **gpedit.msc** to open **Local Group Policy Editor**.

Selecting the Specified Remote Desktop License Servers

Step 1 Choose **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Licensing**.

Step 2 Double-click **Use the specified Remote Desktop license servers**.

Step 3 In the displayed dialog box, select the **Enabled** option.

Step 4 Click **OK**.

----End

Hiding Notifications About RD Licensing Problems that Affect the RD Session Host Server

Step 1 Choose **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Licensing**.

Step 2 Double-click **Hiding notifications about RD Licensing problems that affect the RD Session Host Server**.

Step 3 Select the **Enable** option.

Step 4 Then, click **OK**.

----End

Setting the Remote Desktop Licensing Mode

Step 1 Choose **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Licensing**.

Step 2 Double-click **Set the Remote Desktop licensing mode**.

Step 3 Select **Enabled** to enable the remote desktop licensing mode.

In the displayed window, select the **Enabled** option. In the **Options** area, under **Specify the licensing mode for the RD Session Host server**, select **Per User** from the drop-down list.

Step 4 Then, click **OK**.

----End

Limit number of connections

Step 1 Choose **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Connections**.

Step 2 Double-click **Limit Number of Connections**.

Step 3 Select the **Enabled** option.

Set **RD Maximum Connections allowed** to **999999**.

Step 4 Then, click **OK**.

----End

Allowing Remote Start of Unlisted Programs

Step 1 Choose **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Connections**.

Step 2 Double-click **Allow remote start of unlisted programs**.

Step 3 In the displayed dialog box, select the **Enabled** option.

Step 4 Then, click **OK**.

----End

Restrict Remote Desktop Services users to a single Remote Desktop Services session

Step 1 Choose **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Connections**.

Step 2 Double-click **Restrict Remote Desktop Services users to a single Remote Desktop Services session**.

Step 3 In the displayed window, select the **Disabled** option.

Step 4 Then, click **OK**.

----End

Setting Time Limit for Disconnected Sessions

Step 1 Choose **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Session Time Limits**.

Step 2 Double-click **Set time limit for disconnected sessions**.

Step 3 In the displayed dialog box, select the **Enabled** option.

Set **End a disconnected session** to **1 minute**.

Step 4 Then, click **OK**.

----End

Disabling Automatic Root Certificates Update (Bastion V3.3.26.0 or Later)

If your CBH system is earlier than *V3.3.26.0*, skip this operation. If your CBH system has been upgraded to V3.3.26.0 or later, perform the following steps.

Step 1 Choose **Administrative Templates** > **System** > **Internet Communication Management**.

Step 2 Double-click **Turn off Automatic Root Certificates Update**.

Step 3 Select **Enabled**.

Step 4 Then, click **OK**.

----End

Configuring Certificate Path Validation Settings (V3.3.26.0 or Later)

If your CBH system is earlier than *V3.3.26.0*, skip this operation. If your CBH system has been upgraded to V3.3.26.0 or later, perform the following steps.

Step 1 Choose **Windows Settings** > **Security Settings** > **Public Key Policies**.

Step 2 Double-click **Certificate Path Validation Settings**.

Step 3 Click the **Network Retrieval** tab.

Step 4 Clear the **Automatically update certificates in the Microsoft Root Certificate Program (recommended)** check box.

Set **Default URL retrieval timeout (in seconds)** to **1**.

Step 5 Then, click **OK**.

----End

Refreshing the Local Group Policy

Step 1 Close the **Local Group Policy Editor** window.

Step 2 Open the **Run** box and run the **gpupdate /force** command to refresh the local policy.

Step 3 The application publish server has been deployed. To test its function, add this server and applications on it to your bastion host.

----End

17.2.4 Installing RemoteApp Program

In CBH systems of V3.3.26.0 or later, RemoteAppProxy must be installed on application publishing servers.

Prerequisites

You have obtained the account and its password of the server administrator.

Procedure

Step 1 Log in to the server as the administrator.

Step 2 Download the ***RemoteAPPProxyInstaller_xxx.zip*** (*xxx* indicates the version number) package.

Download **RemoteAppProxy 2.1.1** (compatible with CBH 3.3.26.0 or later)

NOTE

The server must have an EIP bound.

Step 3 Decompress **RemoteAPPProxyInstaller**_*xxx*.**zip** (*xxx* indicates the version number).

Step 4 Double-click **RemoteAPPProxyInstaller**_*xxx*.**msi** (*xxx* indicates the version number) to start the installation.

Select the default installation path.

Step 5 After the installation completes, click **Close**.

----End

17.3 Installing a Windows Server 2016 Application Server

17.3.1 Installing a Server

Prerequisites

You have obtained the account and its password of the server administrator.

Procedure

Step 1 Log in to the server as the administrator.

Step 2 Start **Server Manager** and click **Dashboard**.

Step 3 Click **Add Roles and Features**. In the displayed **Add Roles and Features Wizard** dialog box, complete settings as prompted, and click **Next**.

Step 4 On the **Installation Type** page, select **Role-based or feature-based installation**.

Step 5 Select a destination server.

Step 6 In the **Server Roles** window, select **Active Directory Domain Services**, **DNS Server**, and **Remote Desktop Service**.

Step 7 (Optional) Select features required for the server or click **Next** to skip this step.

Step 8 Choose **Remote Desktop Service** > **Role Service**.

Select **Remote Desktop Session Host**, **Remote Desktop Connection Broker**, **Remote Desktop Licensing**, **Remote Desktop Gateway**, and **Remote Desktop Web Access**.

Step 9 (Optional) Choose **Web Server (IIS)** > **Role Services**. In the displayed window, accept the default settings.

Step 10 (Optional) Choose **Network Policies and Access Services**. Accept the default selection.

Step 11 Confirm the installation settings and click **Install**.

Step 12 When the installation completes, click **Finish** and restart the application server.

----End

17.3.2 Licensing and Activating the Remote Desktop Service

Prerequisites

- You have obtained the enterprise license number and related information.
- You have obtained the account and its password of the server administrator.

Procedure

Step 1 Log in to the server as the administrator.

Step 2 Choose **Start** > **Administrative Tools** > **Remote Desktop Services** > **Remote Desktop Licensing Manager**.

Step 3 In the displayed window, right-click the target server name, and then choose **Activate Server** from the shortcut menu.

Step 4 Open the **Activate Server Wizard** and perform operations as prompted.

Step 5 Select the automatic connection method.

Step 6 Enter the information about your company and user name.

Step 7 (Optional) Enter the detailed contact information about the company.

Step 8 Confirm the installation and start the license installation wizard.

Step 9 Select **Enterprise Agreement** for **License program**.

Step 10 Enter the enterprise agreement number.

NOTE

The enterprise agreement number must be purchased from the third-party platform in advance to obtain the official remote desktop authorization license.

Step 11 Select **Windows Server 2016** for **Product version**, select **RDS Per User CAL** for **License type**, and set **Quantity** to **100**.

Step 12 After the license is installed, activate the server and return to the **Remote Desktop Licensing Manager** console and check whether the server is activated.

----End

17.3.3 Modifying the Group Policy

Prerequisites

You have obtained the account and its password of the server administrator.

Starting Local Group Policy Editor

Open the command line interface and enter **gpedit.msc** to open **Local Group Policy Editor**.

Selecting the Specified Remote Desktop License Servers

Step 1 Choose **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Licensing**.

Step 2 Double-click **Use the specified Remote Desktop license servers**.

Step 3 In the displayed dialog box, select the **Enabled** option.

Step 4 Click **OK**.

----End

Hiding Notifications About RD Licensing Problems that Affect the RD Session Host Server

Step 1 Choose **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Licensing**.

Step 2 Double-click **Hiding notifications about RD Licensing problems that affect the RD Session Host Server**.

Step 3 Select the **Enable** option.

Step 4 Then, click **OK**.

----End

Setting the Remote Desktop Licensing Mode

Step 1 Choose **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Licensing**.

Step 2 Double-click **Set the Remote Desktop licensing mode**.

Step 3 Select **Enabled** to enable the remote desktop licensing mode.

In the displayed window, select the **Enabled** option. In the **Options** area, under **Specify the licensing mode for the RD Session Host server**, select **Per User** from the drop-down list.

Step 4 Then, click **OK**.

----End

Limit number of connections

Step 1 Choose **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Connections**.

Step 2 Double-click **Limit Number of Connections**.

Step 3 Select the **Enabled** option.

Set **RD Maximum Connections allowed** to **999999**.

Step 4 Then, click **OK**.

----End

Allowing Remote Start of Unlisted Programs

Step 1 Choose **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Connections**.

Step 2 Double-click **Allow remote start of unlisted programs**.

Step 3 In the displayed dialog box, select the **Enabled** option.

Step 4 Then, click **OK**.

----End

Restrict Remote Desktop Services users to a single Remote Desktop Services session

Step 1 Choose **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Connections**.

Step 2 Double-click **Restrict Remote Desktop Services users to a single Remote Desktop Services session**.

Step 3 In the displayed window, select the **Disabled** option.

Step 4 Then, click **OK**.

----End

Setting Time Limit for Disconnected Sessions

Step 1 Choose **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Session Time Limits**.

Step 2 Double-click **Set time limit for disconnected sessions**.

