Cloud Bastion Host (CBH)

User Guide

Date **2024-03-25**

Contents

1 Instances

1.1 Permissions Management

1.1.1 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.

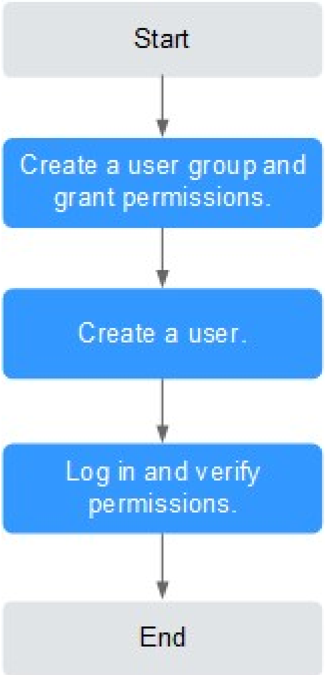
This section describes the procedure for granting permissions. **Figure 1-1** shows the process.

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 1-1 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 **Purchase CBH Instance**. If a message is displayed indicating that you do not have the permission to purchase 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.

1.1.2 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"
            ]
        }
    ]
}
```

1.1.3 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 1-1 Supported Actions

Permission	Action
Creating a CBH instance	cbh:instance:create
Changing CBH instance specifications	cbh:instance:alterSpec
Querying the CBH instance list	cbh:instance:list
Upgrading the CBH system version	cbh:instance:upgrade
Querying total ECS quota	cbh:instance:getEcsQuota
Binding or unbinding an EIP	cbh:instance:eipOperate
Restarting a CBH instance	cbh:instance:reboot
Starting a CBH instance	cbh:instance:start
Stopping a CBH instance	cbh:instance:stop

Permission	Action
Querying the AZ of a CBH instance	cbh:instance:getAvailableZones
Checking whether an IPv6 CBH instance can be created	cbh:instance:checkIpv6
Checking network connection between the CBH instance and the license center	cbh:network:check
Modifying the network of the CBH instance to ensure that the CBH instance can communicate with the license center	cbh:network:change

1.2 Purchasing 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, create a CBH account on the CBH instance you purchased, log in to the CBH system mapped to the CBH instance, and configure the O&M system.

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.

Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page, select a region, and choose **Security & Compliance** > **Cloud Bastion Host** to go to the CBH instance management console.

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

Step 4 Select **CBH Instance** for **Service Type** and specify other parameters as required. For more information, see **Table 1-2**.

Table 1-2 Parameters for purchasing a CBH instance

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Billing Mode</td><td>The billing mode of the CBH 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.</td></tr>
<tr><td>Region</td><td rowspan="4">The region and AZ where the CBH instance is located. You also need to specify enterprise project your instance belongs to.
Select an instance type based on your service requirements. Currently, CBH provides single-node instances and primary/standby instances for H/A deployments.
NOTE
• If you select Primary/Standby for Instance Type, you need to specify the primary AZ and standby AZ.
• If you purchase a primary/standby instance, do not disable HA, or logins to the CBH instance will fail.
Select a region nearest to your ECSs, RDS instances, BMSs to reduce network latency and accelerate service access.</td></tr>
<tr><td>Project</td></tr>
<tr><td>Instance Type</td></tr>
<tr><td>AZ</td></tr>
<tr><td>Instance Name</td><td>Name of the CBH instance.</td></tr>
<tr><td>Edition</td><td>Specifications of your CBH instance.
CBH provides the standard and professional editions. Each edition has 50, 100, 200, 500, 1000, 2000, 5,000, and 10,000 asset specifications.
NOTE
Currently, primary/standby instances cannot manage public network resources using EIPs.</td></tr>
<tr><td>VPC</td><td>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 or use a VPN to connect networks. For details, see Creating a VPC Peering Connection. Managing ECSs across regions is not recommended.
For more information, see VPC Planning.</td></tr>
</table>

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Security Group</td><td>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
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.
When a CBH instance is created, ports 80, 8080, 443, and 2222 are automatically enabled. If you do not need to use them, disable them immediately after the instance is created.
During cross-version upgrade, ports 22, 31036, 31679, and 31873 are automatically enabled for the instance. If you do not need to use these ports, disable them immediately after the upgrade.
For more information about security groups, see How Do I Configure a Security Group for a CBH Instance?</td></tr>
<tr><td>Subnet</td><td>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.</td></tr>
<tr><td>Assign IPv4 Address</td><td>Select Auto or Manual.
If you select Manual, you can view the used IP addresses.</td></tr>
<tr><td>EIP</td><td>(Optional) Select an EIP in the current region.
If no EIP is available in the current region, click Purchase EIP to create one.
NOTE
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.</td></tr>
</table>

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Enterprise Project</td><td>Select the enterprise project the CBH instance belongs to.
The default enterprise project is selected by default.</td></tr>
<tr><td>Username</td><td>The default username admin is used.
admin is the system administrator account. This account has the highest operation permissions. Keep the account information secure.</td></tr>
<tr><td>Password</td><td>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.
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 after a CBH instance is purchased, you can reset the password.</td></tr>
<tr><td>Required Duration</td><td>Required duration of the instance
You can buy a CBH instance on a monthly or yearly basis.</td></tr>
<tr><td>Tag</td><td>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.</td></tr>
</table>

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 can be issued after purchase.

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 Make your purchase and return to the CBH console. Check the newly purchased instance in the CBH instance list.

After a CBH instance is purchased, a mapped CBH system is automatically created for you, which takes about 10 minutes.

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 creation**, view the failure cause in the displayed dialog box. Then, click **Service Ticket** in the upper right corner of the management console, fill in the service ticket, and submit the service ticket.
- 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.

1.3 Viewing CBH 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.

Viewing CBH Instance Information

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page, select a region, and choose **Security & Compliance** > **Cloud Bastion Host** to go to the CBH instance management console.

Step 3 Click the instance to view the instance details.

Table 1-3 Instance parameters

Parameter	Description
Instance Name	Instance name you specify. It cannot be modified after the instance is created.
Instance Type	Instance type you select.

Parameter	Description
VPC	VPC of the instance
Security group	Virtual network security rule.
Enterprise Project	Enterprise project that the instance belongs to.
AZ	AZ where the instance resides.
Instance ID	Unique ID of the instance, which is automatically generated.
Specifications	Edition you select for your instance.
Created	Time when a CBH instance was successfully purchased.
Subnet	Subnet of the VPC
Instance Version	CBH system version of the CBH instance.

----End

1.4 Changing Specifications of a CBH Instance

If the specifications (or edition) of your CBH instance cannot meet your requirements, you can upgrade the specifications of the instance. For example, you can purchase 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 specifications 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 seven types of asset specifications.
- You can scale up the specifications. Scaling down specifications is not supported.

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.

  If you want to change your CBH specifications to that of a professional one, upgrade your CBH system version to 3.2.16.0 or later. To view the CBH version you are using, see **About System**.

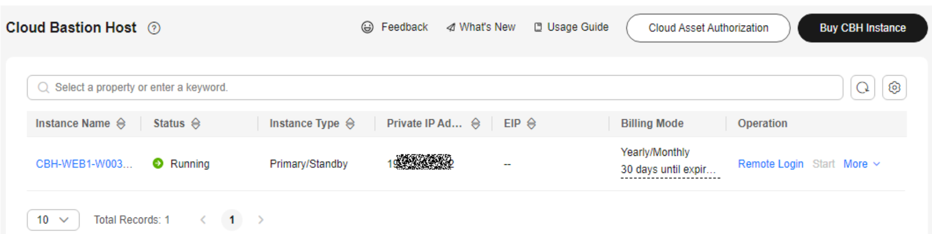
Procedure

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, click and choose **Security & Compliance** > **Cloud Bastion Host** to go to the CBH console.

Figure 1-2 Instances



Step 4 Locate the row containing the instance you want to expand. In the **Operation** column, choose **More** > **Expand** > **Change Specifications**.

Step 5 On the **Change Edition** page, set **Edition** and click **Next**.

Step 6 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 7 Complete the payment.

It takes about 30 minutes for the specification change to complete. During this period, the status of the CBH instance changes from **Changing** to **Restarting**.

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

----End

1.5 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.

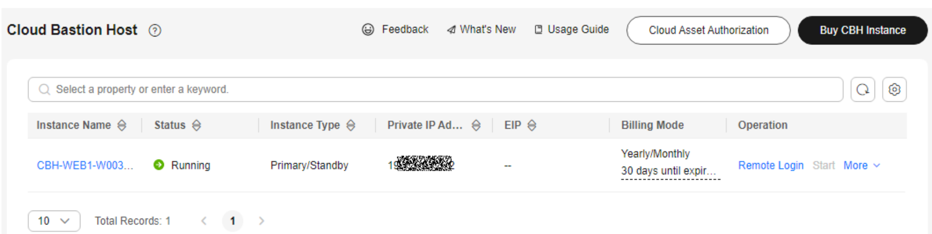
Procedure

Step 1 Log in to the management console.

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

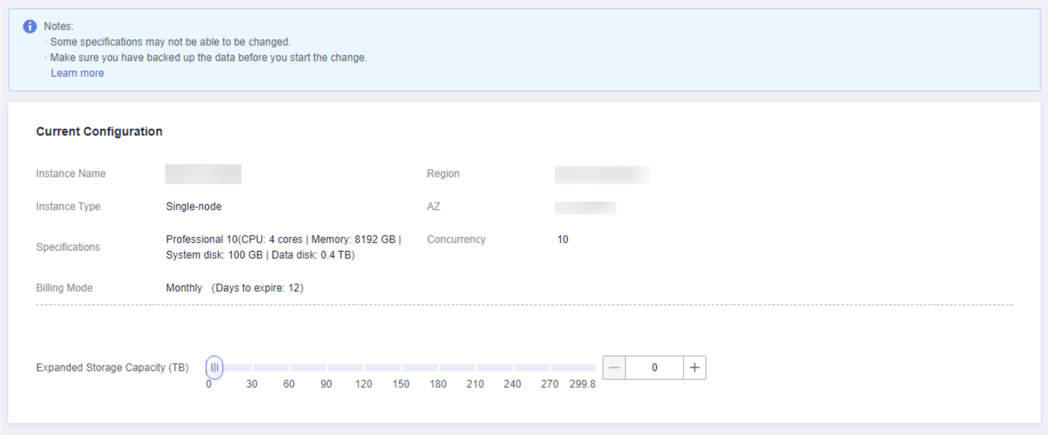
Step 3 In the navigation pane on the left, click and choose **Security & Compliance** > **Cloud Bastion Host** to go to the CBH console.

Figure 1-3 Instances



Step 4 Locate the row containing the instance you want to expand. In the **Operation** column, choose **More** > **Expand** > **Expand Storage**.

Figure 1-4 Expand storage



Step 5 Select the storage space you want to expand, confirm the billing mode and storage space, and then click **Next**.

Step 6 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 7 Complete the payment.

Step 8 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 9 When the CBH instance status changes to **Running**, the CBH system is available.

----End

1.6 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.

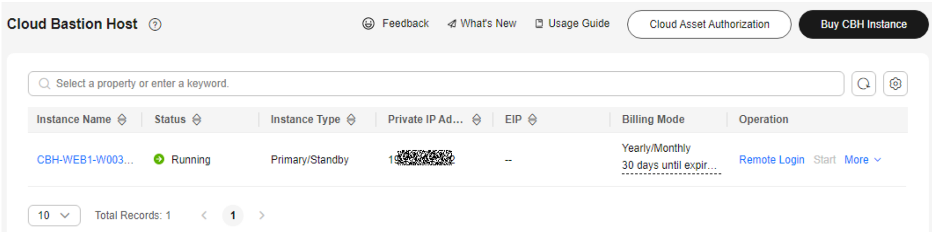
Procedure

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, click and choose **Security & Compliance** > **Cloud Bastion Host** to go to the CBH console.

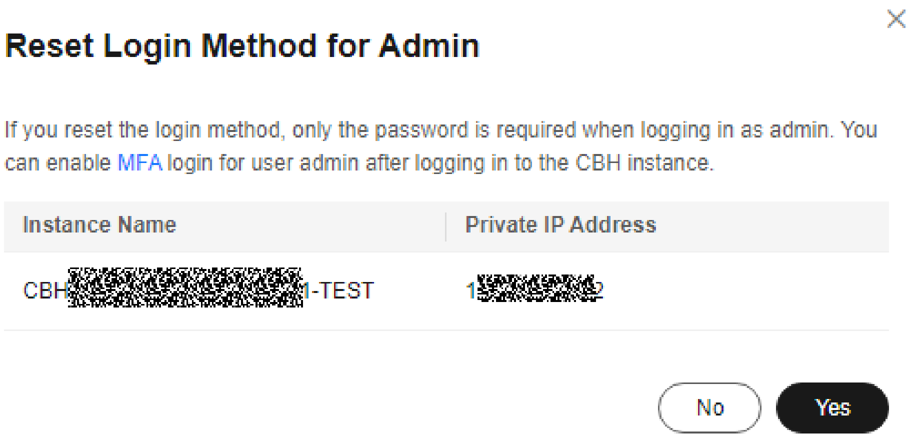
Figure 1-5 Instances



Step 4 Locate the row containing the instance for which you want to reset login passwords. In the **Operation** column, choose **More** > **Reset** > **Reset Login Method for Admin**.

Step 5 In the displayed dialog box, click **OK** to reset the login method for user **admin**.

Figure 1-6 Resetting login method for user **admin**



NOTE

After the login method is reset, a password is required for user **admin** to log in to the CBH system. For details, see **Configuring Multifactor Verification**.

----End

1.7 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?**

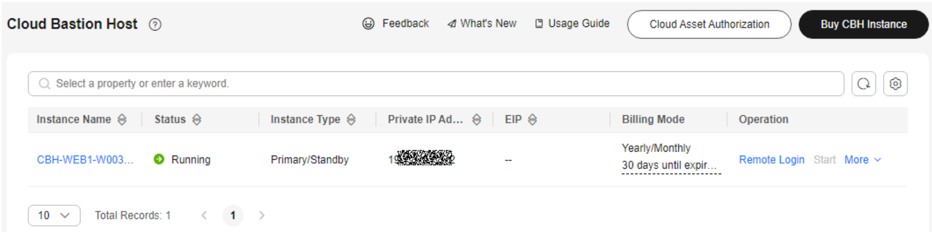
Procedure

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, click ☰ and choose **Security & Compliance** > **Cloud Bastion Host** to go to the CBH console.

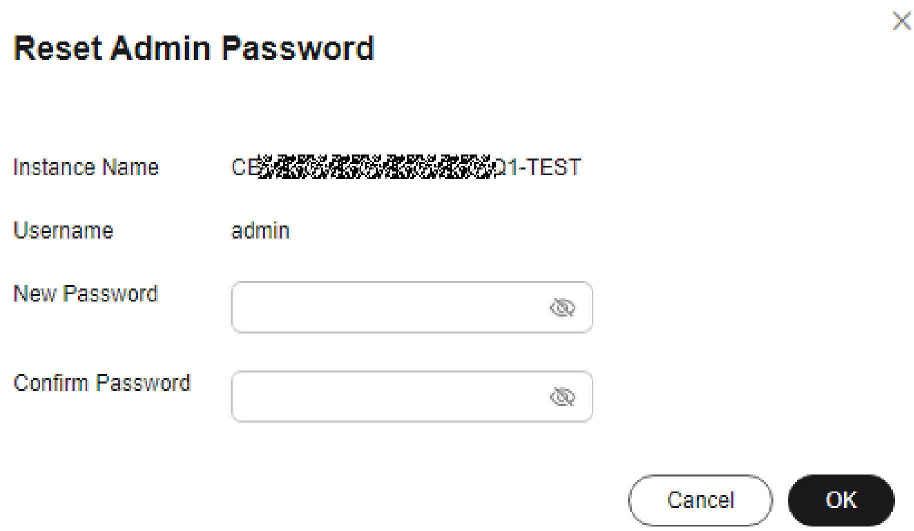
Figure 1-7 Instances



Step 4 Locate the row containing the instance you want to restart. In the **Operation** column, choose **More** > **Reset** > **Reset Admin Password**.

Step 5 In the dialog box displayed, reset the password of the admin account.

Figure 1-8 Resetting a password



Step 6 Click **OK**.

----End

1.8 Upgrading the CBH System Version

A CBH system of the latest version has system optimizations or new functions. To use those functions, upgrade your instances in a timely manner.

Precautions

- Before the upgrade

  Back up data to ensure a quick rollback in case of upgrade failures. For details, see **Which Types of System Data Can Be Backed Up in the CBH System?**

- 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 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.

- Rolling Back the 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 changes to **Rolling back edition**.

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

⚠ CAUTION

- If you plan a scale-out task after an upgrade, start the scale-out task 5 minutes later when the upgrade is finished.
- A scheduled upgrade must be set at least one day before the actual upgrade time. You are advised to upgrade the service during idle hours.
- To upgrade the service to the latest version, version 3.3.37.0 and earlier must be upgraded to 3.3.37.3 first, and versions earlier than 3.3.50.0 must be upgraded to 3.3.50.2 first.
- During the minor version upgrade (upgrading 3.3.37.0 or earlier to 3.3.37.3, and 3.3.50.0 or earlier to 3.5.50.2), manual rollback cannot be performed.
- If a scheduled upgrade is set, you cannot shut down, restart, change, or expand the capacity of the basion host.
- Before the upgrade starts, you can cancel the scheduled upgrade and reset the upgrade time.
- During the cross-version upgrade, you can manually roll back the version.
- There is a seven-day retention period for cross-version upgrades. You can roll back a cross-version upgrade within seven days after the upgrade. No rollbacks are allowed once the retention period expires. So, you need to verify the upgrade in a timely manner.
- If specification change or scale-out tasks are performed after an upgrade, no rollbacks can be performed. So, do not perform any specification change or scale-out operations until you verify the upgrade.
- 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. If you do not need to use these ports, disable them immediately after the upgrade.
- If a web certificate has been imported for an instance, import the certificate again after the cross-version upgrade for the instance.

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**.

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?**

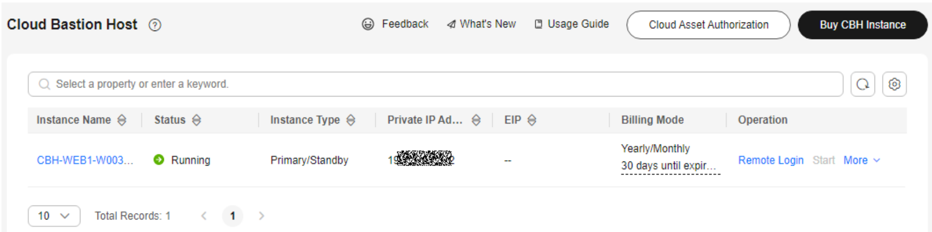
Procedure

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, click and choose **Security & Compliance** > **Cloud Bastion Host** to go to the CBH console.

Figure 1-9 Instances



Step 4 Locate the row containing the instance you want to upgrade. In the **Operation** column, choose **More** > **Upgrade** > **Upgrade Edition**.

Step 5 In the displayed dialog box, select the schedule upgrade time and enter **UPGRADE** to confirm. To cancel the upgrade schedule, enter **CANCEL** in the dialog box. You can also change the upgrade schedule you set before.

NOTE

Upgrade types:

- During a minor version upgrade, the CBH instance you are using will be interrupted. It takes about 15 to 30 minutes to complete the upgrade.
- 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 6 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 7 When the CBH instance status changes to **Running**, the CBH system is available.

NOTE

After the upgrade completes, you can verify the upgrade. To do so, click the instance name in the **Instance Name** column. On the displayed page, check the instance version. If the instance version has not changed, the upgrade fails. In this case, contact technical support.

For details about how to query the version of the upgraded CBH system, see **Device System** in **About System**.

----End

1.9 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.

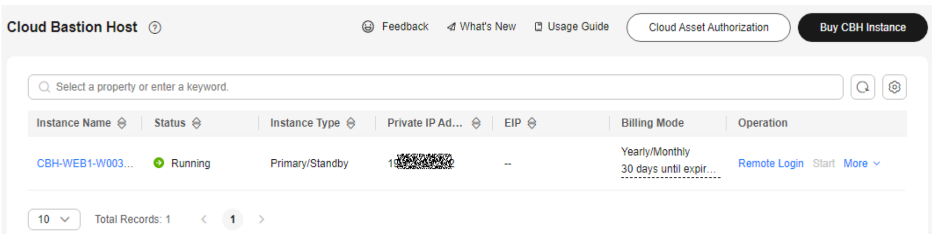
Procedure

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, click and choose **Security & Compliance** > **Cloud Bastion Host** to go to the CBH console.

Figure 1-10 Instances



Step 4 Locate the row containing the instance you want to start. In the **Operation** column, click **Start**.

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

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

----End

1.10 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.

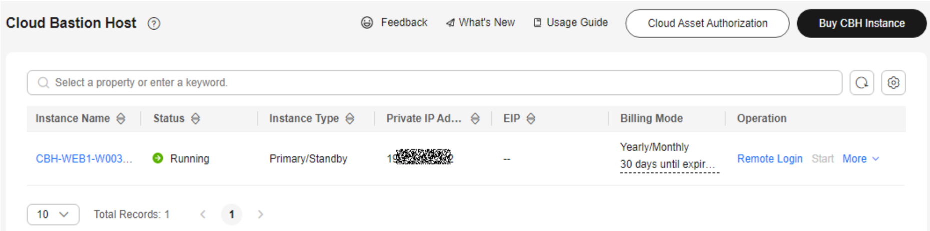
Procedure

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, click and choose **Security & Compliance** > **Cloud Bastion Host** to go to the CBH console.

Figure 1-11 Instances



Step 4 Locate the row containing the instance you want to stop. In the **Operation** column, choose **More** > **Stop**.

Step 5 In the displayed dialog box, click **OK**. After the CBH instance is stopped, its **Status** changes to **Stopped**.

NOTE

To forcibly stop an instance, select the **Forcibly stop** check box in the displayed dialog box. Forcibly stopping an instance may cause data loss. Ensure that all data files have been saved before performing this operation.

----End

1.11 Restarting a CBH Instance

If your CBH system becomes abnormal, you can try restarting the mapped CBH instance.

- You can restart a CBH instance in the **Running** status.
- Restarting a CBH instance will interrupt services of the mapped CBH system for about 5 minutes. During this period, the instance status is **Restarting**.
- The CBH system will be unavailable when the mapped CBH instance is being restarted.

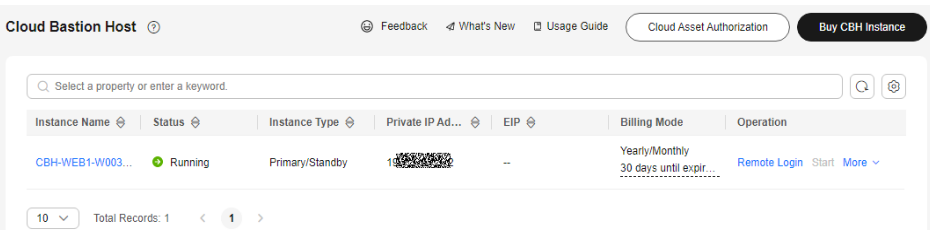
Procedure

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, click and choose **Security & Compliance** > **Cloud Bastion Host** to go to the CBH console.

Figure 1-12 Instances



Step 4 Locate the row containing the instance you want to restart. In the **Operation** column, choose **More** > **Restart**.

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

The restart process usually takes about 5 minutes. During the restart, the CBH instance will be in the **Restarting** status.

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

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

NOTE

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

----End

1.12 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.

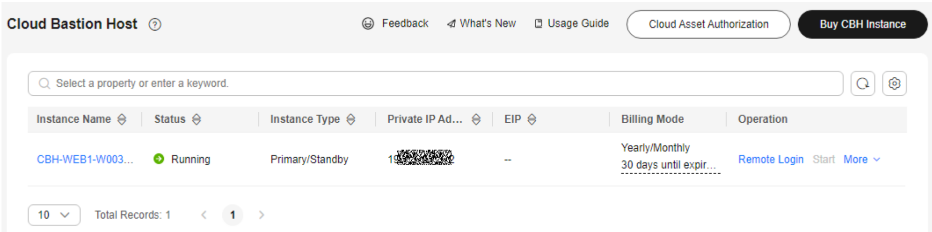
Procedure

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, click and choose **Security & Compliance** > **Cloud Bastion Host** to go to the CBH console.

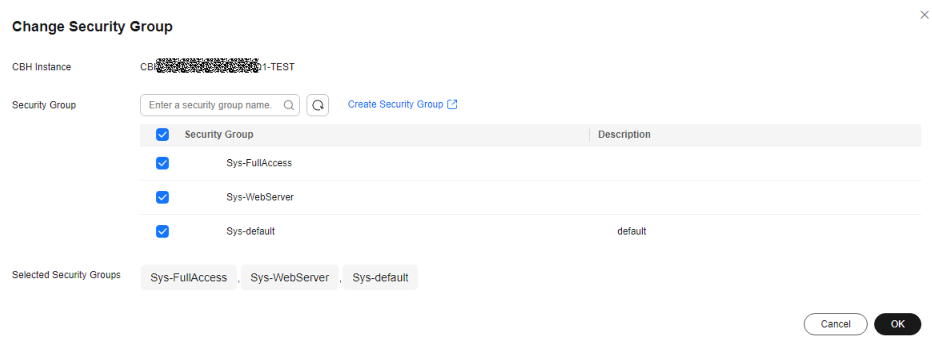
Figure 1-13 Instances



Step 4 Locate the row that contains the target instance. In the **Operation** column, choose **More** > **Configure Network** > **Change Security Group**.

Step 5 In the displayed dialog box, select the security group you want to configure for the instance.

Figure 1-14 Change Security Group



Step 6 Click **Yes**.

----End

1.13 Binding an EIP to a CBH Instance

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

- Log in to the CBH system using a web browser. URL: https:// *EIP of the CBH 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 EIP is bound to a CBH instance, operations such as changing the version specifications, upgrading the version, starting or restarting the instance, and renewing the instance will fail.

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 to purchase CBH instances and EIPs to be bound to them, and the instances and EIPs must be in the same region.

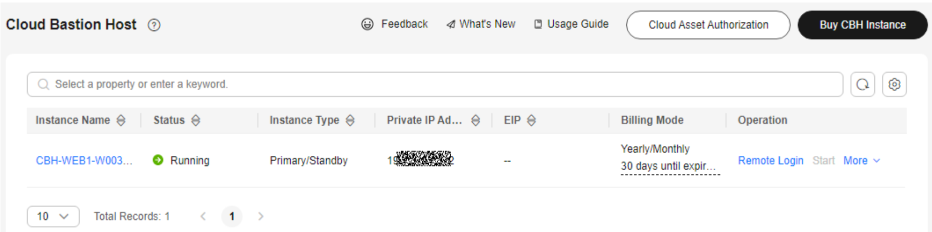
Procedure

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, click the menu icon and choose **Security & Compliance** > **Cloud Bastion Host** to go to the CBH console.

Figure 1-15 Instances



Step 4 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 5 In the displayed dialog box, select an EIP in the **Unbound** status and click **OK**.

After the binding is successful, the **Login** button will be enabled. You can check the bound EIP in the **EIP** column.

NOTE

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

----End

1.14 Unbinding an EIP from a CBH Instance

To bind another EIP to a CBH instance or release an EIP that has been bound to a CBH 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.

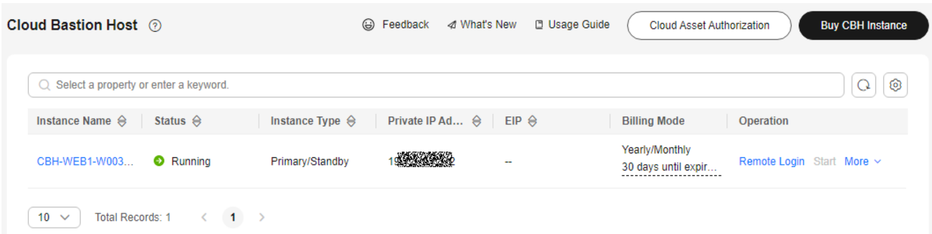
Procedure

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, click and choose **Security & Compliance** > **Cloud Bastion Host** to go to the CBH console.

Figure 1-16 Instances



Step 4 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 5 In the displayed dialog box, click **OK**.

After the EIP is unbound, no IP address is displayed in the **EIP** column, and the **Login** button is disabled.

----End

1.15 Allowing Access to Cloud Assets

In CBH, you can use the secrets managed by Cloud Secret Management Service (CSMS).

NOTICE

After you authorize CBH to access CSMS secrets and KMS keys, it takes about 10 minutes before the bastion host can obtain the delegation token.

For details about how to create a secret, see **Data Encryption Workshop - Credential Management**.

For secrets invoked through the bastion host, the account and password must comply with **Key** specifications.

Example:

username:root

password:*****

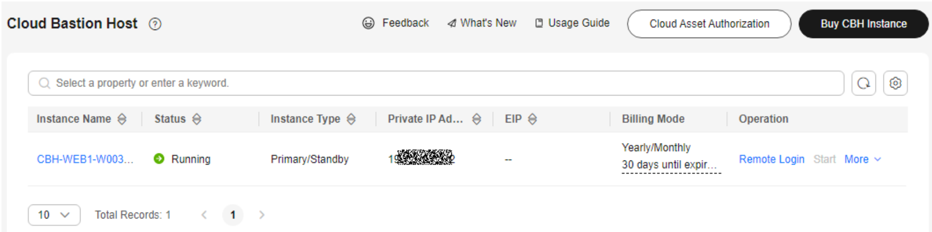
Procedure

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, click and choose **Security & Compliance** > **Cloud Bastion Host** to go to the CBH console.

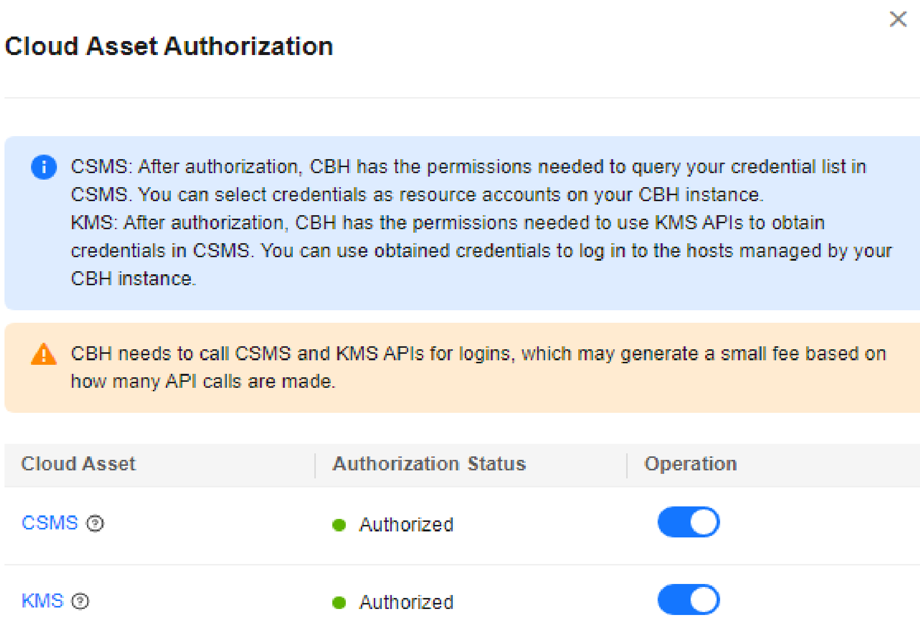
Figure 1-17 Instances



Step 4 Click **Cloud Asset Authorization** in the upper right corner.

Step 5 In the displayed dialog box, switch to  in the **Operation** column. Enable **CSMS** and **KMS** authorization.

Figure 1-18 Cloud asset authorization



Step 6 For details about how to add a resource account, see **Adding Accounts of Managed Host or Application Resources into CBH**.

----End

1.16 Renewing a CBH Instance

To ensure that your CBH system is available all the time, 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.

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.

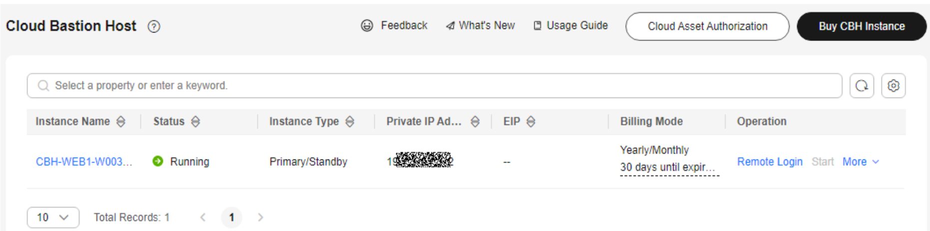
Procedure

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, click and choose **Security & Compliance** > **Cloud Bastion Host** to go to the CBH console.

Figure 1-19 Instances



Step 4 Click the instance you want to renew, choose **More** > **Renew** in the **Operation** column, and select the renewal method you want.

Step 5 Select the renewal duration as needed.

Step 6 Click **Pay** and complete the payment.

Step 7 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

1.17 Unsubscribing from a CBH 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.

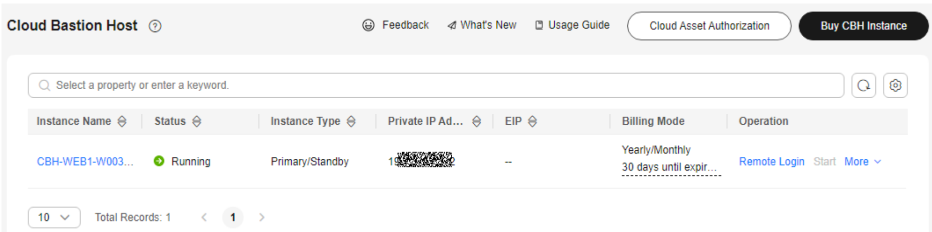
Procedure

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, click and choose **Security & Compliance** > **Cloud Bastion Host** to go to the CBH console.

Figure 1-20 Instances



Step 4 Locate the row containing the instance you want to unsubscribe from. In the **Operation** column, choose **More** > **Unsubscribe**.

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

Step 6 Complete the unsubscription.

----End

1.18 Key CBH Instance Operations Recorded by CTS

1.18.1 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 1-4** lists the CBH instance operations that can be recorded by CTS.

Table 1-4 CBH instance operations

Operation	Resource Type	Trace Name
Creating a CBH	cbh	createInstance
Deleting a CBH	cbh	deleteInstance
Restarting a CBH	cbh	rebootCBH
Starting a CBH	cbh	startCBH
Stopping a CBH	cbh	stopCBH
Submitting a CBH order	cbh	subscribeOrder
Updating a CBH order	cbh	updateCloudServiceType
Updating CBH metadata	cbh	updateMetadata
Querying the job synchronization	cbh	jobsAsynQuery
Upgrading a CBH instance	cbh	upgradeInstance

1.18.2 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 management console.

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

Step 3 Under **Management & Governance**, click **Cloud Trace Service**.

Step 4 On the left navigation pane, choose **Trace List**.

Step 5 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 6 Click on the left of the trace to be queried to extend its details.

Step 7 Click **View Trace** in the **Operation** column for details.

----End

2 Logging In to the CBH System

2.1 Overview

Port Requirements

To use the CBH system for resource management, ensure that the communication between the CBH system and the managed resources is enabled. Before you start, check whether your network ACL configuration allows access to CBH and configure the security group of the mapped CBH instance by referring to **Table 2-1**.

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. If you do not need to use these ports, disable them immediately after the upgrade.

Table 2-1 Inbound and outbound rule configuration reference

Scenario Description	Direction	Protocol/ Application	Port
Accessing CBH through a web browser (HTTP and HTTPS)	Inbound	TCP	80, 443, and 8080
Accessing a CBH system through Microsoft Terminal Services Client (MSTSC)	Inbound	TCP	53389
Accessing a CBH Instance Through an SSH Client	Inbound	TCP	2222

Scenario Description	Direction	Protocol/ Application	Port
Accessing CBH instances through FTP clients	Inbound	TCP	20~21
Remotely accessing Linux ECSs of CBH instances over SSH clients	Outbound	TCP	22
Remotely accessing Windows ECSs of CBH instances over the RDP Protocol	Outbound	TCP	3389
Accessing Oracle databases through CBH instances	Inbound	TCP	1521
Accessing Oracle databases through CBH instances	Outbound	TCP	1521
Accessing MySQL databases through CBH instances	Inbound	TCP	33306
Accessing MySQL databases through CBH instances	Outbound	TCP	3306
Accessing SQL Server databases through CBH instances	Inbound	TCP	1433
Accessing SQL Server databases through CBH instances	Outbound	TCP	1433
Accessing DB databases through CBH instances	Inbound	TCP	50000
Accessing DB databases through CBH instances	Outbound	TCP	50000
Accessing GaussDB databases through CBH	Inbound	TCP	18000
Accessing GaussDB databases through CBH	Outbound	TCP	18000
License servers	Outbound	TCP	9443
Cloud services	Outbound	TCP	443
Accessing a CBH system through the SSH client in the same security group	Outbound	TCP	2222
SMS service	Outbound	TCP	10743 and 443
Domain name resolution service	Outbound	UDP	53

Verification Type

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

Table 2-2 Authentication methods

Verification Type	Authentication Description
Local Authentication	Static passwords configured for the CBH 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 through CBH. 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 CBH system.
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 CBH system.
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 CBH system.
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 CBH system.

Logon Type

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

Table 2-3 Login method description

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

2.2 Using a Web Browser to Log In to a CBH System

You can use mainstream browsers to log in to a CBH system 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.

Browser-based logins can be authenticated by password, SMS message, mobile OTP, USB key, or OTP token.

NOTE

- First-time login users are required to bind a mobile number for password resetting.
- 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 PBH). If you select **IAM Login** or **Admin Login**, no password is required.

Prerequisites

An EIP has been bound to the CBH instance.

Procedure

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

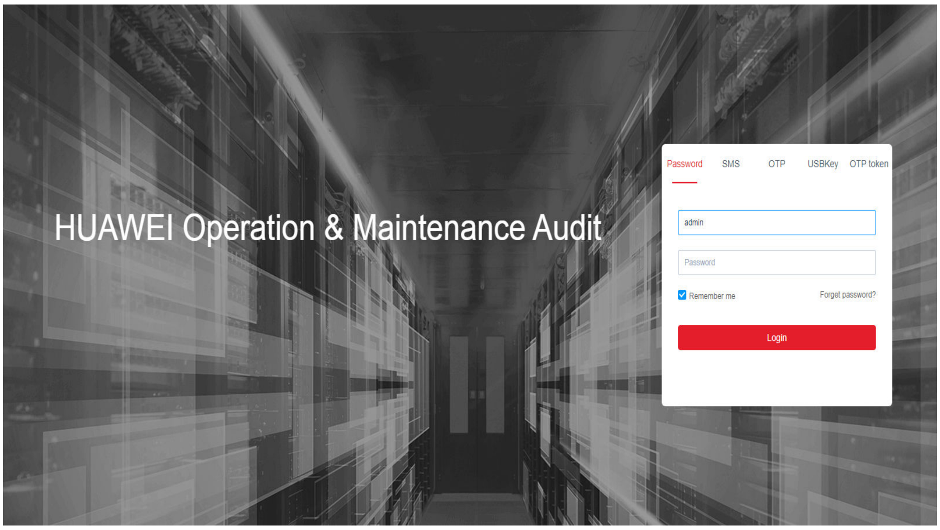
URL: https:// *EIP of PBH*, for example, *https://10.10.10.10*.

NOTE

Use supported browsers to access CBH. 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 authentication method.

Figure 2-1 CBH system login page



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

The following content walks you through how to log in to your CBH system using different authentication methods.

----End

Using Static Passwords for Logging

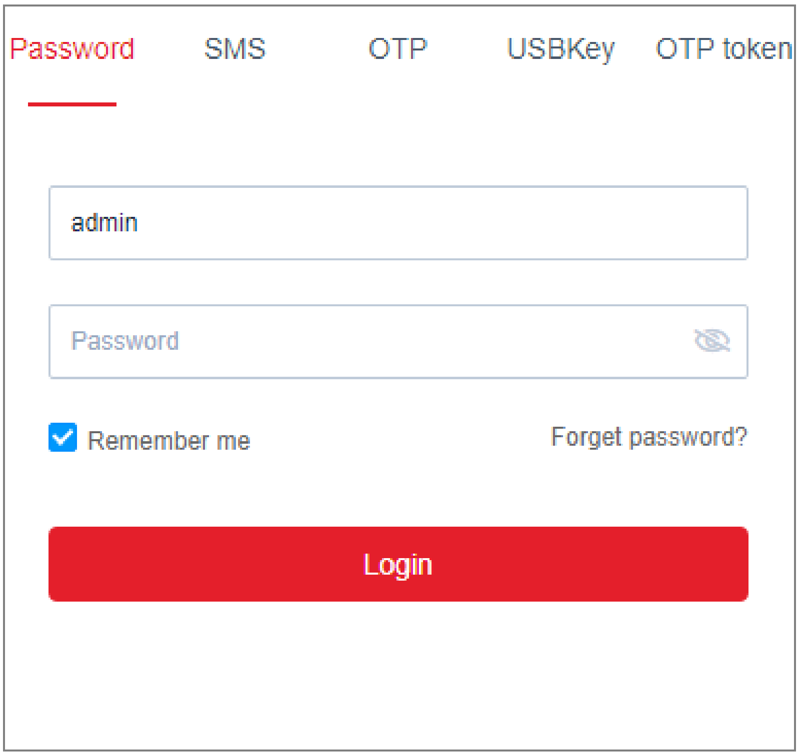
Step 1 Select **Password**.

Step 2 Enter the username and password of your PBH account.

Step 3 Click **Login**.

----End

Figure 2-2 Password authentication



Using SMS Verification for Logging

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

Step 1 Select **SMS**.

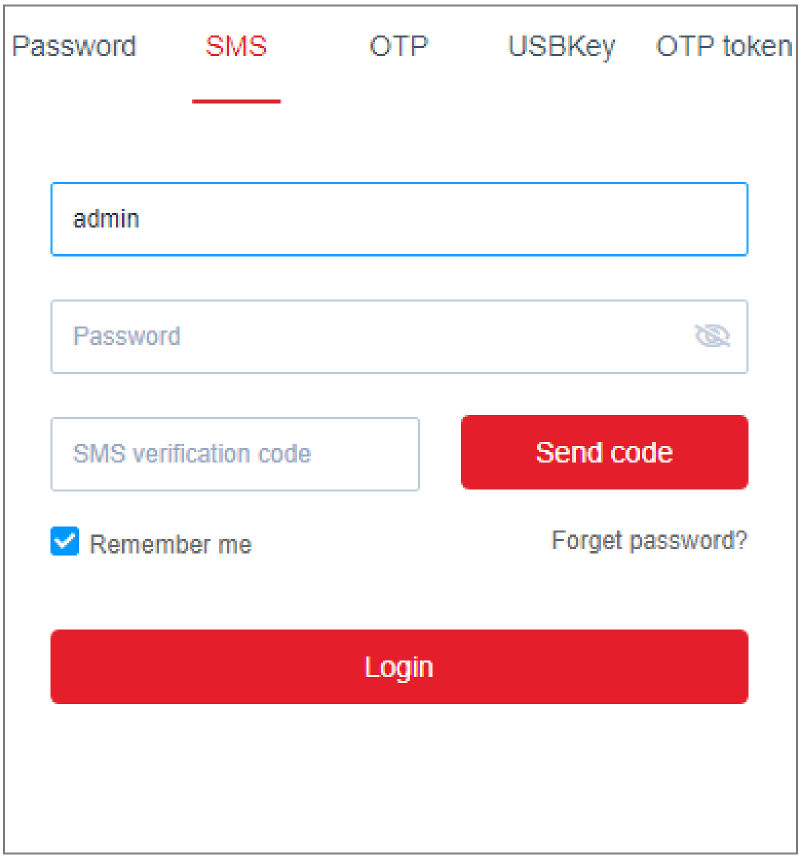
Step 2 Enter the username and password of your PBH account.

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

Step 4 Click **Login**.

----End

Figure 2-3 SMS authentication



Using Mobile OTPs for Logging

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

NOTICE

The mobile phone token applet of CBH is stored in the applet cache. The applet cache may be cleared by mistake in the background.

It is recommended that you 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**.

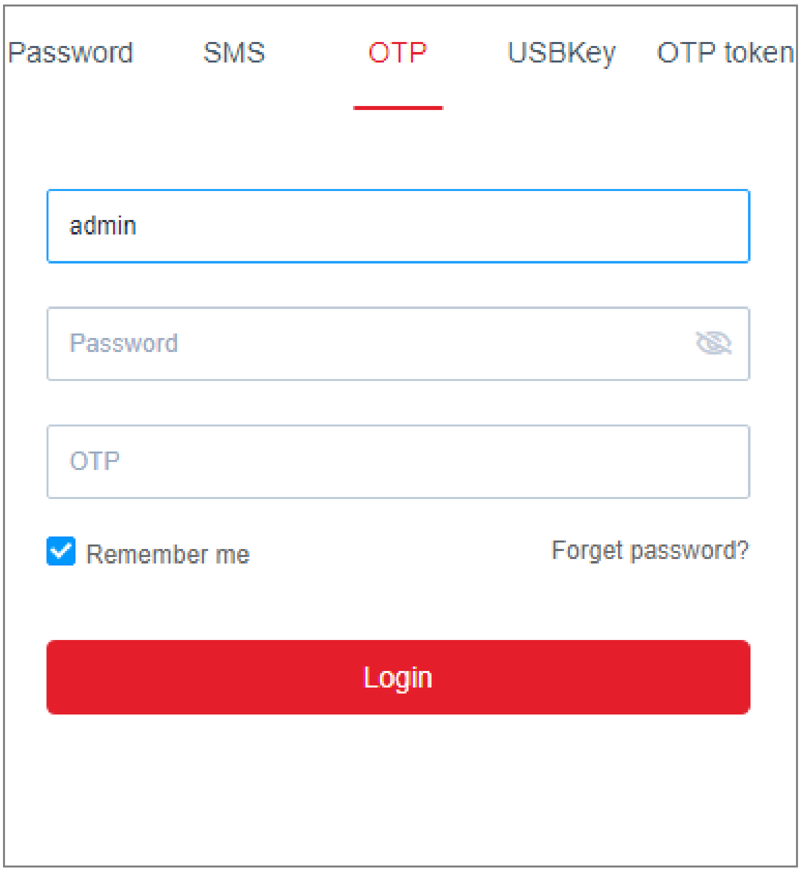
Step 2 Enter the username and password of your CBH account.

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

Figure 2-4 OTP authentication



Login Through USB Key Authentication

Step 1 Select **USBKey**.

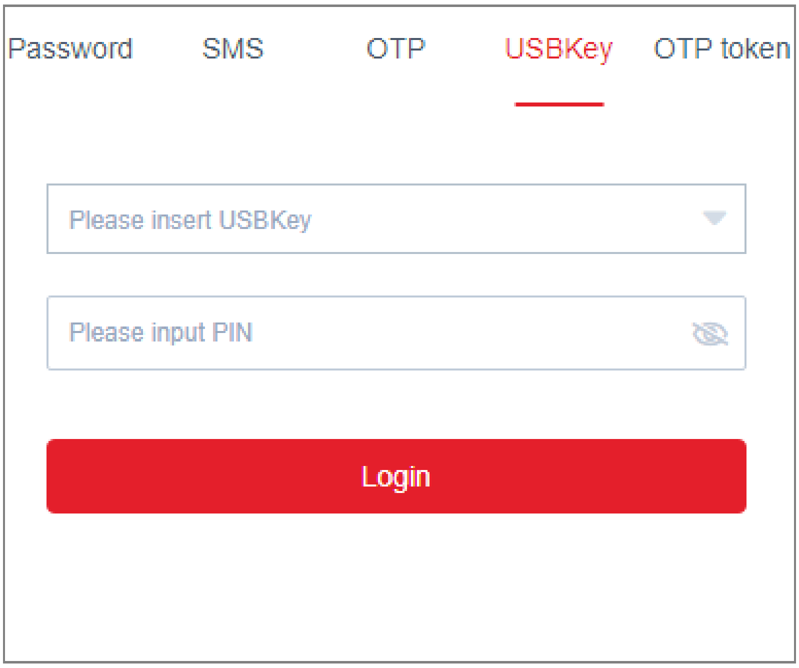
Step 2 Insert your USB key. The CBH system automatically identifies the issued USB key.

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

Step 4 Click **Login**.

----End

Figure 2-5 USB key authentication



Using OTP Tokens for Logging

Step 1 Select **OTP token**.

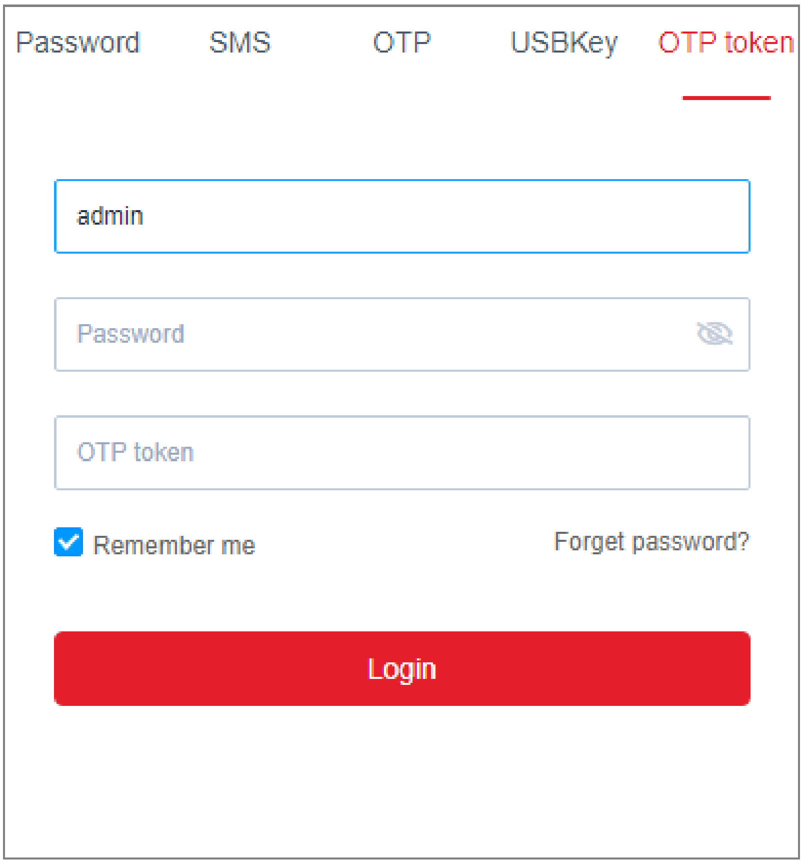
Step 2 Enter the username and password of your CBH account.

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

Figure 2-6 OTP token authentication



Login Through Azure AD 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 **Login**.

----End

2.3 Using a Client to Log In to a CBH System

With CBH, your current client-based O&M experience is still useful. You can use an SSH or Microsoft Terminal Services Client (MSTSC) client to directly log in to the CBH system for resource O&M.

- 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 a CBH System

CBH allows you to use an SSH client to log in to your CBH system for authorized resource O&M.

- 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 user session connection.

- Method 1

  In the displayed dialog box, select a protocol type, enter the EIP address and port number (2222) of the CBH 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.

- 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.

Step 3 Authenticate user identities.

Enter your identity credentials as prompted.

When an SSH client is used for establishing connections, you can use the **Password**, **SSH Pubkey**, **SMS**, **Mobile OTP**, and/or **OTP Token** authentication. To use **SMS**, **Mobile OTP**, and **OTP token**, configure multifactor verification. For details, see **Configuring Multifactor Verification**.

Table 2-4 SSH client login authentication

Authentication Method	Login Description	Configuration Description
Password	Enter the username and password of your CBH system user account.	Default login mode. 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**.

Authentication Method	Login Description	Configuration Description
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 system user account to a mobile OTP and contact the administrator to configure multi-factor authentication for this account. For details, see **Mobile OTP**.
OTP token	After the **Password** or **SSH Pubkey** login is authenticated, select **OTP token** and enter the verification code.	An OTP token has been issued to the user. For details, see **Issuing an OTP Token**.

Step 4 After logging in to the CBH system, you can view system information and start O&M operations.

NOTE

You can also use an API to directly log in to a managed host.

Enter the username in the format of *Username*@*Resource account*@*Host IP address*:*Port*, for example, **admin@root@192.0.0.0:22**.

----End

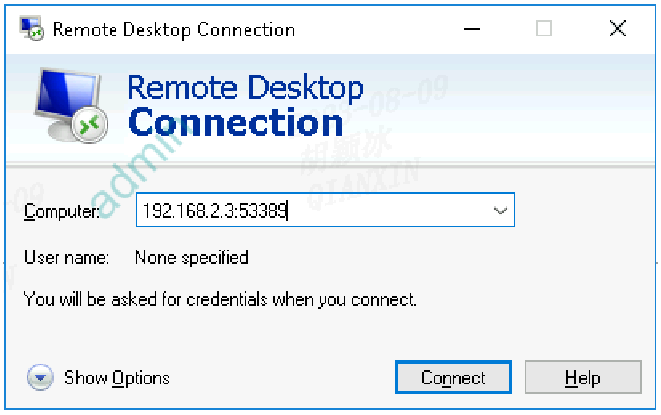
Accessing a CBH system through Microsoft Terminal Services Client (MSTSC)

CBH allows you to use an MSTSC client to log in to authorized resources for O&M.

Step 1 Open the MSTSC dialog box.

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

Figure 2-7 Configuring the computer



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

- Username: Enter *Login Name of the CBH 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.

- **Password**: Enter the password of the CBH user.

----End

2.4 Configuring Multifactor Verification

2.4.1 Configuring SMS Login Authentication

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.

Constraints

- Only one phone number can be bound to a CBH system user account.
- You have enabled the SMS gateway IP address and port 10743 and port 443 for the security group of the CBH instance, and the CBH 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.

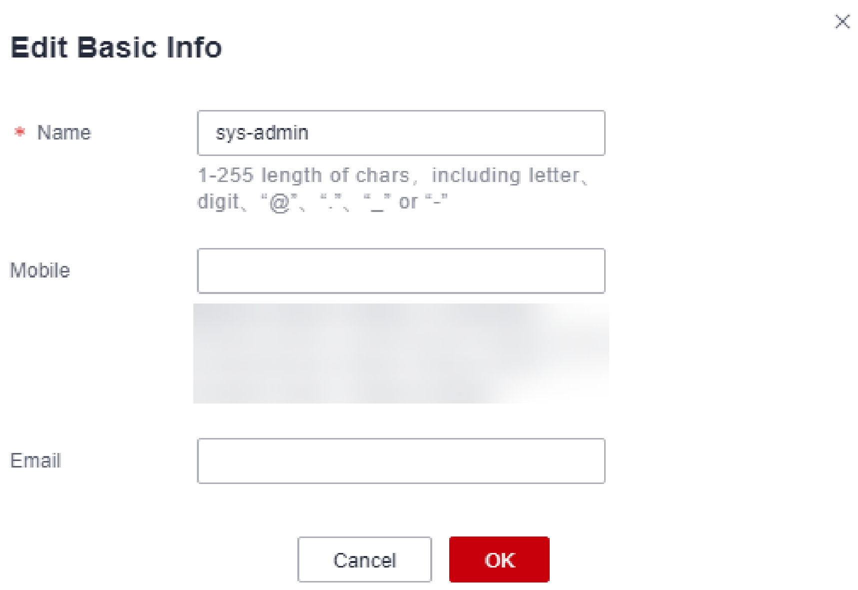
Method 1: Binding a phone number as an individual system user

Step 1 Log in to the CBH system 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**.

Figure 2-8 Binding a phone number



Step 4 In the displayed **Edit Basic Info** dialog box, enter a valid phone number in the **Mobile** text box.

Step 5 Click **OK**.

----End

Method 2: Changing a user's phone number as the administrator

Step 1 Log in to a CBH system 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

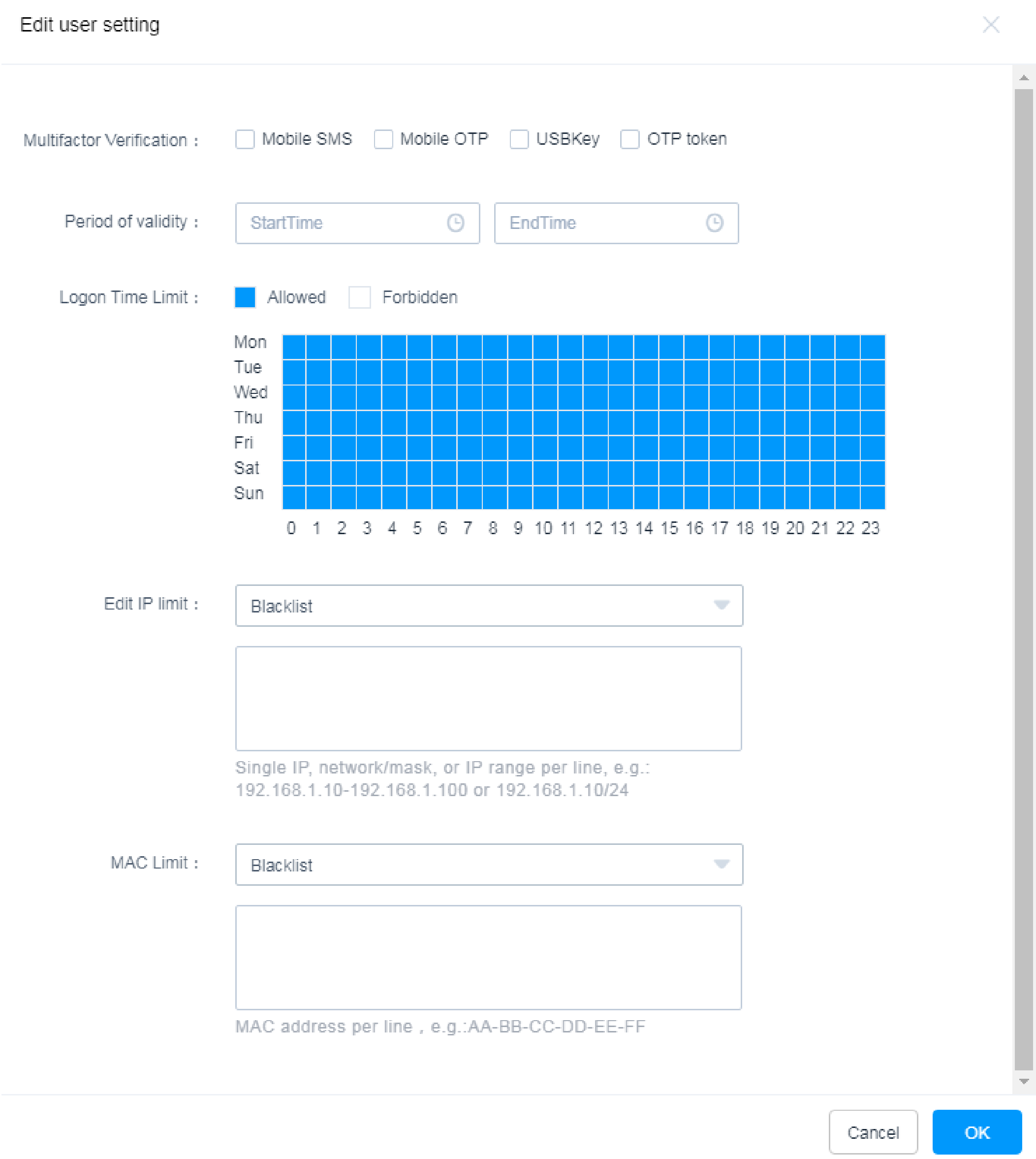
Step 1 Log in to a CBH system as the administrator.

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**.

Figure 2-9 Editing user setting



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 CBH system, they will have to provide an SMS code.

----End

2.4.2 Configuring Mobile OTP Login Authentication

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.

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.

Currently, CBH supports built-in mobile OTP and Remote Authentication Dial In User Service (RADIUS) mobile OTP.

- Built-in mobile OTP: WeChat applet OTP
- RADIUS mobile OTP applications: Microsoft Authenticator, Google Authenticator, and FreeOTP

Constraints

Ensure that your CBH system 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 CBH system time to the mobile phone time. Refresh the page, scan the new QR code, and try again.

Step 1: Bind a Mobile OTP as a Common User

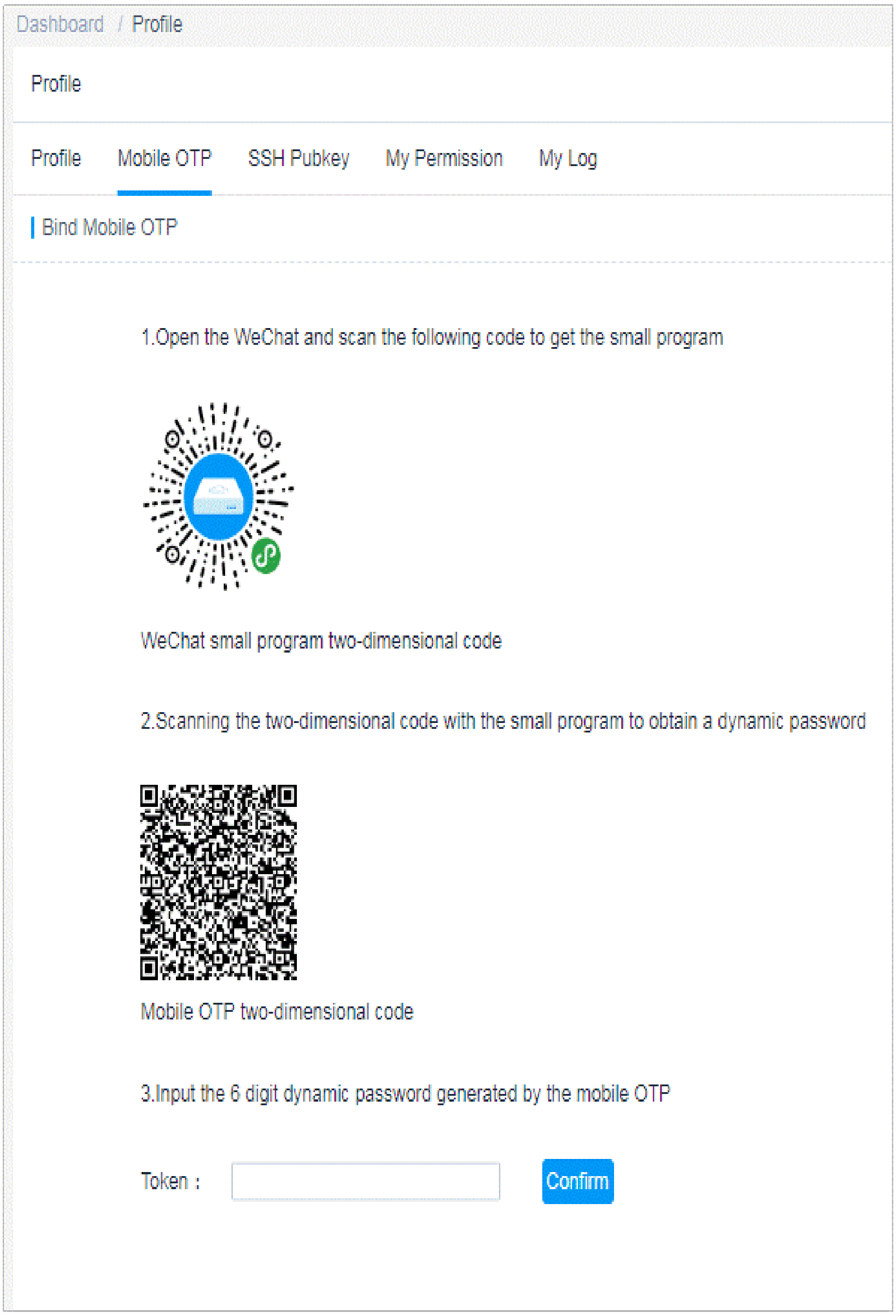
Step 1 Log in to the CBH system using your static password.

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.

Figure 2-10 Mobile OTP configuration



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

Step 2: Enable Mobile OTP Authentication for a User as the Administrator

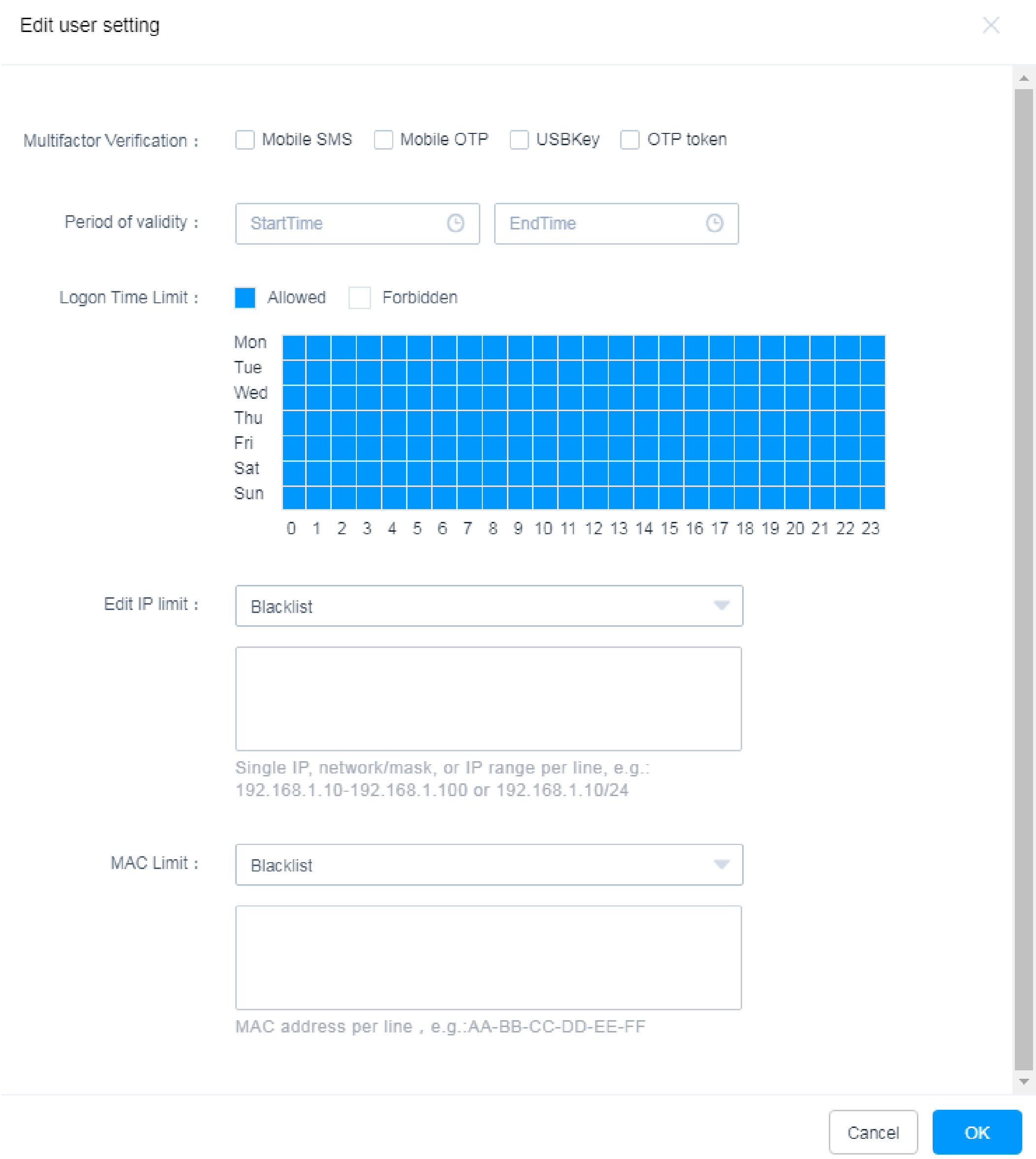
Step 1 Log in to a CBH system as the administrator.

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**.

Figure 2-11 Editing user setting



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 CBH system, they will have to provide a mobile OTP.

----End

2.4.3 Configuring USB Key Login Authentication

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.

Constraints

- Currently, CBH can identify USB keys of Century Longmai, BJCA, and JIT only Currently, CBH can identify USB keys of Feitian Technologies. USB keys of 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

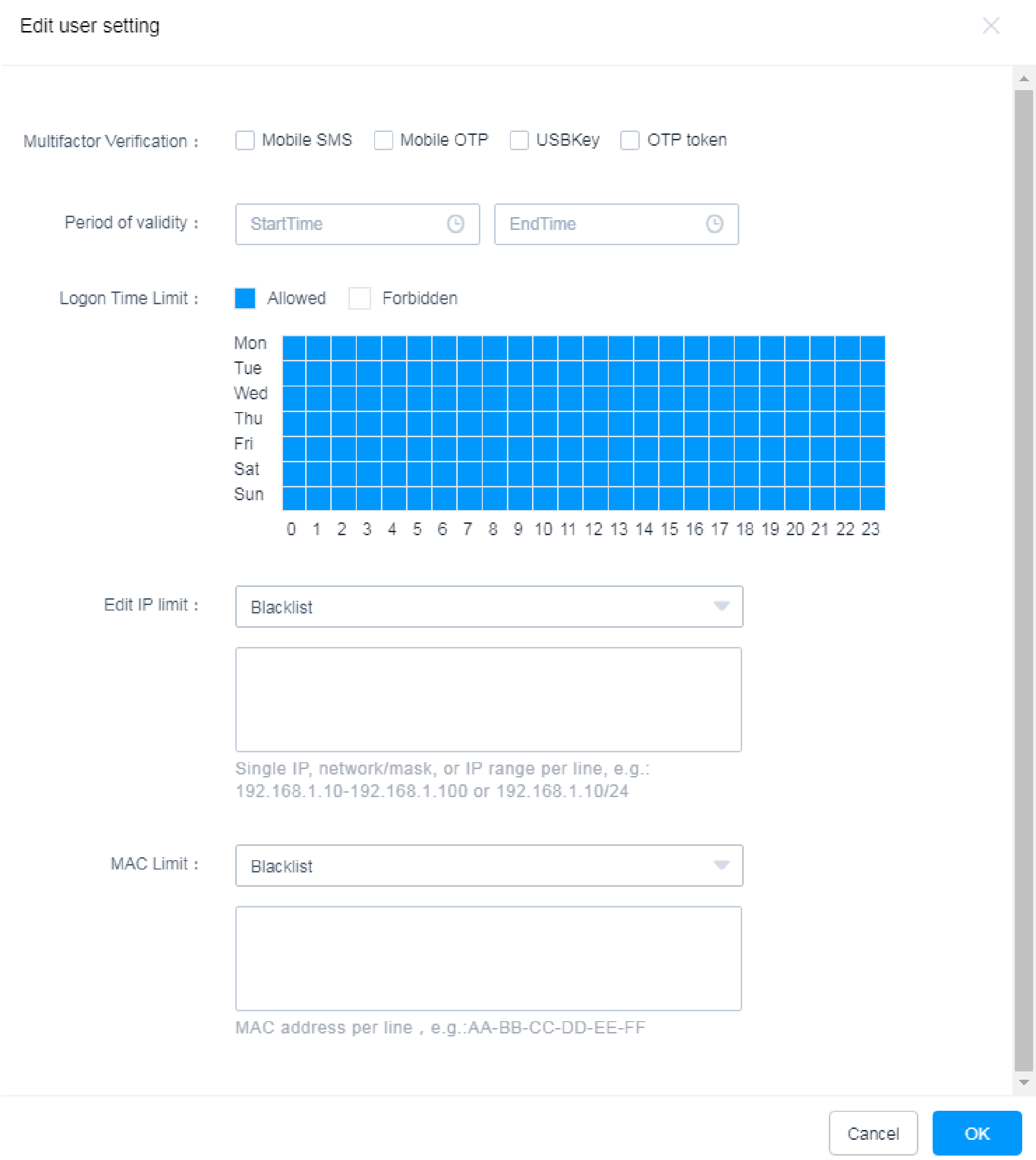
Step 1 Log in to a CBH system as the administrator.

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**.

Figure 2-12 Editing user setting



Step 5 In the displayed **Edit user setting** dialog box, select **USBKey** for **Multifactor Verification**.

Step 6 Click **OK**.

----End

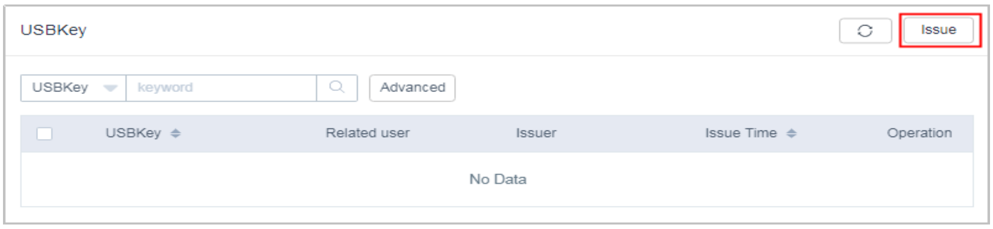
Step 2: Issue the USBKey

Step 1 Log in to a CBH system as the administrator.

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

Step 3 Click **Issue** to issue a USB key.

Figure 2-13 USBKey



Step 4 Select a user with the USB key multifactor verification enabled as the related user.

Figure 2-14 Procedure

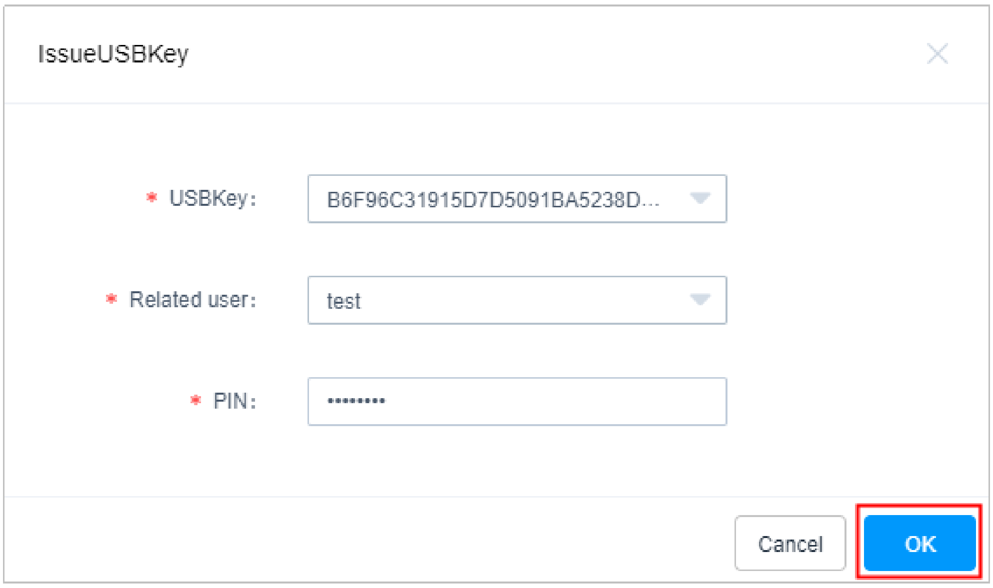


Table 2-5 Parameters for issuing a USB key

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.

To log in to the CBH system in USB key authentication method, insert your USB key into your local host, select the USB key on the CBH login page, and enter the PIN as prompted.

----End

2.4.4 Configuring OTP Token Login Authentication

An OTP token is a security hardware device that generates one-time passwords. You can use event-based OTP tokens for CBH. 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, CBH only supports Jansh ETZ201/ETZ203 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

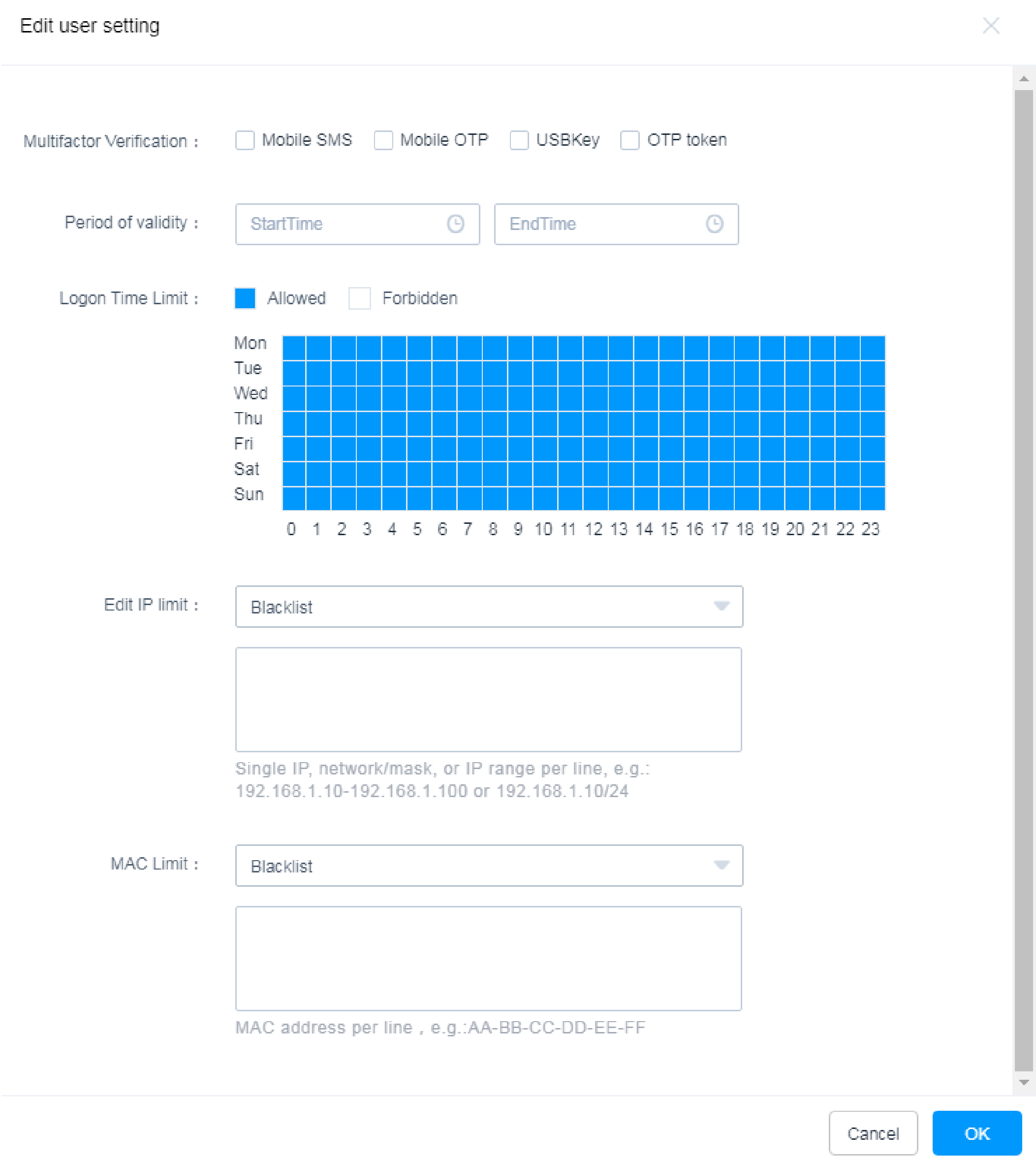
Step 1 Log in to a CBH system as the administrator.

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**.

Figure 2-15 Editing user setting



Step 5 In the displayed **Edit user setting** dialog box, select **OTP token** for **Multifactor Verification**.

Step 6 Click **OK**.

----End

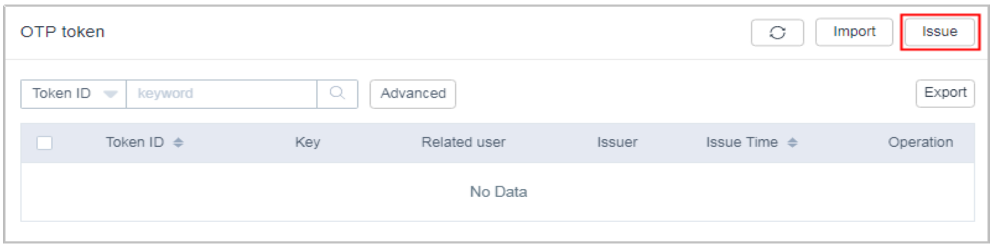
Step 2: Issue an OTP Token

Step 1 Log in to a CBH system as the administrator.

Step 2 Choose **User** > **OTP token** in the navigation pane.

Step 3 Click **Issue** to issue an OTP token.

Figure 2-16 New OTP token



Step 4 Enter the required token information.

Figure 2-17 Issuing an OTP Token

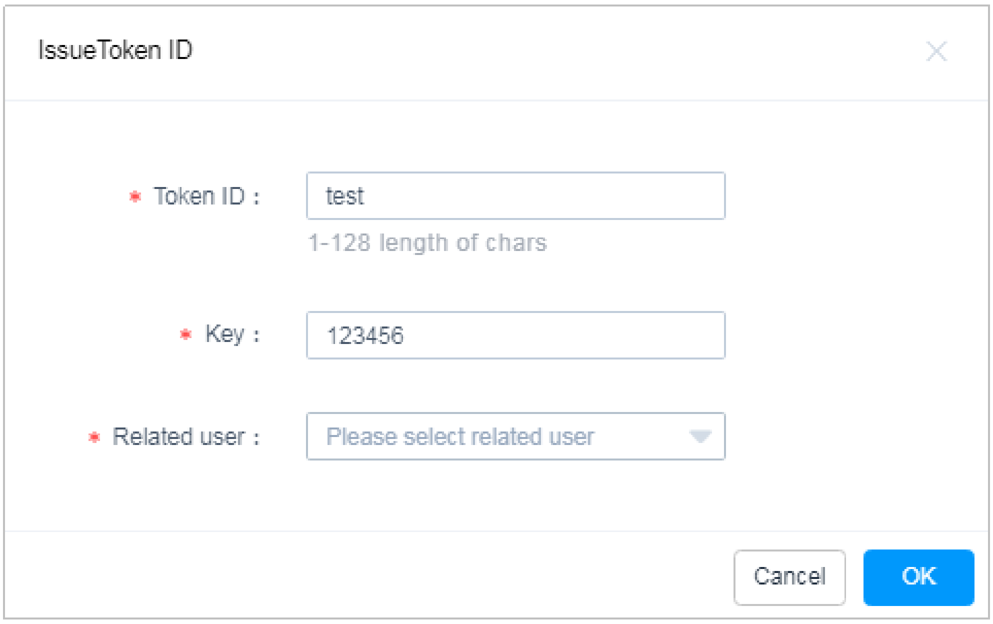


Table 2-6 Parameters for issuing an OTP token

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 name, static password, and the dynamic password on the OTP token are required for login.

----End

2.5 Managing Login Security

2.5.1 Configuring User Login Lockout

For login security purposes, the 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

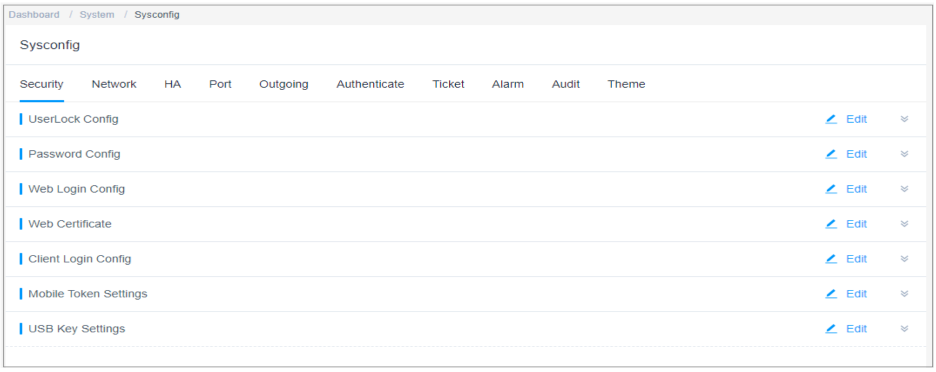
You have the management permissions for the **System** module.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **System** > **Sysconfig** > **Security**.

Figure 2-18 System security configuration



Step 3 In the **UserLock Config** area, click **Edit**.

Complete configurations as prompted.

Figure 2-19 UserLock Config

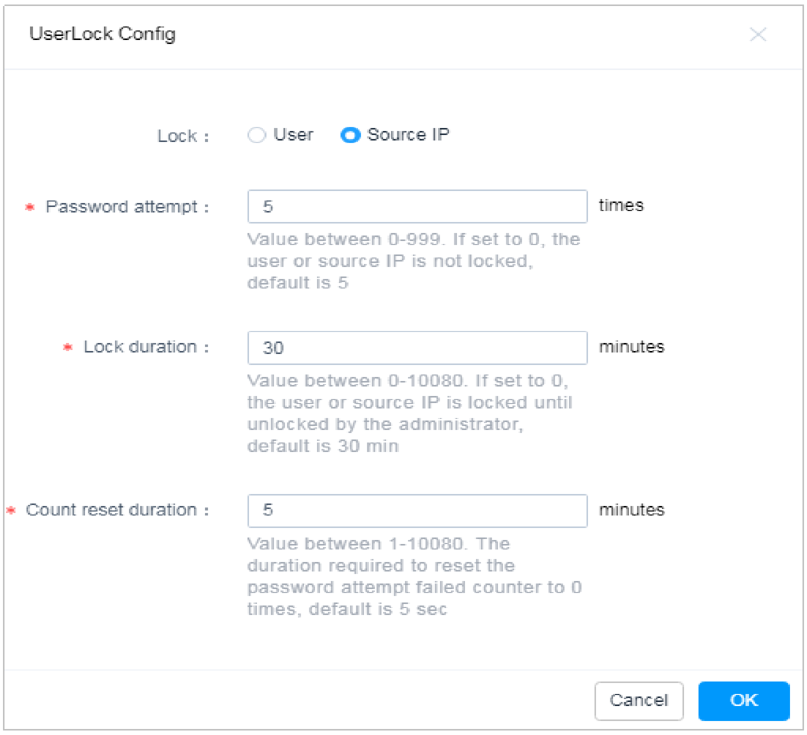


Table 2-7 Parameters for configuring user lockout

Parameter	Description
Lock	Lockout method. The options are **User** and **Source IP**. ● **User**: If the number of consecutive failed password attempts exceeded the upper limit, the user is blocked by the CBH system. ● **Source IP**: If the number of consecutive failed password attempts exceeded the upper limit, the source IP address is blocked by the CBH system.
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.

Parameter	Description
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.

Figure 2-20 UserLock Config

----End

2.5.2 Configuring the Login Password Policies

This topic describes how to configure the user password policies, including the password strength, number of password verification times, and password change period.

Prerequisites

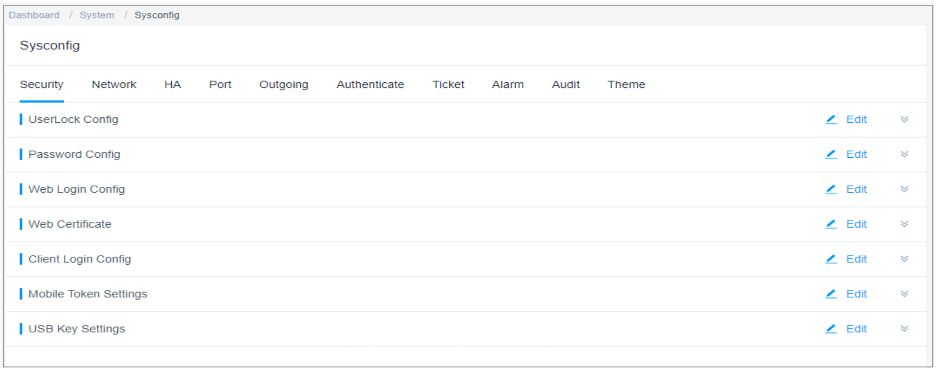
You have the management permissions for the **System** module.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **System** > **Sysconfig** > **Security**.

Figure 2-21 System security configuration



Step 3 In the **Password Config** area, click **Edit**.

Complete configurations as prompted.

Figure 2-22 Password Config

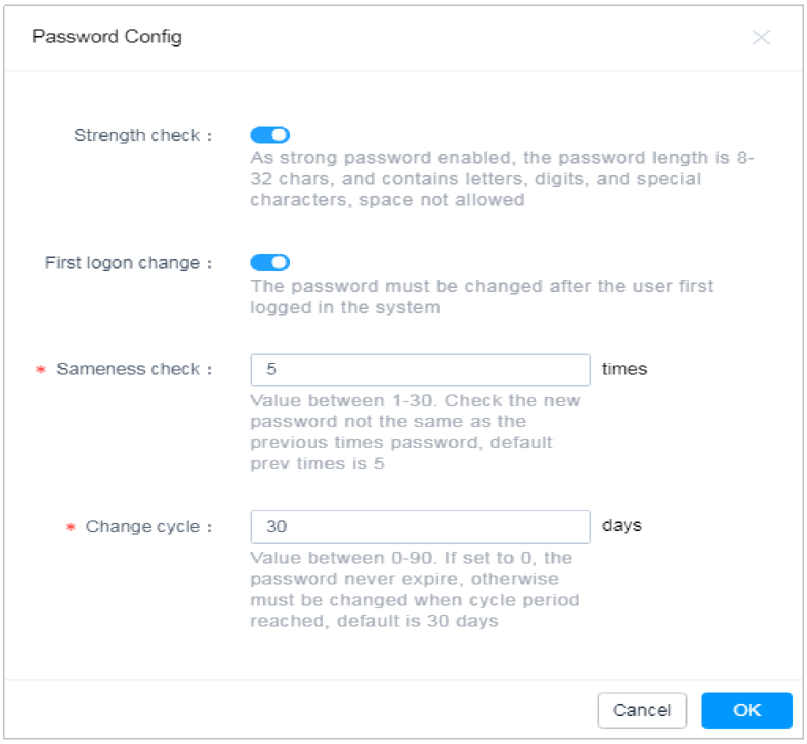


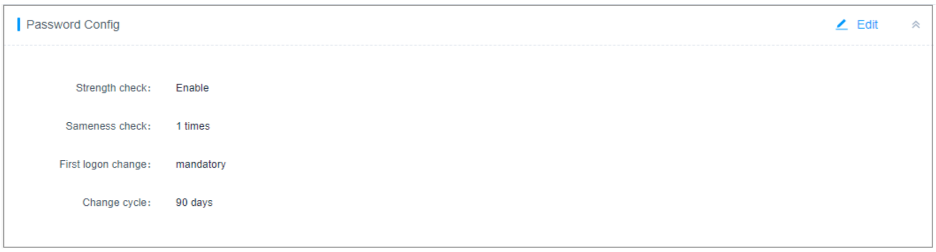
Table 2-8 Parameters for configuring a password policy

Parameter	Description
Strength check	Checks password strength. It is enabled ( ) by default. ● : disabled ● : enabled. A password must contain 8 to 32 characters, including letters, digits, and special characters and cannot contain spaces.
First logon change	Forces a user to change password upon first login to the CBH 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 policy of the current system user on the **Security** tab.

Figure 2-23 Password Config



----End

2.5.3 Configuring Login Timeout and Login 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

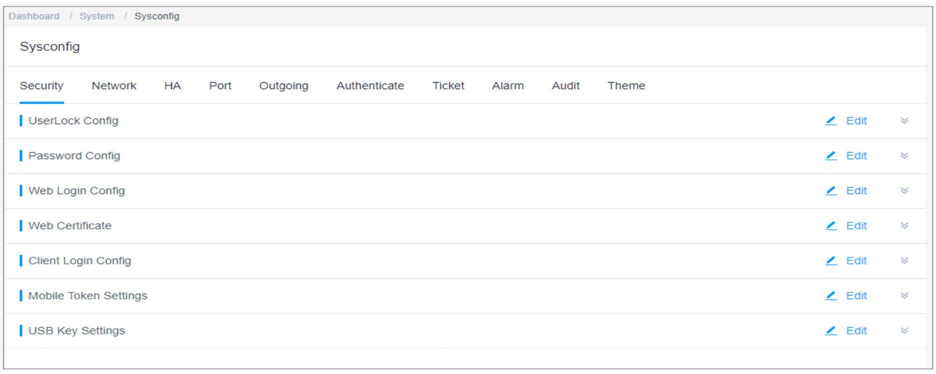
You have the management permissions for the **System** module.

Configuring Web Login Requirements

Step 1 Log in to the CBH system.

Step 2 Choose **System** > **Sysconfig** > **Security**.

Figure 2-24 System security configuration



Step 3 In the **Web Login Config** area, click **Edit**.

Complete configurations as prompted.

Figure 2-25 Configuring Web Login Requirements

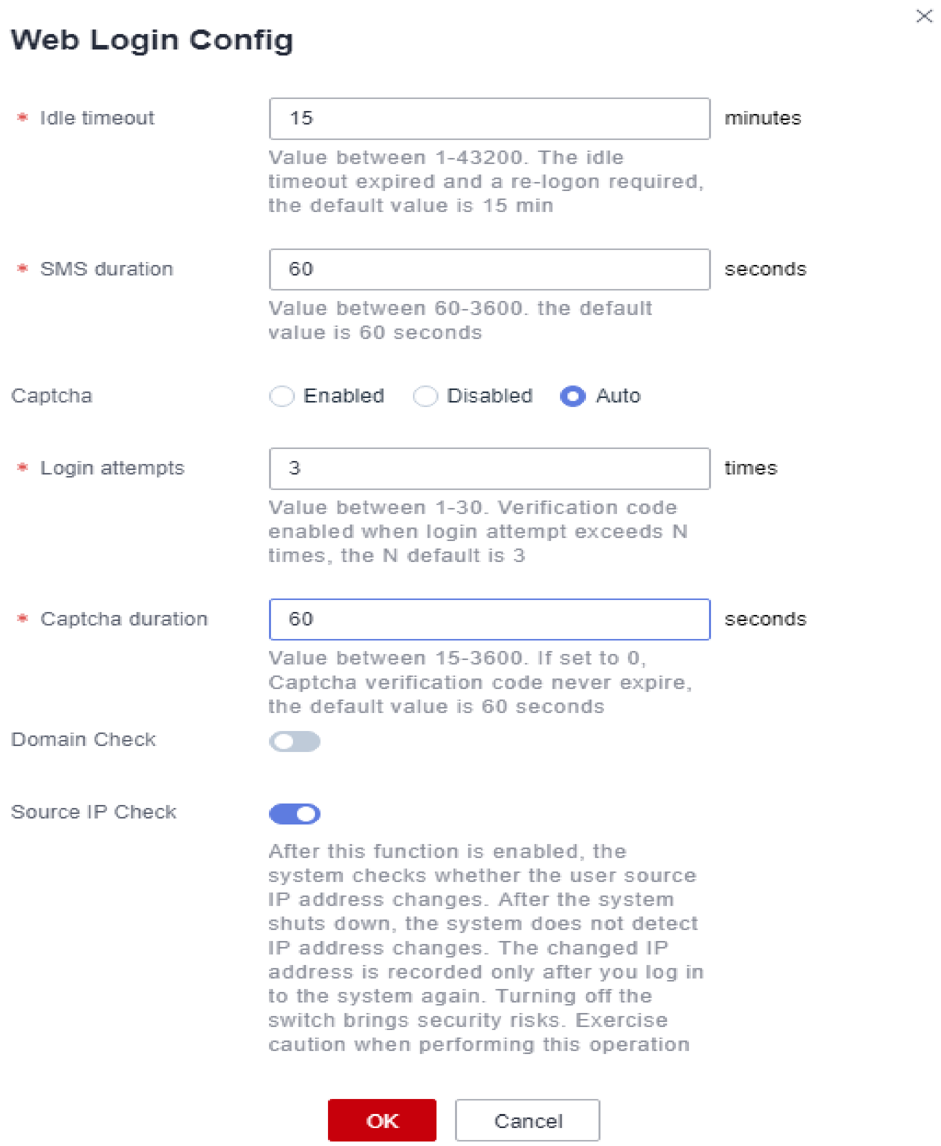


Table 2-9 Parameters for configuring web login

Parameter	Description
Idle timeout	Duration to wait before an inactive user is logged out. After a system user logs in to the CBH system 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 **43200**, in minutes

Parameter	Description
SMS duration	SMS verification code validity period. ● Default value: **60** seconds ● Value range: **15** to **3600**, 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 to log in to the CBH system. ● : disabled
Source IP Check	Whether to check source IP address. The default status is . ● : The **Source IP Check** is enabled. If you enable this check, the system checks whether there is any change to the source IP address of a user. If you keep this check disabled, the system only records the source IP address for a new login but does not check such changes. Note that there may be security risks if you keep this check disabled. ● : This **Source IP Check** is disabled.

Step 4 Click **OK**. You can then check the web login configuration of the current system on the **Security** tab.

Figure 2-26 Web Login Config

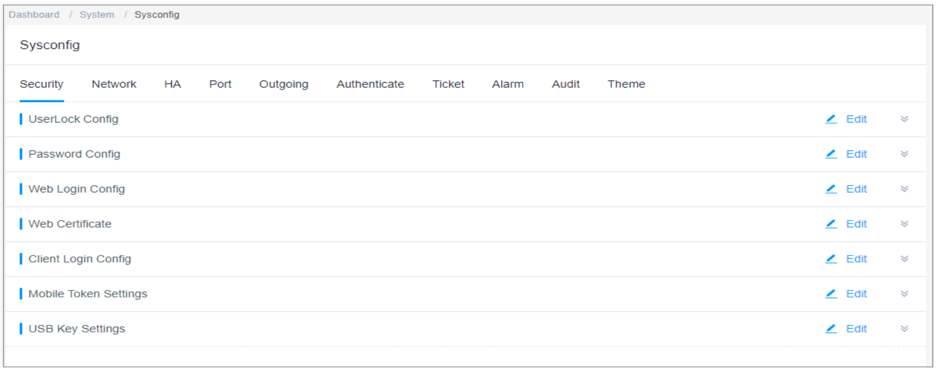
----End

Configuring Login Using a Client

Step 1 Log in to the CBH system.

Step 2 Choose **System** > **Sysconfig** > **Security**.

Figure 2-27 System security configuration



Step 3 In the **Client Login Config** area, click **Edit**.

Complete configurations as prompted.

Figure 2-28 Configuring Login Using a Client

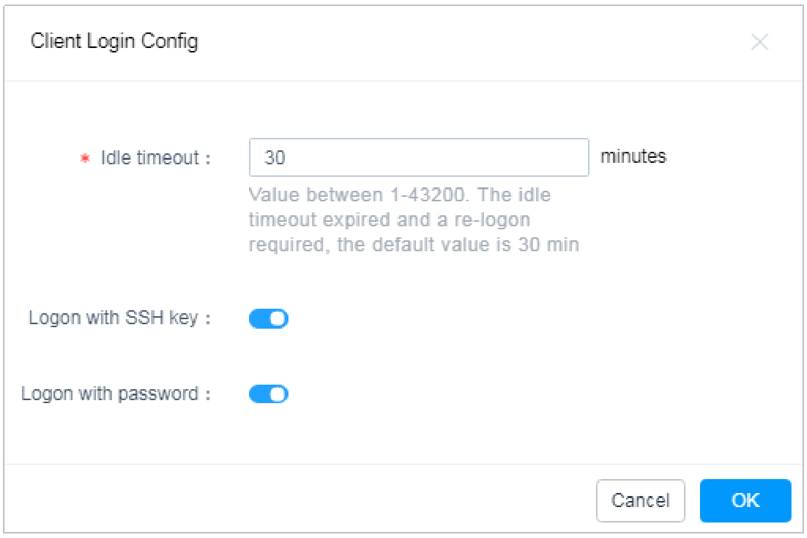
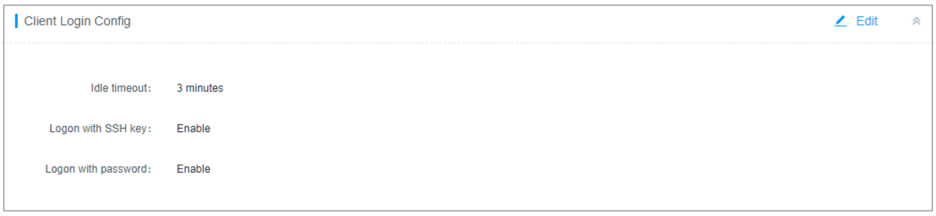


Table 2-10 Parameters for configuring client login

Parameter	Description
Idle timeout	Duration to wait before an inactive user is logged out of the CBH 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 CBH 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.

Figure 2-29 Client Login Config



----End

2.5.4 Updating a System Web Certificate

A web certificate in CBH is a Secure Sockets Layer (SSL) server digital certificate issued by a trusted root certificate authority (CA) and used to verify the website identity and security of the CBH system.

A secure self-issued certificate is configured for each CBH system 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 CBH instance. For details, see **Adding an A Record Set**.
- You have the management permissions for the **System** module.

Constraints

- Currently, the CBH system supports only the Java Keystore certificate file of Tomcat, that is, the certificate file in .jks.
- A certificate file cannot exceed 20 KB and must contain a certificate password.

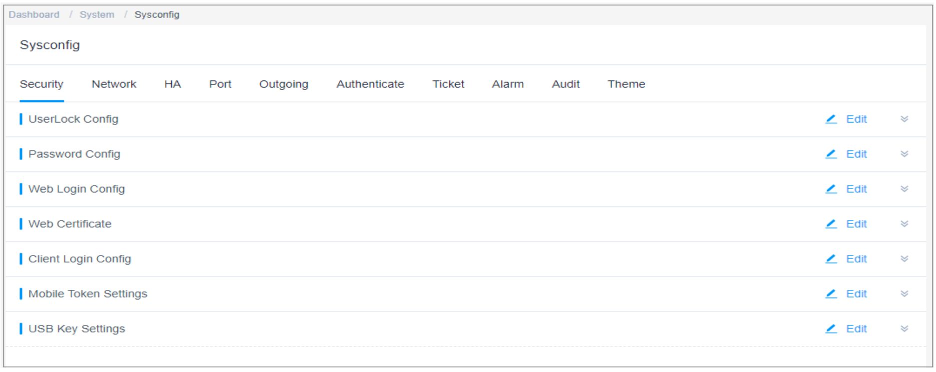
  When you upload an SSL certificate, provide its password for verification, or the upload will fail.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **System** > **Sysconfig** > **Security**.

Figure 2-30 System security configuration

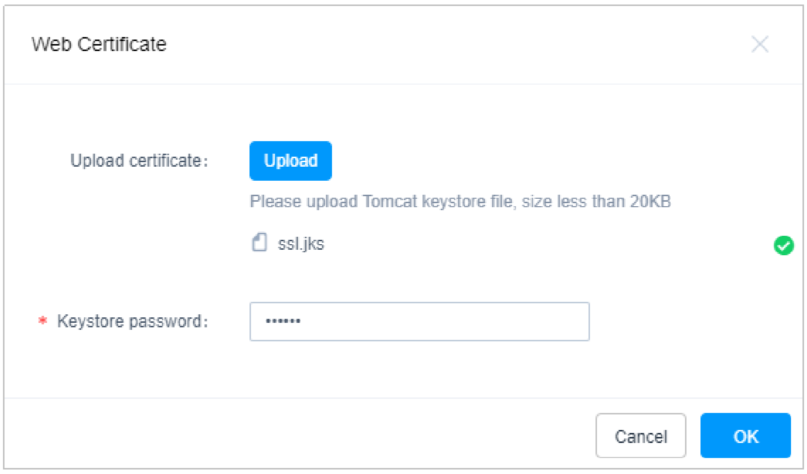


Step 3 In the **Web Certificate** configuration area, click **Edit**.

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.

Figure 2-31 Web 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 CBH system for the updated certificate to take effect.

You can use either of the following methods to restart the CBH system:

- Restart the instance on the management console. For details, see **Restarting a CBH Instance**.
- Use the system tool in the CBH system to restart the system. For details, see **Managing System Tools**.

Figure 2-32 System web certificate information

----End

2.5.5 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 the CBH system.

This topic describes how to set the mobile OTP type.

Constraints

- Currently, only the following OTP types are supported:
  - Built-in mobile OTP: WeChat applet OTP
  - RADIUS mobile OTP: OTP applications, including Google Authenticator and FreeOTP
- For the mobile token to take effect, ensure that the mobile token types configured in the CBH system and on your mobile phone are the same.

Prerequisites

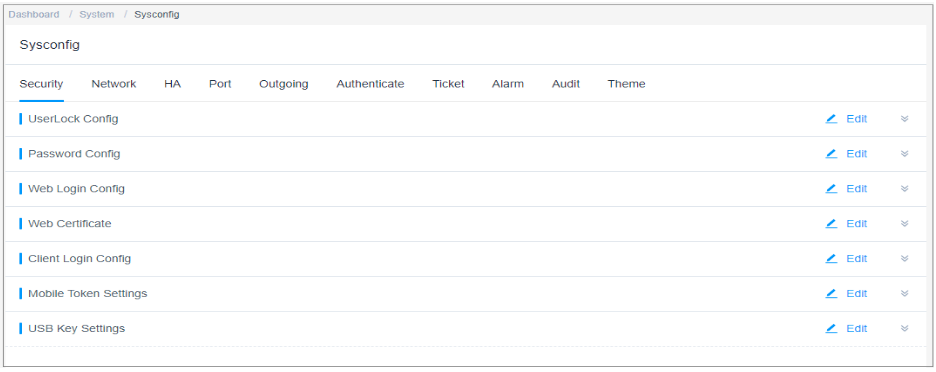
You have the management permissions for the **System** module.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **System** > **Sysconfig** > **Security**.

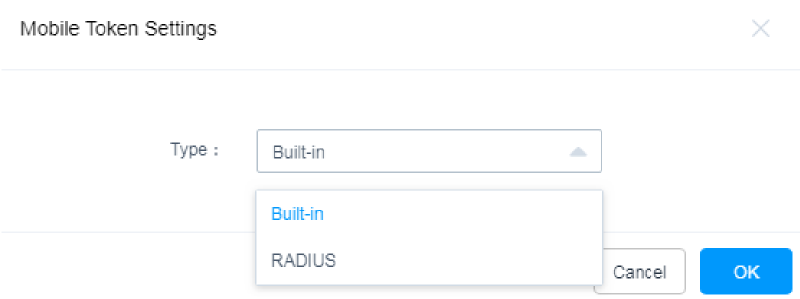
Figure 2-33 System security configuration



Step 3 In the **Mobile Token Settings** area, click **Edit**.