Step 3 In the displayed dialog box, select the **Enabled** option.

Set **End a disconnected session** to **1 minute**.

Step 4 Then, click **OK**.

----End

Disabling Automatic Root Certificates Update (CBH V3.3.26.0 or Later)

If your CBH system is earlier than V3.3.26.0, skip this operation. If your CBH system is upgrade to V3.3.26.0 or later, perform the following steps.

Step 1 Choose **Administrative Templates** > **System** > **Internet Communication Management**.

Step 2 Double-click **Turn off Automatic Root Certificates Update**.

Step 3 Select **Enabled**.

Step 4 Then, click **OK**.

----End

Configuring Certificate Path Validation Settings (CBH V3.3.26.0 or Later)

If your CBH system is earlier than V3.3.26.0, skip this operation. If your CBH system is upgrade to V3.3.26.0 or later, perform the following steps.

Step 1 Choose **Windows Settings** > **Security Settings** > **Public Key Policies**.

Step 2 Double-click **Certificate Path Validation Settings**.

Step 3 Click the **Network Retrieval** tab.

Step 4 Clear the **Automatically update certificates in the Microsoft Root Certificate Program (recommended)** check box.

Set **Default URL retrieval timeout (in seconds)** to **1**.

Step 5 Then, click **OK**.

----End

Refreshing the Local Group Policy

Step 1 Close the **Local Group Policy Editor** window.

Step 2 Open the **Run** box and run the **gpupdate /force** command to refresh the local policy.

Step 3 The application publish server has been deployed. To test its function, add this server and applications on it to your bastion host.

----End

17.3.4 Installing RemoteApp Program

In CBH systems of V3.3.26.0 or later, RemoteAppProxy must be installed on application publishing servers.

Prerequisites

You have obtained the account and its password of the server administrator.

Procedure

Step 1 Log in to the server as the administrator.

Step 2 Download the ***RemoteAPPProxyInstaller_xxx.zip*** (*xxx* indicates the version number) package.

Download **RemoteAppProxy 2.1.1** (compatible with CBH 3.3.26.0 or later)

NOTE

The server must have an EIP bound.

Step 3 Decompress **RemoteAPPProxyInstaller**_*xxx*.**zip** (*xxx* indicates the version number).

Step 4 Double-click **RemoteAPPProxyInstaller**_*xxx*.**msi** (*xxx* indicates the version number) to start the installation.

Select the default installation path.

Step 5 After the installation completes, click **Close**.

----End

17.4 Installing a Windows Server 2012 R2 Application Server

17.4.1 Installing a Server

Step 1 Start **Server Manager** and click **Dashboard**.

Step 2 Click **Add Roles and Features**. In the displayed **Add Roles and Features Wizard** dialog box, complete settings as prompted, and click **Next**.

Step 3 On the **Installation Type** page, select **Role-based or feature-based installation**.

Step 4 Select a destination server.

Step 5 In the **Server Roles** window, select **Active Directory Domain Services**, **DNS Server**, and **Remote Desktop Service**.

Step 6 (Optional) Select features required for the server or click **Next** to skip this step.

Step 7 Choose **Remote Desktop Service** > **Role Service**.

Select **Remote Desktop Session Host**, **Remote Desktop Connection Broker**, **Remote Desktop Licensing**, **Remote Desktop Gateway**, and **Remote Desktop Web Access**.

Step 8 (Optional) Choose **Web Server (IIS)** > **Role Services**. In the displayed window, accept the default settings.

Step 9 (Optional) Choose **Network Policies and Access Services**. Accept the default selection.

Step 10 Confirm the installation settings and click **Install**.

Step 11 When the installation completes, click **Finish** and restart the application server.

----End

17.4.2 Licensing and Activating the Remote Desktop Service

Prerequisites

- You have obtained the enterprise license number and related information.
- You have obtained the account and its password of the server administrator.

Procedure

Step 1 Open the Remote Desktop Licensing Manager.

Step 2 In the displayed window, right-click the target server name, and then choose **Activate Server** from the shortcut menu.

Step 3 Open the **Activate Server Wizard** and perform operations as prompted.

Step 4 Select the automatic connection method.

Step 5 Enter the information about your company and user name.

Step 6 (Optional) Enter the detailed contact information about the company.

Step 7 Confirm the installation and start the license installation wizard.

Step 8 Select **Enterprise Agreement** for **License program**.

Step 9 Enter the enterprise agreement number.

NOTE

The enterprise agreement number must be purchased from the third-party platform in advance to obtain the official remote desktop authorization license.

Step 10 Select **Windows Server 2012 R2** for **Product version**, select **RDS Per User CAL** for **License type**, and set **Quantity** to **100**.

Step 11 After the license is installed, activate the server and return to the **Remote Desktop Licensing Manager** console and check whether the server is activated.

----End

17.4.3 Modifying the Group Policy

Local Group Policy Editor

Open the **Run** box and enter **gpedit.msc** to open **Local Group Policy Editor**.

Using the Specified Remote Desktop License Servers

Step 1 Choose **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Licensing**. Double-click **Use the specified Remote Desktop license servers**.

Step 2 In the displayed window, select the **Enabled** option.

Step 3 Click **OK**.

----End

Hiding Notifications About RD Licensing Problems that Affect the RD Session Host Server

Step 1 Choose **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Licensing**. Double-click **Hide notifications about RD Licensing problems that affect the RD Session Host Server**.

Step 2 In the displayed window, select the **Enabled** option.

Step 3 Then, click **OK**.

----End

Setting the Remote Desktop Licensing Mode

Step 1 Choose **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Licensing**. Double-click **Set the Remote Desktop licensing mode**.

Step 2 In the displayed window, select the **Enabled** option. In the **Options** area, under **Specify the licensing mode for the RD Session Host server**, select **Per User** from the drop-down list.

Step 3 Then, click **OK**.

----End

Limit number of connections

Step 1 Choose **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Connections**. Double-click **Limit number of connections**.

Step 2 In the displayed window, select the **Enabled** option, then set **RD Maximum Connections allowed** to **999999**.

Step 3 Then, click **OK**.

----End

Allowing Remote Start of Unlisted Programs

Step 1 Choose **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Connections**. Double-click **Allow users to connect remotely using Remote Desktop Services**.

Step 2 In the displayed dialog box, select the **Enabled** option.

Step 3 Then, click **OK**.

----End

Restrict Remote Desktop Services users to a single Remote Desktop Services session

Step 1 Choose **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Connections**. Double-click **Restrict Remote Desktop Services user to a single Remote Desktop Services session**.

Step 2 In the displayed window, select the **Disabled** option.

Step 3 Then, click **OK**.

----End

Setting Time Limit for Disconnected Sessions

Step 1 Choose **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Session Time Limits**. Double-click **Set time limit for disconnected sessions**.

Step 2 In the displayed window, select **Enabled** for **Set time limit for disconnected sessions**, and change the value of **End a disconnected session** to **1 minute**.

Step 3 Then, click **OK**.

----End

Disabling Automatic Root Certificates Update (Bastion V3.3.26.0 or Later)

If your CBH system is earlier than *V3.3.26.0*, skip this operation. If your CBH system has been upgraded to V3.3.26.0 or later, perform the following steps.

Step 1 Choose **Administrative Templates** > **System** > **Internet Communication Management**.

Step 2 Double-click **Turn off Automatic Root Certificates Update**.

Step 3 Select **Enabled**.

Step 4 Then, click **OK**.

----End

Configuring Certificate Path Validation Settings (V3.3.26.0 or Later)

If your CBH system is earlier than *V3.3.26.0*, skip this operation. If your CBH system has been upgraded to V3.3.26.0 or later, perform the following steps.

Step 1 Choose **Windows Settings** > **Security Settings** > **Public Key Policies**.

Step 2 Double-click **Certificate Path Validation Settings**.

Step 3 Click the **Network Retrieval** tab.

Step 4 Clear the **Automatically update certificates in the Microsoft Root Certificate Program (recommended)** check box.

Set **Default URL retrieval timeout (in seconds)** to **1**.

Step 5 Then, click **OK**.

----End

Refreshing the Local Group Policy

Step 1 Close the **Local Group Policy Editor** window.

Step 2 Open the **Run** box and run the **gpupdate /force** command to refresh the local policy.

Step 3 The application publish server has been deployed. To test its function, add this server to your bastion host.

----End

17.4.4 Installing RemoteApp Program

In CBH systems of V3.3.26.0 or later, RemoteAppProxy must be installed on application publishing servers.

Prerequisites

You have obtained the account and its password of the server administrator.

Procedure

Step 1 Log in to the server as the administrator.

Step 2 Download the ***RemoteAPPProxyInstaller_xxx.zip*** (*xxx* indicates the version number) package.

Download **RemoteAppProxy 2.1.1** (compatible with CBH 3.3.26.0 or later)

NOTE

The server must have an EIP bound.

Step 3 Decompress **RemoteAPPProxyInstaller**_*xxx*.**zip** (*xxx* indicates the version number).

Step 4 Double-click **RemoteAPPProxyInstaller**_*xxx*.**msi** (*xxx* indicates the version number) to start the installation.

Select the default installation path.

Step 5 After the installation completes, click **Close**.

----End

17.5 Installing a Windows Server 2008 R2 Application Server

17.5.1 Installation Environment

The following is the information of the server where the AD domain is installed:

- Windows Server version: Windows Server 2008 R2 (All software packages have been installed.)
- IP address: 192.168.*X.X*/*X*
- Gateway address: 192.168.*X.X*
- DNS: 192.168.*X.X*
- Domain name: example.com

- Computer name: server

17.5.2 Installing the AD Domain

Changing the Computer Name and Static Server IP Address

Change the service IP address, point the DNS address to the local host, and then change the computer name to **server**. After the AD domain service is installed, the host name is automatically changed to the format of *host-name.domain-name*, for example, server.huawei.com.

Installing the AD Domain

Run the **dcpromo.exe** command on the CLI to install the AD domain and DNS server. Do not install the AD domain and DNS server using the wizard for adding roles.

AD Domain Service Installation Wizard

Step 1 To install the AD domain, click **Next**.

Step 2 Click **Next**.

Step 3 Select the option indicating creating a domain in a new forest and click **Next**.

Step 4 Click **Next**.

Step 5 Set the forest function level, select **Windows Server 2008 R2** from the drop-down list, and click **Next**.

Step 6 Select **DNS server** and click **Next**.

Step 7 If a message is displayed indicating that the DNS delegation fails to be created, click **Yes** and continue.

Step 8 Select the directories for storing database files and log files. You can retain the default settings and click **Next**.

Step 9 Set the password for the directory services restore mode (DSRM). The **Administrator** password in DSRM is not the same as the system password. Click **Next**.

Step 10 On the summary page that is displayed, click **Next**.

Step 11 Tick the box indicating to restart the system after installation.

Step 12 After the restart, log in as a domain user.

Step 13 The AD domain environment has been installed.

----End

17.5.3 Installing and Licensing Remote Desktop Service

Remote Desktop Service Installation and Configuration

Step 1 Choose **Server Manager** > **Roles** > **Add Roles Wizard**.

Step 2 Select **Remote Desktop Services** and click **Next**.

Step 3 Click **Next**.

Step 4 Click **Next**.

Step 5 Select **Install Remote Desktop Session Host Anyway**, and then click **Next**.

Step 6 Select **Role Services**. Select **Remote Desktop Session Host** and **Remote Desktop Licensing**, and click **Next**.

Step 7 Click **Next**.

Step 8 Select the option **Do not require Network Level Authentication**, and then click **Next**.

Step 9 Select **Configure later** and click **Next**.

Step 10 By default, **Administrators** can connect to the RD session host server (if necessary, add required users or user groups) and click **Next**.

Step 11 Click **Next**.

Step 12 Click **Next**.

Step 13 Select **Choose a certificate for SSL encryption later** and click **Next**.

Step 14 Select **Later** and click **Next**.

Step 15 Retain the default configuration and click **Next**.

Step 16 Select **Role Services**. Select **Network Policy Server** and click **Next**.

Step 17 Install IIS and click **Next**.

Step 18 Retain the default configuration and click **Next**.

Step 19 Retain the default configuration and click **Install**.

Step 20 The installation process is displayed. Please wait.

Step 21 After the installation is complete, click **Close**. In the displayed dialog box, select **Yes** to restart the server, and then click **Next**.

Step 22 After the server is restarted, the role service configuration window is displayed. After the automatic configuration is complete, click **Close**.

Step 23 Choose **Start** > **Administrative Tools** > **Remote Desktop Service** > **Remote Desktop Session Host Configuration**. In the right pane, double-click the line indicating that only one session is allowed for each user. In the **Properties** page, deselect the option indicating that only one session is allowed for each user and click **OK**.

----End

Activating Remote Desktop Authorization

Step 1 Choose **Start** > **Administrative Tools** > **Remote Desktop Services** > **Remote Desktop Licensing Manager**. Because the RD authorization server is not activated, the red cross (x) is displayed in the lower right corner of the authorization server icon. Right-click **Server** and select **Activate Server**.

Step 2 Click **Next**.

Step 3 Click **Next**.

Step 4 Enter the mandatory registration information and click **Next**.

Step 5 Retain the default configuration and click **Next**.

Step 6 By default, the option indicating that the license installation wizard starts immediately is selected. Click **Next**.

Step 7 Click **Next**.

Step 8 Select **Enterprise contract** for **License Plan** and click **Next**.

Step 9 Enter the contract number and click **Next**.

Step 10 Select **Windows Server 2008 or Windows Server 2008 R2** for the product version. Select **TS or RDS per user CAL** for the license type. Enter the maximum number of remote connections allowed.

Step 11 Click **Finish**.

Step 12 The RD authorization server has been activated, and the icon changes from a red cross (x) to a green tick (√). The configuration and activation of the remote desktop service are complete.

----End

17.5.4 Modifying the Group Policy

Local Group Policy Editor

Step 1 Choose **Start** > **Run** and enter **gpedit.msc** to open the group policy.

Step 2 Choose **Computer Configuration** > **Management Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Licensing**. Double-click **Use the specific Remote Desktop license servers** on the right.

----End

Hiding Notifications About RD Licensing Problems that Affect the RD Session Host Server

Open the **Hide notification about RD Licensing problems that affect the RD Session Host server** dialog box, select **Enabled**, and click **Next Setting**.

Setting the Remote Desktop Licensing Mode

In the **Set the Remote Desktop licensing mode** dialog box, select **Enabled**. In the **Specify the licensing mode for the RD Session Host server** drop-down list, select **Per User** and click **OK**.

Configuring Multiple Users for the Terminal Service

Step 1 Choose **Start** > **Run** and enter **gpedit.msc** to open the group policy.

Step 2 Choose **Computer Configuration** > **Management Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Connections**.

Step 3 Select **Enabled** for **Limit number of connections** and set the maximum number of connections to **999999**.

Step 4 Select **Enabled** for **Allow users to connect remotely using Remote Desktop Services**.

Step 5 Click **OK**.

Step 6 Choose **Computer Configuration** > **Management Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Session Time Limits**.

Step 7 Select **Enabled** for **Set time limit for disconnected sessions**, and change the value of **End a disconnected session** to **1 minute**.

Step 8 Click **OK**.

----End

Disabling Automatic Root Certificates Update (Bastion V3.3.26.0 or Later)

If your CBH system is earlier than *V3.3.26.0*, skip this operation. If your CBH system has been upgraded to V3.3.26.0 or later, perform the following steps.

Step 1 Choose **Administrative Templates** > **System** > **Internet Communication Management**.

Step 2 Double-click **Turn off Automatic Root Certificates Update**.

Step 3 Select **Enabled**.

Step 4 Then, click **OK**.

----End

Configuring Certificate Path Validation Settings (V3.3.26.0 or Later)

If your CBH system is earlier than *V3.3.26.0*, skip this operation. If your CBH system has been upgraded to V3.3.26.0 or later, perform the following steps.

Step 1 Choose **Windows Settings** > **Security Settings** > **Public Key Policies**.

Step 2 Double-click **Certificate Path Validation Settings**.

Step 3 Click the **Network Retrieval** tab.

Step 4 Clear the **Automatically update certificates in the Microsoft Root Certificate Program (recommended)** check box.

Set **Default URL retrieval timeout (in seconds)** to **1**.

Step 5 Then, click **OK**.

----End

Update Policy

Step 1 Close the local group policy editor. Choose **Start** > **Run**, and enter **gpupdate /force**.

Step 2 Update the local policy.

Step 3 The application publish server has been deployed. To test its function, add this server to your bastion host.

----End

17.5.5 Installing RemoteApp Program

In CBH systems of V3.3.26.0 or later, RemoteAppProxy must be installed on application publishing servers.

Prerequisites

You have obtained the account and its password of the server administrator.

Procedure

Step 1 Log in to the server as the administrator.

Step 2 Download the ***RemoteAPPProxyInstaller_xxx.zip*** (*xxx* indicates the version number) package.

Download **RemoteAppProxy 2.1.1** (compatible with CBH 3.3.26.0 or later)

NOTE

The server must have an EIP bound.

Step 3 Decompress **RemoteAPPProxyInstaller**_*xxx*.**zip** (*xxx* indicates the version number).

Step 4 Double-click **RemoteAPPProxyInstaller**_*xxx*.**msi** (*xxx* indicates the version number) to start the installation.

Select the default installation path.

Step 5 After the installation completes, click **Close**.

----End

17.6 Installing a Linux Application Server

Basic Environment Requirements

- OS requirements: EulerOS 2.9.8
- Network requirements: The server must have an EIP for public network access.
- Firewall requirements: Port 2376 for Docker services and ports 35000 to 40000 must be allowed.
- Disk space requirements: The installation directory **/var/lib** must have more than 50 GB of free space.

Prerequisites

You have obtained the password of the **root** user for logging in to the Linux server.

Procedure

Step 1 Log in to the Linux server as user **root**.

Step 2 On the Linux server, download the **Linux app_publisher_x86_64_*xxx*.tar.gz** package (xxx indicates the version number).