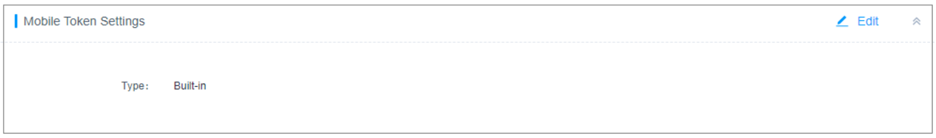
Step 4 In the displayed **Mobile Token Settings** dialog box, select a mobile OTP type.

Figure 2-34 Configuring the Mobile OTP Type



Step 5 Click **OK**. You can then check the mobile token settings of the current system user on the **Security** tab.

Figure 2-35 Viewing mobile token settings



----End

2.5.6 Configuring the USB Key Vendor

This topic describes how to configure the USB key vendor.

Constraints

- Currently, only the USB keys from BJCA, Century Longmai, Century Longmai (SM series cryptographic algorithms), JDZY (or JIT), and Feitian Technologies are supported.
- If you change the vendor of a USB key, the issued USB key cannot be identified by the CBH system.

Prerequisites

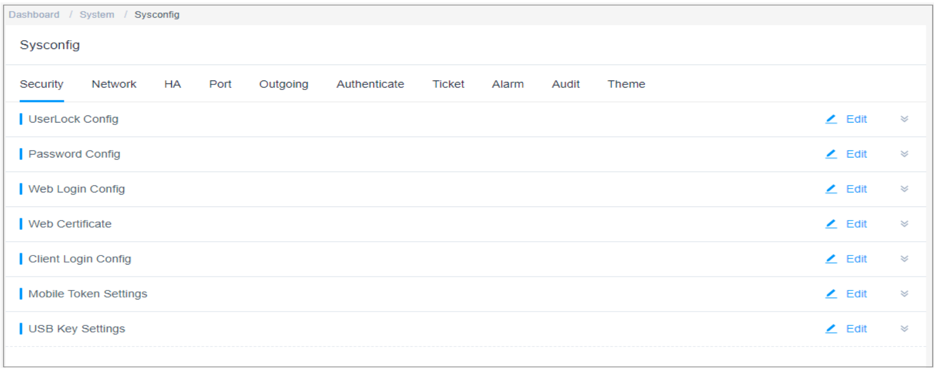
You have the management permissions for the **System** module.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **System** > **Sysconfig** > **Security**.

Figure 2-36 System security configuration

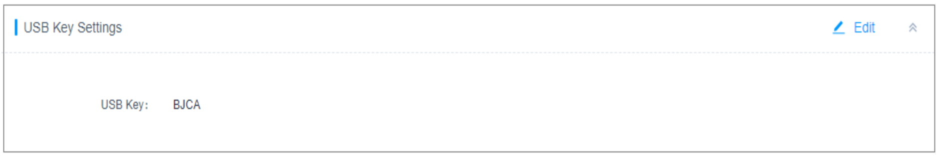


Step 3 In the **USB Key Settings** area, click **Edit**.

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.

Figure 2-37 Viewing the USB Key vendor



----End

2.5.7 Configuring Policies to Disable Zombie Users (Available in V3.3.30.0 and Later Versions)

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 CBH 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

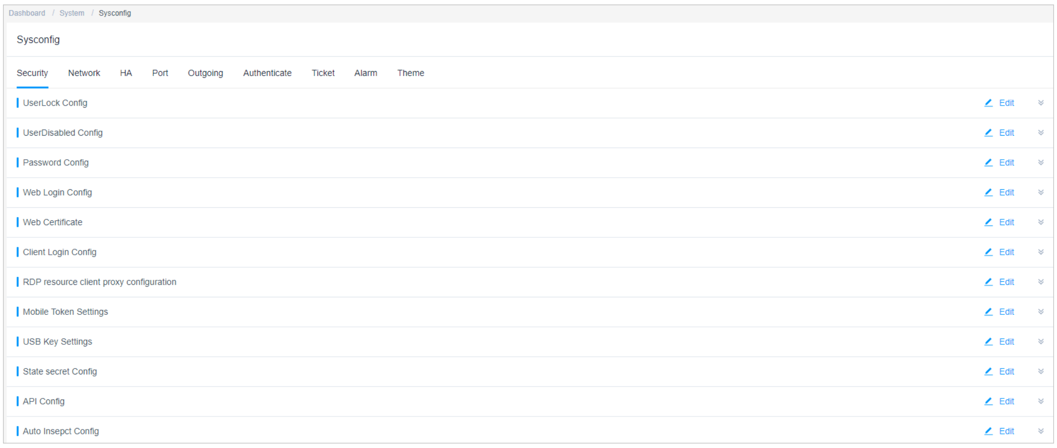
You have the management permissions for the **System** module.

Procedure

Step 1 Log in to the CBH system.

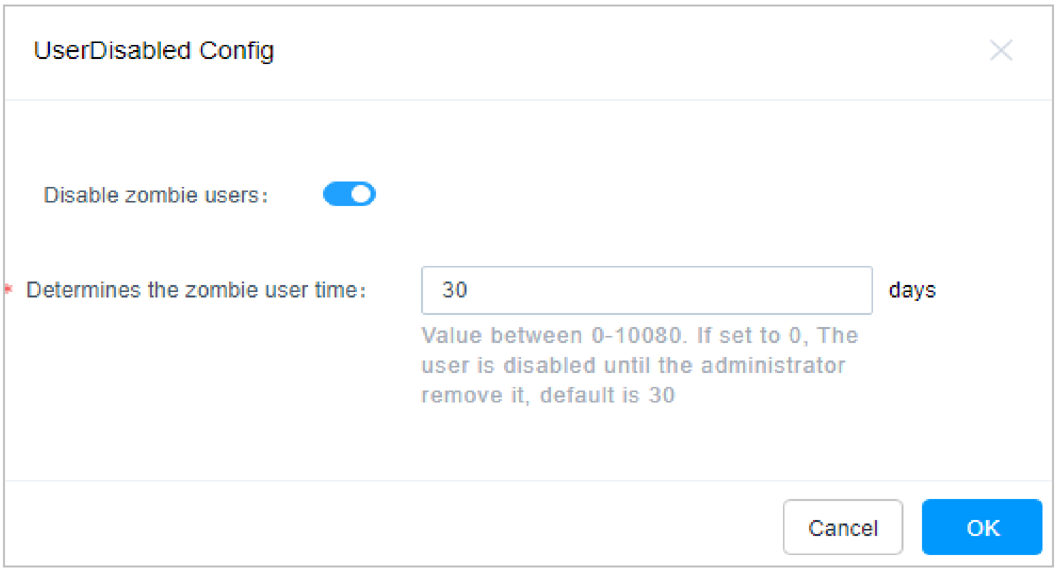
Step 2 Choose **System** > **Sysconfig** > **Security**.

Figure 2-38 System security configuration



Step 3 In the **UserDisabled Config** area, click **Edit**.

Figure 2-39 UserDisabled Config



- **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

2.5.8 Configuring the RDP Resource Client Proxy (Available in 3.3.26.0 and Later Versions)

This topic describes how to configure the RDP resource client proxy.

Prerequisites

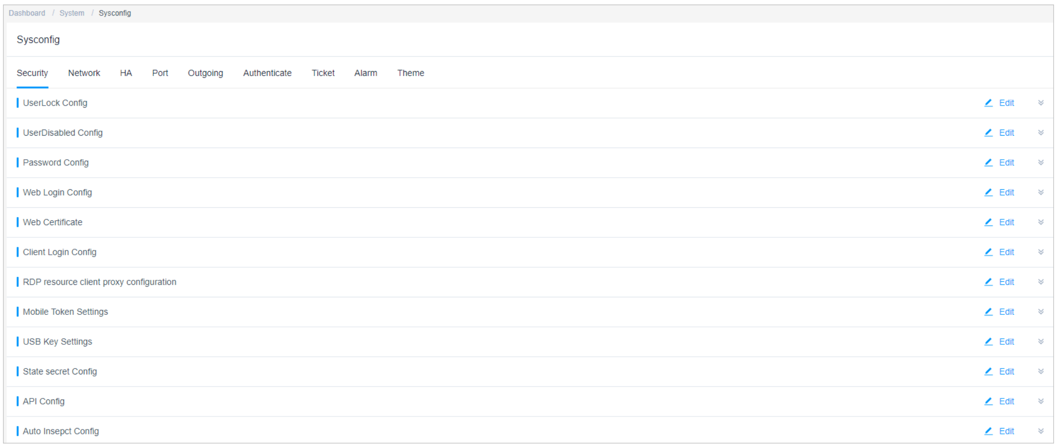
You have the management permissions for the **System** module.

Procedure

Step 1 Log in to the CBH system.

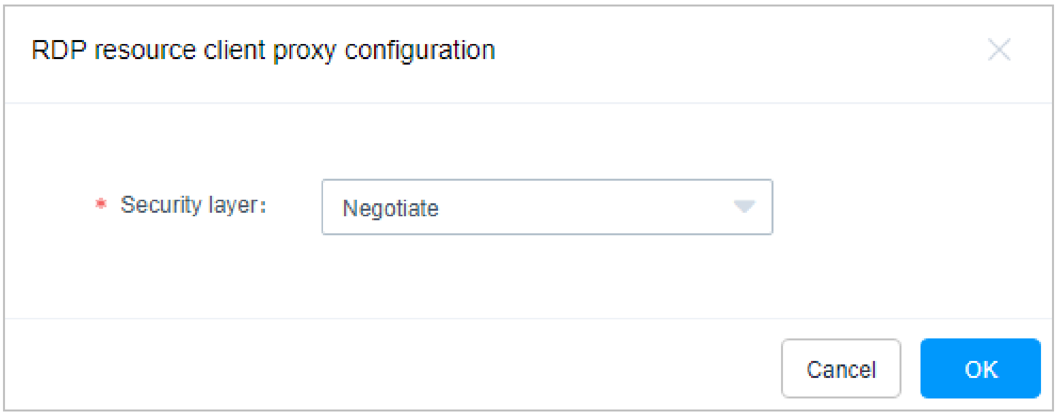
Step 2 Choose **System** > **Sysconfig** > **Security**.

Figure 2-40 System security configuration



Step 3 In the **RDP resource client proxy Configuration** area, click **Edit**.

Figure 2-41 RDP resource client proxy configuration



Step 4 In the **Security layer** drop-down list, select a client proxy and click **OK**.

You can select **RDP**, **TLS**, or **Negotiate**.

----End

2.5.9 Enabling API Configuration (Included in V3.3.34.0 and Later Versions Only).

After you enable the API configuration, the CBH system can be used by calling APIs.

Prerequisites

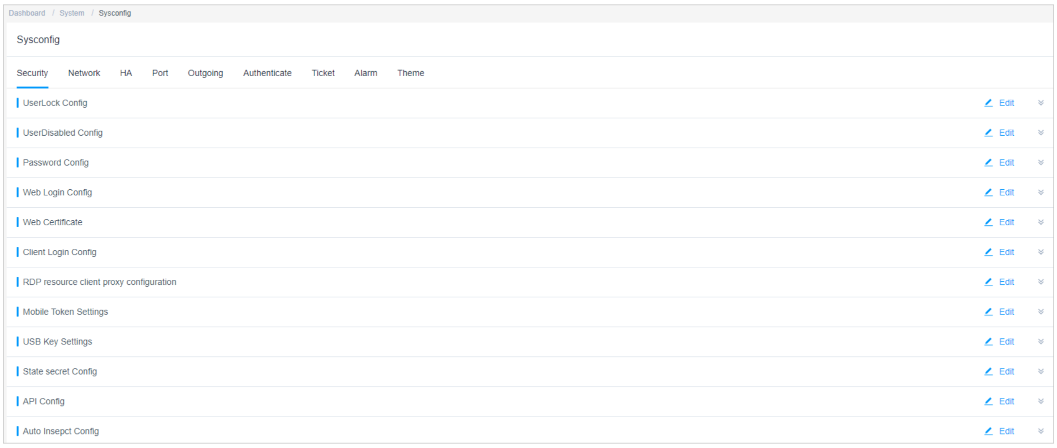
You have the management permissions for the **System** module.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **System** > **Sysconfig** > **Security**.

Figure 2-42 System security configuration



Step 3 In the **API Config** area, click **Edit**.

Step 4 Click .

Step 5 Click **OK**.

----End

2.5.10 Configuring Automatic Inspection (Available in V3.3.36.0 and Later)

After automatic inspection is enabled, the CBH system automatically verifies accounts of managed resources at 01:00 on the 5th, 15th, and 25th days of each month.

Prerequisites

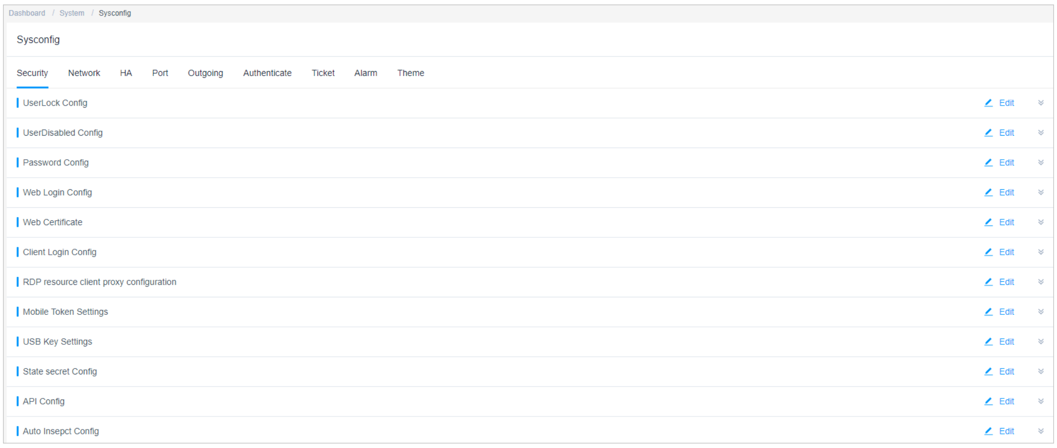
You have the management permissions for the **System** module.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **System** > **Sysconfig** > **Security**.

Figure 2-43 System security configuration



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

3 Dashboard of the CBH System

3.1 Dashboard

In the CBH system, the **Dashboard** module presents the CBH system information and statistics on system user actions and host and application operations from different dimensions. The **Dashboard** module consists of a basic statistic area and 17 graph panels, including basic statistics area, **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 Applications**, **My Hosts**, and **My APPs**.

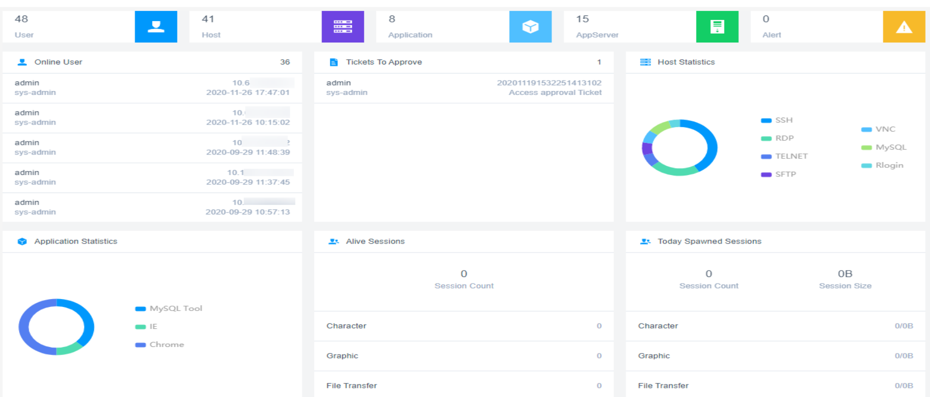
These panels are visible for you based on your roles. This topic uses the system administrator **admin** as an example to describe how to get information on the **Dashboard** page.

Procedure

Step 1 Log in to the CBH system.

Step 2 In the navigation tree on the left, choose Desktop. The Desktop Dashboard page is displayed.

Figure 3-1 Dashboard



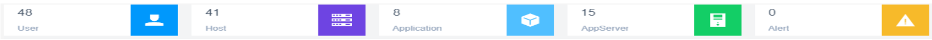
Step 3 View different panels based on your needs. For details about the functions of each panel, see the following topics.

----End

Basic Statistics

Displays statistics about users, hosts, applications, and application servers that can be managed by the current user, and the number of unprocessed alerts.

Figure 3-2 Basic Statistics



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.

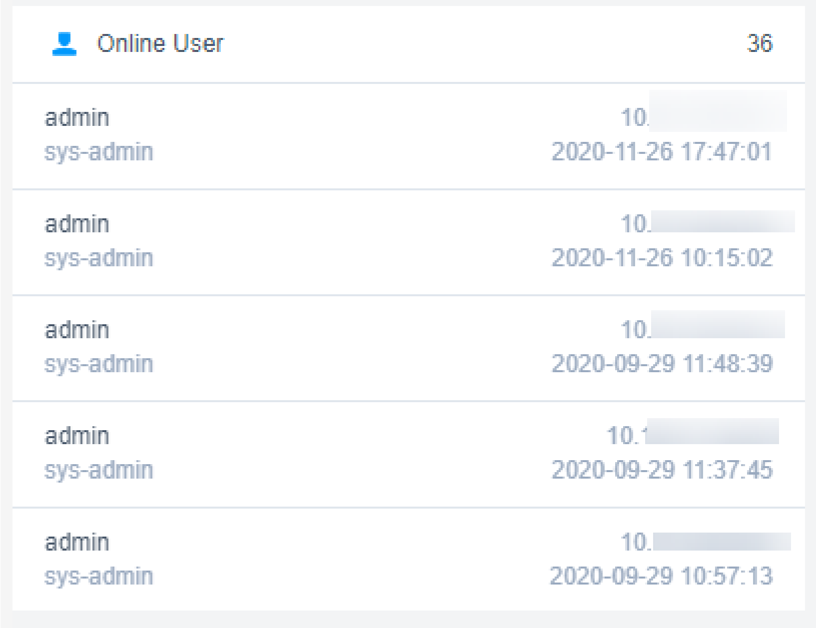
Online User

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.

Figure 3-3 Online User



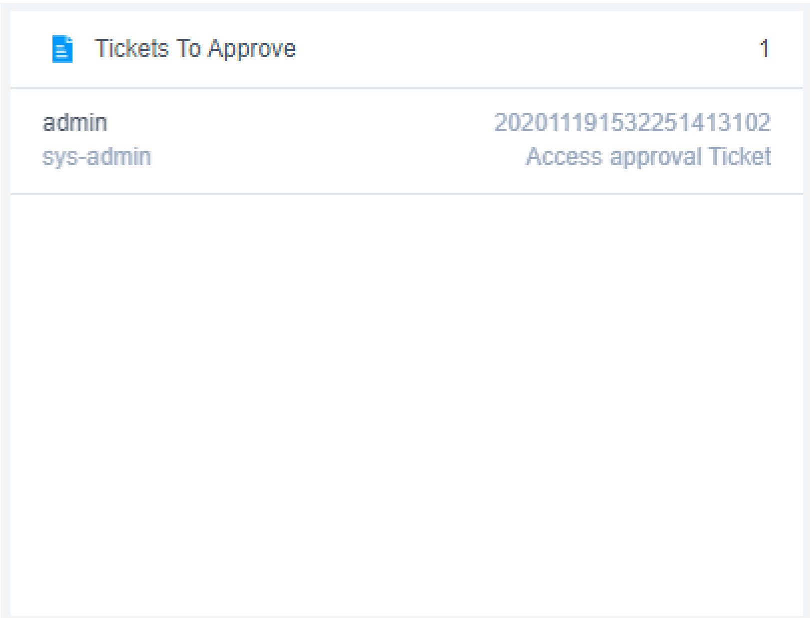
Tickets to Approve

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.

Figure 3-4 Tickets to Approve



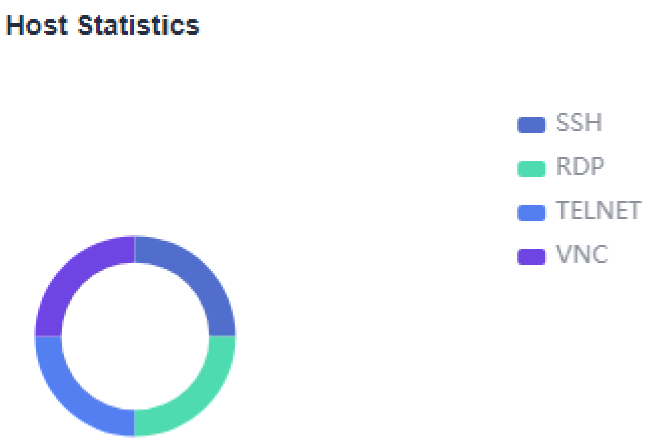
Host Statistics

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.

Figure 3-5 Host Statistics



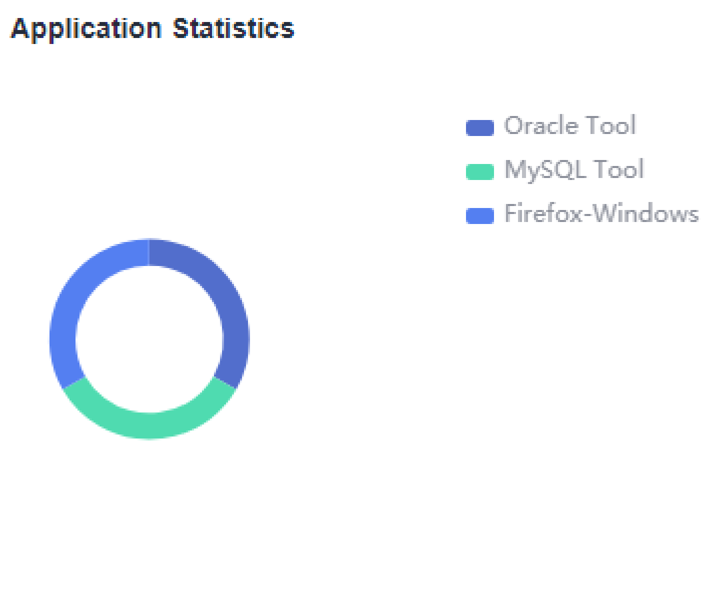
Application Statistics

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.

Figure 3-6 Application Statistics



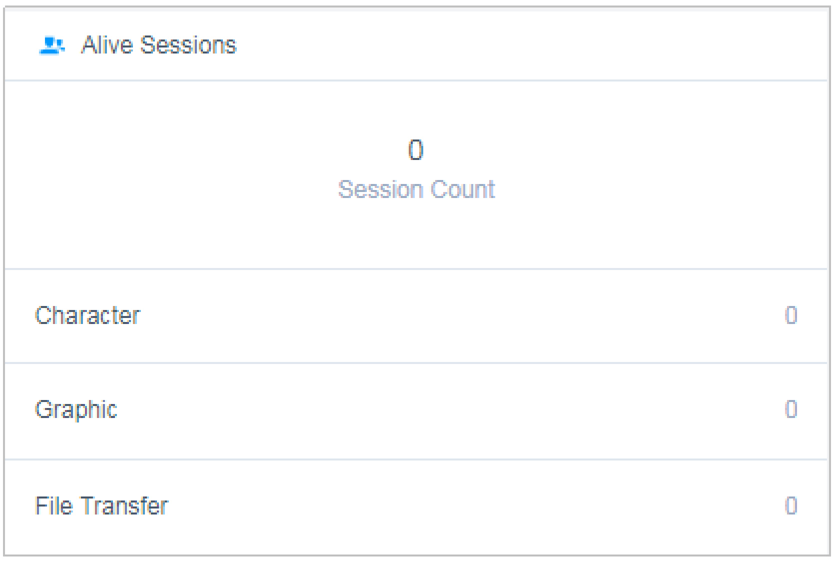
Alive Sessions

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.

Figure 3-7 Alive Sessions



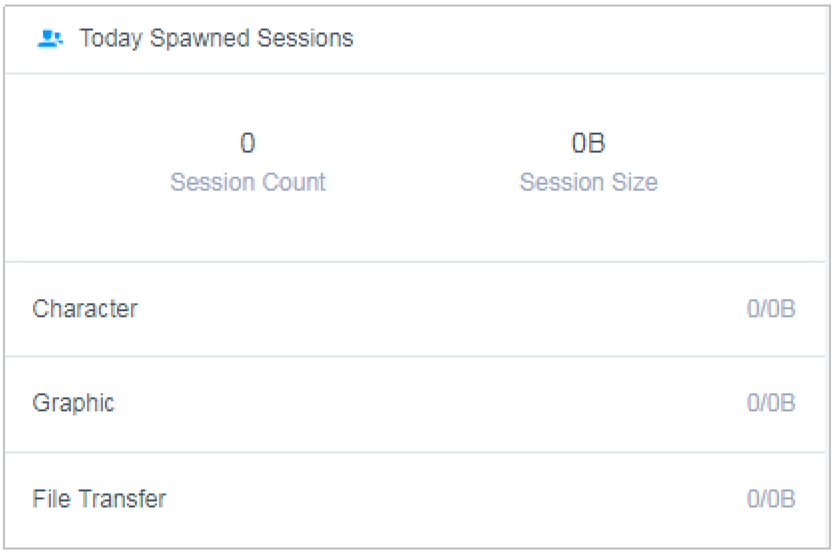
Today Spawned Sessions

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.

Figure 3-8 Today Spawned Sessions



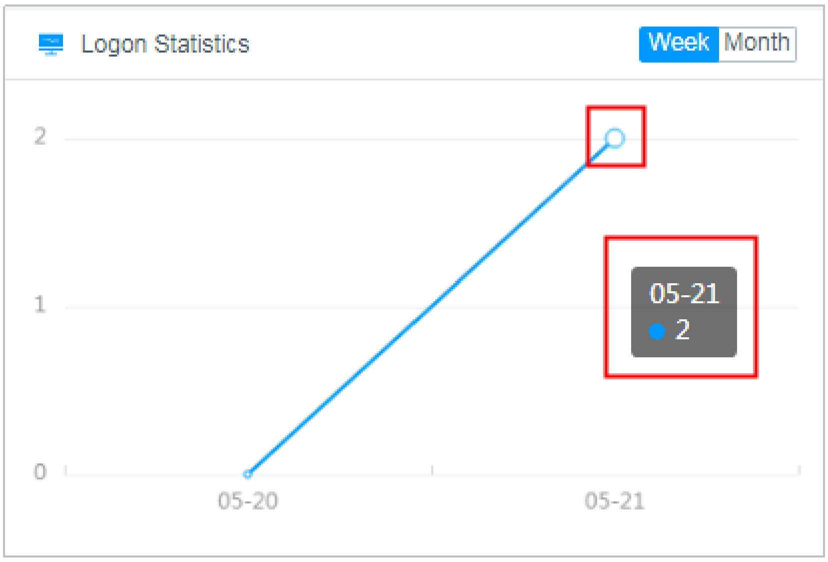
Logon Statistics

Displays the trend chart of the number of logins to the CBH 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 CBH system is logged in within a certain day, move your cursor over the corresponding date.

Figure 3-9 Logon Statistics



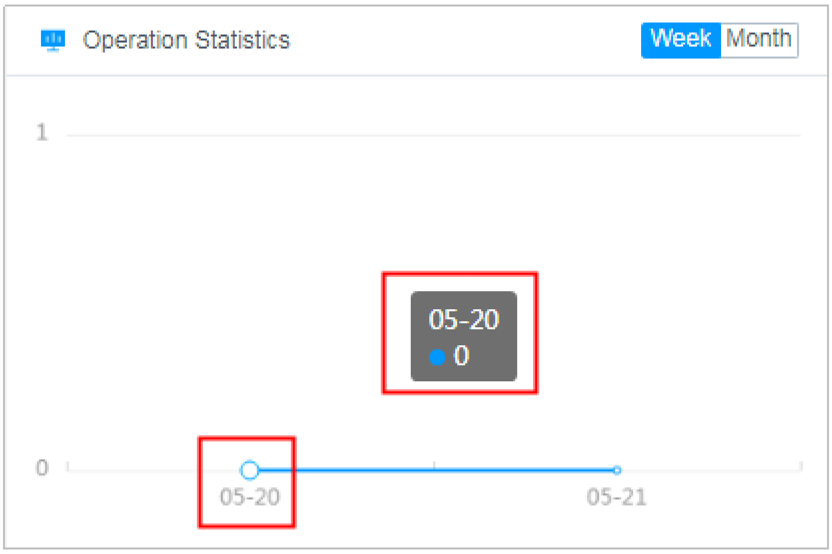
Operation Statistics

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 CBH system within a certain day, move your cursor over the corresponding date.

Figure 3-10 Operation Statistics



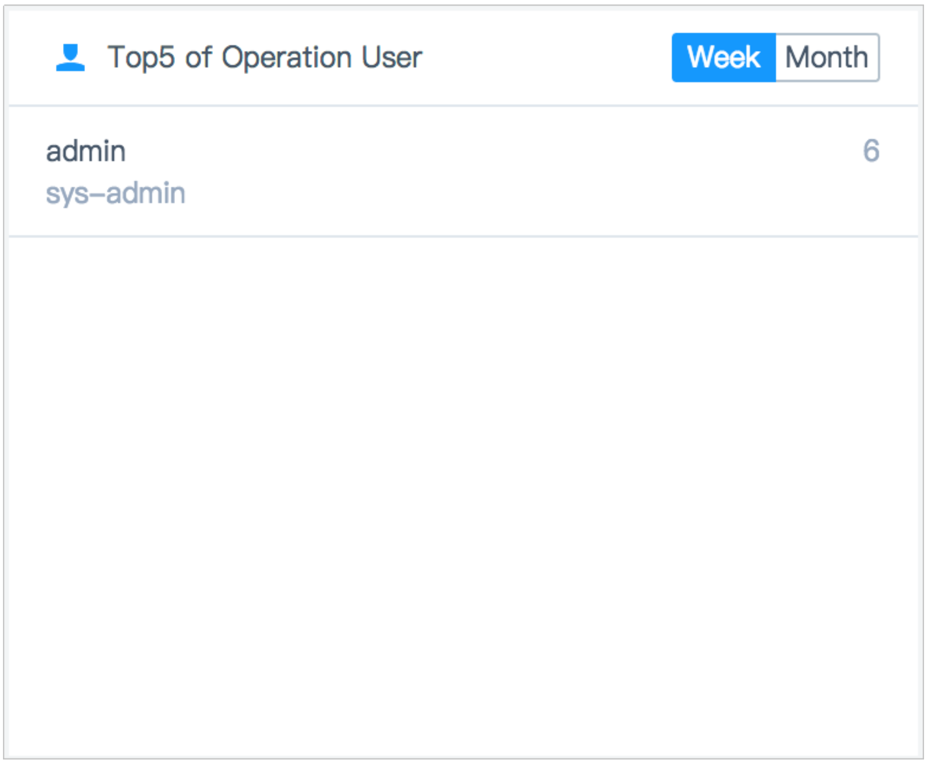
Top 5 of Operation User

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.

Figure 3-11 Top 5 of Operation User



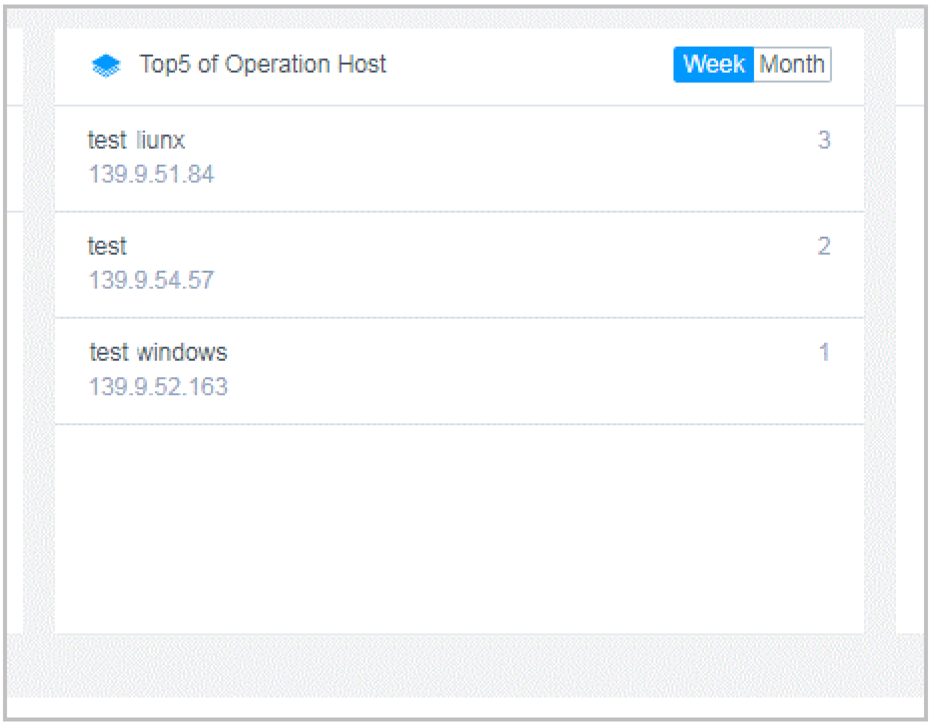
Top 5 of Operation Host

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.

Figure 3-12 Top 5 of Operation Host

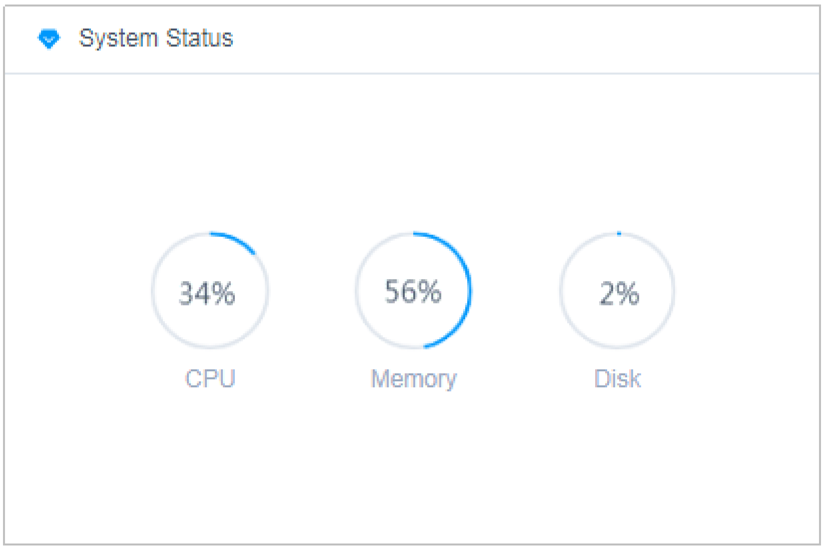


System Status

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.

Figure 3-13 System Status

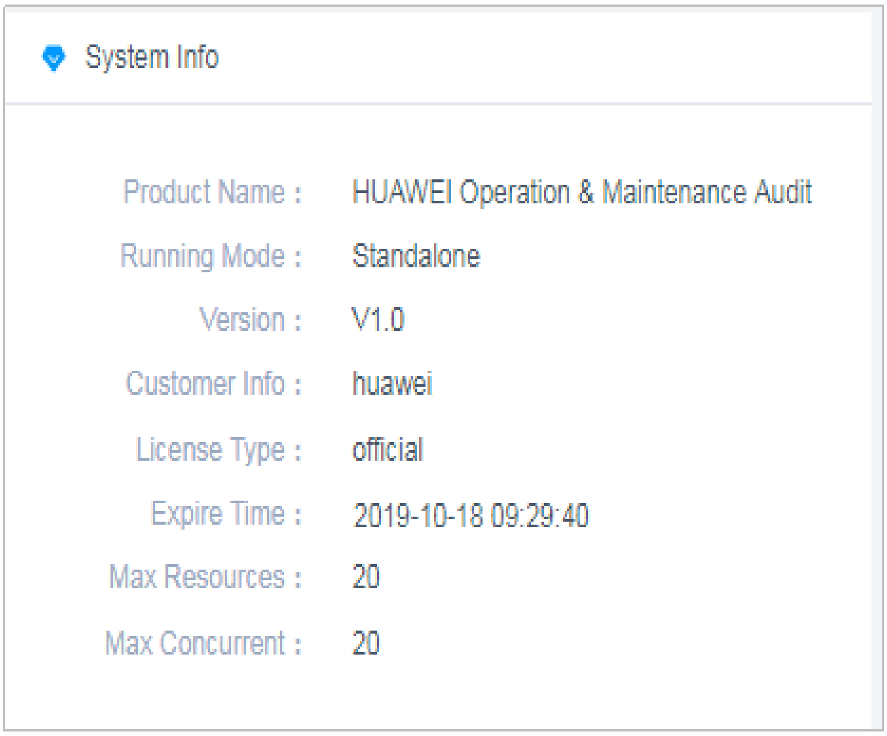


System Info

Displays the basic information about the current system and the specifications of the authorized system version.

To view information about your CBH system, obtain the management permission of the **System** module and the role management permission.

Figure 3-14 System Info



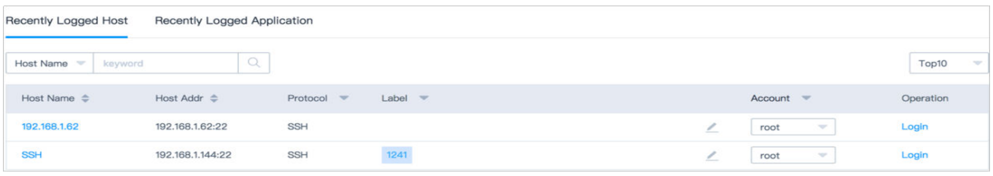
Recently Logged Host

Lists the host resources you have logged in recently.

To view recently logged in hosts, obtain the management permissions for the **Host Operation** 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.

Figure 3-15 Recently Logged Host



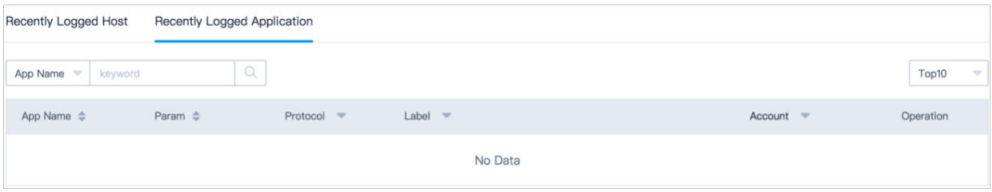
Recently Logged Application

Lists the application resources you have logged in recently.

To view recently logged in application resources, obtain the management permissions for the **App Operation** 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.

Figure 3-16 Recently Logged Application



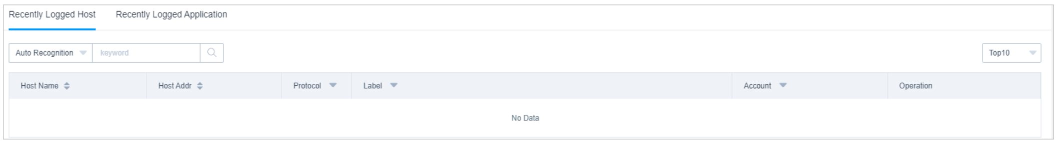
My Hosts

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 Operation** 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.

Figure 3-17 My Hosts



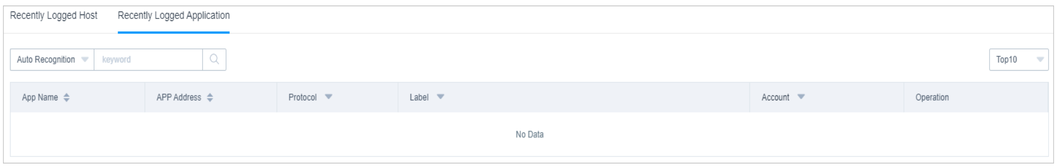
My APPs

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 Operation** 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.

Figure 3-18 My APPs



3.2 Profile

3.2.1 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.

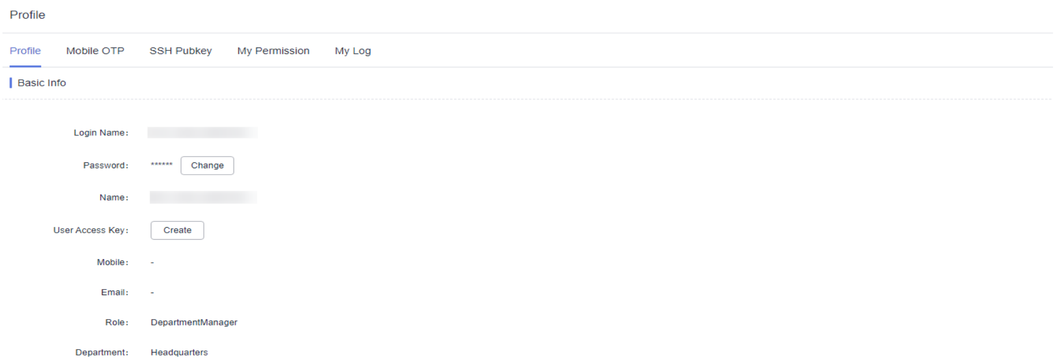
This topic walks you through how to view your profile.

Procedure

Step 1 Log in to the CBH system.

Step 2 On the **Dashboard** page, click the user name in the upper right corner and choose **Profile**.

Figure 3-19 Profile



Step 3 Click each tab to view the corresponding information.

You can view profile, mobile OTP, SSH public key, permission, and log information.

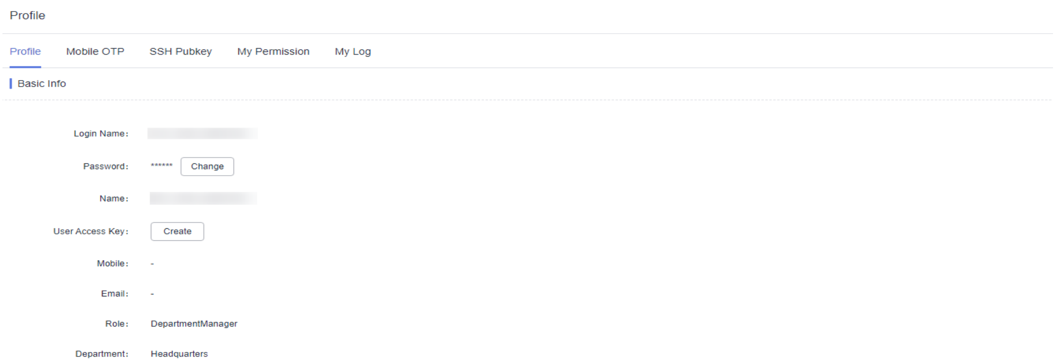
----End

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 3-20 Profile

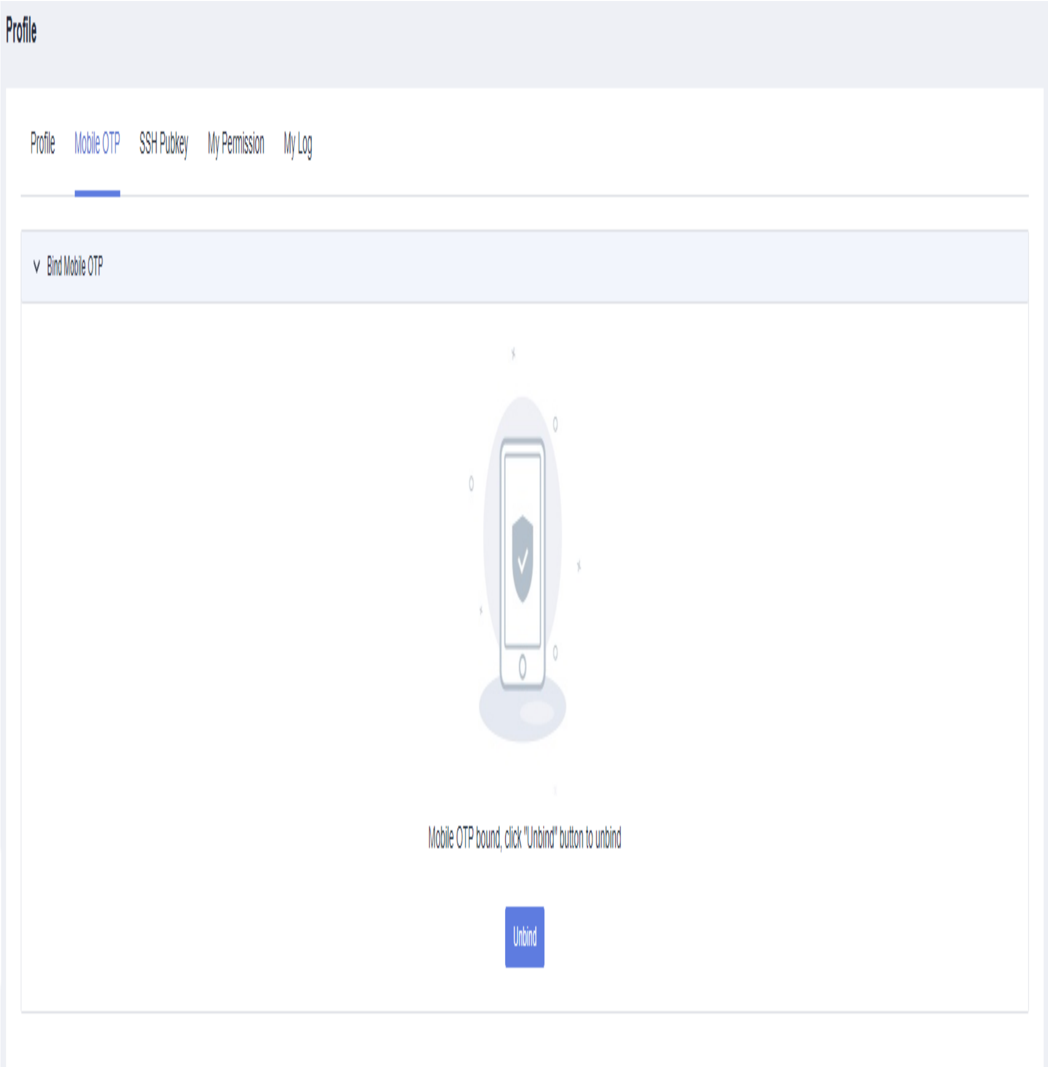


Mobile OTP

To view the mobile phone token bound to your current account, click the **Mobile OTP** tab.

For more details about how to bind or unbind a mobile phone token, see **Managing Mobile OTPs**.

Figure 3-21 Mobile OTP

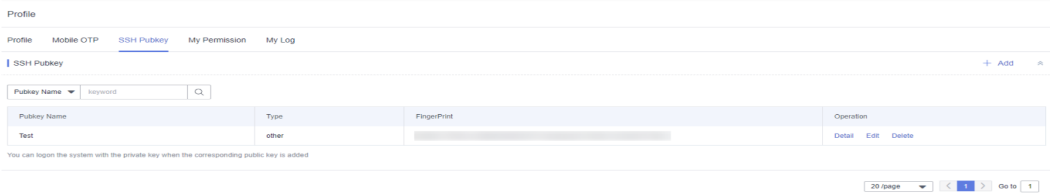


SSH Public Key

To view SSH public keys and their basic information, click the **SSH Pubkey** tab.

For details about how to add, modify, and delete a public key, see **Managing SSH Public Keys**.

Figure 3-22 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 the CBH system as system administrator **admin**.

Figure 3-23 Permissions of user **admin**


Dashboard / Profile

Profile

Profile | Mobile OTP | SSH Pubkey | My Permission | My Log

Permission List

Managing Permission : Enabled

Module	Function
Dashboard	-
Department	New Department、Modify Department、Delete Department
User	New User、Modify User、Delete User、View Password
User Group	New User Group、Modify User Group、Delete User Group
Role	New Role、Modify Role、Delete Role
USBKey	IssueUSBKey、RevokeUSBKey
OTP token	IssueOTP token、RevokeOTP token
Host	New Host、Modify Host、Delete Host、Download Host、Login Host、Auth Host、View Password、Del...
AppServer	New AppServer、Modify AppServer、Delete AppServer
Application	New App、Modify App、Delete App、Login App、Auth App、View Password
Account	New Account、Modify Account、Delete Account、View Password
Account Group	New Account Group、Modify Account Group、Delete Account Group
ACL Rules	New ACL Rules、Modify ACL Rules、Delete ACL Rules
Cmd Rules	New Cmd Rules 、Modify Cmd Rules 、Delete Cmd Rules
Chpwd Rules	New Chpwd Rules、Modify Chpwd Rules、Delete Chpwd Rules、common.receivePwd、common.recei...
Sync Rules	New Sync Rules、Modify Sync Rules、Delete Sync Rules
DB Rules	New DB Rules、Modify DB Rules、Delete DB Rules
Host Ops	-
App Ops	-
Script	New Script、Modify Script、Delete Script
Fast Ops	CMD ConsoleFast Ops、Script ConsoleFast Ops、File ConsoleFast Ops
OM Task	New OM Task、Modify OM Task、Delete OM Task
Live Session	Monitor Session、Interrupt Session
History Session	Download History Session
System Login	-
OperationLog	-
Ops Report	-
System Report	-
ACL Ticket	New ACL Ticket、Modify ACL Ticket、Delete ACL Ticket
Cmd Ticket	New Cmd Ticket、Modify Cmd Ticket、Delete Cmd Ticket
Approve	Approve Ticket
DB Tickets	New DB Tickets、Modify DB Tickets、Delete DB Tickets
System	-

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**.

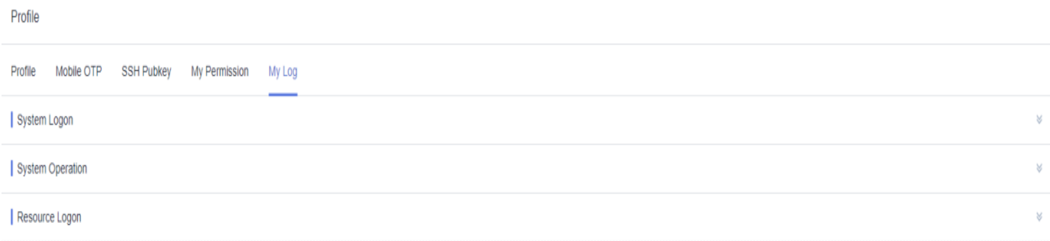
- System logon logs

  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 3-24 My Log



3.2.2 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 the CBH system 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**.

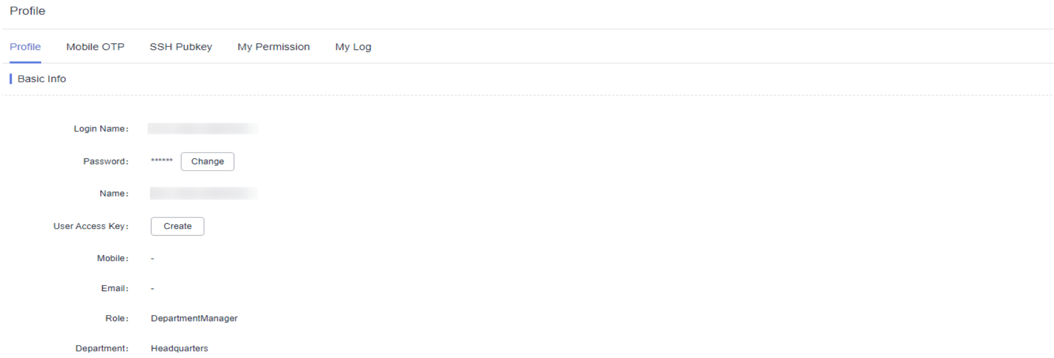
This topic describes how to change your password and modify basic information in the **Profile** area.

Changing Your Password

Step 1 Log in to the CBH system.

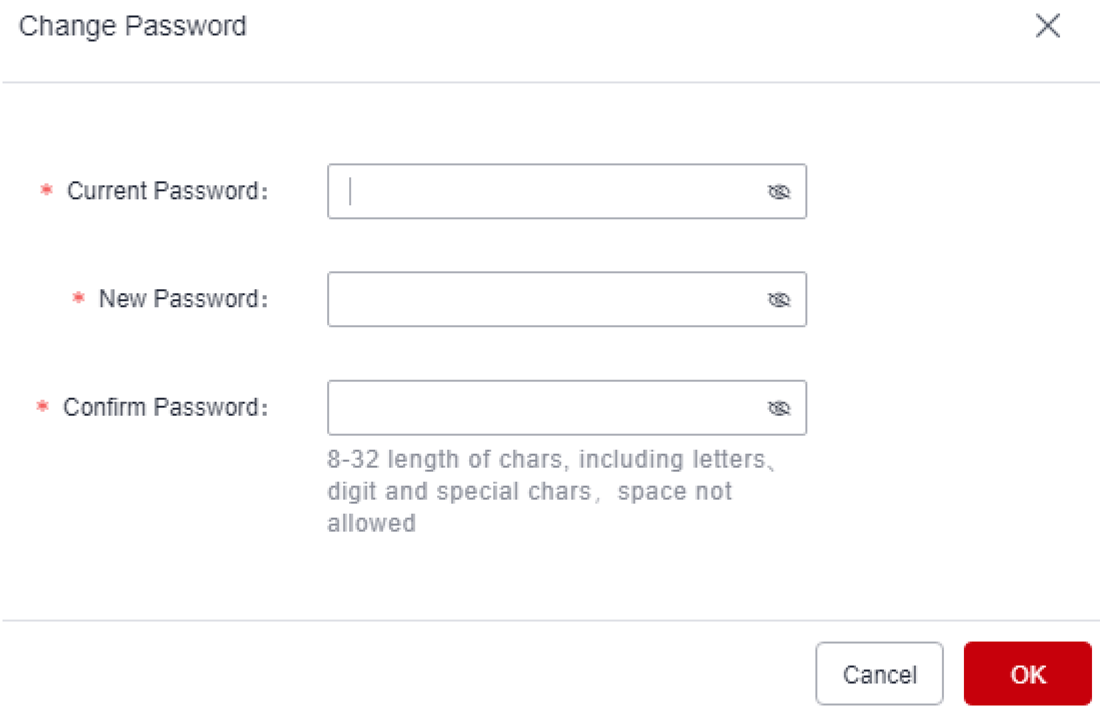
Step 2 On the **Dashboard** page, click the user name in the upper right corner and choose **Profile**.

Figure 3-25 Profile



Step 3 In the **Basic Info** area, click **Change** next to the **Password** field.

Figure 3-26 Change Password



Step 4 In the displayed dialog box, enter the current password and then specify a new password.

The new 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.

Step 5 Click **OK**.

Log out of the system. The new password takes effect after you log in to the system again.

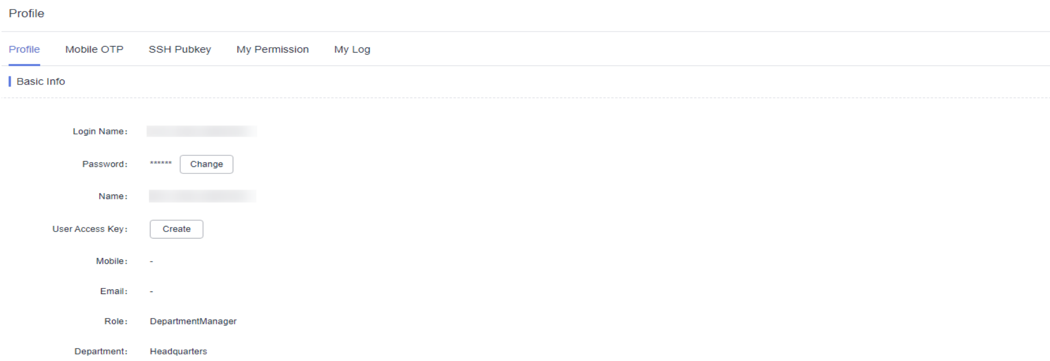
----End

Modifying Basic Information

Step 1 Log in to the CBH system.

Step 2 On the **Dashboard** page, click the user name in the upper right corner and choose **Profile**.

Figure 3-27 Profile



Step 3 Click **Edit** in the **Basic Info** area.

Figure 3-28 Modifying Basic Information

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

3.2.3 Managing Mobile OTP Application for Login Authentication

A mobile OTP application is a software token application used to generate a dynamic password on a bound mobile phone. A CBH system allows you to configure mobile one-time password (OTP) verification for multifactor login verification. After mobile OTP verification is configured, you are required to enter the user password and a 6-digit mobile OTP verification code when you log in to the CBH system. For details, see **Configuring Mobile OTP Login Authentication**.

Currently, CBH supports built-in mobile OTP and Remote Authentication Dial In User Service (RADIUS) mobile OTP.

- Built-in mobile OTP application: WeChat applet mobile OTP.
- RADIUS mobile OTP applications: Google Authenticator and FreeOTP

NOTICE

- Ensure that your CBH system 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 CBH 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.

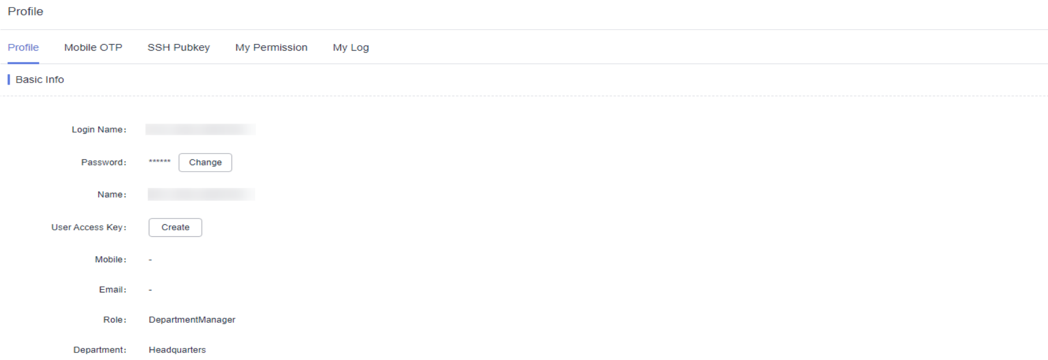
This topic describes how to bind and unbind a mobile OTP application.

Binding a Mobile OTP application to a User

Step 1 Log in to the CBH system.

Step 2 On the **Dashboard** page, click the user name in the upper right corner and choose **Profile**.

Figure 3-29 Profile



Step 3 Click the **Mobile OTP** tab.

Step 4 In the displayed **Mobile OTP** dialog box, bind a mobile OTP application as prompted.

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.

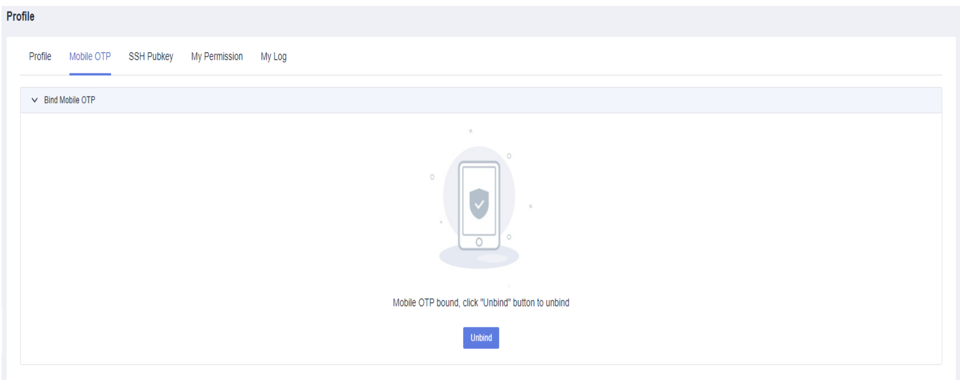
----End

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 3-30 Unbinding a mobile OTP application



3.2.4 Managing SSH Public Keys

Your SSH public key is used for passwordless login over the SSH client.

This topic describes how to add, modify, and delete an SSH public key.

Constraints

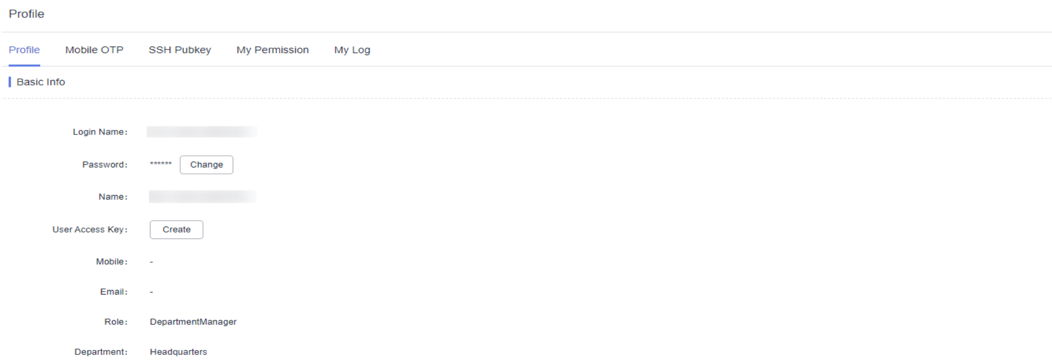
Only OpenSSH public keys are supported.

Adding an SSH Public Key

Step 1 Log in to the CBH system.

Step 2 On the **Dashboard** page, click the user name in the upper right corner and choose **Profile**.

Figure 3-31 Profile

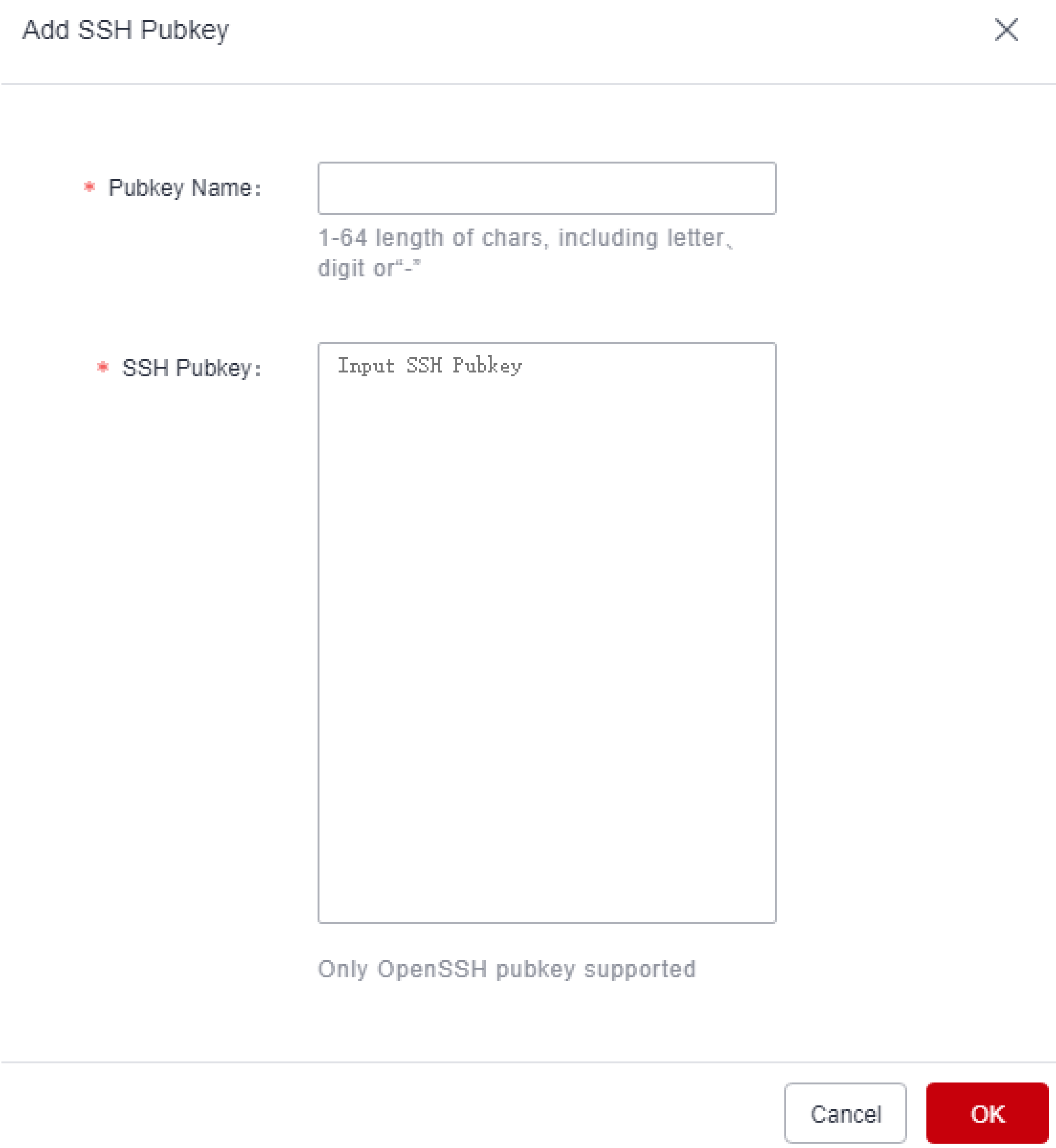


Step 3 Click the **SSH Pubkey** tab.

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.

Figure 3-32 Adding an SSH Public Key



Step 6 Click **OK**. You can view the added SSH public key.

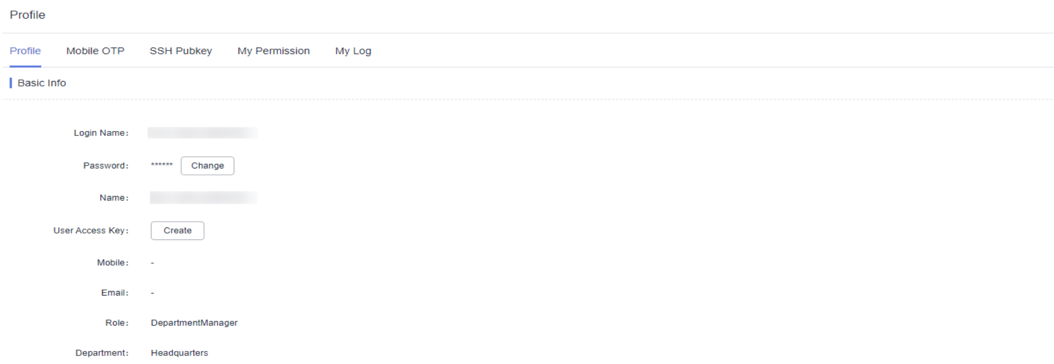
----End

Deleting an SSH Public Key

Step 1 Log in to the CBH system.

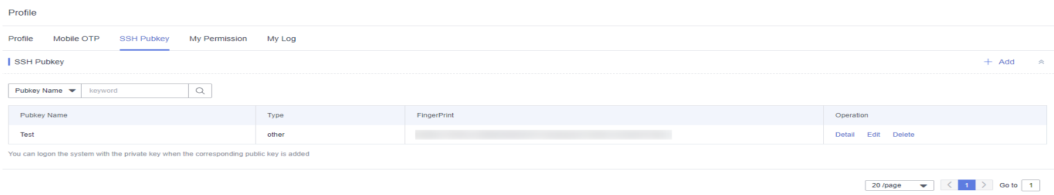
Step 2 On the **Dashboard** page, click the user name in the upper right corner and choose **Profile**.

Figure 3-33 Profile



Step 3 Click the **SSH Pubkey** tab.

Figure 3-34 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**.

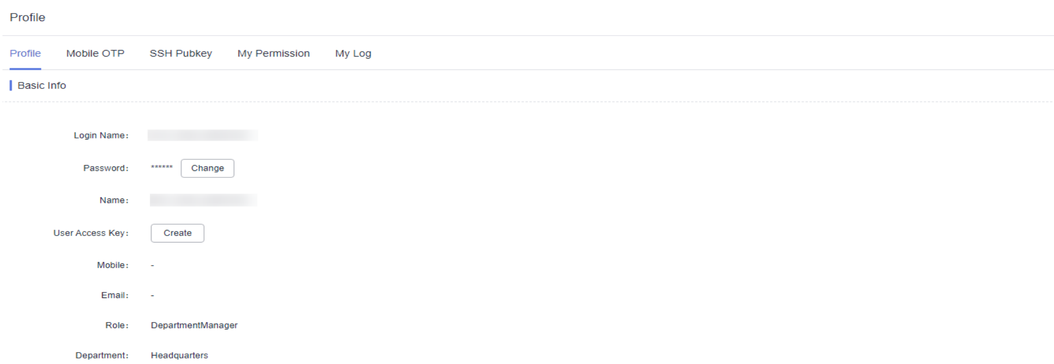
----End

Editing an SSH Public Key

Step 1 Log in to the CBH system.

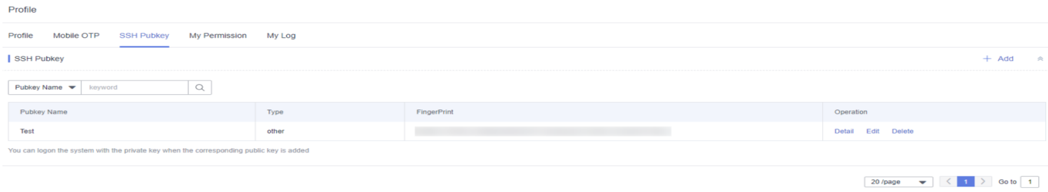
Step 2 On the **Dashboard** page, click the user name in the upper right corner and choose **Profile**.

Figure 3-35 Profile



Step 3 Click the **SSH Pubkey** tab.

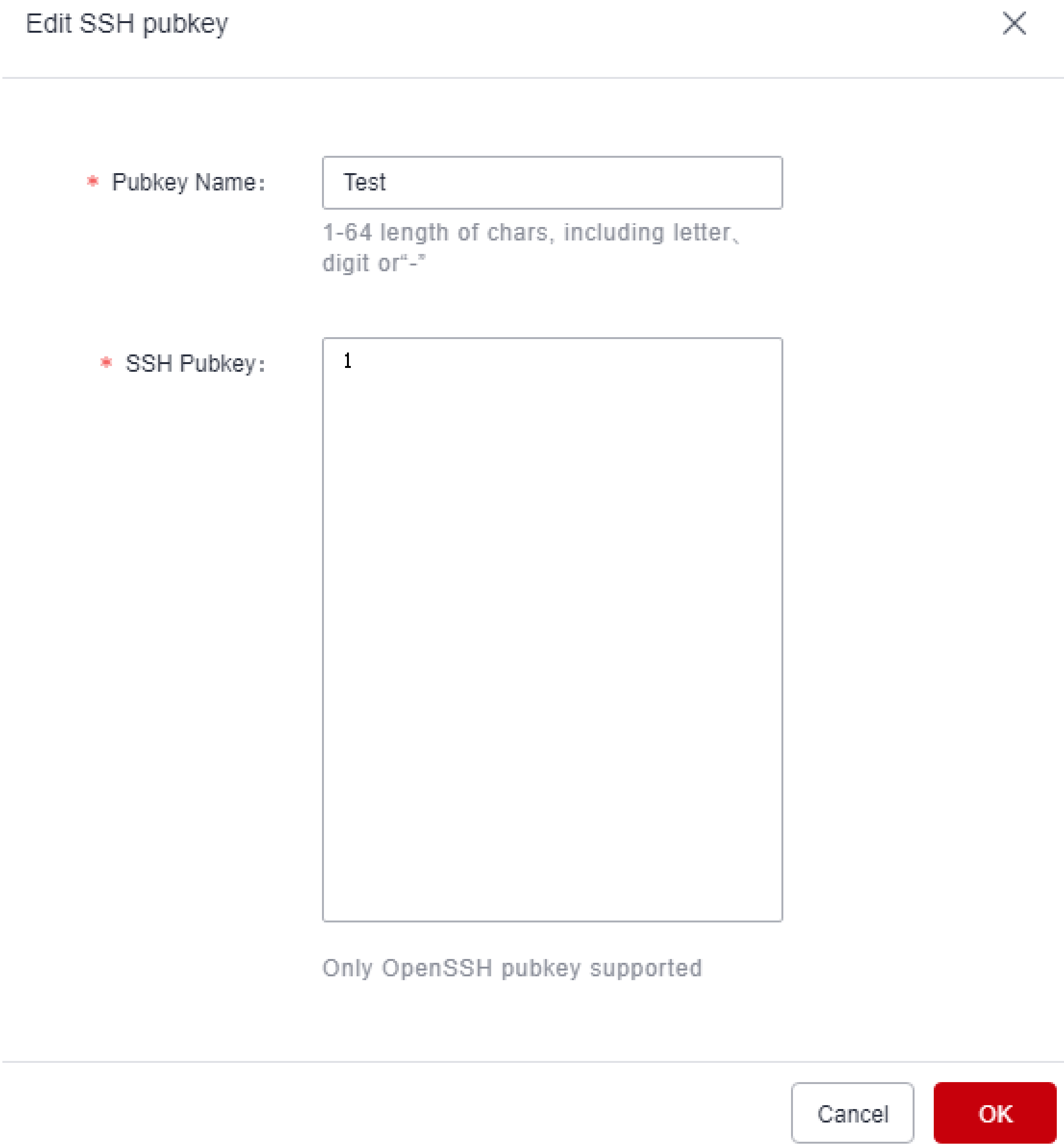
Figure 3-36 SSH Pubkey



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.

Figure 3-37 Editing an SSH Public Key



Step 6 Click **OK**. You can view the modified SSH public key.

----End

3.3 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, PBH 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**.

This topic describes how to view a task in the task center.

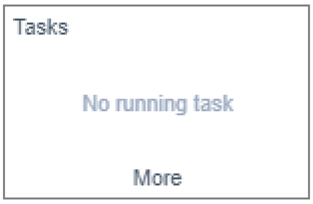
Procedure

Step 1 Log in to the CBH system.

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 3-38 Small task center window



Step 3 Click **More** to go to the **Tasks** page.

Figure 3-39 Viewing a task list

Step 4 Query tasks.

Enter a keyword in the search box and search for tasks by title.

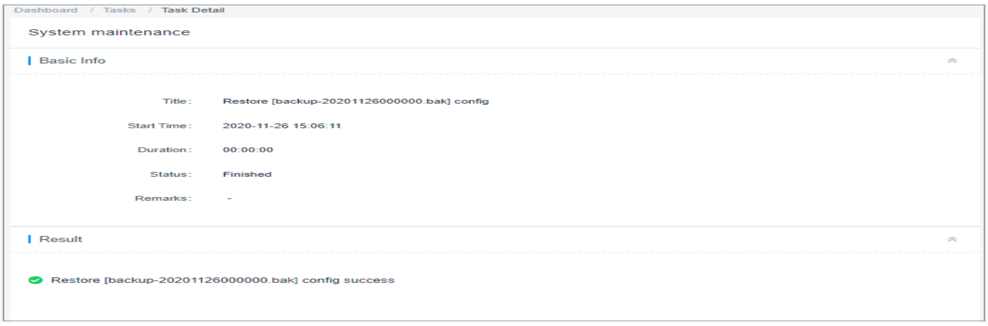
Step 5 View the tasks.

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 3-40 View task details.



----End

3.4 Messages

3.4.1 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**.

This topic describes how to view, delete, and mark messages in CBH message center.

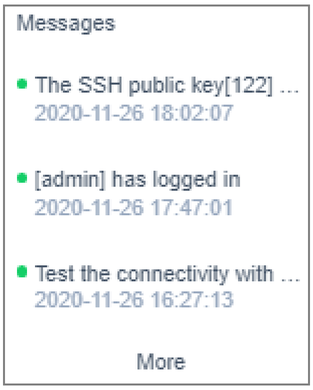
Viewing Messages

Step 1 Log in to the CBH system.

Step 2 Click in the upper right corner to view the latest three unread messages.

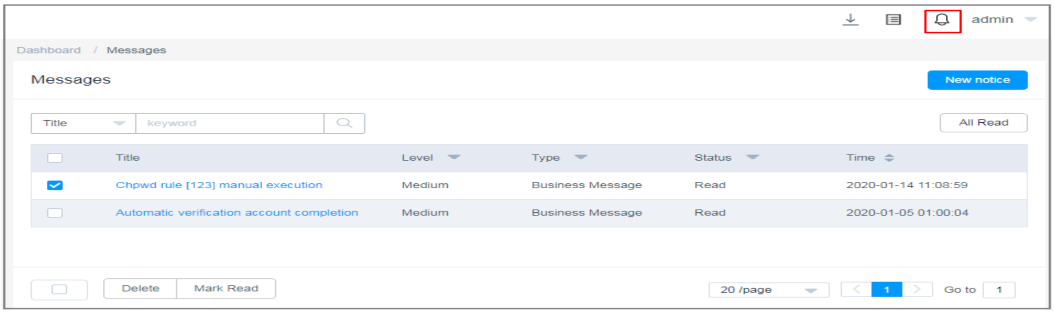
The following figure shows an example.

Figure 3-41 Small message center window



Step 3 Click **More** to go to the **Messages** page.

Figure 3-42 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 3-43 Message details

----End

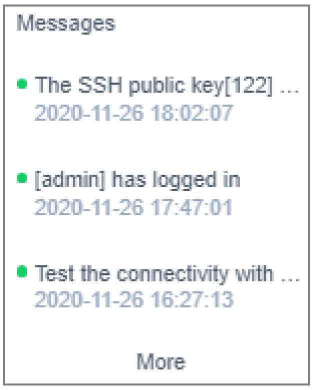
Deleting a Message

Step 1 Log in to the CBH system.

Step 2 Click in the upper right corner to view the latest three unread messages.

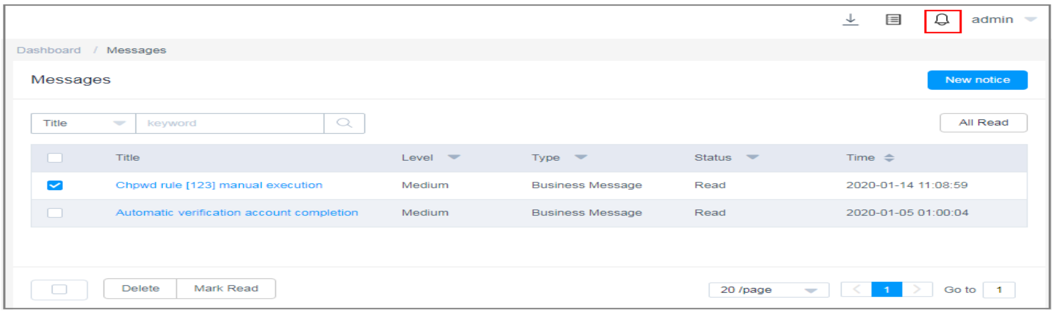
The following figure shows an example.

Figure 3-44 Small message center window



Step 3 Click **More** to go to the **Messages** page.

Figure 3-45 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

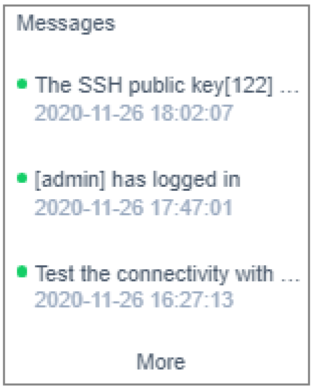
Marking a Message

Step 1 Log in to the CBH system.

Step 2 Click in the upper right corner to view the latest three unread messages.

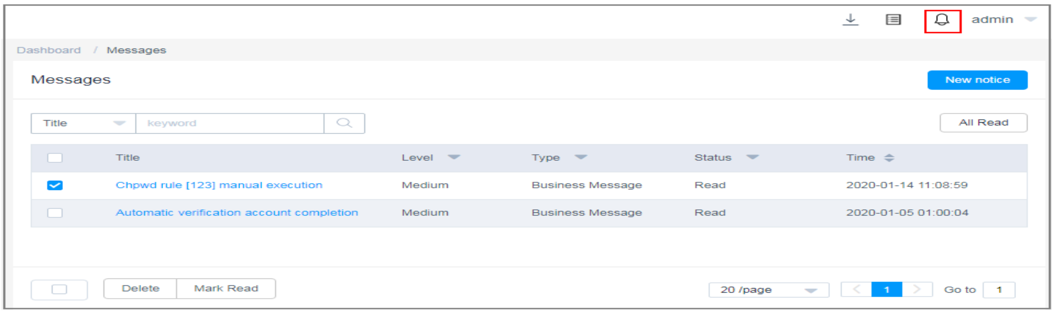
The following figure shows an example.

Figure 3-46 Small message center window



Step 3 Click **More** to go to the **Messages** page.

Figure 3-47 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

3.4.2 Creating a CBH 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.

This topic describes how to create system notices in the message center.

Constraints

- Only system administrator **admin** can create system notices.
- A system notice is intended for all users in the CBH system. It cannot be customized.
- Only one system notice can be shown each time.

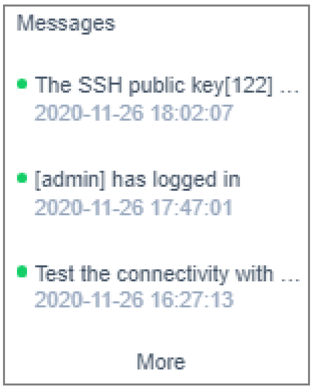
Procedure

Step 1 Log in to the CBH system.

Step 2 Click in the upper right corner to view the latest three unread messages.

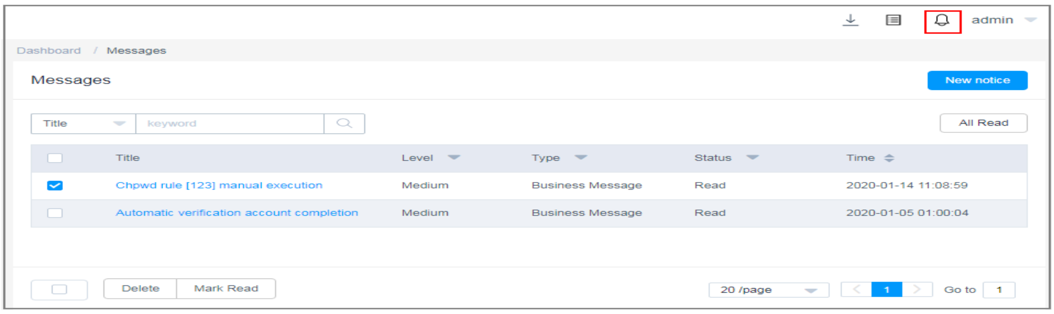
The following figure shows an example.

Figure 3-48 Small message center window



Step 3 Click **More** to go to the **Messages** page.

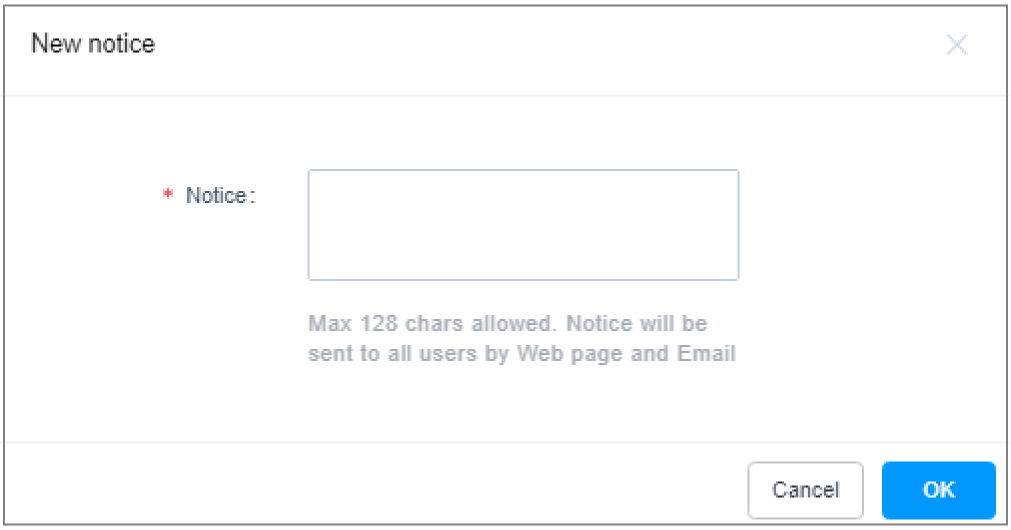
Figure 3-49 Message list



Step 4 Click **New notice**.

Step 5 In the displayed **New notice** dialog box, enter the content.

Figure 3-50 New notice



Step 6 Click **OK**. You can view the unread system notice.

Figure 3-51 Example notice

----End

3.5 Download Center

The CBH system is compatible with a wide range of client tools, including database clients. We provide their download links in the **Download Center**.

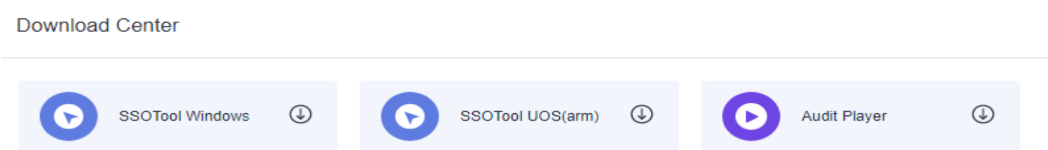
The topic describes how to enter the download center of your CBH system.

Procedure

Step 1 Log in to the CBH system.

Step 2 Click in the upper right corner. The download center client tool list page is displayed.

Figure 3-52 Download Center



Step 3 Click ⓘ next to a client tool to go to the third-party tool page and download the tool as required.

----End

4 Department

4.1 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 4-1 Department management

4.2 Creating a Department

The default department **HQ** is the top department in a CBH system. You can create departments only under **HQ**.

Prerequisites

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

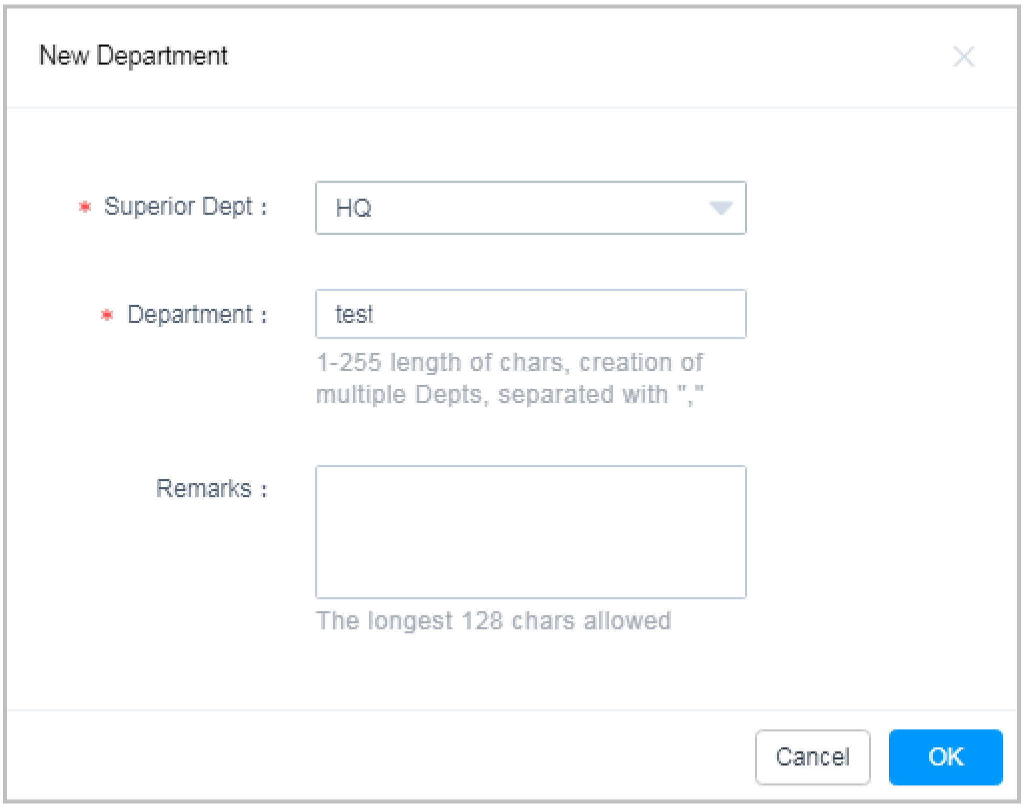
Procedure

Step 1 Log in to the CBH system.

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.

Figure 4-2 Creating a Department



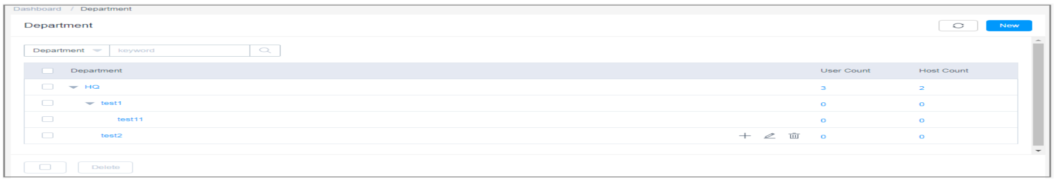
Step 4 Select a superior department for **Superior Dept**, enter a name of the department to be created in the **Department** field, and enter the description in the **Remarks** area if necessary.

NOTE

- The department name defined in a CBH system 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.

Figure 4-3 Creating a department



----End

How to Create a Department Quickly

Step 1 Log in to the CBH system.

Step 2 Select **Department** in the navigation pane on the left.

Step 3 In the column of the corresponding superior department, click + to create a lower-level department.

Step 4 Change the department name.

----End

4.3 Deleting a Department

The default department **HQ** is the top department in a CBH system 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 the CBH system.

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

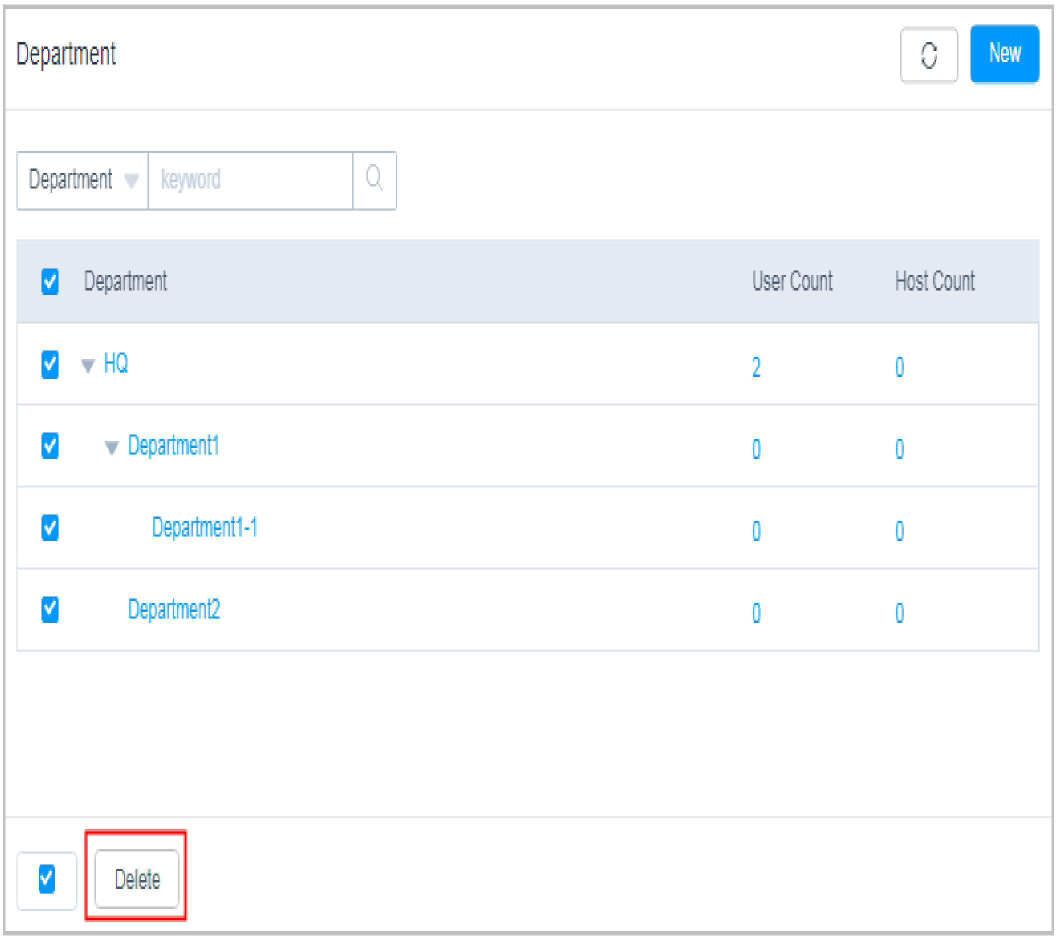
Deleting a department will delete all its lower-level departments, users, and resources under the department and all its lower-level departments.

Figure 4-4 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 4-5 Batch deleting departments



----End

4.4 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 the CBH system.

Step 2 Select **Department** in the navigation pane on the left.

Step 3 Click the name of the department to be edited.

Figure 4-6 Basic department information

Step 4 In the **Basic Info** area, view the detailed information about the department.

Click **Edit** and edit basic information.

----End

4.5 Querying Configurations of a Department

CBH collects 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.

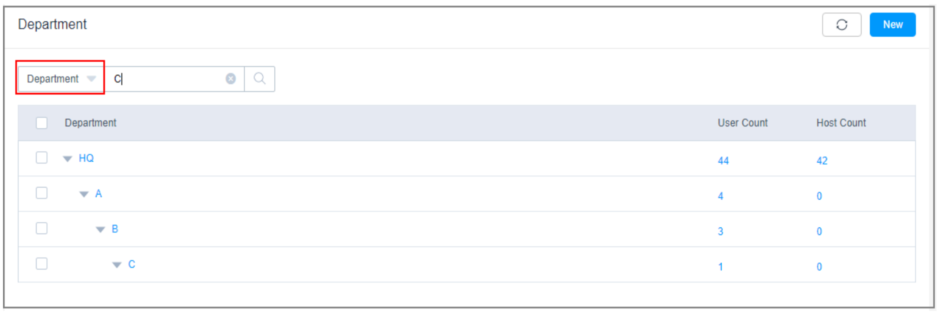
Procedure

Step 1 Log in to the CBH system.

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.

Figure 4-7 Querying a department



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

5 User

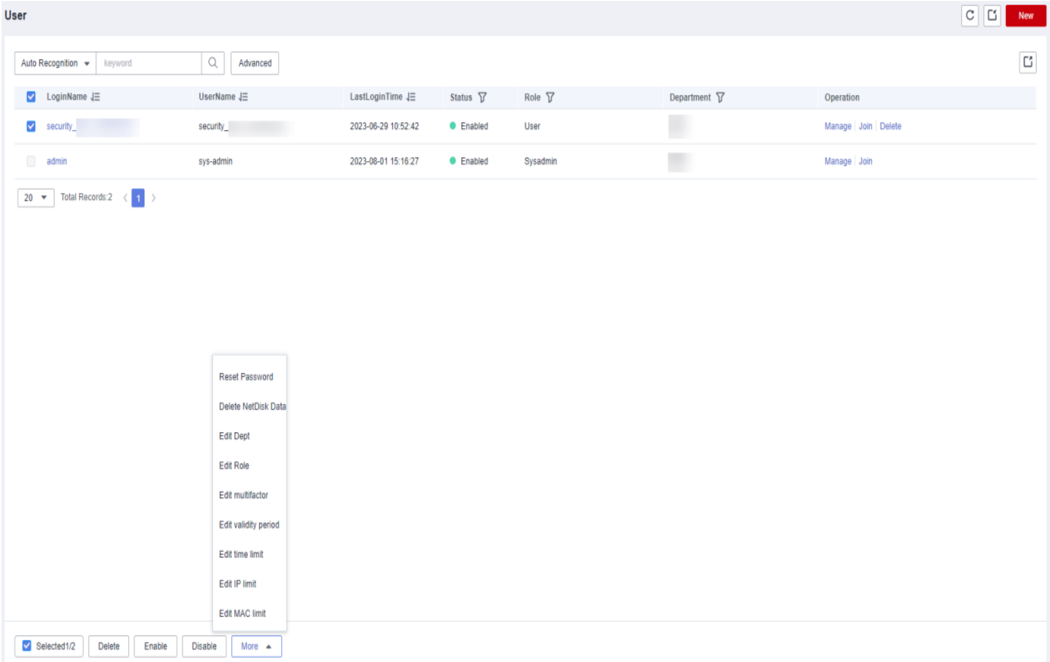
5.1 Overview

A CBH system allows you to centrally manage users. Creating a CBH system user is to create an account for logging in to the CBH system. The system administrator **admin** is the first account for users to log in to a CBH system 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 CBH 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.

Figure 5-1 User Management



5.2 User Management

5.2.1 Creating a User and Assigning a Role to the User

You can create users, import external users, and synchronize users from an Active Directory (AD) server so that those users can log in to and use the CBH system for O&M.

The **admin** user has the highest permissions for the corresponding CBH system and is the first user who can log in to the CBH system. 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 the CBH system.

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 5-2 New User

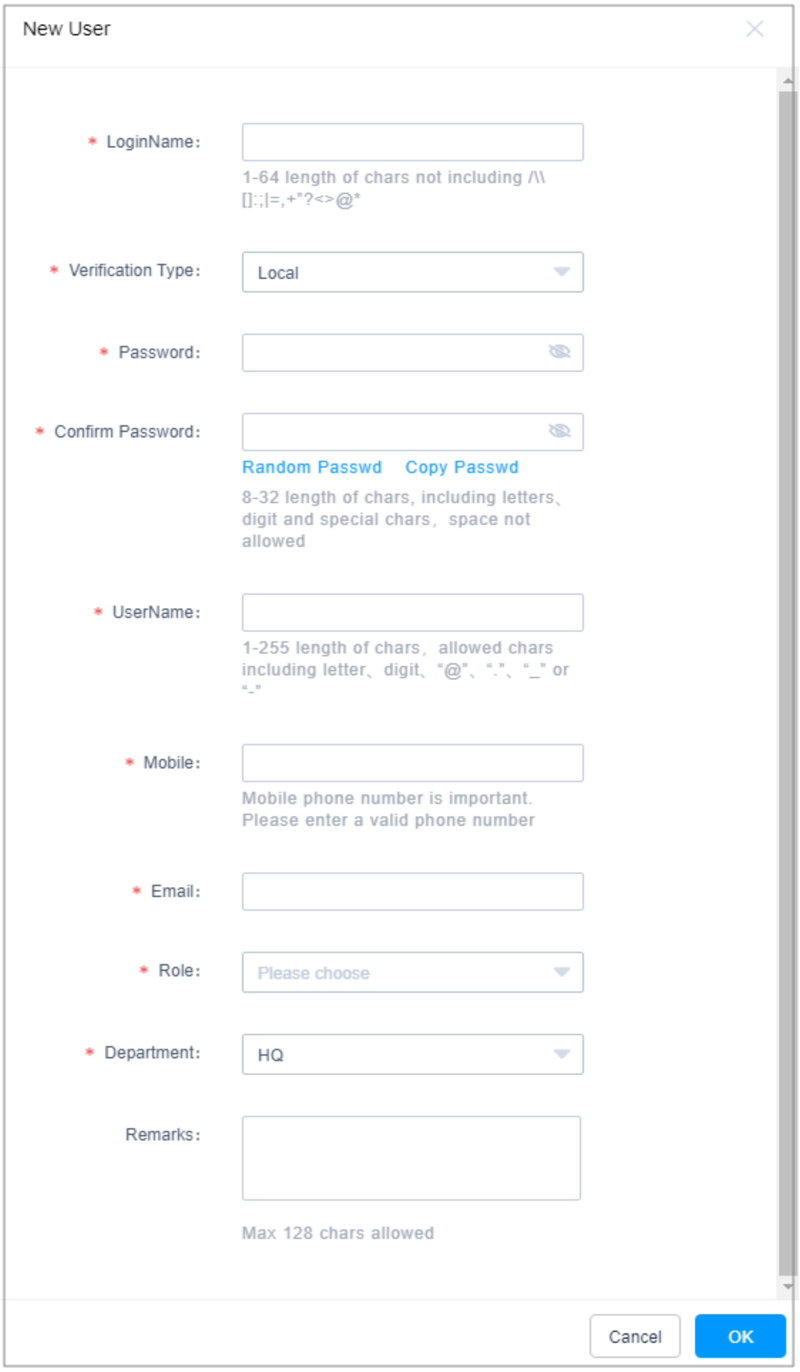


Table 5-1 Parameters for creating a user

Parameter	Description
LoginName	Specifies the username for logging in to the CBH system. The **LoginName** must be unique in a CBH system and cannot be changed once created.
Verification Type	Specifies how the user is verified for logging in to the CBH system. • **Local**: (default method) The user is verified against the account management system of the CBH system. • **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 CBH system. 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 CBH system if you select **Local** for **Verification Type**.
Authentication server	An authentication server must be configured if you select **AD** or **LDAP** for **Verification Type**.
UserName	Specifies the user-defined user name. This name indicates the name of the person who uses the account so that CBH 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 CBH system 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 Operation**, **App Operation**, and **Ticket approval** modules. • User-defined role: Only the **admin** user can customize a new role or edit permissions of a default role. For details, see **Role Overview**.
Department Name	Specifies the department to which the user belongs. For details about how to create a department in a CBH system, see **Creating a Department**.
Remarks	(Optional) Provides supplementary information about the user.

Step 4 Click **OK**.

----End

Batch Importing Users

Step 1 Log in to the CBH system.

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

Step 3 Click **Import** 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 5-2 Template parameters

Parameter	Description
LoginName	(Mandatory) Specifies the username for the user to log in to the CBH system.

Parameter	Description
Verification Type	(Mandatory) Specifies the authentication method. Only one authentication method can be entered. This parameter can be set to **Local**, **AD Domain**, **LDAP**, or **RADIUS**.
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	(Mandatory) Specifies the name of a system user.
Mobile	(Mandatory) Specifies the mobile number of a system user.
Email	(Mandatory) Specifies the email address of a system user.
Role	(Mandatory) Specifies 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 CBH system can be entered.
Department Name	(Mandatory) Specifies 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 CBH 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 CBH 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 CBH 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

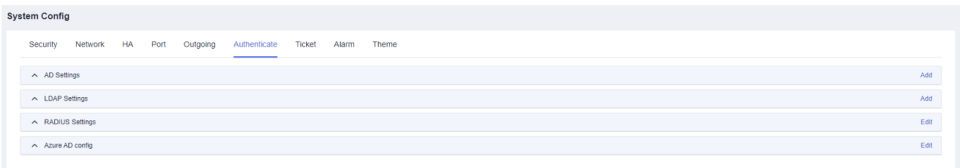
Synchronizing AD Domain Users

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

Step 1 Log in to the CBH system.

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

Figure 5-3 Configuring remote authentication



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

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

Figure 5-4 AD Settings

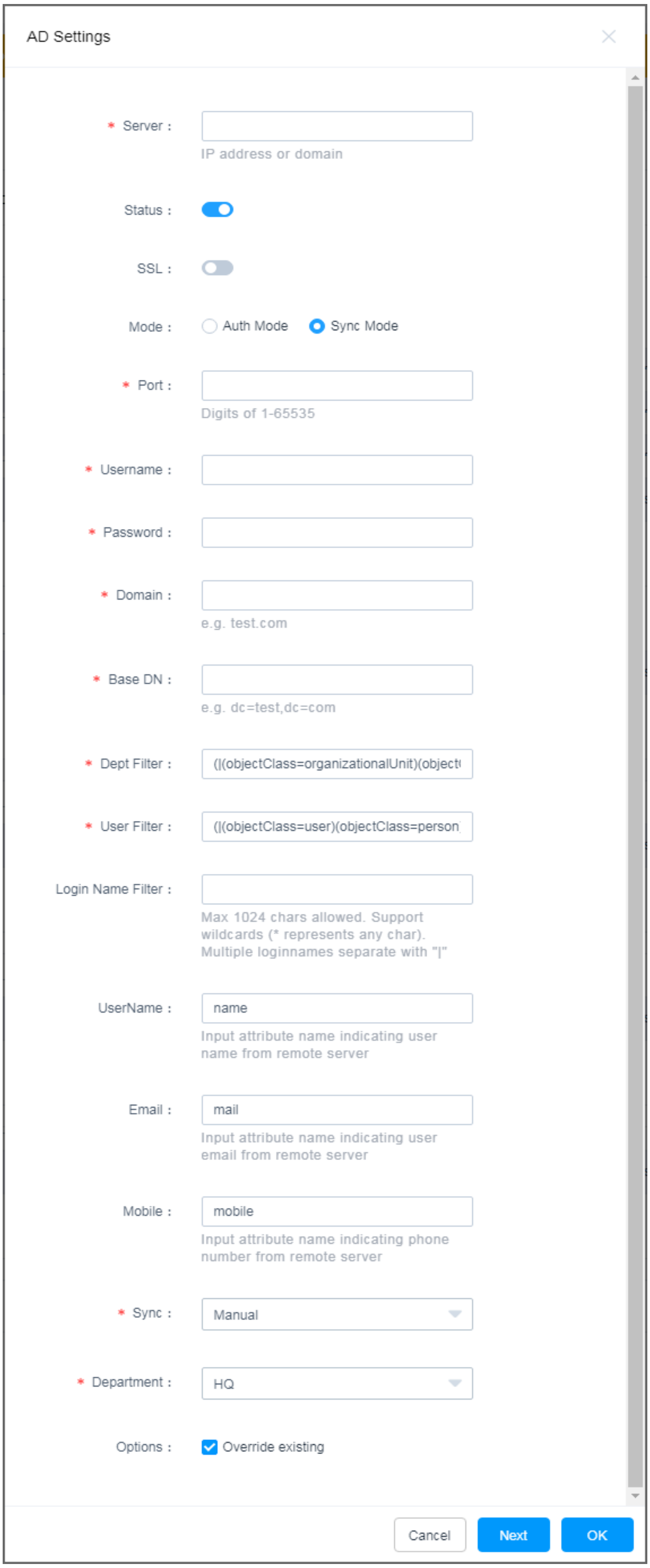


Table 5-3 AD settings for synchronizing users

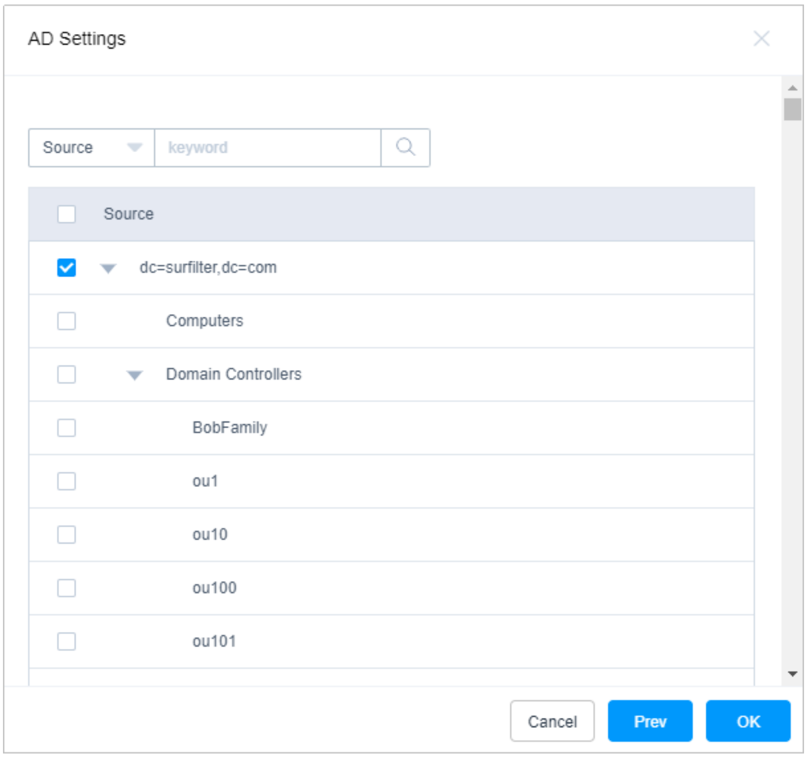
Parameter	Description
Server	Specifies the IP address of the AD domain server.