Table 17-2 app_publisher version description

CBH Version	Supported Architecture	app_publisher Version	Download URL
V3.3.66.0 and later	x86	3.3.66.0 (EulerOS 2.9.8, CentOS 7, and NeoKylin OS are supported.)	**Software Package**
	Arm	3.3.66.0 (EulerOS 2.9.8 and UOS are supported.)	**Software Package**
V3.3.60.0 and later	x86	1.7.0_EulerOS	**Software Package**
	Arm	1.7.0_EulerOS	**Software Package**
	Arm	1.7.0_UOS	**Software Package**
V3.3.52.0 and later	x86	1.6.1_EulerOS	**Software Package**
	Arm	1.6.1_EulerOS	**Software Package**
	x86	1.6.1_CentOS7	**Software Package**
	Arm	1.6.1_UOS	**Software Package**
V3.3.46.0 or later	x86	V1.5.0_CentOS7	**Software Package**
	Arm	V1.5.0_UOS	**Software Package**
V3.3.43.0 or later	x86	V1.4.0_CentOS7	**Software Package**
	Arm	V1.4.0_UOS	**Software Package**
V3.3.40.0 or later	x86	V1.3.0_CentOS7	**Software Package**
	Arm	V1.3.0_UOS	**Software Package**
V3.3.38.0 or later	x86	V1.2.0_CentOS7	**Software Package**
	Arm	V1.2.0_UOS20	**Software Package**
V3.3.30.0 or later	x86 and Arm	V1.1.0	**Software Package**
V3.3.26.0 or later	x86 and Arm	V1.0.0	**Software Package**

Step 3 On the Linux server, run the following commands to decompress the **app_publisher_x86_64_*xxx*.tar.gz** package:

 # tar -xvf app_publisher_*.tar.gz

 # cd app_publisher

Step 4 Check whether the Firefox application publish server has been installed.

- If the server is installed, run the following command to delete the previously installed Docker image for Mozilla Firefox:

  # docker rmi 127.0.0.1:5000/psm-firefox:0.2

  After it is deleted, go to **Step 5**.
- If no such server is installed, go to **Step 5**.

Step 5 Run the following command to deploy the script:

 # /bin/bash install.sh

Step 6 Run the following command to check the service status:

 # service docker status

```
[root@localhost firefox]# service docker status
Redirecting to /bin/systemctl status docker.service
● docker.service - Docker Application Container Engine
   Loaded: loaded (/usr/lib/systemd/system/docker.service; enabled; vendor preset: disabled)
  Drop-In: /usr/lib/systemd/system/docker.service.d
           └─docker.conf
   Active: active (running) since Fri 2021-02-26 14:30:25 CST; 3 weeks 6 days ago
     Docs: https://docs.docker.com
 Main PID: 995 (dockerd)
    Tasks: 19
   Memory: 161.3M
   CGroup: /system.slice/docker.service
           ├─  995 /usr/bin/dockerd
           └─29505 /usr/bin/docker-proxy -proto tcp -host-ip 0.0.0.0 -host-port 8908 -container-i
```

active (running): indicates that the application server is successfully installed.

Step 7 Create the **share** directory (only required for CBH V3.3.26.0).

 # mkdir /opt/autorun/share

Step 8 (Optional) Restart the application release server.

----End

17.7 Upgrading the RemoteApp or app_publisher Program

After the CBH instance is upgraded, you need to upgrade RemoteApp on Windows application servers or app_publisher on Linux application servers to the new version. Otherwise, the application publishing function cannot work properly. This section describes how to upgrade RemoteApp and app_publisher.

The procedure for upgrading the RemoteApp and app_publisher is as follows: Uninstall the old version and then install the new version.

Prerequisites

- You have obtained the administrator account and password of the target application server.
- The **/var/lib** directory has enough space to install the package on Linux servers.
- You have obtained the RemoteApp or app_publisher installation package of the latest version.

- RemoteApp

Table 17-3 app_publisher version description

CBH Version	Supported Architecture	app_publisher Version	Download URL
V3.3.66.0 and later	x86	3.3.66.0 (EulerOS 2.9.8, CentOS 7, and NeoKylin OS are supported.)	**Software Package**
	Arm	3.3.66.0 (EulerOS 2.9.8 and UOS are supported.)	**Software Package**
V3.3.60.0 and later	x86	1.7.0_EulerOS	**Software Package**
	Arm	1.7.0_EulerOS	**Software Package**
	Arm	1.7.0_UOS	**Software Package**
V3.3.52.0 and later	x86	1.6.1_EulerOS	**Software Package**
	Arm	1.6.1_EulerOS	**Software Package**
	x86	1.6.1_CentOS7	**Software Package**
	Arm	1.6.1_UOS	**Software Package**
V3.3.46.0 or later	x86	V1.5.0_CentOS7	**Software Package**
	Arm	V1.5.0_UOS	**Software Package**
V3.3.43.0 or later	x86	V1.4.0_CentOS7	**Software Package**
	Arm	V1.4.0_UOS	**Software Package**
V3.3.40.0 or later	x86	V1.3.0_CentOS7	**Software Package**
	Arm	V1.3.0_UOS	**Software Package**
V3.3.38.0 or later	x86	V1.2.0_CentOS7	**Software Package**
	Arm	V1.2.0_UOS20	**Software Package**
V3.3.30.0 or later	x86 and Arm	V1.1.0	**Software Package**
V3.3.26.0 or later	x86 and Arm	V1.0.0	**Software Package**

- app_publisher

The new version is always forward compatible. The latest version is **RemoteAppProxy 2.1.1**.

Upgrading RemoteApp (for Windows Application Publishing Servers)

Step 1 Log in to the Windows application publishing server, choose **Control Panel** > **Programs** > **Programs and Features**, and uninstall the earlier version RemoteApp.

Log in to the bastion host instance and choose **Resources** > **Application** > **AppServer** to view the Windows application server address.

Step 2 After the uninstallation, upload and decompress the new version RemoteApp installation package.

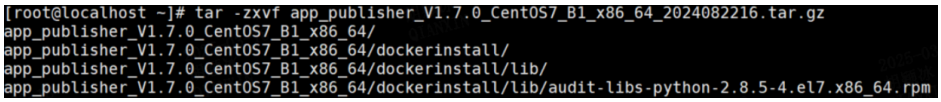
Step 3 Double-click **setup.exe** in the decompressed package to start the installation and complete the installation.

----End

Upgrading app_publisher (for Linux Application Servers)

Step 1 Log in to the Linux application publishing server, upload the **app_publish** installation package of the new version, and decompress it.

tar -zxvf app_publisher_V1.xxxxxxxxxx.tar.gz



Log in to the bastion host instance and choose **Resources** > **Application** > **AppServer** to view the Linux application server address.

Step 2 Run the following commands to uninstall the Docker image of the earlier version:

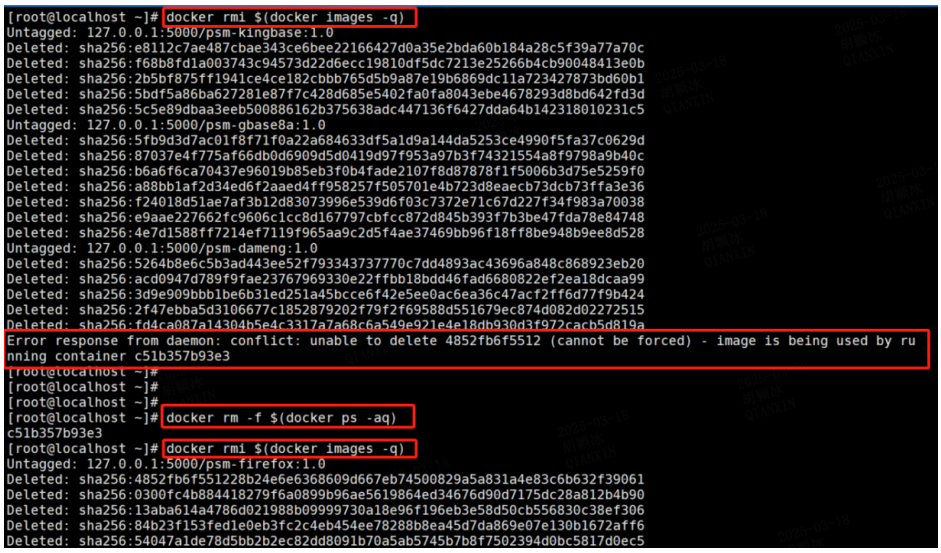
```
docker rmi $(docker images -q)
```

CAUTION

If the message "Error response from daemon: conflict: unable to delete 4852fb6f5512 (cannot be forced) - image is being used by running container xxxx" is displayed when you uninstall an image:

Run the following commands in sequence to delete container sessions and uninstall the image again:

```
docker rm -f $(docker ps -aq)
docker rmi $(docker images -q)
```

Step 3 After the uninstallation is complete, run the following commands to install the installation package and image in the **app_publish** directory of the new version:

```
cd app_publisher_V1.xxxxxxx
./install.sh
```

After the installation is complete, if the current bastion host version is 3.3.38.0 or earlier and the app_publisher version is V1.2.0 or earlier, update app_publish to a version later than 1.2.0. Then run the following commands in sequence to manually update the Docker certificate time:

```
docker swarm update --cert-expiry 867240h0m0s
docker swarm ca --rotate
```

----End

18 Permissions Management

18.1 Creating a User and Granting Permissions for CBH Instances to It

To implement fine-grained permissions control for your CBH resources, **Identity and Access Management (IAM)** is exactly what you need. With IAM, you can:

- Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has their own security credentials, providing access to CBH resources.
- Grant only the permissions required for users to perform a task.
- Entrust an account or cloud service to perform professional and efficient O&M on your CBH resources.

If your account does not require individual IAM users, skip over this section.

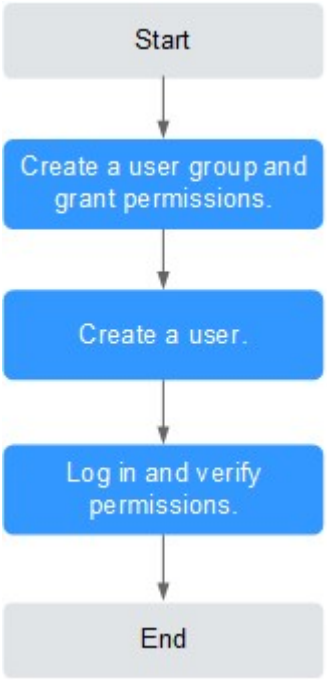
This section describes the procedure for granting permissions. **Figure 18-1** shows the process.

Prerequisites

Learn about the permissions supported by CBH and choose policies or roles based on your requirements. For more details, see **CBH Instance Permissions Management**.

Authorization Process

Figure 18-1 Process for granting permissions



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

   Create a user group on the IAM console, and attach the **CBH ReadOnlyAccess** policy to the group.

2. **Creating an IAM User**.

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

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

   Log in to the CBH console by using the created user, and verify that the user only has read permissions for CBH.

   - Choose **Service List** > **Cloud Bastion Host**. On the displayed page, click **Buy CBH Instance**. If a message is displayed indicating that you do not have the permission to buy the CBH instance (assume that the current permission contains only CBH ReadOnlyAccess), the CBH ReadOnlyAccess policy has taken effect.
   - Choose any other service in **Service List**. (Assume that the current permission contains only CBH ReadOnlyAccess). If a message appears indicating that you have insufficient permissions to access the service, the CBH ReadOnlyAccess policy has already taken effect.

18.2 Creating Custom Policies for CBH Instances

Custom policies can be created to supplement the system-defined policies of CBH. For the actions that can be added to custom policies, see **CBH Permissions and Supported Actions**.

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: Edit JSON policies from scratch or based on an existing policy.

For details, see **Creating a Custom Policy**. The following section contains examples of common custom policies for CBH instances.

Example Custom Policies

- Example 1: Allowing users to change CBH instance specifications and upgrade CBH instance version.

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "cbh:instance:upgrade",
            "cbh:instance:alterSpec"
         ]
      }
   ]
}
```

- Example 2: Denying a user request of restarting a CBH instance

  A deny policy must be used together with other policies. If the policies assigned to a user contain both Allow and Deny actions, the Deny actions take precedence over the Allow actions.

  The following method can be used to create a custom policy to disallow users who have the **CBH FullAccess** policy assigned to restart a CBH instance. Assign both **CBH FullAccess** and the custom policies to the group to which the user belongs. Then the user can perform all operations on CBH except restarting a CBH instance. The following is an example of a deny policy:

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Deny",
         "Action": [
            "cbh:instance:reboot"
         ]
      }
   ]
}
```

- Example 3: Defining permissions for multiple services in a policy

  A custom policy can contain the actions of multiple services that are of the global or project-level type. The following is an example policy containing actions of multiple services:

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "cbh:instance:create"
         ]
      },
      {
         "Effect": "Allow",
         "Action": [
            "vpc:subnets:get"
```