Status	Specifies whether to enable AD domain remote authentication. AD domain remote authentication is enabled by default. ● Enabled: AD domain authentication is enabled. If the configuration information is valid, AD domain authentication is enabled or AD domain users are synchronized to the CBH system when the user logs in to the CBH system. ● 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.
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.

Parameter	Description
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 CBH 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 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.

Figure 5-5 Importing users from a source



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 the CBH system. You can view the synchronized user information in the user list.

----End

5.2.2 Enabling or Disabling a User

CBH allows you to batch **Enable** or **Disable** other users and change the user account status with 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 CBH system within the permission scope.

- Disable

  The user account status is changed to **Disabled**. Disabled users cannot log in to the CBH system. 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.

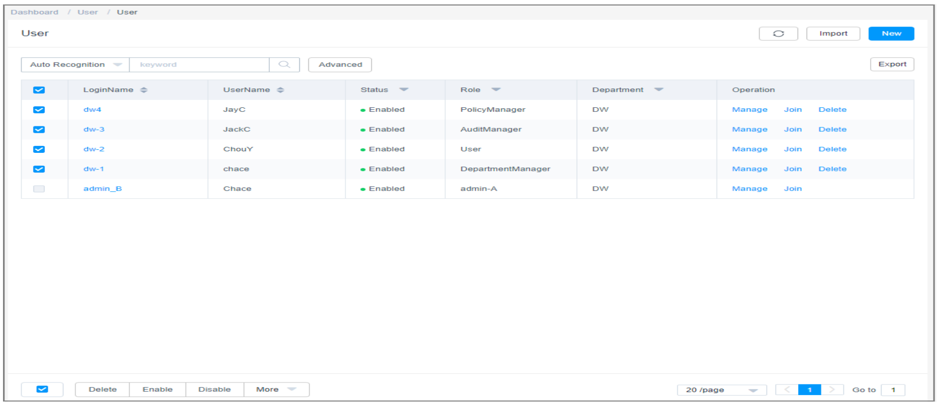
Procedure

Step 1 Log in to the CBH system.

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

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.

Figure 5-6 Enabling or Disabling a User



----End

5.2.3 Deleting a User

CBH allows you to delete users one by one or in batches.

After a user account is deleted, the user has no permissions, and files in the user's personal net disk are cleared.

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

Prerequisites

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

Procedure

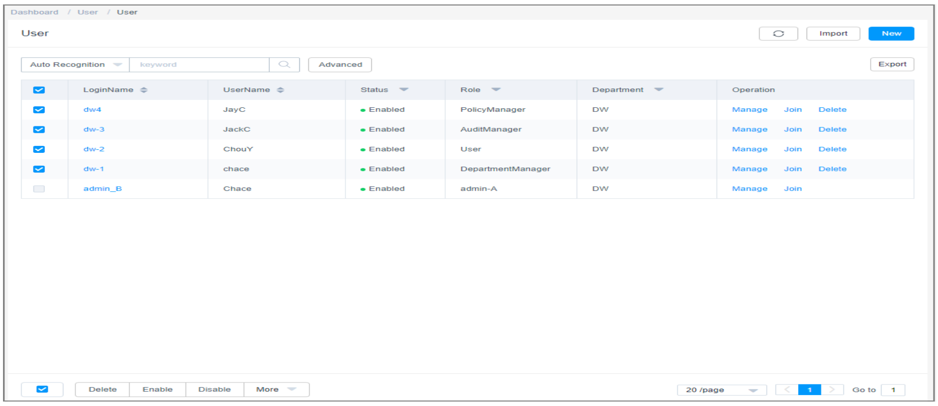
Step 1 Log in to the CBH system.

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

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.

Figure 5-7 Deleting a User



----End

5.2.4 Configuring User Login Restrictions

Overview

To effectively reduce security risks caused by user account leakage, CBH allows you to 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 the CBH system.
- Login limit by time: allows or forbids a user account to log in to the CBH system at the specified duration.
- Login limit by IP address: allows or forbids only users from specified IP addresses to log in to the CBH system.
- Login limit by MAC address: allows or forbids only users with specified MAC addresses on a LAN to log in to the CBH system.

Constraints

- To use the **Mobile OTP** authentication, ensure that the CBH 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.

Procedure

Step 1 Log in to the CBH system.

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

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.

Figure 5-8 Editing user setting

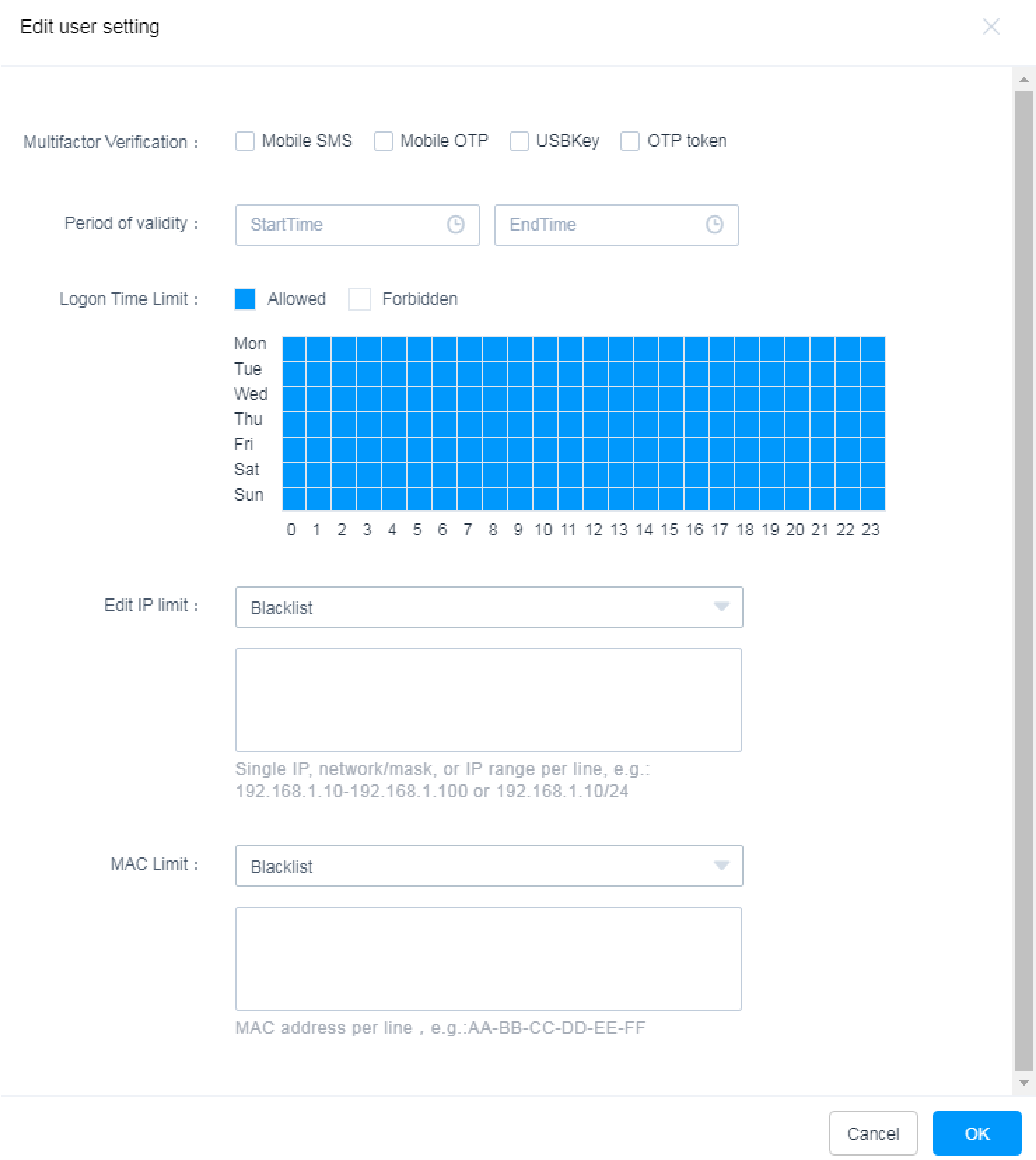


Table 5-4 User login limit parameters

Parameter	Description
Multifactor Verification	Specifies the authentication methods for users to log in to the CBH system. 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**.
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 CBH system 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 CBH system 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 CBH system. ● **Whitelist**: allows only users from configured MAC addresses to log in to the CBH system. ● 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

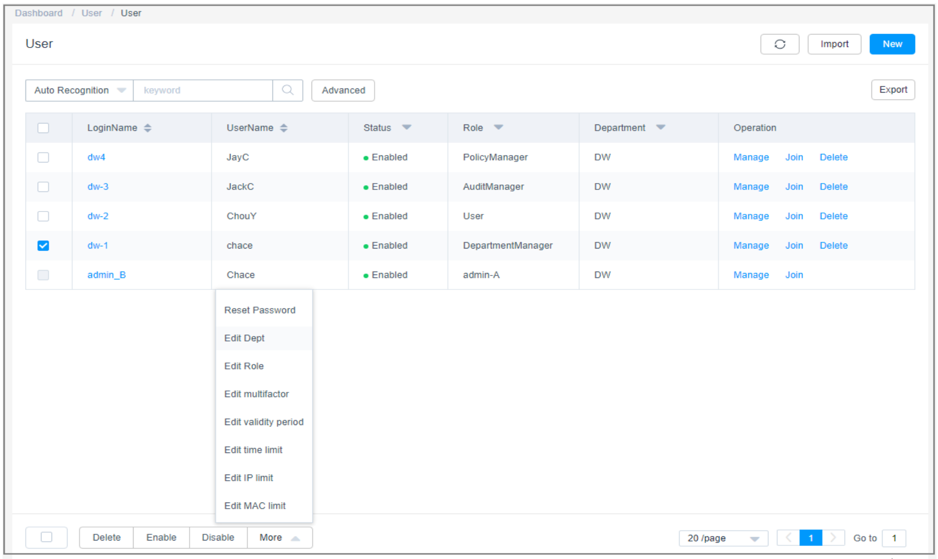
Batch Changing User Login Configurations

Step 1 Log in to the CBH system.

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

Step 3 Select the user accounts you want to edit and click **More** in the lower left corner.

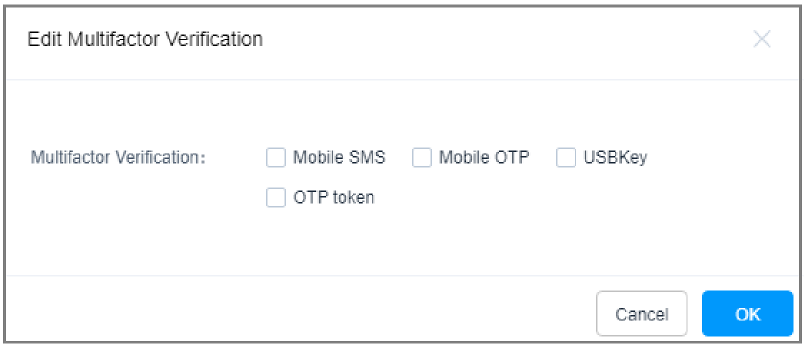
Figure 5-9 Batch editing login configurations



Step 4 Edit or disable multifactor verification configuration for several users at a time.

1. Click **Edit multifactor**.

Figure 5-10 Batch editing multifactor verification



2. In the displayed **Edit Multifactor Verification** dialog box, select or deselect one or more multifactor verification methods.
3. Click **OK**.

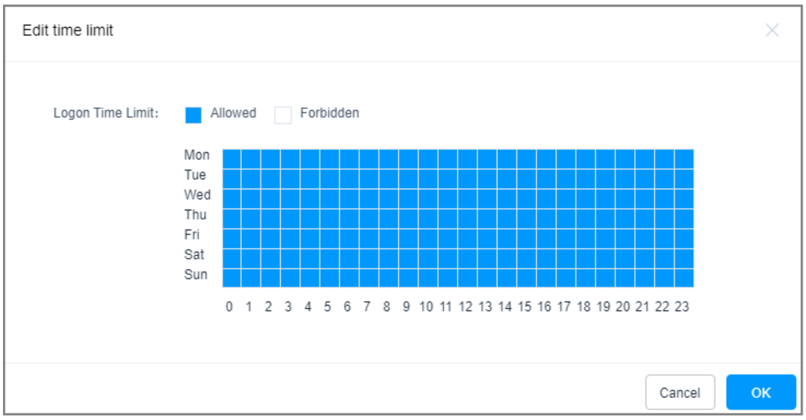
Step 5 Edit or disable period of validity for several users at a time.

1. Click **Edit validity period**.
2. In the displayed **Edit period of validity** dialog box, select **Edit StartTime** or **Edit EndTime** and specify the time. If you deselect the check box, the corresponding validity period configuration is disabled.
3. Click **OK**.

Step 6 Edit login limit configurations for several users at a time.

1. Click **Edit time limit**.

Figure 5-11 Edit time limit



2. In the displayed **Edit time limit** dialog box, select **Allowed** or **Forbidden** and specify time limit by the day and hour.
3. Click **OK**.

Step 7 Edit or disable IP address login limit for several users at a time.

1. Click **Edit IP limit**.

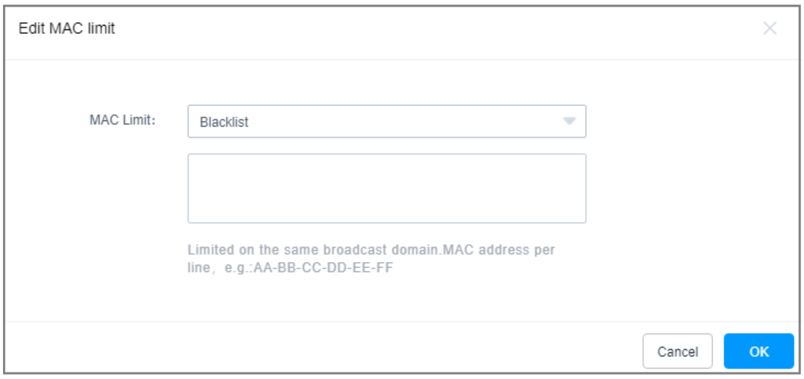
Figure 5-12 Edit IP limit

2. In the displayed **Edit IP limit** dialog box, select **Blacklist** or **Whitelist** and enter or delete the IP address or address range.
3. Click **OK**.

Step 8 Edit or disable the MAC login limit for several users at a time.

1. Click **Edit MAC limit**.

Figure 5-13 Edit MAC limit



2. In the displayed **Edit MAC limit** dialog box, select **Blacklist** or **Whitelist** and enter or delete the MAC address.
3. Click **OK**.

----End

5.2.5 Querying and Editing User Information

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

CBH allows you to 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.

Querying a User

Step 1 Log in to the CBH system.

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

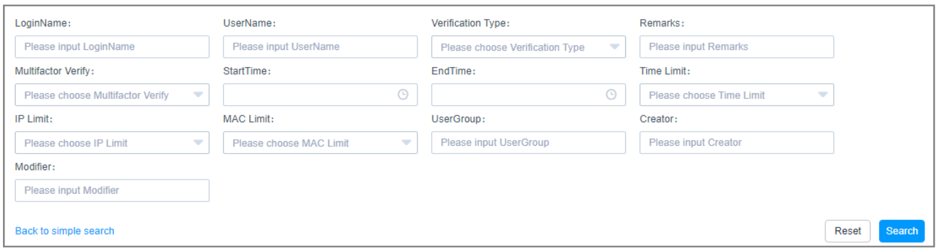
Step 3 Quick search

Enter a keyword in the search box and search for a user by login name or username.

Step 4 Advanced search

Enter keywords in the corresponding attribute search boxes to search for users in exact mode.

Figure 5-14 Advanced search



----End

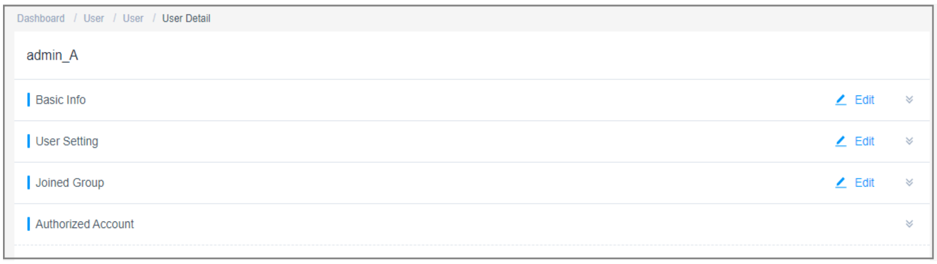
Viewing and Editing User Information

Step 1 Log in to the CBH system.

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

Step 3 In the user list, click the login name of the user you want, or click **Manage** in the row of the user in the **Operation** column.

Figure 5-15 User details

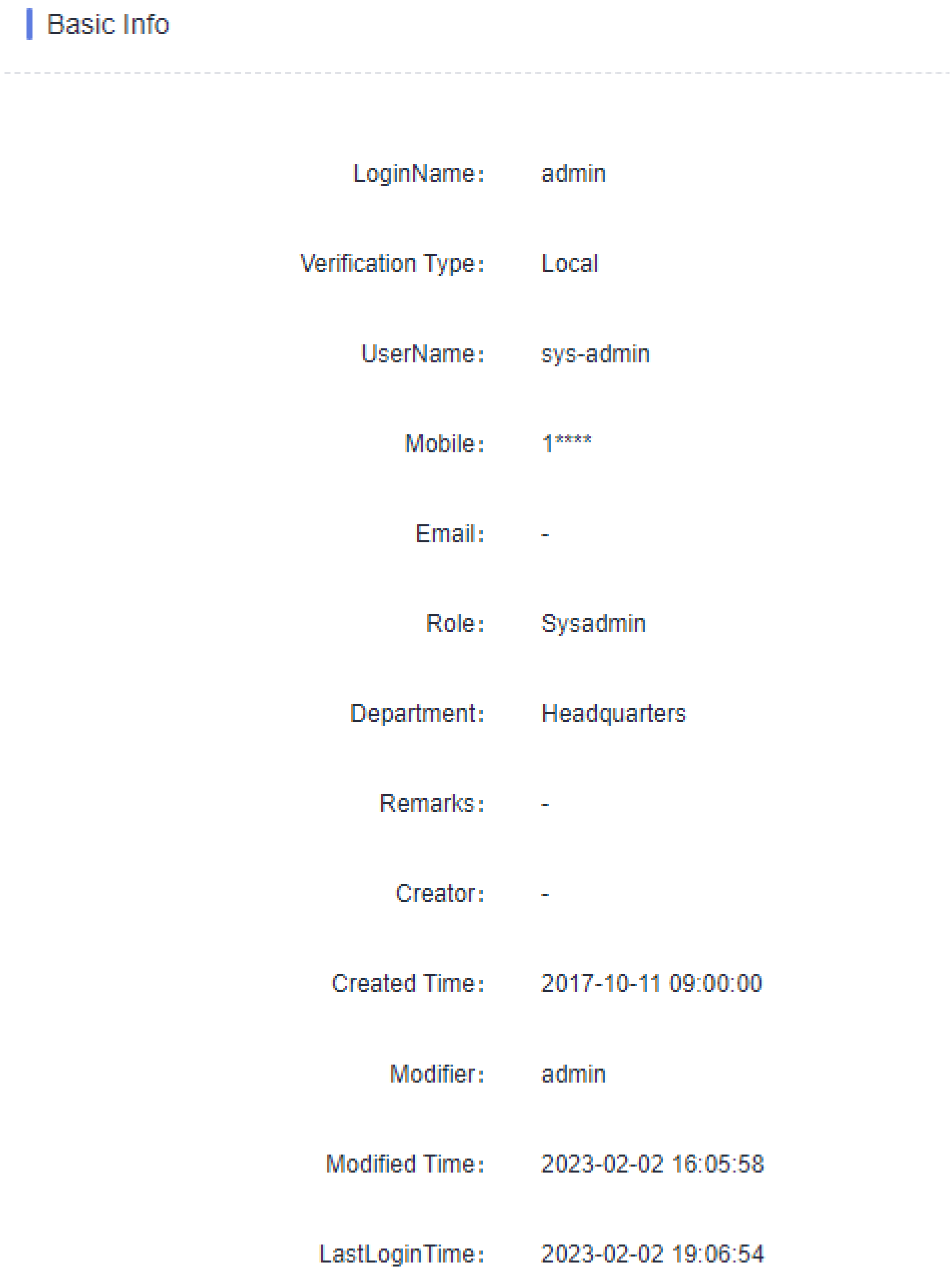


Step 4 Edit basic information.

In the **Basic Info** area on the displayed page, click **Edit**. In the displayed dialog box, edit the user information.

- You can edit **Verification Type**, **UserName**, **Mobile**, **Email**, **Role**, **Department**, and **Remarks**.
- The value of **LoginName** cannot be changed.

Figure 5-16 Basic user information



Step 5 Edit user login configurations.

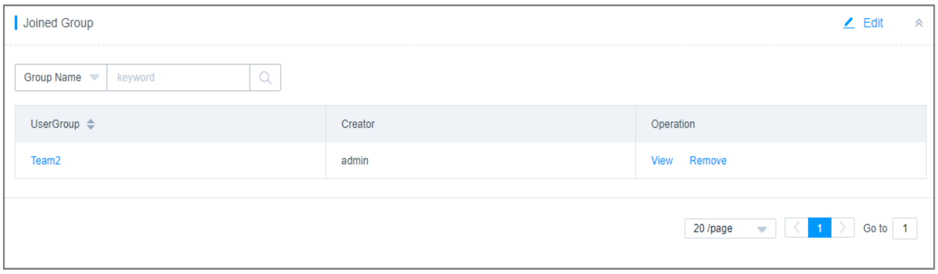
In the **User Setting** area on the displayed page, click **Edit**. In the displayed dialog box, edit the login configurations.

Figure 5-17 User login configurations

Step 6 View and change the user group to which a user belongs.

- In the **Joined Group** area, view the user group to which the user belongs.
- Click **Edit**. In the displayed dialog box, change the user group to which the user belongs.
- In the **Operation** column, click **Remove** to remove the user from the user group.

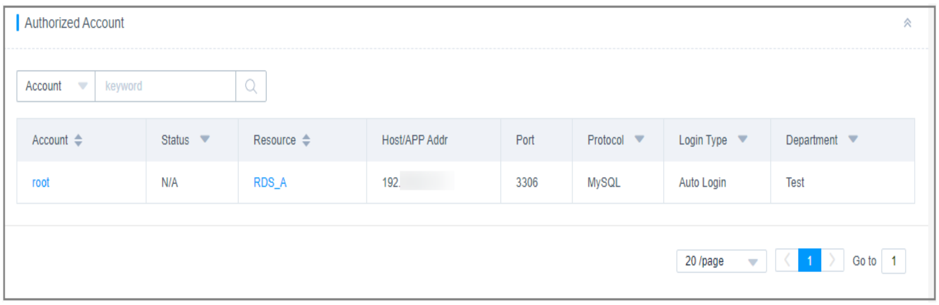
Figure 5-18 Adding a user to a user group



Step 7 View the authorized accounts and resources.

Expand the **Authorized Account** area to view resource accounts that can be used by the user.

Figure 5-19 Authorized Account



----End

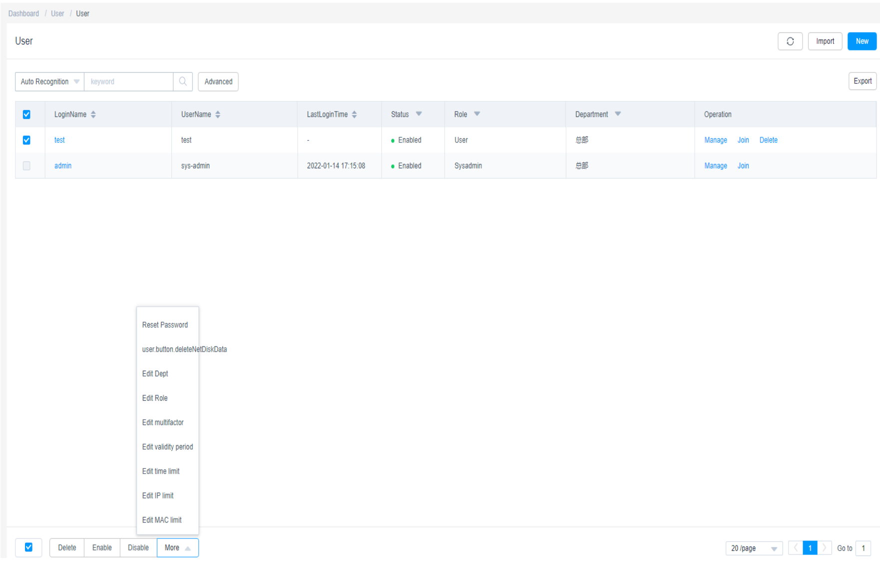
Batch Editing User Information

Step 1 Log in to the CBH system.

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

Step 3 In the user list, select the users you want to edit and click **More** in the lower left corner.

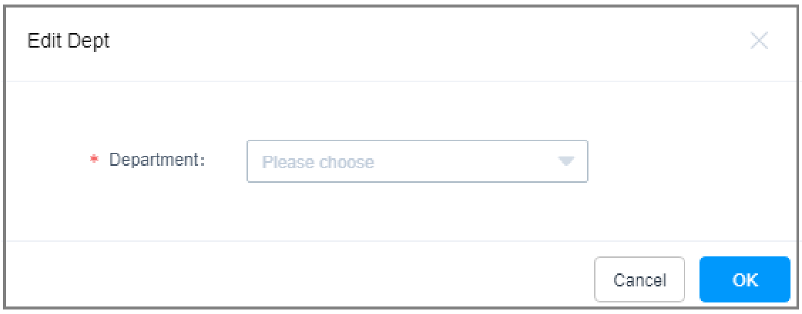
Figure 5-20 Batch Editing User Information



Step 4 Edit department of multiple selected hosts at a time.

1. Click **Edit Dept**.

Figure 5-21 Edit Dept

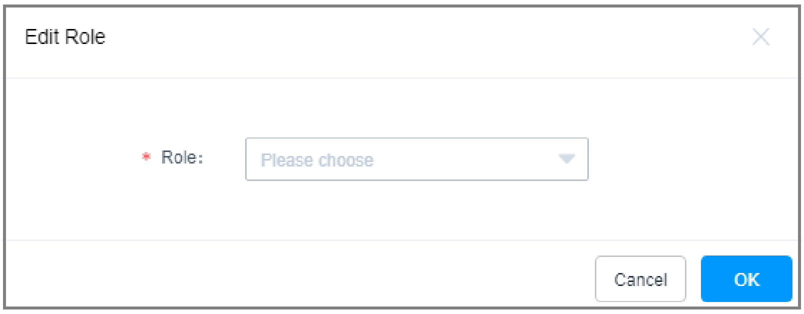


2. In the displayed dialog box, select a department.
3. Click **OK**.

Step 5 Edit role of several users at a time.

1. Click **Edit Role**.

Figure 5-22 Edit Role



2. In the displayed dialog box, select a role you want.
3. Click **OK**.

----End

5.2.6 Changing User Login Passwords

Forgotten, lost, or expired passwords may cause login security accidents. To reduce password login risks, CBH allows you to 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 CBH system 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 CBH system, 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 instead of CBH.

Prerequisites

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

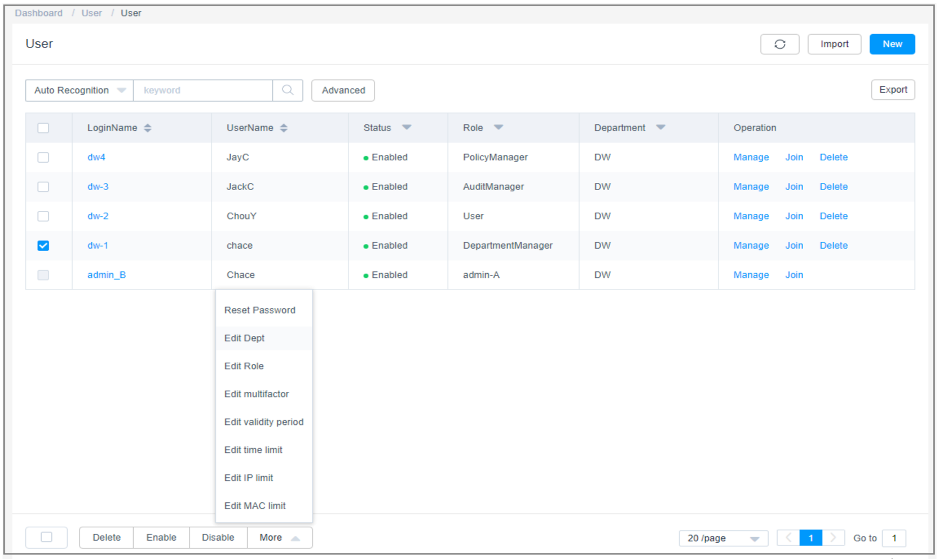
Procedure

Step 1 Log in to the CBH system.

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

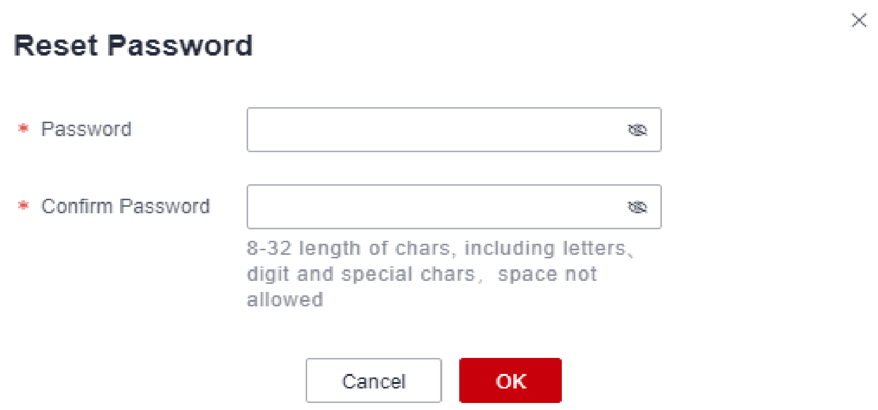
Step 3 Select the user accounts you want to edit and click **More** in the lower left corner.

Figure 5-23 Batch editing user login passwords



Step 4 Click **Reset Password**.

Figure 5-24 Reset Password



Step 5 Set the password.

Step 6 Click **OK**.

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

----End

5.2.7 Exporting User Information

CBH allows you to export user information in batches so that you can have a local backup and edit basic user information quickly.

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 the CBH system.

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

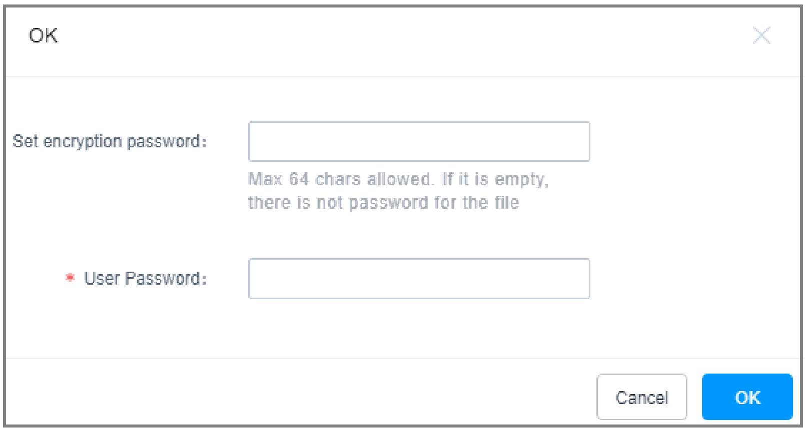
Step 3 Select the user accounts you want to export.

If no users are selected, all user accounts are exported by default.

Step 4 Click **Export**. In the displayed **OK** dialog box:

- Enter your password.
- (Optional) Set the encryption password to encrypt the exported file.

Figure 5-25 Confirmation dialog box



Step 5 Click **OK** to save the user information locally.

Step 6 Open the local file to view the exported basic user information.

----End

5.2.8 Adding Users to a User Group

This topic describes how to add a user to a 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.

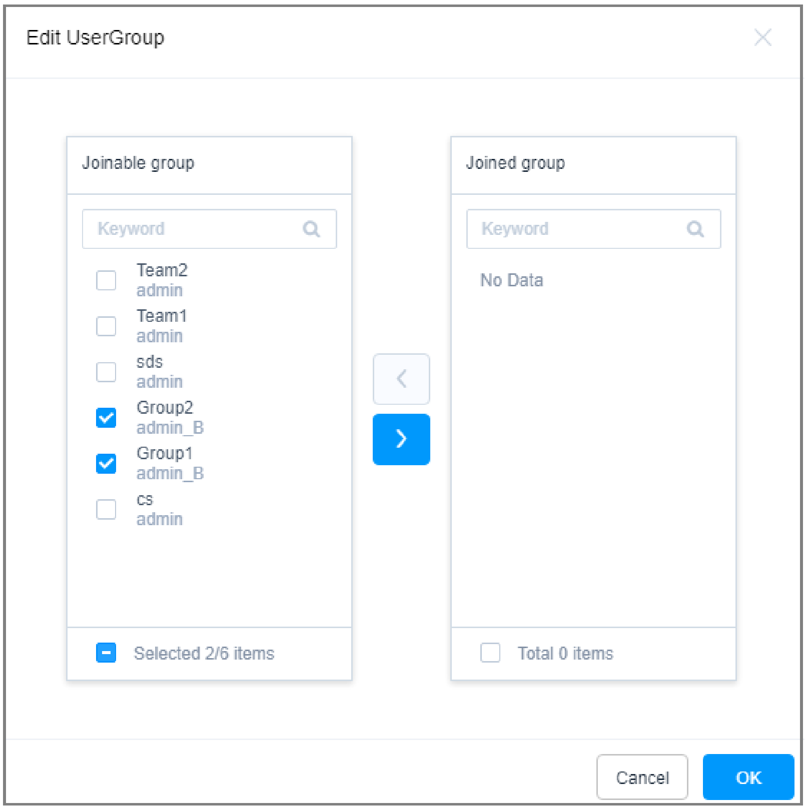
Adding a User to a User Group

Step 1 Log in to the CBH system.

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

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

Figure 5-26 Adding a user to a user group



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**. You can then view the user groups the user has been added.

----End

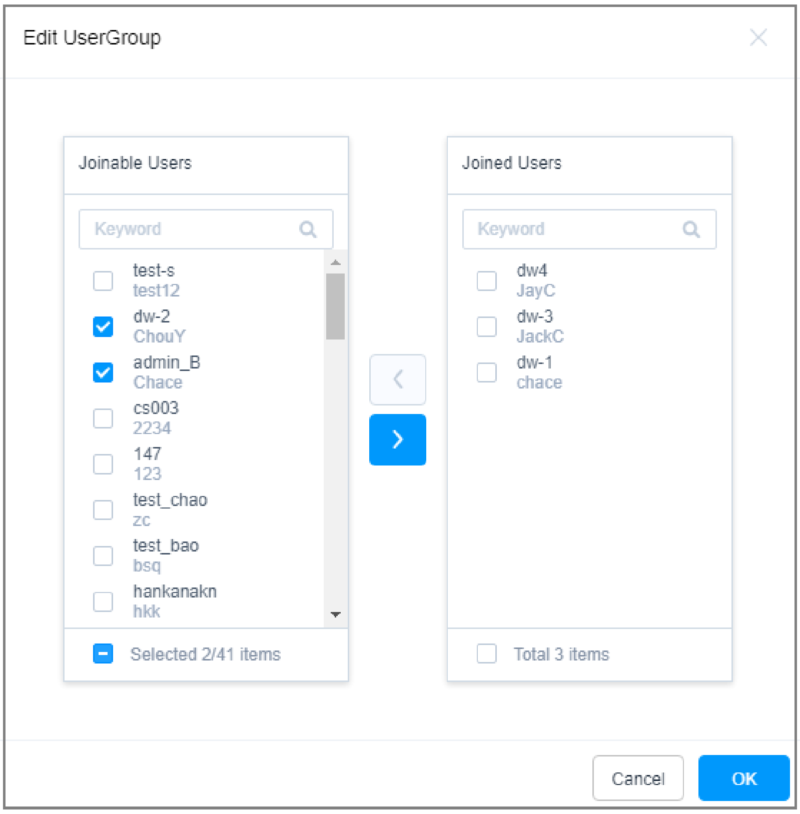
Adding Multiple Users to a User Group

Step 1 Log in to the CBH system.

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

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

Figure 5-27 Batch adding users to a user group



Step 4 In the displayed **Edit UserGroup** dialog box, select multiple user accounts and add them to the user group.

Step 5 Click **OK**. You can view the added members on the **User Group** page.

----End

5.3 User Role Management

5.3.1 Overview

You can relate different roles to different users to let them have certain permissions for the CBH system.

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

In a CBH system, default roles include **DepartmentManager**, **PolicyManager**, **AuditManager**, and **User**. The default roles cannot be deleted, but you can change the permissions of the default roles.

Table 5-5 Default roles

Parameter	Description
DepartmentManager	Specifies the operation administrator of the department, who manages the CBH system. **DepartmentManager** 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.
User	Specifies common users and operators. This role has the permissions for O&M of resources, such as host and application resources, and service ticket authorization management.

5.3.2 Creating a Custom Role

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

Constraints

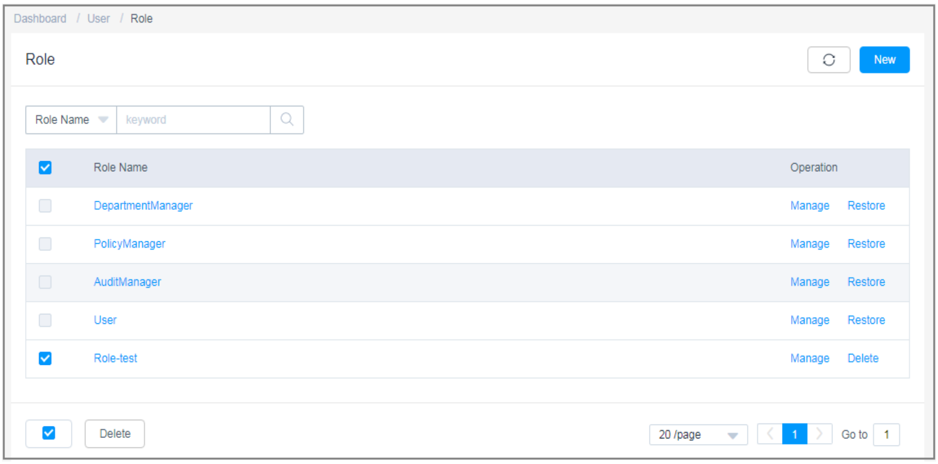
- Only system administrator **admin** can create a system role.
- To obtain permissions for the user group and account group modules, configure the **User** and **Account** modules.

Creating a Role

Step 1 Log in to the CBH system.

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

Figure 5-28 Role list



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

Figure 5-29 Creating a Role

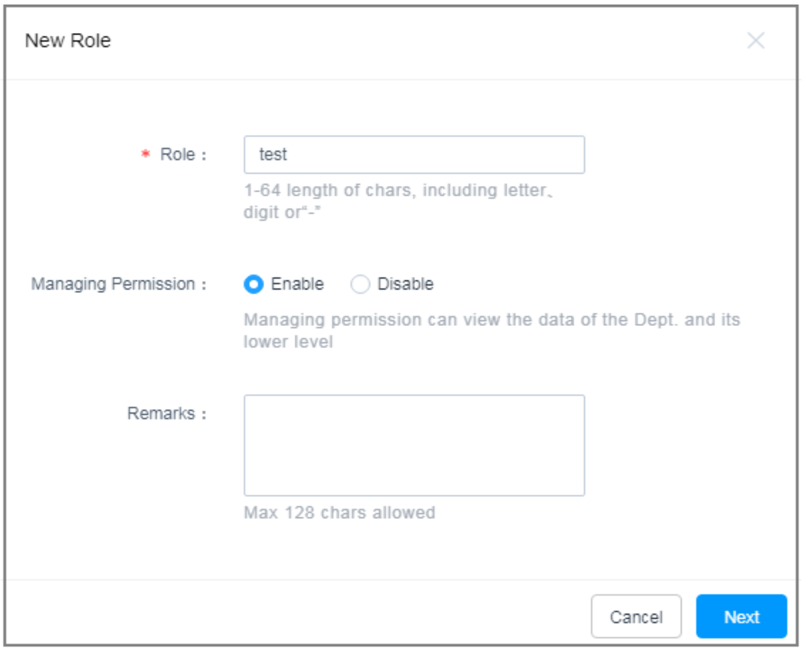


Table 5-6 Parameters for creating a role

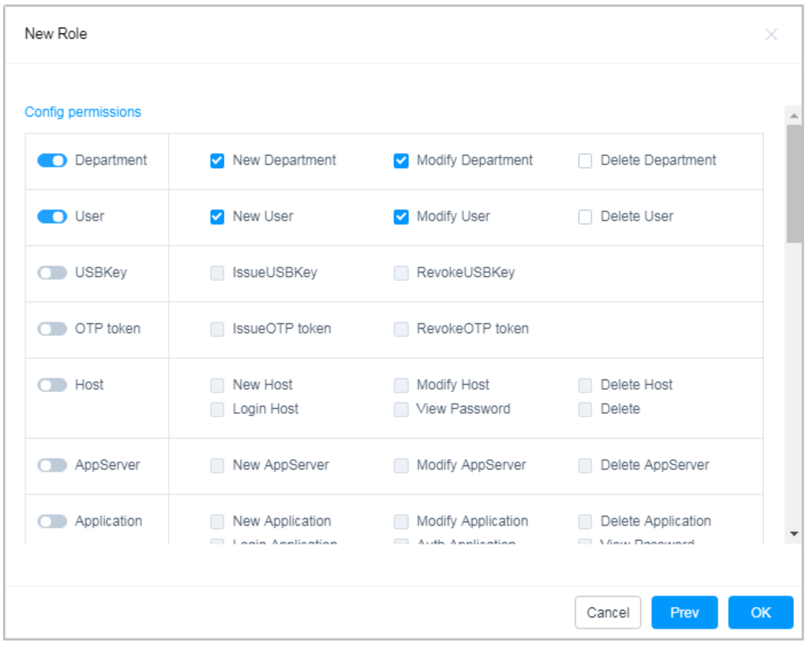
Parameter	Description
Role	Specifies the role name. The value of **Role** must be unique in a CBH system and cannot be changed after it is created.

Parameter	Description
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.

Figure 5-30 Assigning permissions to a role



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

----End

5.3.3 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.

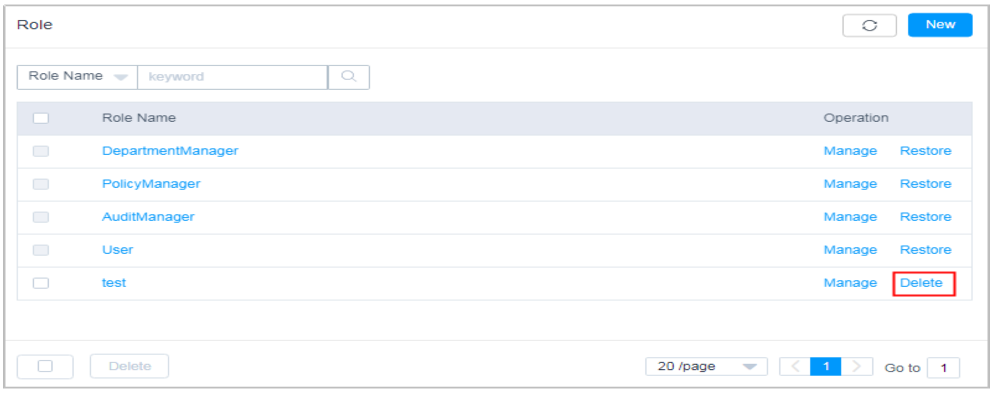
Procedure

Step 1 Log in to the CBH system.

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

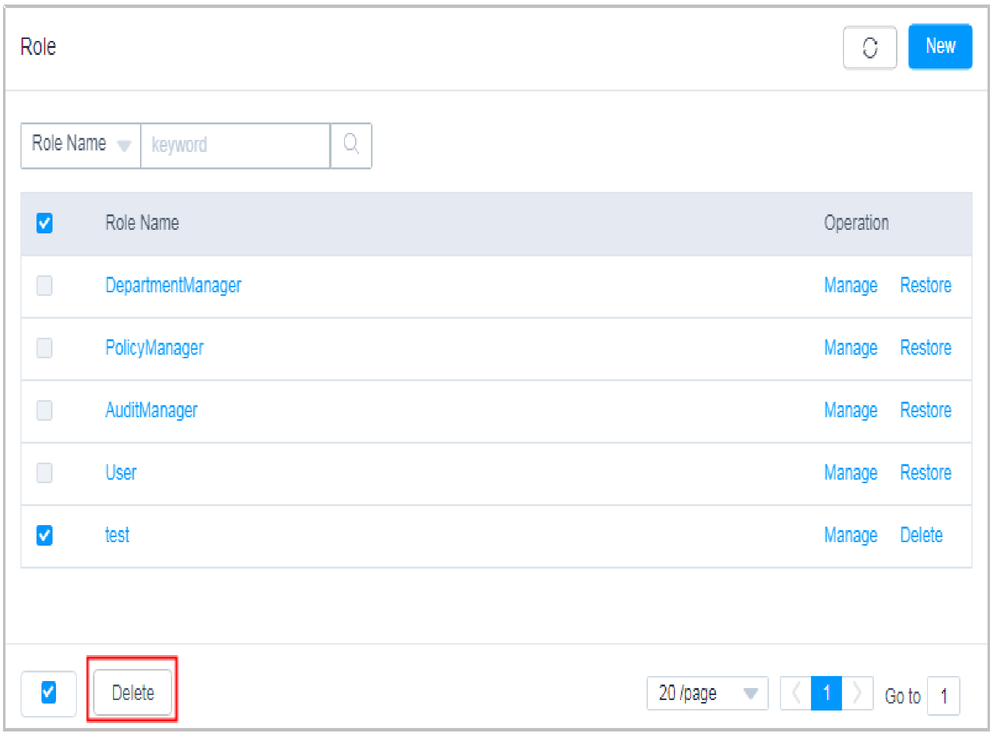
Step 3 To delete a single role, click **Delete** in the **Operation** column.

Figure 5-31 Deleting a role



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.

Figure 5-32 Batch deleting roles



----End

5.3.4 Querying and Editing Role Information

You can log in to your CBH system as user **admin** to view or change role information, 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, CBH allows you to restore default permissions with just a few clicks.

Procedure

Step 1 Log in to the CBH system.

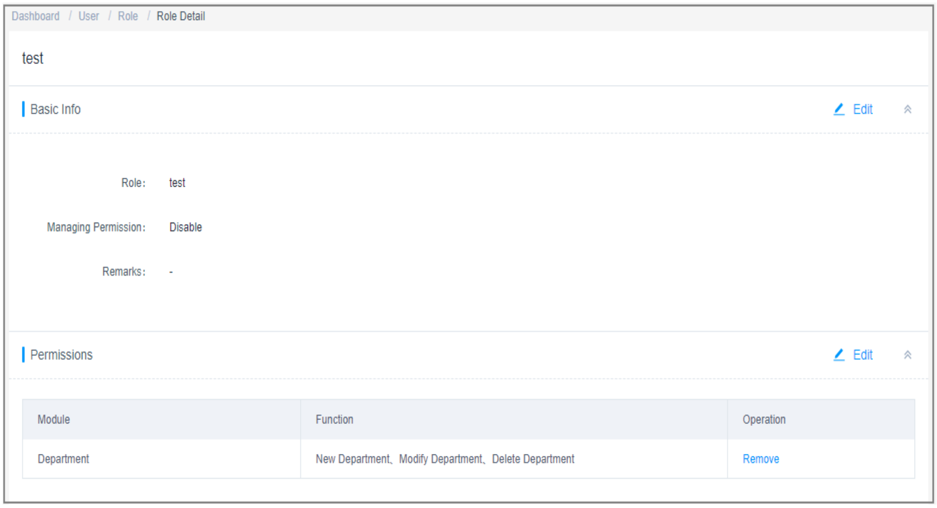
Step 2 In the navigation pane on the left, choose **User** > **Role** to go to the role list page.

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.

Figure 5-33 Role Detail



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

5.4 User Group Management

5.4.1 Overview

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.

5.4.2 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 the CBH system.

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.

Figure 5-34 Creating a User Group

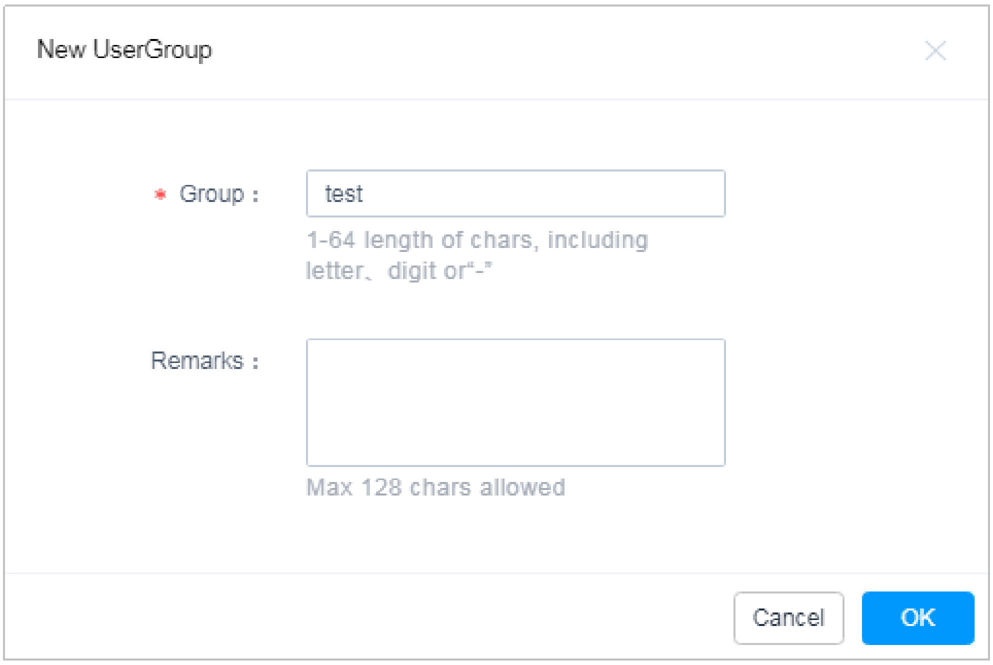


Table 5-7 Creating a User Group

Parameter	Description
User Groups	Specifies user-defined user group name, which must be unique in a CBH system.
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 CBH system 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

5.4.3 Deleting a User Group

CBH allows you to delete user groups. 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.

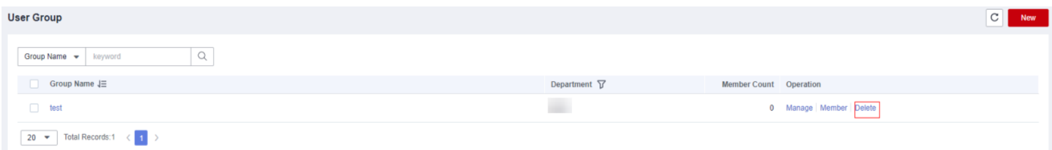
Procedure

Step 1 Log in to the CBH system.

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.

Figure 5-35 Deleting a 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

5.4.4 Querying and Editing User Group Information

CBH allows you to 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 the CBH system.

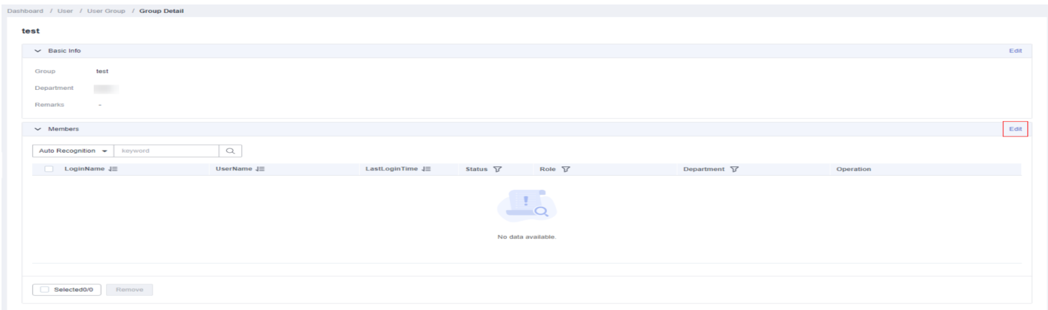
Step 2 Choose **User** > **User Group** in the navigation pane.

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.

Figure 5-36 User group details



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 Remote Authentication Management

5.5.1 Configuring Remote AD Authentication

CBH interconnects with the AD server to authenticate user logins. You can configure authentication mode or synchronization mode for the AD domain service.

- Auth Mode

  If this mode is selected, CBH does not synchronize user information from the AD domain server. The administrator needs to manually create users of the CBH system. When a user logs in to a CBH system, the user identify is authenticated by the AD domain server.

- Sync Mode

  If this mode is selected, CBH synchronizes user information from the AD domain server. Therefore, the administrator does not need to create users of the CBH system. When a user logs in to a CBH system, the user identify is authenticated by the AD domain server. For details, see **Synchronizing AD Domain Users**.

This topic describes how to configure the AD authentication mode.

Prerequisites

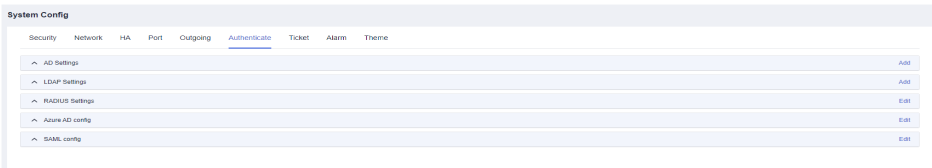
- You have the management permissions for the **System** module.
- You have obtained the information about the AD domain server.

Procedure

Step 1 Log in to the CBH system.

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

Figure 5-37 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 5-8**.

Figure 5-38 AD Settings

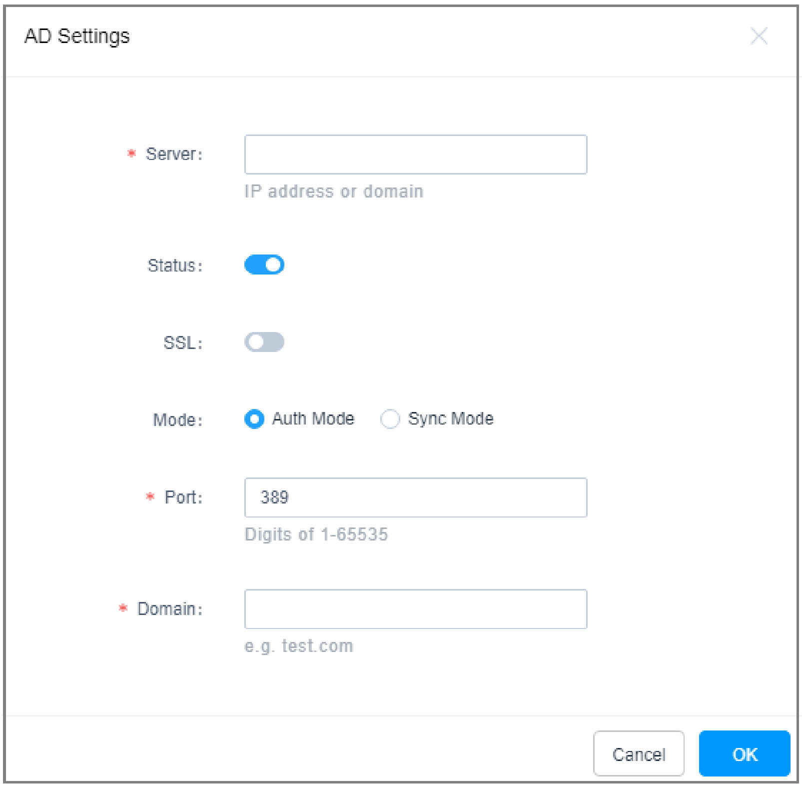


Table 5-8 AD authentication parameters

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 CBH system when the user logs in to the CBH system. • : 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**.
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.

Figure 5-39 AD domain authentication

----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.

5.5.2 Configuring Remote LDAP Authentication

CBH interconnects with the LDAP server to authenticate CBH system user logins.

This topic describes how to configure the LDAP authentication mode.

Constraints

- One-click synchronization of LDAP server users is not supported.
- Identical configurations of two LDAP authentication servers are not allowed. Each LDAP server has unique combination of IP address, port number, and user OU.

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 the CBH system.

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

Figure 5-40 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 5-9**.

Figure 5-41 Configuring LDAP authentication

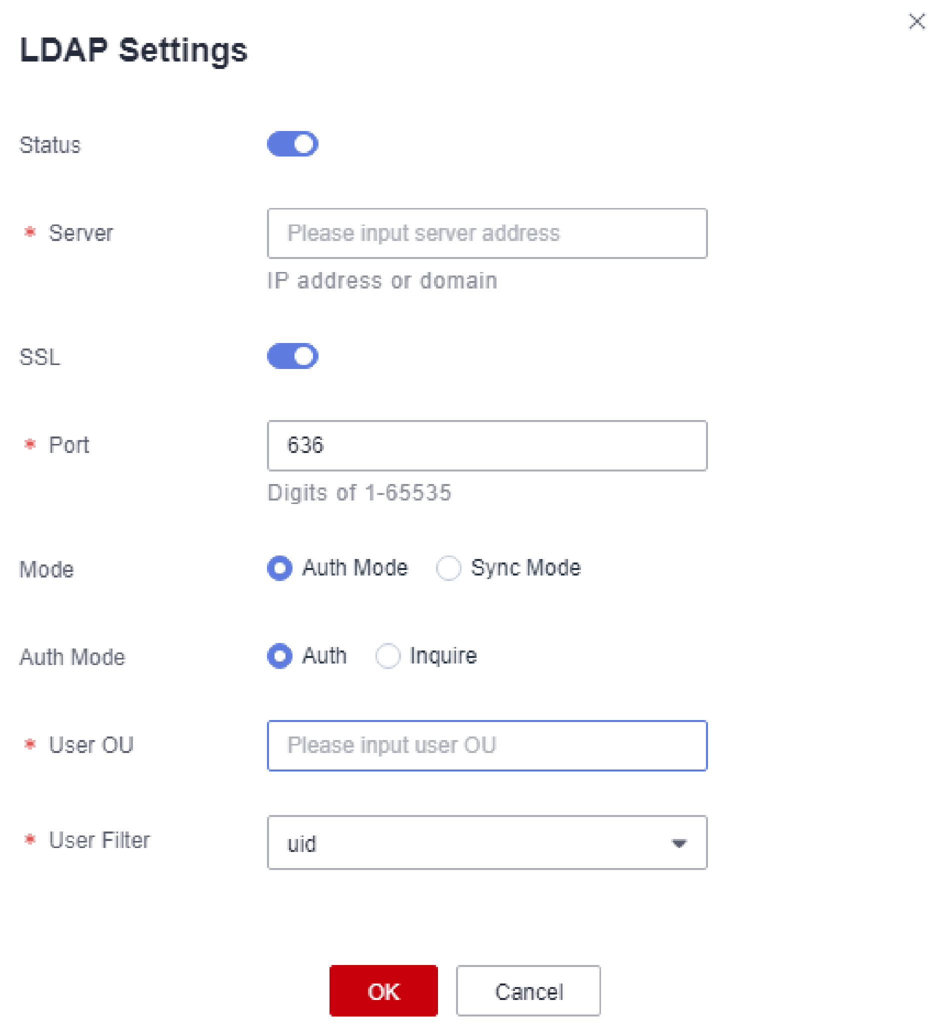


Table 5-9 LDAP authentication parameters

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 the user logs in to the CBH system. – : 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 5-10**.

  NOTE

  Querying authentication method is included in version V3.3.36.0 and later only. To use this function, upgrade your CBH system to V3.3.36.0 or later by referring to **Upgrading the CBH System Version**.

Figure 5-42 Inquire

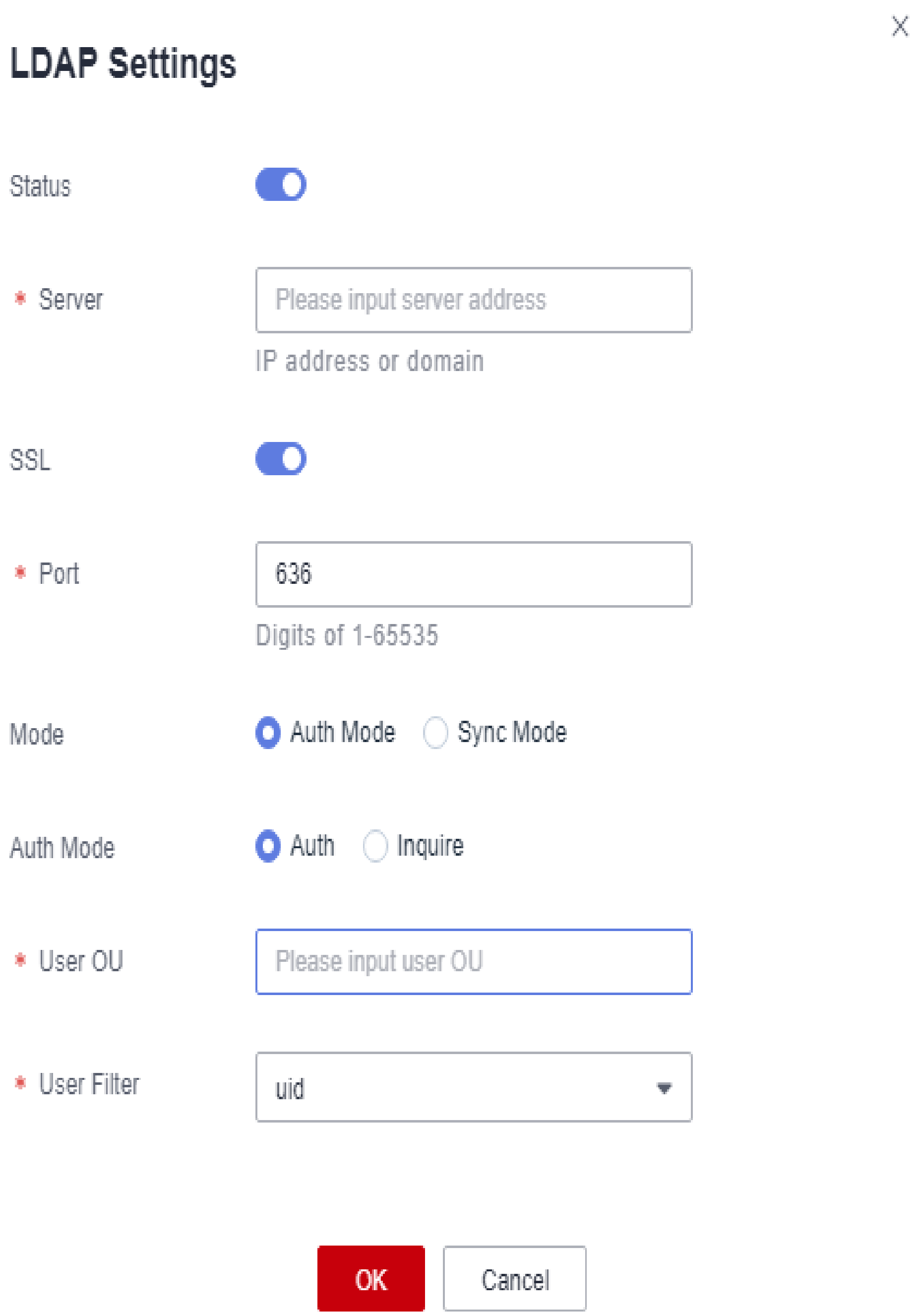


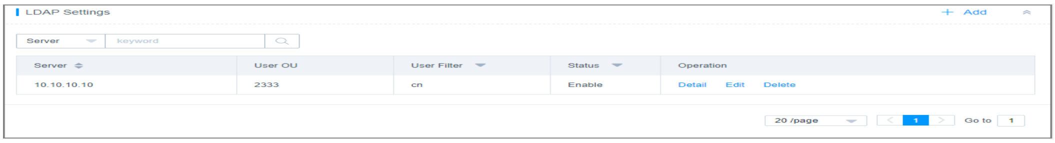
Table 5-10 LDAP inquiring mode parameters

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 the user logs in to the CBH system. – : 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 CBH instance 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.

Figure 5-43 LDAP authentication



----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.

5.5.3 Configuring Remote RADIUS Authentication

CBH interconnects with the RADIUS server to authenticate CBH system user logins.

This topic describes how to configure the RADIUS authentication and how to test the user validity of the configured RADIUS authentication.

Prerequisites

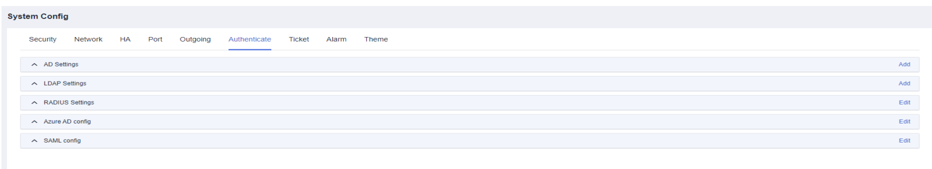
- You have the management permissions for the **System** module.
- You have obtained the information about the RADIUS server.

Procedure

Step 1 Log in to the CBH system.

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

Figure 5-44 Configuring remote authentication



Step 3 Click **Edit** in the **RADIUS Settings** area.

Figure 5-45 Configuring RADIUS authentication

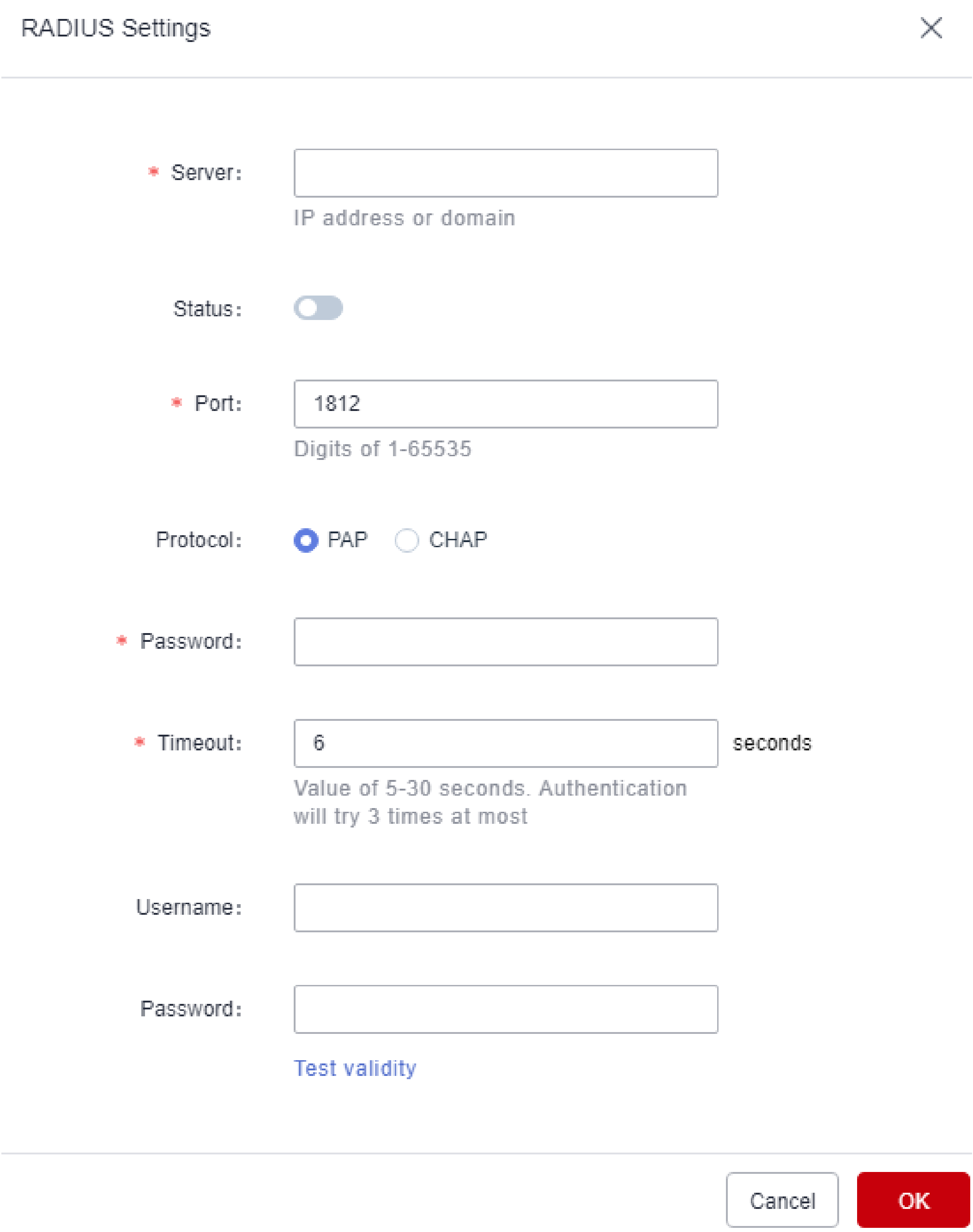


Table 5-11 RADIUS authentication parameters

Parameter	Description
Server	Specifies the IP address of the RADIUS server.

Parameter	Description
Status	Specifies the status of remote RADIUS authentication (default:). • : RADIUS authentication is enabled. Remote RADIUS authentication is enabled when the user logs in to the CBH system. • : RADIUS authentication is disabled.
Port	Specifies the access port of the remote RADIUS server. The default port number is 1812.
Protocol	Specifies the remote authentication protocol. This parameter can be set to **PAP** or **CHAP**.
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.

Figure 5-46 RADIUS authentication

----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.

5.5.4 Configuring Remote Azure AD Authentication

CBH interconnects with the Azure AD platform to authenticate CBH system user logins.

This topic describes how to configure the Azure AD authentication.

Prerequisites

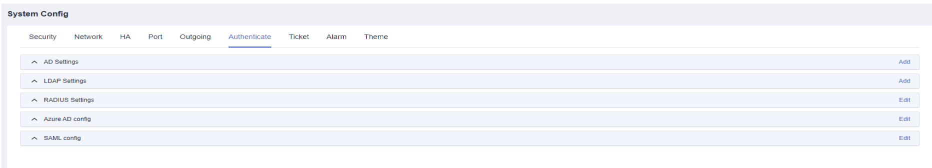
- You have the management permissions for the **System** module.
- You have created users and added enterprise application resources on Azure AD, and obtained information about the Azure AD platform configuration.

Procedure

Step 1 Log in to the CBH system.

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

Figure 5-47 Configuring remote authentication



Step 3 Click **Edit** in the **Azure AD config** area.

Figure 5-48 Configuring remote Azure AD authentication

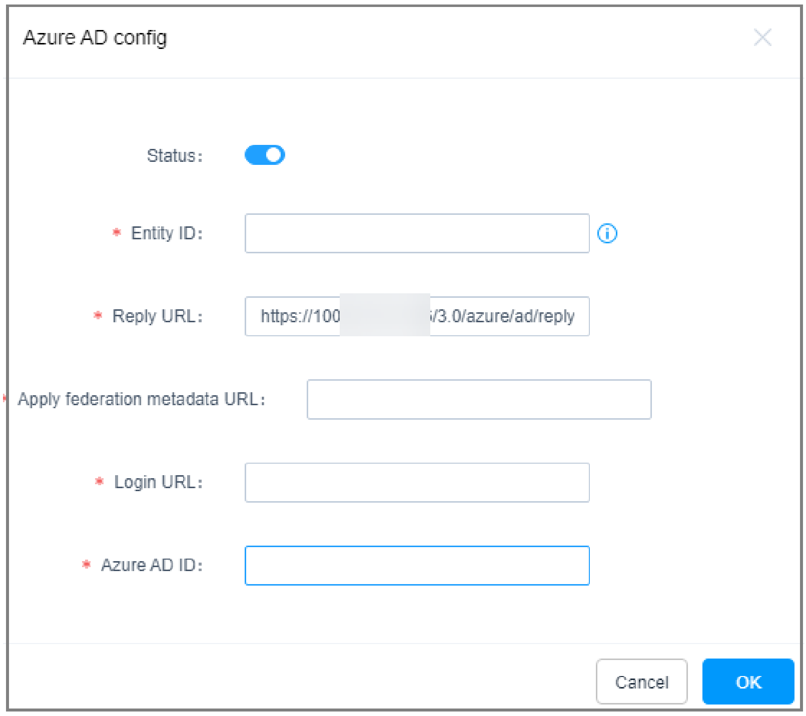


Table 5-12 Azure AD authentication parameters

Parameter	Description
Status	Specifies the status of remote Azure AD authentication (default:). • : Azure AD authentication is enabled. Remote Azure AD authentication is enabled when the user logs in to the CBH system. • : 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 CBH system. If the IP address or domain name of the CBH system is changed, change the IP address or domain name in the URL.
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.

Figure 5-49 Azure AD authentication

NOTICE

If the Azure AD certificate is updated, you need to delete the old certificate on the Azure AD control plane before logging.

----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**.

5.6 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. A USB key from a vendor cannot be identified by other vendors for login authentication. So, the vendor must be specified for each USB key. For details, see **Configuring USB Keys**.

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

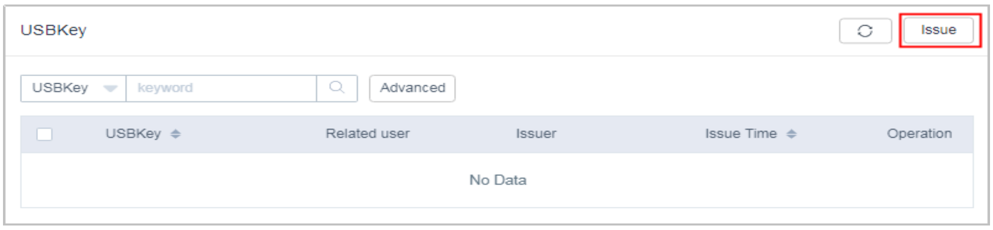
One USB key can be issued to one user only.

Step 1 Log in to the CBH system.

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

Step 3 Click **Issue** to issue a USB key.

Figure 5-50 USBKey



Step 4 Select a user with the USB key multifactor verification enabled as the related user.

Figure 5-51 Procedure

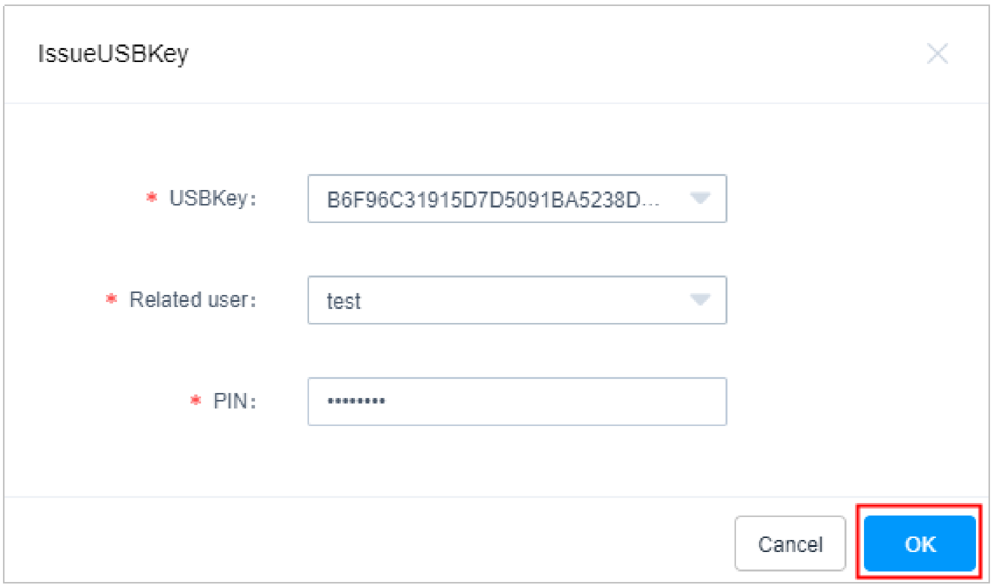


Table 5-13 Parameters for issuing a USB key

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 the CBH system as a related user, insert the issued USB key to the local host. The CBH system automatically identifies the USB key. On the displayed page, select the corresponding USB key and enter the PIN number to complete the authentication.

----End

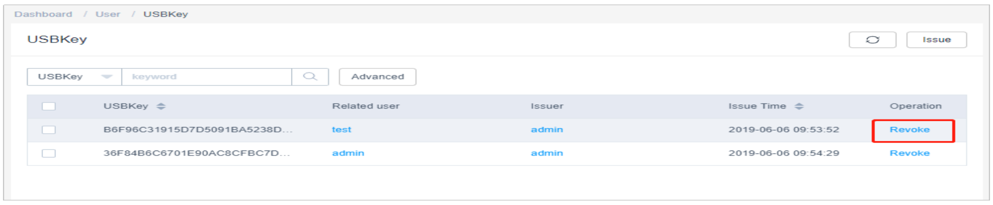
Revoking a USB Key

Step 1 Log in to the CBH system.

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

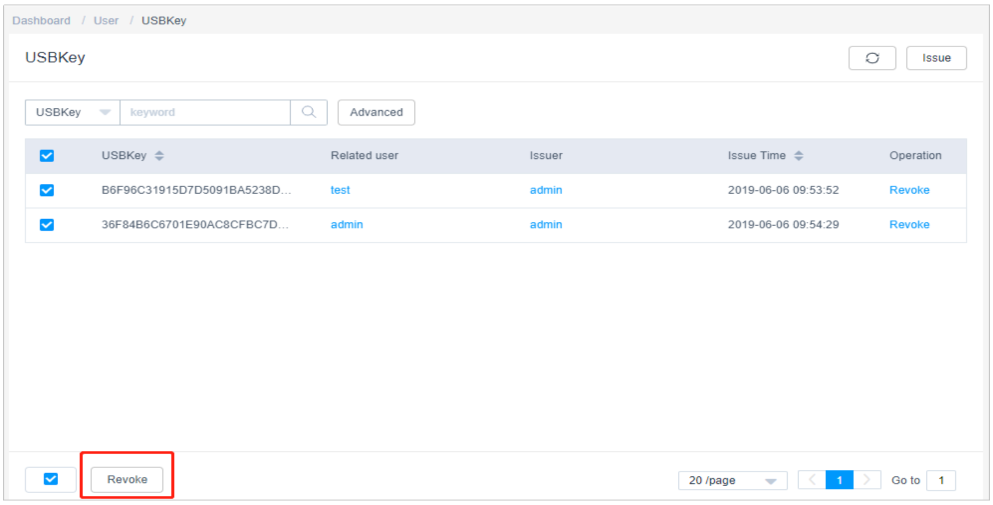
Step 3 In the **Operation** column of the row containing the USB key to be revoked, click **Revoke**.

Figure 5-52 Revoking a USB key



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.

Figure 5-53 Batch revoking USB keys



----End

5.7 OTP Token Management

OTP tokens can be issued only to users with **OTP Token** enabled in multifactor verification.

OTP tokens need to be prepared before binding. You can use Jansh ETZ201/203 OTP tokens in CBH.

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

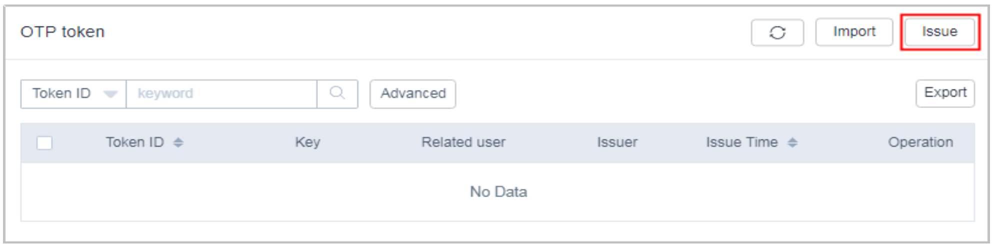
One OTP token can be issued only to one user.

Step 1 Log in to the CBH system.

Step 2 Choose **User** > **OTP token** in the navigation pane.

Step 3 Click **Issue** to issue an OTP token.

Figure 5-54 New OTP token



Step 4 Enter the required token information.

Figure 5-55 Issuing an OTP Token

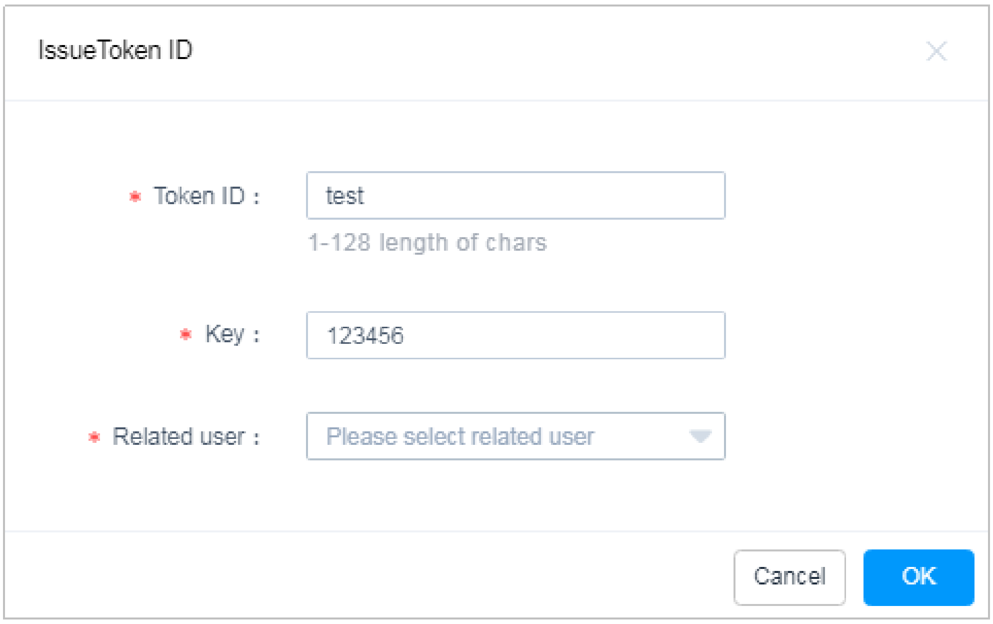


Table 5-14 Parameters for issuing an OTP token

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	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 on the OTP token to log in to the CBH system.

----End

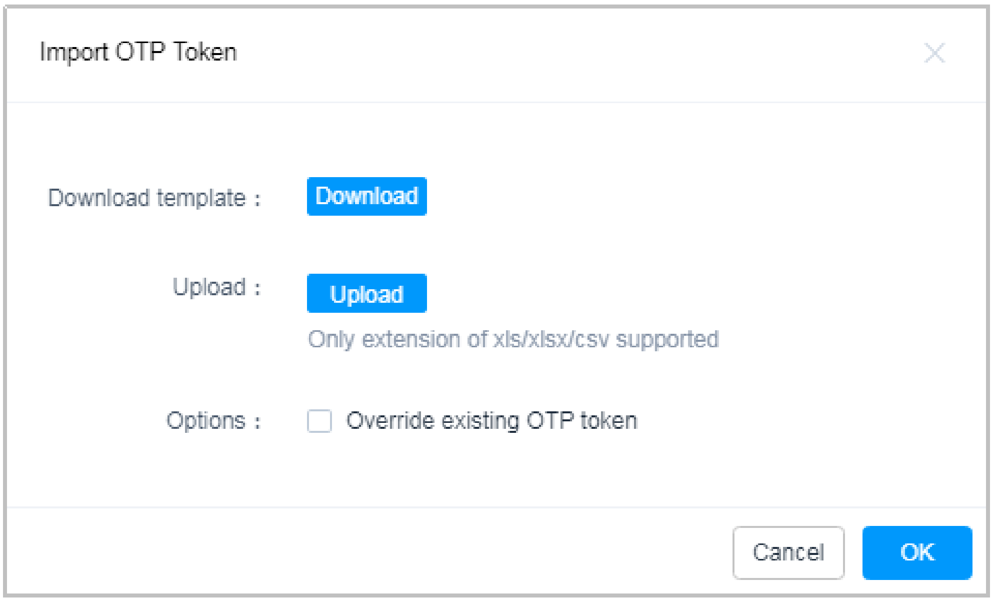
Importing an OTP Token

Step 1 Log in to the CBH system.

Step 2 Choose **User** > **OTP token** in the navigation pane.

Step 3 Click **Import** to batch import OTP tokens.

Figure 5-56 Importing an OTP Token



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 the CBH system.

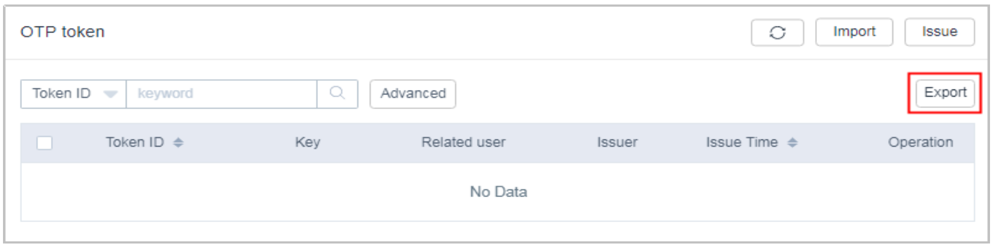
Step 2 Choose **User** > **OTP token** in the navigation pane.

Step 3 Select the OTP token to be exported.

If no tokens are selected, all tokens are exported by default.

Step 4 Click **Export** in the upper right corner next to the **Advanced** search box.

Figure 5-57 Exporting an OTP Token



----End

Revoking an OTP Token

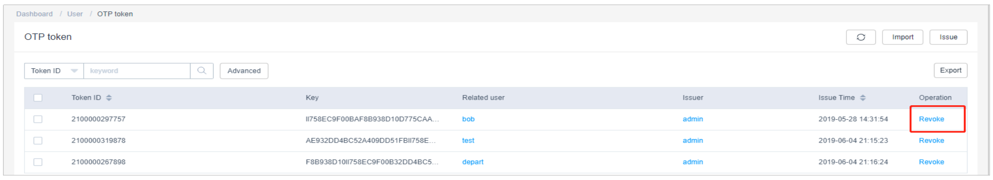
After an OTP token is deleted, the related user account cannot be used to log in to the CBH system through the OTP token.

Step 1 Log in to the CBH system.

Step 2 Choose **User** > **OTP token** in the navigation pane.

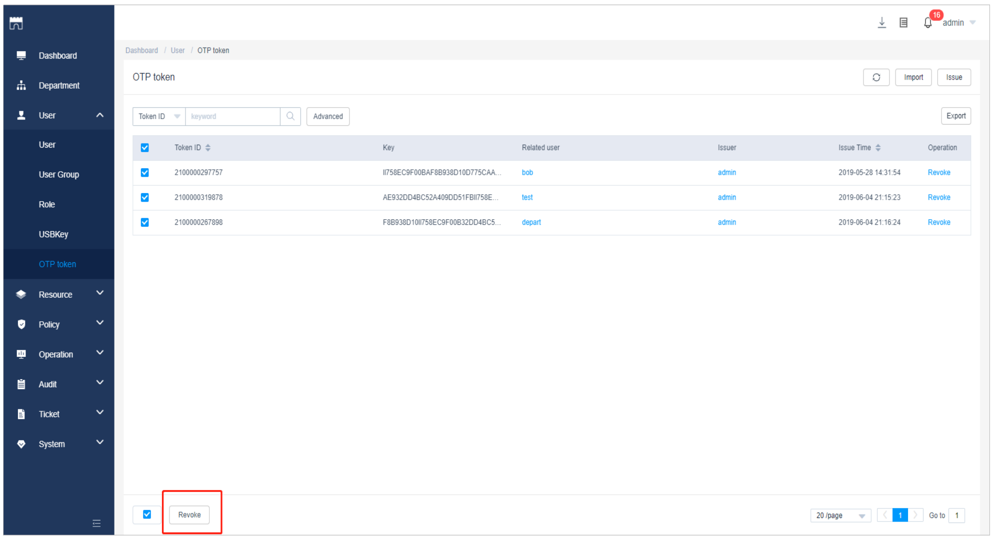
Step 3 In the **Operation** column of the row containing the OTP token to be revoked, click **Revoke**.

Figure 5-58 Revoking an OTP token



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.

Figure 5-59 Batching revoking OTP tokens



----End

6 Resource

6.1 Overview

CBH 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 types

  CBH can manage a wide range of resource types, including Windows and Linux hosts, 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 managed in CBH, 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-side Windows applications, such as Microsoft Edge, Google Chrome, and Oracle tools.

- Resource management

  – Batch importing

    CBH enables quick auto-discovery, synchronization, and bulk importing of cloud resources, such as Elastic Cloud Server (ECS) and Relational Database Server (RDS) instances for centralized O&M.

  – Account group management

    CBH manages resource accounts by group, enabling you to grant permissions to multiple resource accounts quickly by adding resource accounts of the same attribute to an account group and granting permissions to the account group.

– Batch management

CBH allows you to batch manage information and accounts of managed resources, including modifying and deleting resource information, adding resource labels, verifying managed resource accounts, and deleting managed resource accounts.

6.2 Managing Host Resources Using CBH

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

This topic describes 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 to CBH for centralized management.

Constraints

- The total number of host and application resources to be added cannot exceed the **number of assets**.
- The values of **Protocol** and **Host Address** must be unique in the CBH 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 Resource

Step 1 Log in to the CBH system.

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

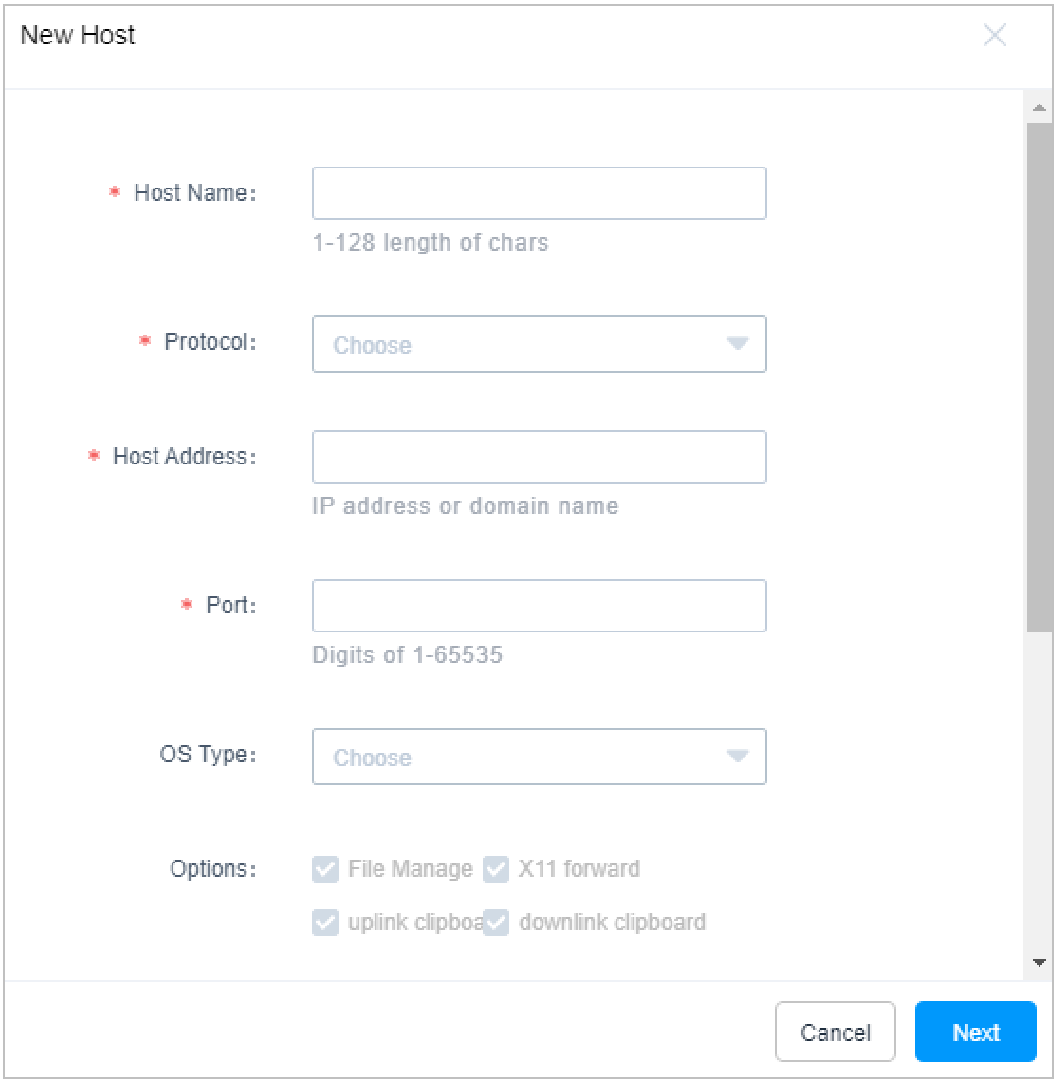


Table 6-1 Host resource network parameters

Parameter	Description
Host Name	Custom name of the host resource. A host name must be unique in the CBH system.
Protocol	Type of the protocol configured for the host. ● In the CBH professional editions, you can configure SSH, RDP, VNC, Telnet, FTP, SFTP, DB2, MySQL, SQL Server, Oracle, SCP, and Rlogin for a host. ● In the CBH standard editions, you can configure SSH, RDP, VNC, Telnet, FTP, SFTP, SCP, and Rlogin for a host. .

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Host Address</td><td>Host IP address that can be used to establish connection with the CBH system.
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
It is recommended that you set Host Address to a private IP address on the same VPC network. This is because CBH manages host resources on the same VPC network based on network stability and proximity. The external access port of the private IP address is not restricted by the network security (security group and ACL) policies. While the EIP of the host is an independent elastic IP address. The port for external access over an EIP is restricted by network security policies. As a result, you may fail to log in to the host from the CBH system.
So we recommend private IP addresses.</td></tr>
<tr><td>Port</td><td>Port number of the host.</td></tr>
<tr><td>OS Type</td><td>(Optional) Type of the host OS or device OS.
This parameter is automatically set by the CBH system.
14 OS types are supported, 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.
In addition, system administrator admin can customize OS types.
For details, see OS Types.</td></tr>
<tr><td>Terminal Speed</td><td>If you select Rlogin for Protocol, you can select different terminal speed.</td></tr>
<tr><td>Encode</td><td>If you select SSH or TELNET for Protocol, the Chinese character can be used on the O&M page.
The options are UTF-8, Big5, and GB18030.</td></tr>
<tr><td>Terminal Type</td><td>If you select SSH or TELNET for Protocol, you can specify the O&M terminal you want.
The options are Linux and Xterm.</td></tr>
<tr><td>Options</td><td>(Optional) Select File Manage, X11 forward, uplink clipboard, and/or downlink clipboard.
File Manage: This option is supported only by SSH, RDP, and VNC hosts.
Clipboard: This option is supported only by RDP hosts.
X11 forward: This option is supported only by SSH hosts.</td></tr>
</table>

Parameter	Description
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.

Figure 6-2 Adding an account for a host resource

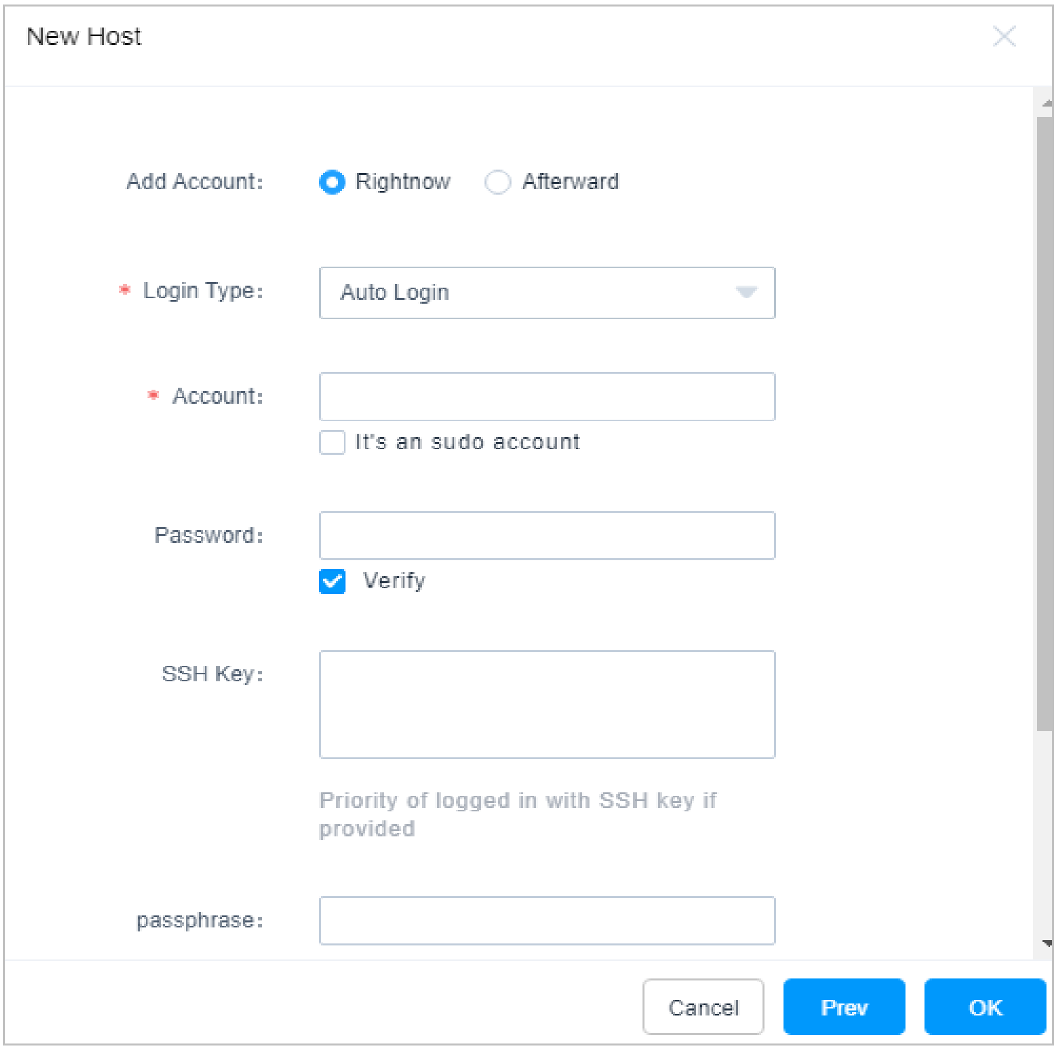


Table 6-2 Parameters of managed host accounts

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 of the host resource. The options are **Auto Login** and **Manual Login**. ● If you select **Auto Login**, **Account** and **Password** are mandatory. ● If you select **Manual Login**, **Account** and **Password** are optional.
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 verification times out, return to the configuration window and modify the resource information. – 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.
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 CBH for O&M, 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 Resources from a File

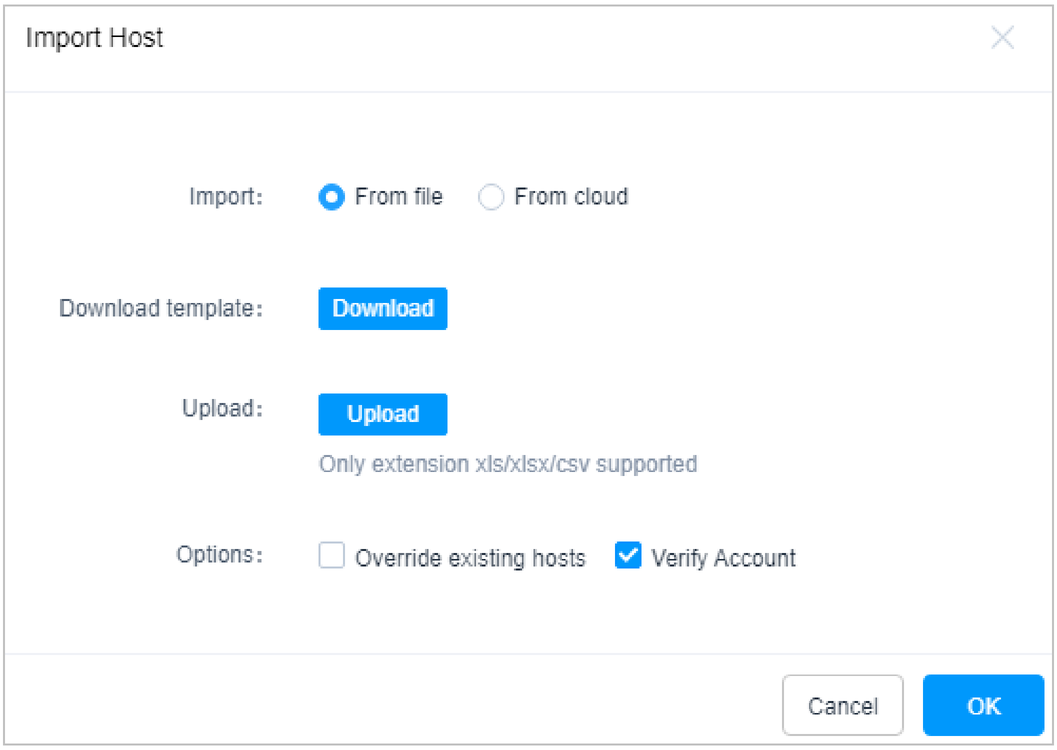
To import application server from a file, the file must be in .csv, .xls, or .xlsx format.

Step 1 Log in to the CBH system.

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

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

Figure 6-3 Importing host resources in batches



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.

Table 6-3 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 the CBH professional editions, you can configure SSH, RDP, VNC, Telnet, FTP, SFTP, DB2, MySQL, SQL Server, Oracle, SCP, and Rlogin for a host. ● In the 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 CBH system can be entered.
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.

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.
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 (,).
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 CBH 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**.

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 Hosts from a Cloud Platform

Step 1 Log in to the CBH system.

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

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

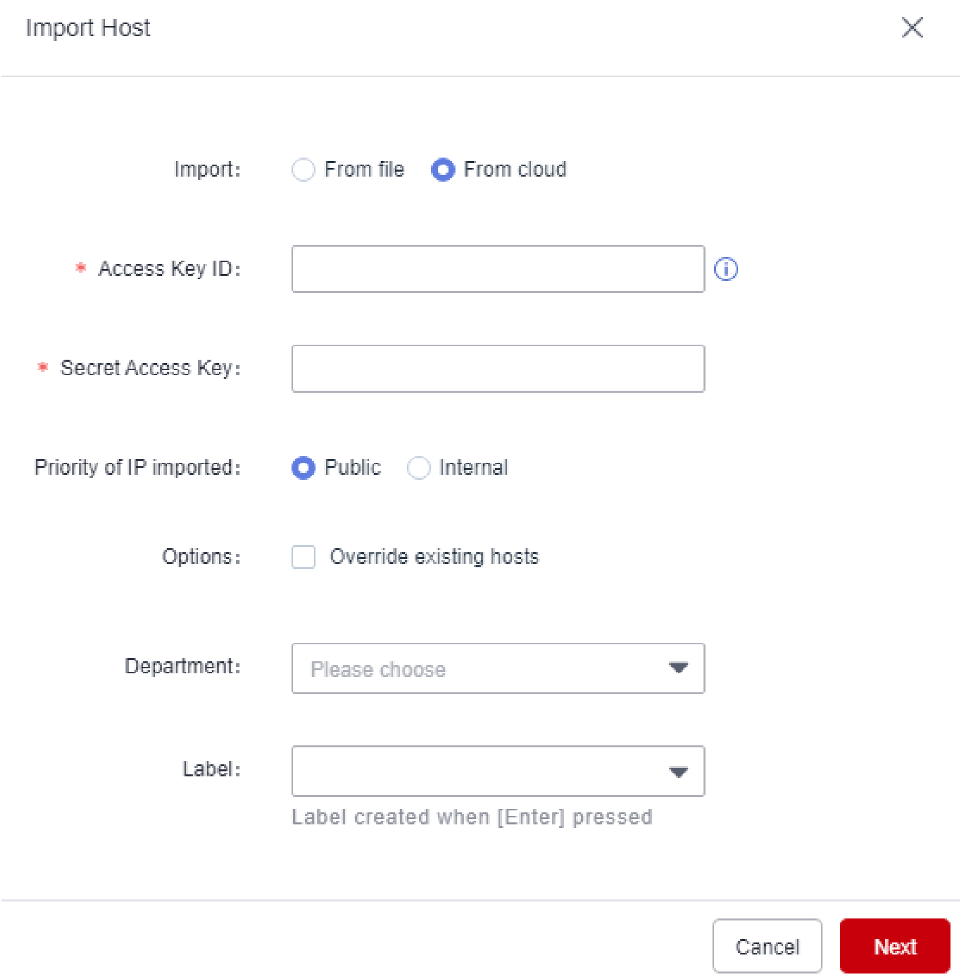
Step 4 Select **From cloud** for **Import**.

Table 6-4 Parameters for importing host resources from a cloud platform

Parameter	Description
Cloud Vendor	Cloud platform from which the host resources are imported. Currently, CBH supports importing of cloud host resources from multiple platforms.
Access Key ID	To get the access key ID, click the information icon on the right of the text box.
Access Key Secret	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**.

Parameter	Description
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.
Import Area	Regions supporting host resource importing. The value varies depending on the cloud platform. Currently, this parameter is available for Baidu Cloud, HUAWEI CLOUD, and AWS.
Operating Environment	Running environment of the imported host resources. Currently, this parameter is required only for cloud hosts on the Azure cloud platform.

Figure 6-4 Batch importing of cloud host resources



Step 5 Click **OK**.

----End

Auto Discovery of Host 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 CBH are in the same VPC and the network connection is normal.

Step 1 Log in to the CBH system.

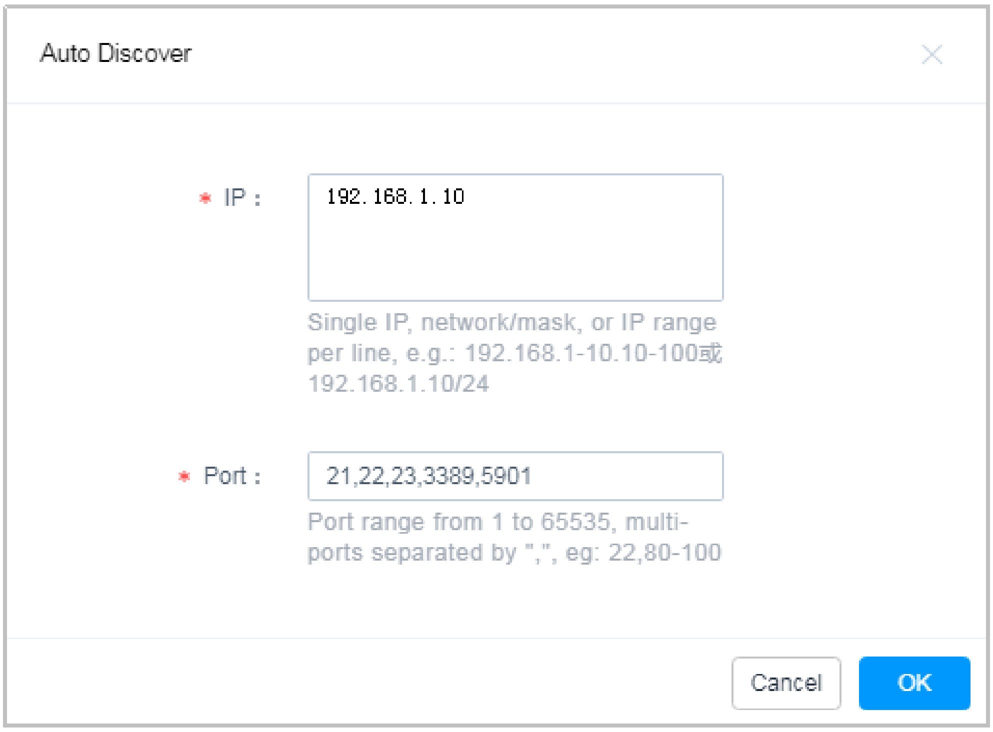
Step 2 Choose **Resource** > **Host** in the navigation pane on the left.

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 6-5 Auto Discover

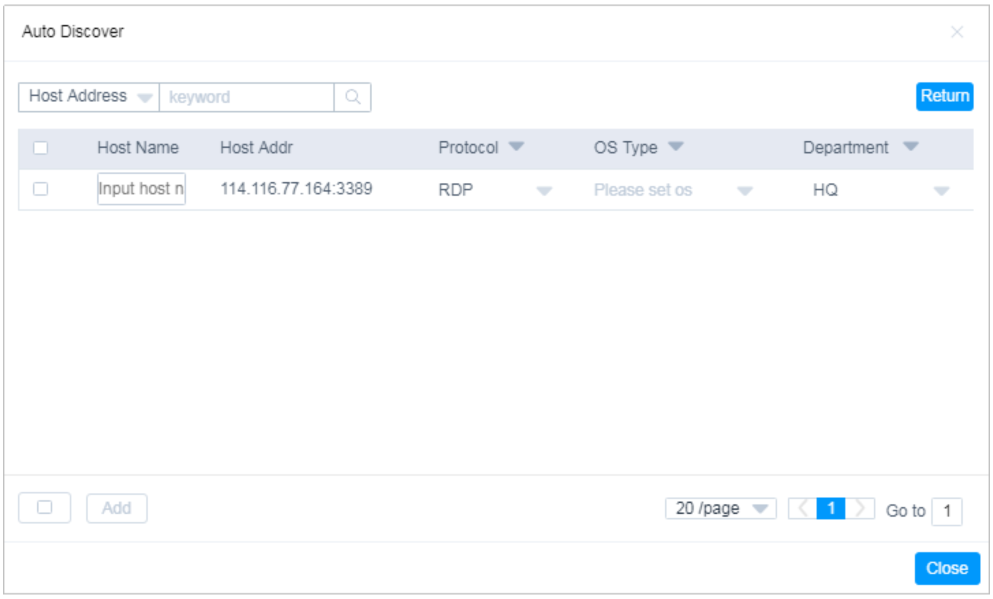


Step 5 Click **OK** to start the auto discovery.

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.

Figure 6-6 Auto Discover



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 Resources

If a host has multiple types of resources added, CBH enables you to quickly add other types of host resources by just modifying configurations of a certain type of host resource you have added to CBH.

Step 1 Log in to the CBH system.

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**.

----End

6.3 Managing Application Servers Using CBH

CBH allows you 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, the CBH system allows you to access client-based application resources and browser-based application resources without manually entering usernames and passwords. This is because the CBH system automatically provides the credentials. In addition, the CBH system 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 CBH 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.

This topic describes how to add an application server, import an application server from a file, add an application resource, and import application resources from a file to the CBH system for centralized management.

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.

- Only the Mozilla Firefox browser applications and Dameng data management tool V8 can be invoked for Linux servers.
- Port 2376 and ports 35000 to 40000 must be enabled between a Linux server and CBH. The port cannot be changed once it is enabled.
- Contact Huawei Cloud technical support to obtain the password for logging in to a Linux server.
- 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.

Prerequisites

- You have purchased resources, 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 the CBH system.

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

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

Figure 6-7 New AppServer

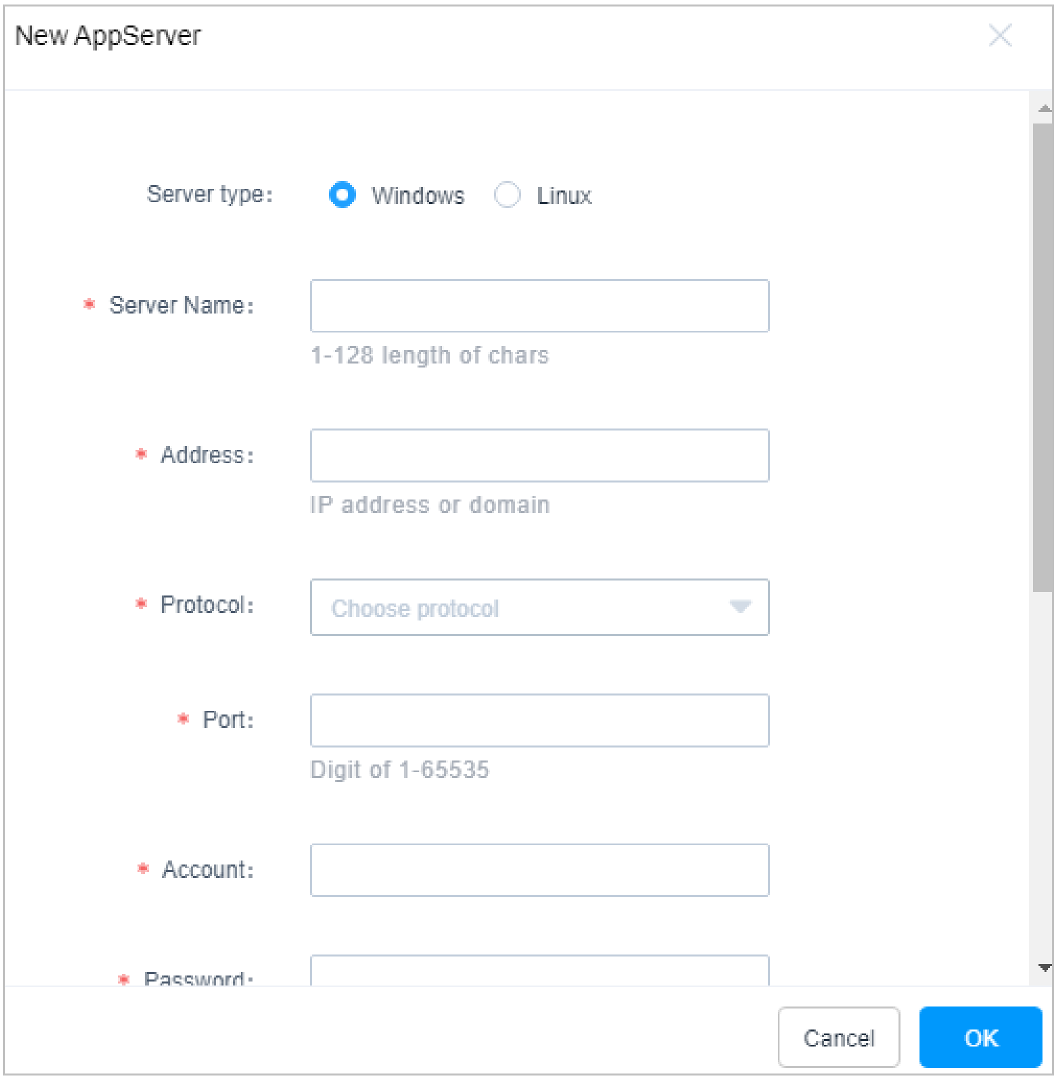


Table 6-5 New AppServer parameters

Parameter	Description
Server Type	• Windows • Linux
Server Name	Specifies the name of the application server. The server name must be unique in the CBH system.
Server	Specifies the IP address or domain name of the application server.

Parameter	Description
Type	Specifies the type of the browser or client tool used to access the application. ● If you set **Server type** to **Windows**: 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. ● If you set **Server type** to **Linux**: Only the Mozilla Firefox browser applications and Dameng data management tool V8 can be invoked. By default, each application resource type corresponds to an application program. You can obtain the application name from the default **Program Path**.
Port	Enter the port number for accessing the application publish server. The default port 3389 is used for a Windows server and default port 2376 is used for a Linux server.
Account	This parameter is mandatory if **Server type** is set to **Windows**. 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	● If you set **Server type** to **Windows**, enter the password of the server account used to access the application. ● If you set **Server type** to **Linux**, contact technical support to obtain the password.
Department Name	Specifies the department of the application server.
Program Path	This parameter is mandatory if **Server type** is set to **Windows**. 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.
Remarks	(Optional) Provides the description of the application server.

Step 4 Click **OK**.

----End

Importing Application Servers from a File

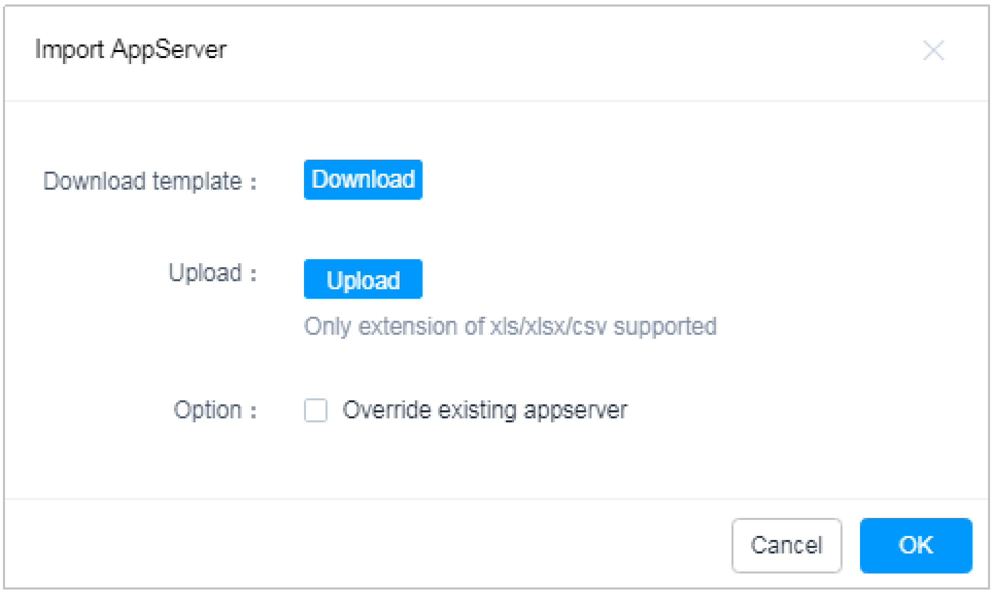
To import application server from a file, the file must be in .csv, .xls, or .xlsx format.

Step 1 Log in to the CBH system.

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

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

Figure 6-8 Importing application servers



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**.

----End

Adding an Application Resource

Step 1 Log in to the CBH system.

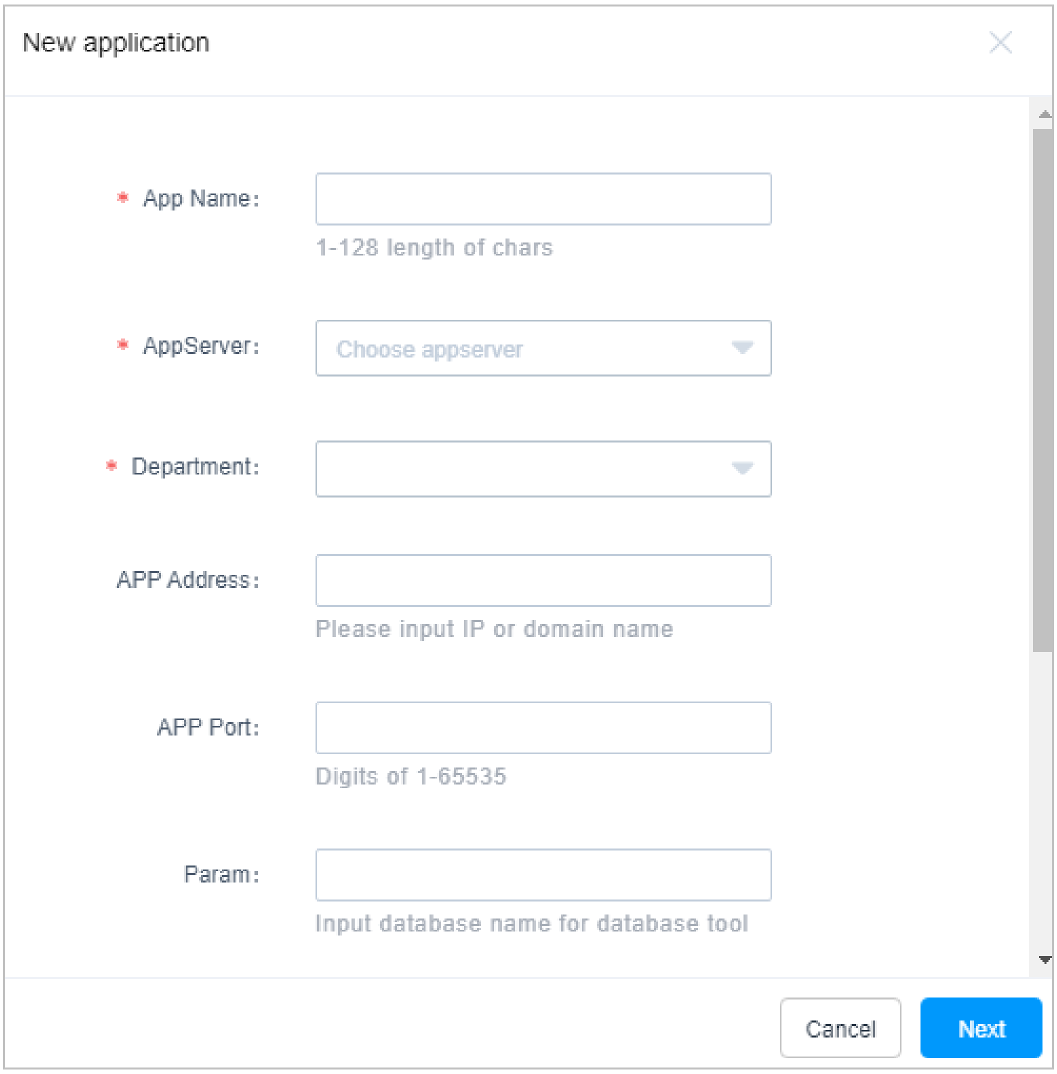
Step 2 Choose **Resource** > **Application** > **Application**.

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

Table 6-6 Parameters for adding a new 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 the CBH system. **NOTE** The application name must be unique in the CBH system. This means it cannot be the same as the name of any managed hosts or other application resources.
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.
Options	(Optional) Select **File Manage**, **uplink clipboard**, and/or **downlink clipboard**.
Label	(Optional) You can customize a label or select an existing one.
Remarks	(Optional) Provides the description of the application resource.

Figure 6-9 Creating an application



Step 4 Click **Next**.

Figure 6-10 Adding accounts for a new application

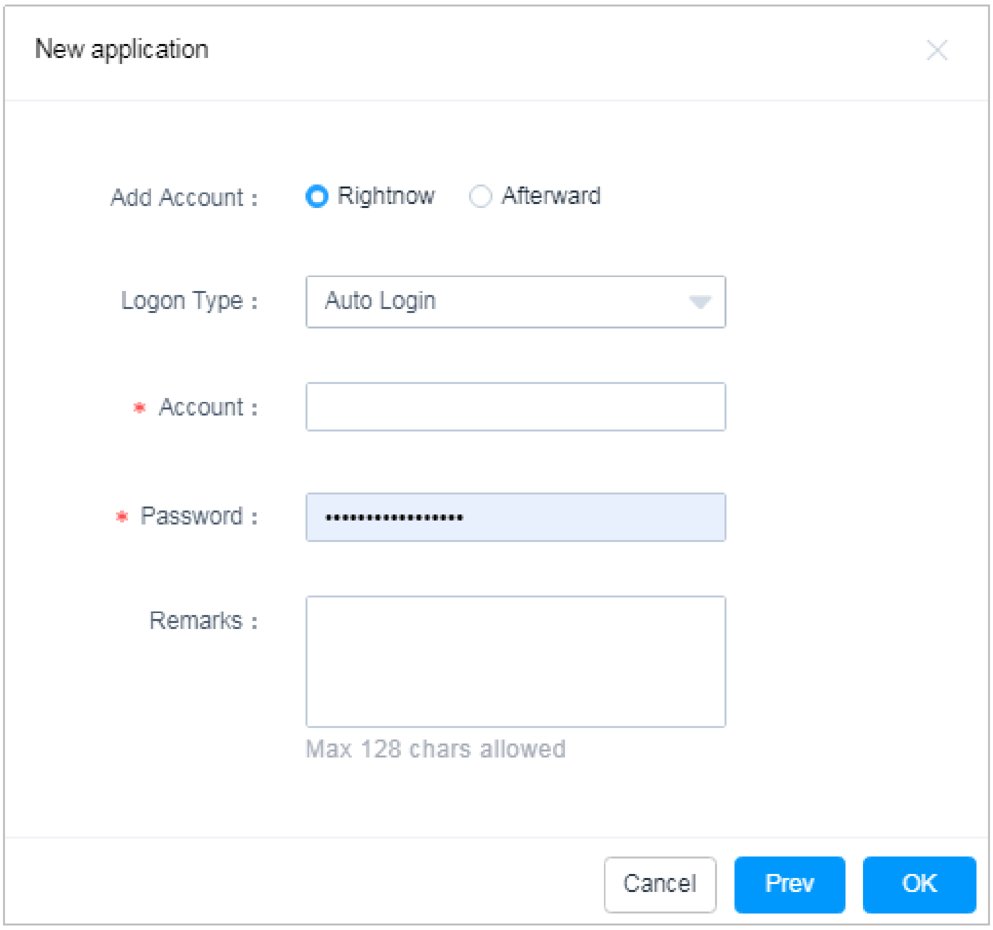


Table 6-7 Parameters for adding accounts for an application resource

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

Parameter	Description
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**.

----End

Importing Application Resources from a File

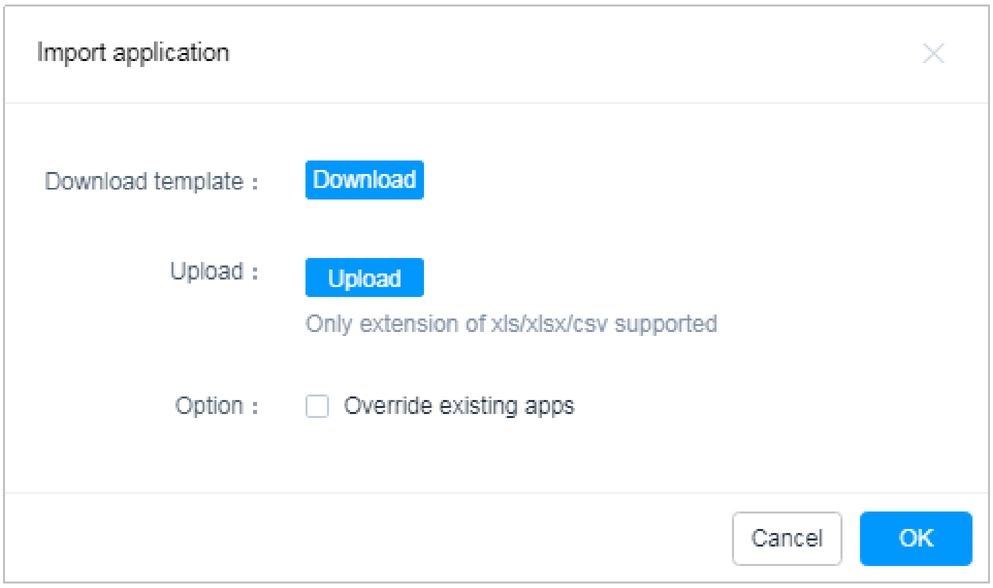
To import application server from a file, the file must be in .csv, .xls, or .xlsx format.

Step 1 Log in to the CBH system.

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

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

Figure 6-11 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**.

----End

6.4 Adding Accounts of Managed Host or Application Resources into CBH

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 account is added for a host or application resource in the CBH system, the **Empty** account is generated by default. In this situation, when you log in to the host or application resource through CBH, a username and password is required.

This topic describes how to add a managed resource account after resources are managed in CBH.

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 the CBH system.

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

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

Figure 6-12 New account of managed resources

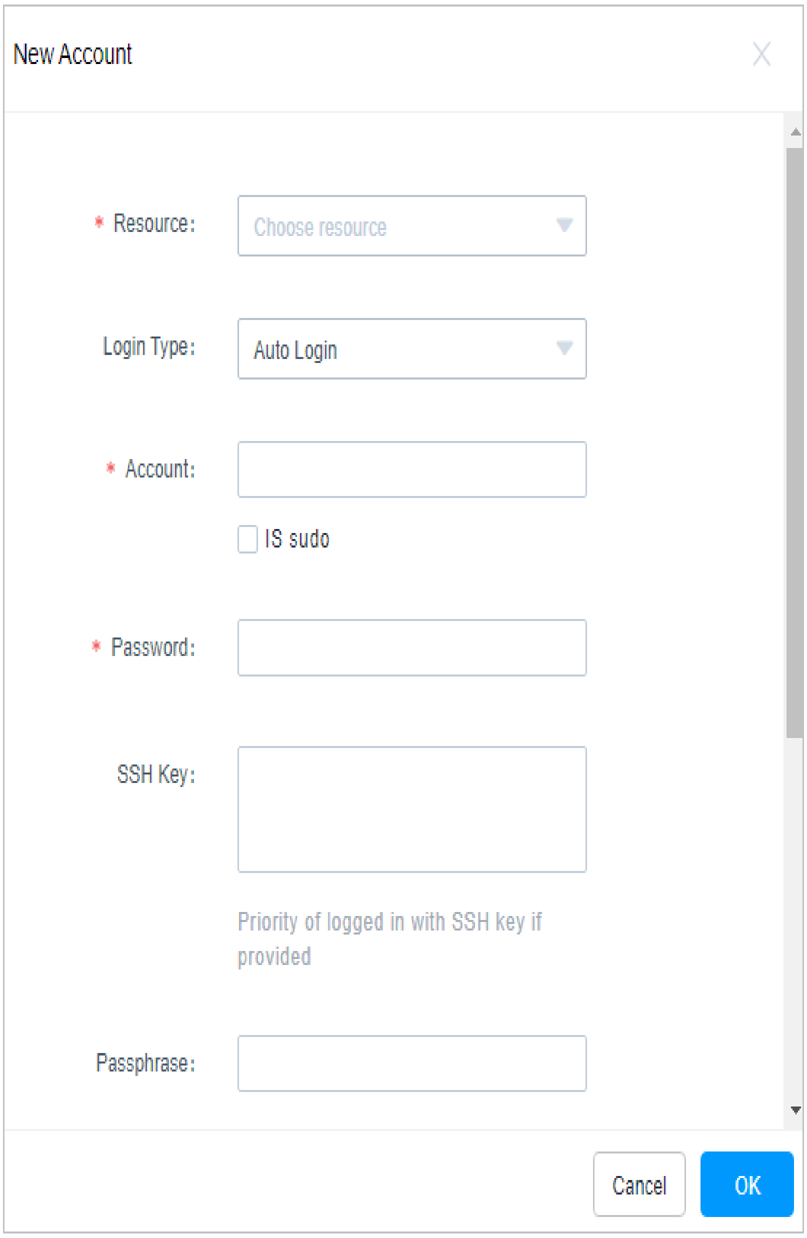


Table 6-8 Parameters for new managed resource accounts

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

Parameter	Description
Logon Type	Login mode. You can select **Manual Login**, **Auto Login**, or **Sudo 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**. ● **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 CBH system 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.
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**.
CSMS Credentials	(This parameter is available only when login mode is CSMS credential login.) Select the CSMS credential to be managed.
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 CBH

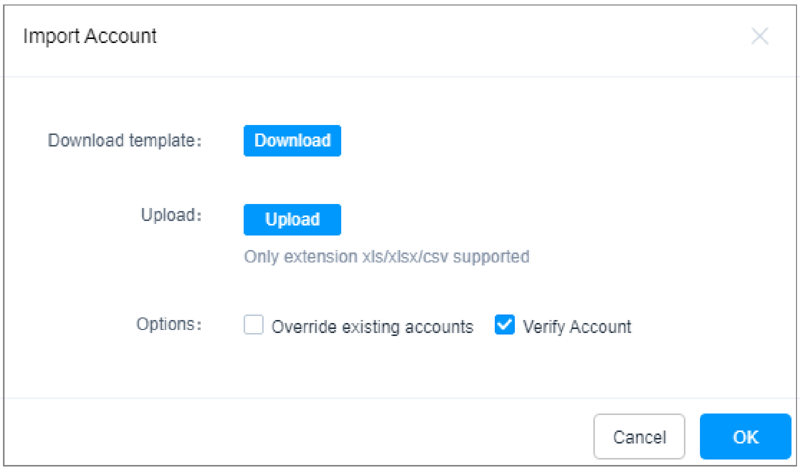
To import application server from a file, the file must be in .csv, .xls, or .xlsx format.

Step 1 Log in to the CBH system.

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

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

Figure 6-13 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 6-9 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.
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**, **VNC**, **Telnet**, **FTP**, **SFTP**, **DB2**, **MySQL**, **SQL Server**, **Oracle**, **SCP**, and **Rlogin**. ● Application resource types: – Windows servers: 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 and Other. – Linux servers: DM Tool and Mozilla Firefox for Linux
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 CBH 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**.

----End

6.5 Cloud Service Management

6.5.1 Creating a Kubernetes Server

You can add Kubernetes servers to CBH for management. This section describes how to add a Kubernetes server to CBH.

Constraints

- The number of managed Kubernetes servers is restricted by the CBH system license.
- You must have the permission to create a **Kubernetes server**.
- Only the Kubernetes service of the professional edition can be managed with CBH.
- To use this function, the bastion host version must be V3.3.48.0 or later.

Procedure

Step 1 Log in to the CBH system.

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 6-14 Creating a Kubernetes server

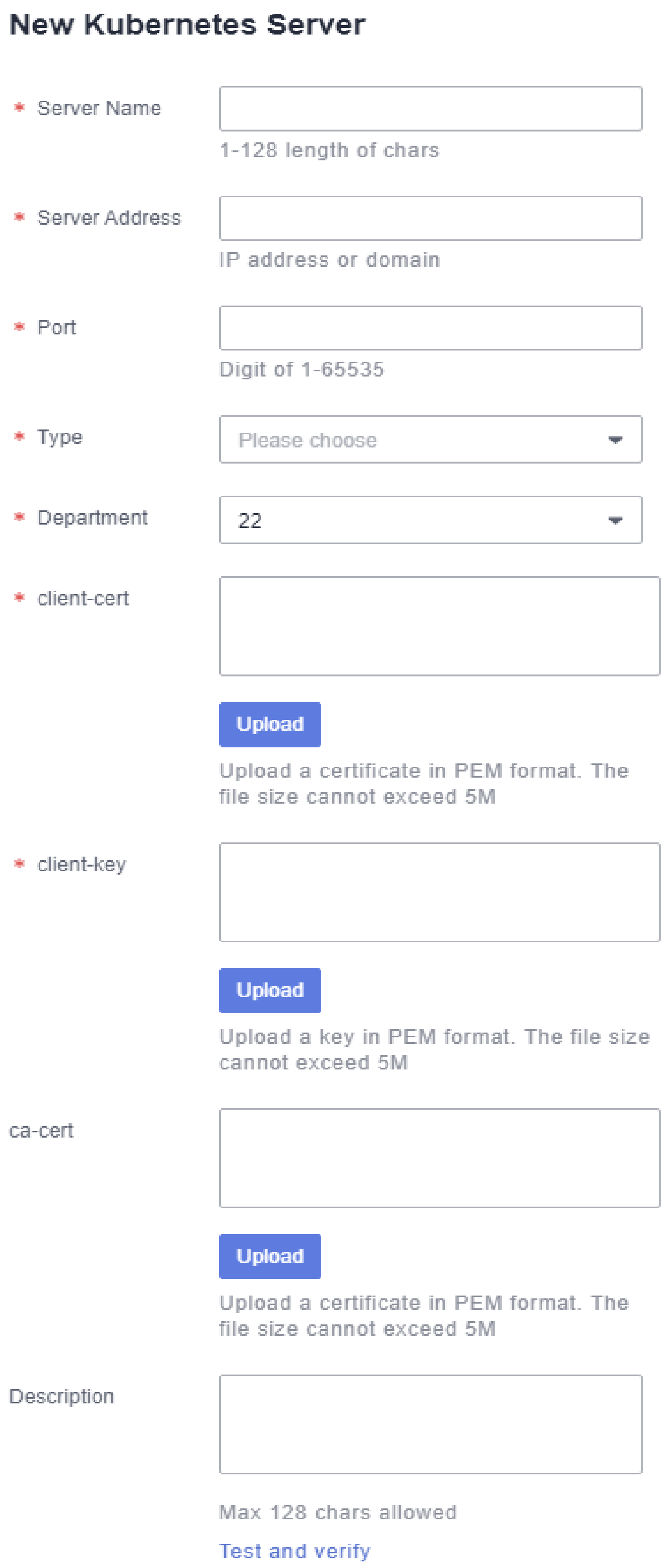


Table 6-10 Parameters

Parameter	Description
Server Name	Customize a service name.
Server	Enter your Kubernetes server address.
Port	Enter your Kubernetes server port number.
Type	For V3.3.48.0, only **Kubernetes** can be selected for the bastion host.
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

6.5.2 Operations About Kubernetes Servers

After Kubernetes servers are managed by CBH, you can delete managed servers or modify information at any time.

Constraints

- The number of managed Kubernetes servers is restricted by the CBH system license.
- 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

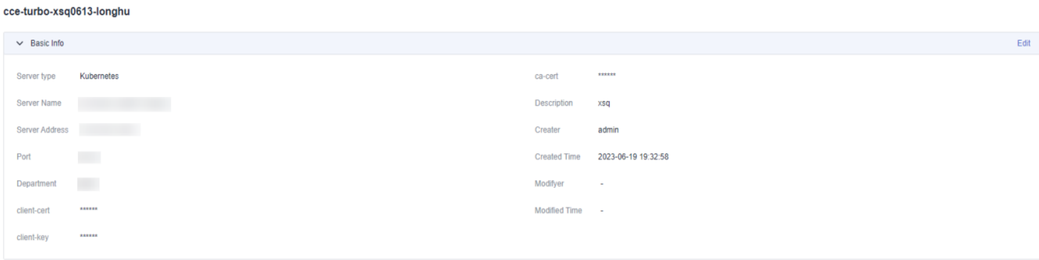
Step 1 Log in to the CBH system.

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 6-15 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 6-10**.

Step 6 Click **OK**. The Kubernetes server information is modified.

----End

Deleting a Kubernetes Server

Step 1 Log in to the CBH system.

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

6.5.3 Creating a Container

You can add Kubernetes containers to CBH for management. This section describes how to add a container to CBH.

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 the CBH system.

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 6-16 Creating a Container

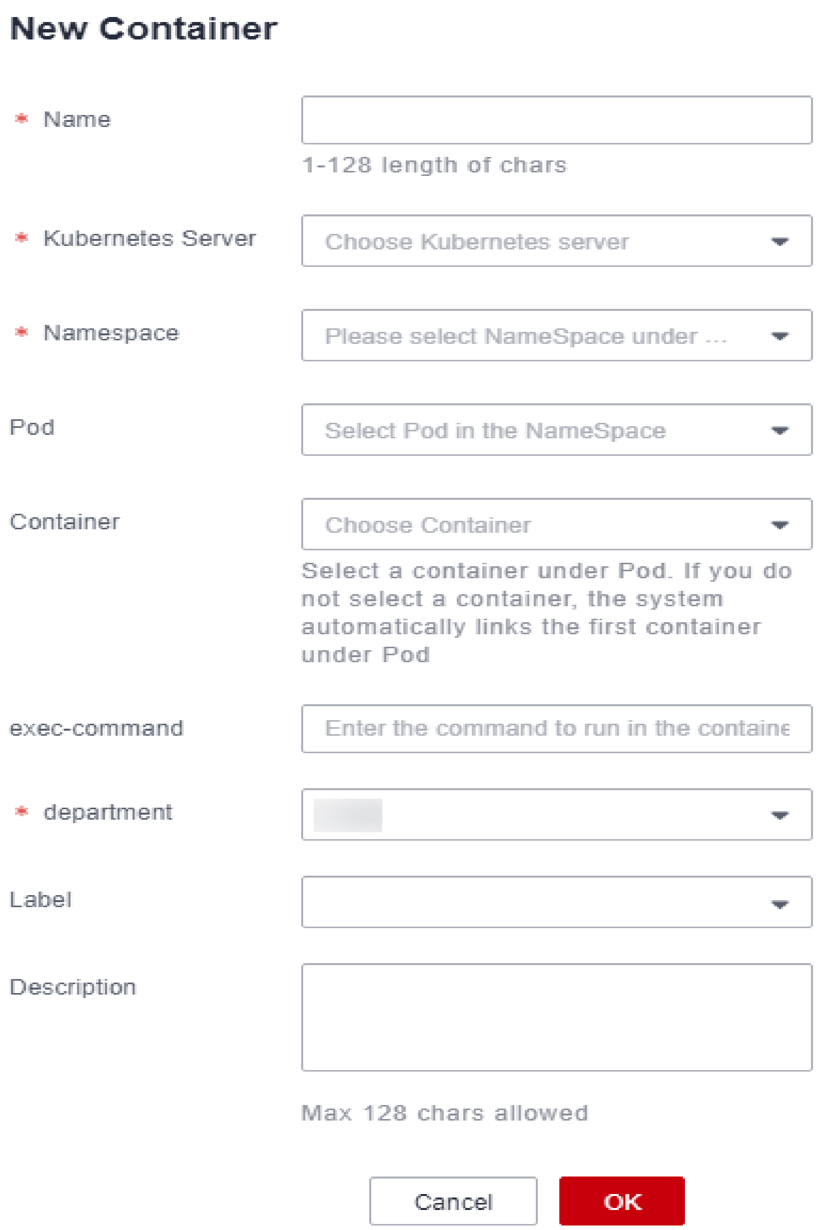


Table 6-11 Parameters for creating a container

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

6.5.4 Operations About Containers

After a container is managed by CBH, 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.

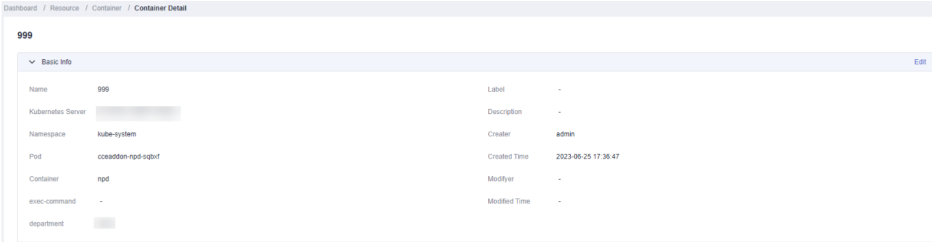
Editing a Container

Step 1 Log in to the CBH system.

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 6-17 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 6-11**.

Step 5 After modifying the parameters, click **OK**.

----End

Delete Containers

Step 1 Log in to the CBH system.

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**.

----End

6.6 Resource Management

6.6.1 Verifying Managed Resource Accounts

The status of a managed resource account is used to identify whether the password of the account is correct. 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 the history sessions.

Table 6-12 Resource account status description

Status	Description
Normal	If the account username and password are correct and the account can be used to log in to the system, the account is in the **Normal** status.

Status	Description
Abnormal	If the account username or password is incorrect, the 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 to CBH, the account is in the **N/A** status.

Constraints

Accounts for application resources cannot be verified online.

Prerequisites

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

Automatic Inspection

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 Log in to the CBH system.

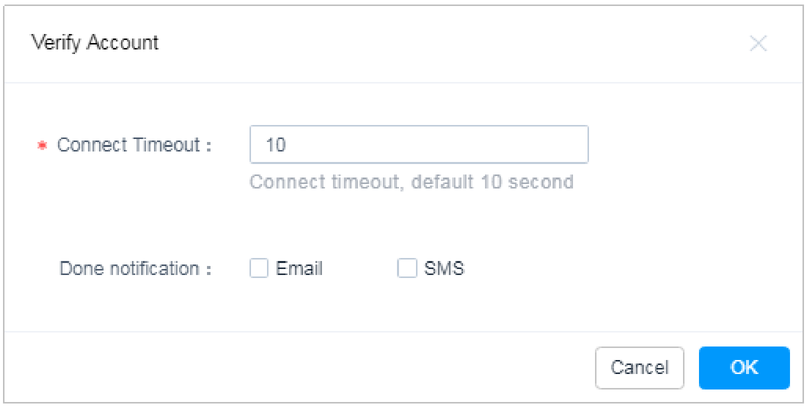
Step 2 Choose **Resource** > **Account** in the navigation pane.

Step 3 Select an account and click **Test and verify** at the bottom of the list. The verification configuration dialog box is displayed.

Step 4 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 notification is sent.
- To receive notifications, select **Email** or **SMS**. Additionally, you can view the verification results on the **Tasks** page.

Figure 6-18 Verify Account



Step 5 Click **OK**. Refresh the managed resource account list page and view the verification results in the **Status** column.

----End

Batch Account Verification

CBH gives you the ability to verify managed resource accounts by account group with just one click.

Step 1 Log in to the CBH system.

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

Step 3 Select an account group and click **Test and verify** at the bottom of the list. The verification configuration dialog box is displayed.

Step 4 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 notification is sent.
- To receive notifications, select **Email** or **SMS**. Additionally, you can view the verification results on the **Tasks** page.

Step 5 Click **OK**. Go to the managed resource account list page and view the verification results in the **Status** column.

----End

6.6.2 Deleting Managed Resources from the CBH System

This topic describes how to delete managed resources, such as host resources, application servers, application resources, and managed resource accounts, from the CBH system.

- Managed resource accounts will be deleted together with the related resources the instant the resources are deleted.
- Application resources will be deleted together with the related application servers the instant the application servers are deleted.

Prerequisites

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

Deleting One or More Managed Resource Accounts

Step 1 Log in to the CBH system.

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

Step 3 Click **Delete** in the **Operation** column of the row where the account locates.

Step 4 Select multiple accounts and click **Delete** at the bottom of the account list to delete all selected accounts together.

----End

Deleting One or More Host Resources

Step 1 Log in to the CBH system.

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

Step 3 Locate the row where the host resource you want to delete resides and click **More** > **Delete** in the **Operation** column.

Step 4 Select multiple host resources and click **Delete** at the bottom of the list to delete all selected host resources.

----End

Deleting One or More Application Servers

Step 1 Log in to the CBH system.

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

Step 3 Locate the row containing the application server you want to delete and click **Delete** in the **Operation** column to delete the application server.

Step 4 Select multiple application servers and click **Delete** at the bottom of the application server list to delete all selected application servers.

----End

Deleting One or More Application Resources

Step 1 Log in to the CBH system.

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

Step 3 Locate the row where the application you want to delete resides and click **More** > **Delete** in the **Operation** column to delete the application resource.

Step 4 Select multiple application resources and click **Delete** at the bottom of the application list to delete all selected application resources together.

----End

6.6.3 Querying and Editing Managed Resource Configurations

This topic describes how to query and edit configurations of managed resources, including host resources, application servers, application resources, and managed resource accounts.

Prerequisites

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

Querying and Editing Host Configurations

Step 1 Log in to the CBH system.

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

Step 3 Query host resources.

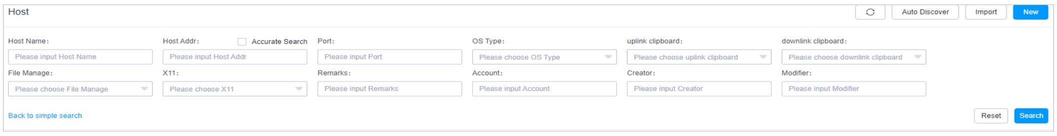
- Quick search

  Enter a keyword in the search box to quickly query host resources by host name, host IP address, and port number.

- Advanced search

  Enter keywords in the corresponding attribute search boxes to search for host resources in exact mode.

Figure 6-19 Advanced search



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

Figure 6-20 Viewing host resource configurations

Step 5 View and edit basic information of the host resource.

In the **Basic Info** area, click **Edit**. In the displayed dialog box, edit the basic information.

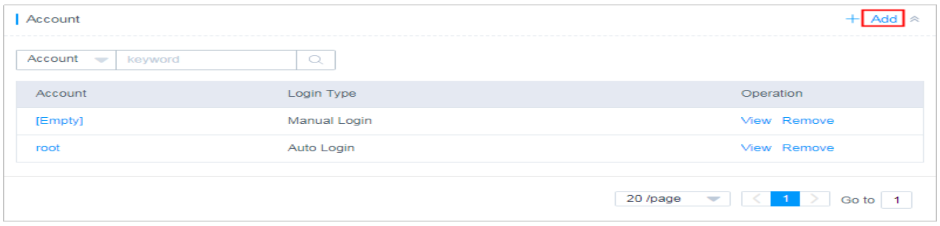
- You can edit the **Host Name**, **Host Address**, **Port**, **OS Type**, **Department**, and **Remarks**.
- The **Protocol** cannot be modified.

Figure 6-21 Viewing basic host information

Step 6 View and edit accounts of the host resource.

- To add an account for the host resource, click **Add** in the **Account** area and complete configurations in the displayed dialog box.
- To only remove an account, click **Remove** in the row of the account.

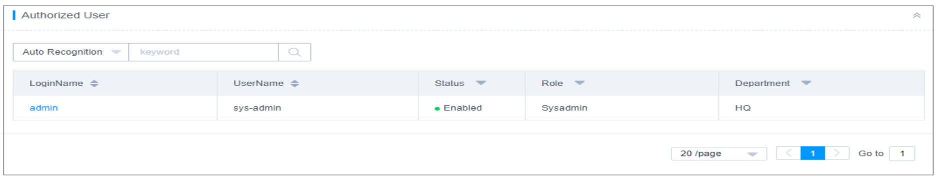
Figure 6-22 Viewing accounts of a host resource



Step 7 View authorized users of the host resource.

Expand the **Authorized User** area to view information about system users who are authorized to manage the host.

Figure 6-23 Viewing authorized users of a host resource



----End

Batch Editing Host Resource Configurations

- Batch editing department of multiple hosts
- Batch editing options, including file management, uplink and downlink clipboard function, and X11 forwarding.
- Batch editing the host encoding formats

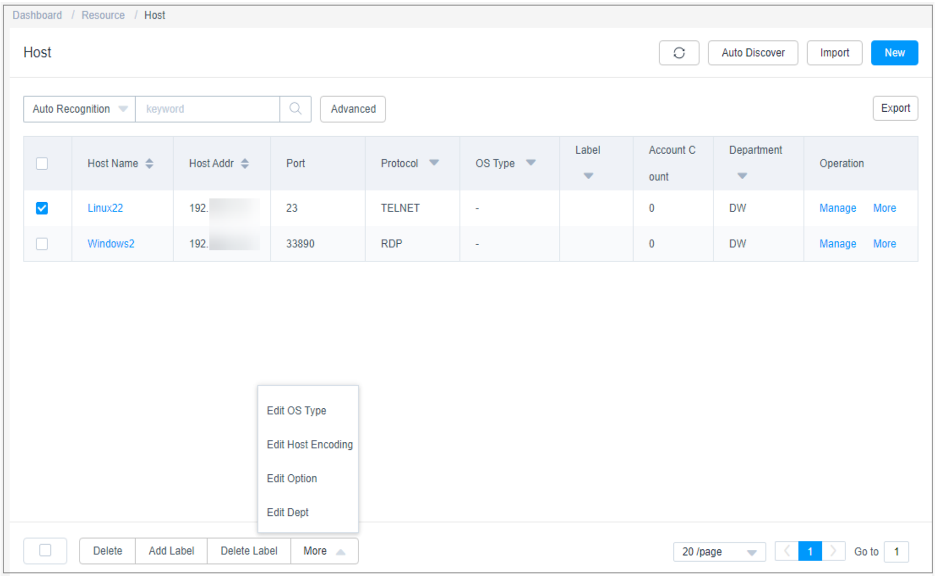
- Batch editing the host OS types

Step 1 Log in to the CBH system.

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

Step 3 In the host resource list, select the host resource you want to edit and click **More** in the lower left corner to expand the batch operation buttons.

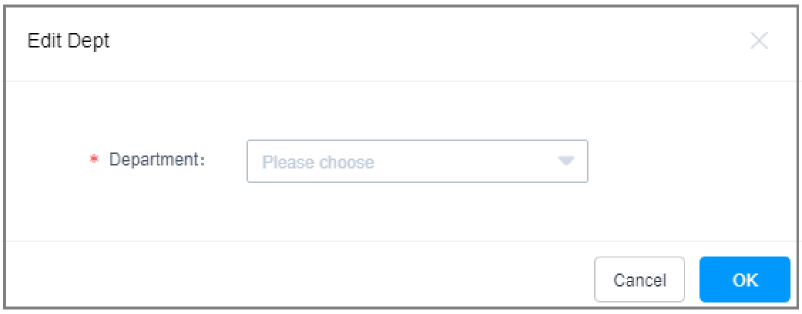
Figure 6-24 Batch editing host resource configurations



Step 4 Edit department of multiple selected hosts at a time.

1. Click **Edit Dept**.

Figure 6-25 Edit Dept



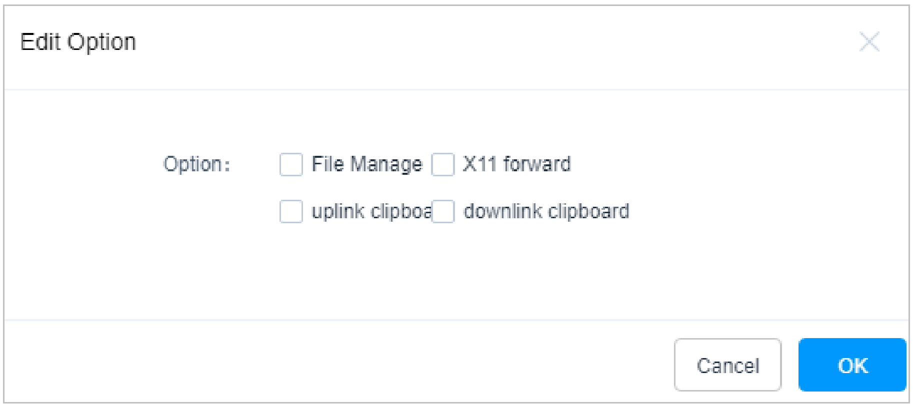
2. In the displayed dialog box, select a department.
3. Click **OK**.

Step 5 Edit options for multiple hosts.

- **File Manage**: This option is supported only by host resources using the SSH, RDP, or VNC protocol.
- Configurations for uplink and downlink clipboard can only be modified for hosts with **Protocol** set to **RDP**.
- **X11 forward**: This option is supported only by hosts resources using the SSH protocol.

1. Click **Edit Option**.

Figure 6-26 Edit Option

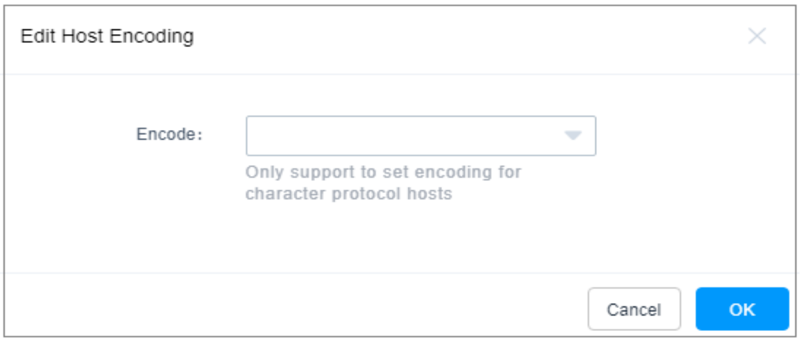


2. Select **File Manage**, **uplink clipboard**, **downlink clipboard**, and/or **X11 forward**.
3. Click **OK**.

Step 6 Edit encode of hosts using SSH or Telnet protocol.

1. Click **Edit Host Encoding**.

Figure 6-27 Edit Host Encoding

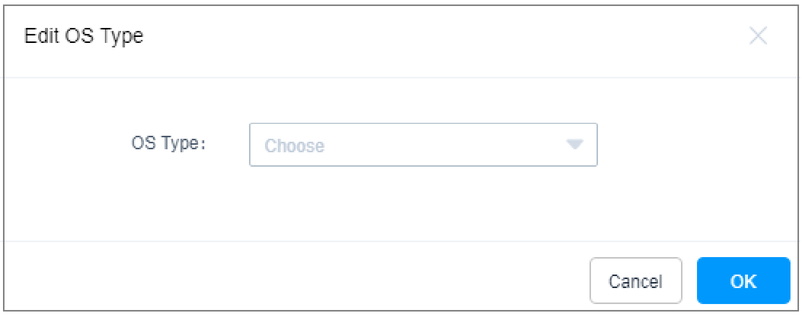


2. Select the encode format. Options are **UTF-8**, **Big5**, and **GB 18030**.
3. Click **OK**.

Step 7 Edit OS type of multiple selected hosts.

1. Click **Edit OS Type**.

Figure 6-28 Edit OS Type



2. Select an OS type.
3. Click **OK**.

----End

Viewing and Editing Application Server Configurations

Step 1 Log in to the CBH system.

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

Step 3 Query application servers.

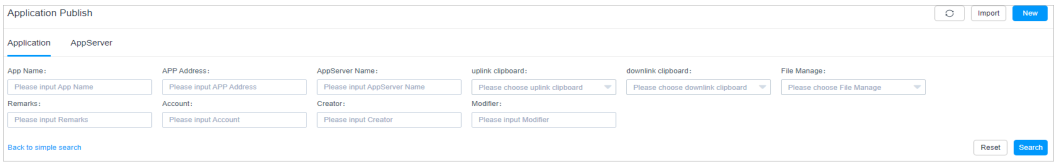
- Quick search

  Enter a keyword in the search box and search for application servers by server name, server address, or application server account.

- Advanced search

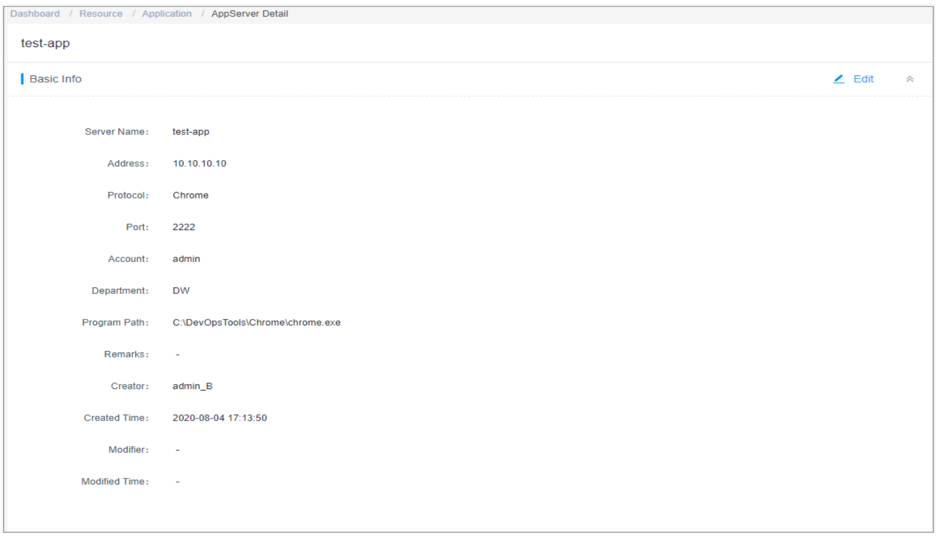
  Enter keywords in the corresponding attribute search boxes to search for application servers in exact mode.

Figure 6-29 Advanced search



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

Figure 6-30 Viewing application server configurations



Step 5 View and edit basic information.

In the **Basic Info** area on the displayed page, click **Edit**. In the displayed dialog box, edit the basic information.

- You can edit **Server Name**, **Address**, **Port**, **Account**, **Password**, **Department**, **Program Path**, and **Remarks**.
- The **Protocol** cannot be modified.

----End

Batching Editing Application Server Configurations

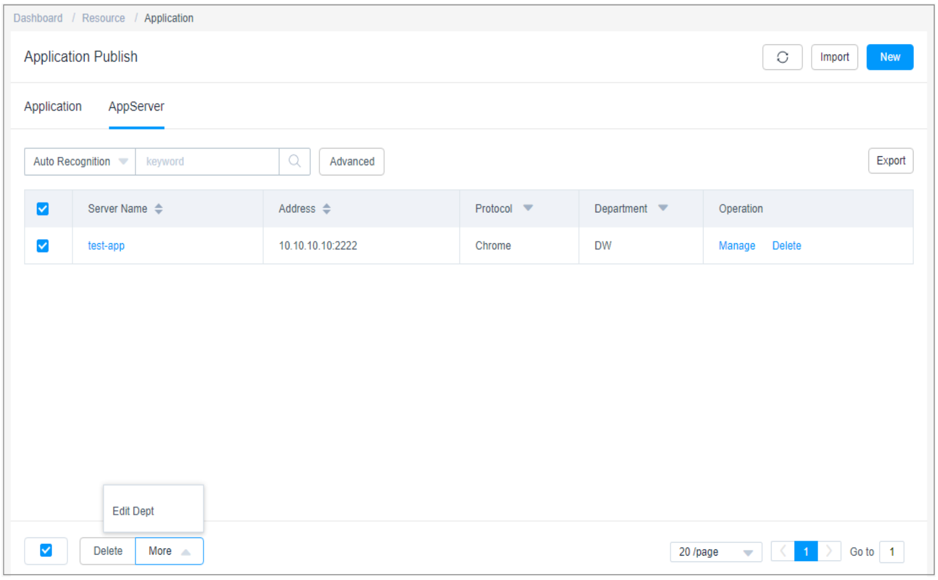
Batching editing departments of multiple application servers

Step 1 Log in to the CBH system.

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

Step 3 In the application server list, select the application servers you want to edit and click **More** in the lower left corner.

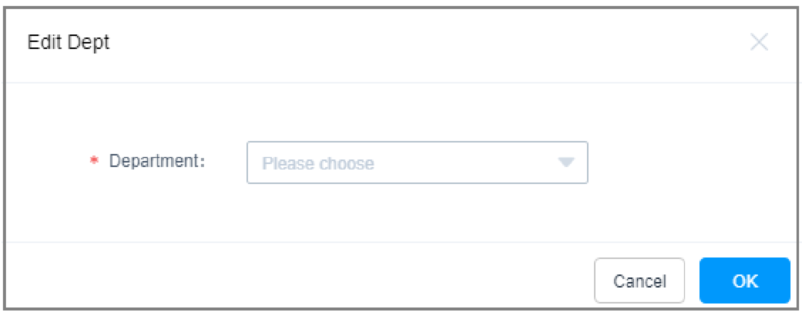
Figure 6-31 Batching Editing Application Server Configurations



Step 4 Edit department of multiple selected hosts at a time.

1. Click **Edit Dept**.

Figure 6-32 Edit Dept



2. In the displayed dialog box, select a department.

3. Click **OK**.

----End

Viewing and Editing Application Publish Configurations

Step 1 Log in to the CBH system.

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

Step 3 Query application resources.

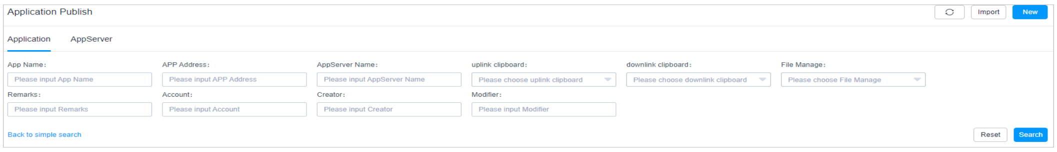
- Quick search

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

- Advanced search

  Enter keywords in the corresponding attribute search boxes to search for application resources in exact mode.

Figure 6-33 Advanced search



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

Figure 6-34 Viewing configurations of an application

Step 5 View and edit basic information.

In the **Basic Info** area, click **Edit**. In the displayed dialog box, edit the basic information.

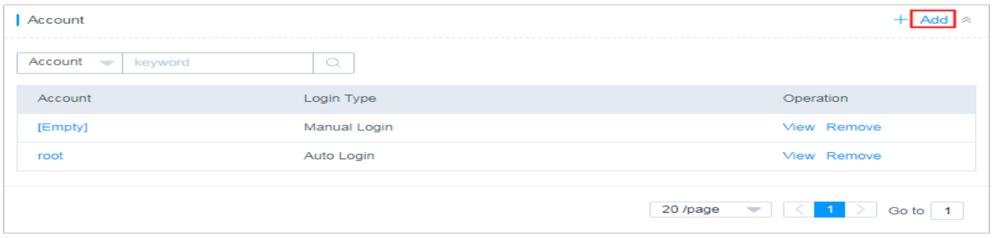
- You can edit the **App Name**, **AppServer**, **APP Port**, **APP Address**, **Department**, and **Remarks** fields.

Figure 6-35 Viewing basic application information

Step 6 View and edit accounts of the application resource.

- To add an account for an application resource, click **Add** in the **Account** area and complete configurations in the displayed dialog box.
- To only remove an account, click **Remove** in the row of the account.

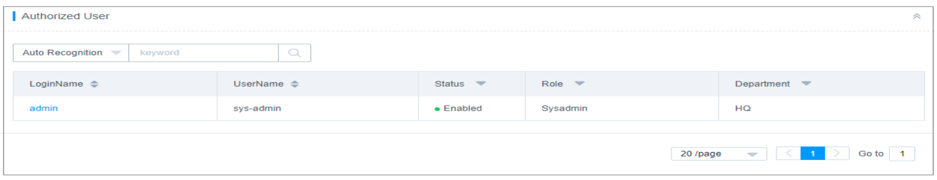
Figure 6-36 Viewing accounts of an application resource



Step 7 View authorized users of the application resource.

Expand the **Authorized User** area to view information about system users who are authorized to manage the application.

Figure 6-37 Viewing authorized users of a host resource



----End

Batch Editing Configurations of Application Resources

- Batching editing departments of multiple application resources

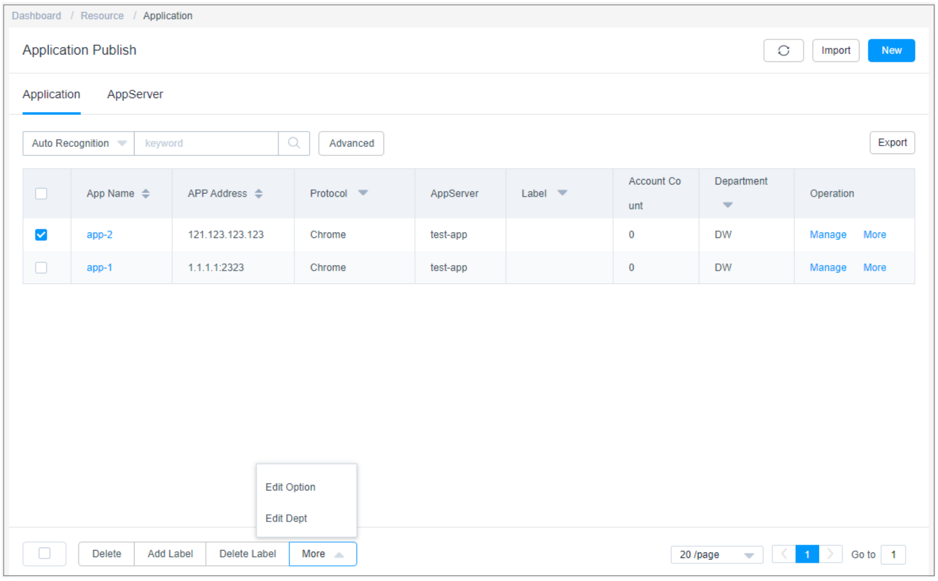
- Batch editing options, including file management and clipboard function, of multiple applications and X11 forwarding

Step 1 Log in to the CBH system.

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

Step 3 In the application resource list, select the application resource you want to edit and click **More** in the lower left corner.

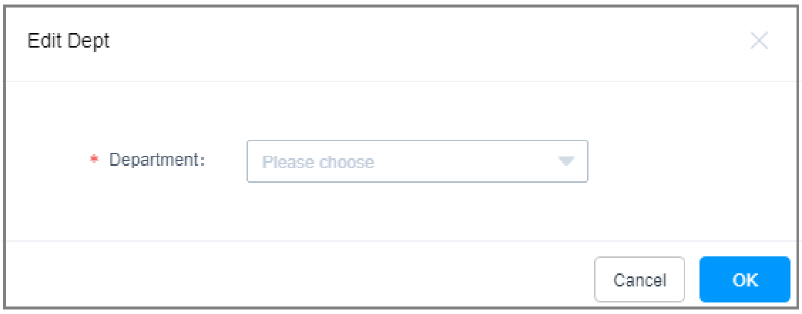
Figure 6-38 Batch editing application configurations



Step 4 Edit department of multiple selected hosts at a time.

1. Click **Edit Dept**.

Figure 6-39 Edit Dept

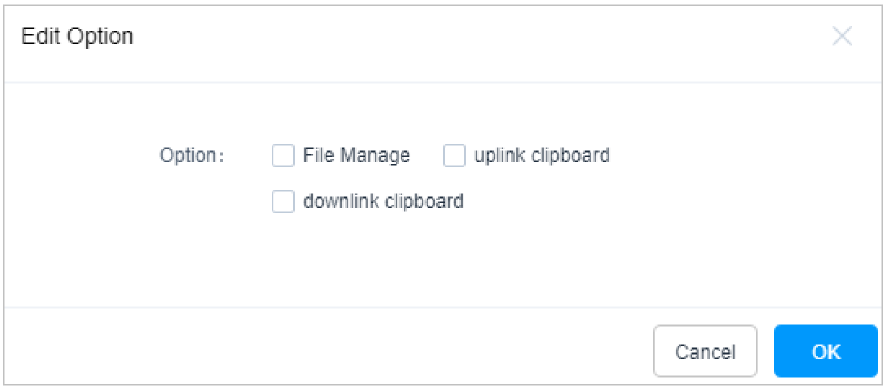


2. In the displayed dialog box, select a department.
3. Click **OK**.

Step 5 Edit options for multiple hosts.

1. Click **Edit Option**.

Figure 6-40 Edit Option



2. Select **File Manage** and/or **Clipboard**.
3. Click **OK**.

----End

Querying and Editing Account Configurations

Step 1 Log in to the CBH system.

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

Step 3 Query application resources.

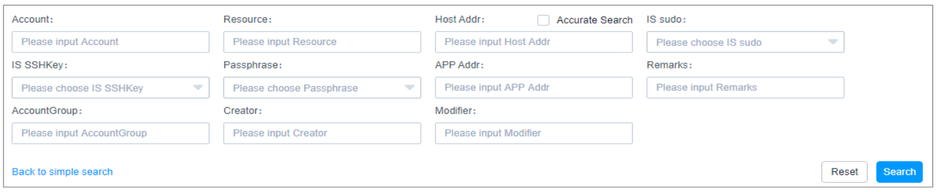
- Quick search

  Enter a keyword in the search box to quickly search for application resources by account, related resource, host address, and privileged account.

- Advanced search

  Enter keywords in the corresponding attribute search boxes to search for accounts in exact mode.

Figure 6-41 Advanced search



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

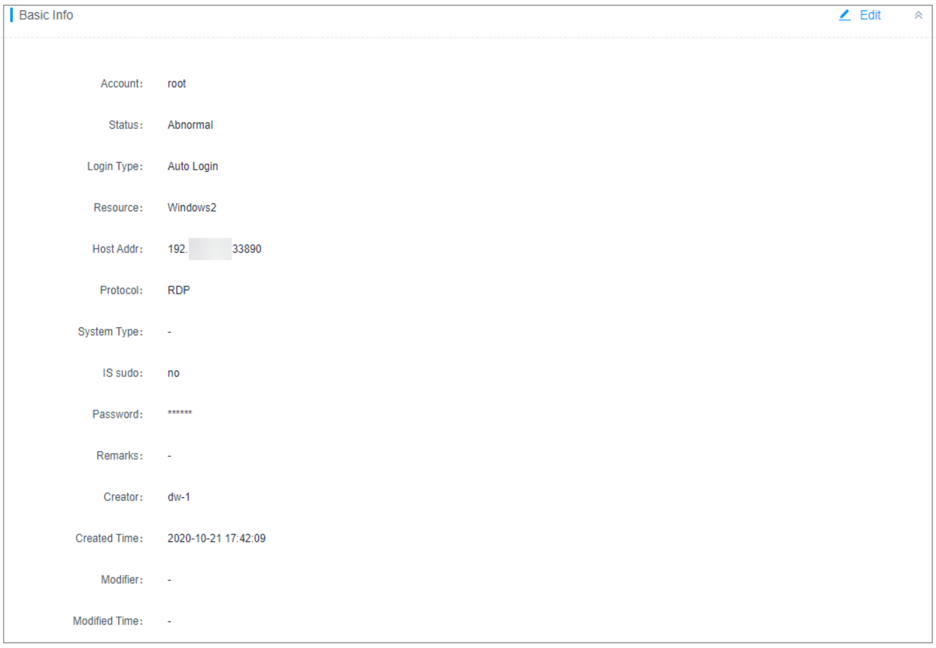
Figure 6-42 Viewing account configurations

Step 5 View and edit basic information of the account.

In the **Basic Info** area on the displayed page, click **Edit**. In the displayed dialog box, edit the basic information.

- You can edit the **IS sudo**, **Password**, and **Remarks** fields.
- The **Account**, **Resource**, **Login Type**, **SSH Key**, and **Passphrase** fields cannot be modified.

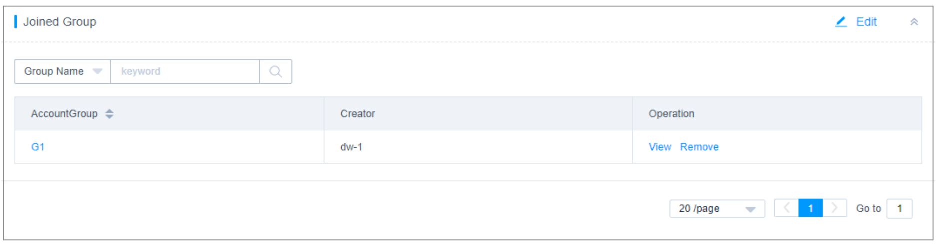
Figure 6-43 Viewing basic application information



Step 6 View and edit the account groups to which an account is added.

- To change the account groups that the account belongs to, click **Edit** in the **Joined Group** area and complete modifications in the displayed dialog box.
- To remove the account from an account group, click **Remove** in the row of the account group.

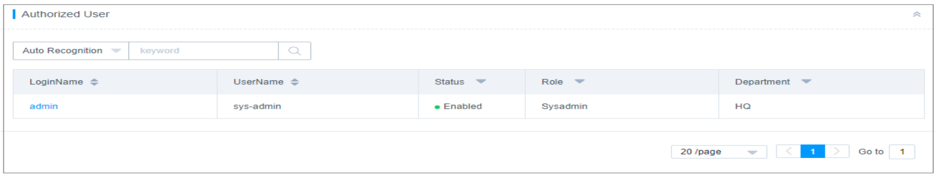
Figure 6-44 Viewing the account groups that an account belongs to



Step 7 View authorized users of the account.

Expand the **Authorized User** area to view information about system users who have been granted permissions to use the account.

Figure 6-45 Viewing authorized users of a host resource



----End

6.6.4 Exporting Resource Information

CBH allows you to export resource information in batches so that you can have a local backup and edit basic resource information quickly.

- To enhance information security of resources, CBH allows you to 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.

Prerequisites

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

Batch Editing Host Information

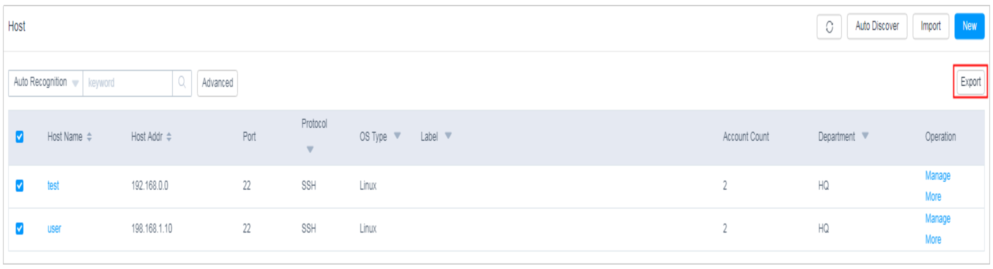
Step 1 Log in to the CBH system.

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

Step 3 Select the hosts you want to export.

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

Figure 6-46 Exporting host information



Step 4 Click **Export**.

Step 5 In the displayed **OK** dialog box, configure encryption options.

1. **Set encryption password**: This parameter is optional. If this parameter is not set, the downloaded file is an unencrypted CSV file. If you set a password, the downloaded file is an encrypted .zip file.
2. **User Password**: This parameter is mandatory. You are required to enter your login password for verification. The host resource file can be downloaded only after the verification is successful. This ensures password security of managed resource accounts.
3. Click **OK** to download the file locally.

Figure 6-47 Exporting host information

----End

Batch Exporting Application Server Information

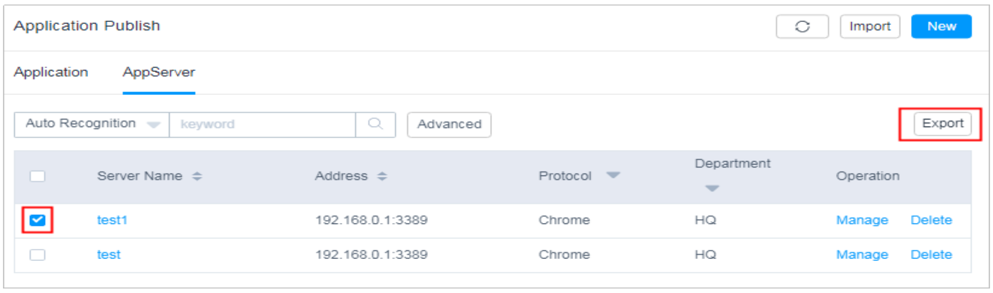
Step 1 Log in to the CBH system.

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

Step 3 Select the application servers you want.

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

Figure 6-48 Exporting application server information



Step 4 Click **Export**.

Step 5 In the displayed **OK** dialog box, configure encryption options.

1. **Set encryption password**: This parameter is optional. If this parameter is not set, the downloaded file is an unencrypted CSV file. If you set a password, the downloaded file is an encrypted .zip file.

2. **User Password**: This parameter is mandatory. You are required to enter your login password for verification. The application server resource file can be downloaded only after the verification is successful. This ensures password security of managed resource accounts.
3. Click **OK** to download the file locally.

Figure 6-49 Exporting application server information

----End

Batch Exporting Application Resource Information

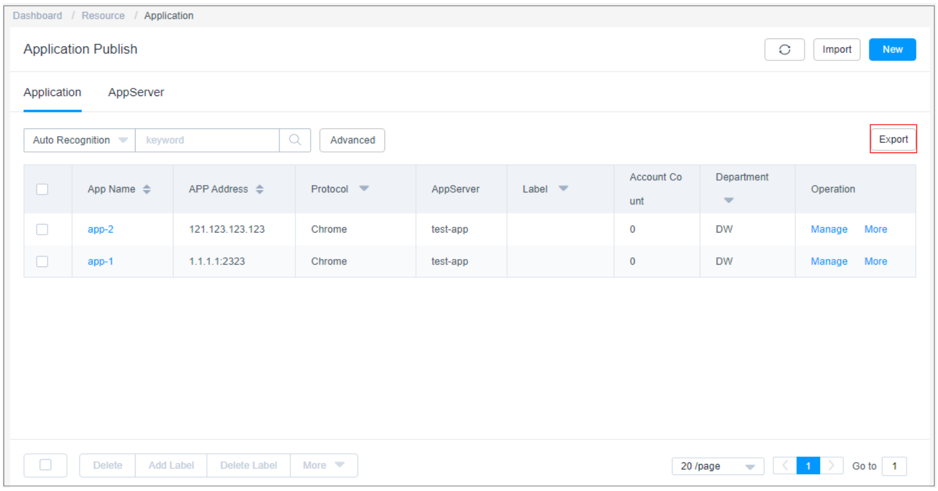
Step 1 Log in to the CBH system.

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

Step 3 Select the application resources you want.

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

Figure 6-50 Exporting application information



Step 4 Click **Export**.

Step 5 In the displayed **OK** dialog box, configure encryption options.

1. **Set encryption password**: This parameter is optional. If this parameter is not set, the downloaded file is an unencrypted CSV file. If you set a password, the downloaded file is an encrypted .zip file.
2. **User Password**: This parameter is mandatory. You are required to enter your login password for verification. The application resource information file can be downloaded only after the verification is successful. This ensures password security of managed resource accounts.
3. Click **OK** to download the file locally.

Figure 6-51 Exporting application information

----End

Batch Exporting Accounts of Resources

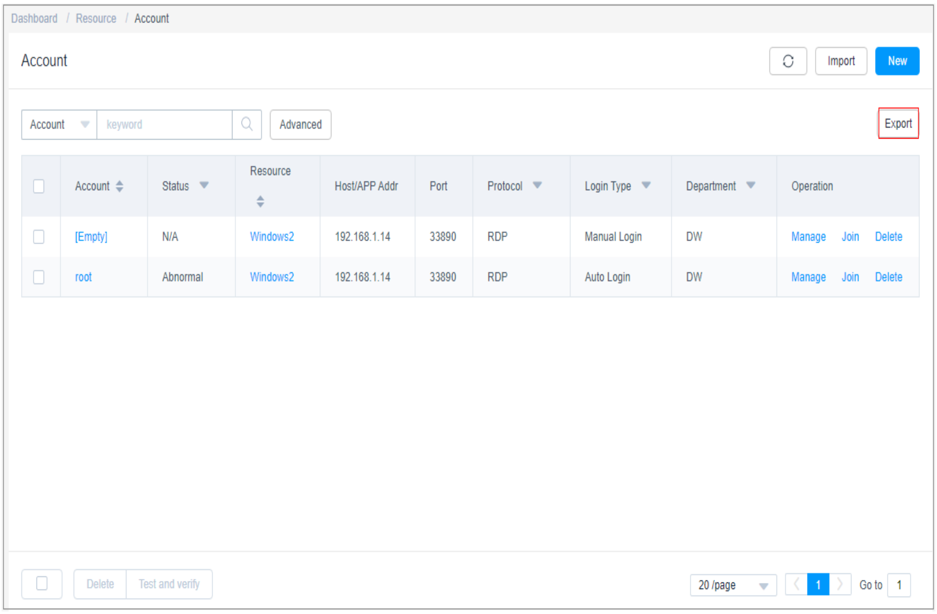
Step 1 Log in to the CBH system.

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

Step 3 Select the accounts you want to export.

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

Figure 6-52 Exporting account information



Step 4 Click **Export**.

Step 5 In the displayed **OK** dialog box, configure encryption options.

1. **Set encryption password**: This parameter is optional. If this parameter is not set, the downloaded file is an unencrypted CSV file. If you set a password, the downloaded file is an encrypted .zip file.
2. **User Password**: This parameter is mandatory. You are required to enter your login password for verification. The account information file can be downloaded only after the verification is successful. This ensures password security of managed resource accounts.
3. Click **OK** to download the file locally.

Figure 6-53 Exporting the account of managed resources

----End

6.6.5 Adding a Resource Account to an Account Group

This section describes how to add a resource account to an account group. A resource account can be added to multiple account groups.

Constraints

- 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.
- An account can be added to multiple account groups.

Prerequisites

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

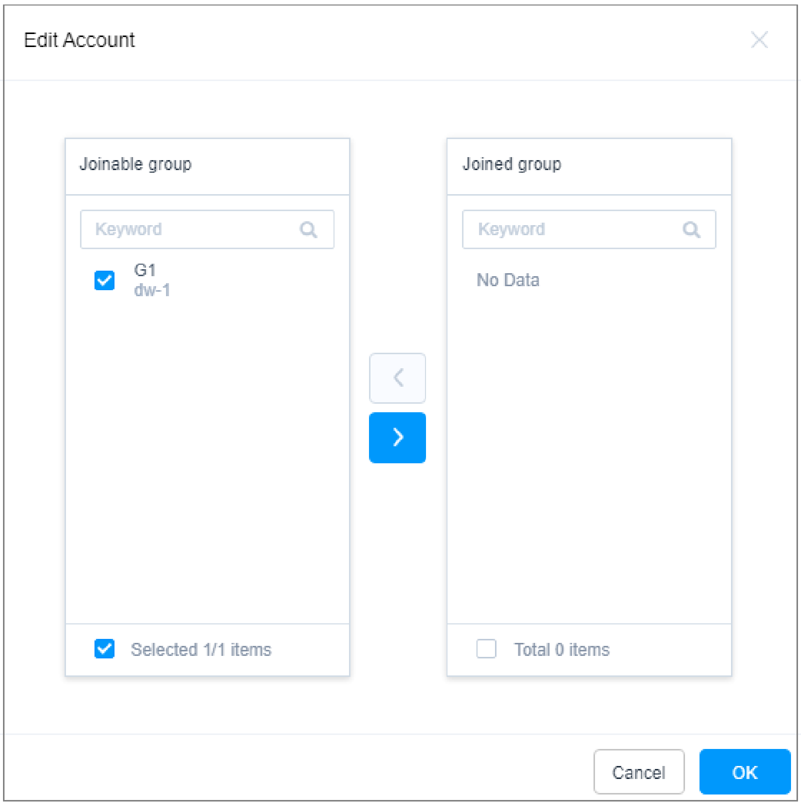
Adding an Account to an Account Group

Step 1 Log in to the CBH system.

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

Step 3 In the **Operation** column of the account, click **Join**.

Figure 6-54 Adding an account to an account group



Step 4 In the displayed **Edit Account** dialog box, select one or more account groups and add the account to them.

Step 5 Click **OK**. You can then view the account groups that the account has been added.

----End

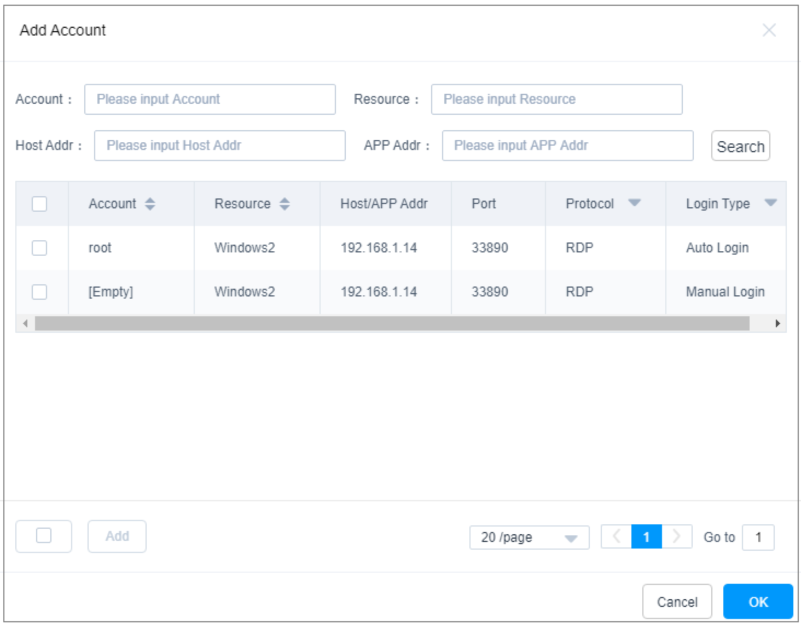
Adding Multiple Accounts to an Account Group

Step 1 Log in to the CBH system.

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

Step 3 In the **Operation** column of the account, click **Add Account**.

Figure 6-55 Batch adding accounts to an account group



Step 4 In the displayed **Add Account** dialog box, select accounts and add them to the account group.

Step 5 Click **OK**. You can view the added members on the **Account Group** page.

----End

6.7 Account Group

6.7.1 Overview

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.

6.7.2 Creating an Account Group

This section describes how to create an account group.

Prerequisites

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

Procedure

Step 1 Log in to the CBH system.

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

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

Table 6-13 Creating an Account Group

Parameter	Description
Account Group	Specifies user-defined user group name, which must be unique in a CBH system.
Remarks	(Optional) Provides supplementary information about the account group.

Step 4 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

6.7.3 Deleting an Account Group

This topic describes how to delete an account group. Resource permissions granted to accounts in a deleted account group will become invalid.

Prerequisites

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

Deleting an Account Group

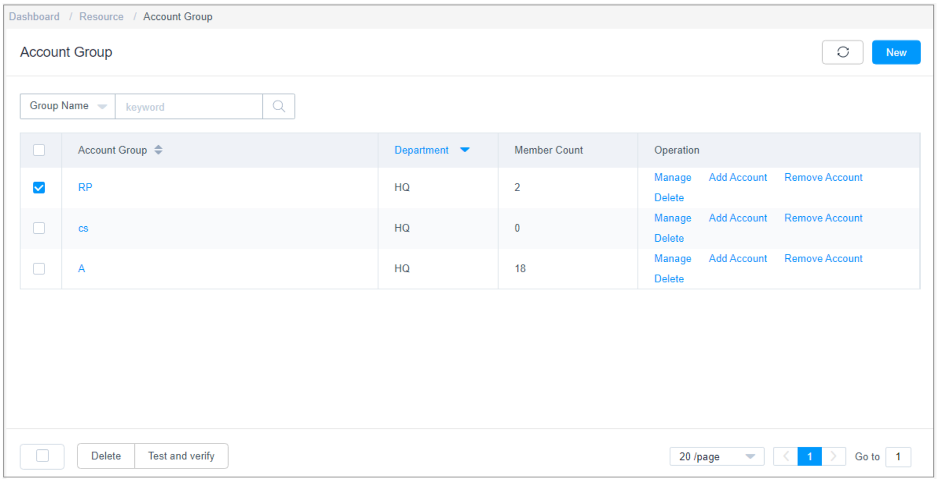
Step 1 Log in to the CBH system.

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

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

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

Figure 6-56 Deleting account groups



----End

6.7.4 Querying and Editing Account Group Information

CBH allows you to query and edit basic information and members of an account group.

Constraints

- As a CBH 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.

Procedure

Step 1 Log in to the CBH system.

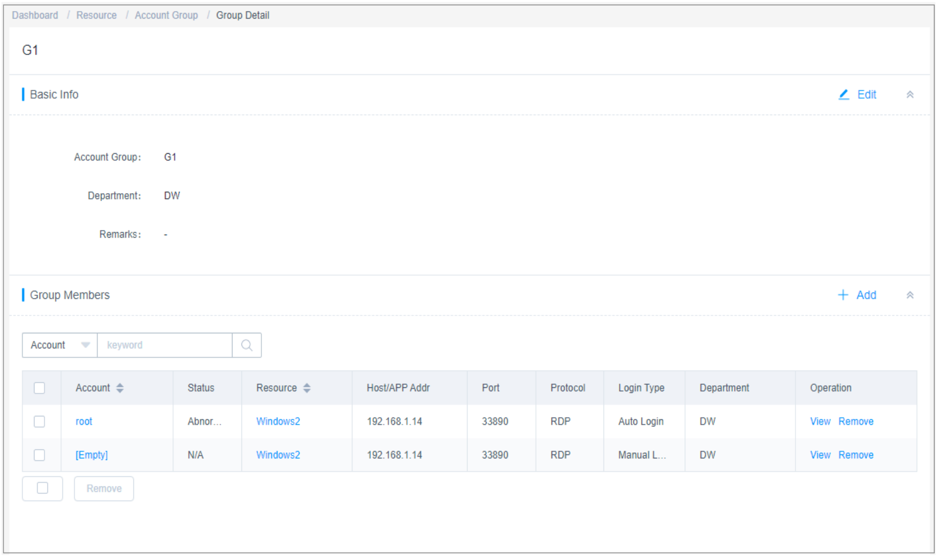
Step 2 Choose **Resource** > **Account Group** in the navigation pane.

Step 3 Query an account group.

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

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

Figure 6-57 Account group details



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

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

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

- Click **Add**. In the displayed dialog box, add or remove member of the account group.
- In the row of a specific member, click **Remove** in the **Operation** column to remove the account from the account group.

----End

6.8 Managing Resource Labels

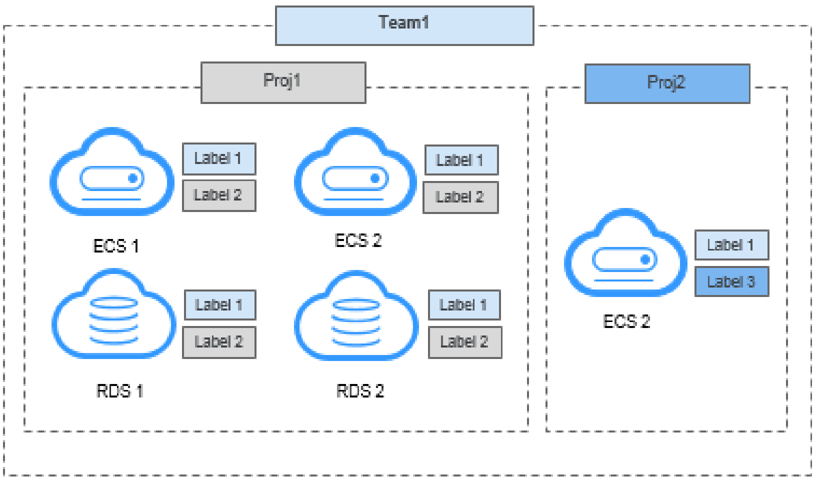
6.8.1 Overview

CBH labels are used to identify managed host and application resources in the CBH system and to 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.

Figure 6-58 shows how labels work. 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 6-58 Examples of labels



After you add labels to resources, you can search for resources by label and manage labels in the CBH system. 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 Operation.	Add or delete labels and search for resources by label.
Operation > App Operation	Add or delete labels and search for resources by label.

6.8.2 Creating a Resource Label

As a CBH system user, you can define your own resource labels for your exclusive use.

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 CBH system. 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

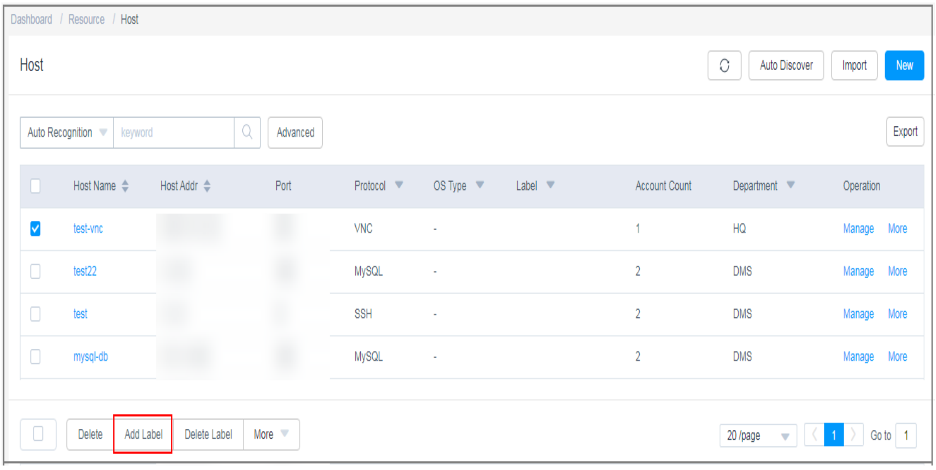
You have the obtained the operation permissions for the **Host**, **Application Publish**, **Host Operation**, and **App Operation** modules.

Adding a Label

Step 1 Log in to the CBH system.

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

Figure 6-59 Host list



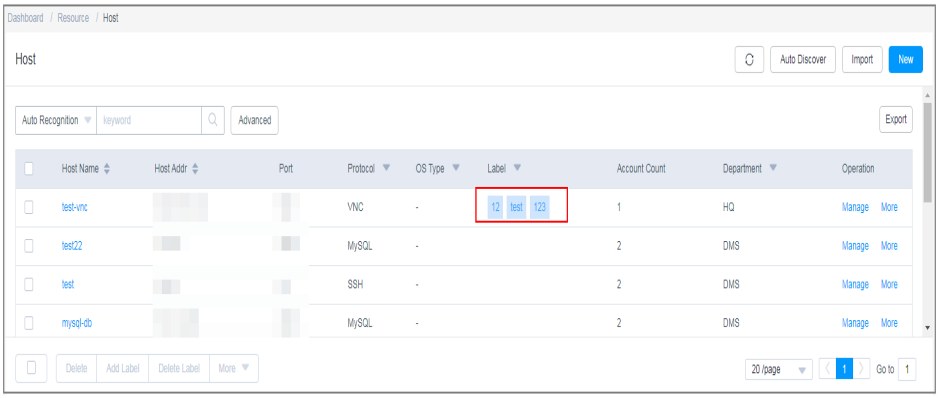
Step 3 Select the host you want to add a label and click **Add Label**. The **Add Label** dialog box is displayed.

Figure 6-60 Add Label

Step 4 Type label information in the **Label** field and press **Enter** to create a customized label, or select an existing label from the **Label** drop-down list.

Step 5 Click **OK**. You can go to the **Host** page in the **Resource** module or the **Host Operation** page in the **Operation** module to view the new label of the managed host.

Figure 6-61 Host page after labels are added



Step 6 Search for resources by label on. Go to the host or application list page in the **Resource** module, select a label from the drop-down list in the **Label** column to search for resources.

----End

6.8.3 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 Operation**, and **App Operation** modules.

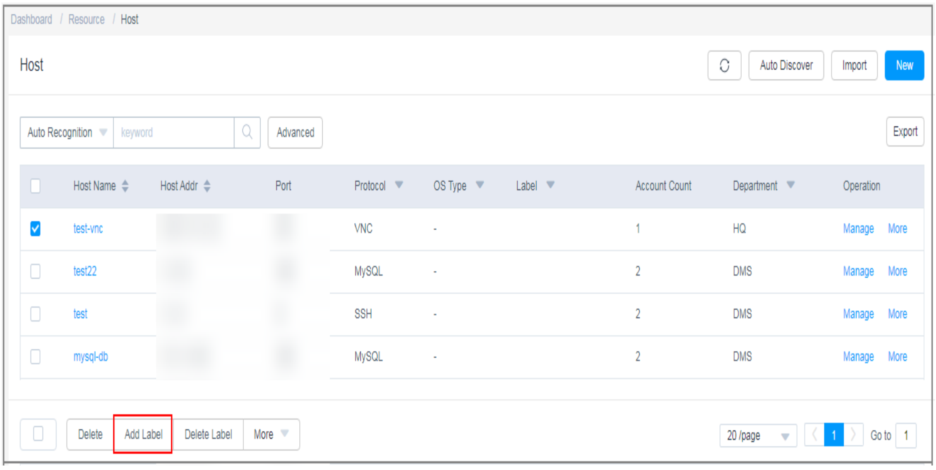
Procedure

You can delete one or more labels from a managed resource. The following describes how to delete all labels from a managed host.

Step 1 Log in to the CBH system.

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

Figure 6-62 Host list



Step 3 Select a 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 Operation** 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

6.9 Customizing OS Types

CBH manages resource system types and allows you to define custom operating system (OS) types.

CBH 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

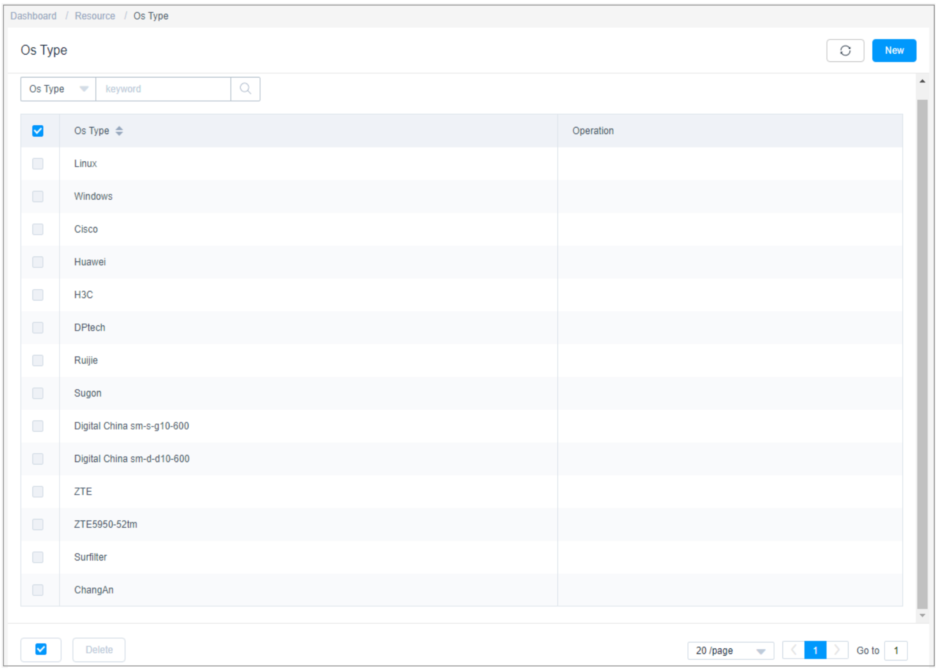
- Only system administrator **admin** can modify the OS type configuration.
- The default OS type cannot be deleted or modified. Only the customized OS types can be deleted or modified.

Customizing OS Types

Step 1 Log in to the CBH system.

Step 2 Choose **Resource** > **OS Type** to switch to the OS type list page.

Figure 6-63 OS types



Step 3 Click **New** to switch to the **New OS Type** dialog box and configure parameters.

Figure 6-64 New OS Type

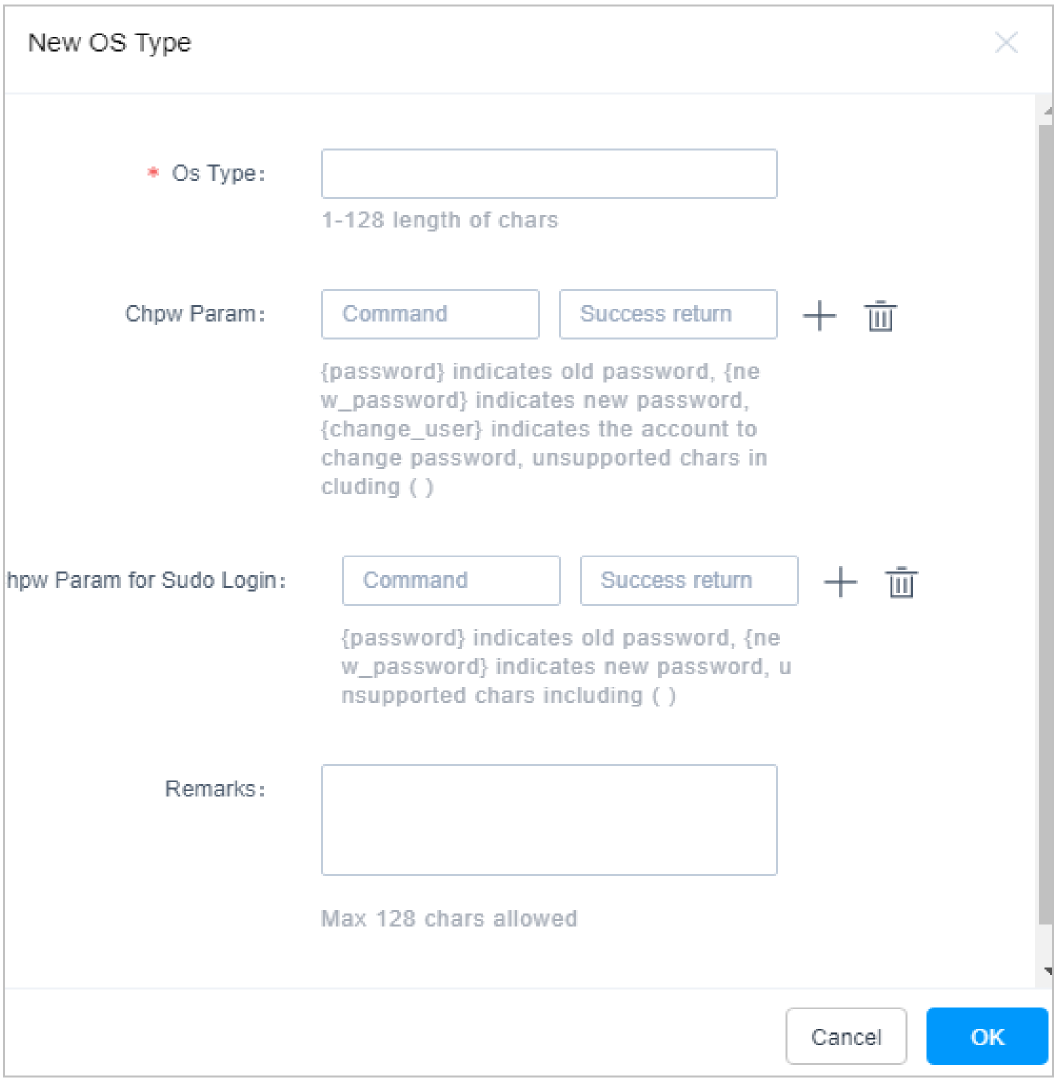


Table 6-15 Parameters for creating an OS type

Parameter	Description
OS Type	Specifies the name of the custom OS type.
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.

Parameter	Description
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 the CBH system.

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 ACL Rules

7.1.1 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:

- 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, 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.
  - Restrict the users of certain source IP addresses to access managed 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.
  - Enable or disable watermarks on the web operation background. The watermark content is the login name of the current system user.

Constraints

To grant the file upload/download permission, enable **File Transmission** and **File Manage**.

Prerequisites

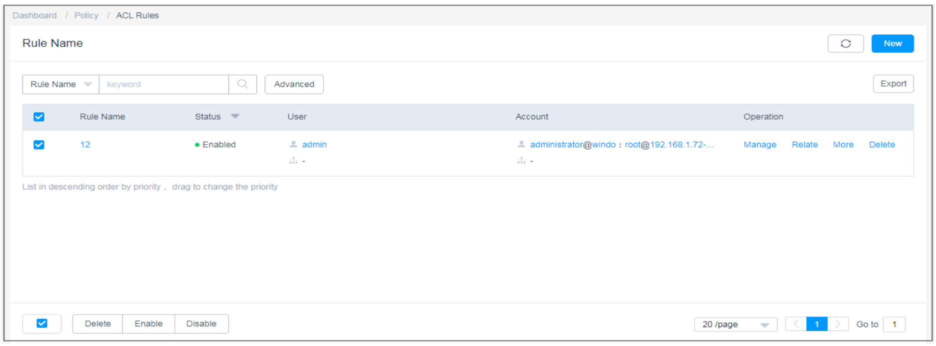
You have the operation permissions for the **ACL Rules** module.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **Policy** > **ACL Rules** to enter the ACL rule list page.

Figure 7-1 ACL Rules



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.

Figure 7-2 Creating an ACL Rule

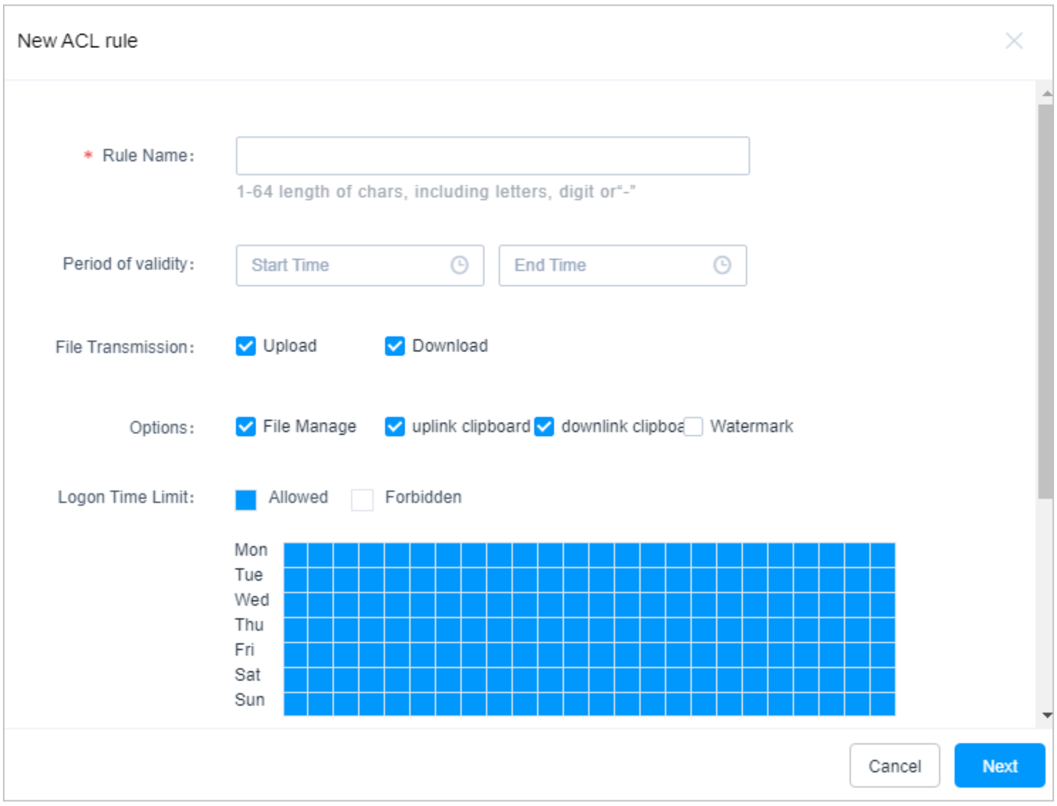


Table 7-1 Basic information about an ACL rule

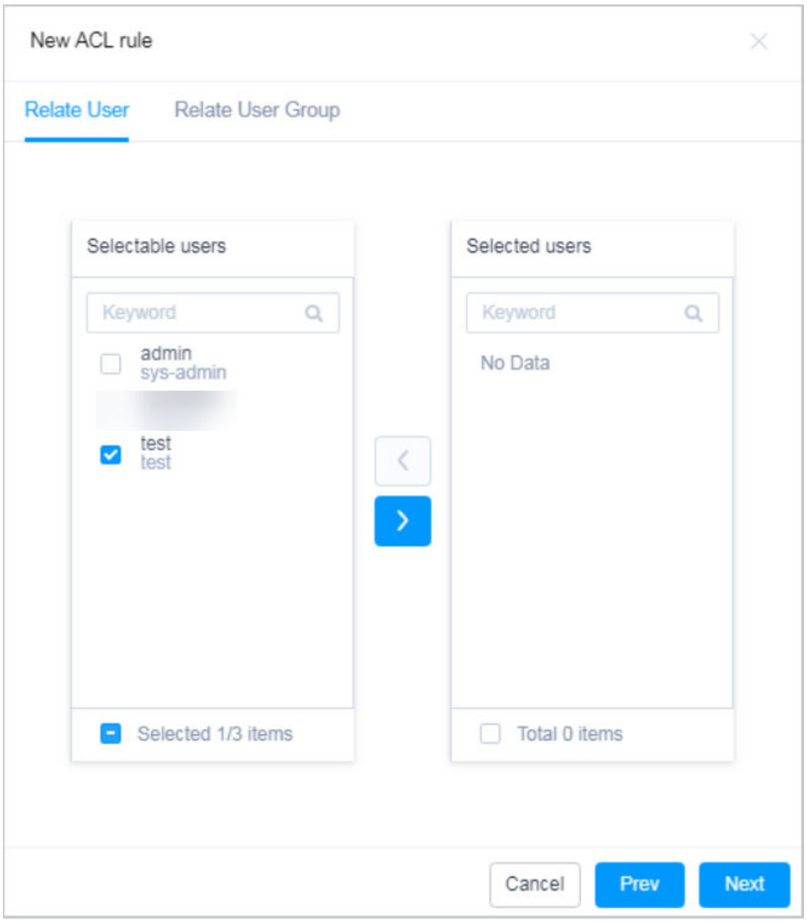
Parameter	Description
Rule Name	Name of a user-defined ACL rule. The rule name must be unique in the CBH system.
Period of validity	Effective time and expiration time of an ACL rule
File Transmission	Permissions to upload and download files during O&M. ● If **Upload** and/or **Download** are selected, files can be uploaded and/or downloaded. ● If **Upload** and **Download** are deselected, files cannot be uploaded or downloaded.
Options	Permissions to manage files or file folders, use clipboards on hosts using the RDP protocol, and display watermarks during O&M. **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.

Parameter	Description
Logon Time Limit	Time period during which managed resources can or cannot be accessed.
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.