```
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ecs:cloudServerFlavors:get"
            ]
        }
    ]
}
```

18.3 Managing CBH Instance Permissions and Supported Actions

This section describes fine-grained permissions management for your CBH. If your account does not need individual IAM users, then you may skip over this section.

By default, new IAM users do not have any permissions assigned. You need to add a user to one or more groups, and assign permissions policies 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.

Permissions are classified into **roles** and **policies** based on the authorization granularity. Roles: A type of coarse-grained authorization mechanism that defines permissions related to user responsibilities. Policies: A type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions.

Supported Actions

CBH provides system-defined policies that can be directly used in IAM. You can also create custom policies and use them to supplement system-defined policies, implementing more refined access control.

- Permission: A statement in a policy that allows or denies certain operations.
- Action: Specific operations that are allowed or denied.

Table 18-1 Supported Actions (IAM 3.0)

Permission	API	Action	IAM Project	Enterprise Project
Querying total ECS quota	GET /v2/{project_id}/cbs/instance/ecs-quota	cbh:instance:getEcsQuota	√	×
Querying the AZ of a CBH instance	GET /v2/{project_id}/cbs/available-zone	cbh:instance:getAvailableZones	√	×

Permission	API	Action	IAM Project	Enterprise Project
Logging in to a CBH instance	POST /v2/{project_id}/cbs/instance/login	cbh:instance:login	√	×
Stopping a CBH instance	POST /v2/{project_id}/cbs/instance/stop	cbh:instance:stop	√	×
Restarting a CBH instance	POST /v2/{project_id}/cbs/instance/reboot	cbh:instance:reboot	√	×
Upgrading the CBH system version	POST /v2/{project_id}/cbs/instance/upgrade	cbh:instance:upgrade	√	×
Changing the password of the **admin** user for a CBH instance	PUT /v2/{project_id}/cbs/instance/password	cbh:instance:resetPassword	√	×
Starting a CBH instance	POST /v2/{project_id}/cbs/instance/start	cbh:instance:start	√	×
Expanding a CBH instance edition	PUT /v2/{project_id}/cbs/instance	cbh:instance:alterSpec	√	×
Creating a CBH instance	POST /v2/{project_id}/cbs/instance	cbh:instance:create	√	√
Binding or unbinding an EIP	• POST /v2/{project_id}/cbs/instance/{server_id}/eip/bind • POST /v2/{project_id}/cbs/instance/{server_id}/eip/unbind	cbh:instance:eipOperate	√	×

Permission	API	Action	IAM Project	Enterprise Project
Creating a CBH agency	POST /v2/{project_id}/cbs/agency/authorization	cbh:agency:authorize	√	×
Querying the CBH instance list	GET /v2/{project_id}/cbs/instance/list	cbh:instance:list	√	×
Changing the VPC a bastion host instance belongs to	PUT /v2/{project_id}/cbs/instance/vpc	cbh:instance:switchInstanceVpc	√	×
Logging in to a bastion host instance as user **admin**	GET /v2/{project_id}/cbs/instances/{server_id}/admin-url	cbh:instance:loginInstanceAdmin	√	×
Changing the type of a single-node CBH instance	PUT /v2/{project_id}/cbs/instance/type	cbh:instance:changeInstanceType	√	×
Obtaining the operation link for an asset managed by the bastion host	GET /v2/{project_id}/cbs/instance/get-om-url	cbh:instance:getOmUrl	√	×

Table 18-2 Supported Actions (IAM 5.0)

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Grants the permission to obtain the ECS quota.	GET /v2/{project_id}/cbs/instance/ecs-quota	cbh::getEcsQuota	ecs:cloudServerFlavors:get	√	×
Grants the permission to query the CBH instance quotas.	GET /v2/{project_id}/cbs/instance/quota	cbh::getQuota	-	√	×
Grants the permission to query the CBH status.	GET /v2/{project_id}/cbs/instance/{server_id}/status	cbh:instance:getInstanceStatus	-	√	×
Grants the permission to obtain the URLs for O&M of assets managed in CBH.	GET /v2/{project_id}/cbs/instance/get-om-url	cbh:instance:getOmUrl	-	√	×
Grants the permission to obtain the authorization information of the CBH service from the tenant.	GET /v2/{project_id}/cbs/agency/authorization	cbh::getAuthorization	• iam:agencies:listAgencies • iam:permissions:listRolesForAgencyOnProject	√	×
Grants the permission to query tags of CBH instances.	GET /v2/{project_id}/cbs/instance/{resource_id}/tags	cbh:instance:getInstanceTags	-	√	×
Grants the permission to start a CBH instance.	POST /v2/{project_id}/cbs/instance/start	cbh:instance:startInstance	-	√	×

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Grants the permission to disable a CBH instance.	POST /v2/{project_id}/cbs/instance/stop	cbh:instance:stopInstance	-	√	×
Grants the permission to restart a CBH instance.	POST /v2/{project_id}/cbs/instance/reboot	cbh:instance:rebootInstance	-	√	×
Grants the permission to upgrade a CBH instance.	POST /v2/{project_id}/cbs/instance/upgrade	cbh:instance:upgradeInstance	-	√	×
Grants the permission to roll back a CBH instance.	POST /v2/{project_id}/cbs/instance/rollback	cbh:instance:rollbackInstance	-	√	×
Grants the permission to log in to a CBH instance as an IAM user.	POST /v2/{project_id}/cbs/instance/login	cbh:instance:loginInstance	-	√	×
Grants the permission to reset a password for logging in to a CBH.	PUT /v2/{project_id}/cbs/instance/password	cbh:instance:resetInstancePassword	-	√	×
Grant the permission to switch the VPC of the bastion host instance.	PUT /v2/{project_id}/cbs/instance/vpc	cbh:instance:switchInstanceVpc	vpc:subnets:get	√	×
Grants the permission to reset the CBH instance login mode.	PUT /v2/{project_id}/cbs/instance/login-method	cbh:instance:resetInstanceLoginMethod	-	√	×

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Grants the permission to delete a faulty CBH instance.	DELETE /v2/{project_id}/cbs/instance	cbh:instance:deleteInstance	-	√	×
Grants the permission to change a CBH instance.	PUT /v2/{project_id}/cbs/instance	cbh:instance:alterInstance	-	√	×
Grants the permission to create a CBH instance.	POST /v2/{project_id}/cbs/instance	cbh:instance:createInstance	• vpc:quotas:list • vpc:subnets:list • vpc:subnets:get • vpc:securityGroups:get • ecs:cloudServerFlavors:get	√	√
Grants the permission to bind an EIP to a CBH instance.	POST /v2/{project_id}/cbs/instance/{server_id}/eip/bind	cbh:instance:bindInstanceEip	• eip:publicIps:list • eip:publicIps:update • eip:publicIps:get • eip:publicIps:associateInstance	√	×
Grants the permission to unbind an EIP from a CBH instance.	POST /v2/{project_id}/cbs/instance/{server_id}/eip/unbind	cbh:instance:unbindInstanceEip	• eip:publicIps:list • eip:publicIps:update • eip:publicIps:disassociateInstance	√	×

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Grants the permission to update the security group of a CBH instance.	PUT /v2/{project_id}/cbs/instance/{server_id}/security-groups	cbh:instance:updateInstanceSecurityGroup	• vpc:ports:update • vpc:securityGroups:list	√	×
Grants the permission to create or cancel the agency authorization for the CBH service.	POST /v2/{project_id}/cbs/agency/authorization	cbh::operateAuthorization	• iam:agencies:listAgencies • iam:permissions:listRolesForAgencyOnProject • iam:agencies:createAgency • iam:agencies:deleteAgency • iam:permissions:grantRoleToAgencyOnProject • iam:permissions:revokeRoleFromAgencyOnProject	√	×
Grants the permission to log in to a CBH instance as user **admin**.	GET /v2/{project_id}/cbs/instances/{server_id}/admin-url	cbh:instance:loginInstanceAdmin	-	√	×

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Grants the permission to modify the type of single-node CBH instances.	PUT /v2/{project_id}/cbs/instance/type	cbh:instance:changeInstanceType	• vpc:quotas:list • vpc:subnets:list • vpc:subnets:get • vpc:securityGroups:get • ecs:cloudServerFlavors:get	√	×
Grants the permission to query all AZs.	GET /v2/{project_id}/cbs/available-zone	cbh::listAvailableZones	-	√	×
Grants the permission to query the CBH specifications.	GET /v2/{project_id}/cbs/instance/specification	cbh::listSpecifications	-	√	×
Grants the permission to list CBH instances.	GET /v2/{project_id}/cbs/instance/list	cbh:instance:listInstances	eps:enterpriseProjects:list	√	×
Grants the permission to query all tags.	GET /v2/{project_id}/cbs/instance/tags	cbh::listTags	-	√	×
Grants the permission to search for instances by tag.	POST /v2/{project_id}/cbs/instance/filter	cbh:instance:listInstancesByTag	-	√	×

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Grants the permission to count the number of instances that meet the tag conditions.	POST /v2/{project_id}/cbs/instance/count	cbh:instance:countInstancesByTag	-	√	×
Grants the permission to operate the resource tags of the CBH instance.	POST /v2/{project_id}/cbs/instance/{resource_id}/tags/action	cbh:instance:operateInstanceTags	-	√	×

19 Monitoring

19.1 CBH Monitoring Metrics

Description

This topic describes metrics reported by a bastion host to Cloud Eye as well as their namespaces. You can use Cloud Eye to query the metrics of the monitored objects and alarms generated for your bastion hosts.

NOTICE

Only CBH V3.3.30 and later versions can be interconnected with Cloud Eye.

Namespaces

SYS.CBH

NOTE

A namespace is an abstract collection of resources and objects. Multiple namespaces can be created in a single cluster with the data isolated from each other. This enables namespaces to share the same cluster services without affecting each other.

Metrics

Table 19-1 Bastion host metrics

Metric ID	Metric Name	Description	Value Range	Unit	Number System	Dimension	Monitoring Period (Original Metric)
cpu_util	CPU Usage	Measures the CPU usage of the physical server accommodating the monitored ECS, which is not accurate as that obtained on the monitored ECS.	0%~100%	%	N/A	server_id	300s
mem_util	Memory Usage	Memory usage of the monitored object	0%~100%	%	N/A	server_id	300s
disk_util	Disk Usage	Disk usage of the monitored object	0%~100%	%	N/A	server_id	300s

Metric ID	Metric Name	Description	Value Range	Unit	Number System	Dimension	Monitoring Period (Original Metric)