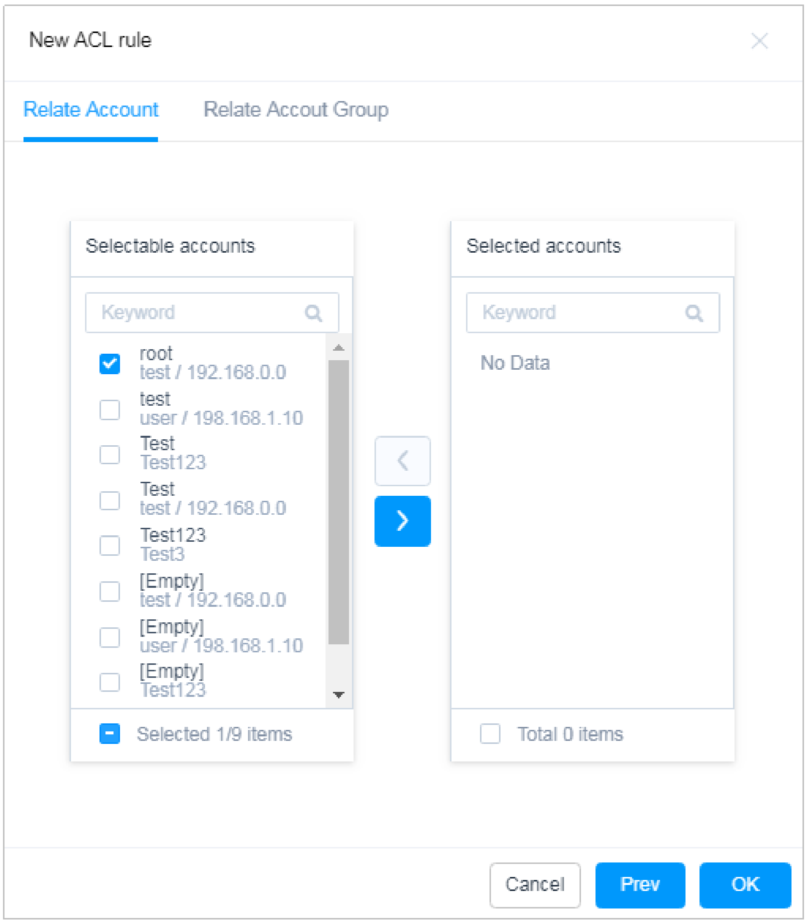
Figure 7-3 Relate User



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.

Figure 7-4 Relate Accounts



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 Operation** and **App Operation** module.

NOTE

Users in the **Relate User** and **Relate User Group** must have been assigned a role that has the permissions for the **Host Operation** or **App Operation** module. Otherwise, the users cannot view the resource operation modules or access managed resources for O&M.

----End

Follow-up Operations

CBH gives you the ability to manage all ACL rules on the rule list page, including managing related users or resources, deleting, enabling, or disabling one or more ACL rules, and sorting 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 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.
- To manage ACL rules offline, click **Export** to export the details about all ACL rules in CSV format.

7.1.2 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.

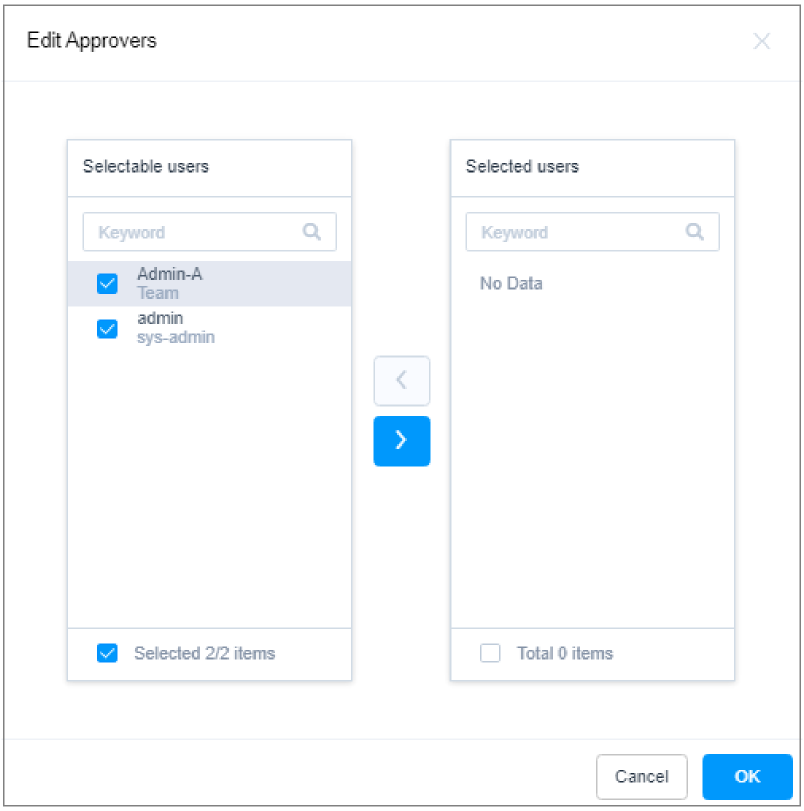
Procedure

Step 1 Log in to the CBH system.

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, choose **More** > **Approver** in the **Operation** column. The **Edit Approvers** dialog box is displayed.

Figure 7-5 Setting two-person authorization



Step 4 Select one or more department administrators and set them as approvers of two-person authorization.

Step 5 Click **OK**.

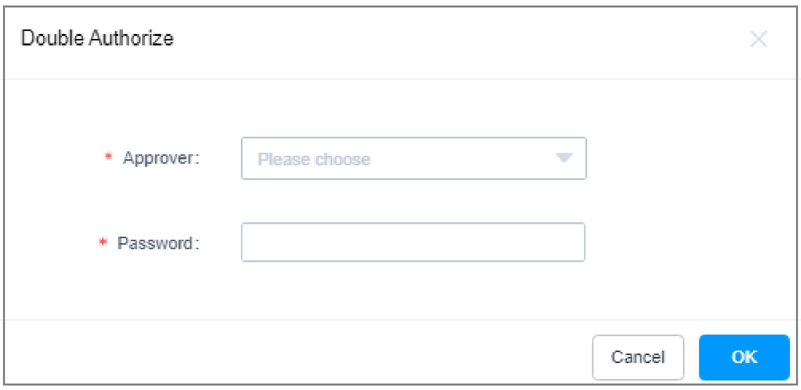
----End

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.

Figure 7-6 Two-person authorization



7.1.3 Querying and Editing an ACL Rule

CBH allows you to 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 the CBH system.

Step 2 Choose **Policy** > **ACL Rules** to enter the ACL rule list page.

Step 3 Query ACL rules.

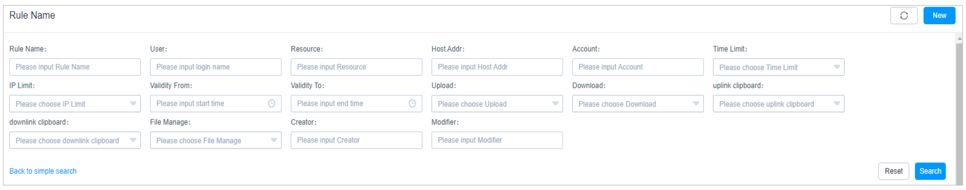
- Quick search

  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

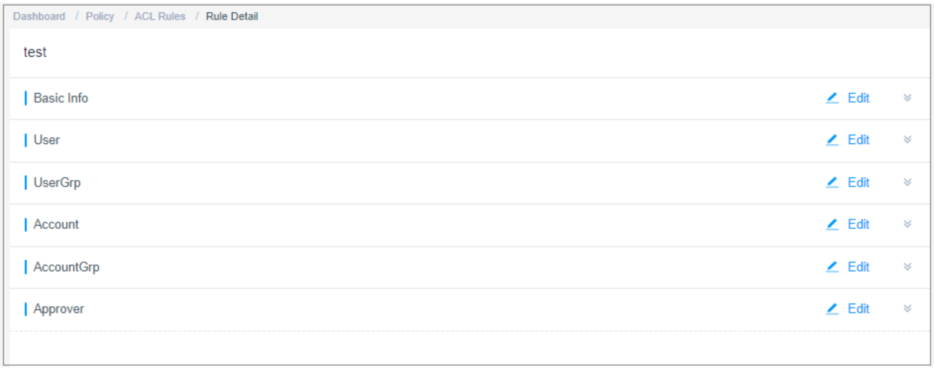
  Enter keywords in the corresponding attribute search boxes to search for database rules in exact mode.

Figure 7-7 Advanced search



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.

Figure 7-8 Viewing rule details

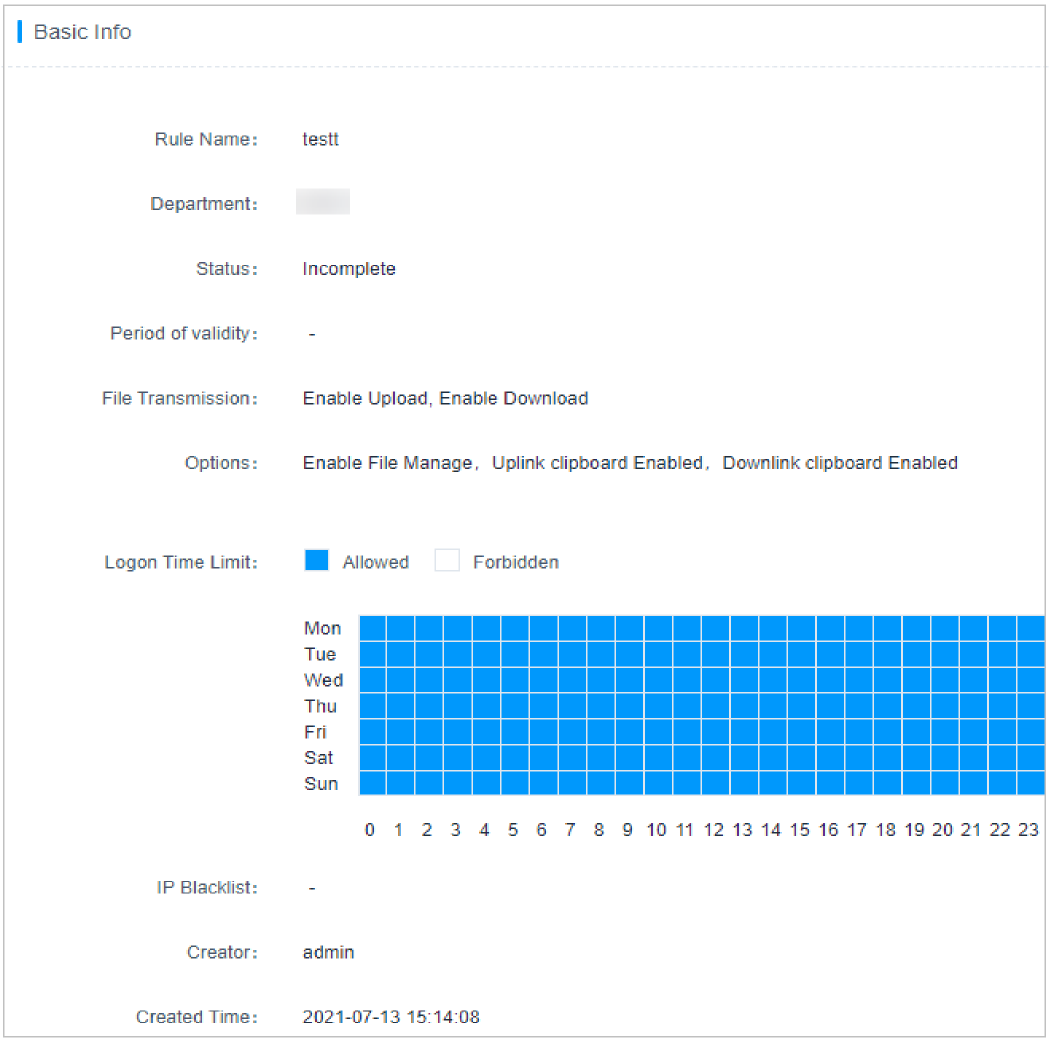


Step 5 View and edit basic information.

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**, **File Manage**, **Uplink clipboard**, **Downlink clipboard**, **Logon Time Limit**, and **IP Limit**.

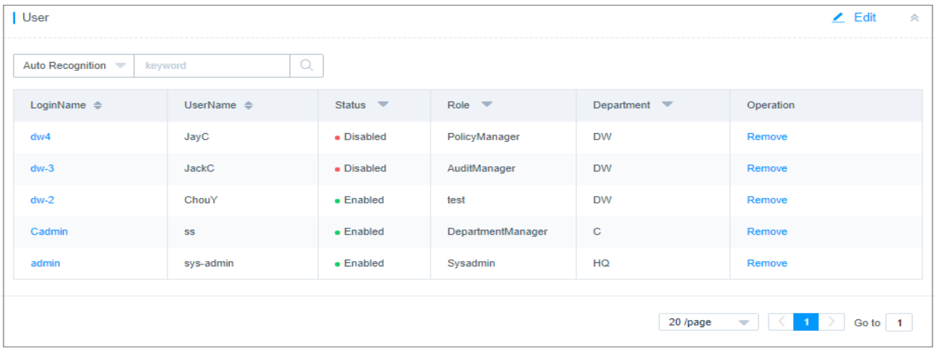
Figure 7-9 Viewing the basic information



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.

Figure 7-10 Viewing related users


User Edit

Auto Recognition keyword

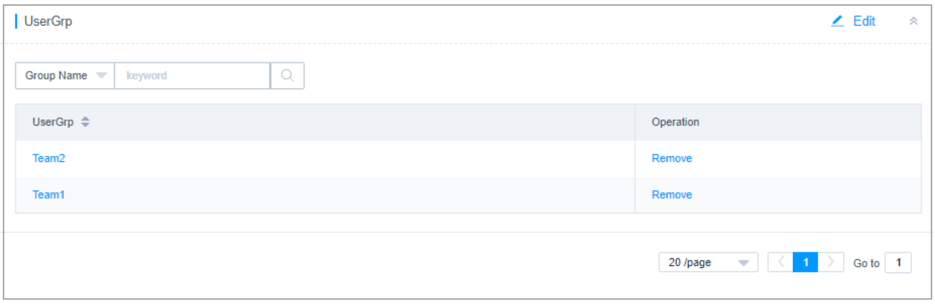
LoginName	UserName	Status	Role	Department	Operation
dw4	JayC	Disabled	PolicyManager	DW	Remove
dw-3	JackC	Disabled	AuditManager	DW	Remove
dw-2	ChouY	Enabled	test	DW	Remove
Cadmin	ss	Enabled	DepartmentManager	C	Remove
admin	sys-admin	Enabled	Sysadmin	HQ	Remove

20 /page 1 Go to 1

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.

Figure 7-11 Viewing related user groups


UserGrp Edit

Group Name keyword

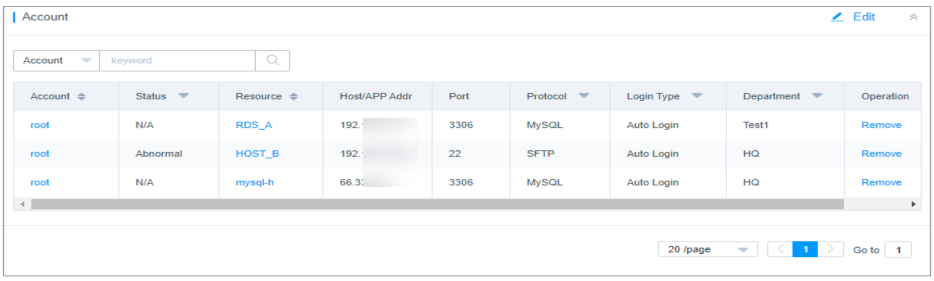
UserGrp	Operation
Team2	Remove
Team1	Remove

20 /page 1 Go to 1

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.

Figure 7-12 Viewing related accounts


Account Edit

Account keyword

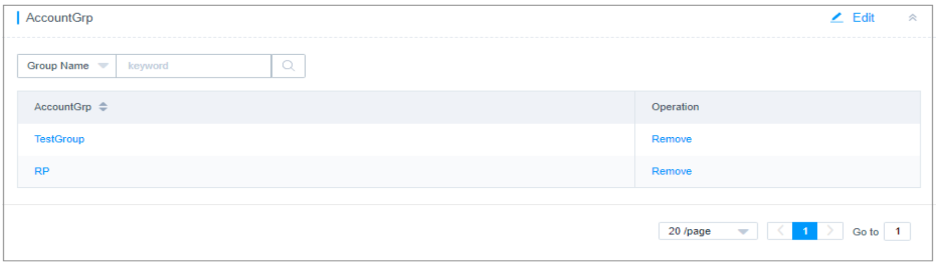
Account	Status	Resource	Host/APP Addr	Port	Protocol	Login Type	Department	Operation
root	N/A	RDS_A	192.	3306	MySQL	Auto Login	Test1	Remove
root	Abnormal	HOST_B	192.	22	SFTP	Auto Login	HQ	Remove
root	N/A	mysql-h	66.3	3306	MySQL	Auto Login	HQ	Remove

20 /page 1 Go to 1

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.

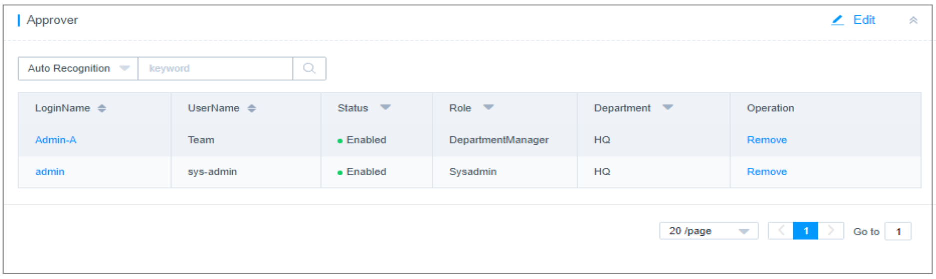
Figure 7-13 Viewing related account groups



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.

Figure 7-14 Viewing approvers of two-person authorization



----End

7.2 Command Rules

7.2.1 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, CBH can record O&M session operations, trigger dynamic authorization, and disconnect connection to an O&M session. The working principles are that CBH uses the guacd proxy to audit and filter the commands executed during O&M 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

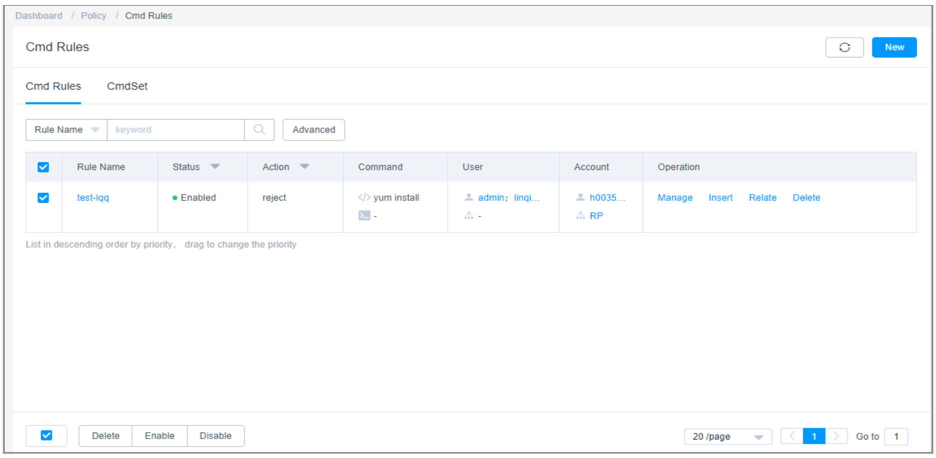
You have obtained the permissions to manage the **Cmd Rules** module.

Creating a Command Rule

Step 1 Log in to the CBH system.

Step 2 Choose **Policy** > **Cmd Rules** > **Cmd Rules**.

Figure 7-15 Cmd Rules



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.

Figure 7-16 New Command Rule

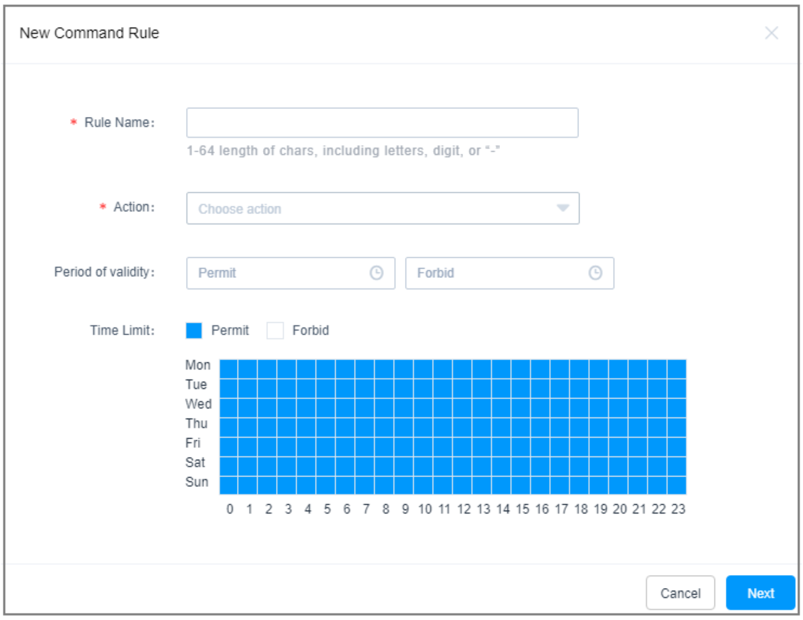


Table 7-2 Basic information parameters

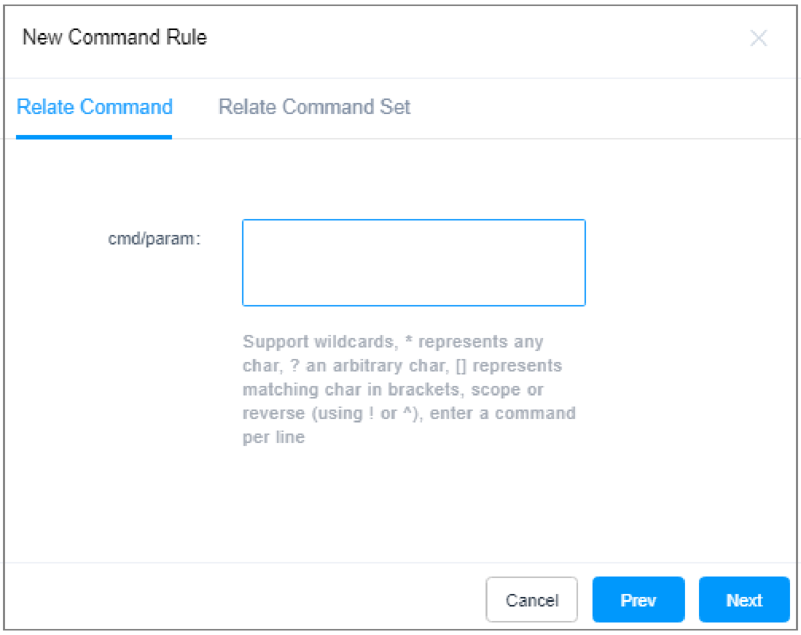
Parameter	Description
Rule Name	Name of a command rule. The rule name must be unique in the CBH system.
Action	Action executed by the command rule. The options are **Disconnect**, **Reject command**, **Dynamic approval**, and **Permit**. ● **Disconnect**: When a session runs the command to bring the 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.

Parameter	Description
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**.

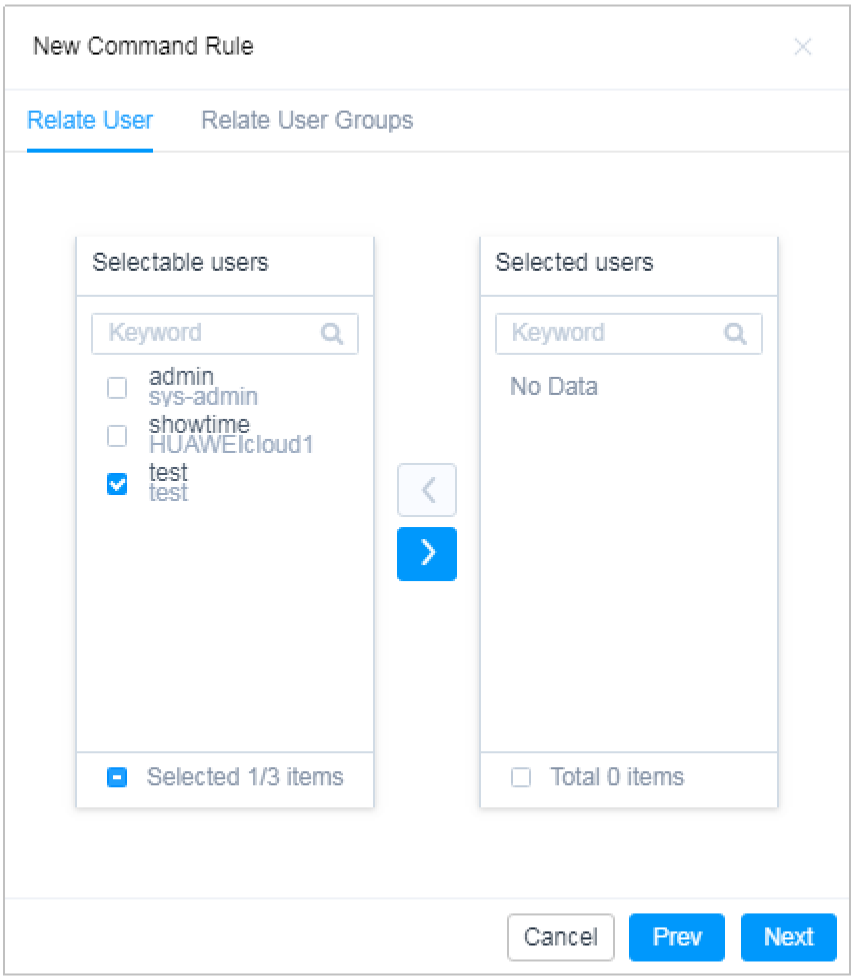
Figure 7-17 Relate Command



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.

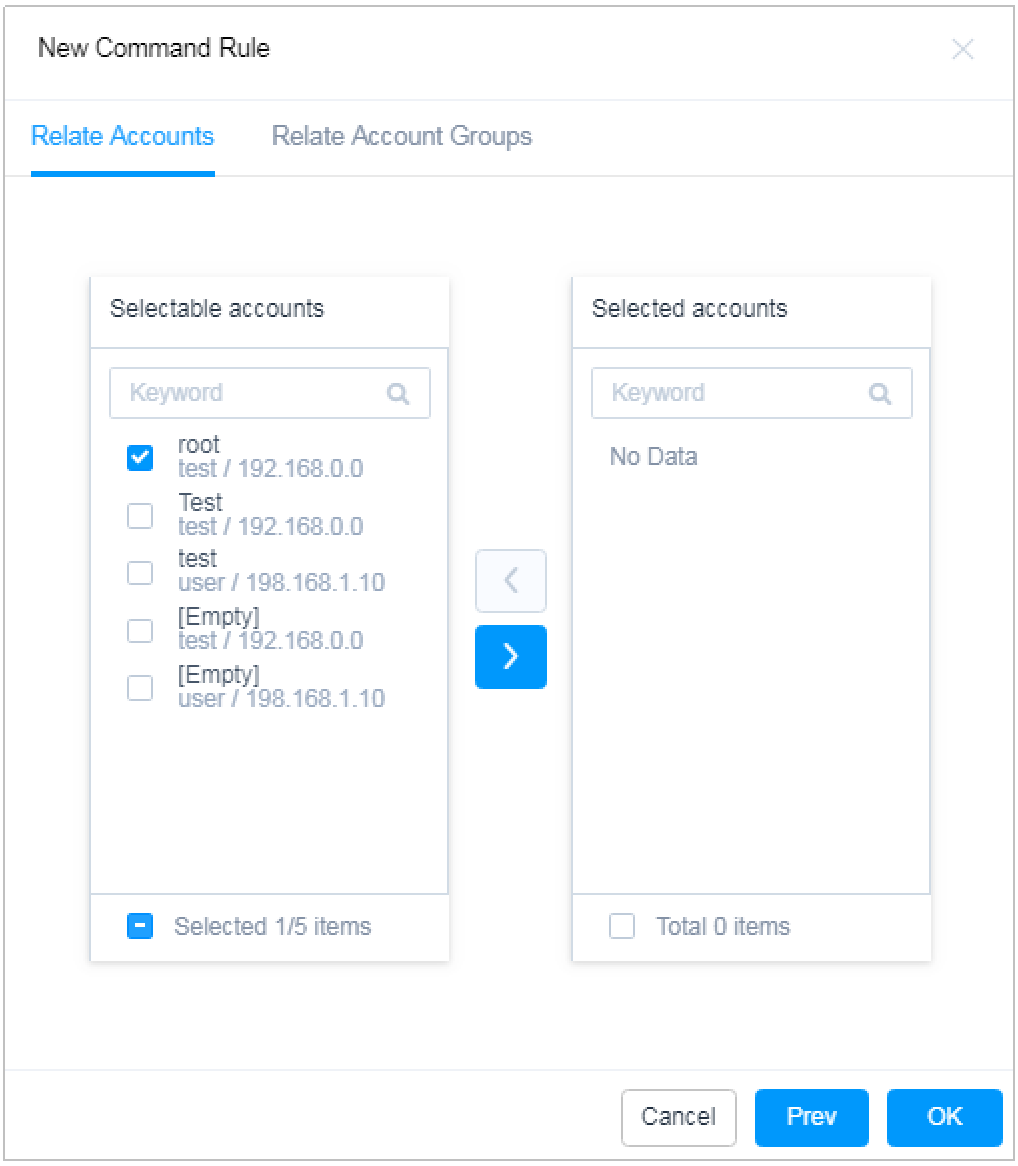
Figure 7-18 Relate User



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.

Figure 7-19 Relate Accounts



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

CBH gives you the ability to 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.

7.2.2 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 the CBH system.

Step 2 Choose **Policy** > **Cmd Rules** > **Cmd Rules**.

Step 3 Query command rules.

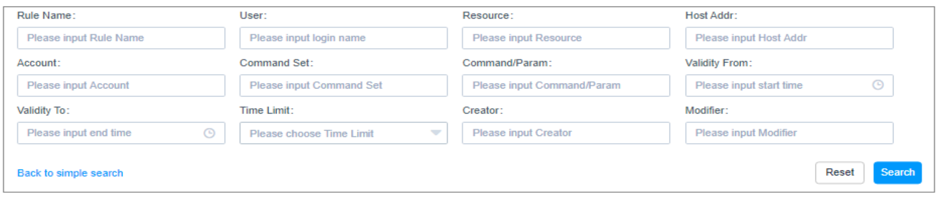
- Quick search

  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

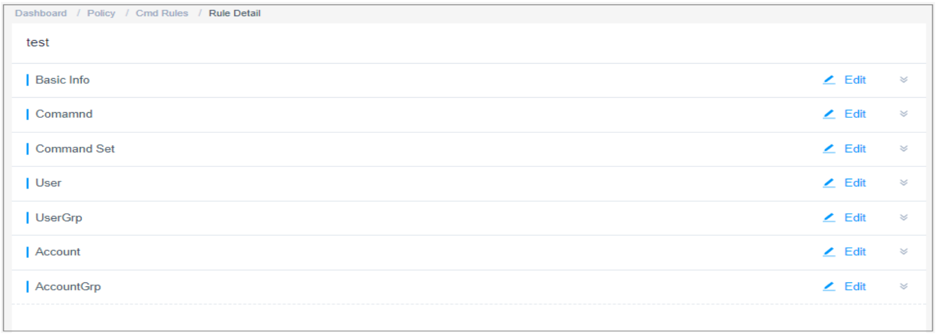
  Enter keywords in the corresponding attribute search boxes to search for database rules in exact mode.

  Figure 7-20 Advanced search



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.

Figure 7-21 Viewing rule details

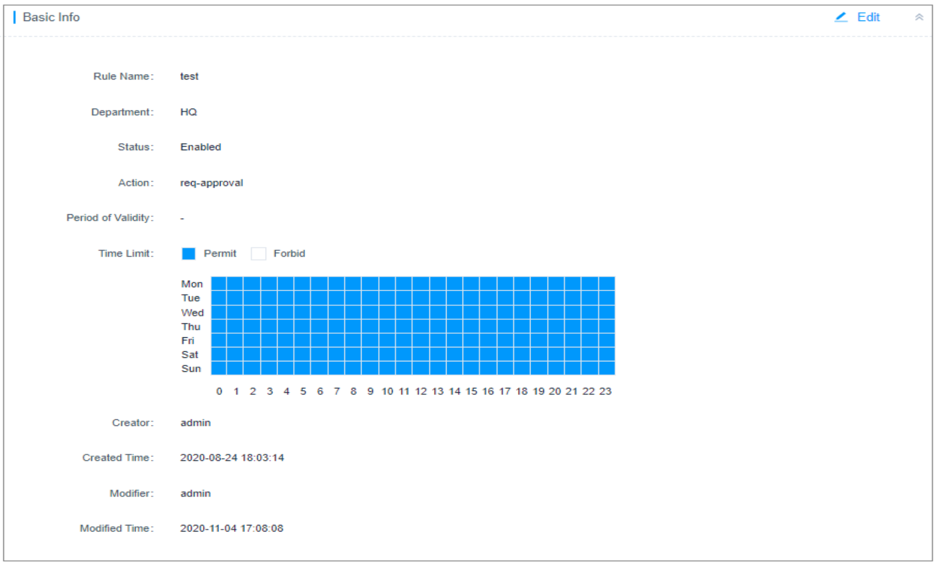


Step 5 View and edit basic information.

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**.

Figure 7-22 Viewing the basic information



Step 6 View and edit commands related to the rule.

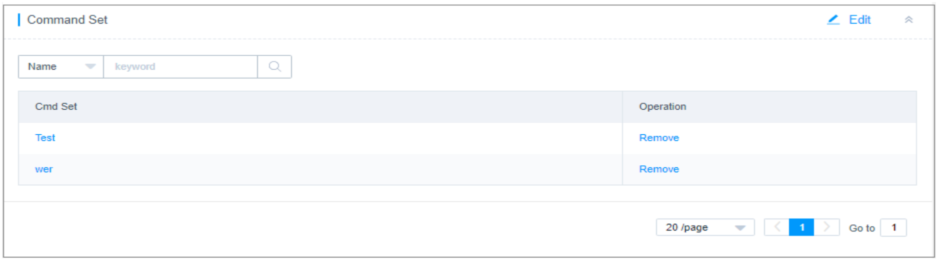
- To edit related commands or parameters, click **Edit** in the **Command** area and complete modifications in the displayed dialog box.
- To only delete a related command, click **Remove** in the row of the related command.

Figure 7-23 Viewing related commands

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.

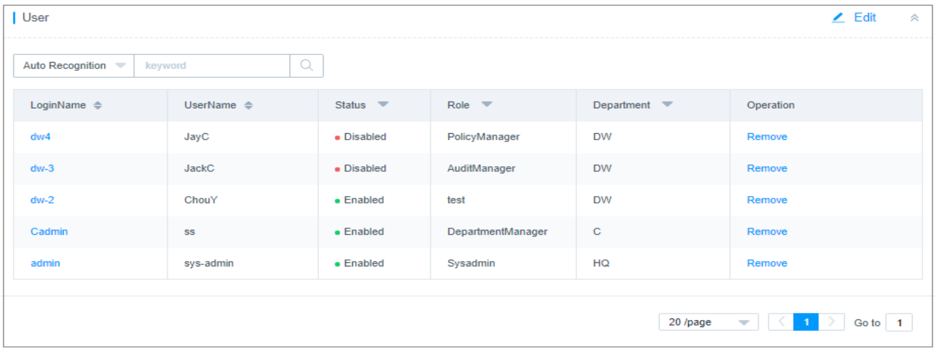
Figure 7-24 Viewing related command sets



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.

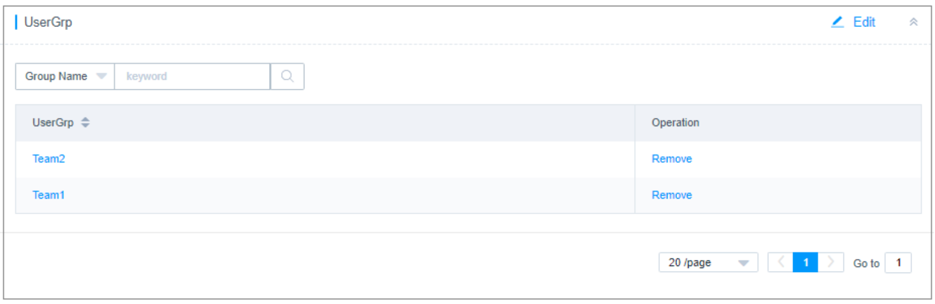
Figure 7-25 Viewing related users



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.

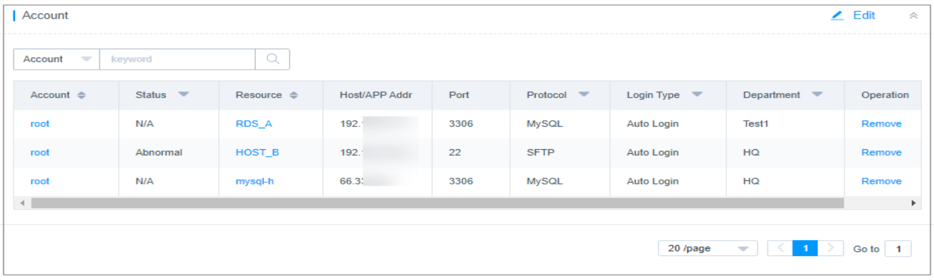
Figure 7-26 Viewing related user groups



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.

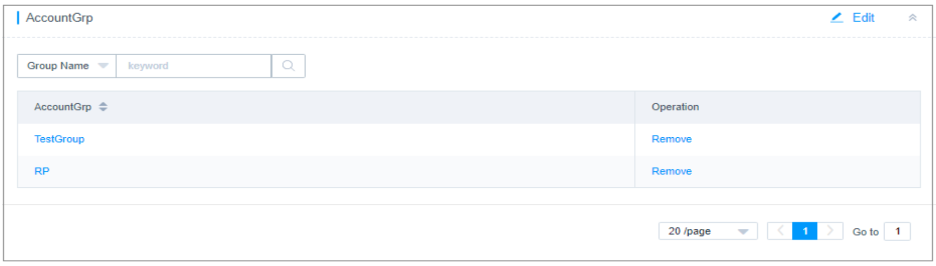
Figure 7-27 Viewing related accounts



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.

Figure 7-28 Viewing related account groups



----End

7.2.3 Managing Command Sets

To relieve you from complicated and repetitive workloads on adding a large number of commands to command rules, CBH provides command sets for you, which includes common commands and parameters used for Linux hosts and network devices.

This topic walks you through how to create, view, modify, and delete a command set.

Prerequisites

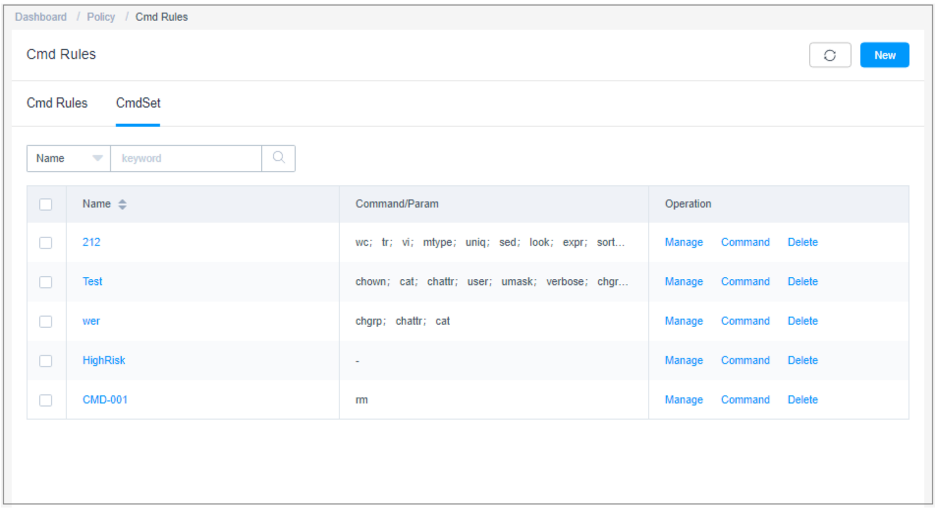
You have obtained the permissions to manage the **Cmd Rules** module.

Creating a Command Set

Step 1 Log in to the CBH system.

Step 2 Choose **Policy** > **Cmd Rules** > **CmdSet** to go to the command set list page.

Figure 7-29 Command set list

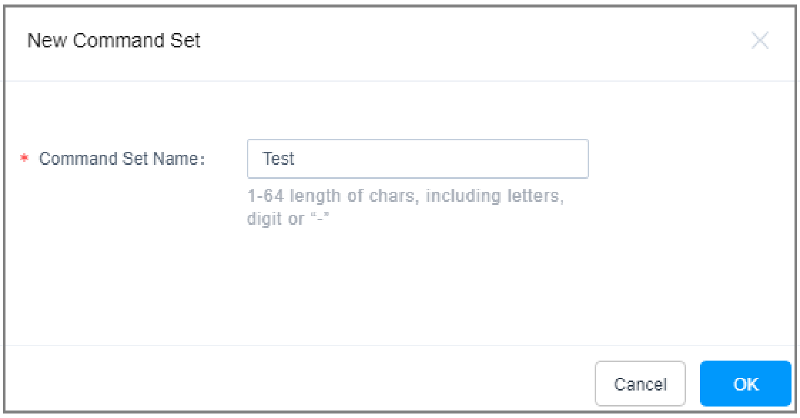


Step 3 Create a command set.

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 the CBH system.
3. Click **OK**. You can then view the new command set on the **CmdSet** tab.

Figure 7-30 Creating a Command Set



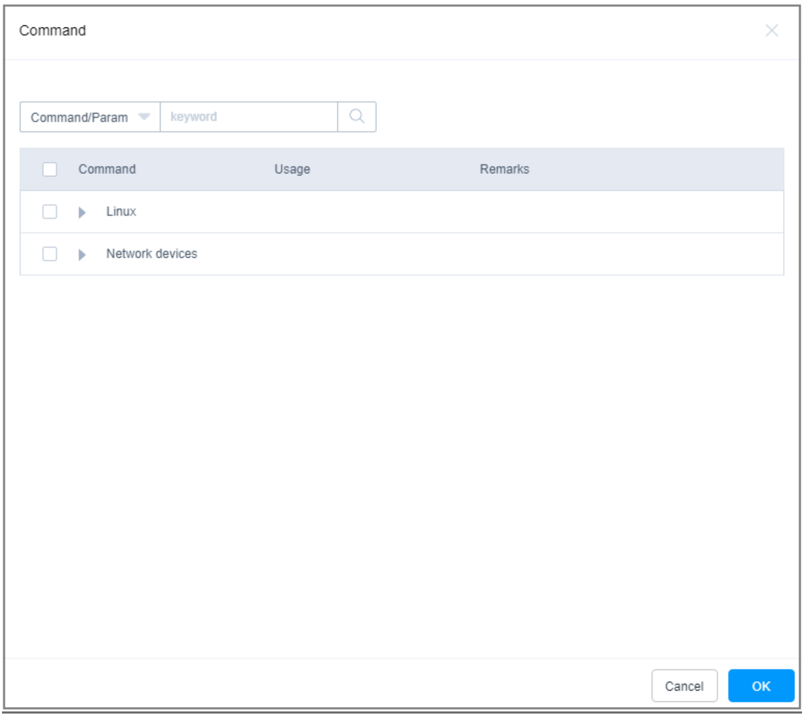
Step 4 Add commands to the command set.

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.

   Currently, common commands for **Linux** and **Network devices** are preset in the CBH system.

3. Click **OK**.

Figure 7-31 Adding commands



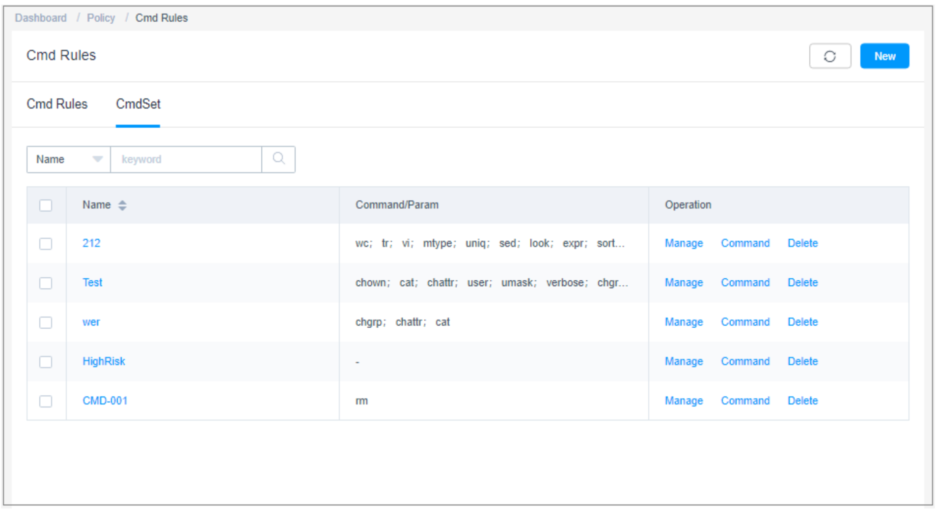
----End

Querying and Editing a Command Set

Step 1 Log in to the CBH system.

Step 2 Choose **Policy** > **Cmd Rules** > **CmdSet** to go to the command set list page.

Figure 7-32 Command set list

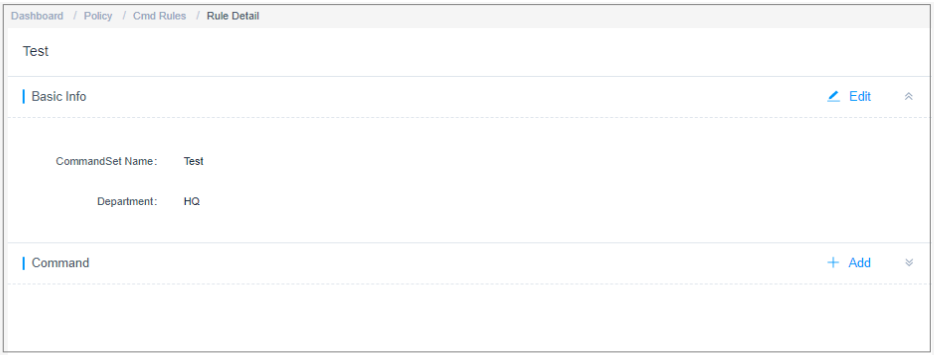


Step 3 Query a command set.

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.

Figure 7-33 Command set details



Step 5 View and edit basic information.

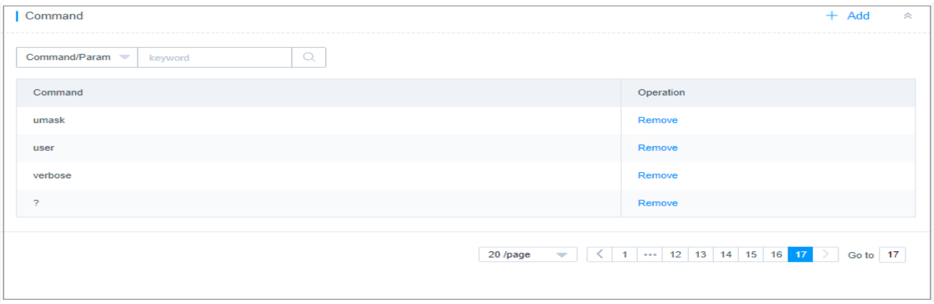
In the **Basic Info** area, click **Edit**. In the displayed dialog box, edit the basic information.

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**.

Figure 7-34 Viewing command and parameters



----End

Deleting a Command Set

Step 1 Log in to the CBH system.

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.

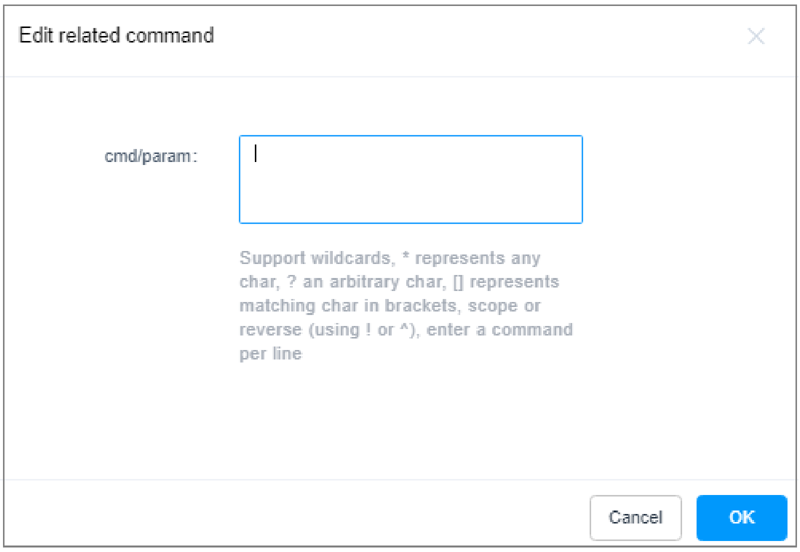
Step 4 To delete multiple command sets at a time, select the ones you want to delete and click **Delete** at the bottom of the list to delete all selected command sets together.

----End

7.2.4 Defining Custom Related Commands

After a custom command is related to a command rule, the CBH system determines whether to execute the command based on the command rule.

Figure 7-35 Defining Custom Related Commands



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.

7.3 Database Rules

7.3.1 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 the CBH professional editions.
- Database rules apply only to MySQL and Oracle databases for fine-grained permission control.

Prerequisites

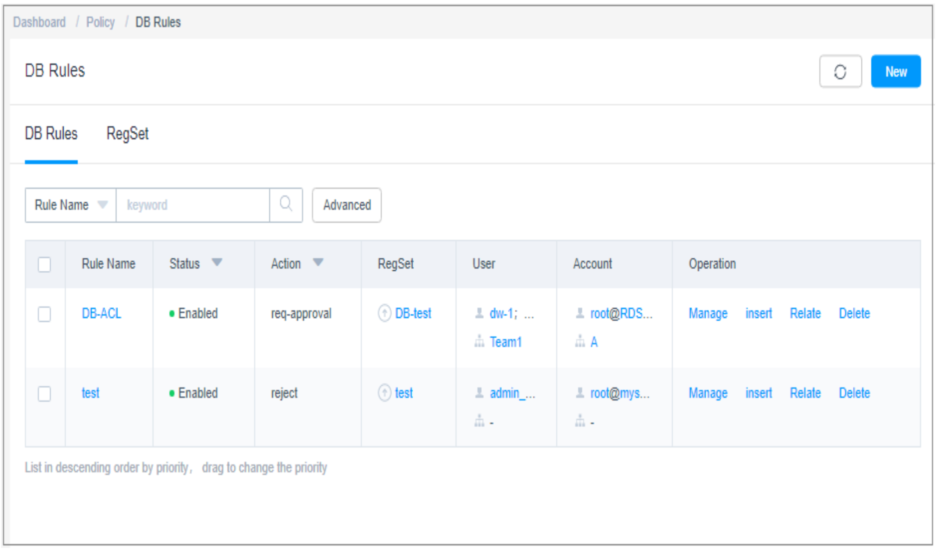
You have the operation permissions for the **DB Rules** module.

Creating a Database Rule

Step 1 Log in to the CBH system.

Step 2 Choose **Policy** > **DB Rules** > **DB Rules**.

Figure 7-36 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.

Figure 7-37 New Command Rule

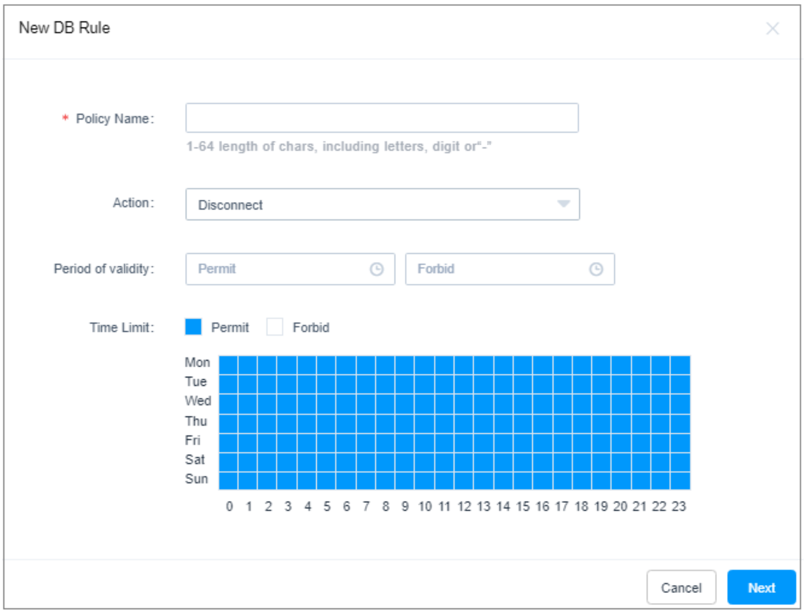


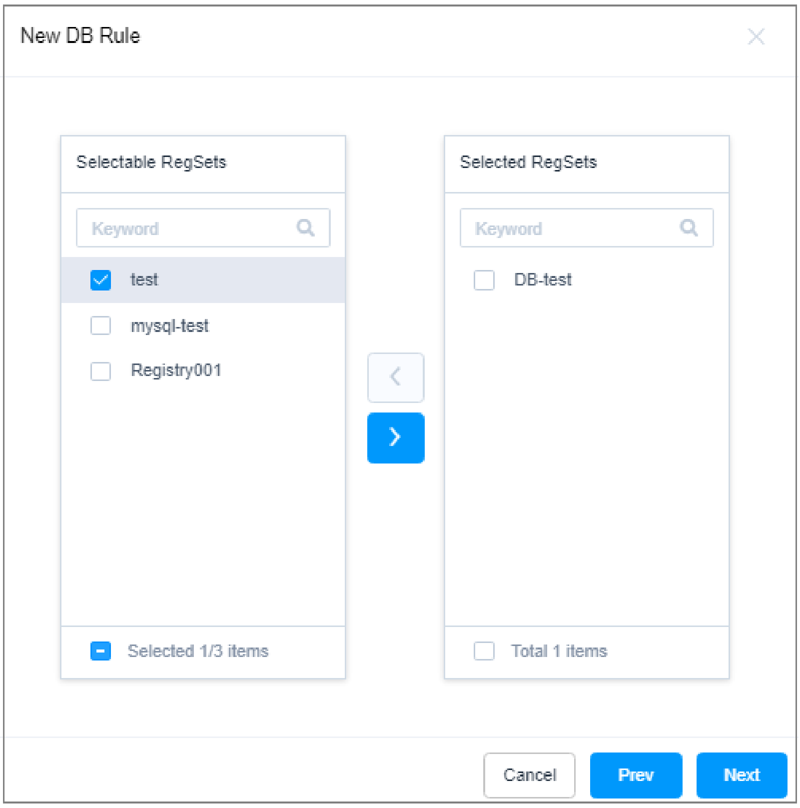
Table 7-3 Basic information parameters

Parameter	Description
Rule Name	Name of the database rule. The rule name must be unique in the CBH system.
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**.

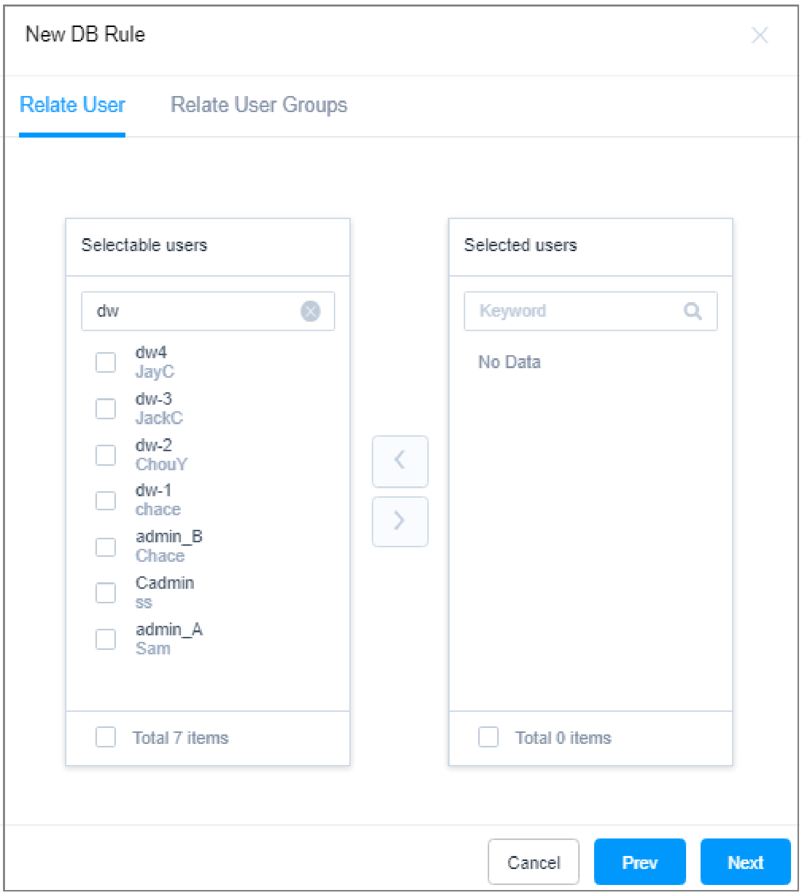
Figure 7-38 Selecting a rule set



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.

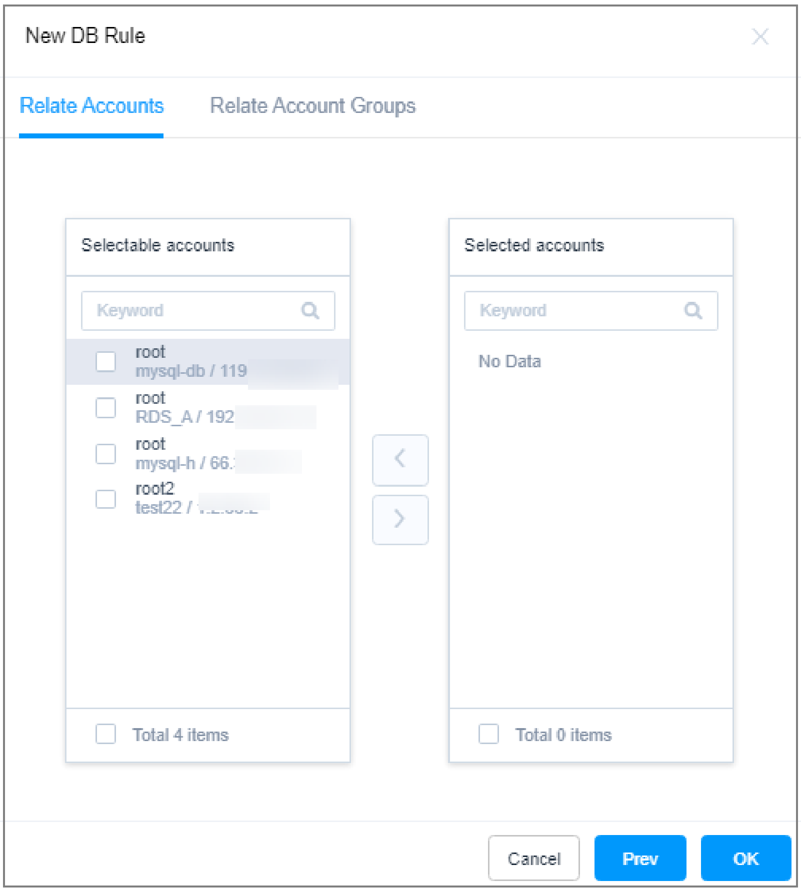
Figure 7-39 Relate User



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.

Figure 7-40 Relate Accounts



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

CBH gives you the ability to 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.

7.3.2 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 the CBH system.

Step 2 Choose **Policy** > **DB Rules** to go to the **DB Rules** page.

Step 3 Query database rules.

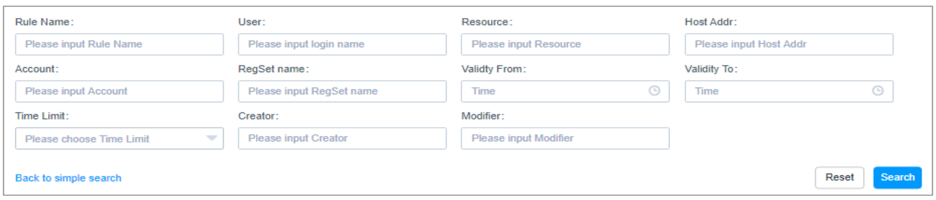
- Quick search

  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

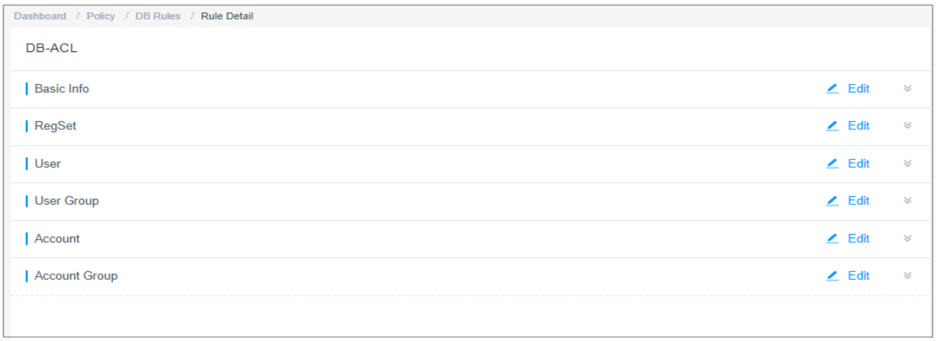
  Enter keywords in the corresponding attribute search boxes to search for database rules in exact mode.

  Figure 7-41 Advanced search

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.

Figure 7-42 Viewing rule details



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**.

Figure 7-43 Viewing the basic information

Step 6 View and edit regulation sets related to the rule.

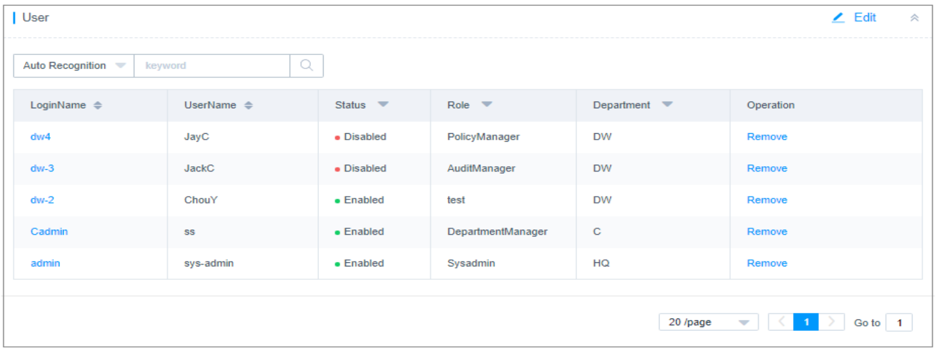
- To relate a regulation set to the rule or remove a related regulation set, click **Edit** in the **RegSet** area and complete modifications in the displayed dialog box.
- To only delete a related regulation set, click **Remove** in the row of the related regulation set.

Figure 7-44 Viewing related regulation sets

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.

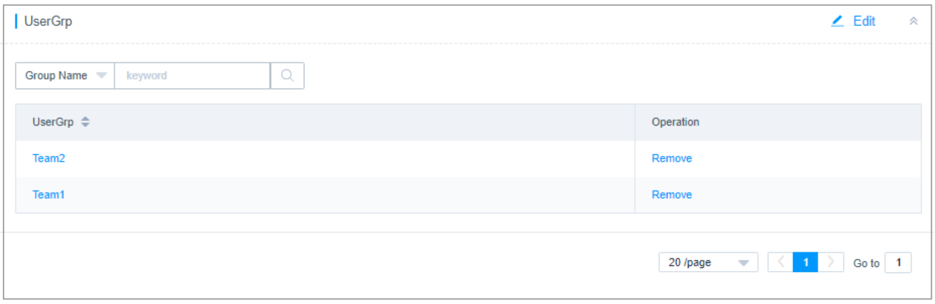
Figure 7-45 Viewing related users



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.

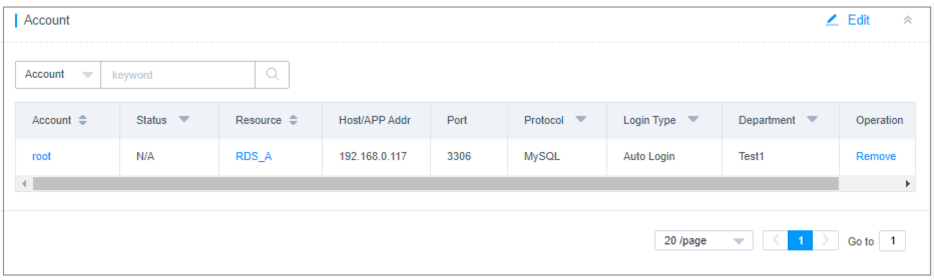
Figure 7-46 Viewing related user groups



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.

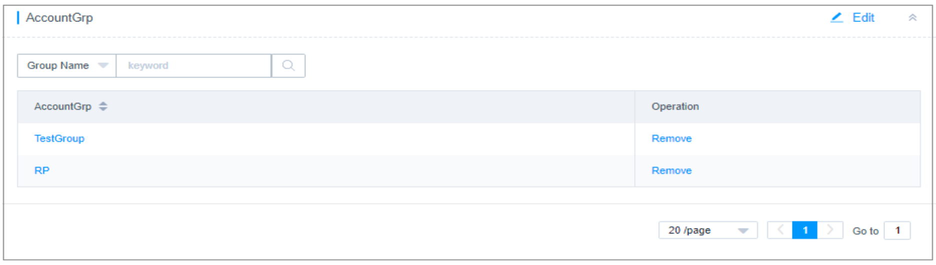
Figure 7-47 Viewing related accounts



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.

Figure 7-48 Viewing related account groups



----End

7.3.3 Managing Regulation Sets

CBH allows you to create regulation sets for quickly adding a large number of database rules, relieving you from complicated and repetitive workloads.

CBH has 29 common database operation commands preset, 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**, **DROPPROCEDURE**, **CREATETABLE**, **DROPTABLE**, **CALL**, and **ACCESS**.

This topic walks you through how to create, view, modify, and delete a regulation set.

Prerequisites

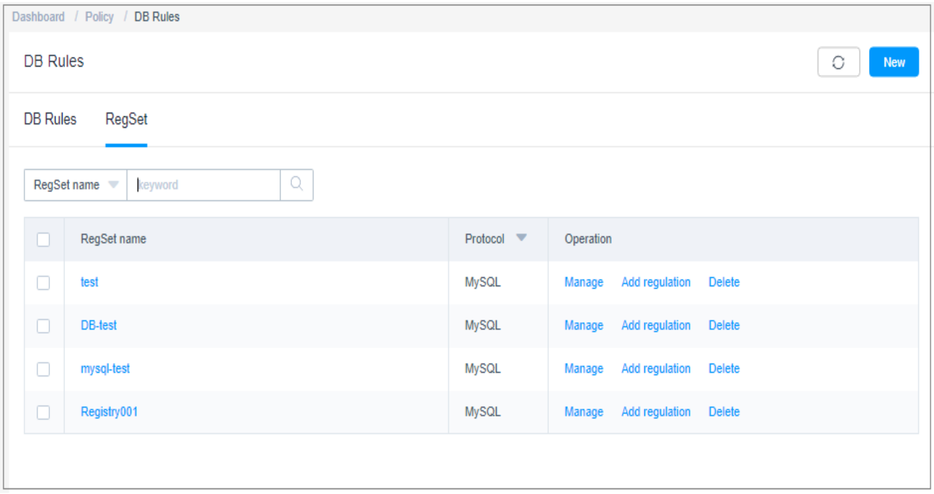
You have the operation permissions for the **DB Rules** module.

Creating a Regulation Set

Step 1 Log in to the CBH system.

Step 2 Choose **Policy** > **Database Rules** > **RegSet** to go to the DB rule list.

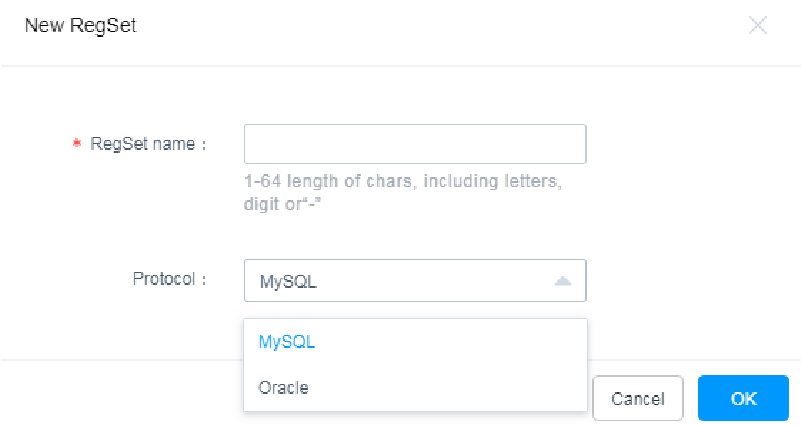
Figure 7-49 RegSet list



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 the CBH system.
   - Currently, only MySQL and Oracle are supported. The protocol type cannot be changed after being selected.
3. Click **OK**. You can then view new regulation set on the list page.

Figure 7-50 Creating a Regulation Set



Step 4 Add database rules.

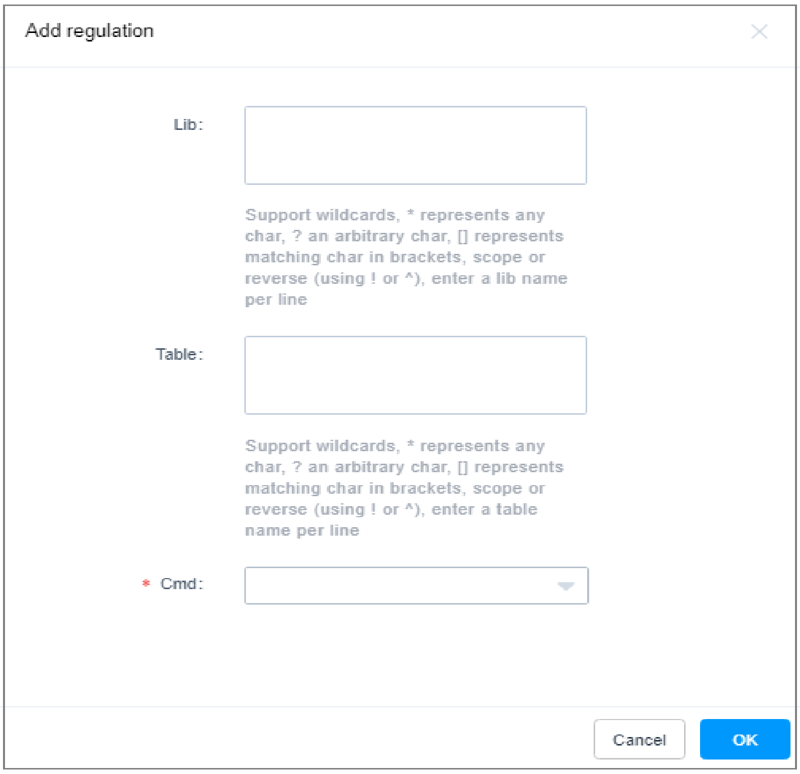
1. In the row of the command set you want to add rules, click **Add regulation** in the **Operation** column.
2. Add libraries, tables, and commands for the regulation set.

Table 7-4 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**.

Figure 7-51 Add regulation



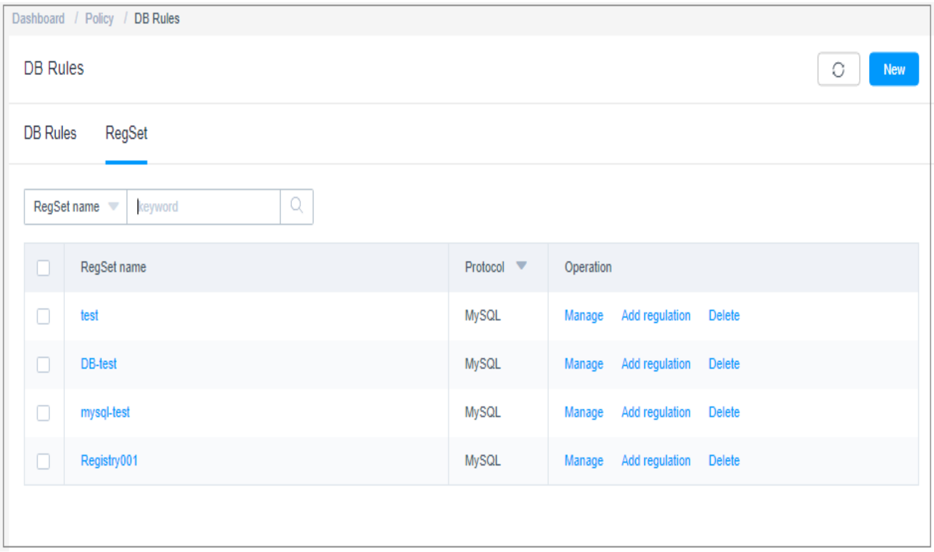
----End

Querying and Editing a Regulation Set

Step 1 Log in to the CBH system.

Step 2 Choose **Policy** > **Database Rules** > **RegSet** to go to the DB rule list.

Figure 7-52 RegSet list

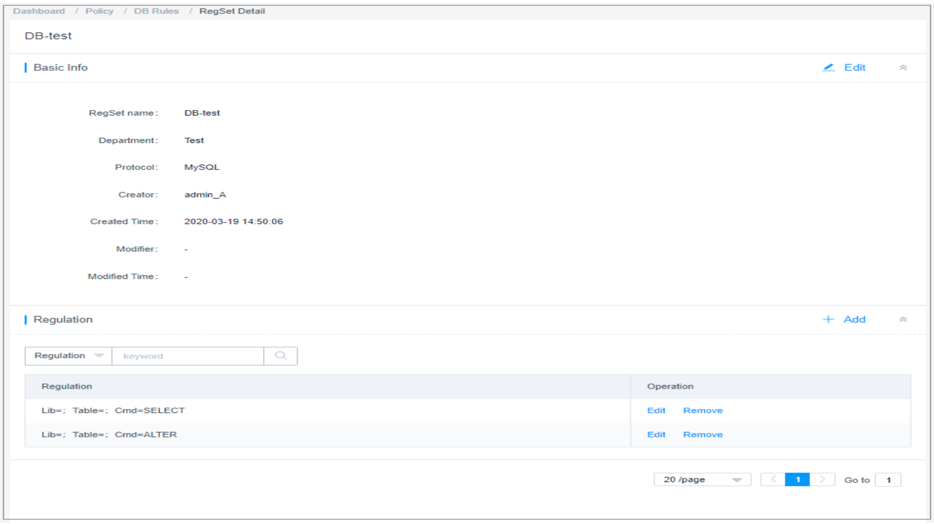


Step 3 Query the regulation sets.

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.

Figure 7-53 Regset details



Step 5 View and edit basic information.

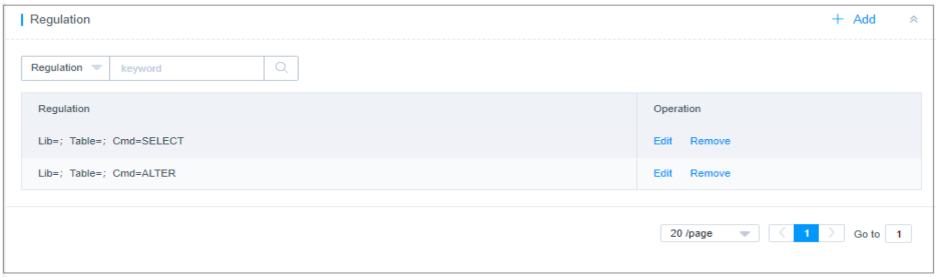
In the **Basic Info** area, click **Edit**. In the displayed dialog box, edit the basic information.

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**.

Figure 7-54 Viewing regulation sets



----End

Deleting a Regulation Set

Step 1 Log in to the CBH system.

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 multiple 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

7.4 Password Rules

7.4.1 Creating a Password Rule

With password rules, you can let the CBH system 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 change 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.
- Before relating to an account of a Windows 10 resource, set server parameters by referring to **Setting Parameters of Windows 10 Servers**.

Prerequisites

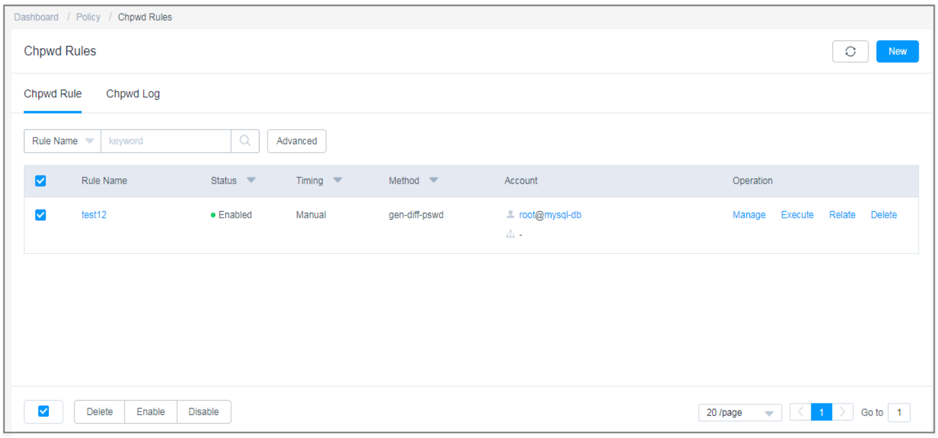
- You have the operation permissions for the **Password Rules** module.
- The configured OS type of the resource whose account password you want to change must be the same as the actual OS type of the resource.

Creating a Password Change Rule

Step 1 Log in to the CBH system.

Step 2 Choose **Policy** > **Password Rules** > **Password Rule**.

Figure 7-55 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.

Figure 7-56 Creating a Password Change Rule

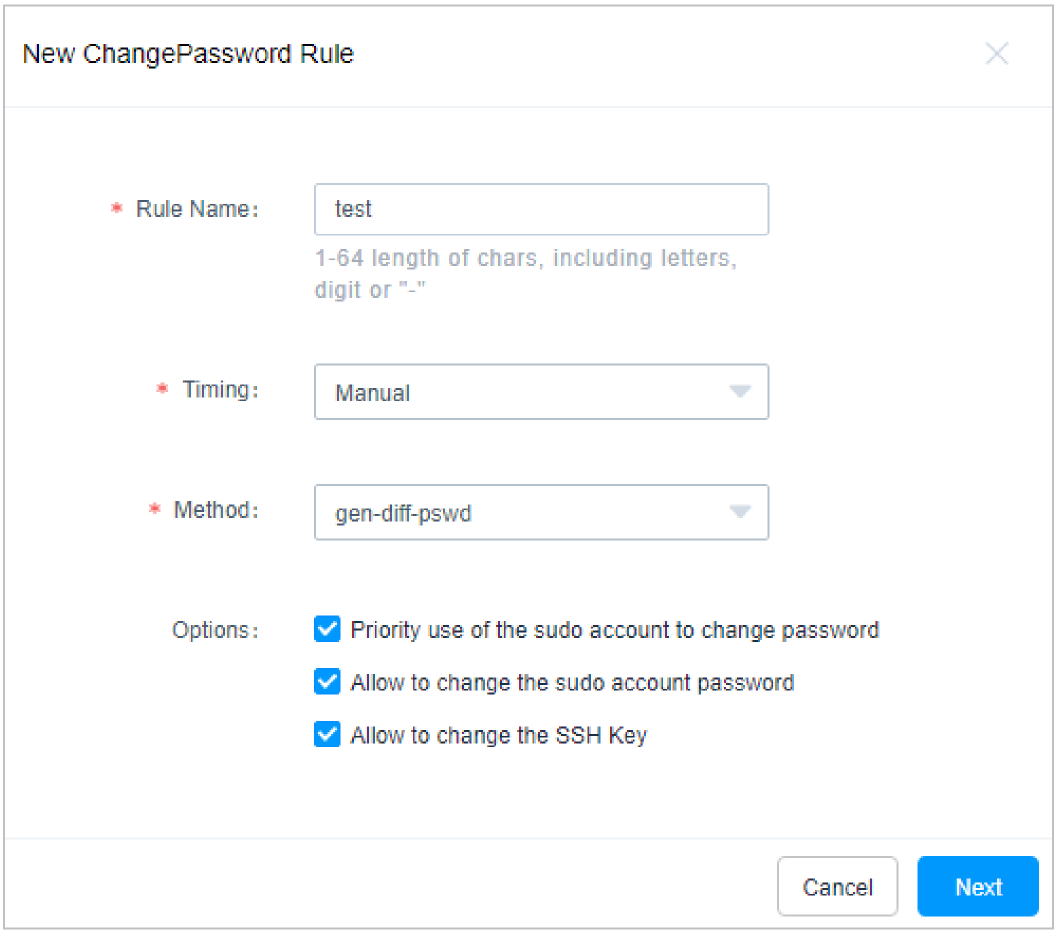


Table 7-5 Parameter for password change rules

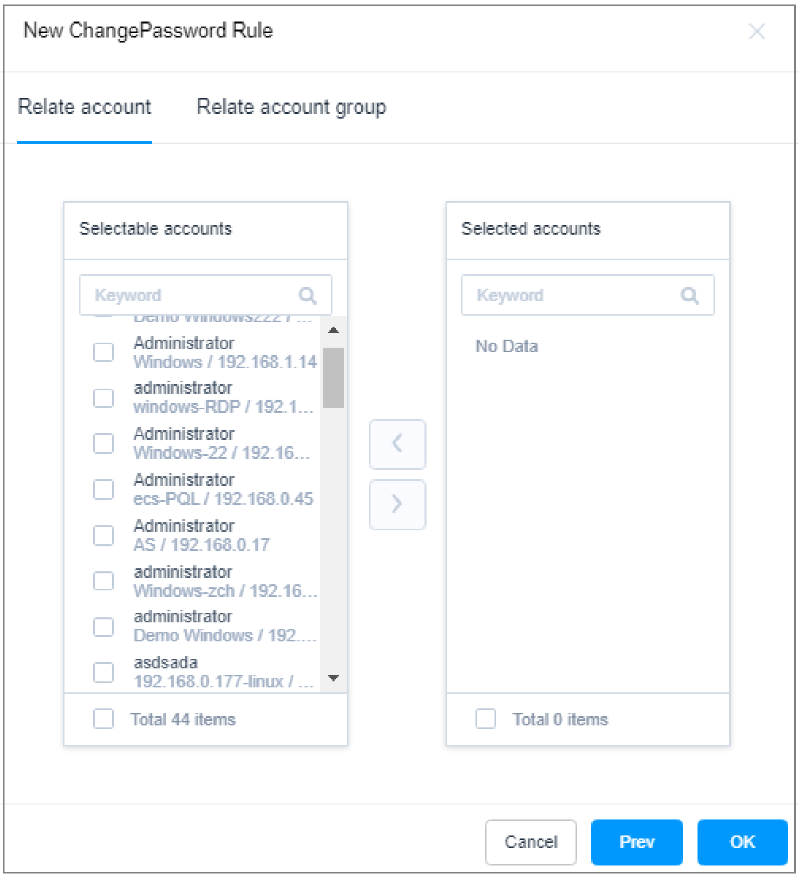
Parameter	Description
Rule Name	Name of a password change rule. The rule name must be unique in the CBH system.
Timing	The options are **Manual**, **Fixed-Time**, and **Cycle**. • **Manual**: Manually trigger the password change rule to change the password of the managed resource account. • **Fixed-Time**: The password change rule is triggered by the CBH system to change the password of the managed resource account at a fixed time. This type of rule is executed only once. • **Cycle**: The password change rule is periodically triggered by the CBH system to change the passwords of the managed resource accounts. This type of password change rule is triggered periodically.
Execute Time	Date when the password change rule is executed. The default execution time is at 00:00 every day.

Parameter	Description
Cycle Frequency	Password change interval. • The unit is day. • 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. **NOTE** A password randomly generated by CBH 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. • Specifying the same password: You manually change passwords of managed resource accounts to the same preset password you specify.
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 CBH system automatically change SSH public keys, select this option. **NOTE** The **Allow to change the SSH Key** option is included in version v3.3.36.0 and later only. To use this function, upgrade your CBH system to V3.3.36.0 or later by referring to **Upgrading the CBH System Version**.

Step 5 Click **Next** and start to relate the ACL rule to one or more accounts or account groups.

- After a password change 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.

Figure 7-57 Relate Accounts



Step 6 Click **OK**. You can then view the new password change rule in the rule list.

To obtain the new password of the managed resource accounts, export host resource details by referring to **Batch Editing Host Information**.

----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

CBH gives you the ability to manage all password change 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 change 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.

7.4.2 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 the CBH system.

Step 2 Choose **Policy** > **Password Rules** > **Password Rule**.

Step 3 Query password rules.

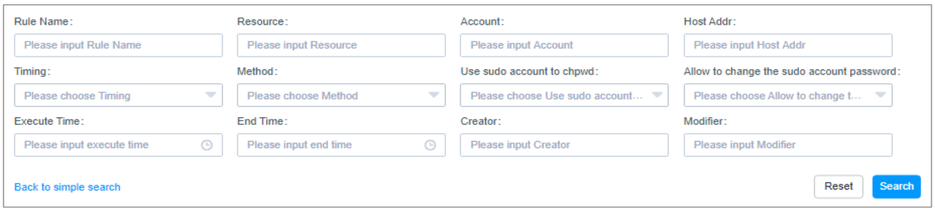
- Quick search

  Enter a keyword in the search box to quickly query password change rules by rule name, resource name, and account,

- Advanced search

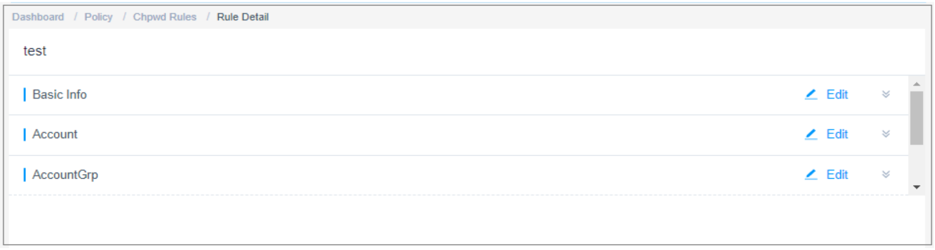
  Enter keywords in the corresponding attribute search boxes to search for database rules in exact mode.

Figure 7-58 Advanced search



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.

Figure 7-59 Viewing rule details

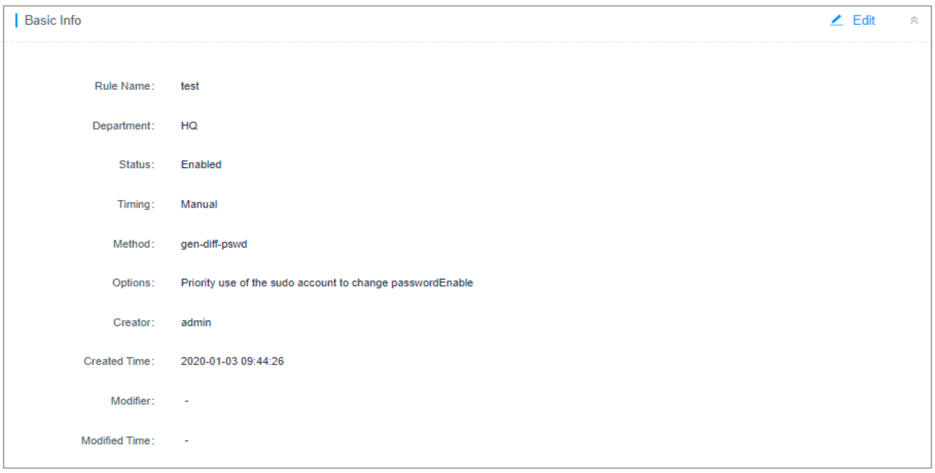


Step 5 View and edit basic information.

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.

Figure 7-60 Viewing the basic information

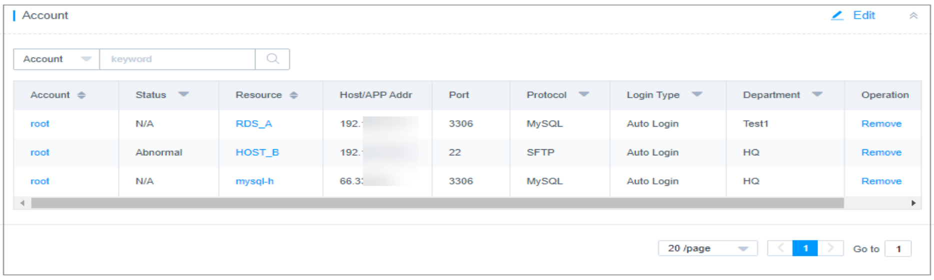


Step 6 View and edit accounts related to the database rule.

- 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.

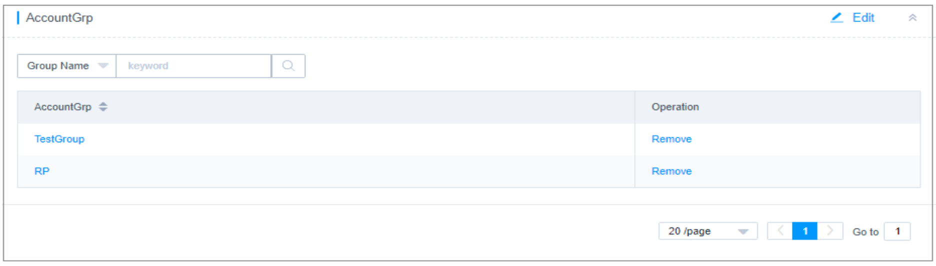
Figure 7-61 Viewing related accounts



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.

Figure 7-62 Viewing related account groups



----End

7.4.3 Managing Password Logs

After a password rule is executed, logs are generated accordingly. You can view the password change details in password change logs.

Prerequisites

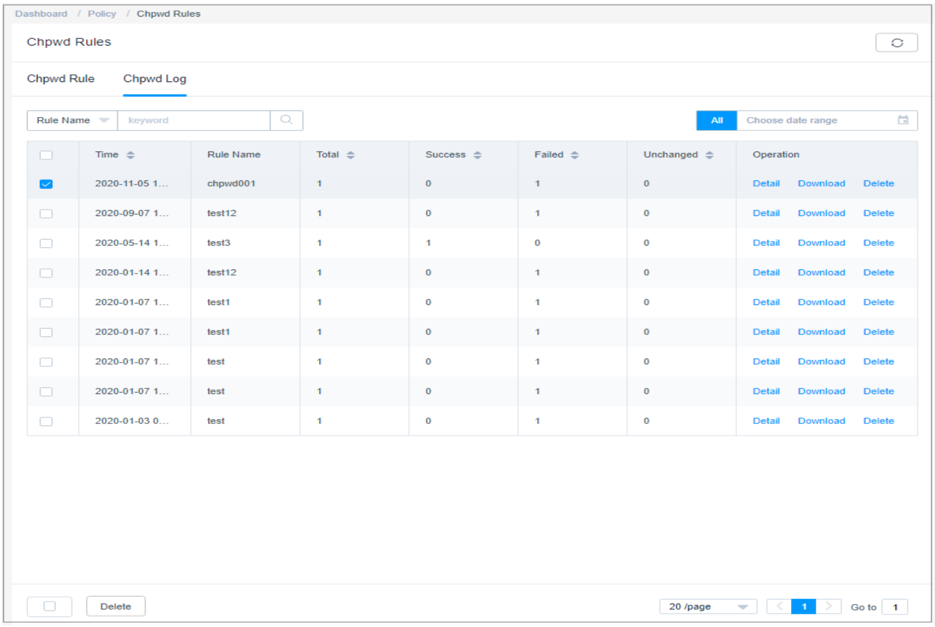
You have the operation permissions for the **Password Rules** module.

Viewing Log Details

Step 1 Log in to the CBH system.

Step 2 Choose **Policy** > **Password Rules** > **Password Log** to view and manage password change logs.

Figure 7-63 Password logs



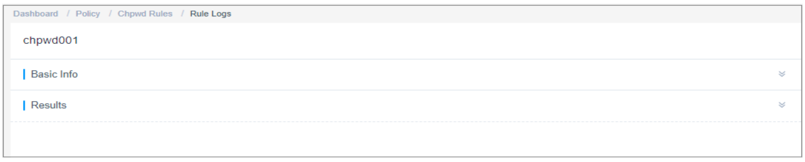
Step 3 Query password change logs.

Quick search: Enter a keyword in the search box and search for password change logs by rule name.

Step 4 Select the password change log and click **Detail**.

You can view the log content, including the basic information and password change result.

Figure 7-64 Viewing password log details



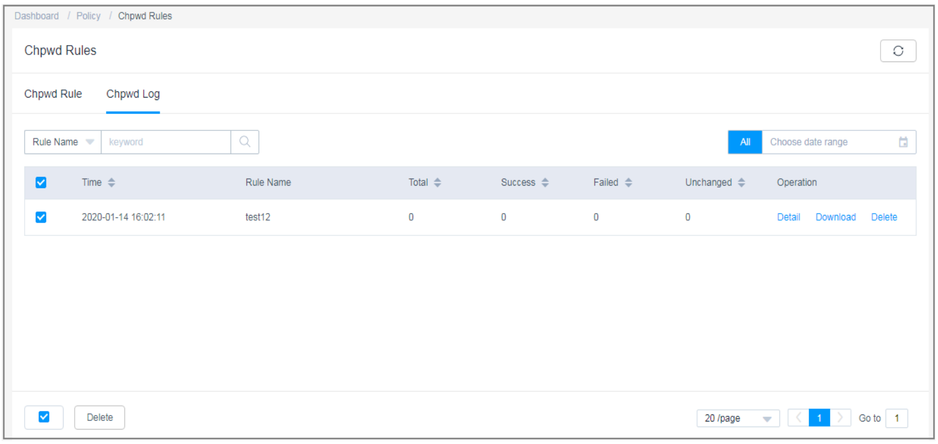
----End

Downloading Password Logs

Step 1 Log in to the CBH system.

Step 2 Choose **Policy** > **Password Rules** > **Password Log** to view and manage password logs.

Figure 7-65 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 change 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.

Figure 7-66 Downloading Password Logs

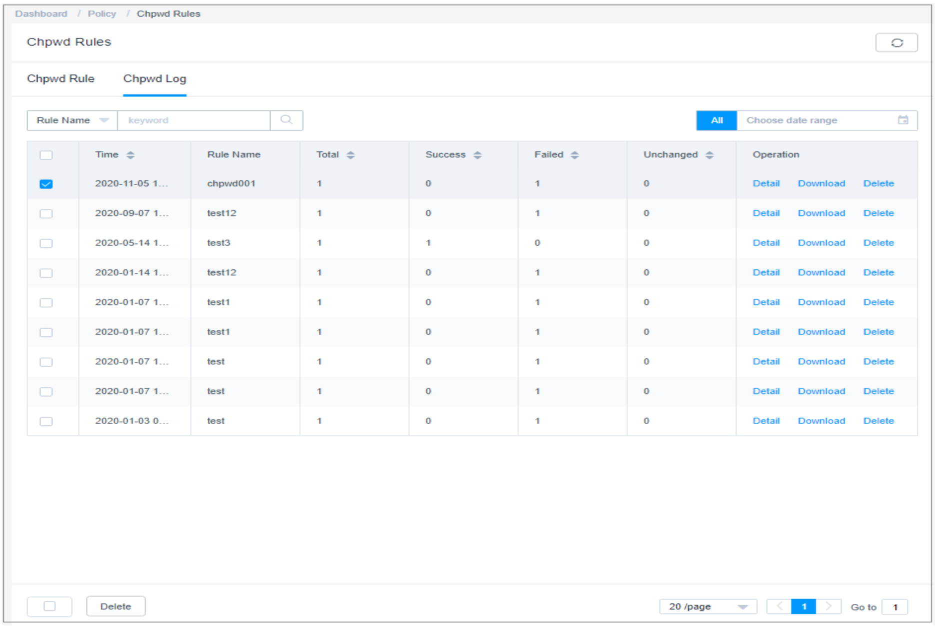
----End

Deleting Execution Logs

Step 1 Log in to the CBH system.

Step 2 Choose **Policy** > **Password Rules** > **Password Log**.

Figure 7-67 Password logs



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

7.5 Account Synchronization Rules

7.5.1 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 available only in CBH 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

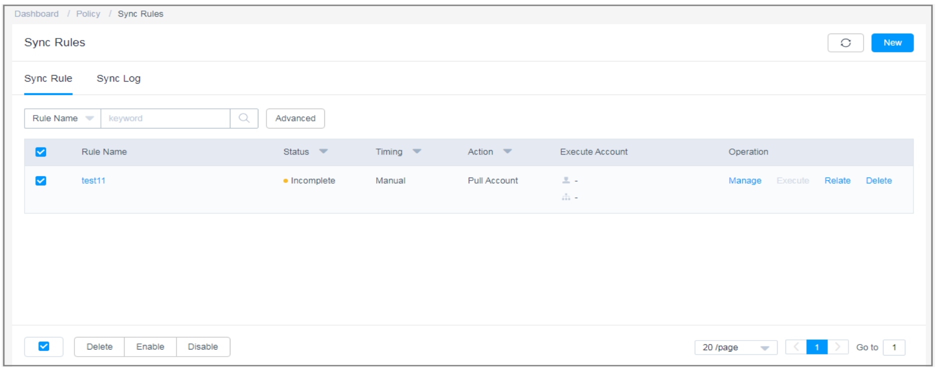
You have the operation permissions for the **Sync Rules** module.

Creating a Synchronization Rule

Step 1 Log in to the CBH system.

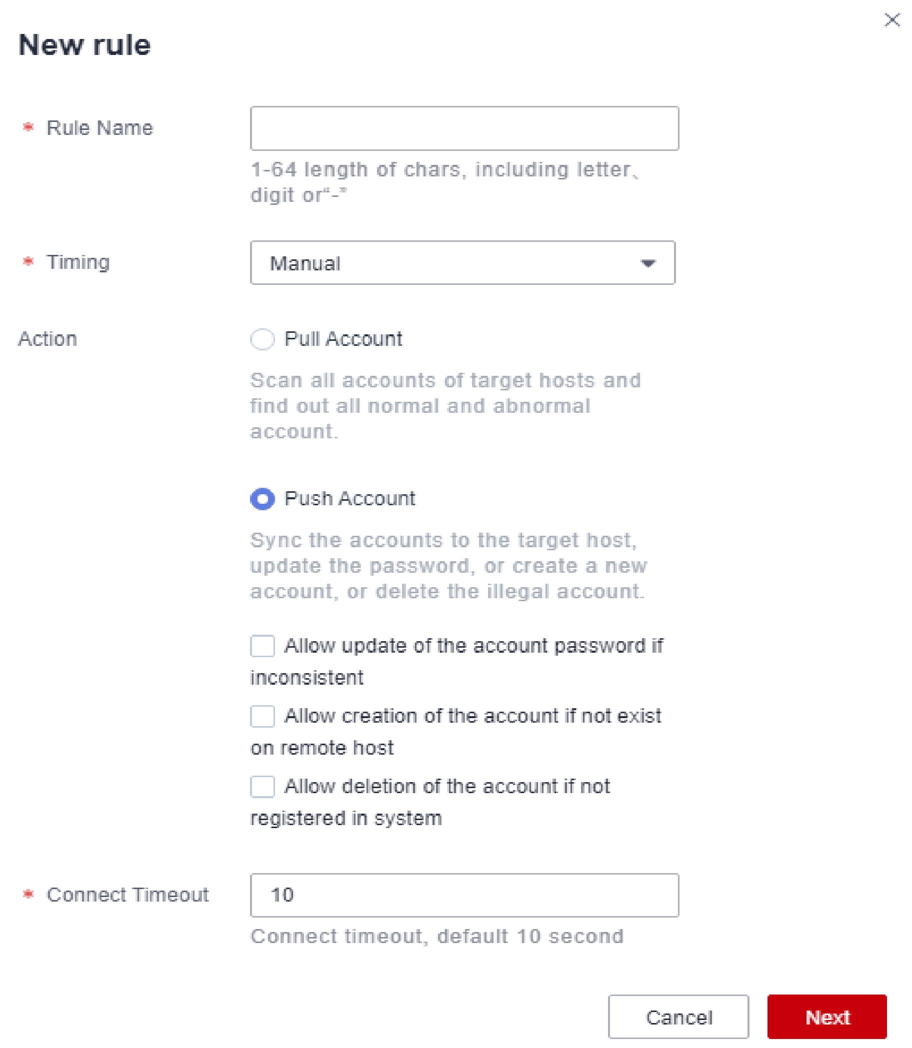
Step 2 Choose **Policy** > **Sync Rules** > **Sync Rules**.

Figure 7-68 Account synchronization rules



Step 3 Click **New** in the upper right corner of the **Sync Rule** area to switch to the **New rule** dialog box.

Figure 7-69 New rule



Step 4 Configure the basic information.

Table 7-6 Parameters for configuring an account synchronization rule

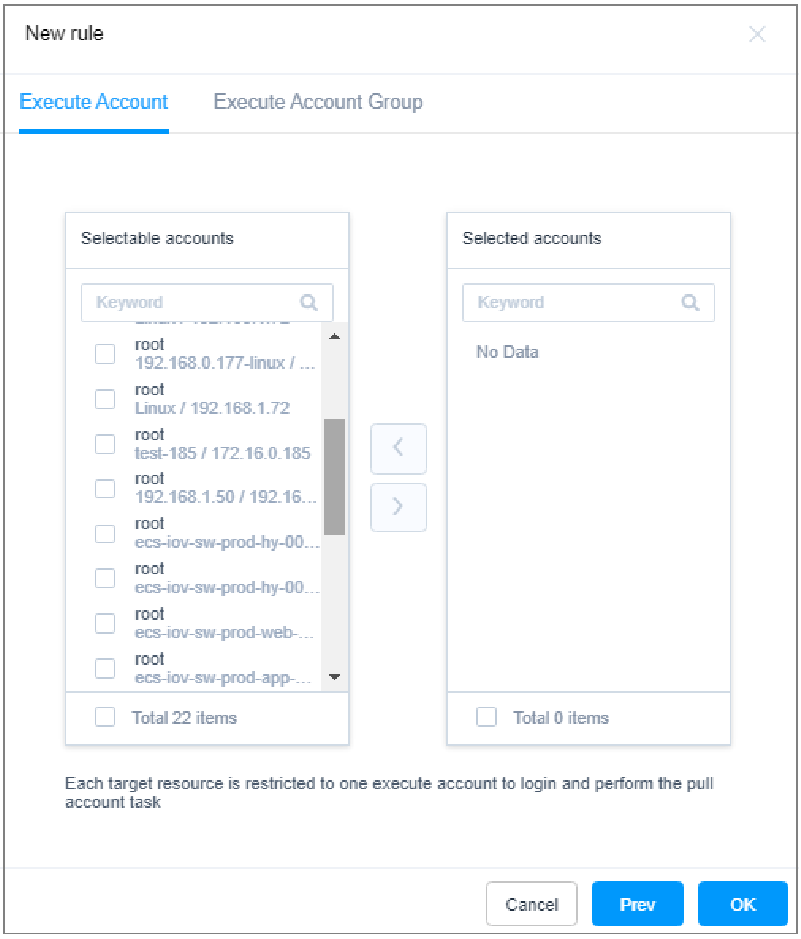
Parameter	Description
Rule Name	Name of an account synchronization rule. The rule name must be unique in the CBH system.

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 CBH system 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 CBH system 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.

Figure 7-70 Configuring execution accounts



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.

7.5.2 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 the CBH system.

Step 2 Choose **Policy** > **Sync Rules** > **Sync Rules**.

Step 3 Query account synchronization rules.

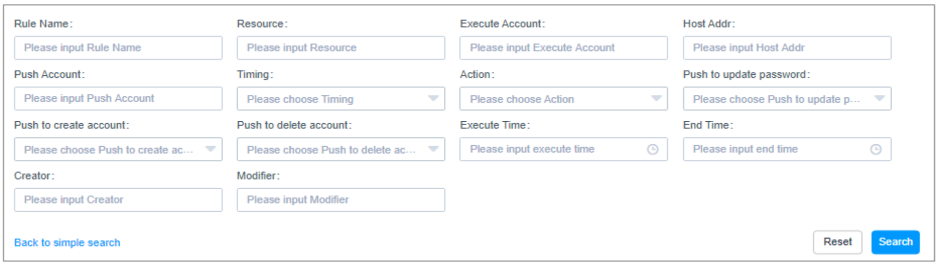
- Quick search

  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.

Figure 7-71 Advanced search



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.

Figure 7-72 Viewing rule details

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.

Figure 7-73 Viewing the basic information

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

7.5.3 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

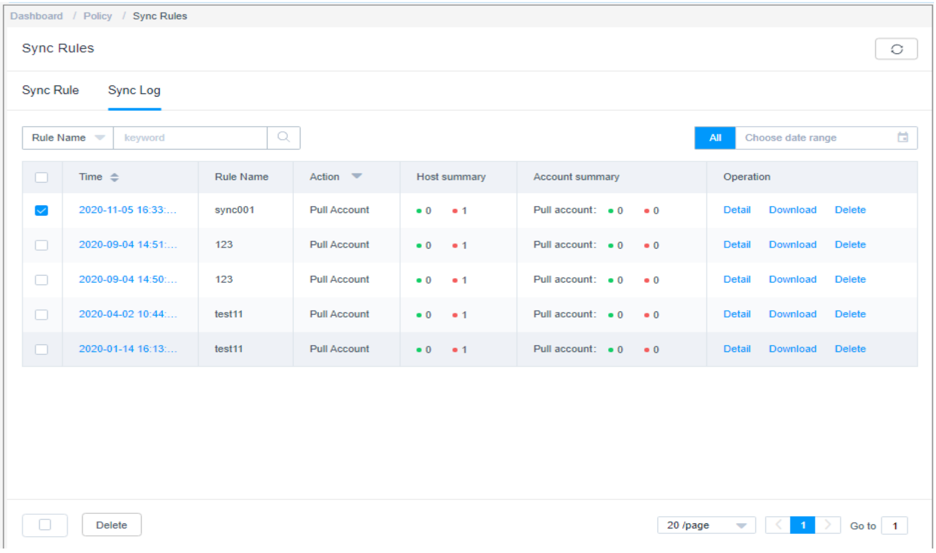
You have the operation permissions for the **Sync Rules** module.

Viewing Log Details

Step 1 Log in to the CBH system.

Step 2 Choose **Policy** > **Sync Rules** > **Sync Log**.

Figure 7-74 Execution logs



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 7-75 Viewing the basic information

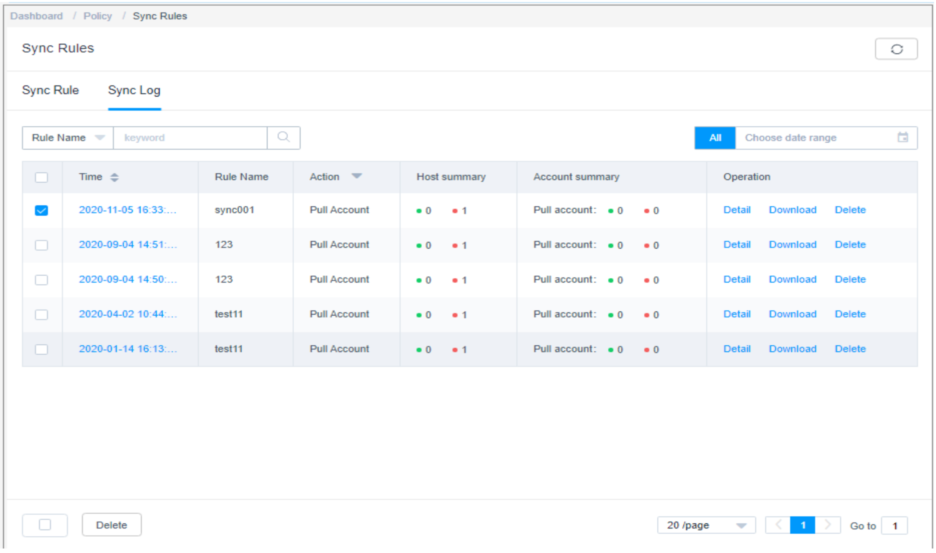
----End

Downloading OM Task Execution Logs

Step 1 Log in to the CBH system.

Step 2 Choose **Policy** > **Sync Rules** > **Sync Log**.

Figure 7-76 Execution logs



Step 3 Select the execution log and click **Download** to download the log in CSV format.

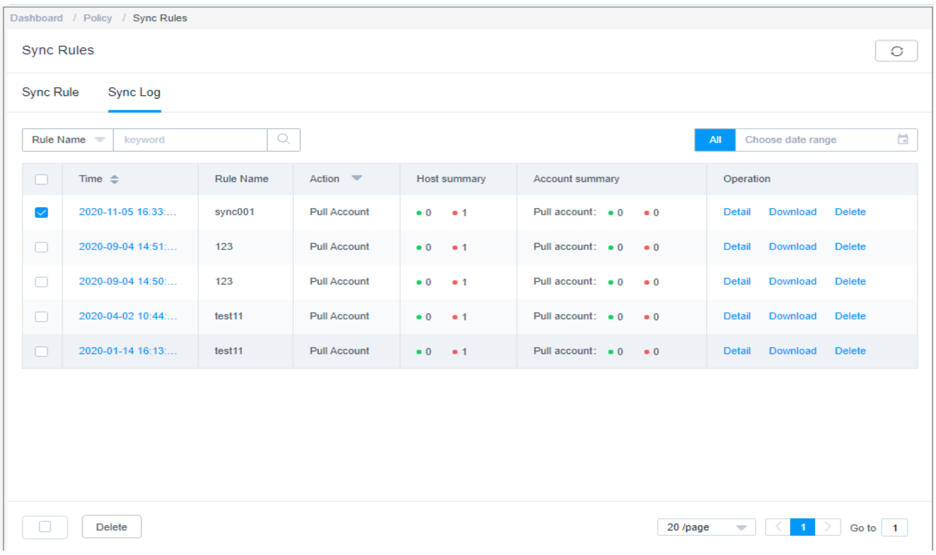
----End

Deleting Execution Logs

Step 1 Log in to the CBH system.

Step 2 Choose **Policy** > **Sync Rules** > **Sync Log**.

Figure 7-77 Execution logs



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 Ticket

8.1 Ticket Configuration Management

8.1.1 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.

This topic describes how to configure the ticket mode.

Prerequisites

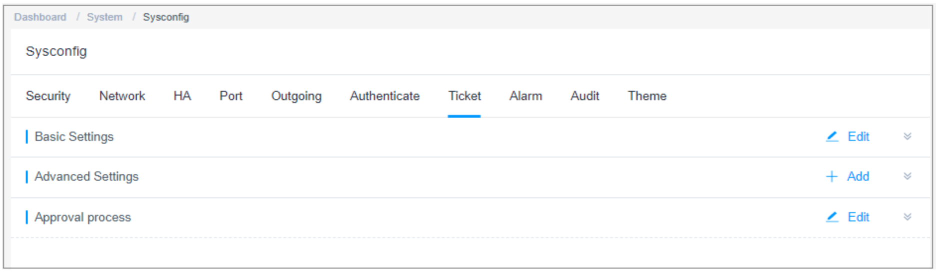
You have the management permissions for the **System** module.

Configuring the Basic Ticket Settings

Step 1 Log in to the CBH system.

Step 2 Choose **System** > **Sysconfig** > **Ticket**.

Figure 8-1 Ticket configuration



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.

Figure 8-2 Basic Settings

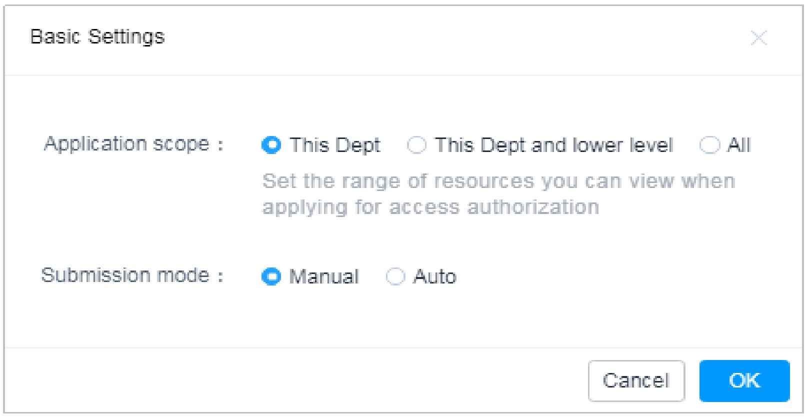
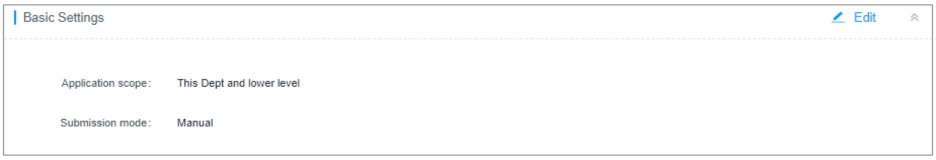


Table 8-1 Parameter description

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.

Figure 8-3 Viewing basic settings



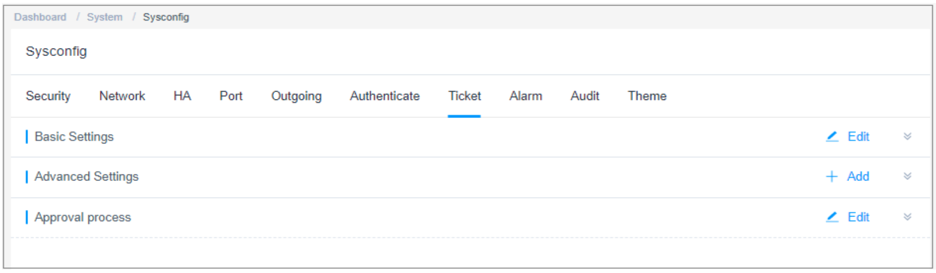
----End

Configuring the Advanced Ticket Settings

Step 1 Log in to the CBH system.

Step 2 Choose **System** > **Sysconfig** > **Ticket**.

Figure 8-4 Ticket configuration

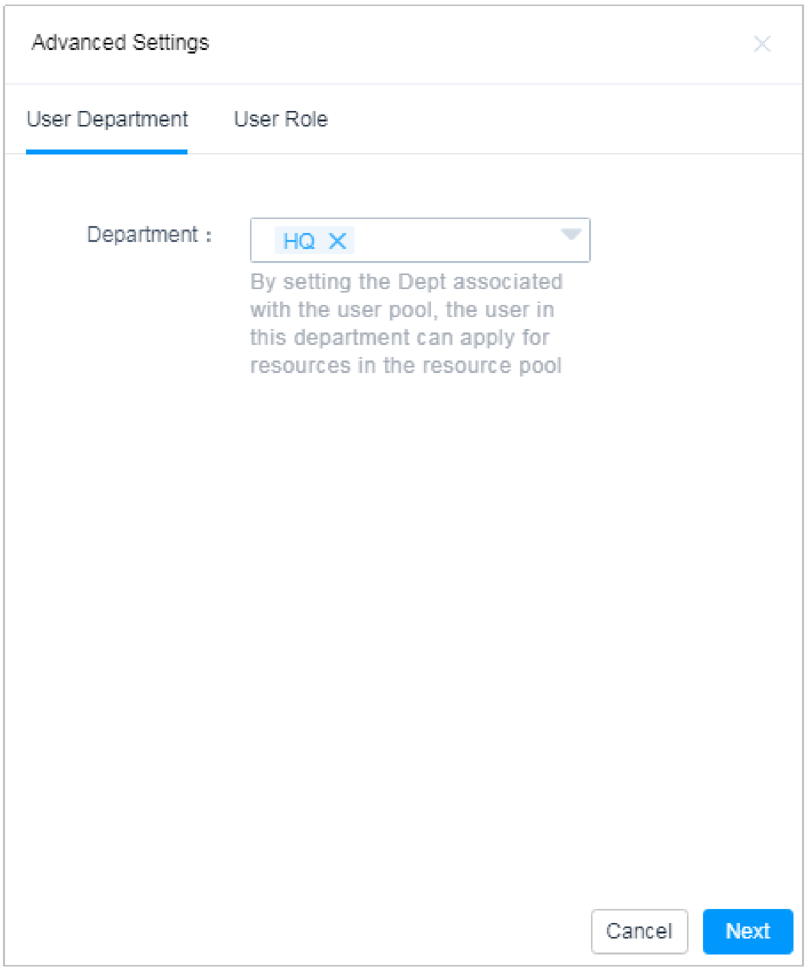


Step 3 In the **Advanced Settings** area, click **Edit**.

Step 4 Configure the user pool.

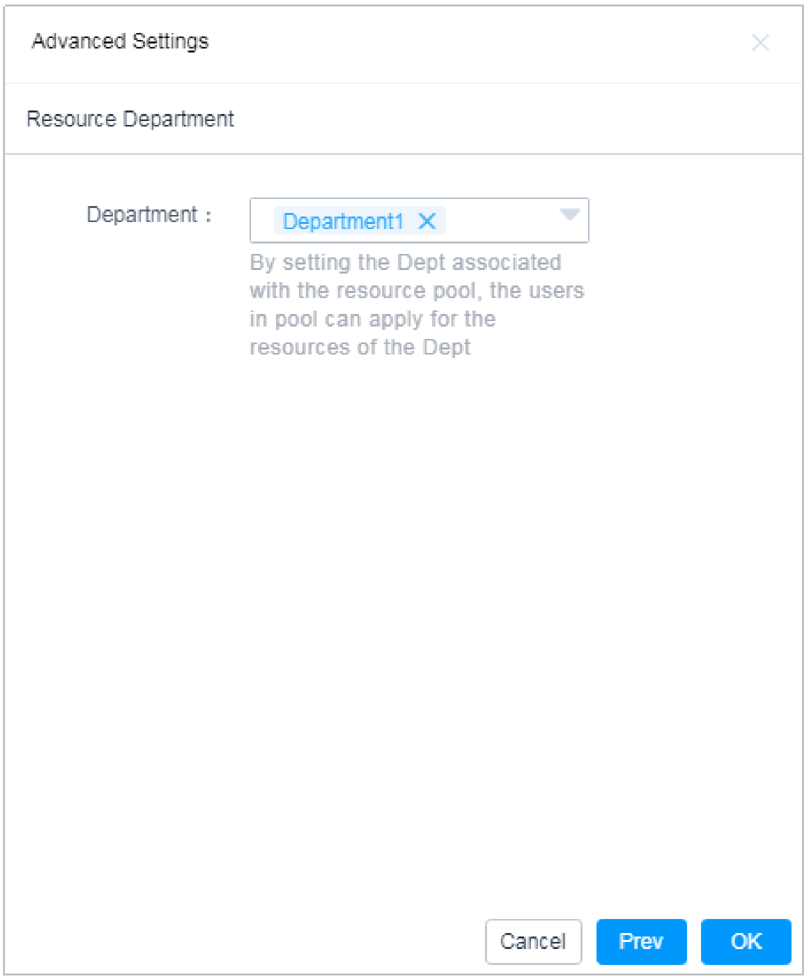
Select user department or user role.

Figure 8-5 Select user department or user role.



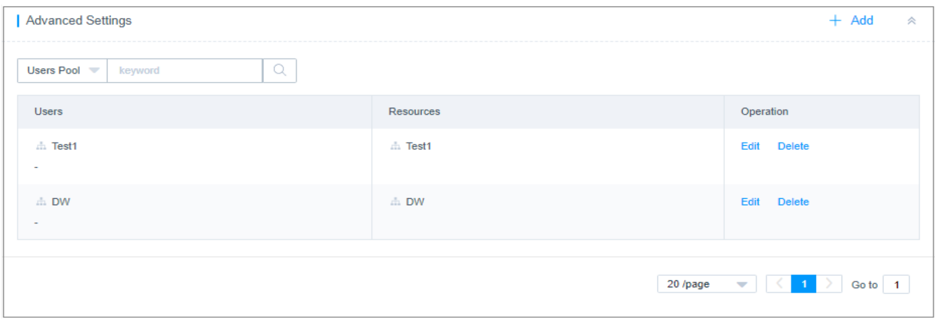
Step 5 Click **Next** and configure resource department.

Figure 8-6 Resource Department



Step 6 Click **OK**. You can then view the configured ticket settings.

Figure 8-7 Viewing advanced 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.

8.1.2 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

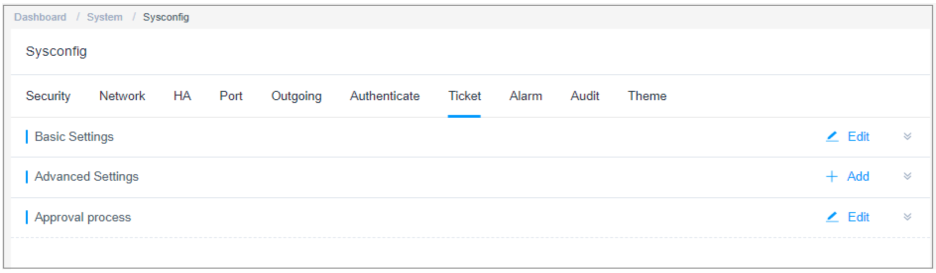
You have the management permissions for the **System** module.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **System** > **Sysconfig** > **Ticket**.

Figure 8-8 Ticket configuration



Step 3 In the **Approval process** area, click **Edit**.

In the displayed **Approval process** dialog box, specify required parameters.

Figure 8-9 Approval processes

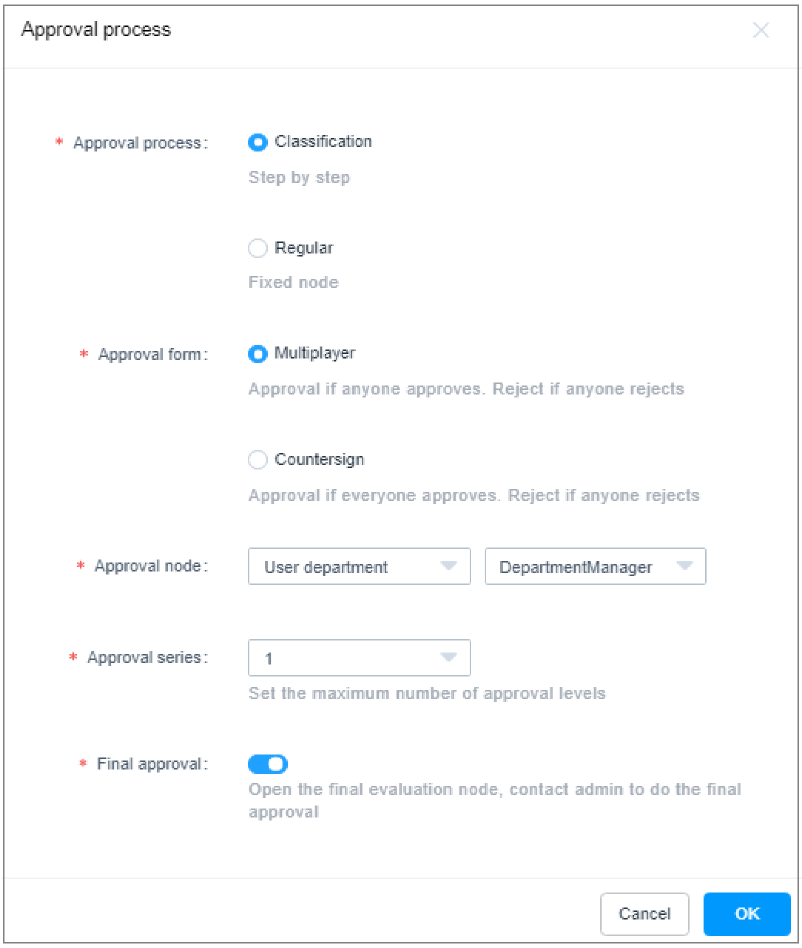


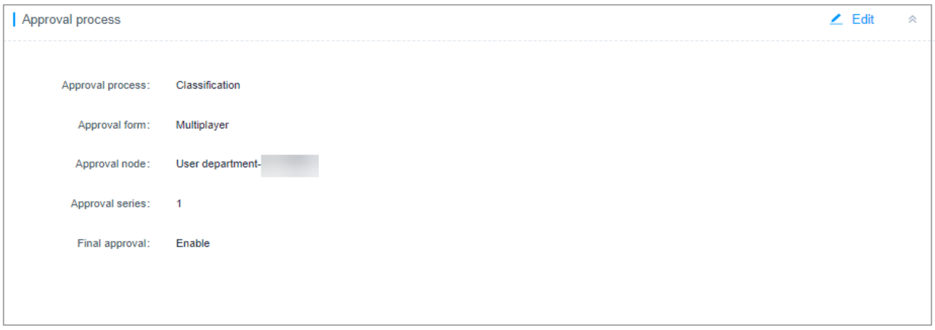
Table 8-2 Parameters for configuring ticket approval processes

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. ● By default, the hierarchical process mode is used. ● Hierarchical process: 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 either of 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.

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.

Figure 8-10 Viewing a ticket approval process



----End

8.2 ACL Ticket

If you have no permissions to access some resources, you can submit a ticket to apply for the required permissions.

This topic describes how to create and manage ACL tickets.

Prerequisites

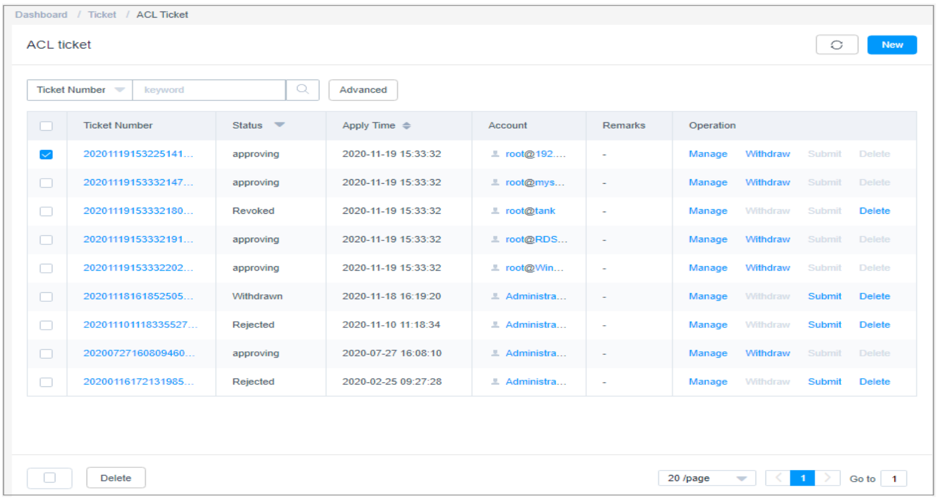
You have the management permissions for the **ACL Ticket** module.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **Tickets** > **ACL Ticket**.

Figure 8-11 ACL ticket



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

In the displayed **New ACL ticket** page, configure basic information.

Figure 8-12 New ACL ticket

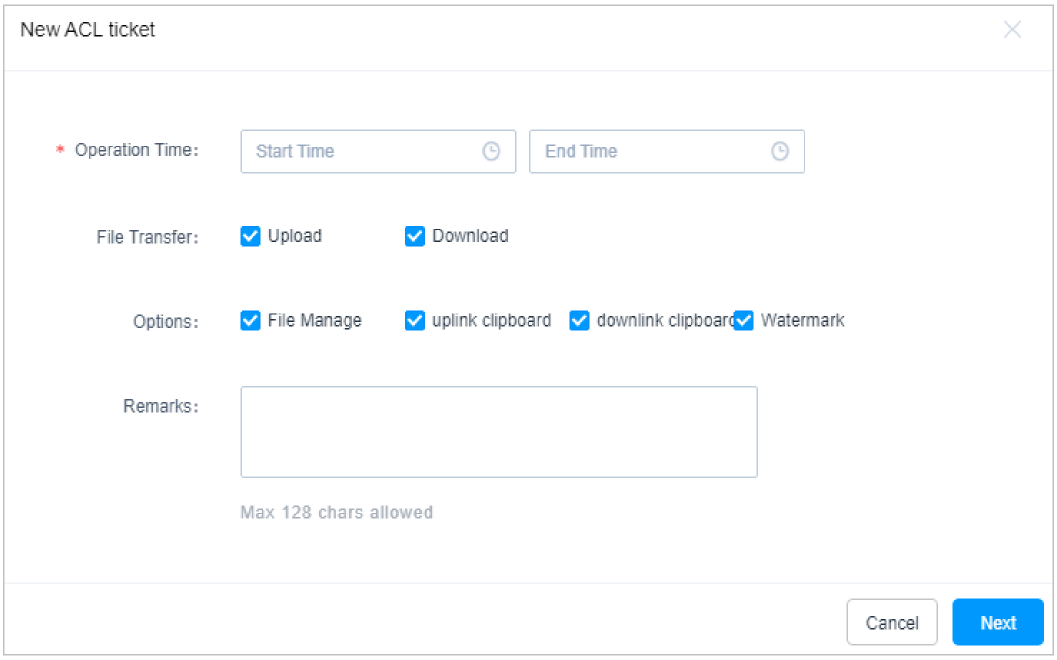
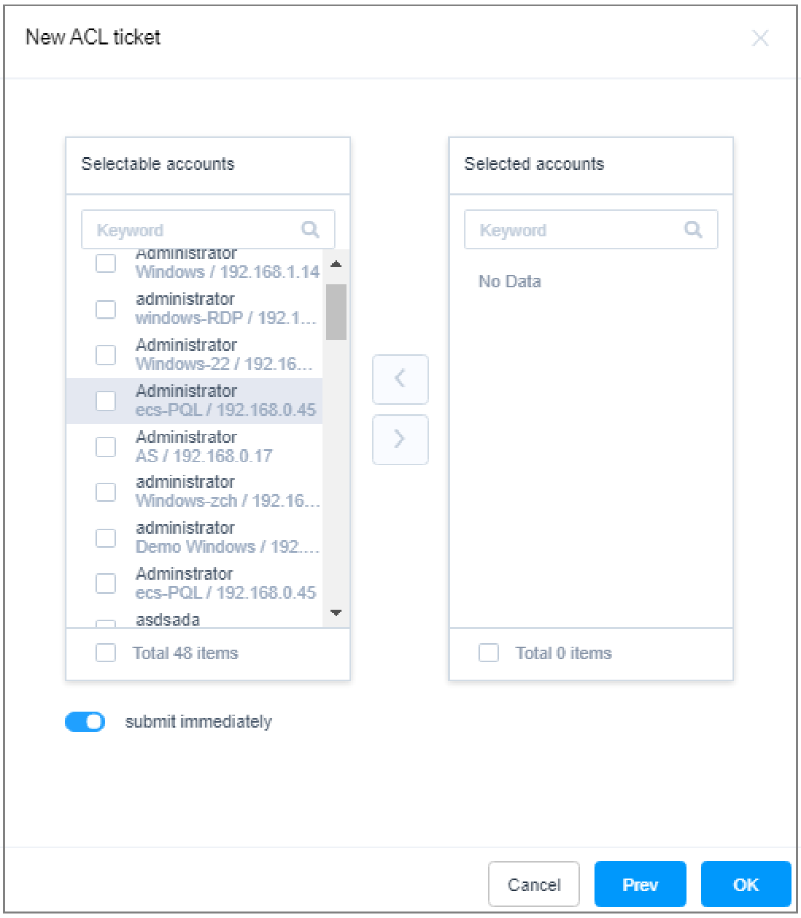


Table 8-3 Parameters for configuring an ACL ticket

Parameter	Description
Operation Time	Specifies the time period for accessing the resource. The start time and end time must be set.
File Transmission	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.
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.

Figure 8-13 Relate Accounts



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

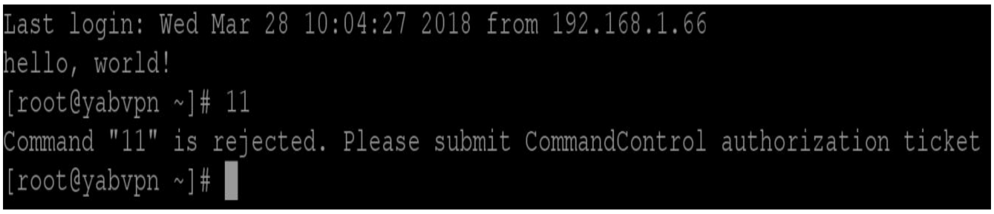
Deleted tickets cannot be recovered. Exercise caution when performing this operation.

8.3 Command Approval Ticket

CBH enables dynamic authorization of operations on Linux hosts. This enhances the restriction of key 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 8-14 Example of command interception



This topic describes how to manage command approval tickets.

Constraints

- CBH can intercept sensitive operation commands and generate tickets only for Linux hosts using the SSH or Telnet protocol.
- A command approval ticket cannot be manually created. It is automatically generated when a user attempts to run a command which triggers a command rule.

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 the CBH system.

Step 2 Choose **Tickets** > **Command Approval Ticket**.

Figure 8-15 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 8-16 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.

8.4 Database Approval Ticket

CBH supports dynamic approval of database operations. This enhances a more strict management of key 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 CBH professional editions.
- CBH 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

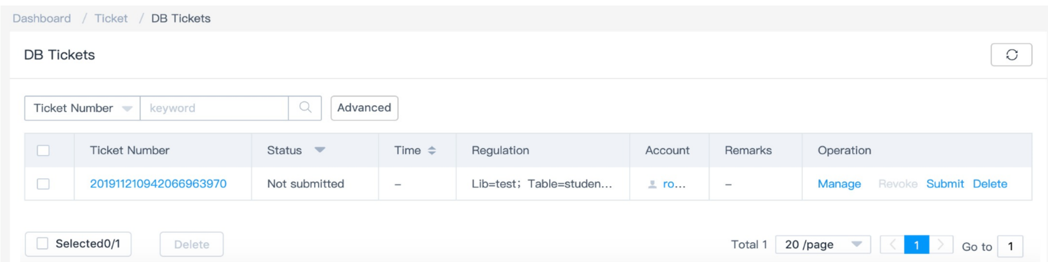
- You have the management permissions for the **DB Tickets** module.
- Operation interception has been triggered, and a database approval ticket has been generated.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **Tickets** > **DB Tickets**.

Figure 8-17 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.

8.5 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 submitted tickets, including viewing ticket details, approving tickets, rejecting tickets, and revoking ticket.

Prerequisites

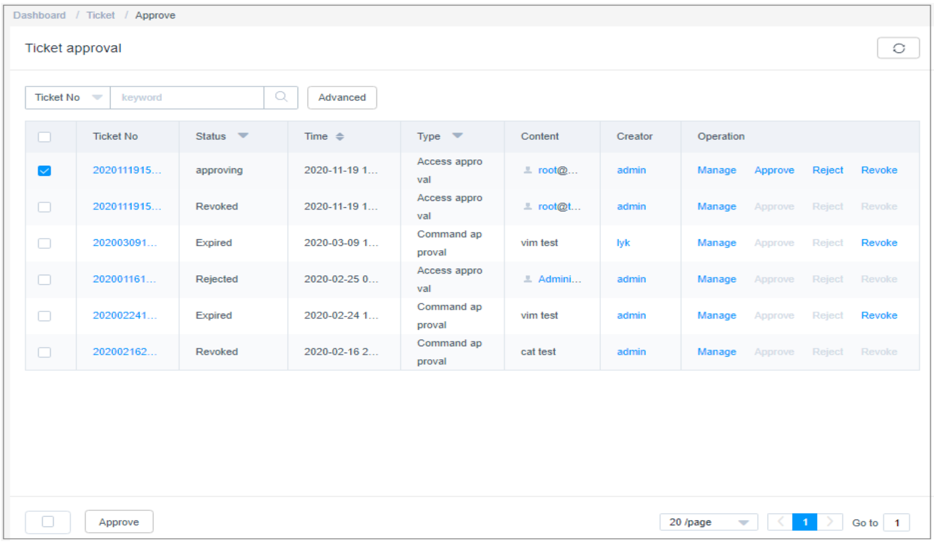
You have the management permissions for the **Ticket approval** module.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **Ticket** > **Ticket approval**.

Figure 8-18 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 8-19 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

8.6 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 8-4**. For more details about ticket approval process, see **Configuring the Ticket Approval Process**.

Table 8-4 Parameters for configuring a ticket approval process

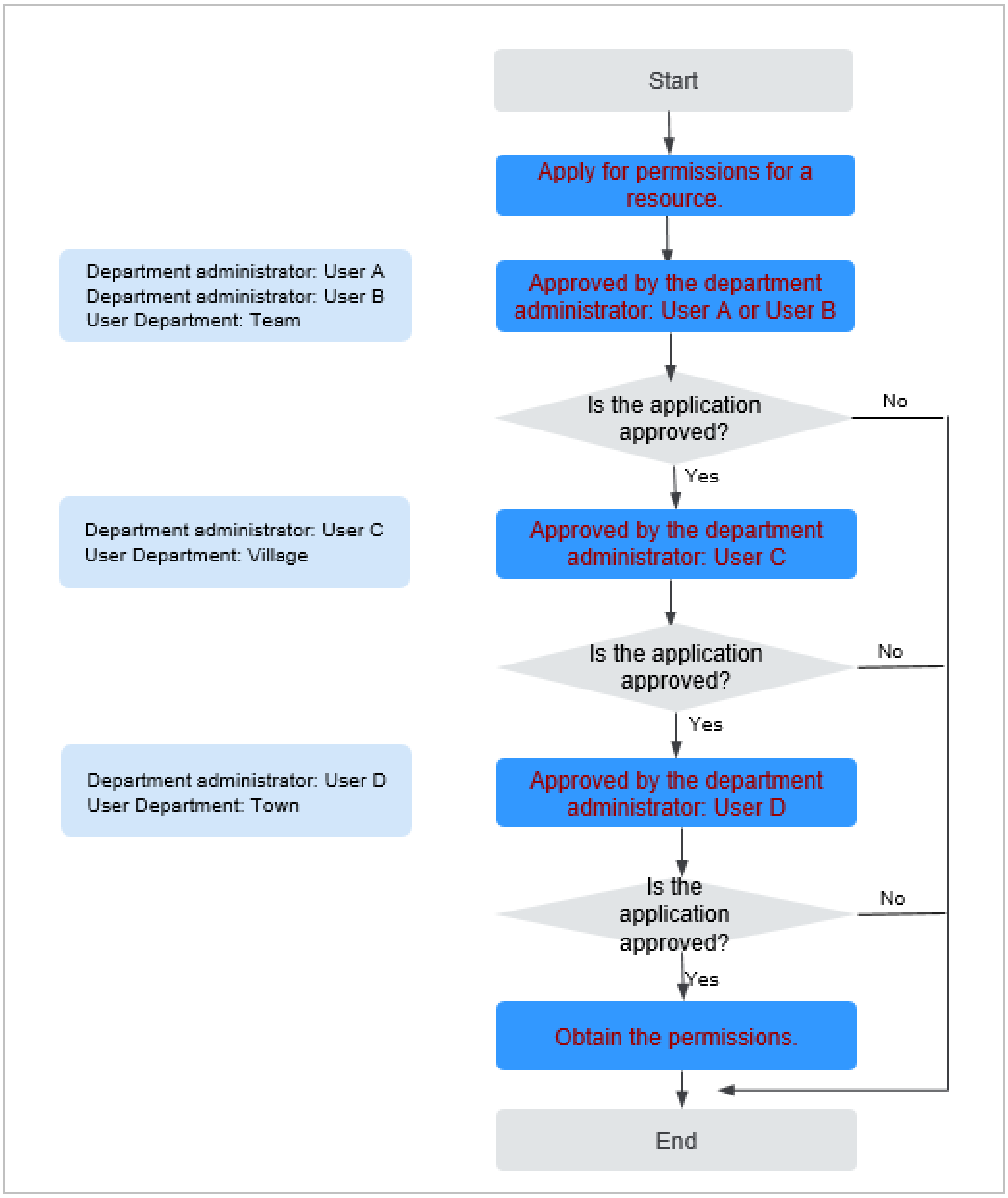
Parameter	Value
Approval process type	Classification
Approval form	Multiplayer
Approval node	User department – Department Manager
Approval series	3

Approval Process

A user submits a ticket to apply for resources access permissions based on the department that the user belongs to. The following figure shows the ticket approval process.

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.

Figure 8-20 Ticket Approval Processes



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 8-5**. For more details about ticket approval process, see **Configuring the Ticket Approval Process**.

Table 8-5 Parameters for configuring a ticket approval process

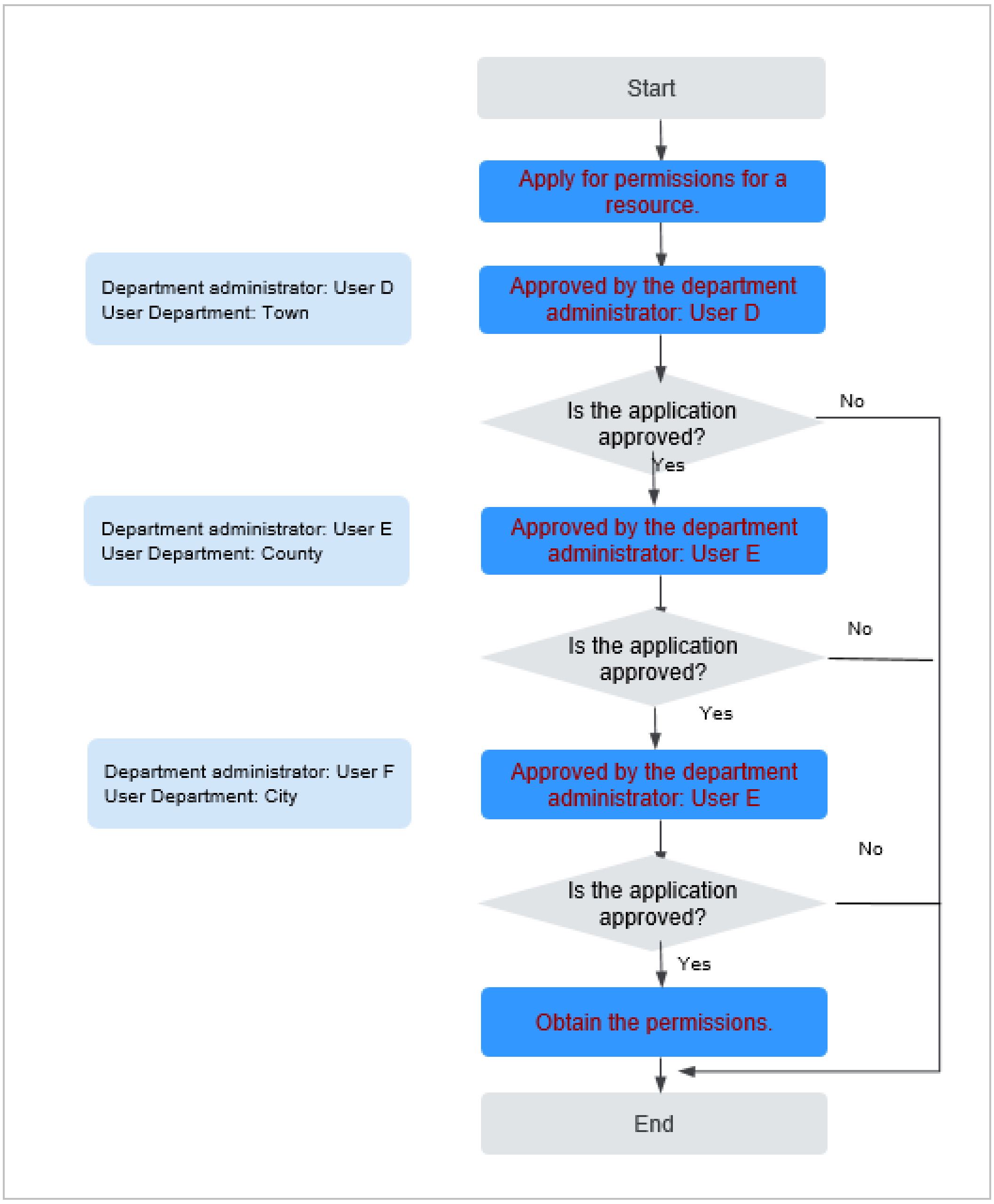
Parameter	Value
Approval process type	Classification
Approval form	Multiplayer
Approval node	User department – Department Manager
Approval series	3

Approval Process

A user submits a ticket to apply for resources access permissions based on the department that the resources belong to. **Figure 8-21** shows the ticket approval process.

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.

Figure 8-21 Approval process type



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 8-6**. For more details about ticket approval process, see **Configuring the Ticket Approval Process**.

Table 8-6 Parameters for configuring a ticket approval process

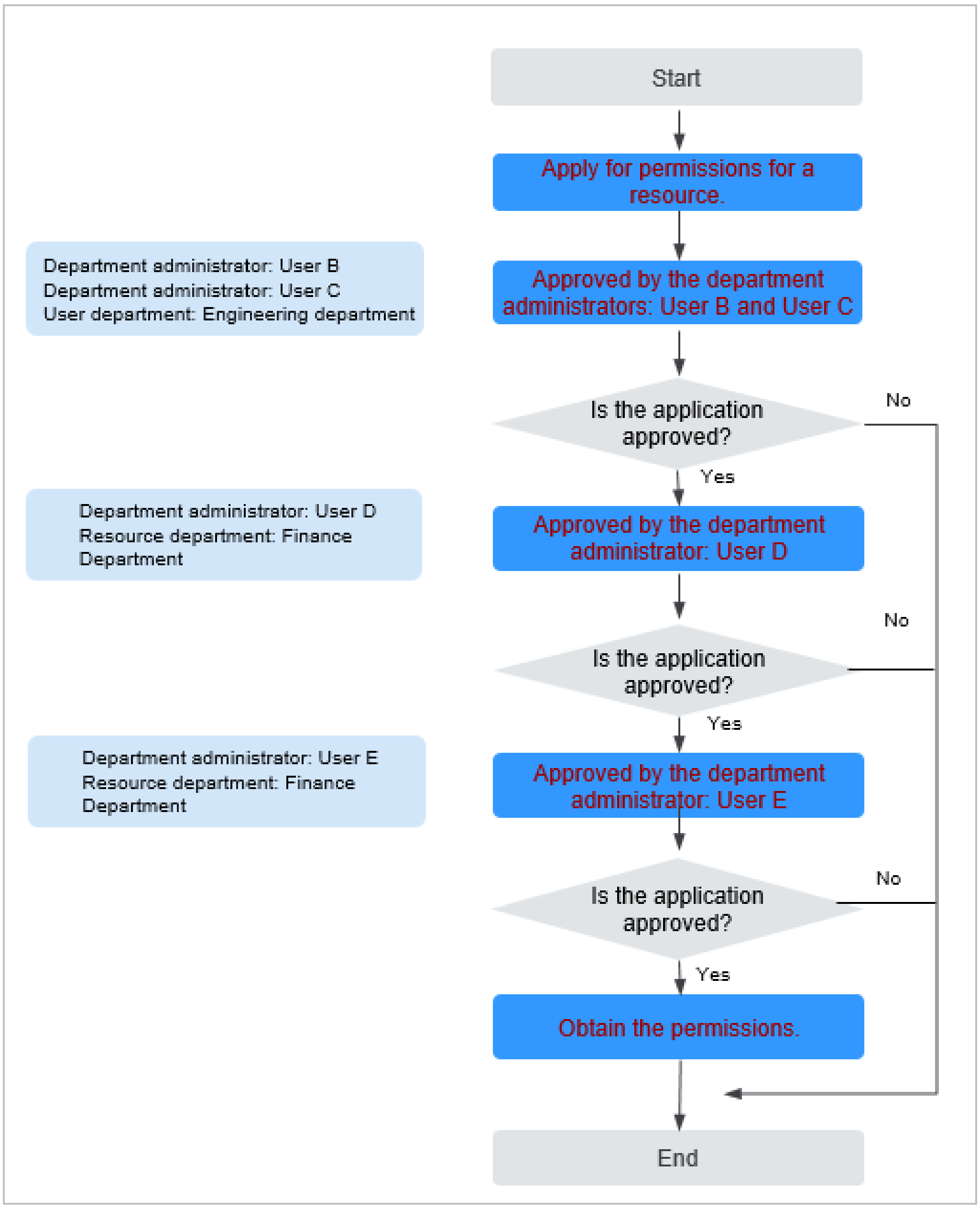
Parameter	Value
Approval process type	Regular
Approval form	Countersign
Approval node	3

Approval Process

A user submits a ticket to apply for access to resources of another department. **Figure 8-22** shows the ticket approval process.

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.

Figure 8-22 Countersigning and approval process



9 Operation

9.1 Host Operation

9.1.1 Viewing the Host Resource List and Setting Resource Labels

After obtaining the access permissions for host resources, you can view authorized host resources in the host operation list and set labels for host 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

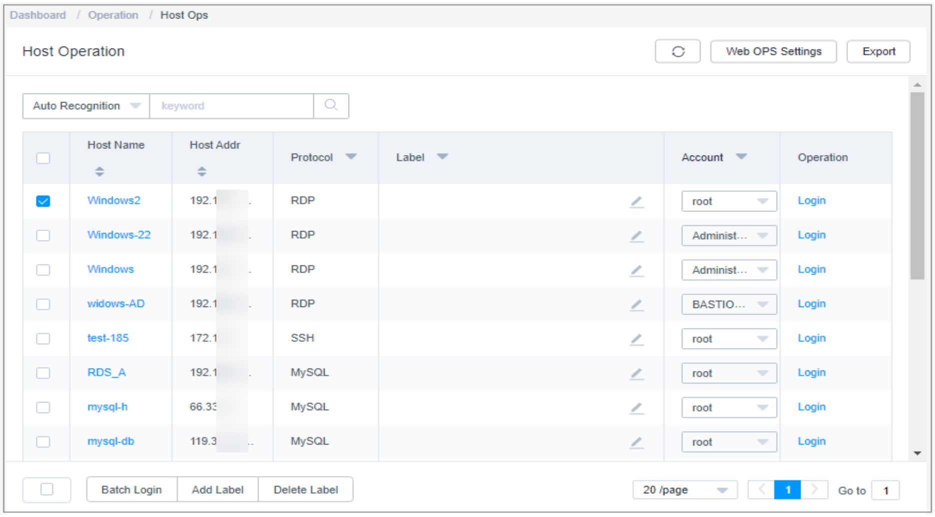
- You have the management permissions for the **Host Operation** module.
- You have obtained the access permissions for the resources.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **Operation** > **Host Operation** to go to the **Host Operation** page.

Figure 9-1 Host Operation



Step 3 Query host 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.

Figure 9-2 Add Label

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 **Host 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 **Host 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. In the displayed dialog box, confirm the deletion and click **OK**.

----End

9.1.2 Logging In to Managed Resources Using a Web Browser 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. All operations performed on a host resource are recorded by CBH for audit.

- 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 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.

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.
- 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.

– Folders cannot be downloaded.

– For the hosts using the RDP protocol, only **Netdisk** can be select as the destination address.

Prerequisites

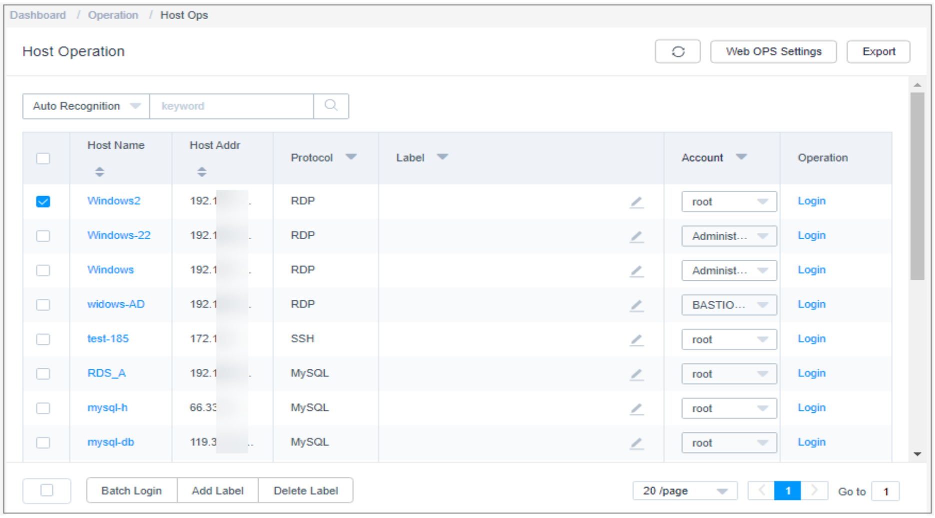
- You have the management permissions for the **Host Operation** module.
- You have obtained the access permissions for the resources.
- The network connection between the managed host and the system is normal, and the account username and password for logging in to the managed host are correct.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **Operation** > **Host Operation** to go to the **Host Operation** page.

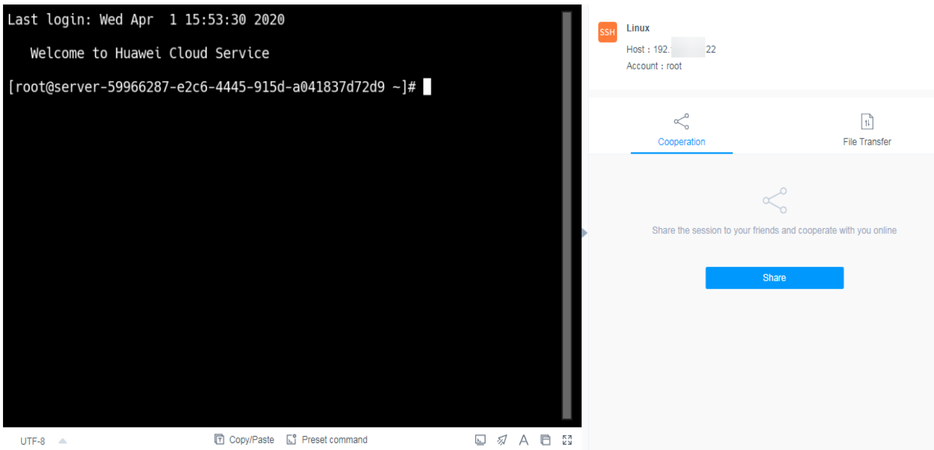
Figure 9-3 Host Operation



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 9-4 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 of the CBH account can access the CBH system. 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 for CBH. Once they receive the link, they can log in to the CBH system, 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 9-1 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.

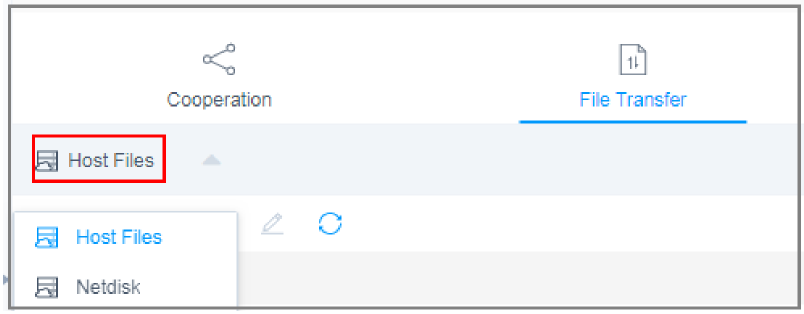
Step 5 Upload files to or download files from the host or host net disk. For details, see **File Transfer**.

1. Click **File Transfer**. The **File Transfer** window is displayed.

Figure 9-5 File Transmission

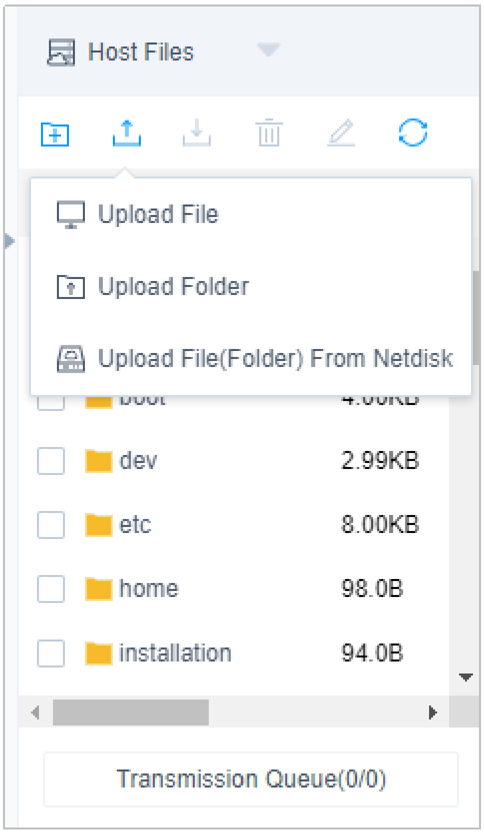
2. **Host Files** is selected by default. You can click **Host Files** to switch the destination address to **Netdisk**.

Figure 9-6 Switchover of destination address



3. Click to upload a file.
4. Select a file and click to download a file.

Figure 9-7 Uploading files



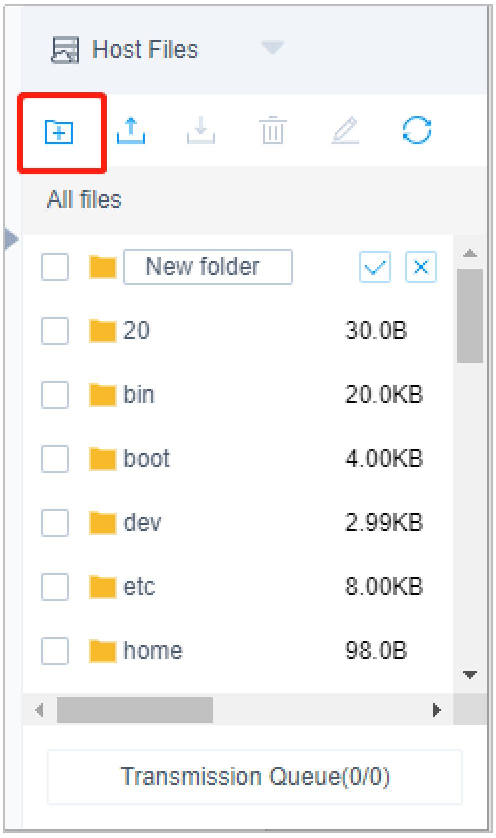
NOTE

- **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 9-8 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

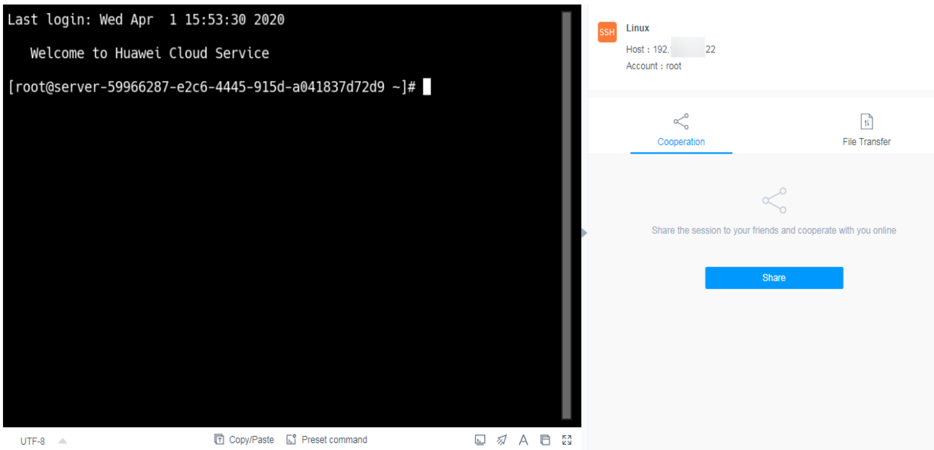
Session Window of Hosts Using the SSH or Telnet Protocol

Table 9-2 Linux host operations

Parameter	Description
Chinese code	The character protocol supports multiple Chinese character 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 9-9 Session window of hosts using the SSH protocol



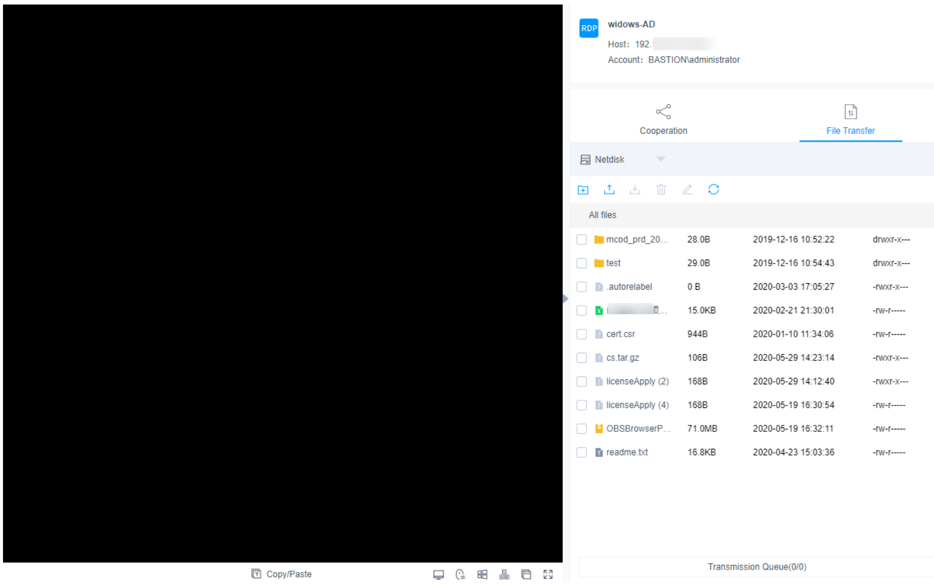
Session Window of Hosts Using the RDP or VNC Protocol

Table 9-3 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	**Ctrl+Alt+Delete**
Copy window	You can copy the current session window.
Full screen	Displays the window in full screen.

Figure 9-10 Session window of hosts using the RDP protocol



9.1.3 Logging In to Resources Using an SSH Client for O&M

CBH gives you the ability to use an SSH client to manage your host resources without changing your habits of using your original SSH client. In addition, 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.

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 login.
- Supported SSH clients include SecureCRT 8.0 or later, Xshell 5 or later, PuTTY, and MAC Terminal 2.0 or later.

Prerequisites

- You have the management permissions for the **Host Operation** 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.

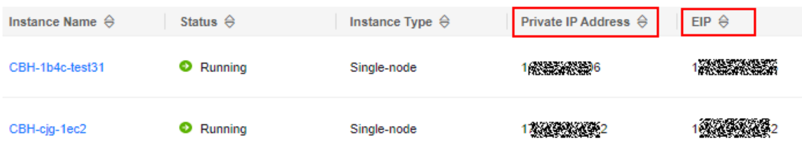
- Method 1
  a. Set **Protocol Type** to **SSH**, enter the elastic IP address of the CBH instance, set **Port** to **2222**, and click **OK**.
  b. Enter the username of the CBH instance and click **Connect**.
- Method 2:

  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

The ***system login IP address*** is the CBH IP address, which can be the private IP address or an EIP. 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**, select a user key from the **Browse** drop-down list, enter the password, and click **OK**.

  After the authentication is successful, the user can use the SSH client to log in to the CBH system without having to enter a password.

Step 4 Log in to the CBH system.

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 CBH system using the local password, select **OTP** and enter the dynamic token verification code.

Step 5 Import multiple 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.

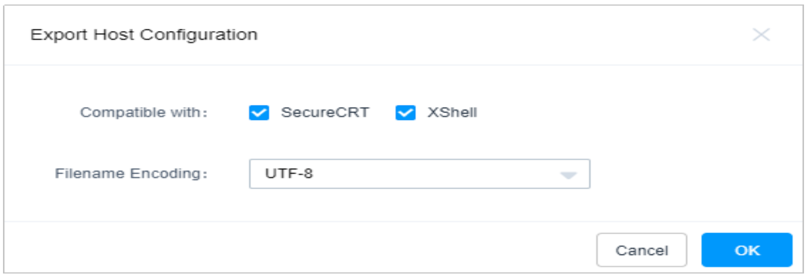
Step 1 Log in to the CBH system using a web browser.

Step 2 Choose **Operation** > **Host Operation** to go to the **Host Operation** page.

Step 3 Click **Export Host Configuration**.

Step 4 Select the configuration file of the client and click **OK** to download the configuration file.

Figure 9-11 Export Host Configuration



----End

9.1.4 Logging In to File Transfer Resources Using an FTP or SFTP Client

CBH allows you to use file transfer clients to transfer files between authorized managed hosts using the file transfer protocol. This means you can transfer files the way you are used to. All operations performed on a host resource are recorded by CBH for audit.

This topic describes how to obtain client login information and log in to resources that use a file transfer protocol.

Constraints

Only hosts with **Protocol** set to **FTP**, **SFTP**, or **SCP** can be logged in to using a web browser. Client tools must meet the requirements in the following table.

Host Protocol	Client Tool Required
SFTP	Xftp 6 or later, WinSCP 5.14.4 or later, and FlashFXP 5.4 or later
FTP Protocol	Xftp 6 or later, WinSCP 5.14.4 or later, FlashFXP 5.4 or later, and FileZilla 3.46.3 or later

Prerequisites

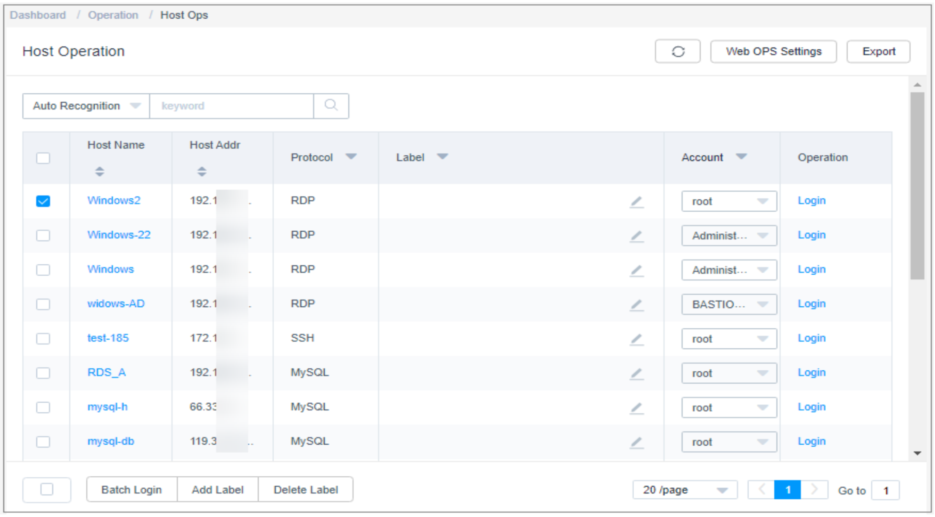
- You have the management permissions for the **Host Operation** module.
- You have obtained the access permissions for the resources.
- You have installed the client tool.
- The network connection between the managed host and the system is normal, and the account username and password for logging in 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**.

Procedure

Step 1 Obtain the login information.

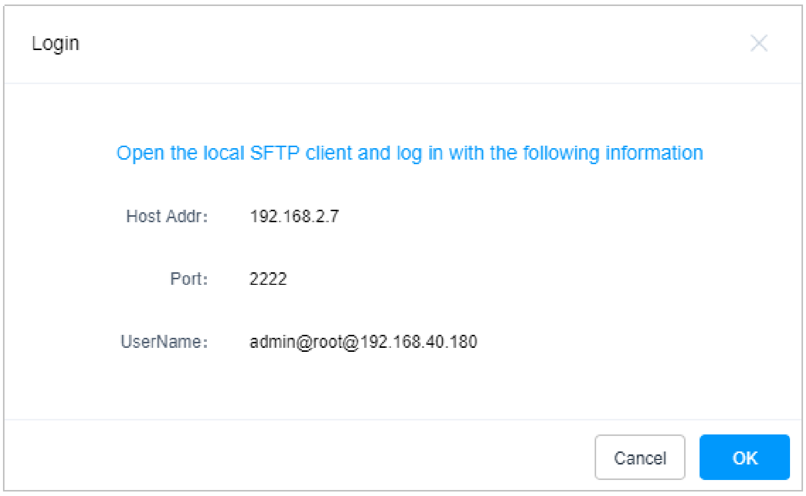
1. Log in to the CBH system.
2. Choose **Operation** > **Host Operation** to go to the **Host Operation** page.

Figure 9-12 Host Operation



3. Select an FTP or SFTP host resource, and click **Login**.

Figure 9-13 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

CBH allows you to use APIs to log in to hosts using the FTP or SFTP protocol.

Table 9-4 Parameter description

Parameter	Description
Host Addr	IP address for logging in to the CBH system
Port	Port number. The default port number is 2222.

Parameter	Description
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 CBH system.

----End

9.1.5 Logging In to and Maintaining Database Resources Using an SSO Client

CBH allows you to 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)

Constraints

- The database operation audit is available only in the CBH professional editions.
- Only MySQL, SQL Server, Oracle, DB2, PostgreSQL, and GaussDB databases can be managed.
- The client tool can be invoked only through SsoDBSettings.
- Only some database clients can be invoked through an SSO tool. For details, see the following table.

Table 9-5 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

Database Type	Version	Supported Client
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
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 databases and versions supported by CBH by yourselves.
- 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

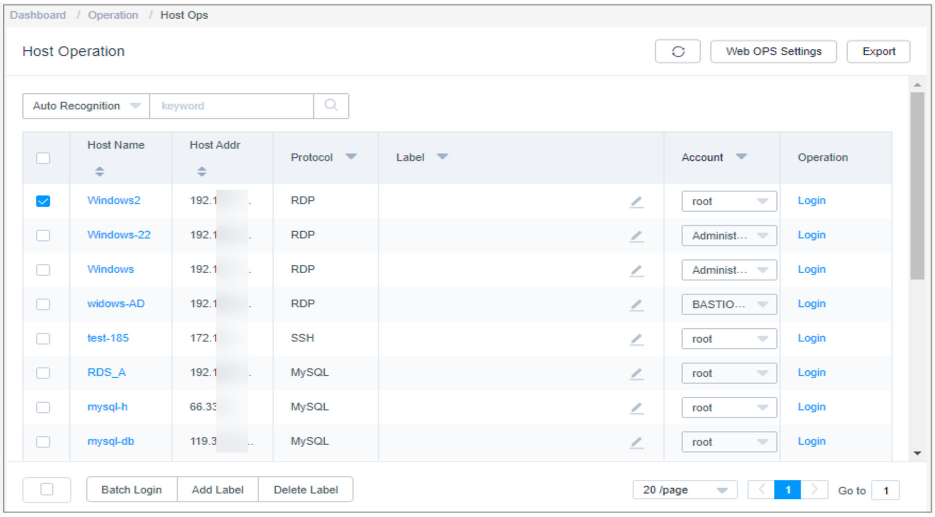
- You have the management permissions for the **Host Operation** module.
- You have obtained the access permissions for the resources.
- You have installed the client tool.
- The network connection between the managed host and the system is normal, and the account username and password for logging in to the managed host are correct.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **Operation** > **Host Operation** to go to the **Host Operation** page.

Figure 9-14 Host Operation



Step 3 Select a host resource of the database protocol type and click **Login**.

NOTE

- When you first time log in to the database, you will see the SsoDBSettings download window.
- The download tool varies depending on the CBH version you are using.

  For example, if you are using CBH V.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 local database client is automatically invoked.

Step 5 Log in to the database for operations.

----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 Operation** page of the CBH system. Then, you can log in to the database using the SSO tool.

----End

9.1.6 Logging In to Hosts in Batches for O&M

CBH also allows you to batch log in to multiple host resources for operation, including file transfer, file management, and command presetting. All operations performed on a host resource are recorded by CBH for audit.

This section describes how to log in to hosts in batches using a web browser.

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.

Prerequisites

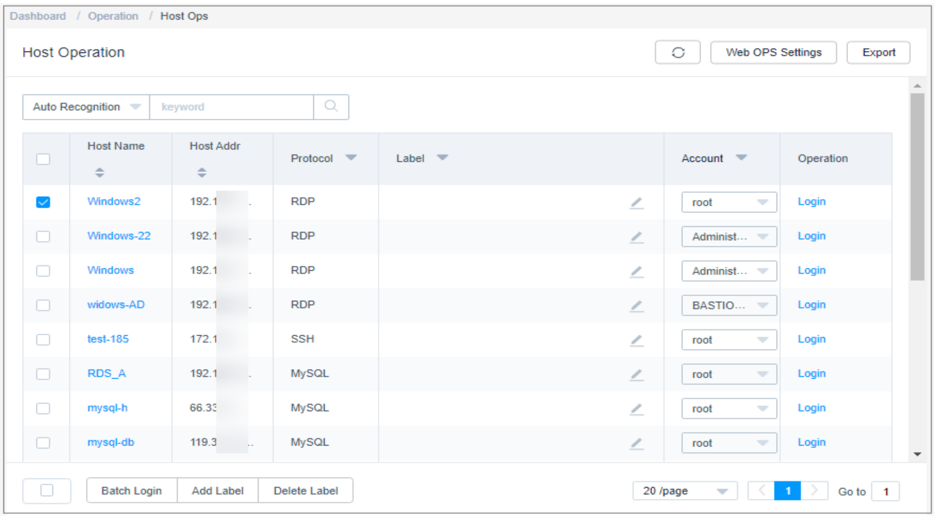
- You have the management permissions for the **Host Operation** module.
- You have obtained the access permissions for the resources.

Procedure

Step 1 Log in to the CBH system.

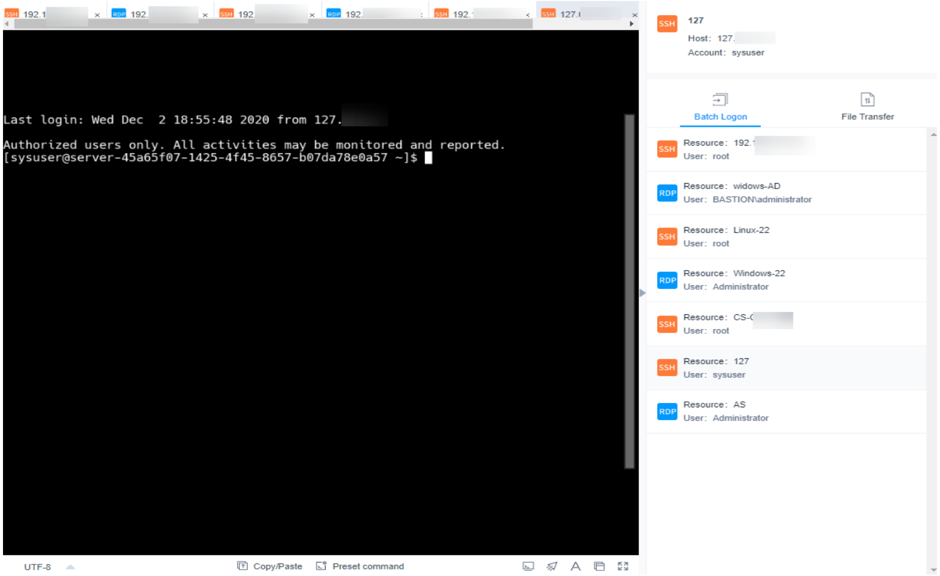
Step 2 Choose **Operation** > **Host Operation** to go to the **Host Operation** page.

Figure 9-15 Host Operation



Step 3 Select multiple resources and click **Batch Logon**.

Figure 9-16 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 Logging In**.

----End

9.1.7 File Transmission

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 CBH 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**.

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.

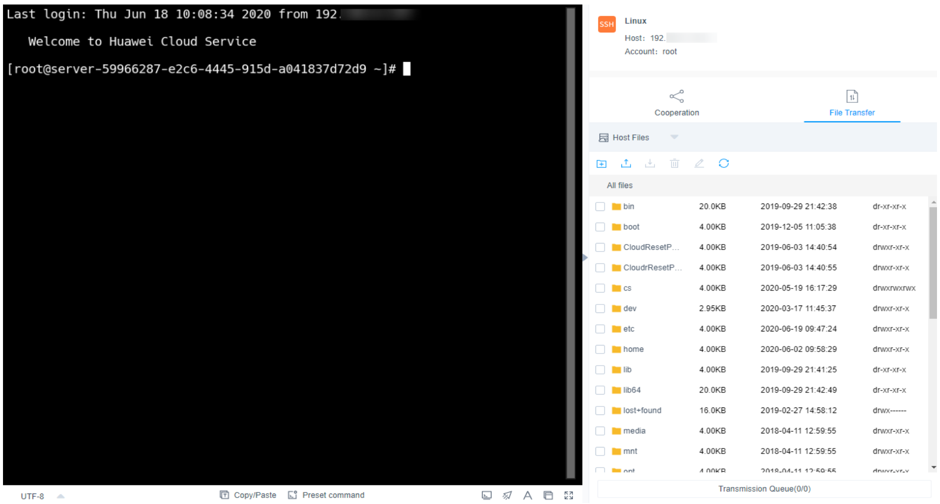
Step 1 Log in to the CBH system.

Step 2 Choose **Operation** > **Host Operation** and locate the target Linux host.

Step 3 Click **Login** to open the Linux host operation session.

Step 4 Click **File Transfer** to list the host files on a Linux host.

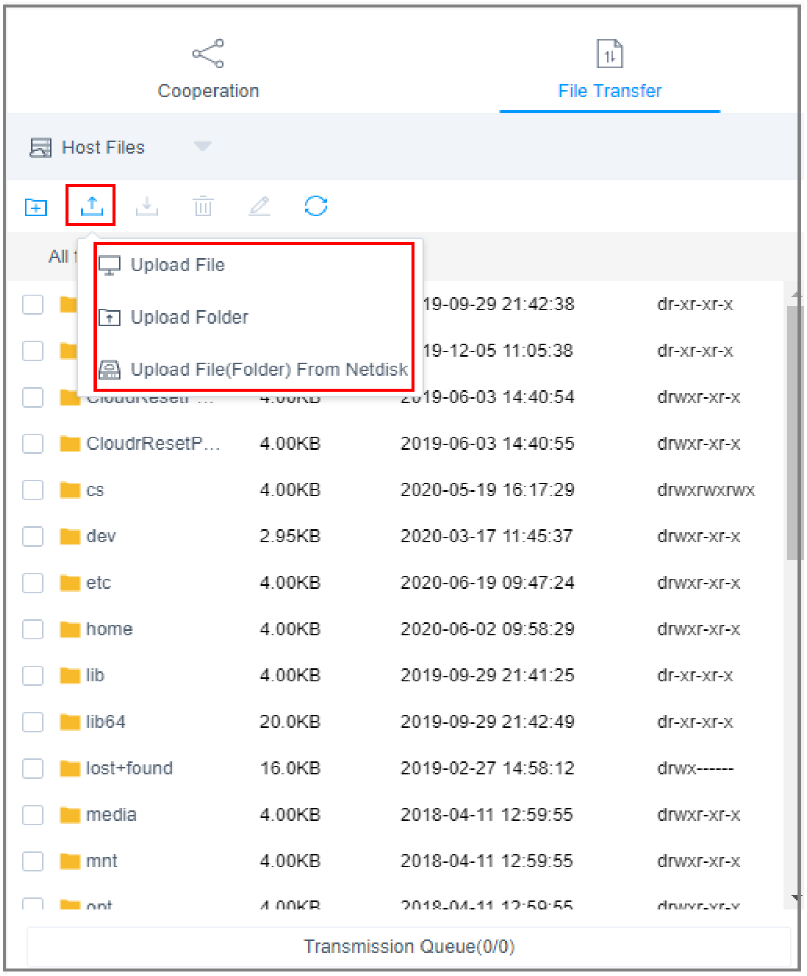
Figure 9-17 Linux host file transfer



Step 5 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.

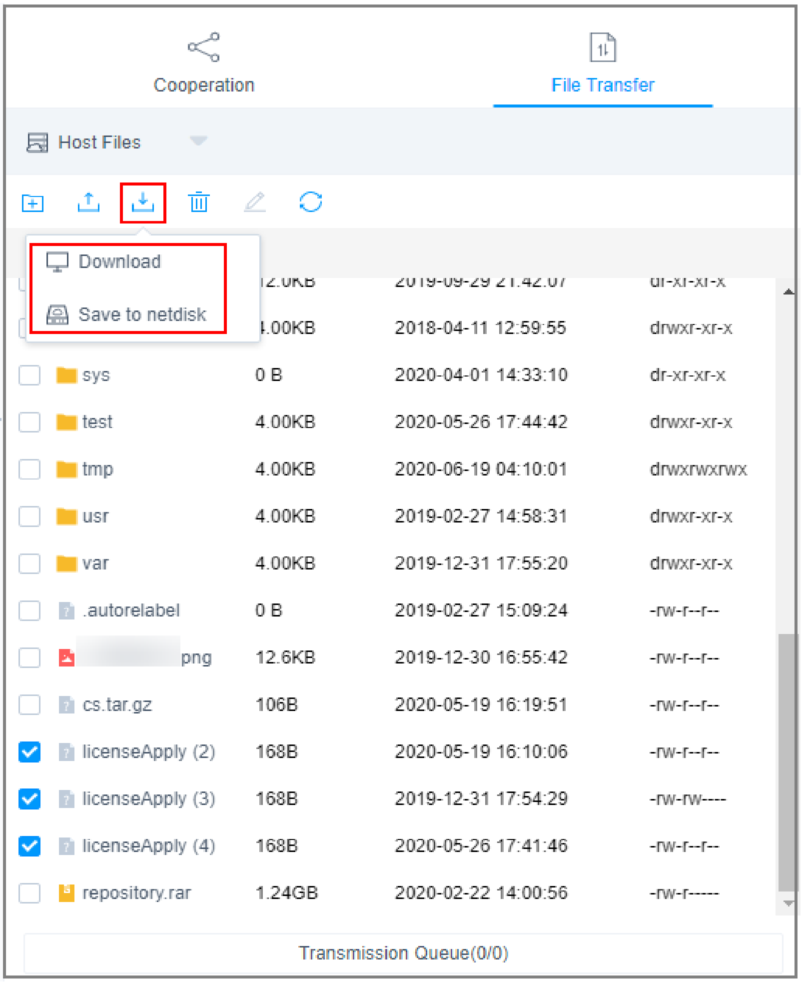
Figure 9-18 Uploading files to a Linux host



Step 6 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.

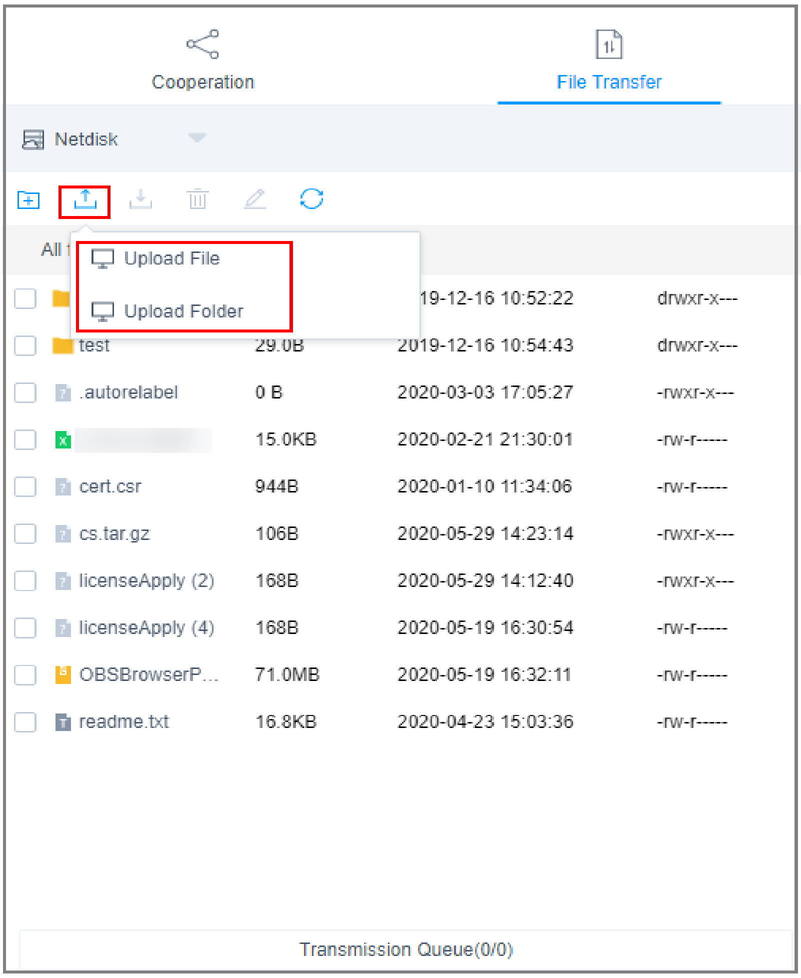
Figure 9-19 Downloading files from a Linux host



Step 7 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.

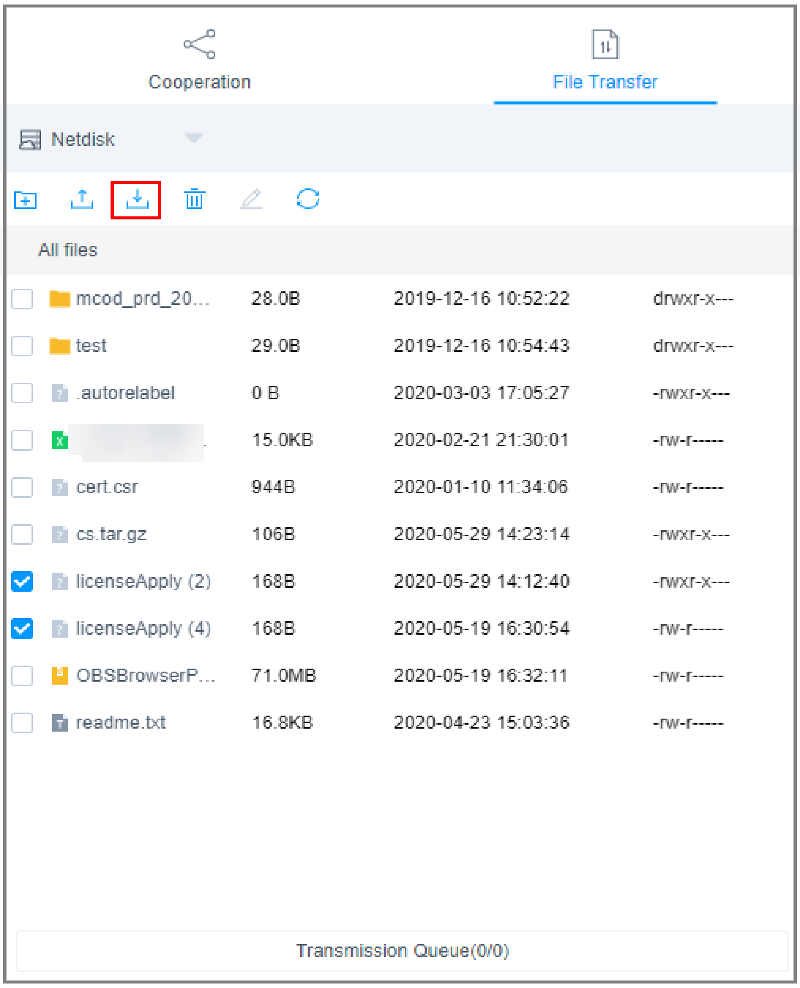
Figure 9-20 Uploading files to the personal net disk



Step 8 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 9-21 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.

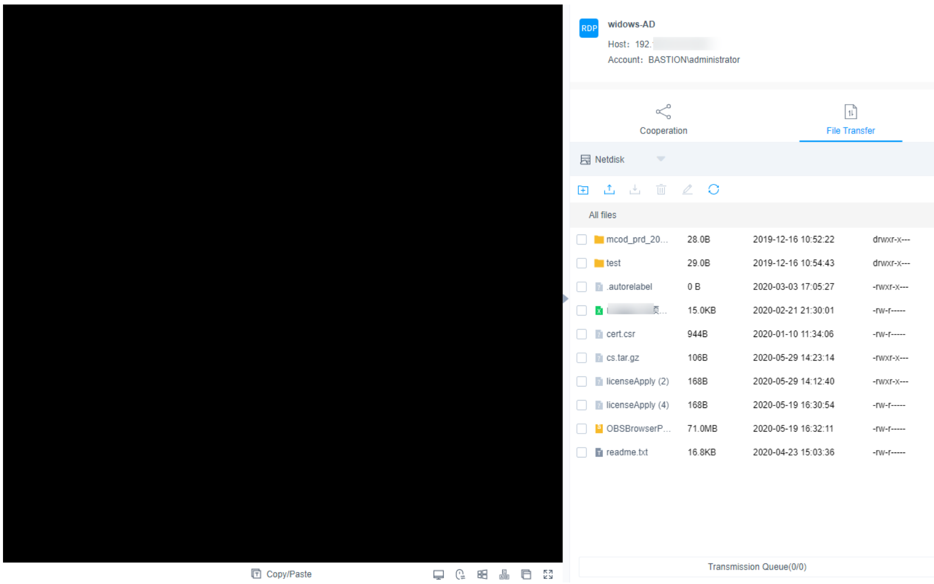
Step 1 Log in to the CBH system.

Step 2 Choose **Operation** > **Host Operation** 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.

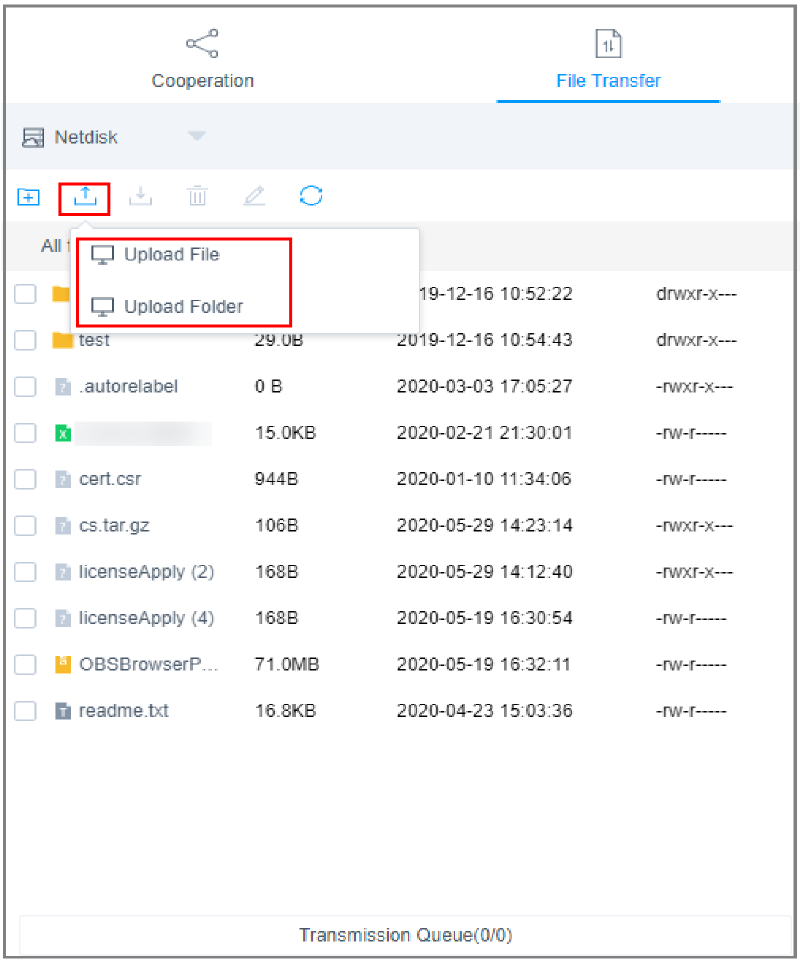
Figure 9-22 Windows host file transfer



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 9-23 Uploading files to the personal net disk



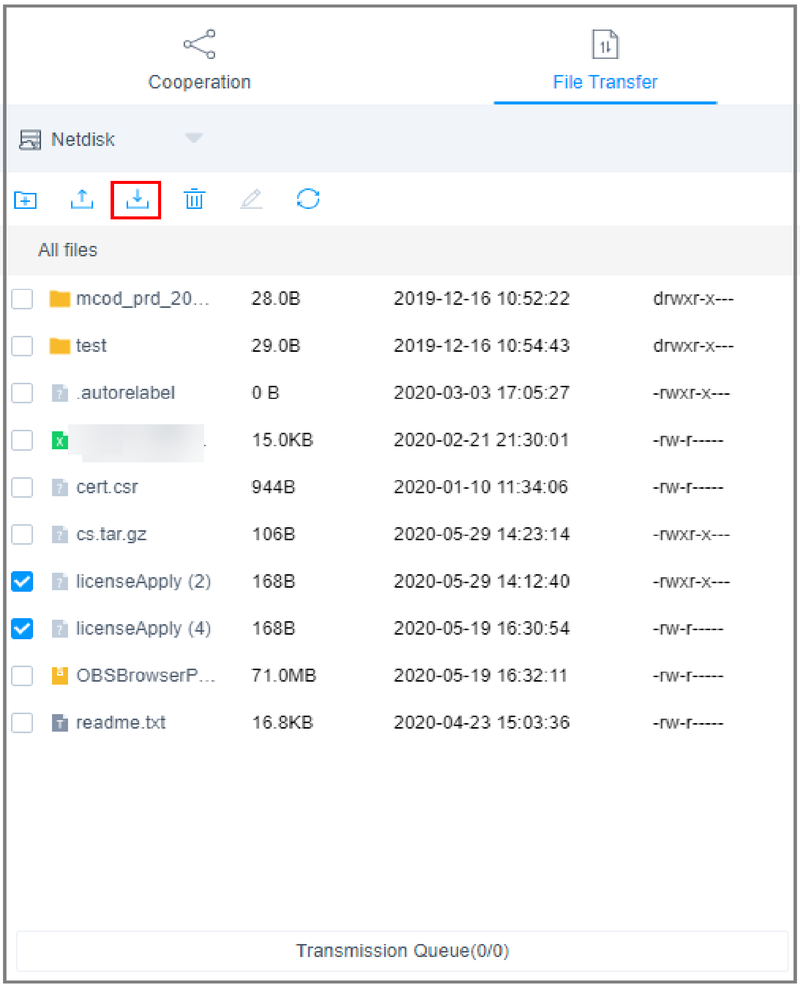
Step 6 Download files from the Windows host.

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 9-24 Downloading files from the personal net disk



----End

9.1.8 Cooperation

With the cooperation function, CBH allows a session creator to 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 CBH system 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

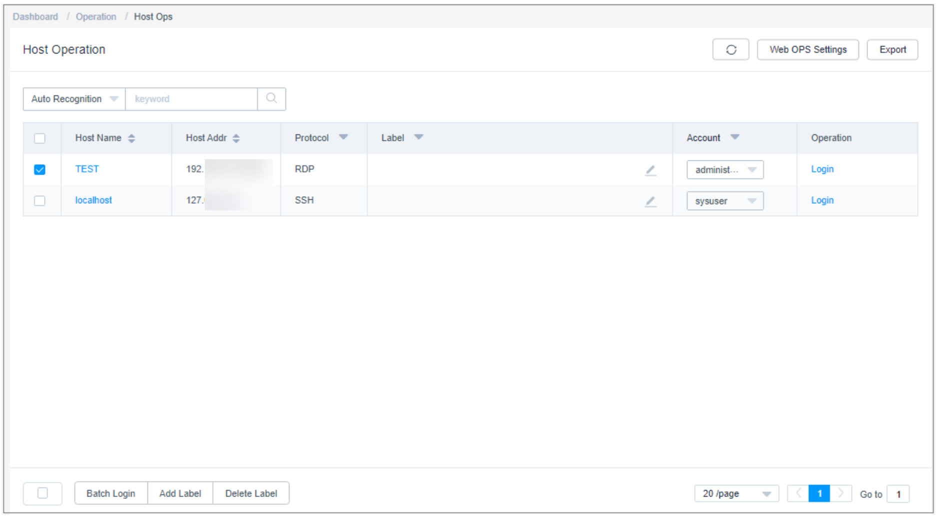
- You have the operation permissions for the host resources.
- You have logged in to the host using a web browser.

Procedure

Step 1 Log in to the CBH system.

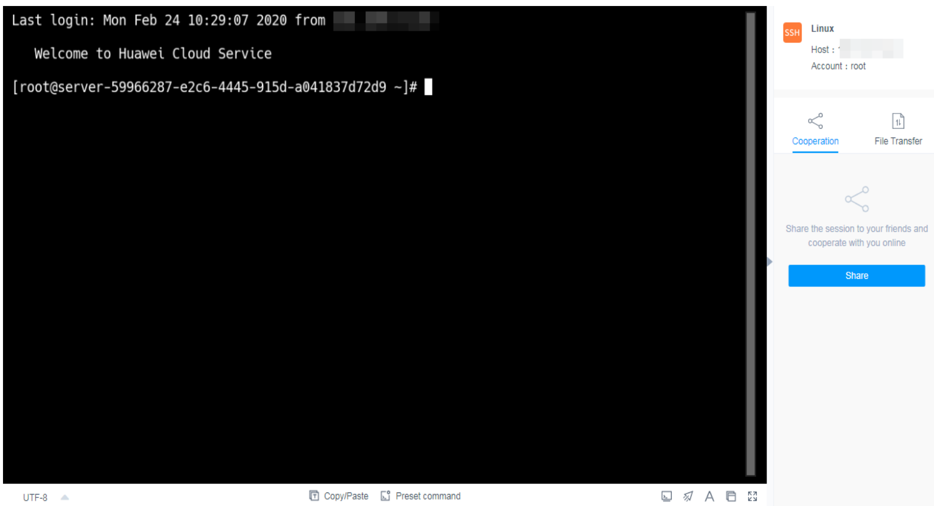
Step 2 Choose **Operation** > **Host Operation** to go to the **Host Operation** page.

Figure 9-25 Host Operation



Step 3 Select the host resource you want to operate and click **Login**.

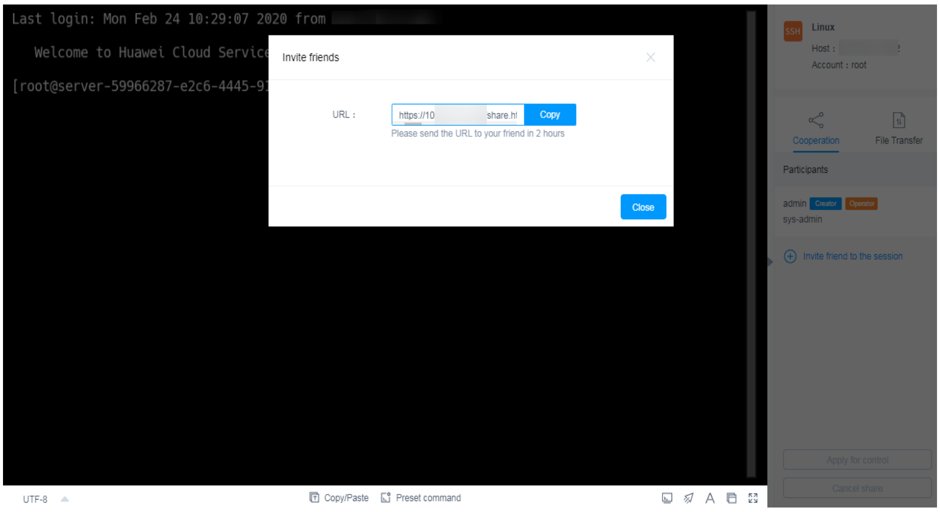
Figure 9-26 Host resource operation page



Step 4 Click **Share** on the right of the dialog box to invite other users to join the session.

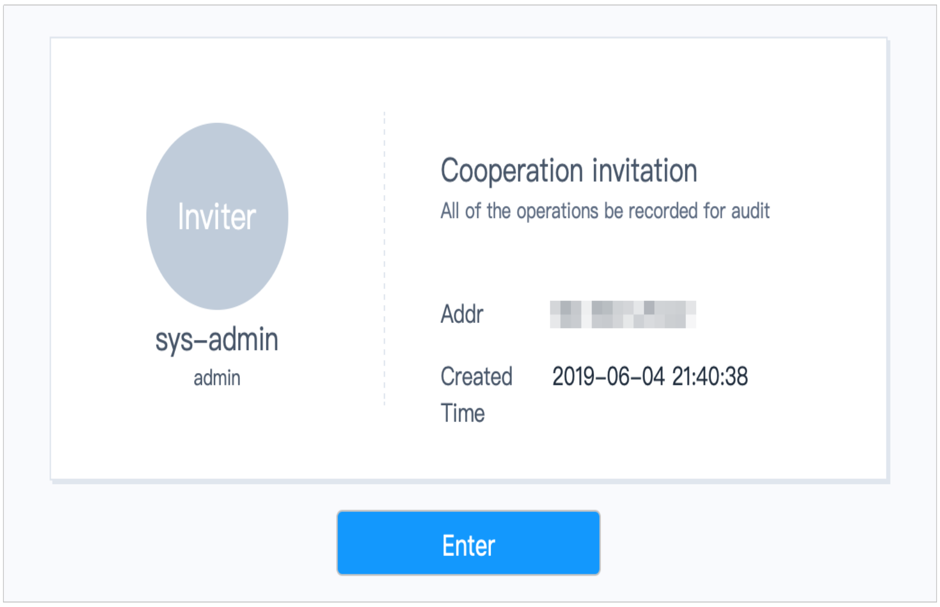
Step 5 Click **Invite friends** to obtain the invitation URL. Copy the URL and send it to the user who has permissions for account of the managed resource.

Figure 9-27 Obtaining the invitation URL



Step 6 The invited user then can log in to the CBH system, open the invitation URL, and view the invitation information.

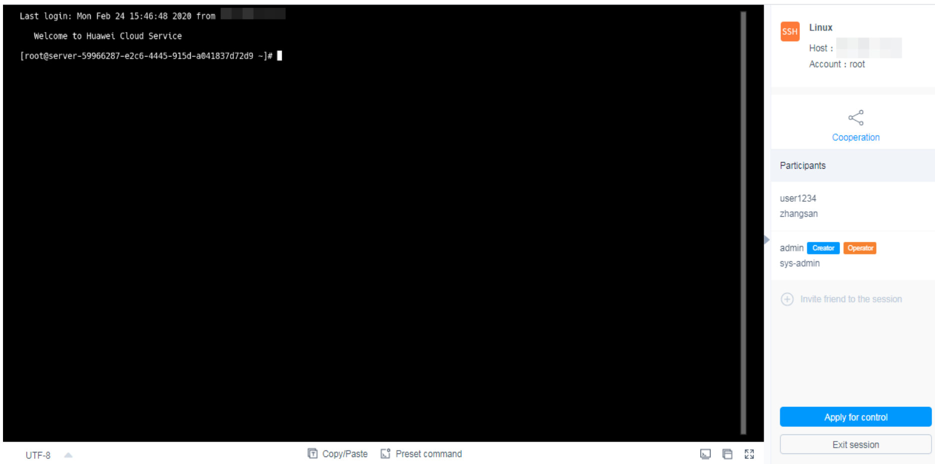
Figure 9-28 Invitation information displayed for the invited users



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.

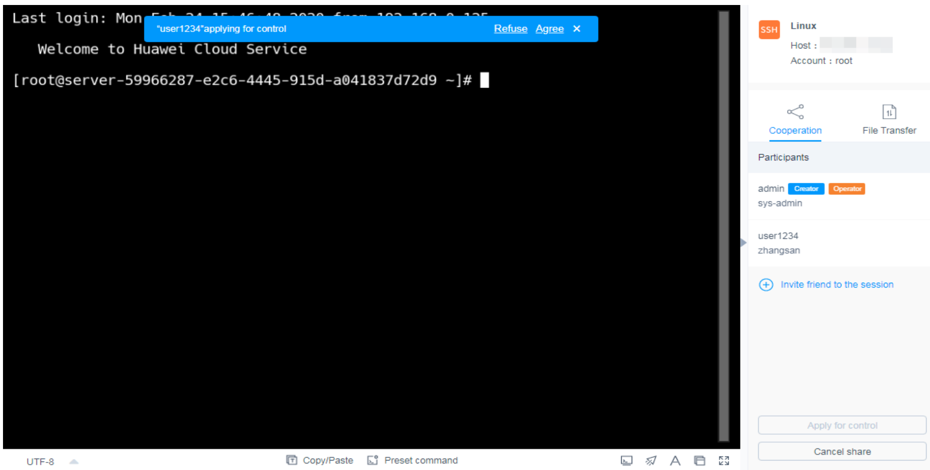
Figure 9-29 Cooperation session page of invited users



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 9-30 Cooperation session page of the inviter



----End

9.1.9 Enabling Forcible RDP Connections

When the number of Windows remote desktop connections exceeds the upper limit, you are not allowed to establish remote connections with the host resources. In this case, you can enable the **admin console** in the CBH system to implement force logins. This means you can force the CBH system to establish login connection 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.

Prerequisites

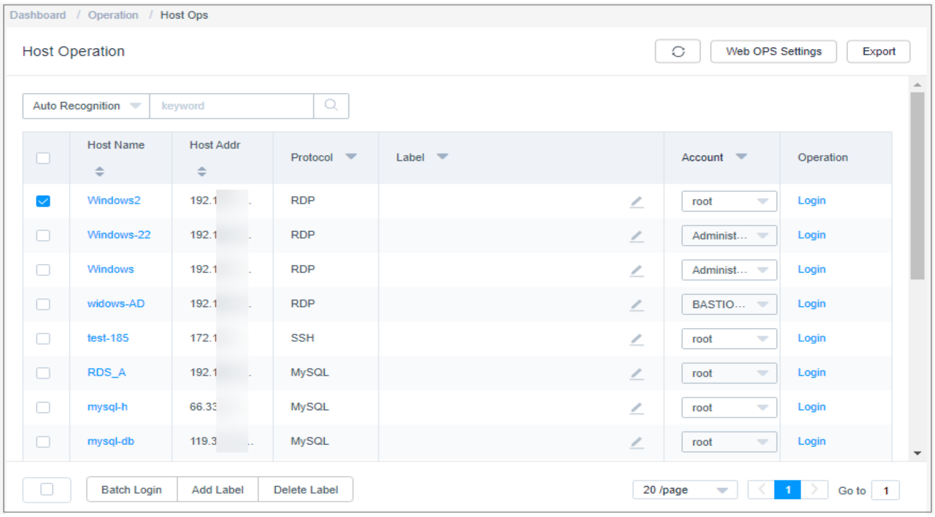
You have the management permissions for the **Host Ops** module.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **Operation** > **Host Operation** to go to the **Host Operation** page.

Figure 9-31 Host Operation



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 Operation** page.

After the configuration is successful, when a user attempts to log in to an RDP host, if the number of connections exceeds the upper limit, the user is forced to log in.

----End

9.2 Application Operation

9.2.1 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

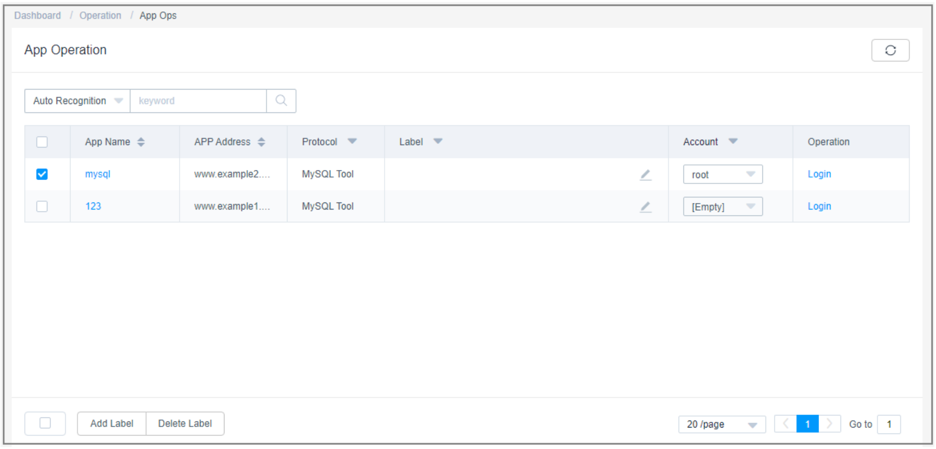
- You have the management permissions for the **App Operation** module.
- You have obtained the access permissions for the resources.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **Operation** > **App Operation** to go to the **App Operation** page.

Figure 9-32 App Operation



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.

Figure 9-33 Add Label

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 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 **App 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. In the displayed dialog box, confirm the deletion and click **OK**.

----End

9.2.2 Logging In to Application Resources Using a Web Browser 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. All operations performed on an application resource are recorded by CBH for audit.

- 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.

Constraints

- Currently, application operation is available only for the x86 CBH instances.
- 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.
  - Folders cannot be downloaded.
  - For application resources, only **Netdisk** can be select as the destination address.

Prerequisites

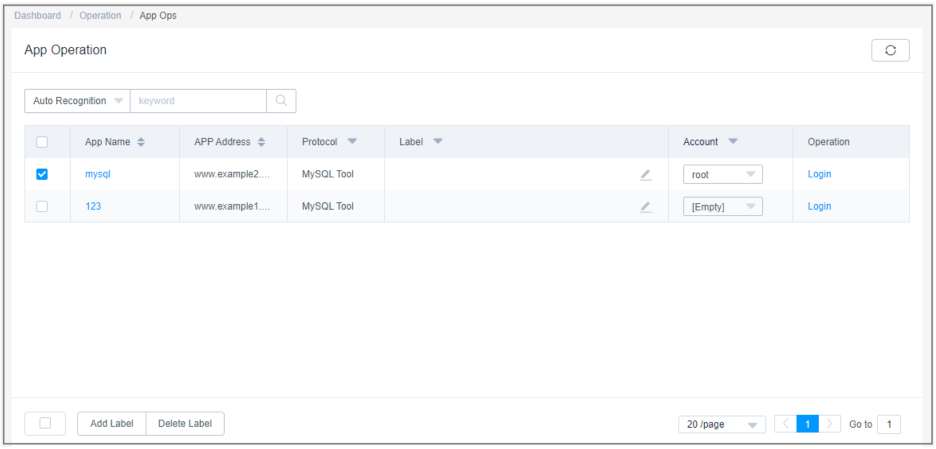
- You have the management permissions for the **App Operation** module.
- You have obtained the access permissions for the resources.
- The network connection between the application server and the system is normal, and the account username and password for logging in to the application server are correct.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **Operation** > **App Operation** to go to the **App Operation** page.

Figure 9-34 App Operation



Step 3 On the displayed page, select the application resource you want and click **Login** in the **Operation** column to open the session.

Figure 9-35 App operation session

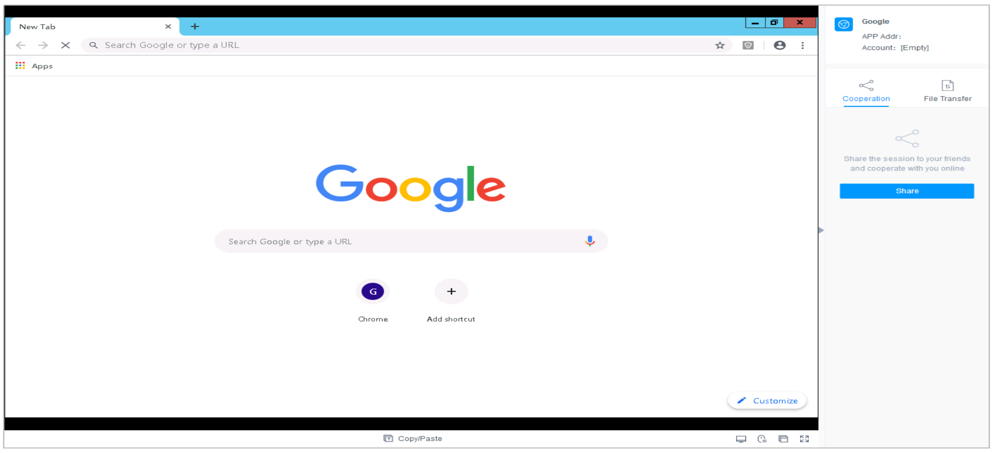


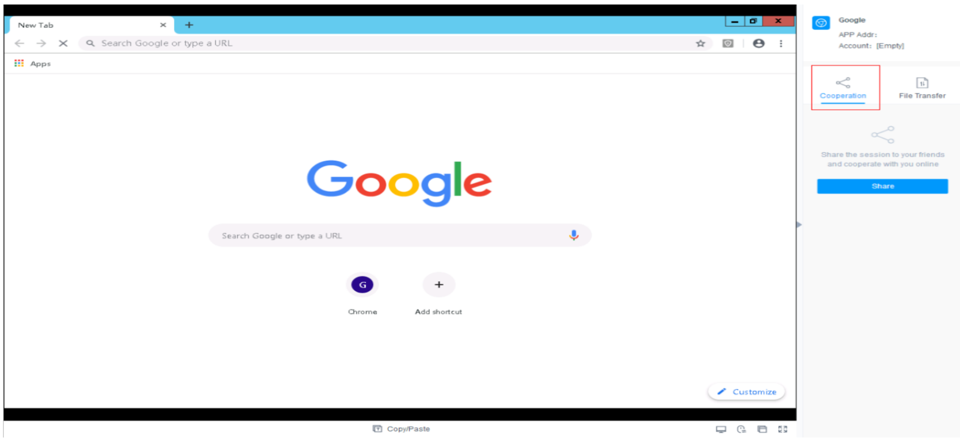
Table 9-6 Parameters for session operation

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.
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	**Ctrl+Alt+Delete**
Copy window	You can copy the current session window.
Full screen	Displays the window in full screen.

Step 4 Invite other system users to participate in the current session. For details, see **Cooperation**.