session_count	Session Connections	Number of session connections of the monitored object	≥0	N/A	N/A	server_id	300s
resource_count	Managed Resources	Total number of resources managed by the monitored object	≥0	N/A	N/A	server_id	300s

Dimensions

Key	Value
server_id	CBH instance ID. To obtain this value, see **Checking Instance Details**.

19.2 Configuring Monitoring Alarm Rules

You can set bastion host alarm rules to customize the monitored objects and notification policies, and set parameters such as the alarm rule name, monitored object, metric, threshold, monitoring scope, and whether to send notifications. This helps you learn your bastion host status in a timely manner.

Prerequisites

A bastion host has been created.

Procedure

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

Step 2 Click in the upper left corner on the displayed page and select a region.

Step 3 In the navigation pane on the left, choose **Alarm Management** > **Alarm Rules**.

Step 4 In the upper right corner of the page, click **Create Alarm Rule**.

Step 5 Enter the alarm rule information by referring to **Table 19-2**. **Figure 19-1** shows an example.

Figure 19-1 Configuring CBH alarm rules

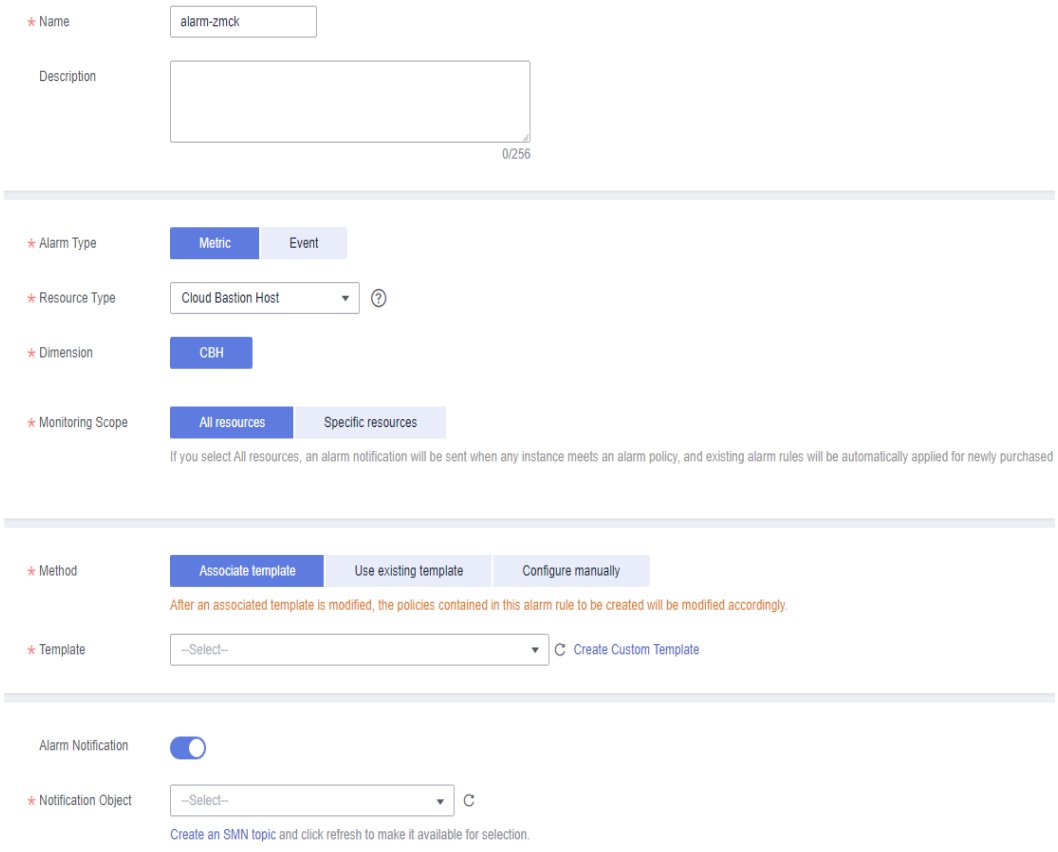


Table 19-2 Parameters for setting CBH alarm rules

Parameter	Description	Example Value
Name	Name of the rule. The system generates a random name and you can modify it.	alarm-lm45
Description	Description of the rule.	-
Alarm Type	Select **Metric**.	Metric

Parameter	Description	Example Value
Resource Type	Select a resource type. Select **Platform Bastion Host**.	Bastion host
Dimension	Select **CBH**.	CBH
Monitoring Scope	Scope where the alarm rule applies to. You can select **All resources**, **Resource groups** or **Specific resources**.	All resources
Method	You can select an associated template, use an existing template, or create a custom template.	Associate template
Template	Select a template from the drop-down list, for example, CBH alarm template.	-
Alarm Policy	Edit alarm policies.	-
Alarm Notification	Whether to notify users when alarms are triggered. Notifications can be sent by email, text message, or HTTP/HTTPS message.	Enabled
Notification Recipient	You can select a notification group or subscript to a topic.	Topic subscription

Parameter	Description	Example Value
Notification Object	Object that receives alarm notifications. You can select the account contact or a topic. • Account contact is the mobile phone number and email address provided for registration. • A topic is used to publish messages and subscribe to notifications. If the required topic is unavailable, create one and add subscriptions to it on the SMN console. For details, see **Creating a Topic** and **Adding Subscriptions**.	-
Notification Window	Cloud Eye sends notifications only within the notification window specified in the alarm rule.	00:00-8:00
Trigger Condition	Condition for triggering the alarm notification. Select **Generated alarm** when an alarm is generated or **Cleared alarm** when an alarm is triggered, or both.	-

Step 6 Click **Create**. In the displayed dialog box, click **OK**.

----End

19.3 Viewing Metrics

You can view bastion host metrics on the management console to learn about the protection status in a timely manner and set protection policies based on the metrics.

Prerequisites

CBH alarm rules have been configured in Cloud Eye. For more details, see **Configuring Monitoring Alarm Rules**.

Procedure

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

Step 2 Click  in the upper left corner on the displayed page and select a region.

Step 3 In the navigation pane on the left, choose **Cloud Service Monitoring** > **Cloud Bastion Host**.

Step 4 In the row containing the target CBH instance, click **View Metric** in the **Operation** column.

----End

20 Sharing

20.1 Sharing a VPC

Scenario

To use CBH to manage ECSs, the ECSs and the CBH instance you are using must be in the same VPC.

Creating a VPC

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

Step 2 In the navigation pane on the left, choose **Shared by Me** > **Resource Shares**. The **Resource Shares** page is displayed.

Step 3 Click **Create Resource Share** in the upper right corner.

Step 4 Set resource type to **vpc:subnet**, choose the corresponding region, and select the VPC to be shared. Click **Next: Associate Permissions**.

Step 5 On the **Associate Permissions** page, associate a RAM managed permission with each resource type, and then click **Next: Specify Principals** in the lower right corner.

Step 6 Specify the principals that you want to have access to the resources on the displayed page. Then, click **Next: Confirm** in the lower right corner.

Table 20-1 Description

Parameter	Description
Principal Type	• Organization For details about how to create an organization, see **Creating an Organization**. **NOTE** If you have not enabled resource sharing with organizations, this parameter cannot be set to **Organization**. For details, see **Enabling Sharing with Organizations**. • Huawei Cloud account ID

Step 7 Check the configurations and click **OK** in the lower right corner.

----End

Using a VPC

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

Step 2 Click  in the upper left corner on the displayed page and select a region.

Step 3 Click **Buy CBH Instance** to go to the **Buy CBH Instance** page.

Step 4 Select **CBH Instance** for **Service Type** and specify other parameters as required. For more information, see **Table 20-2**.

Table 20-2 CBH instance parameters

Parameter	Description
Billing Mode	The billing mode of the instance. Select **Yearly/Monthly**. Yearly/Monthly is a prepaid billing mode in which a CBH instance is billed based on the service duration. This cost-effective mode is ideal when the duration of CBH instance usage is predictable.
Instance Type	Select a single-node or primary/standby instance type based on your service requirements. • **Single-node**: Only one bastion host is available after the purchase. • **Primary/Standby**: After the purchase, two bastion hosts are delivered to form a two-node cluster. Once the primary bastion host is unavailable, the standby one takes over the job immediately. **NOTE** If you buy a primary/standby instance, do not disable HA, or logins will fail.

Parameter	Description
AZ	An AZ is the location where the bastion host instance you buy is deployed. **NOTE** Primary and standby hosts can be deployed in the same AZ or different AZs.
Instance Name	Name of the CBH instance.
Specifications	Specifications of your CBH instance. CBH provides **standard** and **professional** editions. Each edition has 50, 100, 200, 500, 1,000, 2,000, 5,000, and 10,000 asset specifications. Asset quantity indicates the maximum number of resources the instance you buy can manage and the maximum number of concurrent connections your instance can establish. The vCPUs and the size of data and system disks vary depending on the asset quantity. For example, if you select 100 assets, the number of resources your instance can manage and the maximum number of concurrent connections your instance can establish are both 100. **NOTE** Currently, primary/standby instances cannot manage public network resources using EIPs.
Storage Package	If you need more storage for a CBH instance, you can buy a storage package.
VPC	The Virtual Private Cloud (VPC) where your instance is located. Select a VPC in the current region. If no VPC is available in the current region, click **View VPC** and create one. **NOTE** • By default, networks in VPCs in different regions or even in the same region are not connected. Different networks are isolated from each other. This is not the case for different AZs in the same VPC. Two networks on the same VPC should be able to communicate with each other even if they are in different AZs. • CBH can directly access and manage resources, such as ECSs, in the same VPC in the same region. To manage resources such as ECSs in different VPCs in the same region, establish a VPC peering connection, use a VPN, or use other methods to connect networks. For details, see **Creating a VPC Peering Connection**. Managing ECSs across regions is not recommended. For more information, see **VPC Planning**.

Parameter	Description
Security Group	The security group for your CBH instance. The default security group is **Sys-default** in the current region. If no security group is available, click **Manage Security Groups** to create a security group or configure a new one. **NOTE** • A security group provides access rules for the CBH instances and resources that have the same security protection requirements and are mutually trusted in the same VPC. CBH instances are protected by these access rules after being added to the security group. For details, see • CBH instances and ECSs can be added to the same security groups. They do not affect each other when implementing security group rules. • For details about how to modify a security group, see **Changing Security Groups**. • Before creating HA instances, ensure that the security group allows inbound traffic from ports 22, 31036, 31679, and 31873. • During cross-version upgrade, ports 22, 31036, 31679, and 31873 are automatically enabled for the instance. After the upgrade, keep port 31679 enabled and disable other ports immediately if you do not need to use them. For more information about security groups, see **How Do I Configure a Security Group for a CBH Instance?**
Subnet	The subnet in the current VPC for your CBH instance. **NOTE** The selected subnet must be in the VPC network segment. For more information, see **Creating a VPC**.
Assign IPv4 Address	Select **Auto** or **Manual**. If you select **Manual**, you can view the used IP addresses.

Parameter	Description