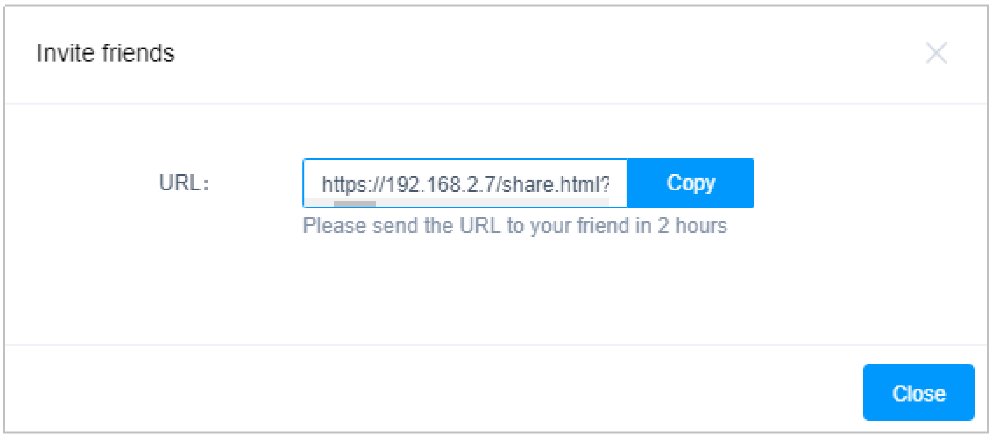
1. Click **Cooperation**. The collaborative session window is displayed.

Figure 9-36 Collaboration session page of the inviter



2. Click **Share**. Complete the information in the displayed **Invite friends** dialog box.

Figure 9-37 Collaboration session page of the inviter

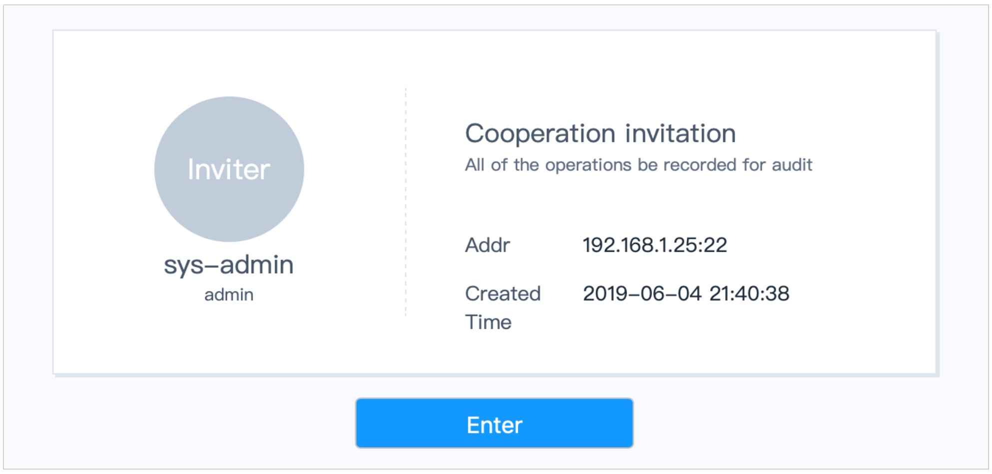


NOTE

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 CBH.
4. Log in to the CBH system as the invited user, open a new browser window, and paste the session link.

Figure 9-38 Collaborative session information



5. If you are invited, click **Enter** to join the session.

Figure 9-39 Collaboration session page of the inviter

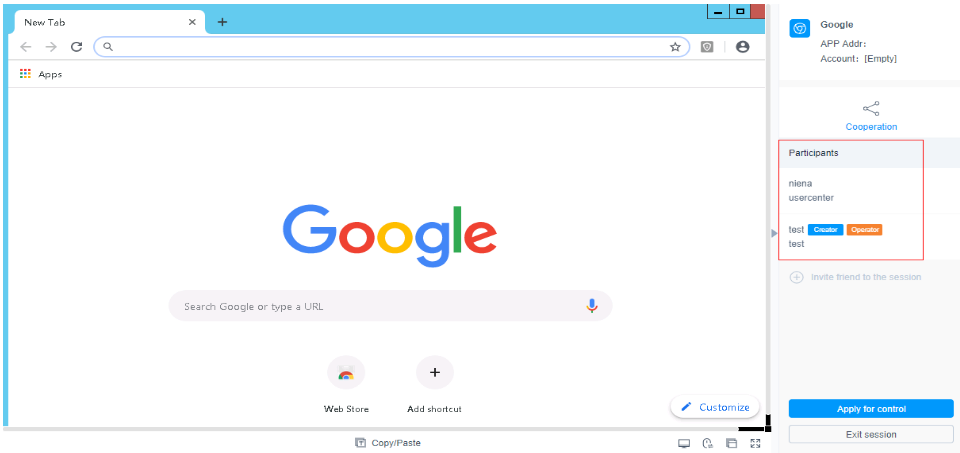


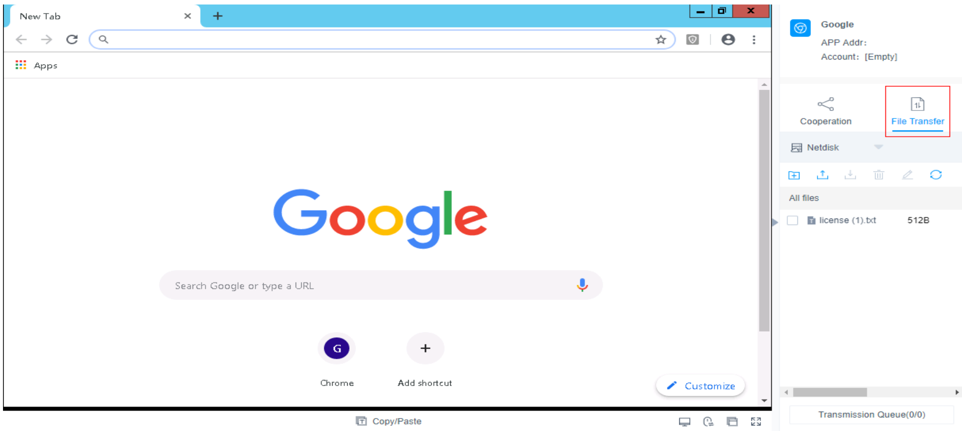
Table 9-7 Parameters for session operation

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**.

Click **File Transfer** to manage files or folders on the personal net disk.

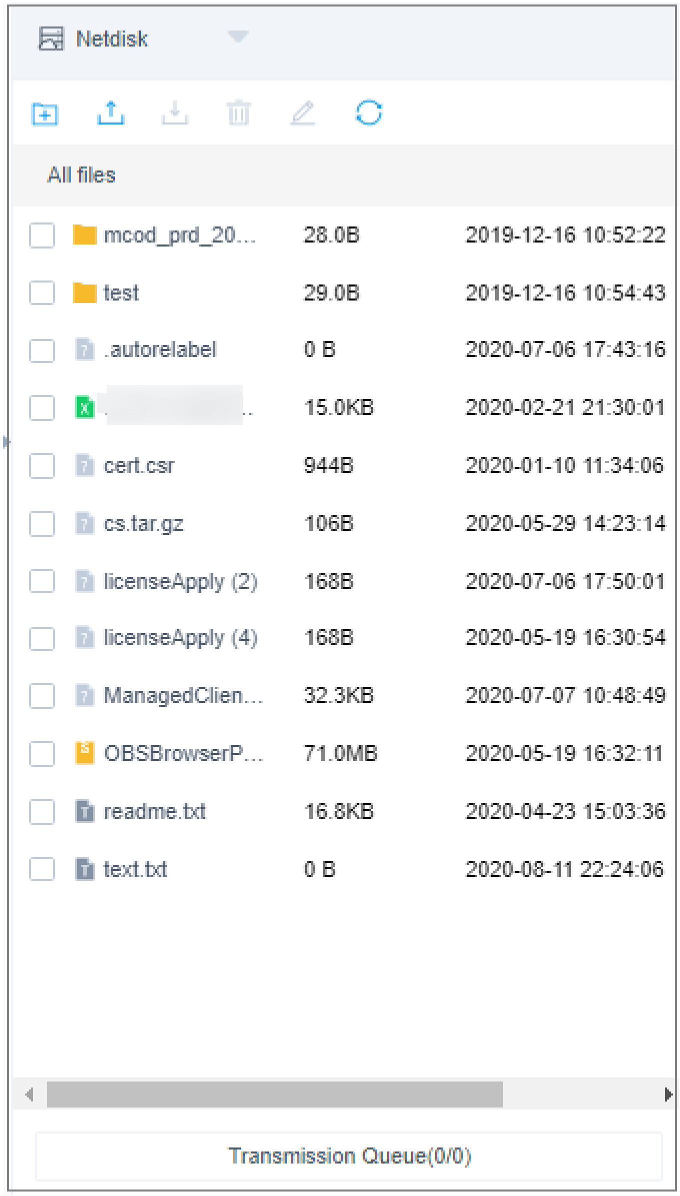
Figure 9-40 File Transmission



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 9-41 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

9.3 Cloud Service Operation

9.3.1 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

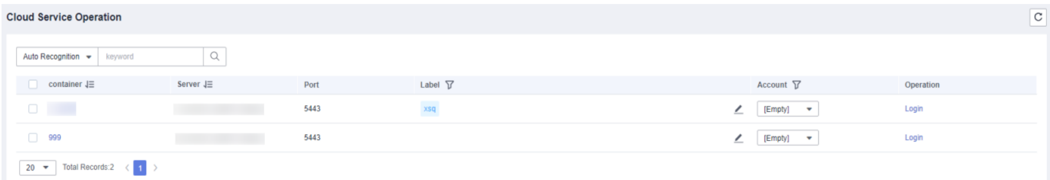
- You have the management permission for the **Cloud Service Operation** module.
- You have obtained the access permissions for the resources.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **Operation > Cloud Service Operation**. The host operation page is displayed.

Figure 9-42 Cloud service operation



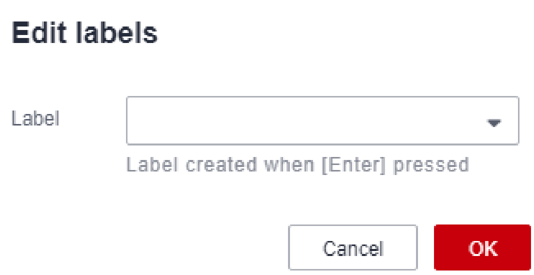
Step 3 Display container resources

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.

Figure 9-43 Add label



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

9.3.2 Logging In to Managed Resources Using a Web Browser for O&M Container

When you use a web browser for O&M, CBH provides **Cooperation**. All operations performed on a host resource are recorded by CBH for audit.

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.

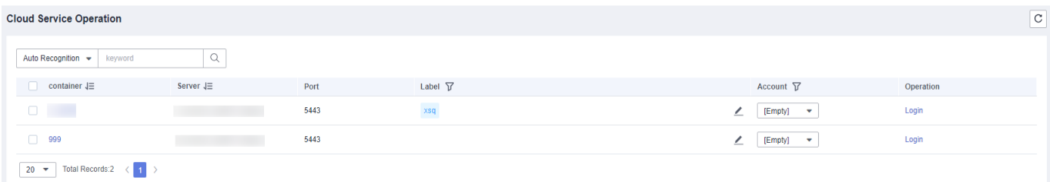
This section describes how to use a web browser to log in to a managed container.

Procedure

Step 1 Log in to the CBH system.

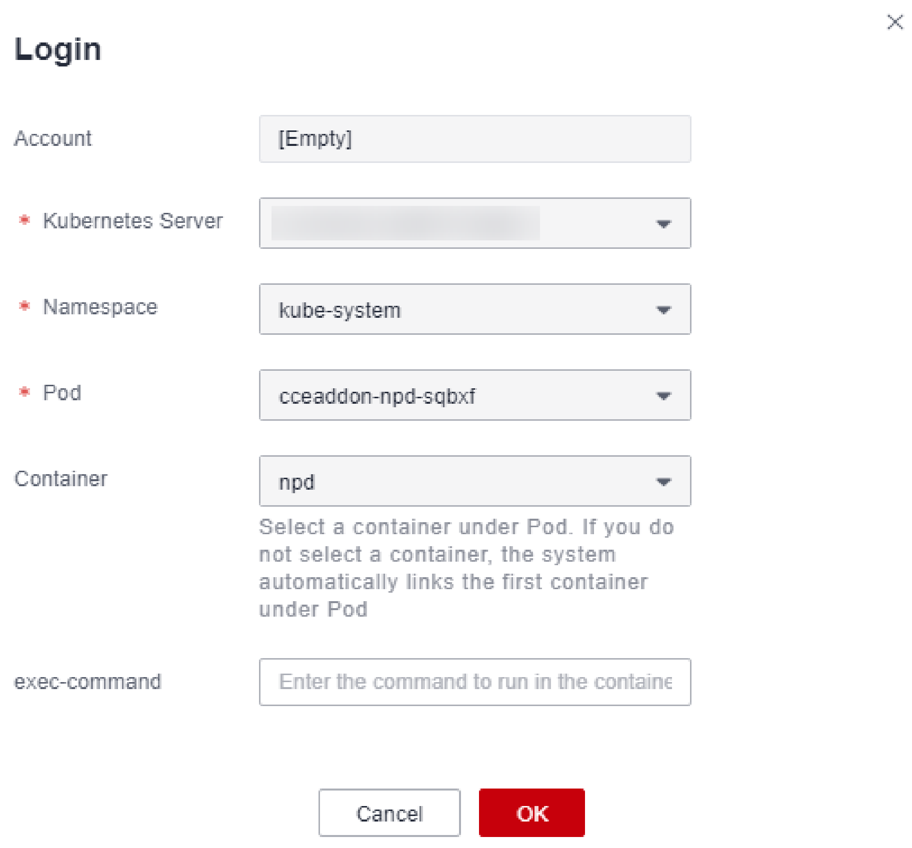
Step 2 Choose **Operation > Cloud Service Operation**. The host operation page is displayed.

Figure 9-44 Cloud service operation



Step 3 Select the container you want to log in and click **Login** in the **Operation** column to open the session.

Figure 9-45 Logging in to a container



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 of the CBH account can access the CBH system. 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 for CBH. Once they receive the link, they can log in to the CBH system, 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 9-8 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

9.4 Script Management

9.4.1 Creating a Script

CBH gives you the ability to manage scripts. You can execute scripts to perform complicated or repetitive operation tasks, improving O&M efficiency. CBH allows you to compile scripts online or import scripts by file.

This topic describes how to create a script.

NOTE

HSS-Agent automatic download and installation scripts have been built-in CBH.

Constraints

- Script management is available only in the CBH professional editions.
- Currently, you can manage Python and Shell scripts with CBH.
- Your scripts can be managed only by yourself and cannot be managed by other users in the CBH system.

Prerequisites

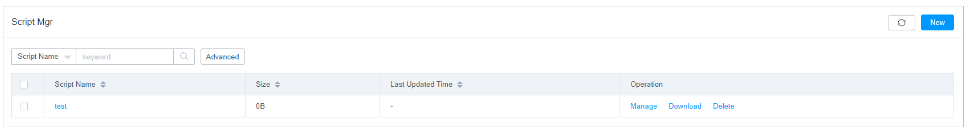
You have the management permissions for the **Script** module.

Procedure

Step 1 Log in to the CBH system.

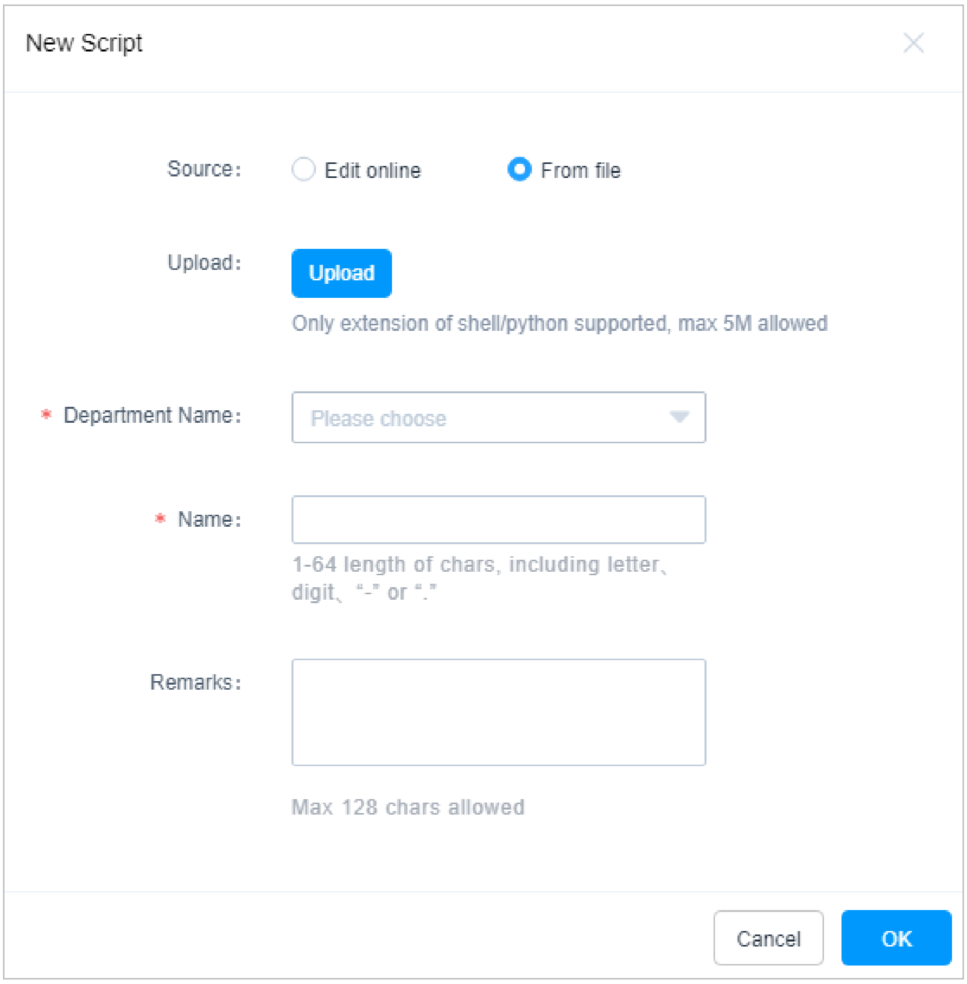
Step 2 Choose **Operation** > **Script** to go to the script management page.

Figure 9-46 List of scripts



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

Figure 9-47 New Script



Step 4 In the displayed **New Script** dialog box, configure the basic information about the script.

Table 9-9 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**: indicates that you can import an offline script file to form your script. The file cannot exceed 5 MB in size.
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.

Parameter	Description
Remarks	Brief script description

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**.

9.4.2 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**.

Prerequisites

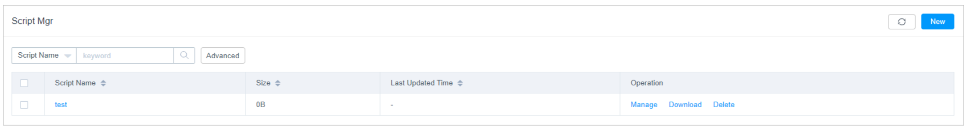
You have the management permissions for the **Script** module.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **Operation** > **Script** to go to the script management page.

Figure 9-48 List of scripts



Step 3 Query a script.

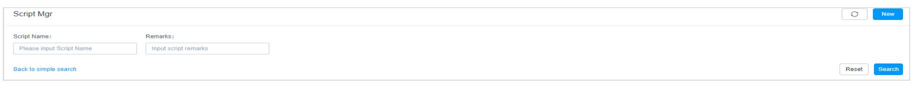
- Quick search

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

- Advanced search

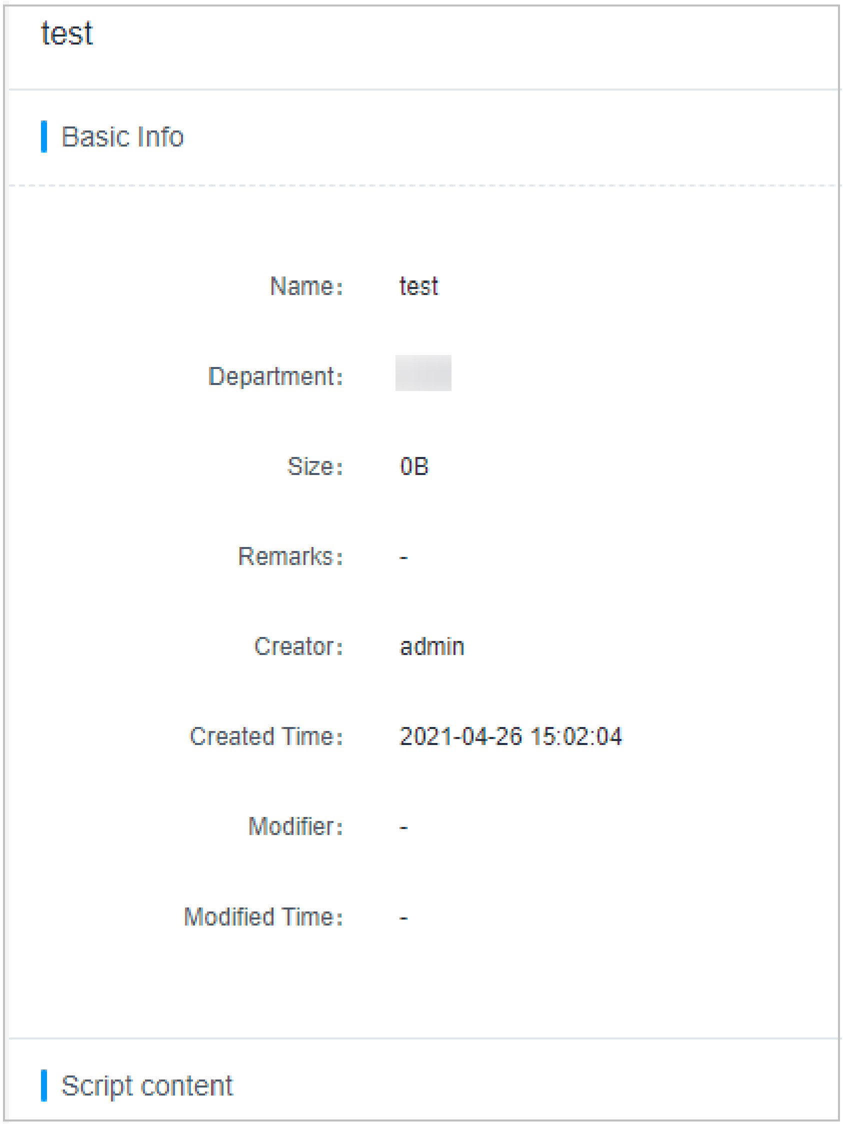
  Enter keywords in the corresponding attribute search boxes to search for scripts in exact mode.

Figure 9-49 Advanced search



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 9-50 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

9.4.3 Downloading a Script

This topic describes how to download a script for local query and management.

Prerequisites

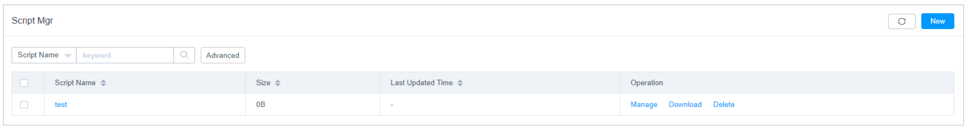
You have the management permissions for the **Script** module.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **Operation** > **Script** to go to the script management page.

Figure 9-51 List of scripts



Step 3 Select the script you want to download and click **Download** in the **Operation** column to download the script.

----End

9.4.4 Deleting a Script

This topic describes how to delete an online script and manage the scripts.

Prerequisites

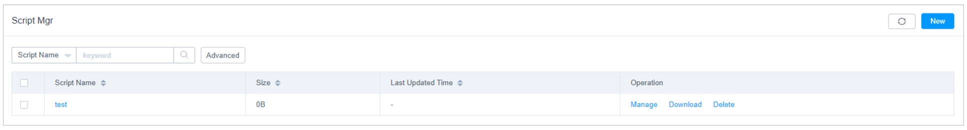
You have the management permissions for the **Script** module.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **Operation** > **Script** to go to the script management page.

Figure 9-52 List of scripts



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

9.5 Fast O&M

9.5.1 Managing Command Operation Tasks

CBH gives you the ability to manage multiple resources concurrently by executing commands, improving O&M efficiency. 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 available only in the CBH professional editions.
- 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

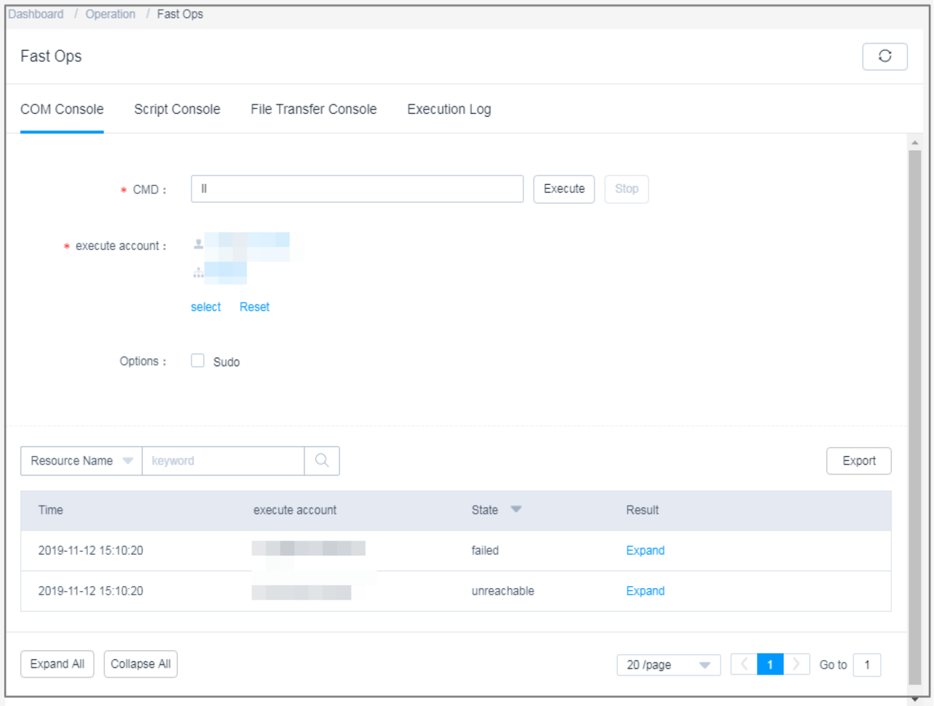
- You have the management permissions for the **Fast Ops** module.
- You have obtained the access permissions for the resources.
- The network connections between the managed hosts and the CBH system are normal.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **Operation** > **Fast Ops** > **COM Console** to go to the quick command OM page.

Figure 9-53 Command console



Step 3 Configure fast command operation information.

Table 9-10 Fast command operation parameters

Parameter	Description
CMD	Enter the command to be executed for host resources.
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) 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

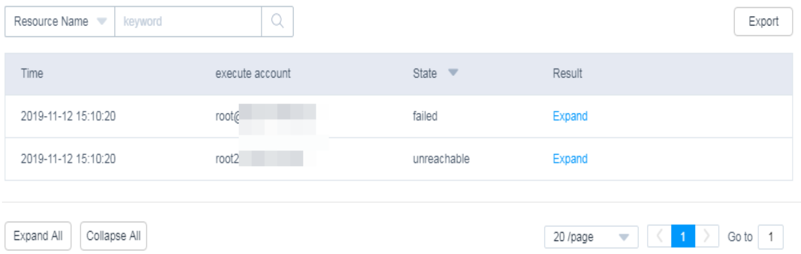
Stopping a task cannot stop the corresponding job that is being executed on a certain resource.

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, 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.

Figure 9-54 Command operation task results



----End

9.5.2 Managing Script Operation Tasks

CBH gives you the ability to manage multiple resources concurrently by executing scripts, improving O&M 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 available only in the CBH professional editions.
- 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

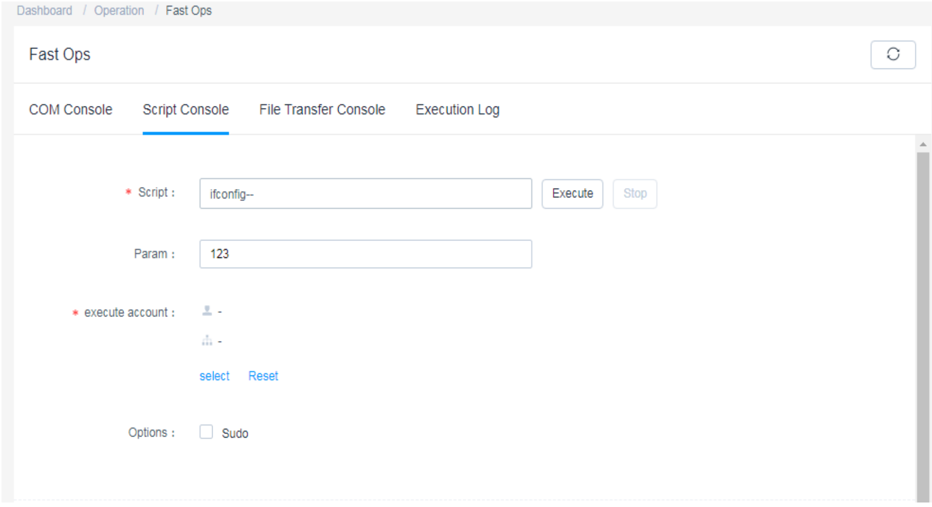
- You have the management permissions for the **Fast Ops** module.
- You have obtained the access permissions for the resources.
- The network connections between the managed hosts and the CBH system are normal.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **Operation** > **Fast Ops** > **Script Console** to go to the quick script operation page.

Figure 9-55 Script Console



Step 3 Configure fast script operation information.

Table 9-11 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	● 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) 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

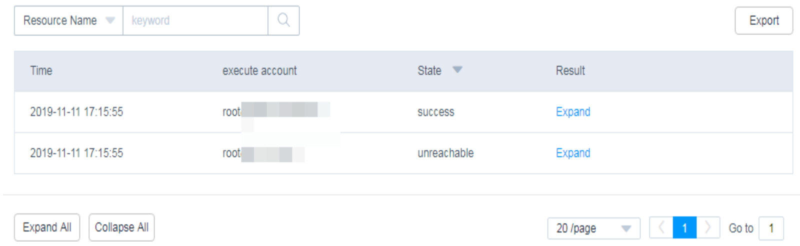
Stopping a task cannot stop the corresponding job that is being executed on a certain resource.

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, 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.

Figure 9-56 Script task results



----End

9.5.3 Managing File Transfer Tasks

CBH gives you the ability to quickly upload system disk files or local files to paths of multiple 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 available only in the CBH professional editions.
- 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

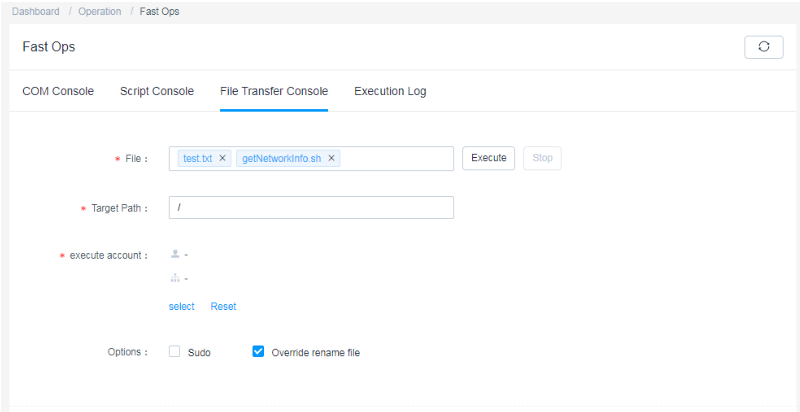
- You have the management permissions for the **Fast Ops** module.
- You have obtained the access permissions for the resources.
- The network connections between the managed hosts and the CBH system are normal.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **Operation** > **Fast Ops** > **File Transfer Console** to go to the **File Transfer Console** tab.

Figure 9-57 File Transfer Console



Step 3 Configure fast file transfer information.

Table 9-12 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

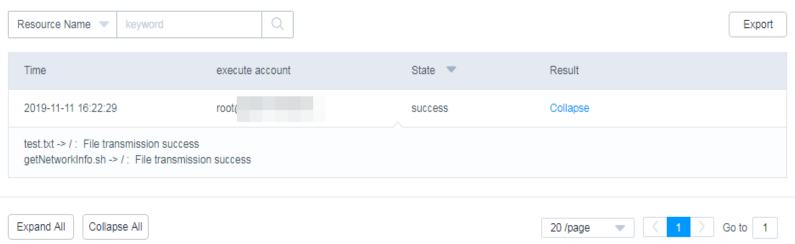
Stopping a task cannot stop the job that is being executed until the job is done.

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, 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.

Figure 9-58 File transfer task results



----End

9.5.4 Managing Fast Operation Task Execution Logs

This topic describes how to manage execution logs after fast operation tasks are executed, including viewing task details, exporting execution logs, and deleting execution logs.

Prerequisites

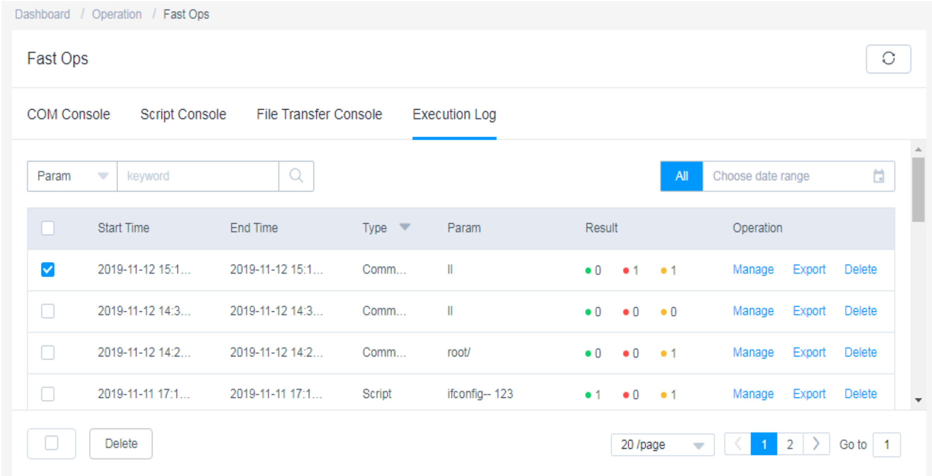
- You have the management permissions for the **Fast Ops** module.
- Fast operation tasks (including fast command tasks, script tasks, and file transfer tasks) have been executed.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **Operation** > **Fast Ops** > **Execution Log** to go to the **Execution Log** tab.

Figure 9-59 Execution logs



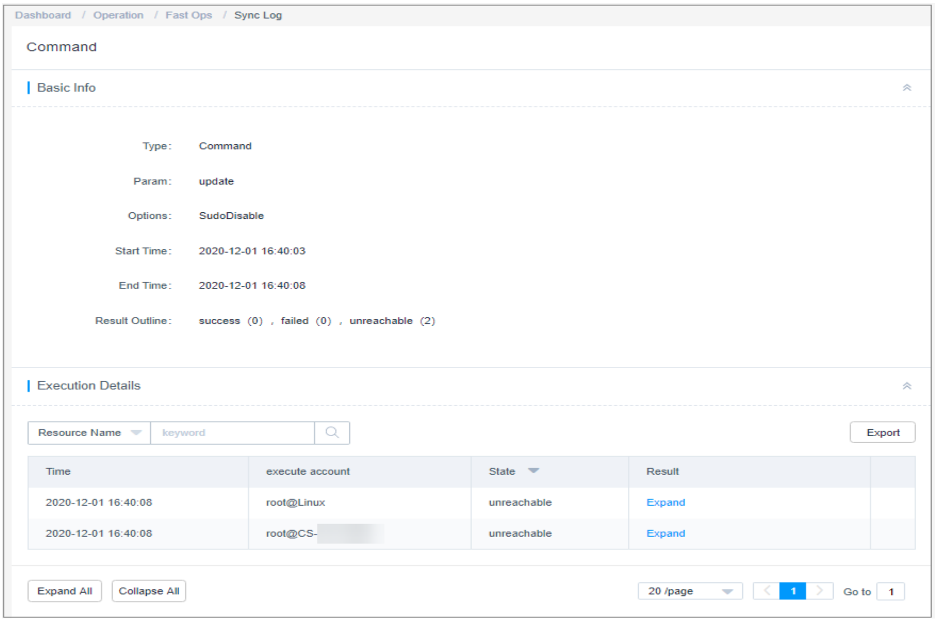
Step 3 Query logs.

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 9-60 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

9.6 OM Task

9.6.1 Creating an OM Task

CBH allows you to create OM tasks that will be automatically executed. After you create an OM task, the system automatically executes 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 multiple designation hosts. With the fast OM function, CBH 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 available only in the CBH professional editions.
- 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

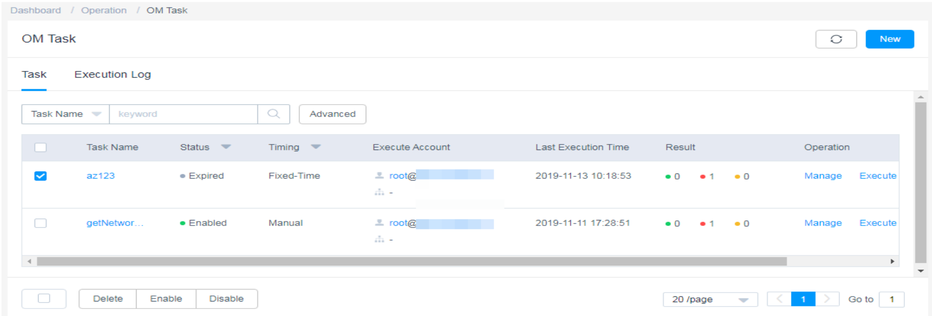
- You have the management permissions for the **OM Task** module.
- You have obtained the access permissions for the resources.
- The network connections between the managed hosts and the CBH system are normal.

Creating an Automated Operation Task

Step 1 Log in to the CBH system.

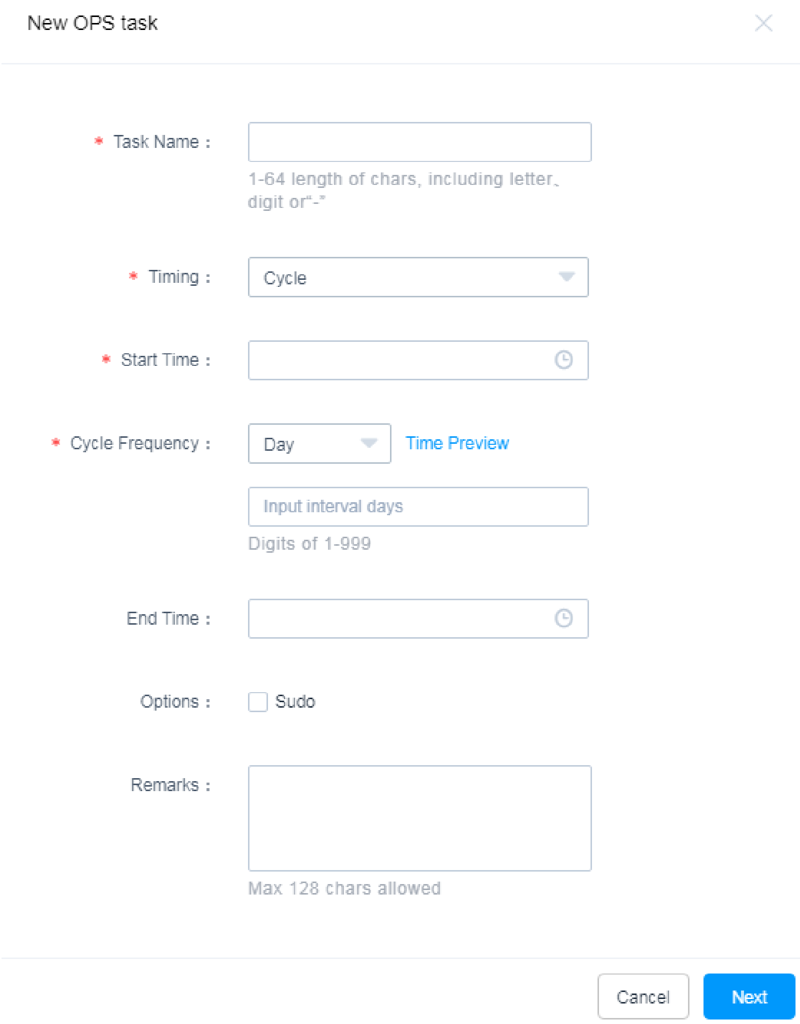
Step 2 Choose **Operation** > **OM Task** > **Task**.

Figure 9-61 Operation task list



Step 3 Click **New** in the upper right of the **OM Task** area.

Figure 9-62 Creating an OM Task



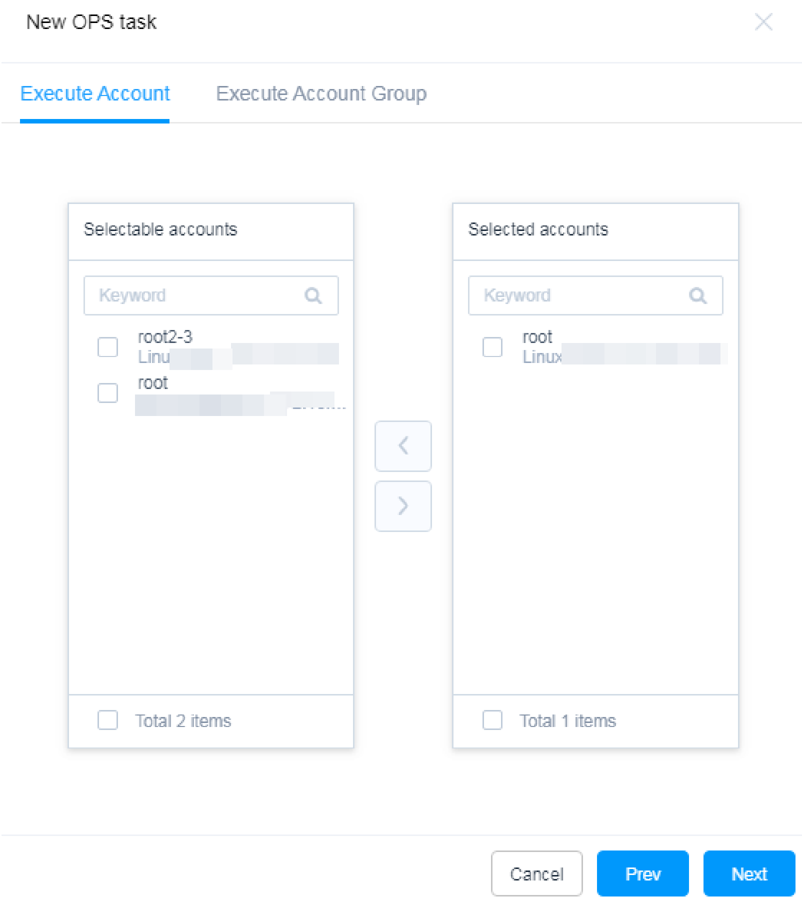
Step 4 Configure basic information about the task.

Table 9-13 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 change rule is triggered periodically.
Execute Time	Date when the task is periodically executed. The default execution time is at 00:00 every day.
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.

Figure 9-63 Configuring execution accounts



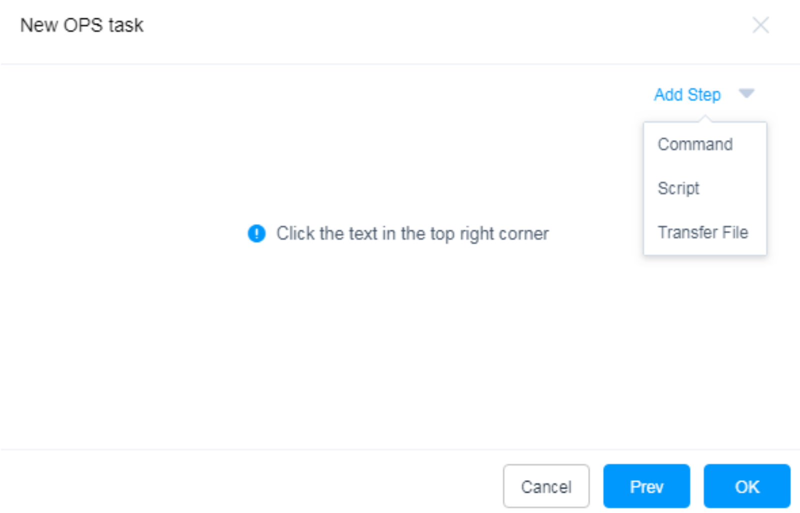
Step 6 Click **Next** and set task steps.

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.

Figure 9-64 Configuring task steps



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.

9.6.2 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 the CBH system.

Step 2 Choose **Operation** > **OM Task** > **Task**.

Step 3 Query OM tasks.

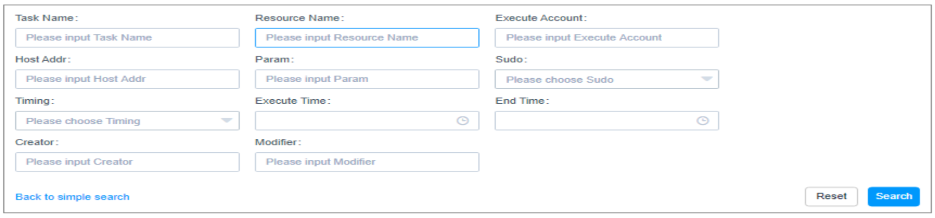
- Quick search

  Enter a keyword in the search box to quickly query tasks by task name, resource name, and execution account.

- Advanced search

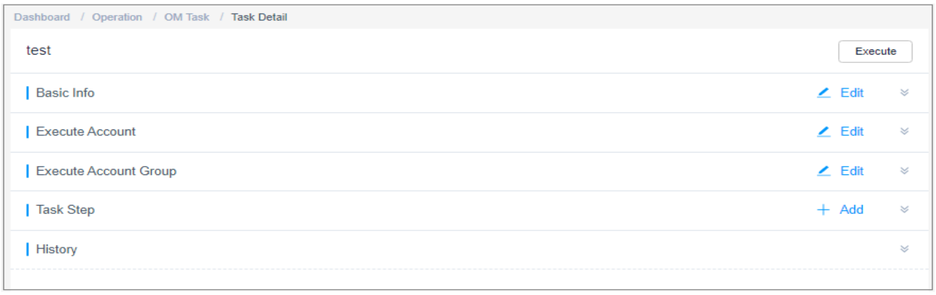
  Enter keywords in the corresponding attribute search boxes to search for tasks in exact mode.

Figure 9-65 Advanced search



Step 4 Click the name of the task or click **Manage** in the **Operation** column of the task row.

Figure 9-66 Viewing details of an OM task



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.

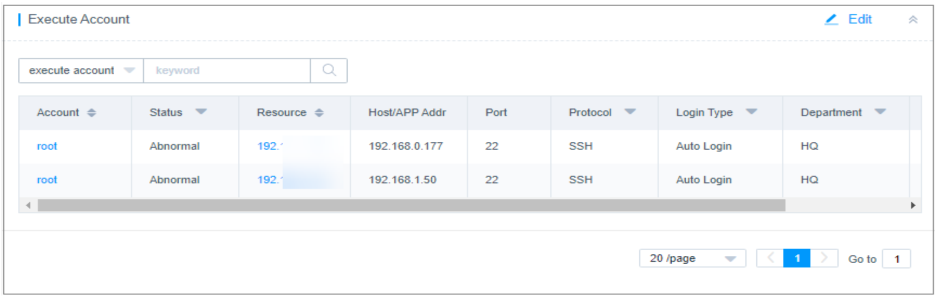
- You can edit **Task Name** and **Timing**.

Figure 9-67 Viewing basic information

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.

Figure 9-68 Viewing execution accounts



Step 7 In the displayed dialog box, view and edit basic information of the execution account.

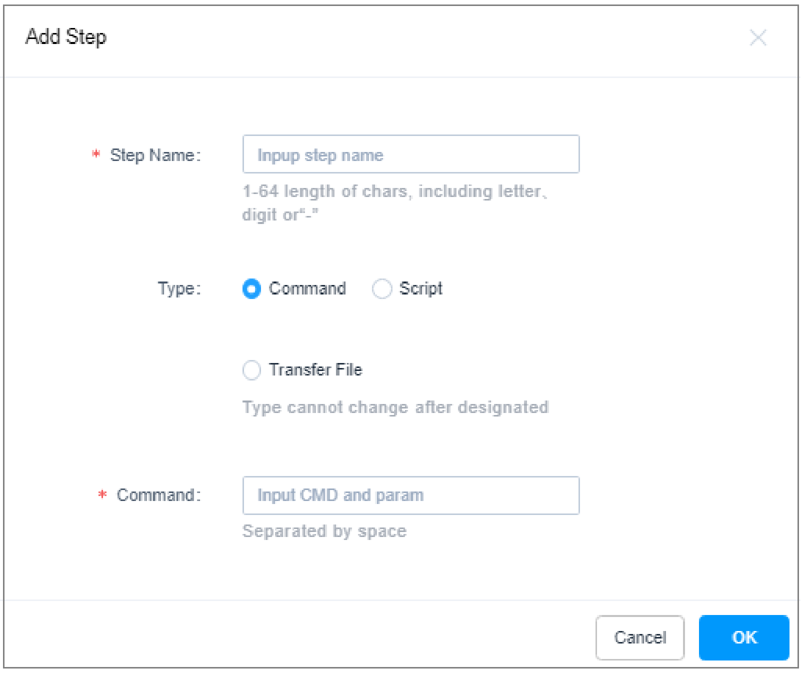
- To add or delete an execution account group, click **Edit** in the **Execute Account Group** area and complete modifications in the displayed dialog box.
- To only remove an execution account group, click **Remove** in the row of the execution account group. Each account in the removed account group cannot be used for executing OM tasks on the corresponding host.

Figure 9-69 Viewing execution account groups

Step 8 In the displayed OM task dialog box, view and edit task steps.

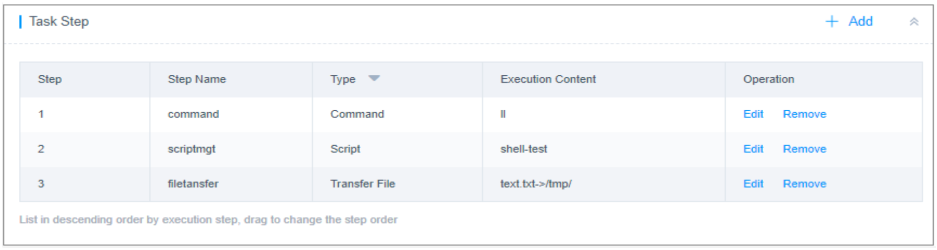
- In the **Task Step** area, click **Add**. In the displayed **Add Step** dialog box, add one or more task steps as needed.

Figure 9-70 Add Step



- 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.

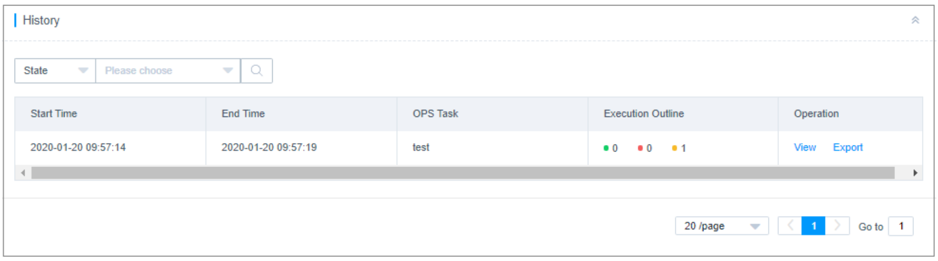
Figure 9-71 Viewing task steps



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.

Figure 9-72 Viewing execution results



----End

9.6.3 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

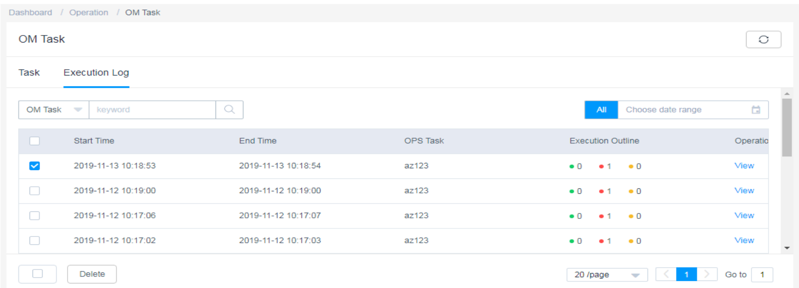
You have the management permissions for the **OM Task** module.

Viewing Log Details

Step 1 Log in to the CBH system.

Step 2 Choose **Operation** > **OM Task** > **Execution Log** to go to the task list page.

Figure 9-73 OM task execution logs



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.

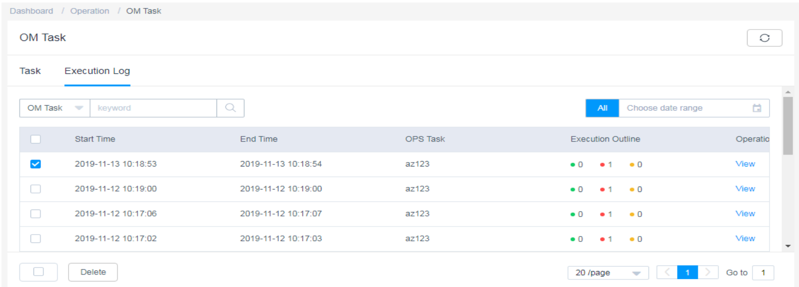
----End

Downloading OM Task Execution Logs

Step 1 Log in to the CBH system.

Step 2 Choose **Operation** > **OM Task** > **Execution Log** to go to the task list page.

Figure 9-74 OM task execution logs



Step 3 Select the task you want and click **Download** in the **Operation** column to download the execution log 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.

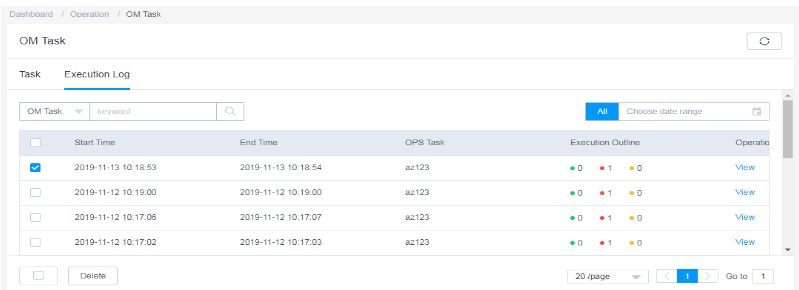
----End

Deleting Execution Logs

Step 1 Log in to the CBH system.

Step 2 Choose **Operation** > **OM Task** > **Execution Log** to go to the task list page.

Figure 9-75 OM task execution logs



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

10 Audit

10.1 Live Session

10.1.1 Viewing Live Sessions

After a system user logs in to a resource through CBH, you, the audit administrator, will receive session records in real time. It enables you to view and audit live operation sessions to prevent losses caused by violations.

This topic walks you through how to query and view live sessions.

Prerequisites

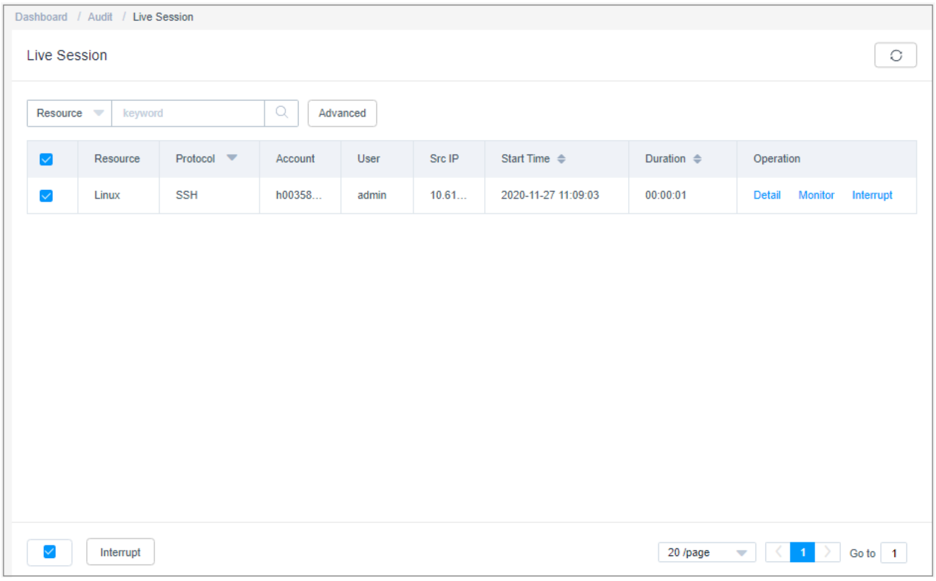
- You have the management permissions for the **Live Session** module.
- There is at least one live session.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **Audit** > **Live Session**.

Figure 10-1 Live Session



Step 3 Query live sessions.

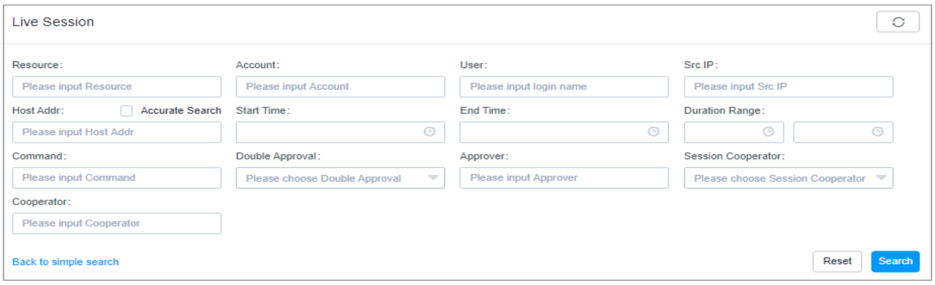
- Quick search

  Enter a keyword in the search box to quickly query live sessions by resource name, account, user, or source IP.

- Advanced search

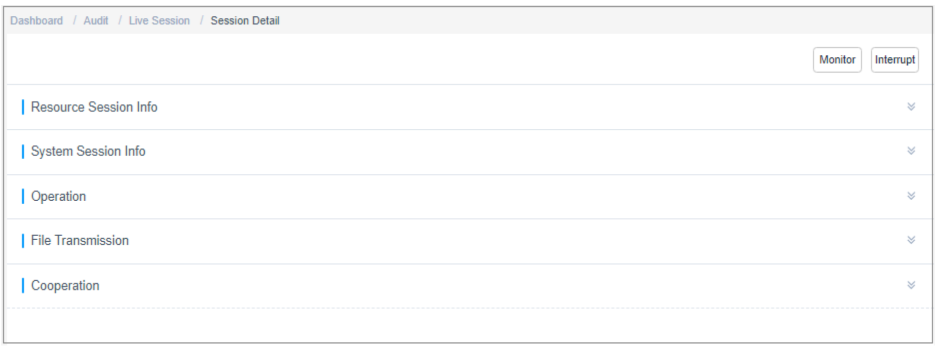
  Enter keywords in the corresponding attribute search boxes to search for live sessions in exact mode.

Figure 10-2 Advanced search



Step 4 Click **Detail** in the **Operation** column of the live session you want to view.

Figure 10-3 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 resource through CBH, you, the audit administrator, will receive session records in real time. You can monitor live sessions to audit real-time operations of other system users.

This topic describes how to monitor OM operations in live sessions.

Prerequisites

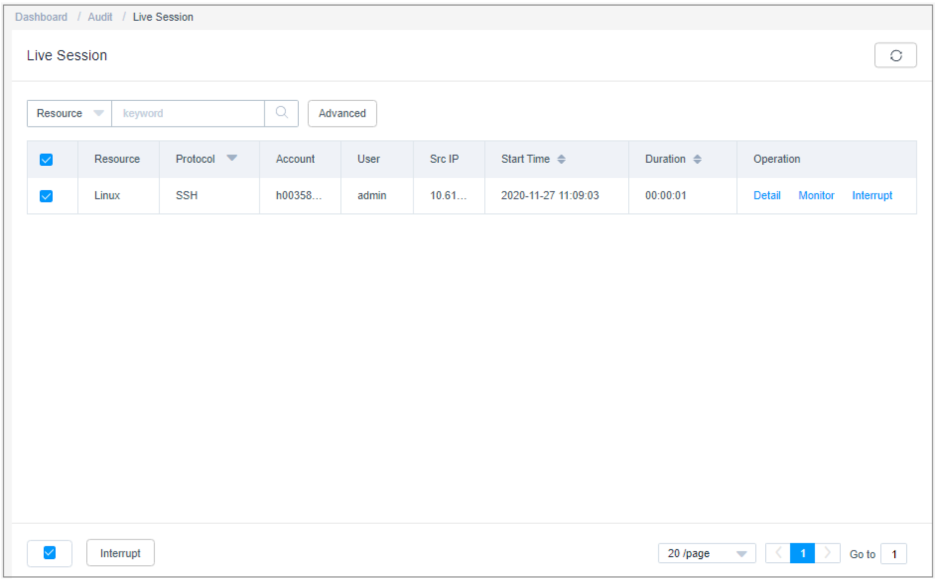
- You have the management permissions for the **Live Session** module.
- There is at least one live session.
- Currently, only H5 O&M sessions and SSH client sessions are supported.

Procedure

Step 1 Log in to the CBH system.

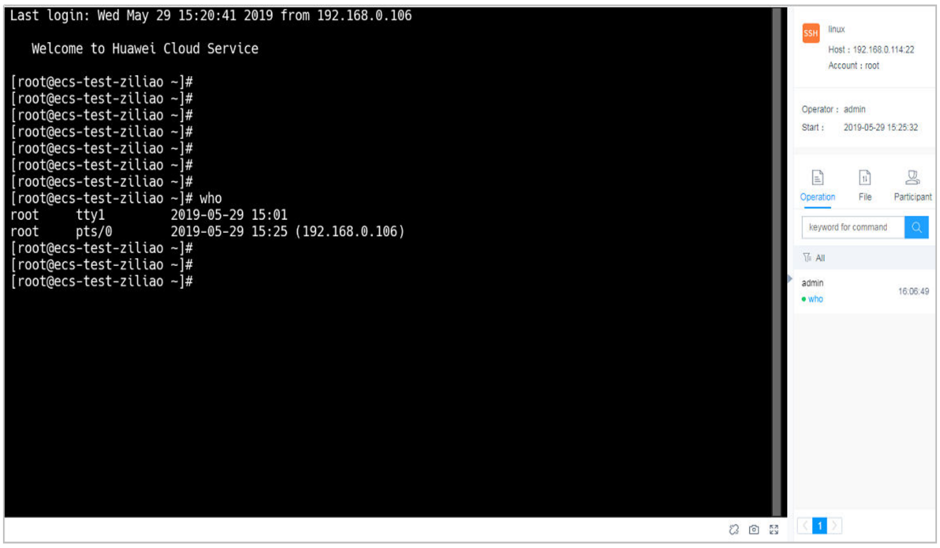
Step 2 Choose **Audit** > **Live Session**.

Figure 10-4 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 10-5 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 resource through CBH, you, the audit administrator, will receive session records in real time. When discovering violations or high-risk operations, you can interrupt the session to prevent the system user from performing further operations.

This topic describes how to interrupt live sessions.

Prerequisites

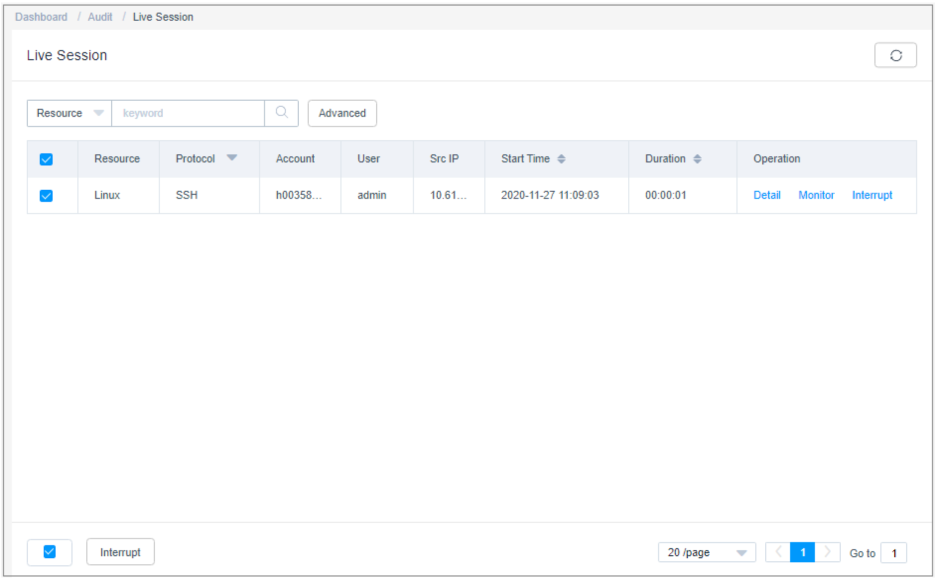
- You have the management permissions for the **Live Session** module.
- There is at least one live session.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **Audit** > **Live Session**.

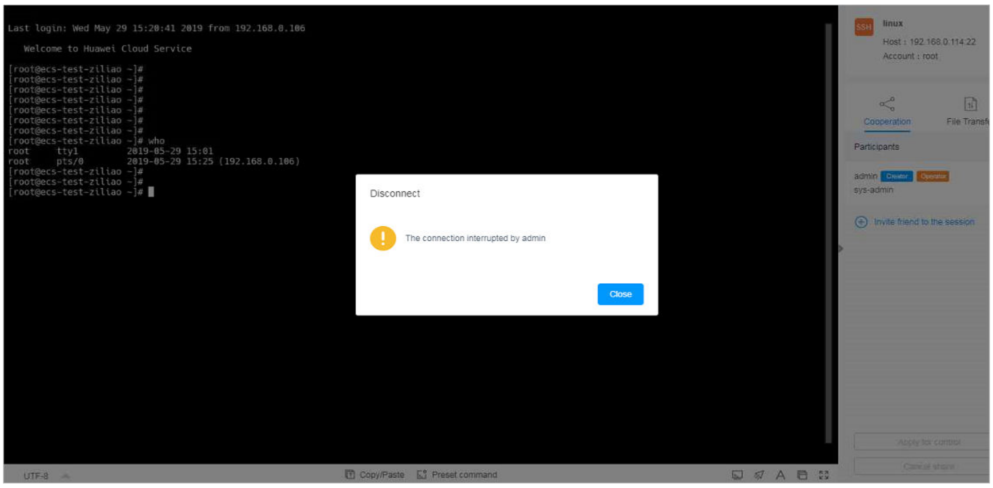
Figure 10-6 Live Session



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 10-7 Session interrupted



----End

10.2 History Session

10.2.1 Viewing History Sessions

After an operation ends, you, the audit administrator, will receive history session records. It makes easy for you to query detailed operation records and audit historical sessions online.

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

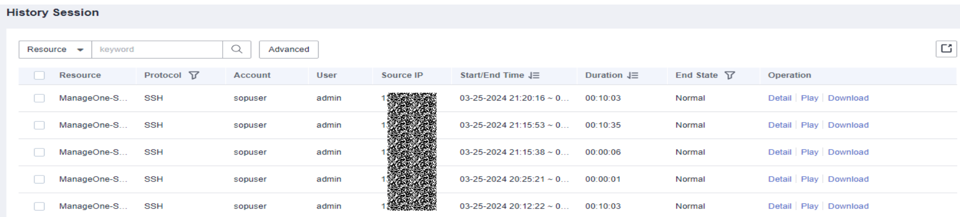
- You have the management permissions for the **History Session** module.
- The OM session has finished.

Viewing History Sessions

Step 1 Log in to the CBH system.

Step 2 Choose **Audit** > **History Session**.

Figure 10-8 History Session



> **NOTE**
>
> The **More** operation in the **Details** column is removed from CBH V3.3.42.0 or later versions.

Step 3 Query history sessions.

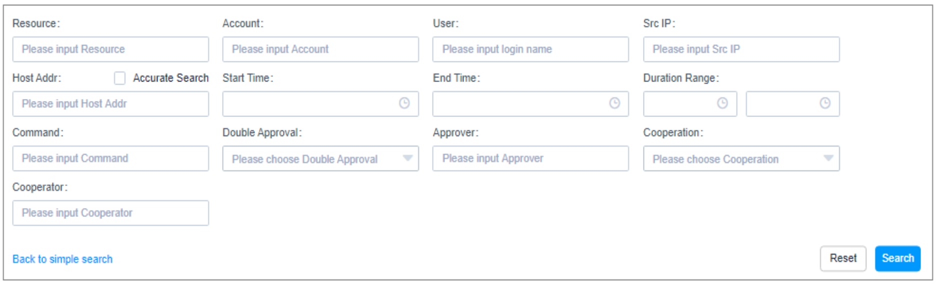
- Quick search

  Enter a keyword in the search box to quickly query history sessions by resource name, account, user, or source IP.

- Advanced search

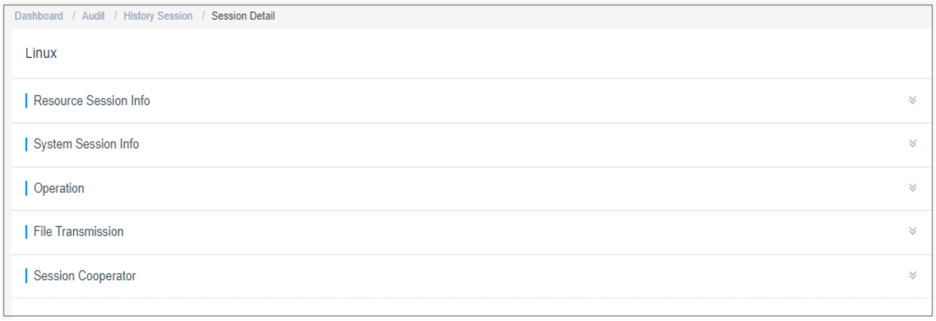
  Enter keywords in the corresponding attribute search boxes to search for history sessions in exact mode.

Figure 10-9 Advanced search



Step 4 Click **Detail** in the **Operation** column of the history session you want to view.

Figure 10-10 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

NOTE

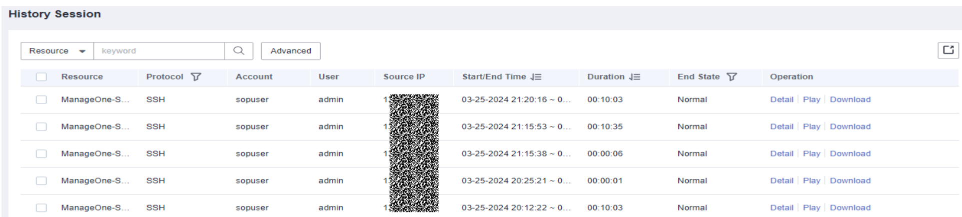
The total duration and playable duration of a downloaded video file may be different because the logout time and last operation time are different.

- 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 the CBH system.

Step 2 Choose **Audit** > **History Session**.

Figure 10-11 History Session

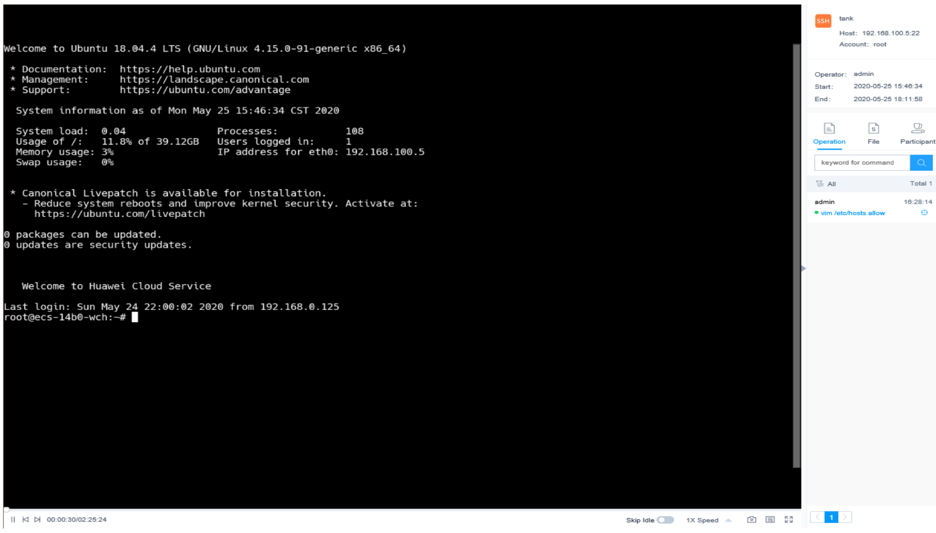


NOTE

The **More** operation in the **Details** column is removed from CBH V3.3.42.0 or later versions.

Step 3 Click **Play** in the **Operation** column of the historical session you want to audit.

Figure 10-12 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**.

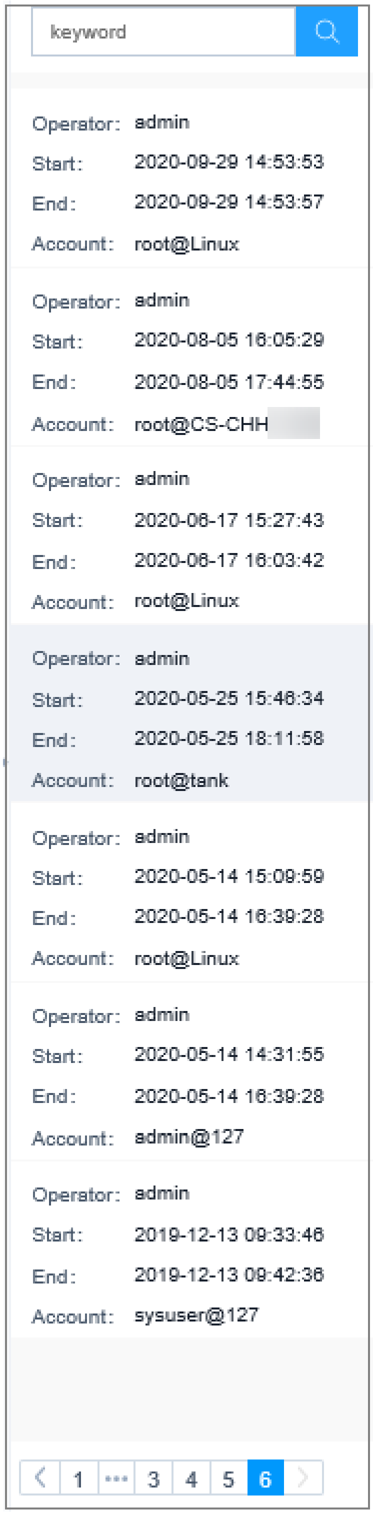
Step 7 Take a quick screenshot of the session.

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 10-13 History session playback list



----End

10.2.2 Exporting History Session Records

CBH allows you to export all history session records for offline audit.

Prerequisites

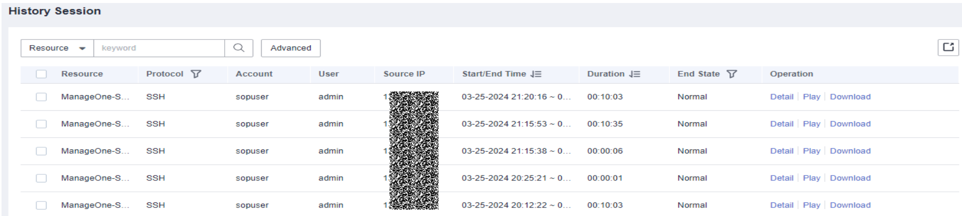
- You have the management permissions for the **History Session** module.
- The OM session has finished.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **Audit** > **History Session**.

Figure 10-14 History Session



NOTE

The **More** operation in the **Details** column is removed from CBH V3.3.42.0 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 **Export** in the upper right corner to download the CSV file.

----End

10.2.3 Managing Session Videos

After an operation ends, you, the audit administrator, will receive history session records. So, 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.

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 logs can be played. Valid session logs start when you initiate a session and end when the last operation is completed.
- Session videos are cached in the CBH system space. You are advised to move the video to a local computer in a timely manner and clear the system disk space.

Prerequisites

- You have the management permissions for the **History Session** module.

- The OM session has finished.

Generating Session Videos

Step 1 Log in to the CBH system.

Step 2 Choose **Audit** > **History Session**.

Figure 10-15 History Session

NOTE

The **More** operation in the **Details** column is removed from CBH V3.3.42.0 or 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 CBH system storage space is abundant, the video duration and size are not limited.
- If the system storage space is insufficient, the video may fail to be generated.
- Session recordings can be backed up to OBS buckets. For details, see **Configuring OBS Buckets for Remote Log Backup**.

----End

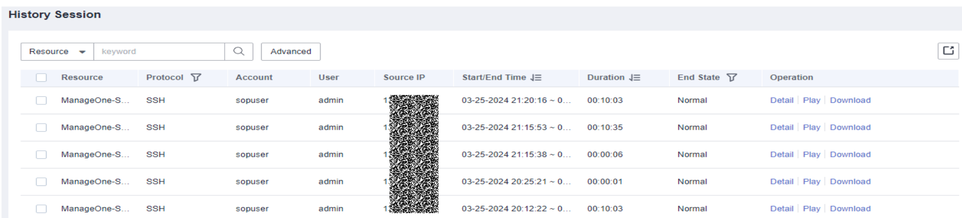
Downloading a Session Video

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 the CBH system.

Step 2 Choose **Audit** > **History Session**.

Figure 10-16 History Session



> NOTE
>
> The **More** operation in the **Details** column is removed from CBH V3.3.42.0 or 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 playback a session recording in a compressed package, perform 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 Logs

10.3.1 Querying System Logs

After a system user logs in to the CBH system and perform operations such as permission configuration and audit management, you, the audit administrator, will receive system log records. You can query detailed login and operation records in the CBH system and audit system logs online. System logs include system login logs and system operation logs.

Prerequisites

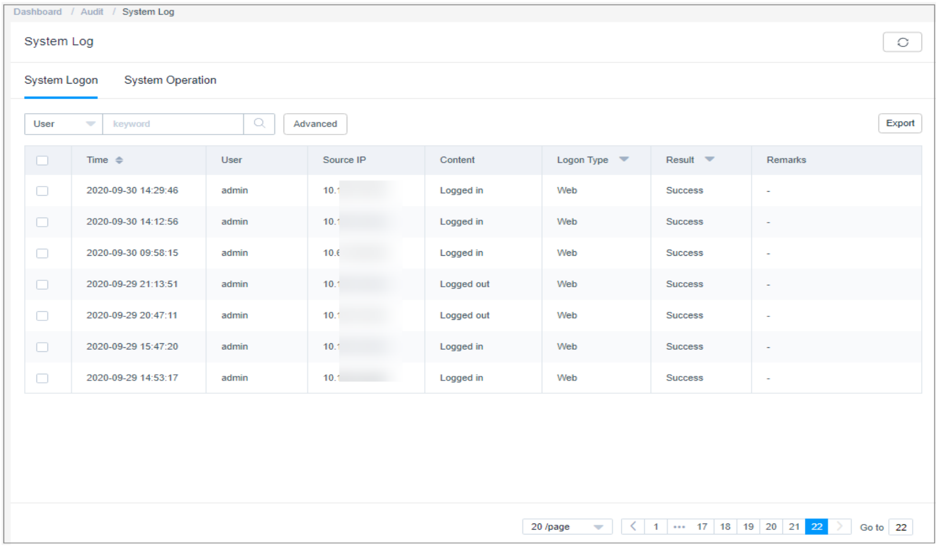
You have the management permissions for the **System Logon** or **System Operation** module under **System Log**.

Querying System Logon Logs

Step 1 Log in to the CBH system.

Step 2 Choose **Audit** > **System Log** > **System Logon** to switch to the system log page.

Figure 10-17 System logon logs



Step 3 Query login logs.

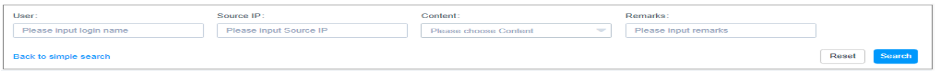
- Quick search

  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.

  Figure 10-18 Advanced search

Step 4 View the login logs in the search result.

----End

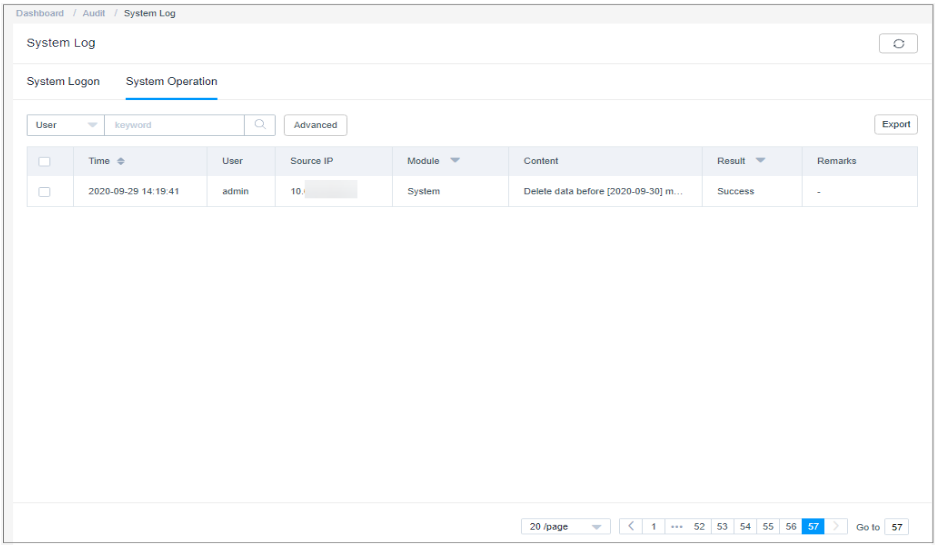
Viewing System Operation Logs

Step 1 Log in to the CBH system.

Step 2 Choose **Audit** > **System Log** to go to the system log page.

Step 3 Click the **System Operation** tab.

Figure 10-19 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 the CBH system and perform operations such as permission configuration and audit management, you, the audit administrator, will receive system log records. You can query detailed login and operation records in the CBH system 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**.

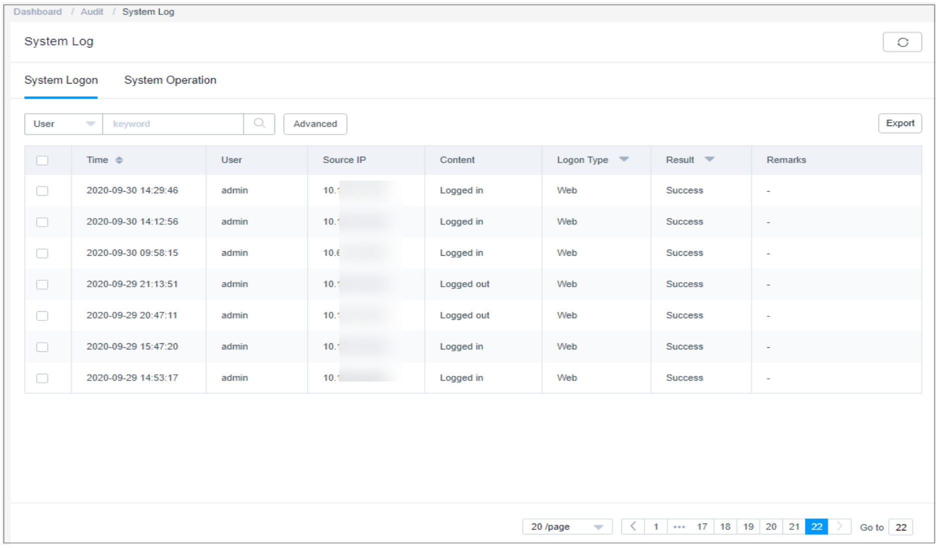
Exporting System Logon Logs

Step 1 Log in to the CBH system.

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 10-20 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 **Export** in the upper right corner to download the CSV file.

----End

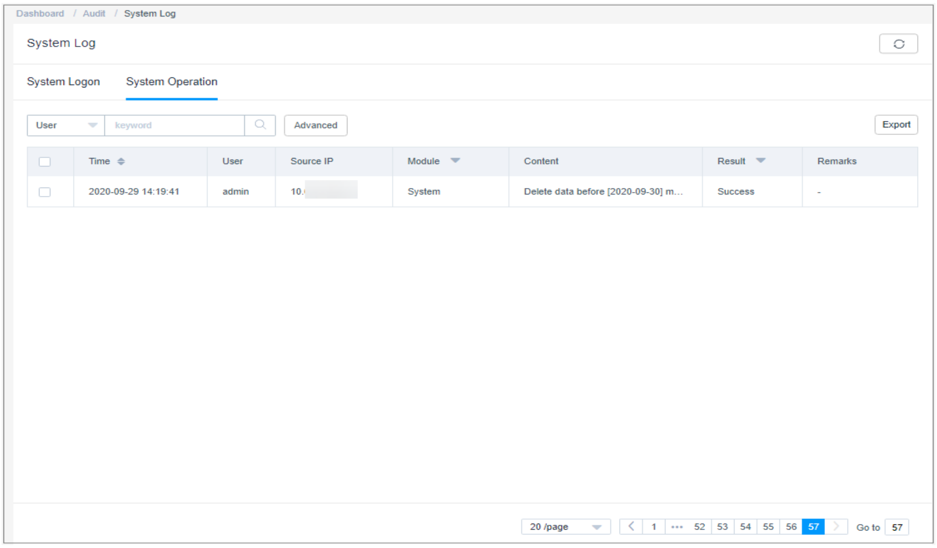
Exporting System Operation Logs

Step 1 Log in to the CBH system.

Step 2 Choose **Audit** > **System Log** to go to the system log page.

Step 3 Click the **System Operation** tab.

Figure 10-21 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 **Export** in the upper right corner to download the CSV file.

----End

10.4 Operation Report

10.4.1 Viewing Operation Reports

As the audit administrator, you can view and export detailed operation reports, including 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.
  - 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.
- 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

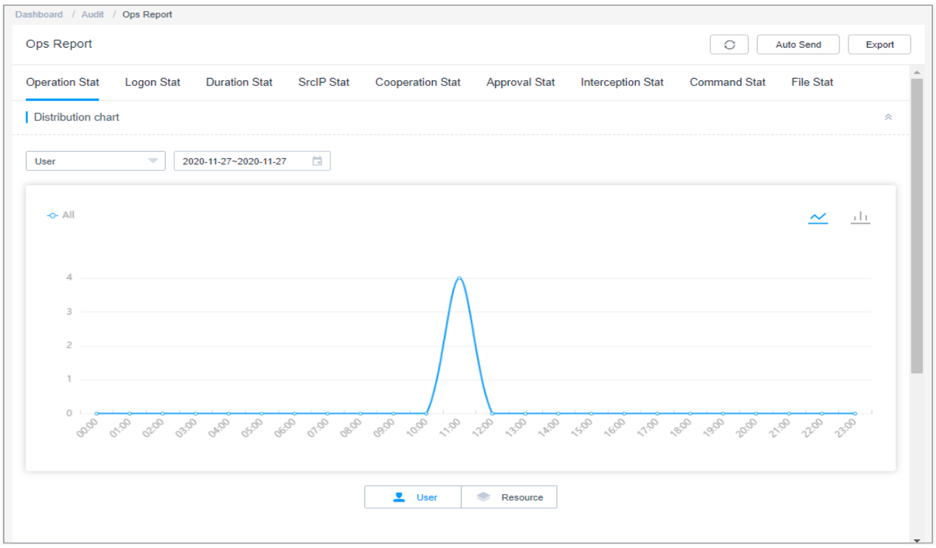
You have the management permissions for the **Operation Report** module.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **Audit** > **Operation Report**.

Figure 10-22 O&M reports



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.

Figure 10-23 Distribution chart of Operation Stat

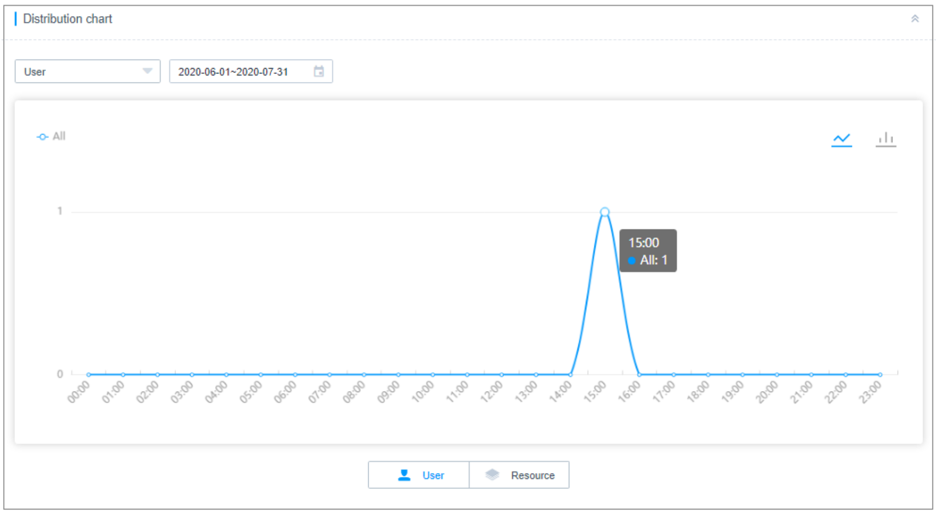
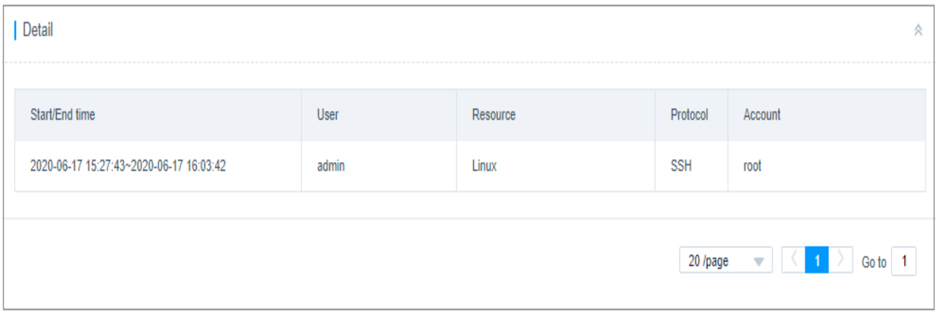


Figure 10-24 Detailed data of Operation Stat



Detail

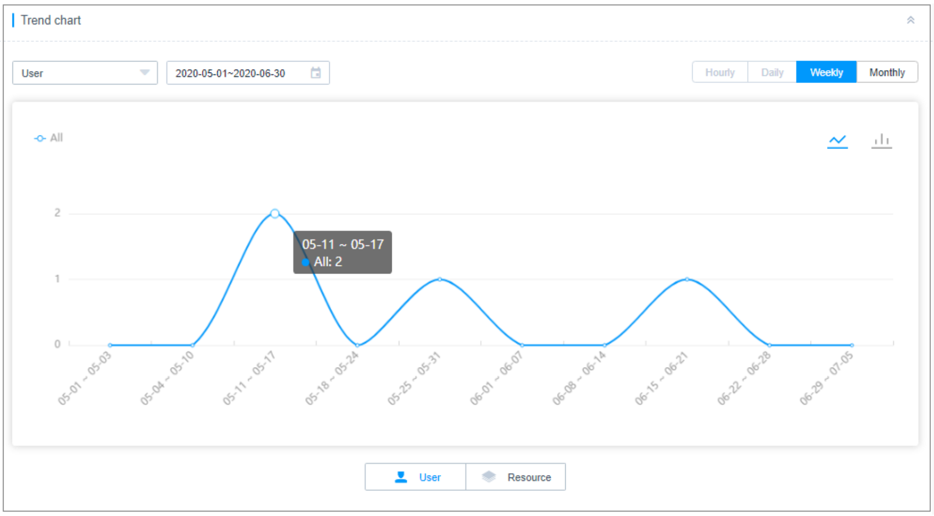
Start/End time	User	Resource	Protocol	Account
2020-06-17 15:27:43~2020-06-17 16:03:42	admin	Linux	SSH	root

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.

Figure 10-25 Trend chart of Logon Stat



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.

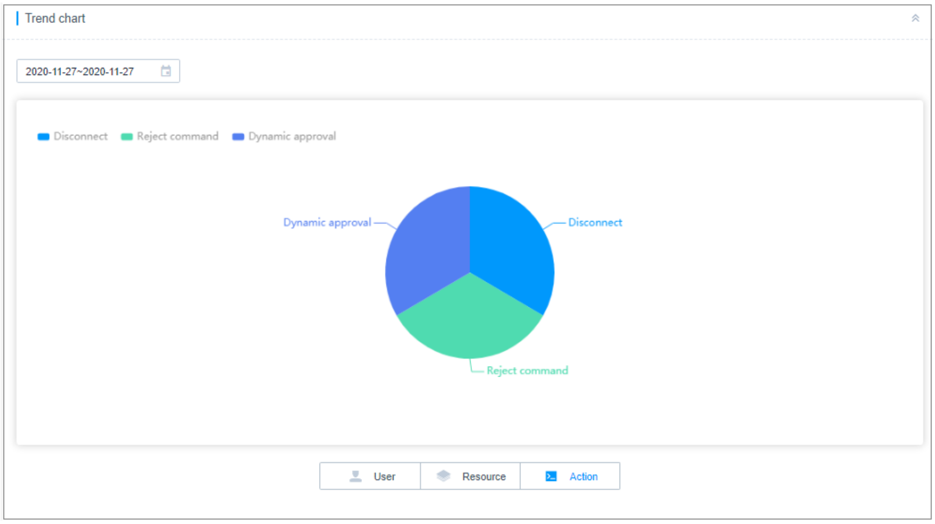
Interception Stat

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.

Figure 10-26 Trend chart of Interception Stat



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 CBH 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

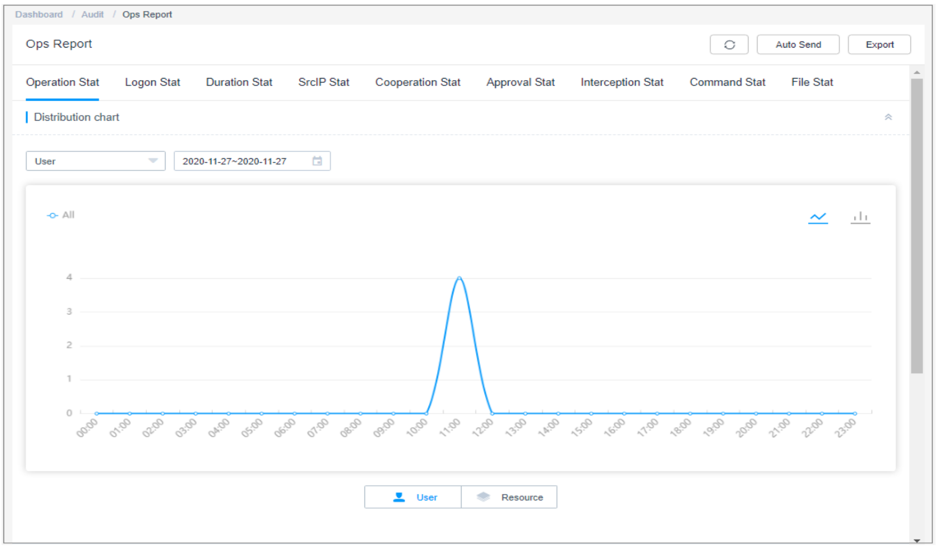
- You have the management permissions for the **Operation Report** module.
- You have configured an available email address to receive reports.

Manually Exporting an Operation Report

Step 1 Log in to the CBH system.

Step 2 Choose **Audit** > **Operation Report**.

Figure 10-27 O&M reports



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.

Figure 10-28 Exporting operation reports

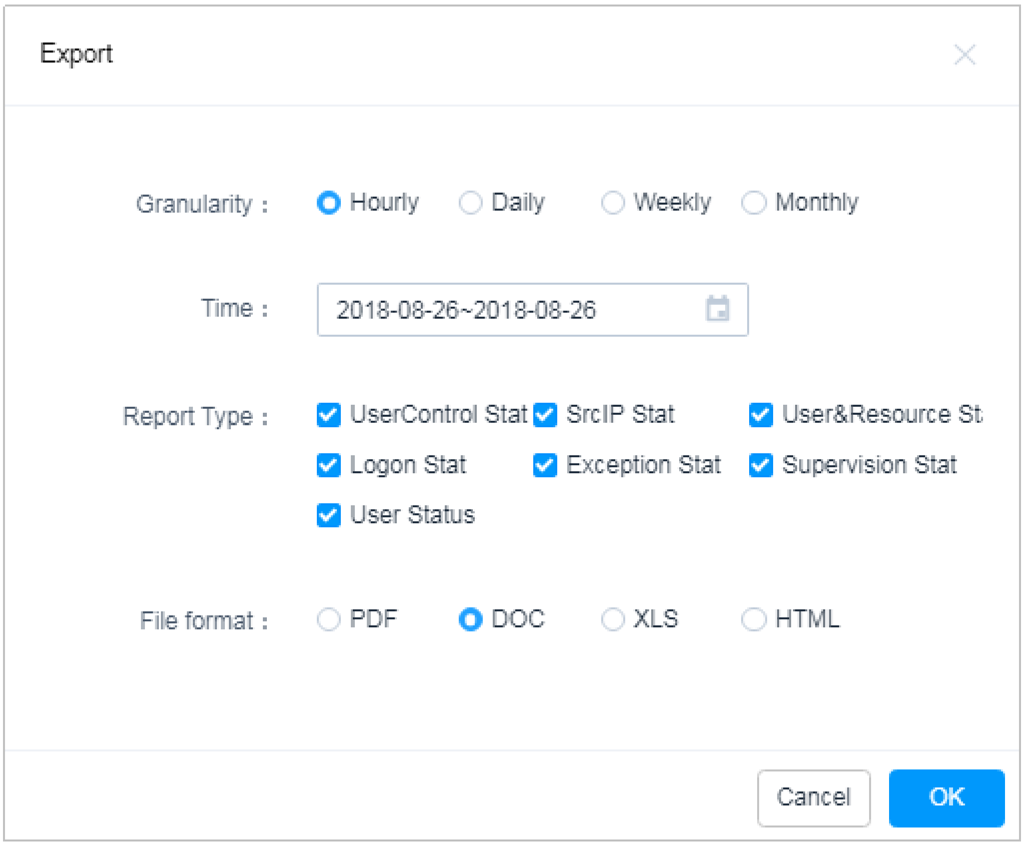


Table 10-1 Parameters for exporting operation reports

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.

Step 6 Go to your email address to check the operation report after you receive the notification in the message center.

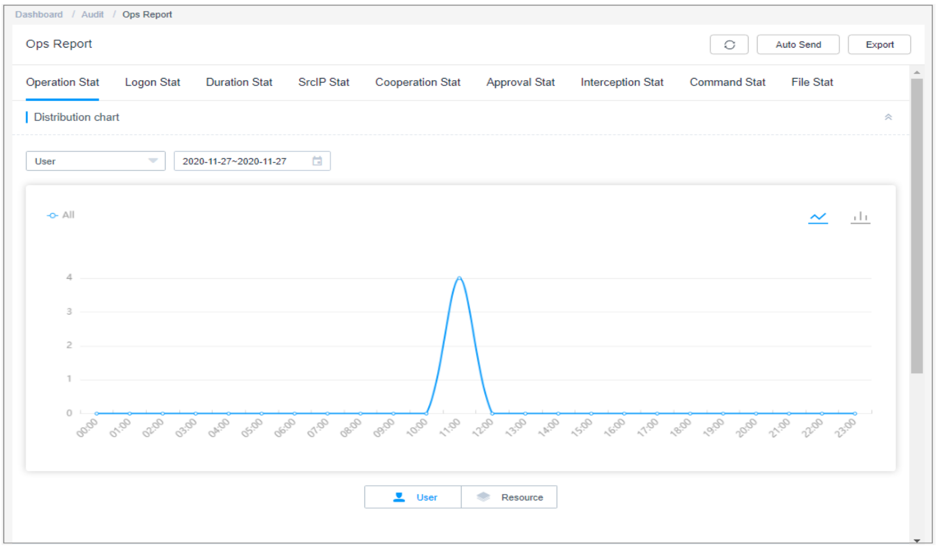
----End

Automatically Pushing a System Report

Step 1 Log in to the CBH system.

Step 2 Choose **Audit** > **Operation Report**.

Figure 10-29 O&M reports



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.

Figure 10-30 Auto Send

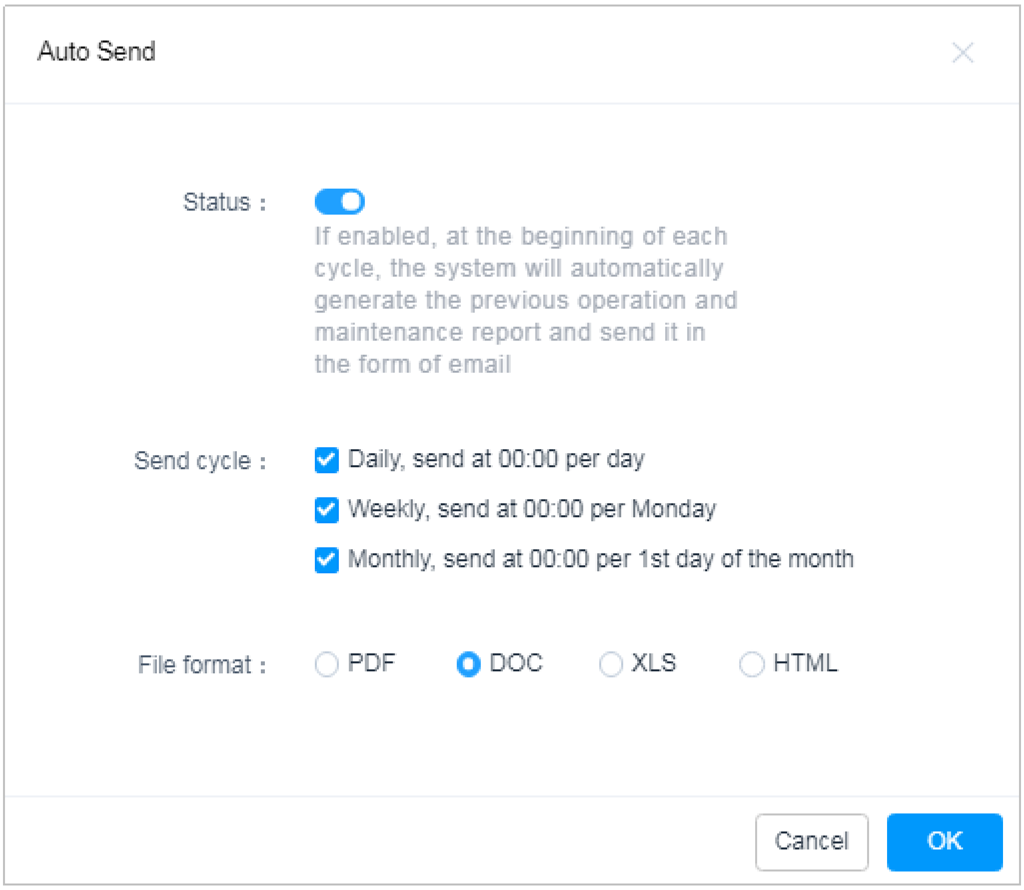


Table 10-2 Auto Send

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.

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**.

----End

10.5 System Report

10.5.1 Viewing System Reports

As an audit administrator, you can view the detailed operation data in the system report, including 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

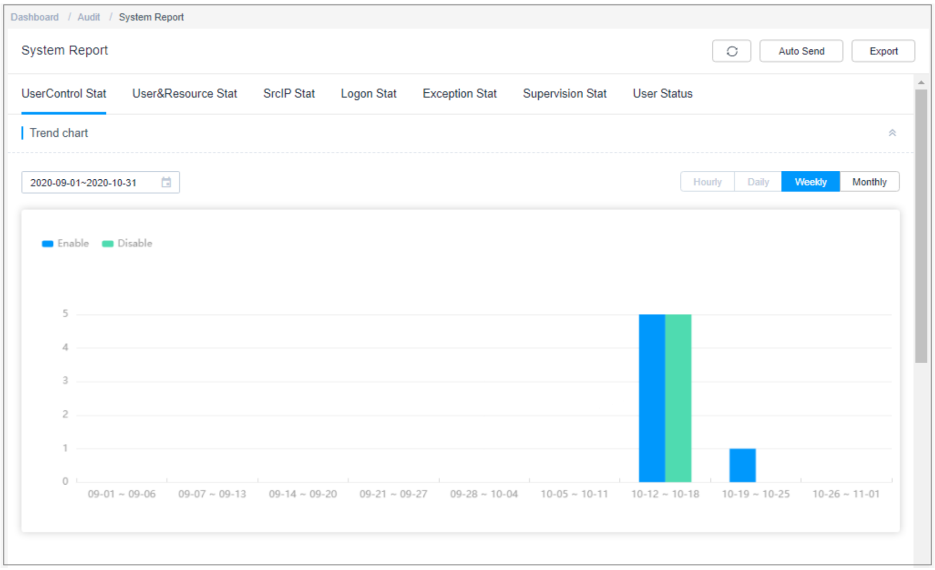
You have the management permissions for the **System Report** module.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **Audit** > **System Report**.

Figure 10-31 System reports



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.