EIP	(Optional) Select an EIP in the current region. If no EIP is available in the current region, click **Buy EIP** to create one. **NOTE** • If you select an EIP when purchasing an instance, but the EIP fails to be bound to the instance after the instance is in the running state, the EIP may have been bound to other servers while the instance is being created. In this case, bind another EIP to the instance by referring to **Binding an EIP to a CBH Instance**. • An EIP can be bound to only one cloud resource. A CBH instance cannot share an EIP with other cloud resources. After a CBH instance is created, the EIP will be used as the IP address for logging in to the CBH system. You need to create at least one EIP for a CBH instance. You can bind an EIP to the CBH instance now or later by referring to **Binding an EIP to a CBH Instance**. • To meet the requirements of the CBH system, set the EIP bandwidth to 5 Mbit/s or higher. • After the CBH instance is created, you can unbind the original EIP from the instance and bind a new EIP to it. For more information about EIPs, see **EIP Overview**.
Enterprise Project	Select the enterprise project the CBH instance you buy belongs to. The **default** enterprise project is selected by default.
Username	The default username is **admin**. **admin** is the system administrator account. This account has the highest operation permissions. Keep the account information secure.
Password	User-defined password of the **admin** user. **NOTE** • The password must meet the following requirements: – Contain 8 to 32 characters. – Contain at least three of the following types of characters: uppercase letters (A to Z), lowercase letters (a to z), digits (0 to 9), and following special characters: !@$%^-_=+[{}]:,./?~#* – Cannot contain the username or the username spelled backwards. – Cannot contain more than two consecutive identical characters. • You need to enter the same password in the **Password** and **Confirm Password** text boxes. • Your CBH system cannot obtain the password of the system administrator **admin**. Keep the account information secure. • When you log in to your CBH system as **admin** for the first time, change the password and configure mobile phone number as prompted. Otherwise, you cannot log in to the CBH system. • If you forget the password of user **admin** of the instance after you buy it, you can **reset the password**.
Required Duration	Required duration of the instance. You can buy a CBH instance on a monthly or yearly basis.

Parameter	Description
Tag	**Tags**: It is recommended that you use the TMS predefined tag function to add the same tag to different cloud resources. If your organization has configured a tag policy for CBH, you need to add tags in compliance with the policy. If a tag does not comply with the tag policies, CBH instances may fail to be created. Contact your organization administrator to learn more about tag policies.

----End

20.2 Sharing Resources

20.2.1 Overview

Based on Resource Access Manager (RAM), resource owners can configure the sharing permissions based on the least privilege principle and different usage requirements. Resource users can only access resources within their permissions, improving resource management security and user experience. For more information about RAM, see **What Is RAM?**

If your account is managed by Huawei Cloud organizations, you can enable this function to share resources more easily. If your account is in an organization, you can share resources with a specified account or all accounts in the organizations, needless to select all accounts one by one. For details, see **Enabling Sharing with Organizations**.

Constraints

- You must own the KMS key resources. You cannot share the KMS key resources that have been shared with you.
- If you need to share KMS key resources with your organization, enable this function. For more information, see **Enabling Sharing with Organizations**.

Key Owner and Recipient Permissions

Key owners can perform all operations on keys, while recipients can only perform certain operations. For details, see **Table 20-3**.

Table 20-3 Operations supported for key recipients

Role	Allowed Operation	Description
Recipient	kms:cmk:get	Access through the console or API
	kms:cmk:createDataKey	Access through API only

Role	Allowed Operation	Description
	kms:cmk:createDataKeyWithoutPlaintext	Access through API only
	kms:cmk:encryptDataKey	Access through API only
	kms:cmk:decryptDataKey	Access through API only
	kms:cmk:encryptData	Access through the console or API
	kms:cmk:decryptData	Access through the console or API
	kms:cmk:sign	Access through API only
	kms:cmk:verify	Access through API only
	kms:cmk:generateMac	Access through API only
	kms:cmk:verifyMac	Access through API only
	kms:cmk:getPublicKey	Access through the console or API
	kms:cmk:getRotation	Access through the console or API
	kms:cmk:getTags	Access through the console or API

Supported Resource Types and Regions

The following table lists the resource types and regions can be shared in DEW.

Table 20-4 Supported resource types and regions in DEW

Cloud Service	Resource Type	Supported Region
KMS	CMK	CN North-Beijing1 CN North-Beijing4 CN East-Shanghai1 CN East-Shanghai2 CN South-Shenzhen CN Southwest-Guiyang1 CN South-Guangzhou

Billing

For details about KMS billing, see **Billing Items**.

Owners of shared keys need to pay for the key instance and API calling fees, that is, only the resource owner will be charged for shared resources.

20.2.2 Sharing KMS Resources

Scenarios

To share your KMS resources with other accounts, create a resource share first. During the creation, you need to specify resources to be shared, configure permissions, specify users to be shared with, and confirm the configuration.

You can use shared KMS to encrypt the secrets and key pairs in DEW, and create an encryption task for instances in Relational Database Service (RDS), Document Database Service (DDS), and Object Storage Service (OBS).

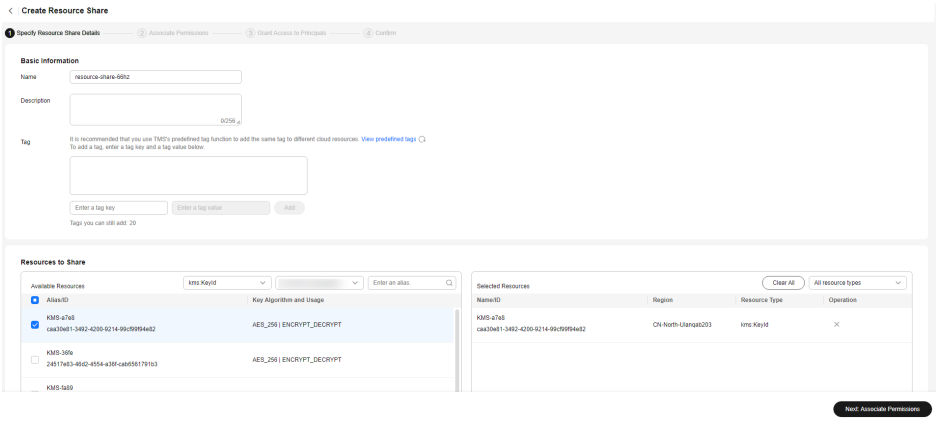
Creating Shared KMS Resources

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

Step 2 In the navigation pane on the left, choose **Shared by Me** > **Resource Shares**. The **Resource Shares** page is displayed.

Step 3 Click **Create Resource Share** in the upper right corner.

Figure 20-1 Specifying shared resources



Step 4 Set resource type to **kms:KeyId**, choose the corresponding region, and select keys to be shared. Click **Next: Associate Permissions**.

Step 5 Associate a RAM managed permission with each resource type on the displayed page. Then, click **Next: Specify Principals** in the lower right corner.

Step 6 Specify the target principals and click **Next: Confirm** in the lower right corner.

Table 20-5 Parameters

Parameter	Description
Principal Type	• Organization For details about how to create an organization, see **Creating an Organization**. **NOTE** If you have not enabled resource sharing with organizations, this parameter cannot be set to **Organization**. For details, see **Enabling Sharing with Organizations**. • Huawei Cloud account ID

Step 7 Check the configurations and click **Submit** in the lower right corner.

NOTE

After a shared instance is created, the organization accepts the instance automatically, while Huawei cloud accounts need to perform certain operations. For details, see **Responding to a Resource Sharing Invitation**.

----End

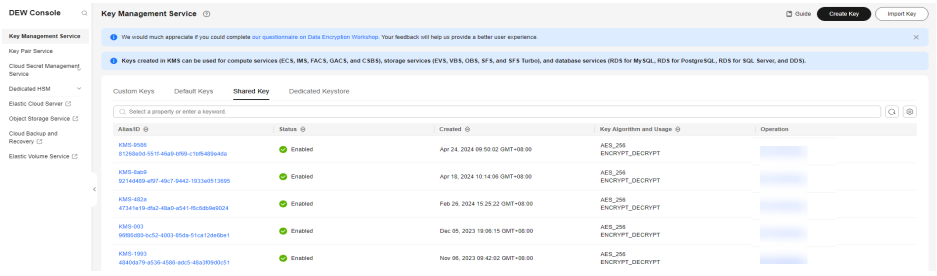
Viewing Shared KMS Resources

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

Step 2 Click  in the upper left corner on the displayed page and select a region.

Step 3 Check the shared key resources in the **Shared Key** tab.

Figure 20-2 Shared keys



NOTE

In the **Shared Key** tab, you can choose a scenario by entering the copied KMS encryption key ID.

----End

Using Shared KMS Resources

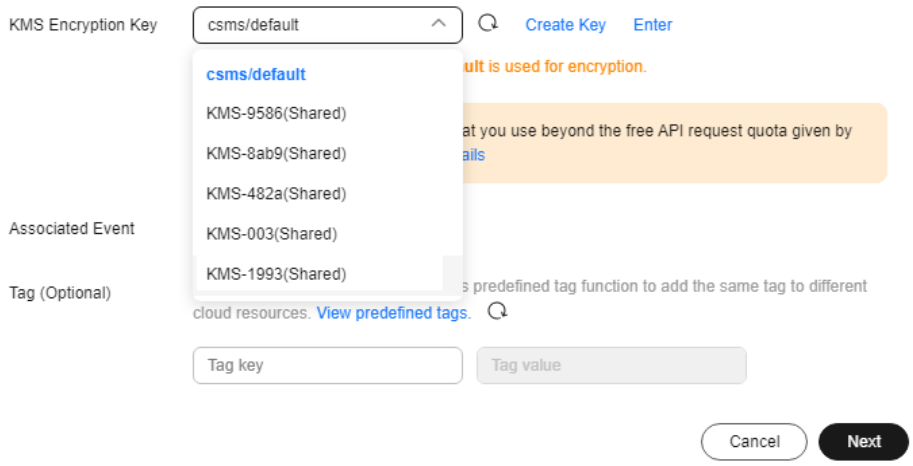
Step 1 **Log in to the DEW console.**

Step 2 Click in the upper left corner on the displayed page and select a region.

Step 3 In the navigation pane on the left, choose **Cloud Secret Management Service** > **Secrets**.

Step 4 Click **Create Secret**. On the displayed page, select or enter a shared key for **KMS Encryption Key**.

Figure 20-3 Selecting a shared key



NOTE

- When creating a key pair, you can select shared KMS keys.
- When creating an RDS, DDS, or OBS instance, you can choose shared KMS keys.

----End

20.2.3 Updating a Resource Share

You can update a resource share at any time, including updating its name, description, tags, shared resources, RAM managed permissions, and principals.

Procedure

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

Step 2 In the navigation pane on the left, choose **Shared by Me** > **Resource Shares**. The **Resource Shares** page is displayed.

Step 3 Select the resource share to be updated and click **Edit** in the **Operation** column.

Step 4 Update the resource share on the displayed page. You can modify its name, description, tags, and add or delete shared resources.

Step 5 After the update is complete, click **Next: Associate Permissions** in the lower right corner.

Step 6 Add or delete the permissions supported by **kms:KeyId**. Wait until the update is complete, click **Next: Grant Access to Principals**.

Step 7 On the displayed page, add or delete principals based on your needs. Then, click **Next: Confirm** in the lower right corner.

Step 8 Confirm the configurations and click **OK** in the lower right corner.

----End

20.2.4 Leaving a Resource Share

If you no longer need to access shared key resources, you can leave at any time. After leaving the share, you cannot access the shared keys.

Procedure

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

Step 2 In the navigation pane on the left, choose **Shared by Me** > **Resource Shares**. The **Resource Shares** page is displayed.

Step 3 In the **Accepted Resource Shares** tab, locate the target instance, and click **Leave** in the **Operation** column.

Step 4 Click **Leave** in the displayed dialog box.

----End