Figure 10-32 Trend chart of UserControl Stat

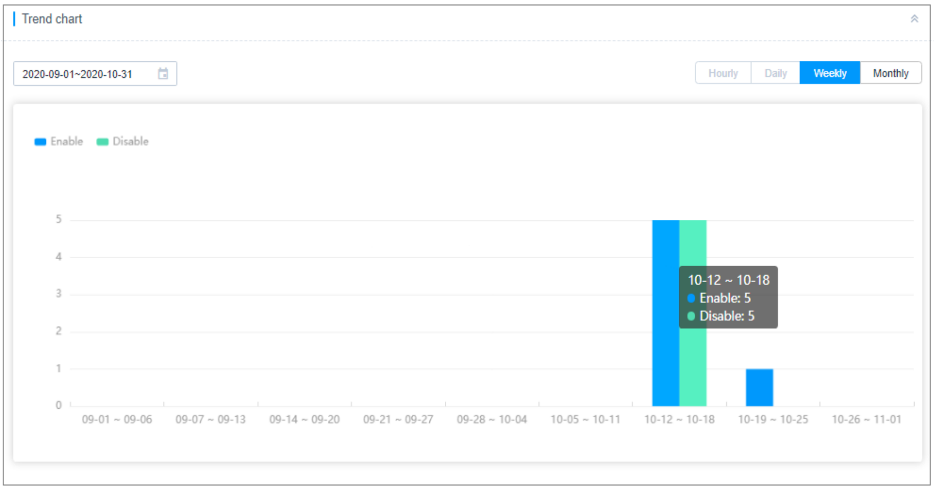
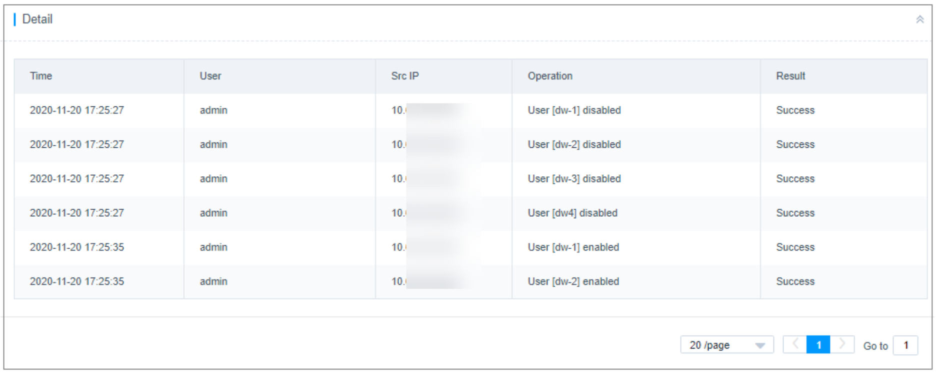


Figure 10-33 Detailed user control results

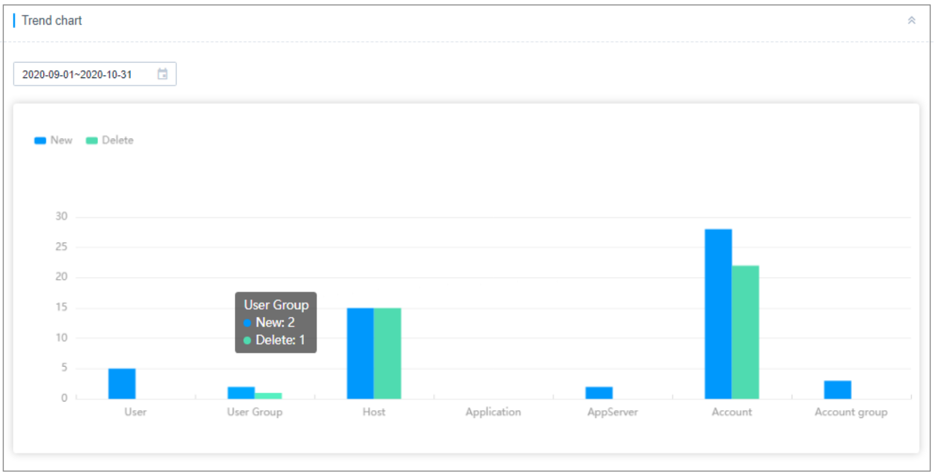


User&Resource Stat

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 10-34 Trend chart of User&Resource Stat



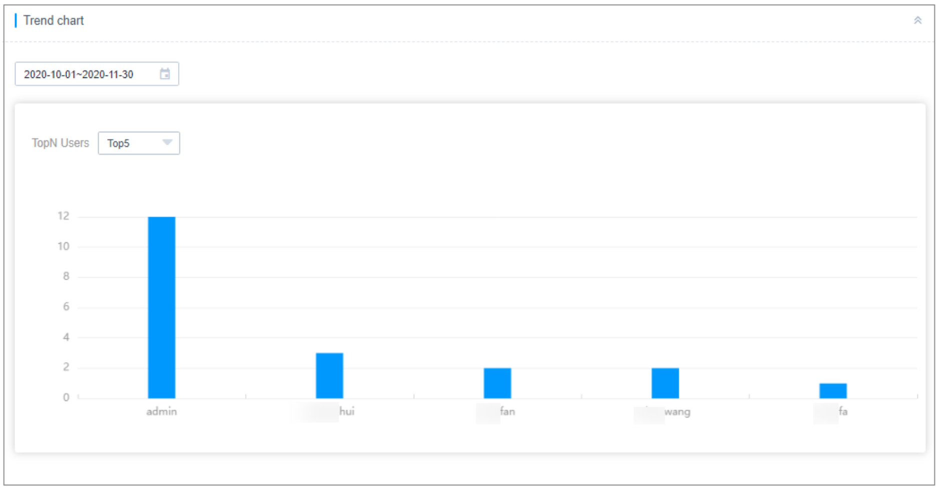
SrcIP Stat

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 10-35 Trend chart of SrcIP Stat



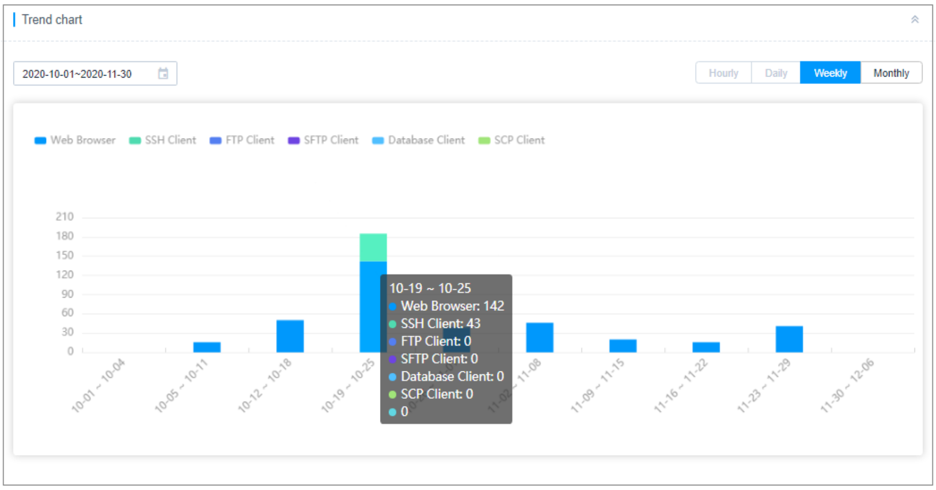
Logon Stat

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 10-36 Trend chart of Logon Stat



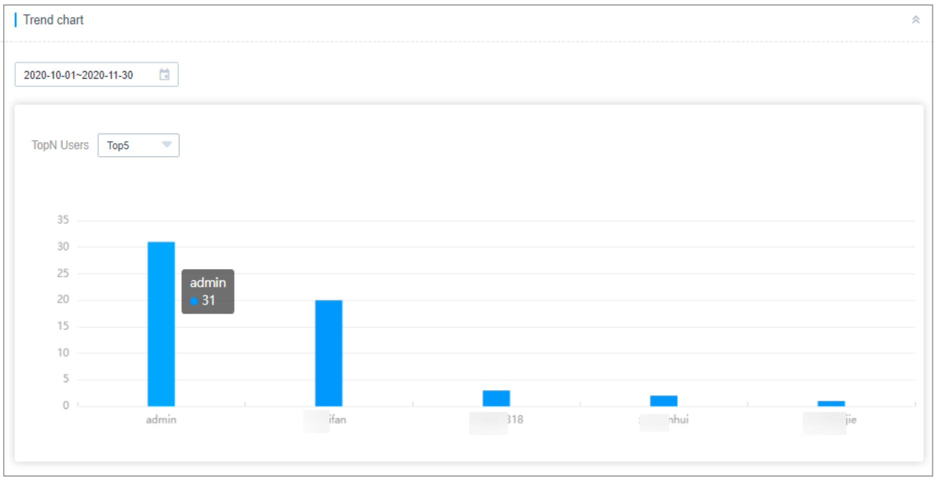
Exception Stat

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 10-37 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

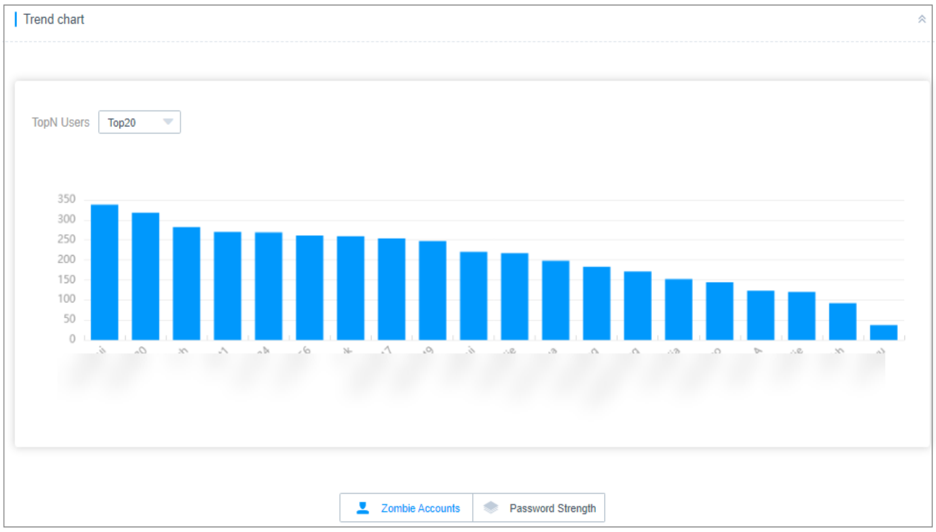
  Password strength classification criteria:

  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.

Figure 10-38 Trend chart of zombie users



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 CBH 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

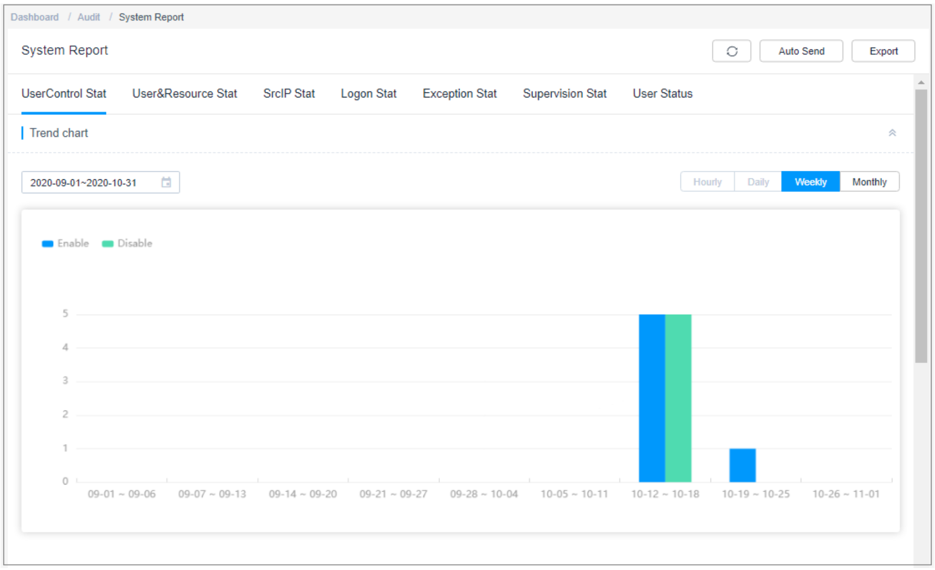
- You have the management permissions for the **System Report** module.
- You have configured an available email address to receive reports.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **Audit** > **System Report**.

Figure 10-39 System reports



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.

Figure 10-40 Exporting system reports

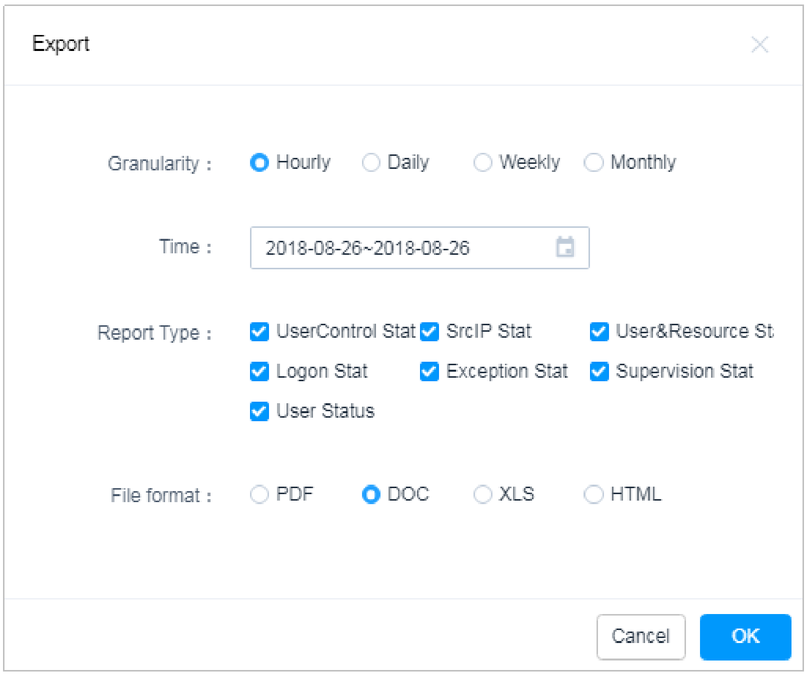


Table 10-3 Parameters for exporting system reports

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.
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.

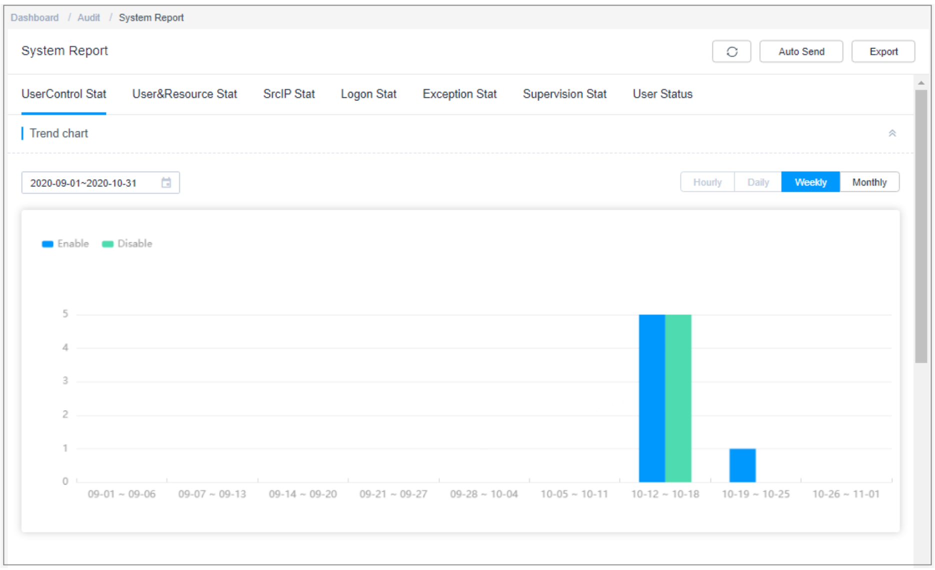
----End

Automatically Pushing a System Report

Step 1 Log in to the CBH system.

Step 2 Choose **Audit** > **System Report**.

Figure 10-41 System reports



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.

Figure 10-42 Auto Send

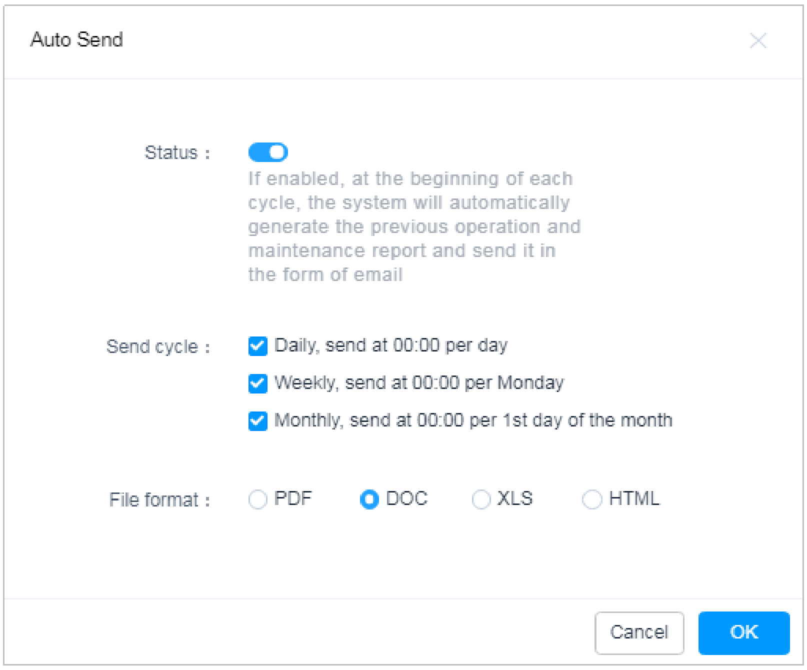


Table 10-4 Parameters for auto-send function

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 System Management

11.1 Sysconfig

11.1.1 System 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**.
- Port configuration: See **Port**.
- Outgoing configuration: See **Outgoing**.
- Authentication configuration: See **Remote Authentication Management**.
- Ticket configuration: See **Ticket Configuration Management**.
- Alarm configuration: See **Alarm**.
- System theme: See **Theme**.

11.1.2 Network

11.1.2.1 View Network Configurations

This topic describes how to view the system network interface, DNS address, default gateway address, and static routes.

Prerequisites

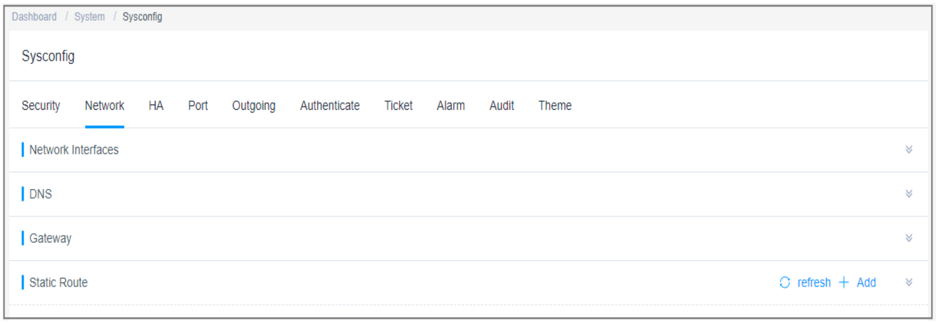
You have the management permissions for the **System** module.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **System** > **Sysconfig** > **Network**.

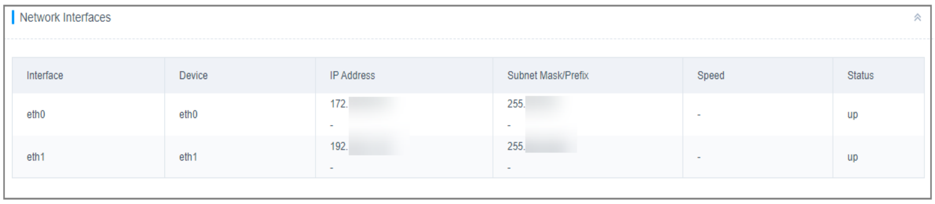
Figure 11-1 Network



Step 3 In the **Network interfaces** area, view the network interface information of the CBH system.

By default, the network interfaces cannot be modified.

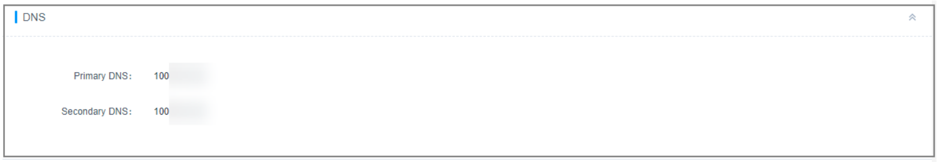
Figure 11-2 Network interfaces



Step 4 In the **DNS** configuration area, view the primary and secondary DNS addresses of the CBH system.

By default, the DNS address cannot be changed.

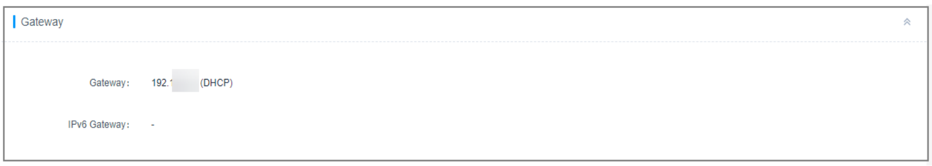
Figure 11-3 System DNS address



Step 5 In the **Gateway** area, view the default gateway of the CBH system.

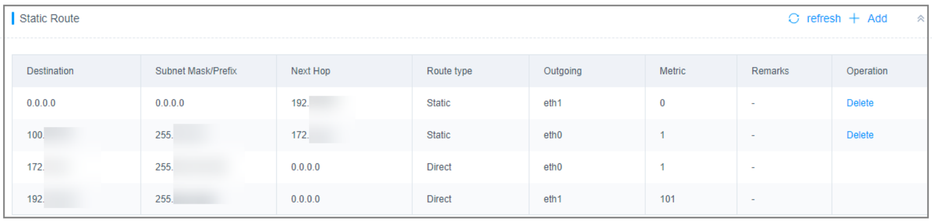
By default, the DHCP gateway address is identified as the system gateway. The default gateway cannot be changed.

Figure 11-4 System default gateway



Step 6 In the **Static Route** configuration area, view accessible servers in other network segments.

Figure 11-5 Static Route



----End

11.1.2.2 Adding a Static Route to the CBH System

After the CBH system restarts, non-static routes may be lost, affecting network availability. To prevent this issue, add static routes to the system.

This topic describes how to add a static route to the CBH system.

Prerequisites

You have the management permissions for the **System** module.

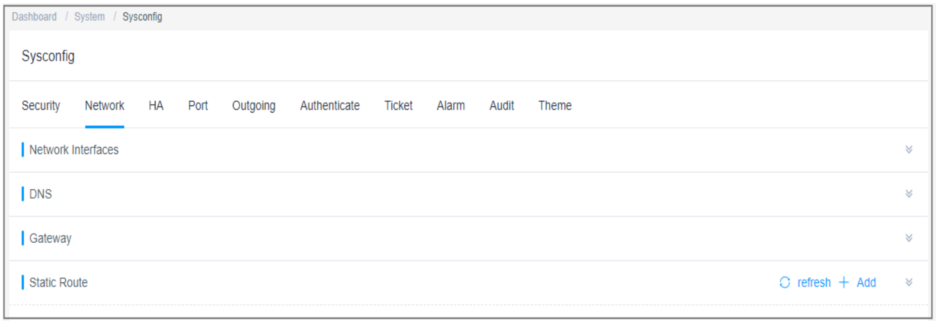
> **CAUTION**
>
> Each static route must be correct. If the information is incorrect, you cannot log in to the CBH system.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **System** > **Sysconfig** > **Network**.

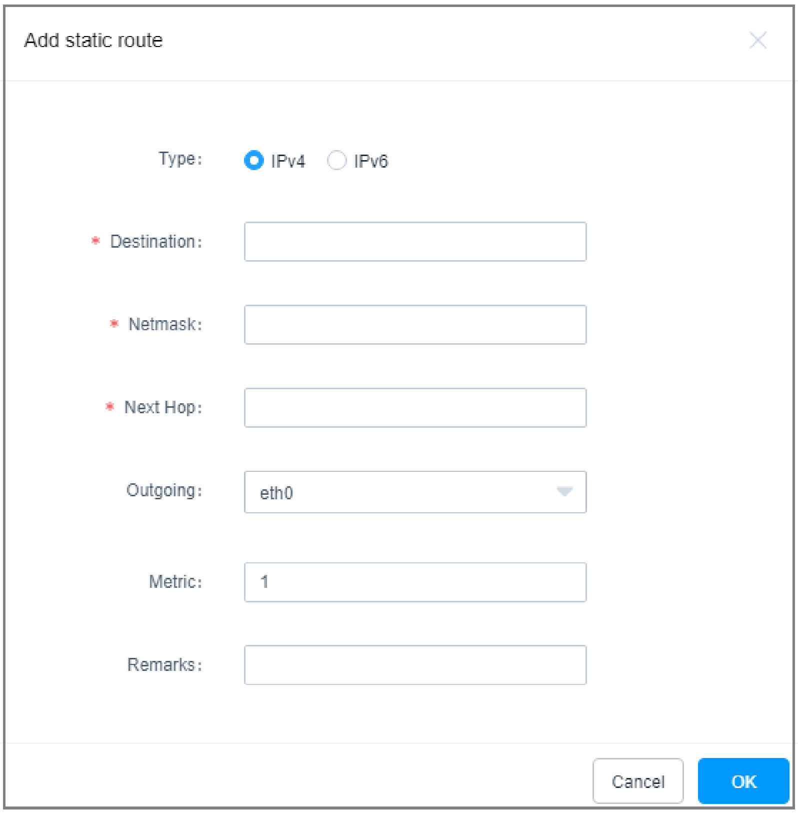
Figure 11-6 Network



Step 3 In the **Static Route** configuration area, click **Add**.

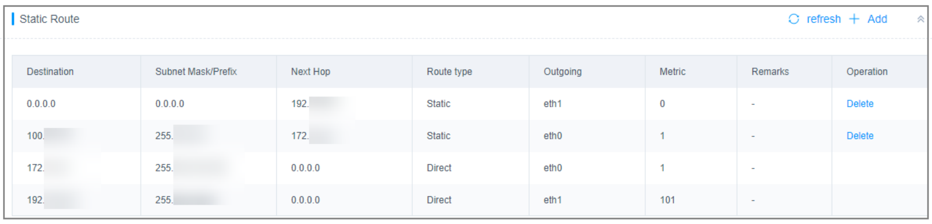
In the displayed **Add static route** dialog box, configure other parameters.

Figure 11-7 Add static route



Step 4 Click **OK**. You can then go to the **Security** configuration page and view the configured static route.

Figure 11-8 Static Route



----End

Follow-up Operations

To delete a static route, click **Delete** in the **Operation** column in the corresponding row.

11.1.3 Port

11.1.3.1 Configuring the Operation Ports

The operation port is required for accessing managed resources, such as SSH, SFTP, or FTP resources, and logging in to the CBH system 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

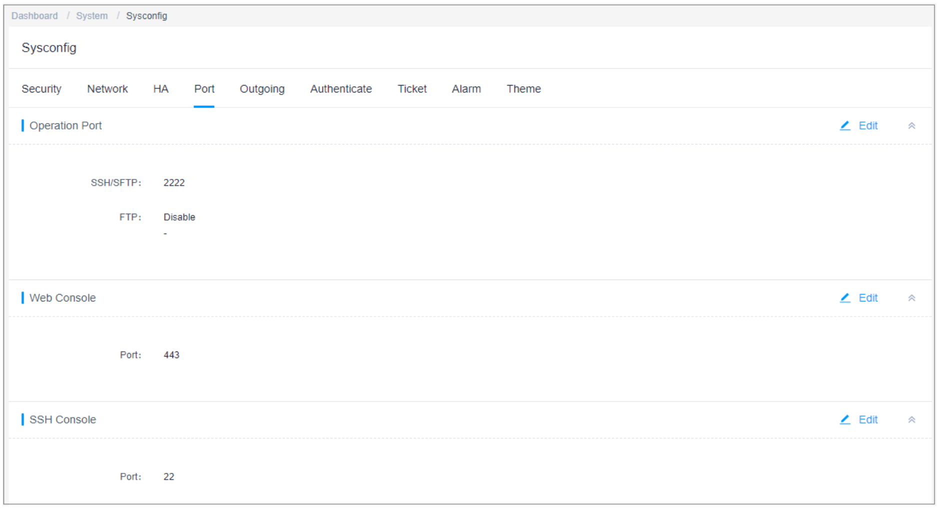
You have the management permissions for the **System** module.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **System** > **Sysconfig** > **Port**.

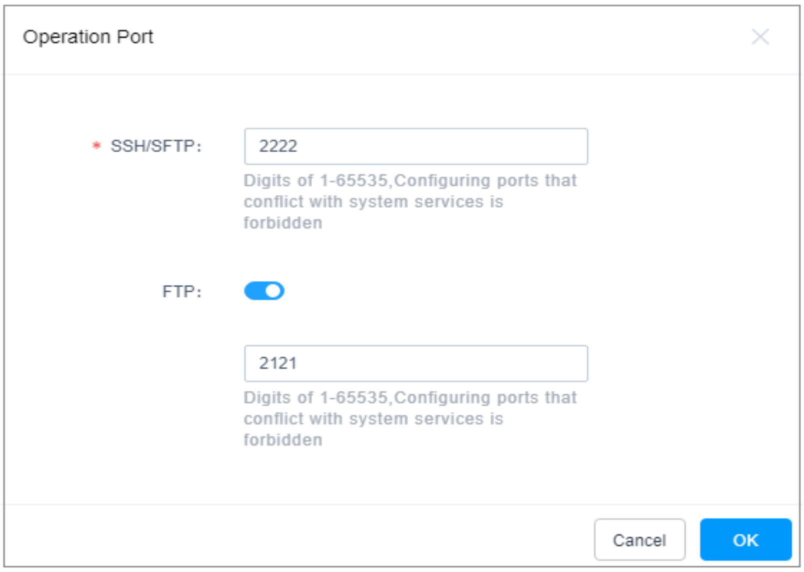
Figure 11-9 Port configuration



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.

Figure 11-10 Operation Port



Step 4 Click **OK** and then restart the system for the configuration to take effect.

----End

11.1.3.2 Configuring the Web Console Port

The web console port is used for logging in to the CBH system 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

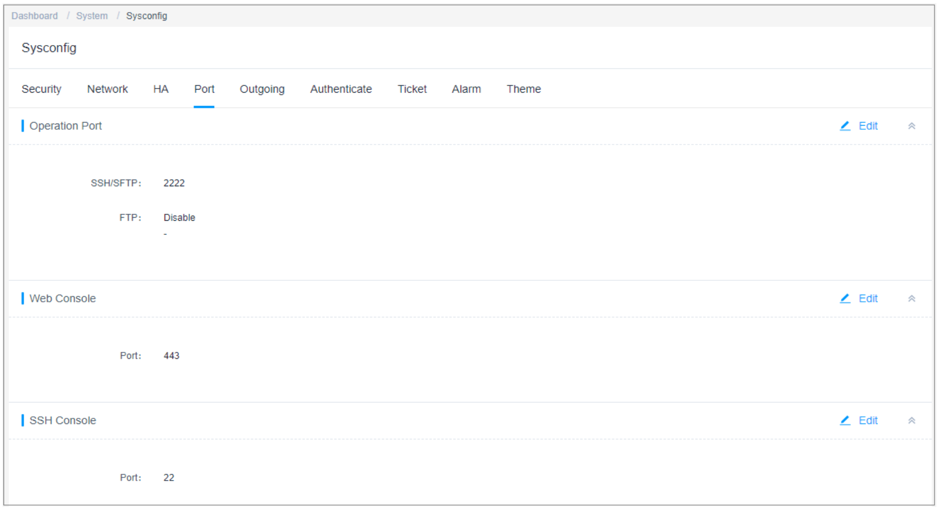
You have the management permissions for the **System** module.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **System** > **Sysconfig** > **Port**.

Figure 11-11 Port configuration



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.

Figure 11-12 Web Console

Step 4 Click **OK** and then restart the system for the configuration to take effect.

----End

11.1.3.3 Configuring the SSH Console Port

The SSH console port is required for logging in to the CBH system 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

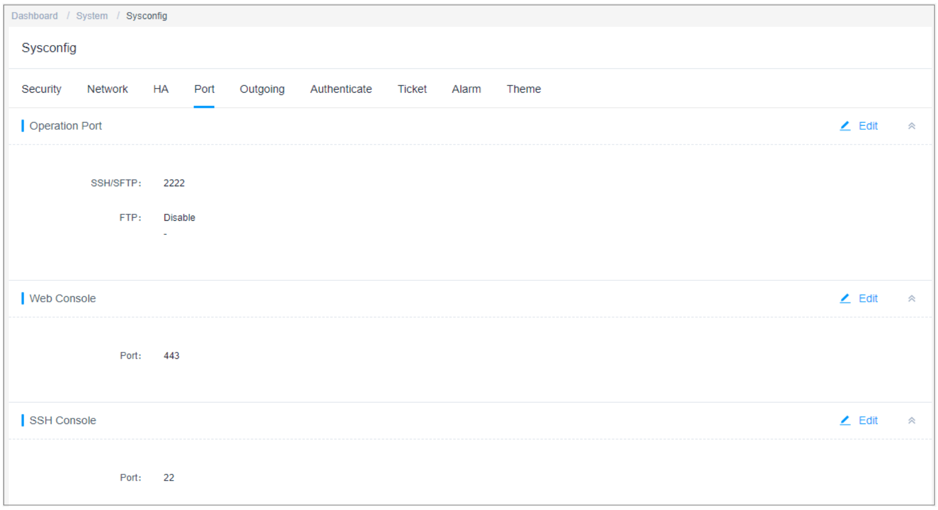
You have the management permissions for the **System** module.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **System** > **Sysconfig** > **Port**.

Figure 11-13 Port configuration



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.

Figure 11-14 SSH Console

Step 4 Click **OK** and then restart the system for the configuration to take effect.

----End

11.1.4 Outgoing

11.1.4.1 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).

This topic describes how to configure an outgoing mail server.

Prerequisites

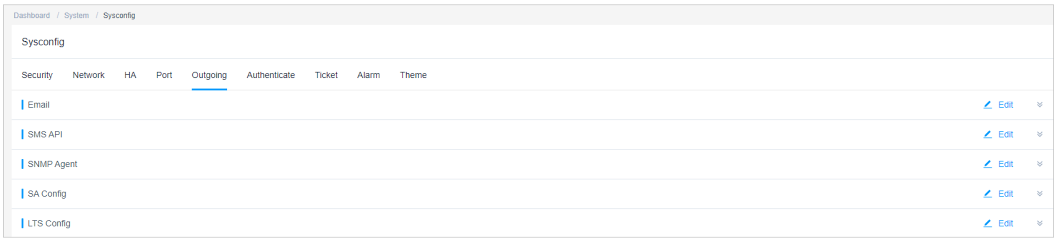
You have the management permissions for the **System** module.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **System** > **Sysconfig** > **Outgoing**.

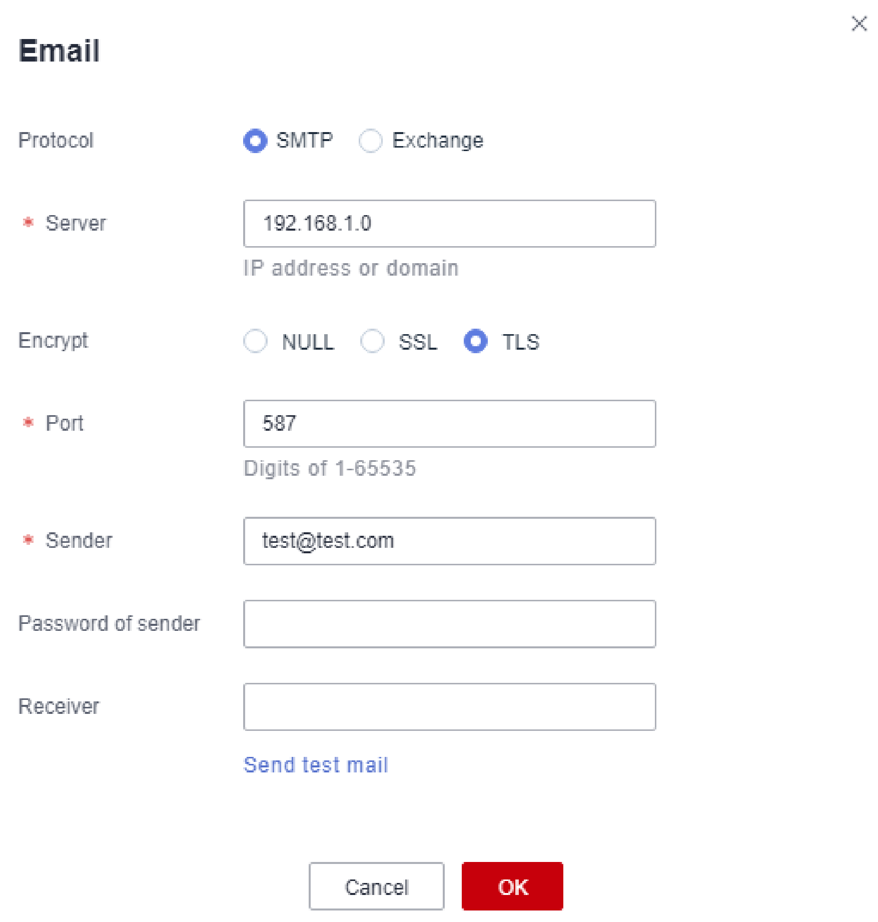
Figure 11-15 Outgoing



Step 3 In the **Email** area, click **Edit**.

In the displayed **Email** dialog box, set **Protocol** to **SMTP** or **Exchange** and specify other parameters.

Figure 11-16 Email configuration



Step 4 Click **OK**. You can then view email configuration on the **Outgoing** tab.

----End

11.1.4.2 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 purchased 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.

This topic describes how to configure an outgoing SMS gateway.

Prerequisites

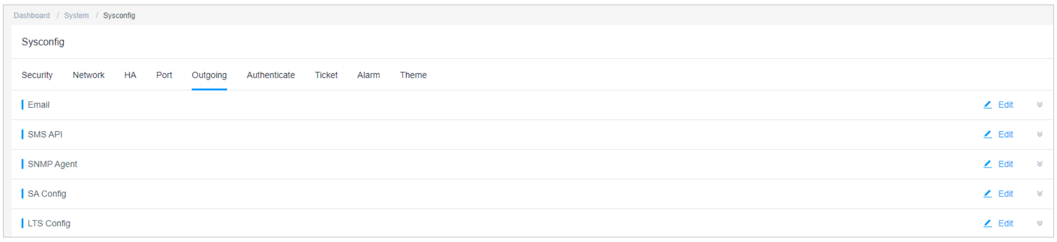
You have the management permissions for the **System** module.

Built-in SMS gateway

Step 1 Log in to the CBH system.

Step 2 Choose **System** > **Sysconfig** > **Outgoing**.

Figure 11-17 Outgoing

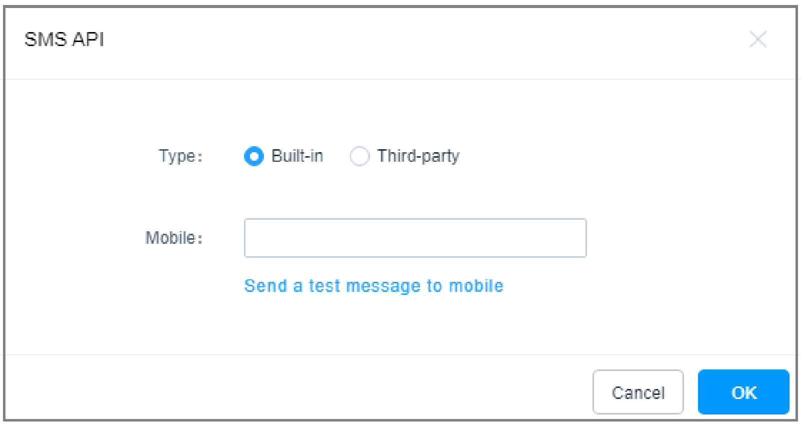


Step 3 In the **SMS API** area, click **Edit**.

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.

Figure 11-18 Built-in SMS gateway



⚠ CAUTION

- The built-in SMS gateway cannot push CBH system alarm notifications.
- The built-in SMS gateway cannot send SMS messages to mobile numbers outside the Chinese mainland. If you need to receive SMS messages from mobile numbers outside the Chinese mainland, configure an SMS gateway outside the Chinese mainland.

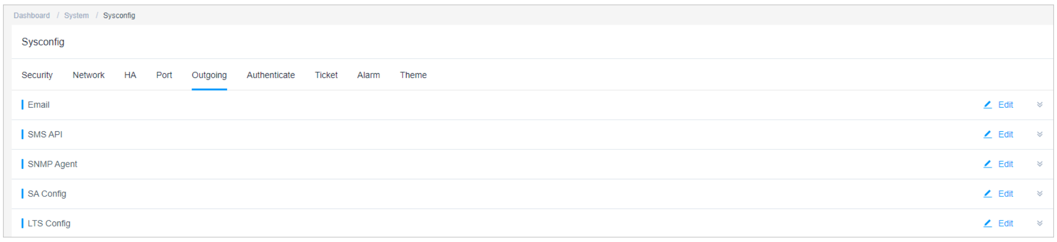
----End

General Third-party SMS Gateway

Step 1 Log in to the CBH system.

Step 2 Choose **System** > **Sysconfig** > **Outgoing**.

Figure 11-19 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.

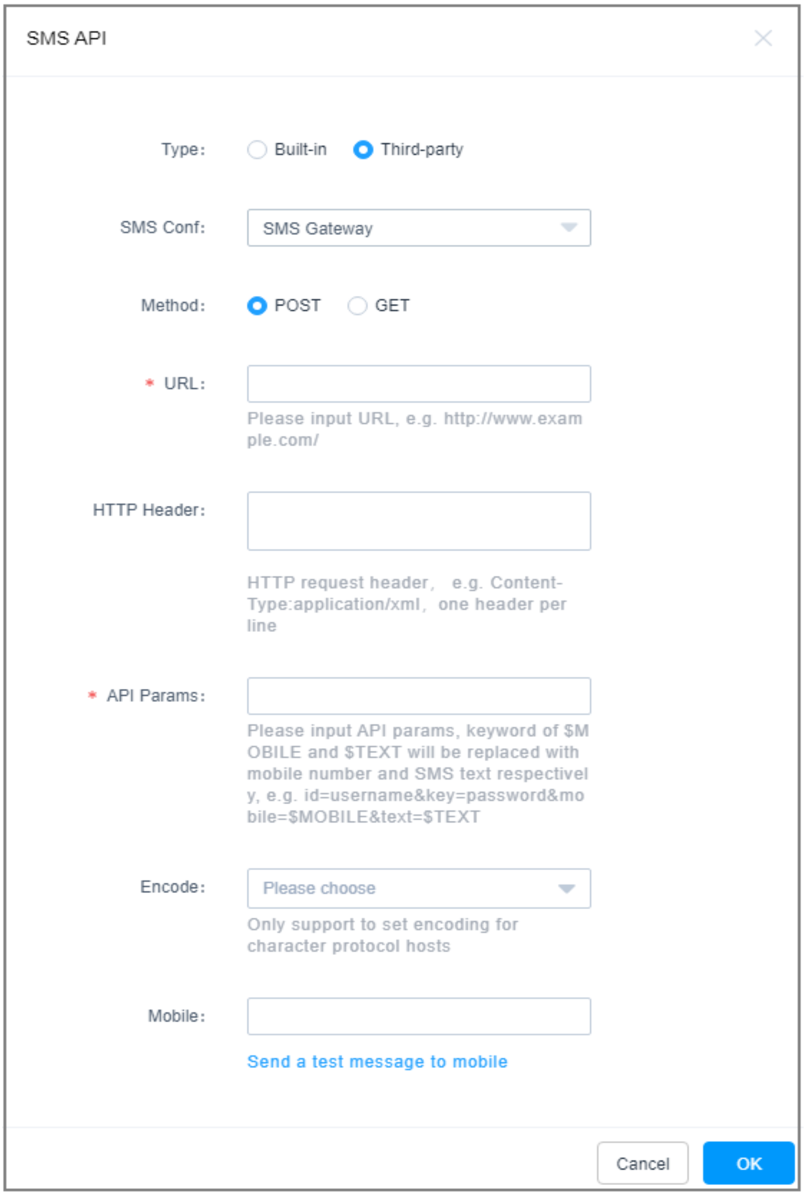
Step 5 Click **OK**. You can then view SMS gateway configuration on the **Outgoing** tab.

Table 11-1 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**.

Parameter	Description
Mobile	Phone number for receiving the SMS messages. Enter an available phone number and verify the SMS message content.

Figure 11-20 General SMS gateway



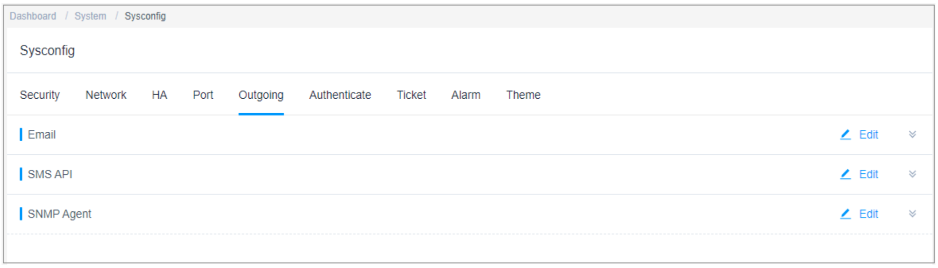
----End

Third-Party Message & SMS Service

Step 1 Log in to the CBH system.

Step 2 Choose **System** > **Sysconfig** > **Outgoing**.

Figure 11-21 Outgoing



Step 3 In the **SMS API** area, click **Edit**.

Step 4 Select **Third-party** and then configure MSGSMS for SMS gateway.

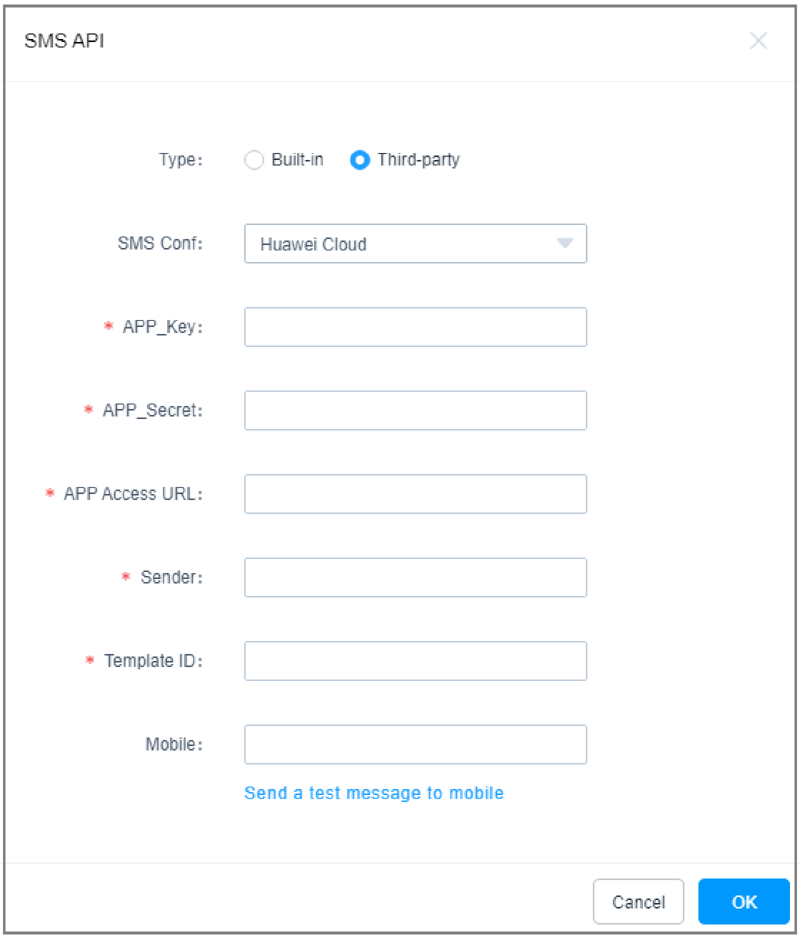
Select the Chinese SMS gateway or international SMS gateway as required.

Step 5 Click **OK**. You can then view SMS gateway configuration on the **Outgoing** tab.

Table 11-2 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.

Figure 11-22 Cloud SMS gateway



----End

11.1.4.3 Configuring LTS

You can use Log Tank Service (LTS) to manage operation logs in the CBH system.

Prerequisites

- You have the management permissions for the **System** module.
- You have enabled Log Tank Service (LTS).
- An EIP has been bound to the CBH instance.

Constraints

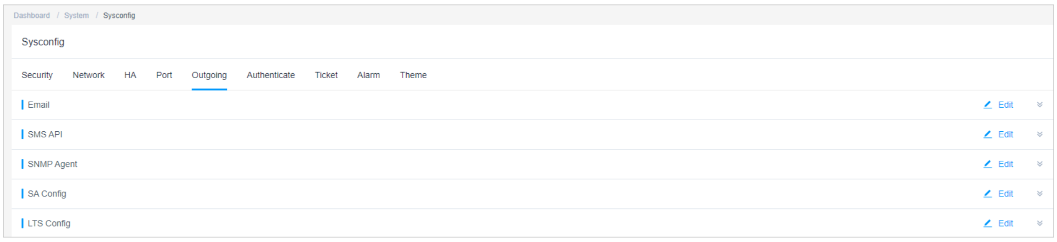
- An EIP must be bound to the CBH instance.
- Log Tank Service (LTS) must be enabled before you configure LTS in CBH.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **System** > **Sysconfig** > **Outgoing**.

Figure 11-23 Outgoing

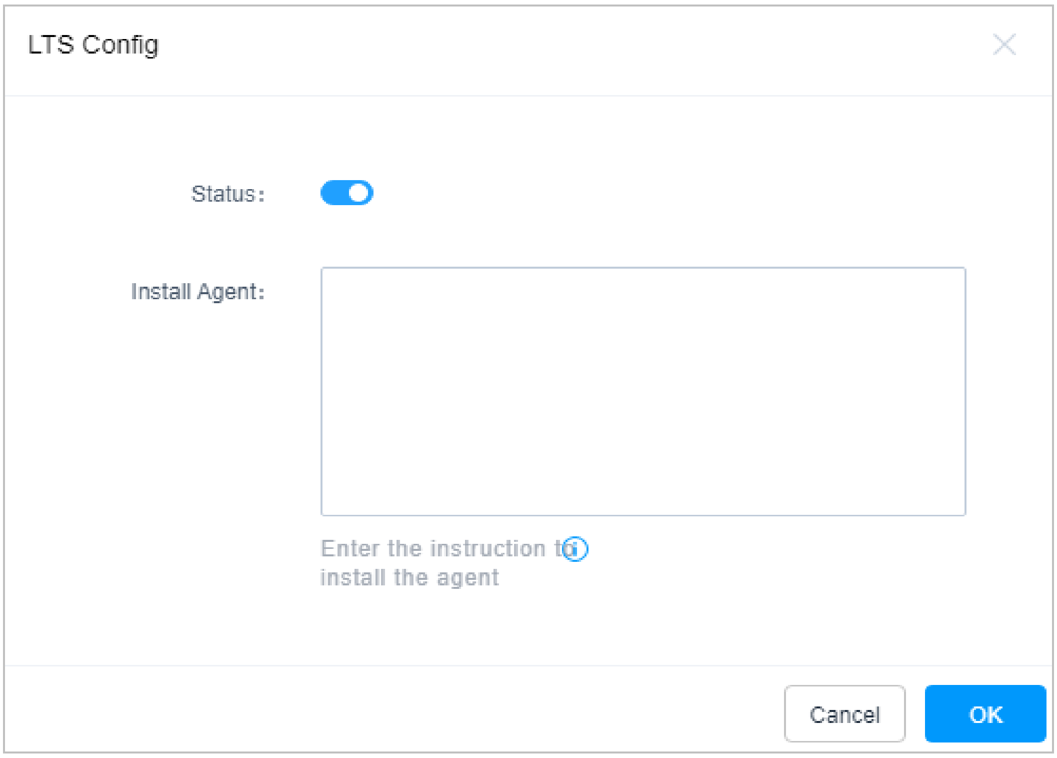


Step 3 On the displayed page, locate the **LTS Config** area and click **Edit**.

Step 4 Click to enable LTS and enter the installation instruction in the **Install Agent** text box.

Click to view how to obtain the installation instruction.

Figure 11-24 LTS Config



Step 5 Click **OK**.

----End

11.1.5 Alarm

11.1.5.1 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 the CBH system.

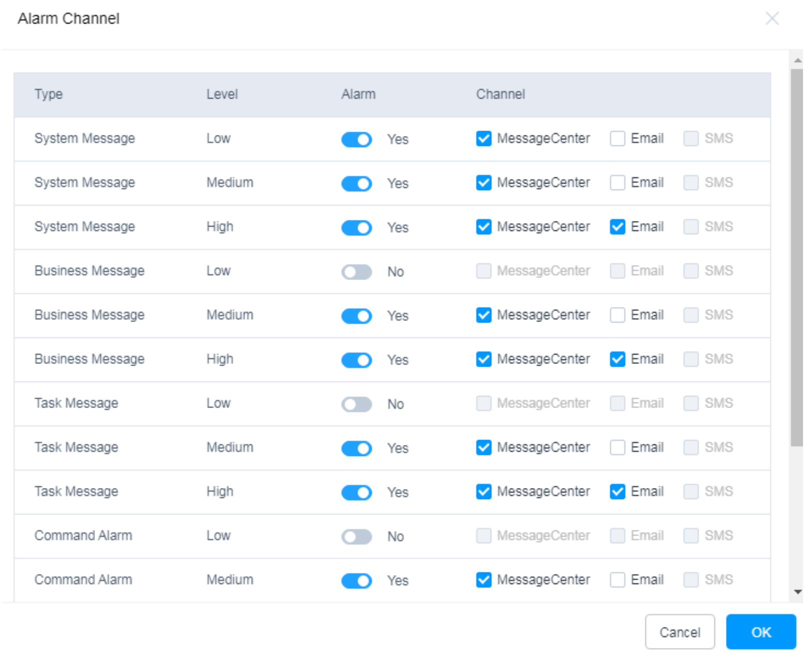
Step 2 Choose **System** > **Sysconfig** > **Alarm**.

Figure 11-25 Alarm

Step 3 In the **Alarm Channel** area, click **Edit**.

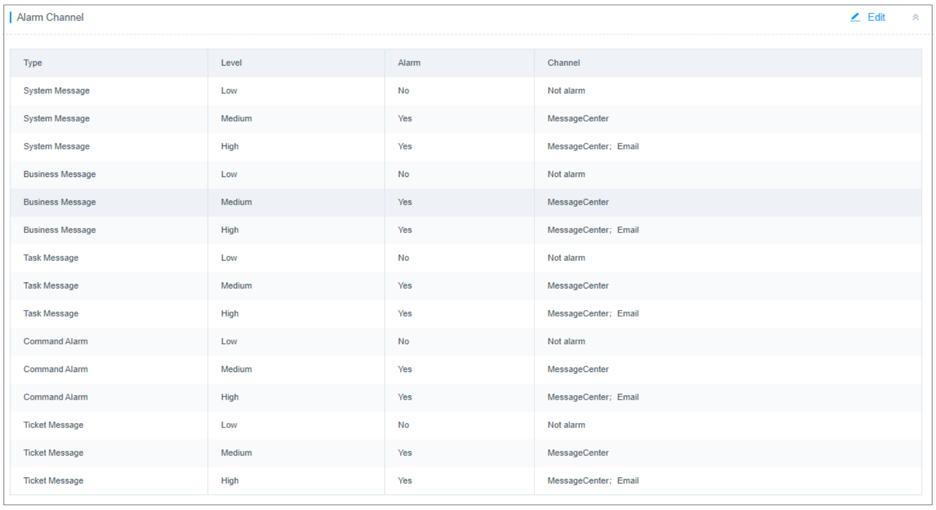
In the displayed **Alarm Channel** dialog box, set alarm channels for different message types.

Figure 11-26 Alarm Channel



Step 4 Click **OK**. You can then view alarm level configuration on the **Alarm** tab.

Figure 11-27 Viewing alarm channels



----End

11.1.5.2 Configuring Alarm Levels

This topic describes how to configure the alarm levels of messages.

Prerequisites

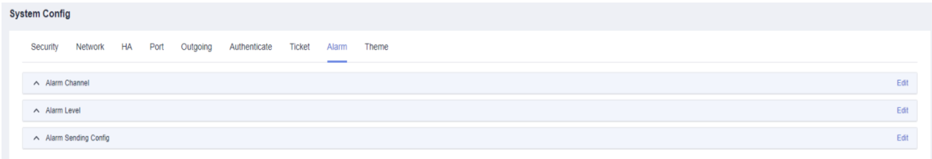
You have the management permissions for the **System** module.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **System** > **Sysconfig** > **Alarm**.

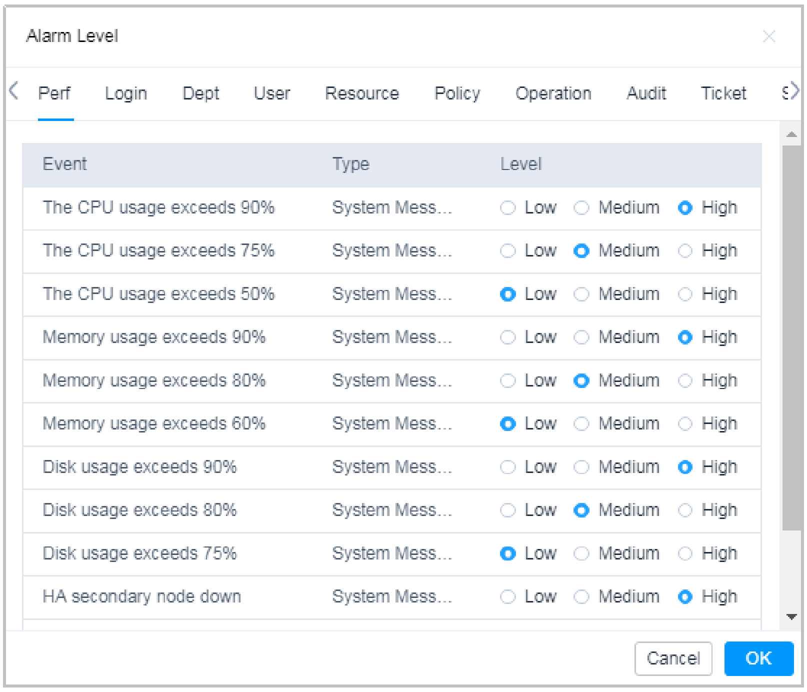
Figure 11-28 Alarm



Step 3 In the **Alarm Level** area, click **Edit**.

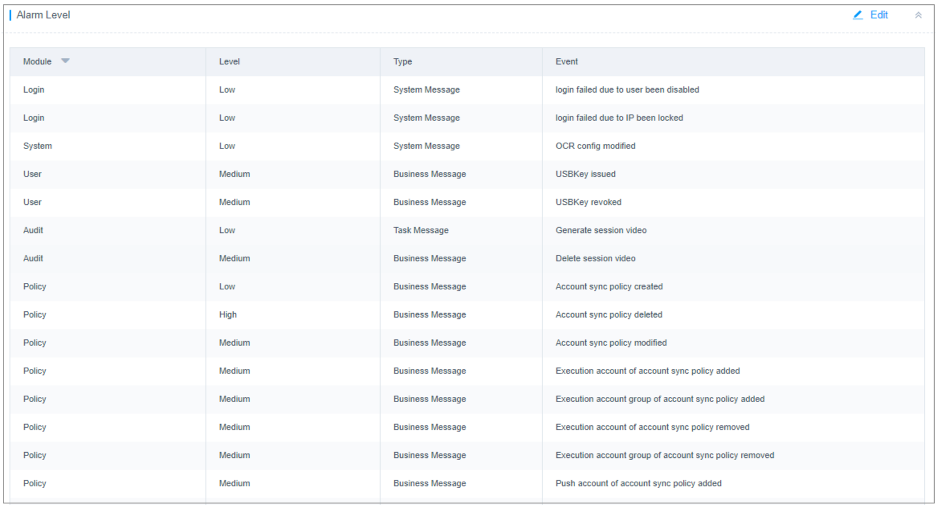
- In the displayed **Alarm Level** dialog box, configure alarm severity levels for different types of messages in each tab.
- The alarm level can be high, medium, or low.

Figure 11-29 Alarm Level



Step 4 Click **OK**. You can then view alarm level configuration on the **Alarm** tab.

Figure 11-30 Viewing alarm levels


Alarm Level

Edit

Module	Level	Type	Event
Login	Low	System Message	login failed due to user been disabled
Login	Low	System Message	login failed due to IP been locked
System	Low	System Message	OCR config modified
User	Medium	Business Message	USBKey issued
User	Medium	Business Message	USBKey revoked
Audit	Low	Task Message	Generate session video
Audit	Medium	Business Message	Delete session video
Policy	Low	Business Message	Account sync policy created
Policy	High	Business Message	Account sync policy deleted
Policy	Medium	Business Message	Account sync policy modified
Policy	Medium	Business Message	Execution account of account sync policy added
Policy	Medium	Business Message	Execution account group of account sync policy added
Policy	Medium	Business Message	Execution account of account sync policy removed
Policy	Medium	Business Message	Execution account group of account sync policy removed
Policy	Medium	Business Message	Push account of account sync policy added

----End

11.1.6 Theme

11.1.6.1 Changing the System Theme

This topic describes how to change the system language and customize system and company logos.

Prerequisites

You have the management permissions for the **System** module.

Theme

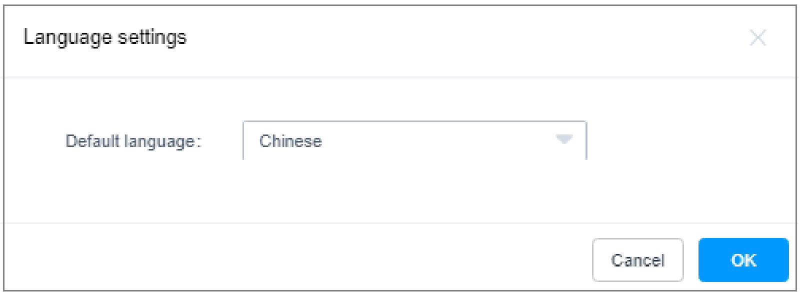
Step 1 Log in to the CBH system.

Step 2 Choose **System** > **Sysconfig** > **Theme**.

Step 3 Switch over the system language.

1. On the displayed page, in the **Language settings** area, click **Edit**.

Figure 11-31 Language settings



2. Select a language. You can select simplified Chinese or English.

3. Click **OK**.

   Then, log out the CBH 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 icon.

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** and then restart the system for the configuration to take effect.

----End

11.2 Data Maintenance

11.2.1 Viewing System Memory

The storage space of the CBH system consists of system partitions and data partitions. If the idle space of the data partition is insufficient, delete historical system data.

This topic describes how to check the system memory usage.

Prerequisites

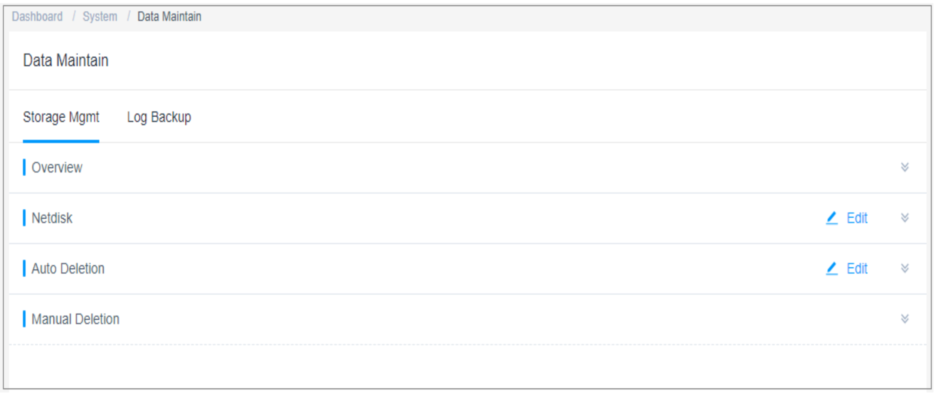
You have the management permissions for the **System** module.

Procedure

Step 1 Log in to the CBH system.

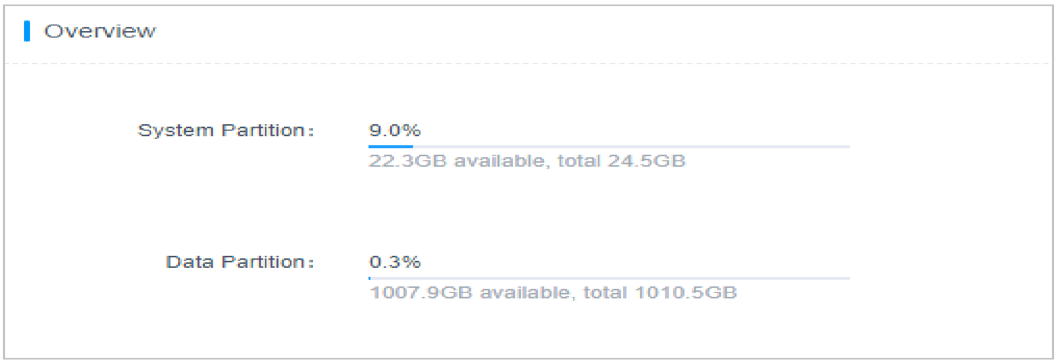
Step 2 Choose **System** > **Data Maintain** > **Storage Mgmt**.

Figure 11-32 Storage Management



Step 3 In the **Overview** area, view the space usage of the system partition and data partition.

Figure 11-33 Storage space overview



----End

11.2.2 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 the CBH system.

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 CBH system 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

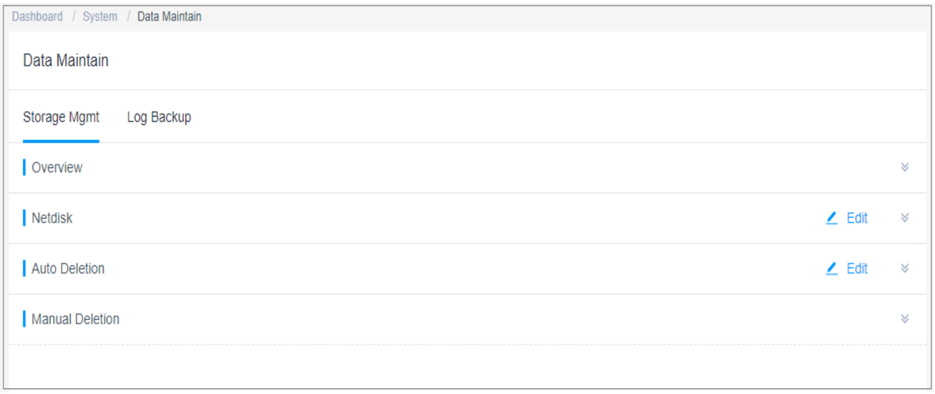
You have the management permissions for the **System** module.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **System** > **Data Maintain** > **Storage Mgmt**.

Figure 11-34 Storage Management

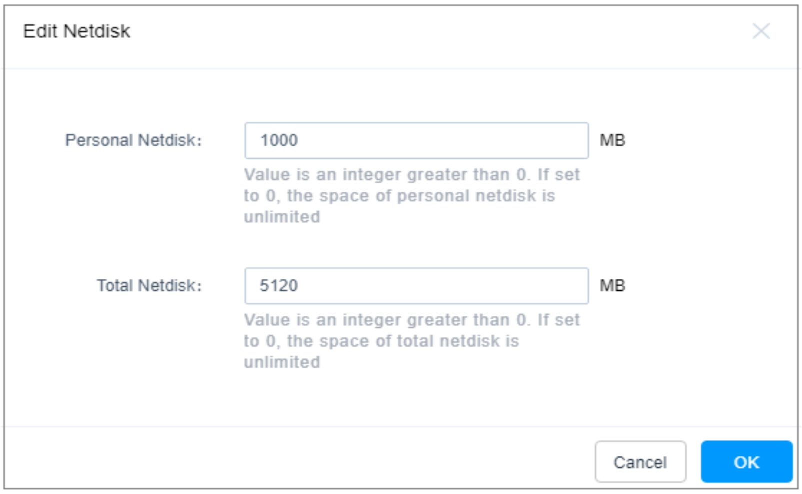


Step 3 In the **Netdisk** area, click **Edit**. In the displayed dialog box, set the disk size.

Table 11-3 Netdisk parameters

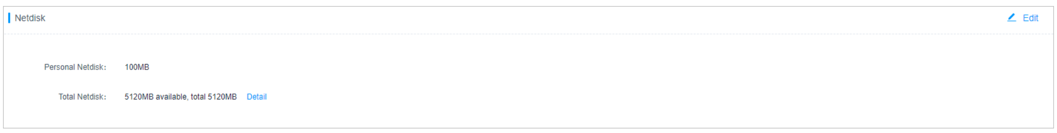
Parameter	Description
Personal Netdisk	A private disk exclusively used by the current user ● The default value is **100 MB**. ● To use the personal net disk unlimitedly when the system data disk capacity is allowed, set **Personal Netdisk** to **0**.
Total Netdisk	Total netdisk capacity. ● The default 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**.

Figure 11-35 Edit Netdisk



Step 4 Click **OK**. You can then view capacity of the configured **Personal Netdisk** and **Total Netdisk** on the **Storage Mgmt** tab.

Figure 11-36 Total Netdisk



Step 5 Click **Detail** and view details about the net disk.

Step 6 In the row containing the net disk, click **user.button.deleteNetDiskData** in the **Operation** column.

NOTE

You can also select all net disks from which you want to delete data and click **user.button.deleteNetDiskData** to clear the disks together.

----End

11.2.3 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.

DANGER

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 the CBH system.

Step 2 Choose **System** > **Data Maintain** > **Storage Mgmt**.

Step 3 In the **Auto Deletion** area, click **Edit**. In the displayed dialog box, set related parameters.

Figure 11-37 Configuring Auto Deletion

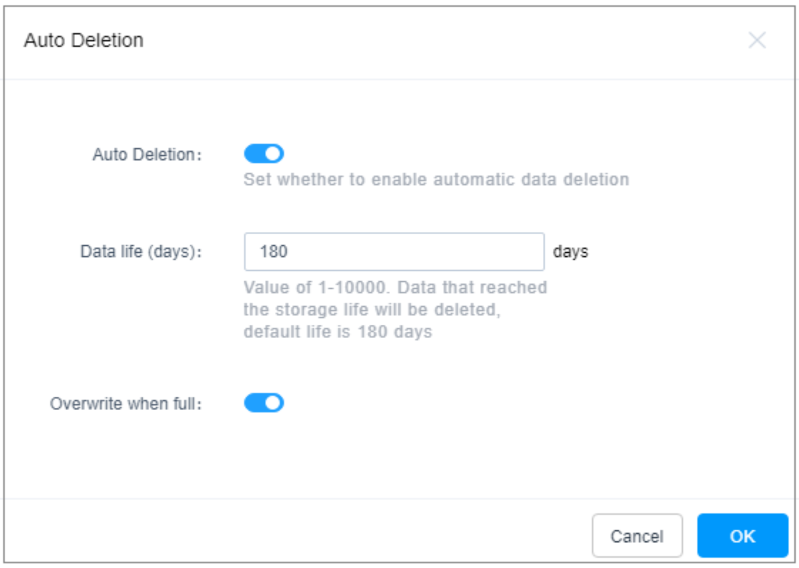
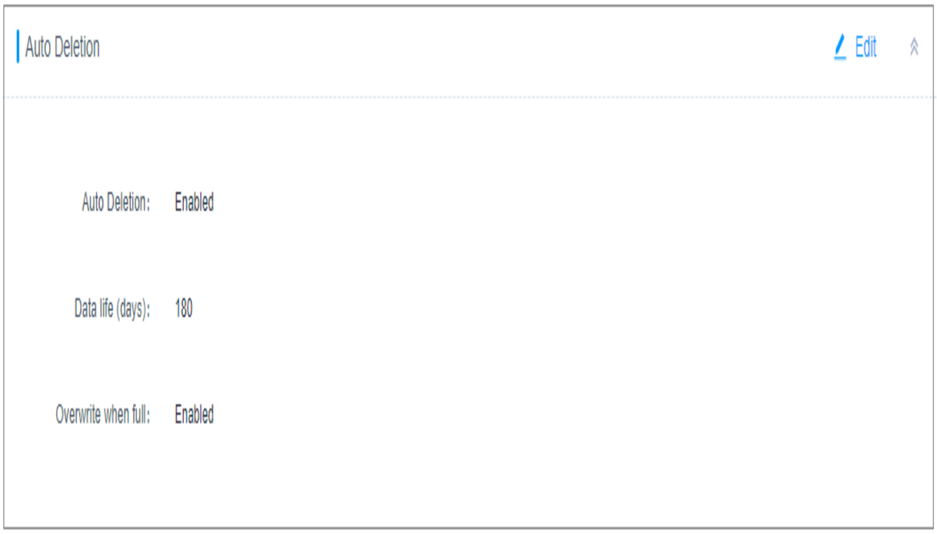


Table 11-4 Configuring Auto Deletion

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	When the data disk usage exceeds 90%, data on the disk will be automatically deleted. 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.
Delete Content	The options are as follows: ● System Log ● Session Log

Step 4 Click **OK**.

Figure 11-38 Auto Deletion



----End

Manual Deletion

Step 1 Log in to the CBH system.

Step 2 Choose **System** > **Data Maintain** > **Storage Mgmt**.

Step 3 In the **Manual Deletion** area, select a date.

Step 4 Click **Delete**. Data generated before the selected date is deleted.

----End

11.2.4 Creating a Local Data Backup

To enhance data disaster recovery management and improve audit data security and system scalability, CBH enables backup of configuration logs.

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 the CBH system.

Step 2 Choose **System** > **Data Maintain** > **Log Backup**.

Figure 11-39 Log Backup

Step 3 In the **Data Backup Locally** area, click **Add**. In the displayed dialog box, configure backup content and date range.

Figure 11-40 Data Backup Locally

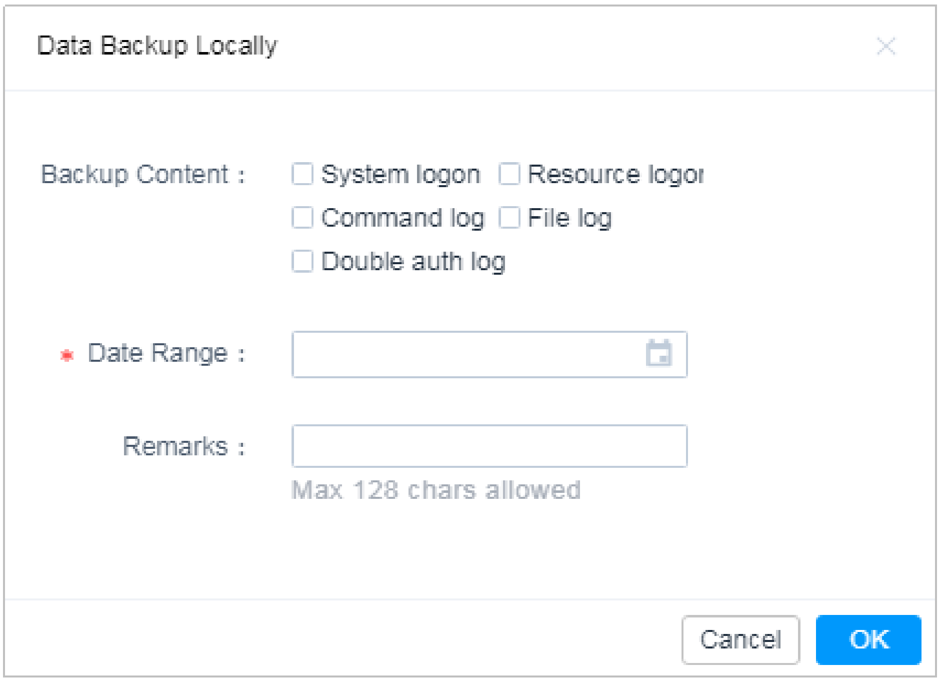
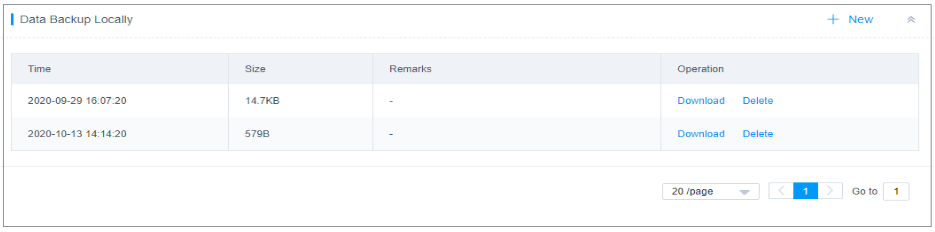


Table 11-5 Creating a Local Backup

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.
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 11-41 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.

11.2.5 Configuring the Syslog Server for Remote Backup

To enhance data disaster recovery management and improve audit data security and system scalability, CBH enables backup of configuration logs.

This topic walks you through how to configure the Syslog 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 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 the CBH system.

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.

Figure 11-42 Backup to the Syslog server

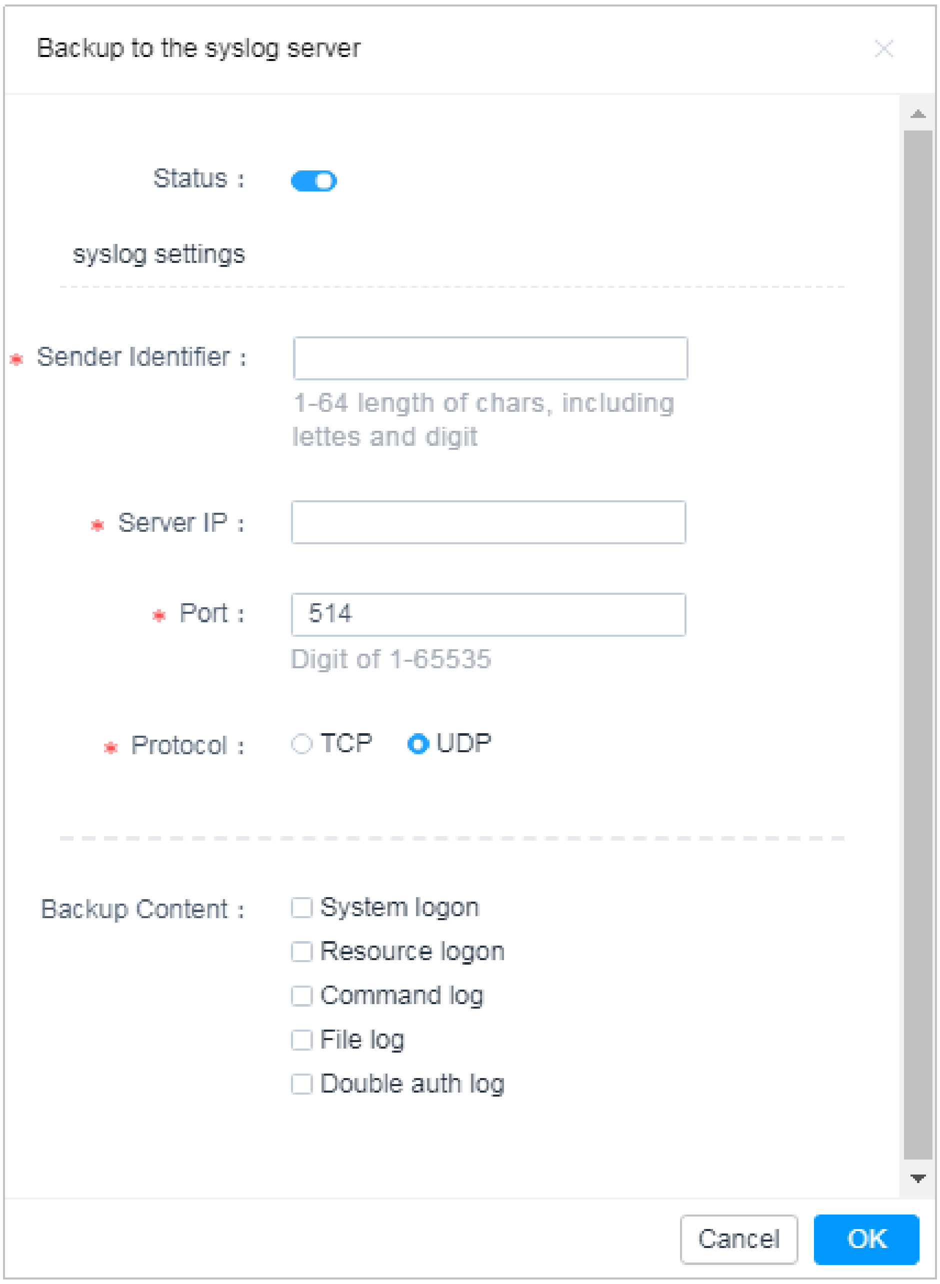


Table 11-6 Parameters for configuring the Syslog server

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.

Parameter	Description
Sender Identifier	Identifier for connecting the CBH system to the Syslog server. The identifier is used to identify the CBH system 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	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.

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.

Figure 11-43 Syslog server backup information

----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.

11.2.6 Configuring an FTP/SFTP Server for Remote Log Backup

To enhance data disaster recovery management and improve audit data security and system scalability, CBH enables backup of configuration logs.

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 the CBH system.

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.

Figure 11-44 Backup to the FTP/SFTP server

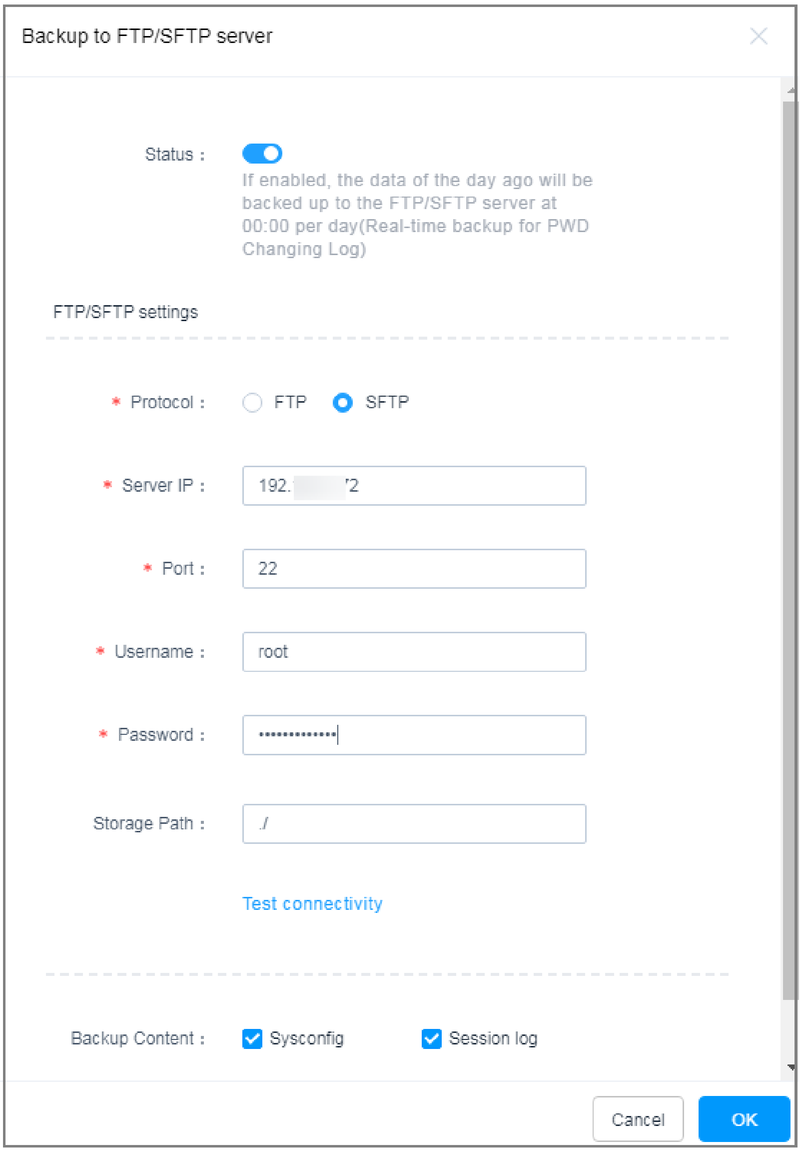


Table 11-7 Parameters for configuring the FTP or SFTP server

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.
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.

Parameter	Description
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.
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 CBH system and the FTP or SFTP server. The user account of the server is not verified.
Backup Content	Type of logs to be backed up ● The options are **Sysconfig** and **Session log**. ● Select at least one log type.

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.

Figure 11-45 FTP or SFTP server backup information

----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.

11.2.7 Configuring OBS Buckets for Remote Log Backup

To enhance data disaster recovery management and improve audit data security and system scalability, CBH enables backup of configuration logs.

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 the CBH system is normal.

Procedure

Step 1 Log in to the CBH system.

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.

Figure 11-46 Remote Backup To OBS

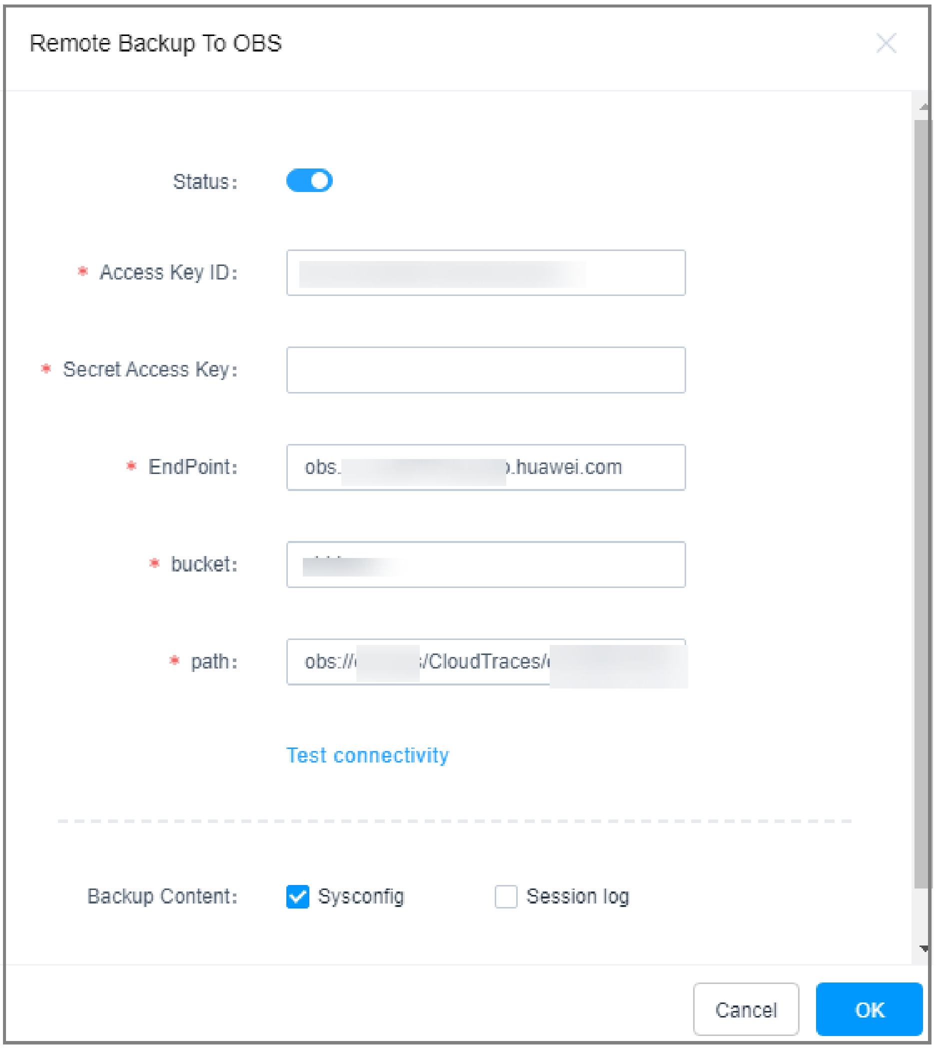


Table 11-8 Parameters for remote backup to OBS

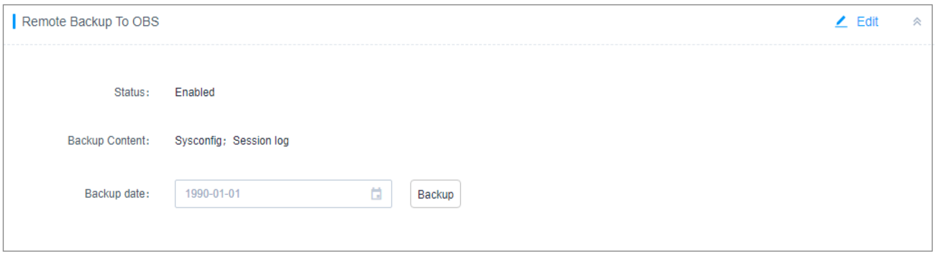
Parameter	Description
Status	Whether to back up logs to an OBS bucket (default:). • : Backing up logs to OBS buckets is enabled. The system automatically starts backup at 00:00 every day. • : Backing up logs to OBS buckets is disabled.
Access Key ID	Specifies the access key ID, which is used to verify 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**.

Parameter	Description
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.
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 the CBH system and the configured OBS bucket is reachable. The connectivity test checks only the network status between the CBH system and the OBS bucket.
Backup Content	Type of logs to be backed up ● The options are **Sysconfig**, **Session log**, **System Login**, **Resource Logon**, **Command log**, **File log**, and **Double auth log**. ● Select at least one log type.

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.

Figure 11-47 OBS bucket information



----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.

11.3 System Maintenance

11.3.1 Viewing System Status

To ensure the healthy running of the CBH system, monitor 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

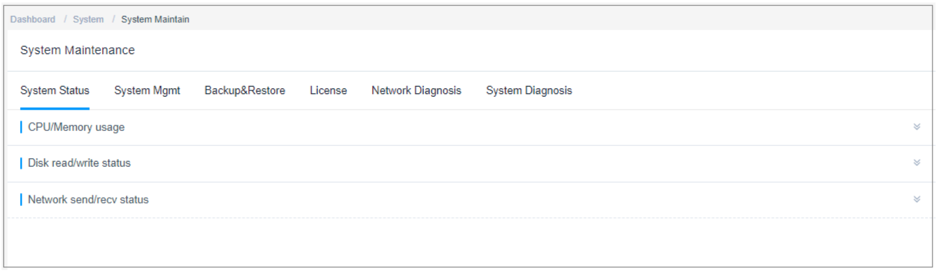
You have the management permissions for the **System** module.

Viewing System CPU and Memory Usage

Step 1 Log in to the CBH system.

Step 2 Choose **System** > **System Maintain** > **System Status**.

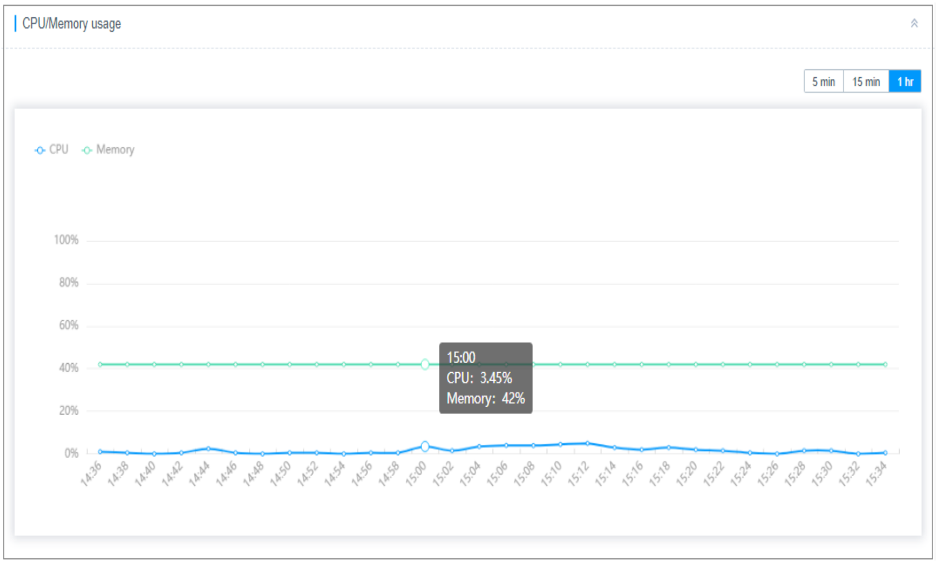
Figure 11-48 Viewing System Status



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.

Figure 11-49 Viewing System CPU and Memory Usage



----End

View Disk Read/write Status

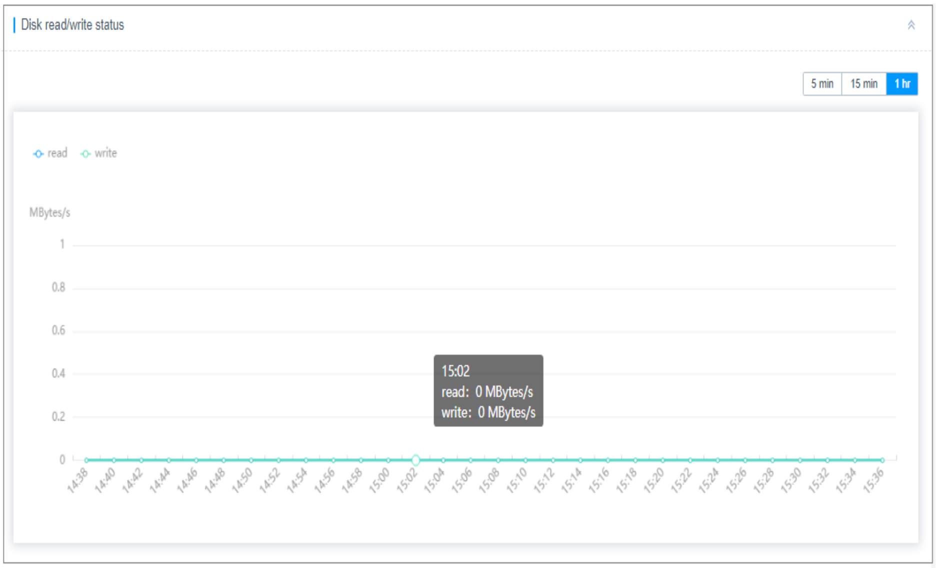
Step 1 Log in to the CBH system.

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.

Figure 11-50 View Disk Read/write Status



----End

Viewing Network Sending and Receiving Status

Step 1 Log in to the CBH system.

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 11-51 Network sending and receiving status

----End

11.3.2 System Mgmt

This topic describes how to update the system IP address, time, and version, how to restart, shut down, and restore the system, and how to manage the basic system information and status.

Prerequisites

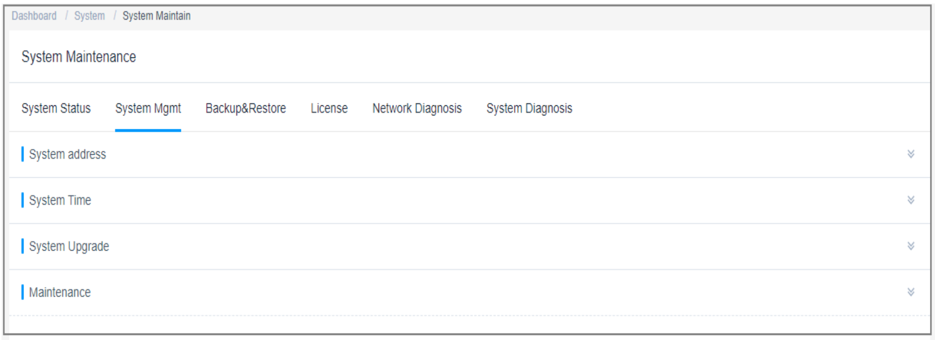
You have the management permissions for the **System** module.

Managing System Addresses

Step 1 Log in to the CBH system.

Step 2 Choose **System** > **System Maintain** > **System Mgmt**.

Figure 11-52 System Mgmt

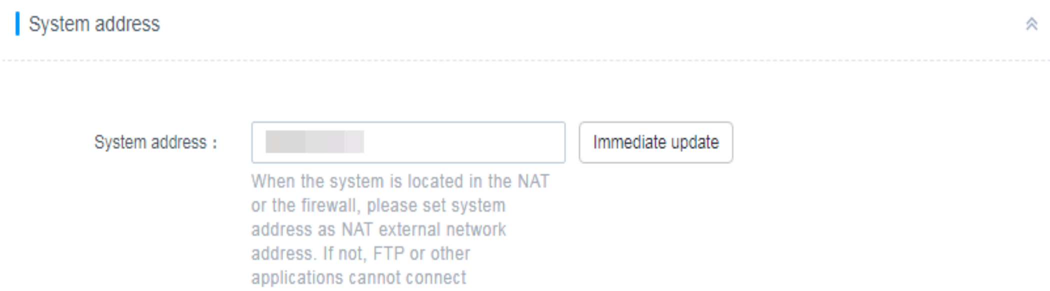


Step 3 Expand the **System address** area.

Step 4 Update the system IP address.

- After the EIP bound to the mapped CBH instance 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 11-53 System address



----End

Managing System Time

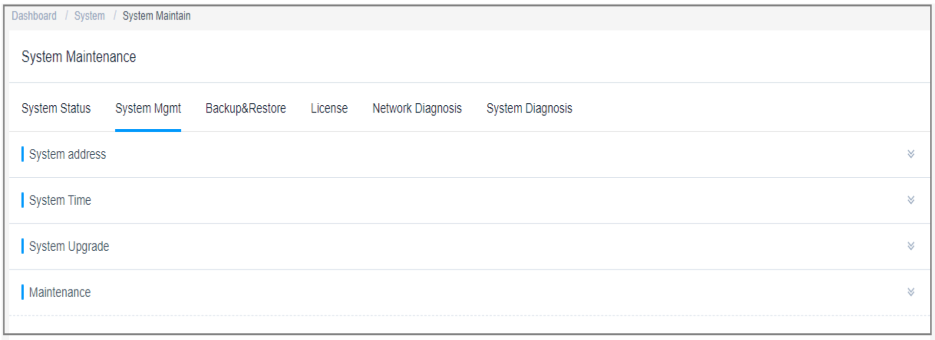
NOTE

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 CBH system.

Step 1 Log in to the CBH system.

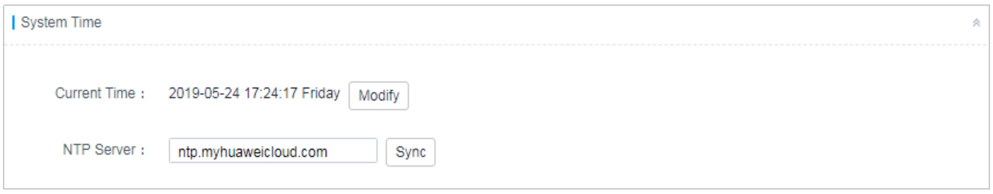
Step 2 Choose **System** > **System Maintain** > **System Mgmt**.

Figure 11-54 System Mgmt



Step 3 Expand the **System Time** area.

Figure 11-55 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**.

Figure 11-56 Edit System Time

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**.

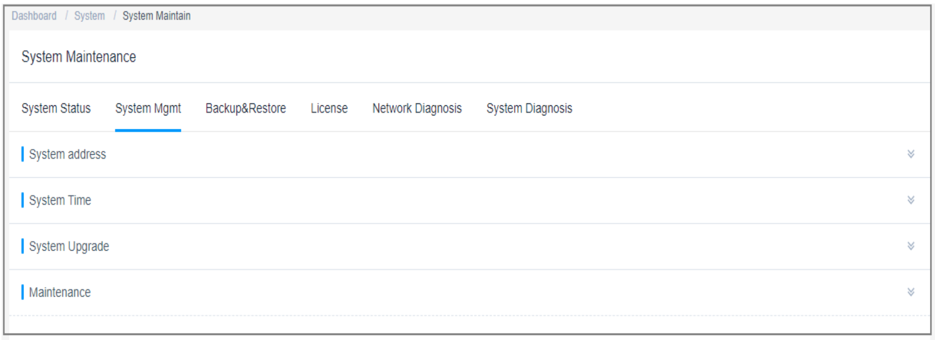
----End

Managing System Version

Step 1 Log in to the CBH system.

Step 2 Choose **System** > **System Maintain** > **System Mgmt**.

Figure 11-57 System Mgmt



Step 3 Expand the **System Upgrade** area.

Figure 11-58 System Upgrade

Step 4 Upgrade 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.

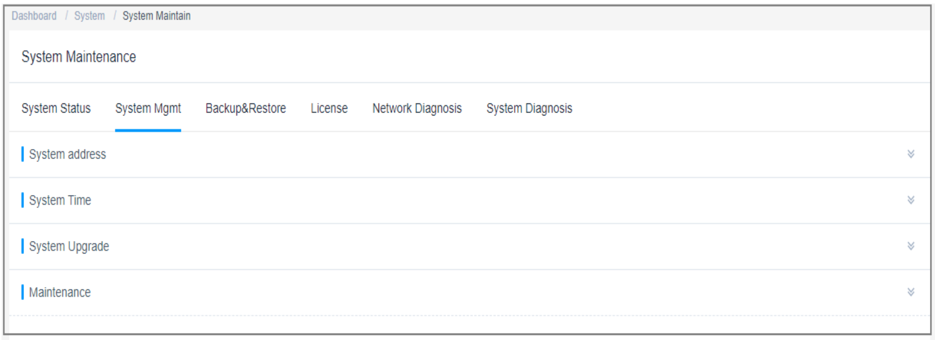
----End

Managing System Tools

Step 1 Log in to the CBH system.

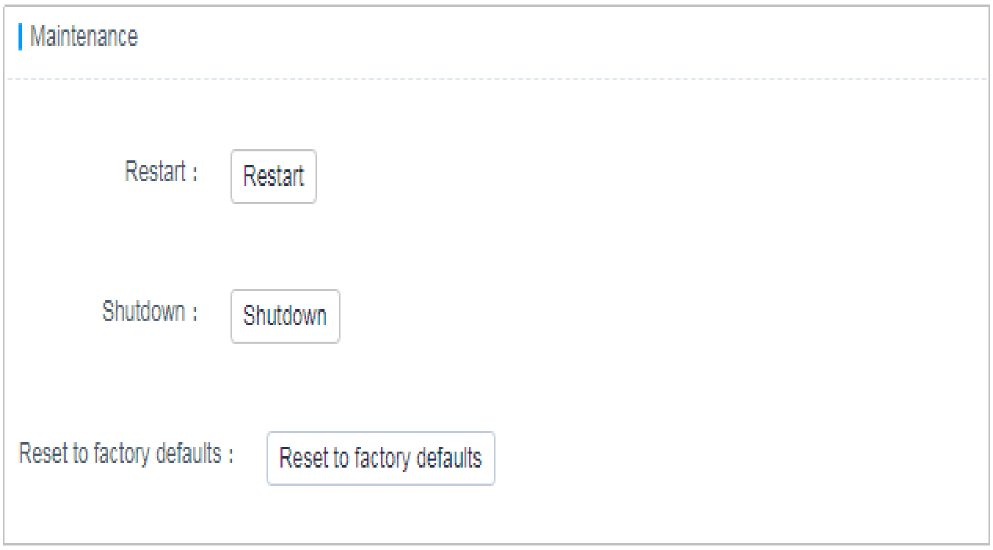
Step 2 Choose **System** > **System Maintain** > **System Mgmt**.

Figure 11-59 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 11-60 Maintenance



- Restarting the system

  NOTE

  To restart a CBH system, restarting the mapped CBH instance is recommended. For details, see **Restarting a CBH Instance**.

  a. Click **Restart**.
  b. In the displayed confirmation dialog box, click **OK**.
  c. Enter the password of system administrator **admin**.
  d. Click **OK**. After the verification is successful, you can log in to the system.

- Shutting down the system

  NOTE

  To stop a CBH system, stopping the mapped CBH instance is recommended. For details, see **Stopping a CBH Instance**.

  a. Click **Shutdown**.
  b. In the displayed confirmation dialog box, click **OK**.

c. Enter the password of system administrator **admin**.
d. Click **OK**.

- Restoring factory settings
  a. Click **Reset to factory defaults**.
  b. In the displayed confirmation dialog box, click **OK**.
  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.

DANGER

Do not restore factory settings unless in emergencies. Otherwise, all system data will be lost.

----End

11.3.3 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

Constraints

- System configuration backup files can be used only for the corresponding CBH system.
- 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

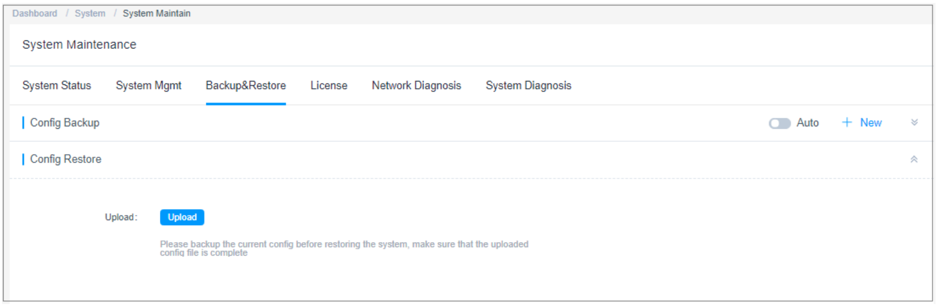
You have the management permissions for the **System** module.

Backing Up System Configuration Data

Step 1 Log in to the CBH system.

Step 2 Choose **System** > **System Maintain** > **Backup&Restore**.

Figure 11-61 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.

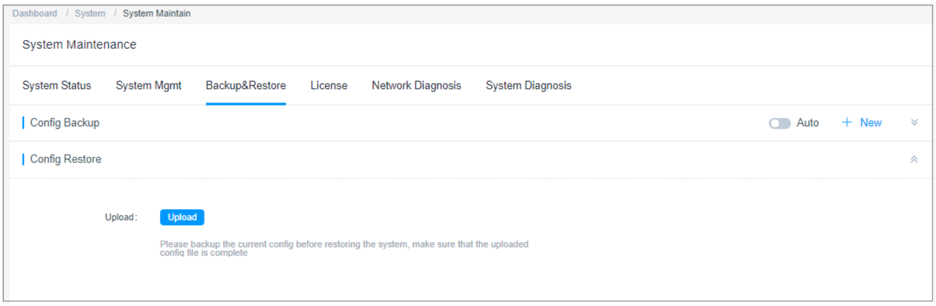
----End

Restoring System Configurations

Step 1 Log in to the CBH system.

Step 2 Choose **System** > **System Maintain** > **Backup&Restore**.

Figure 11-62 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**.

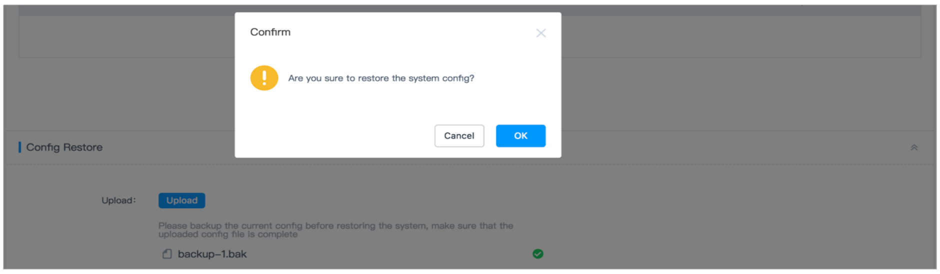
- Using a local backup file to restore system configurations

  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**.

Figure 11-63 Confirming 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.

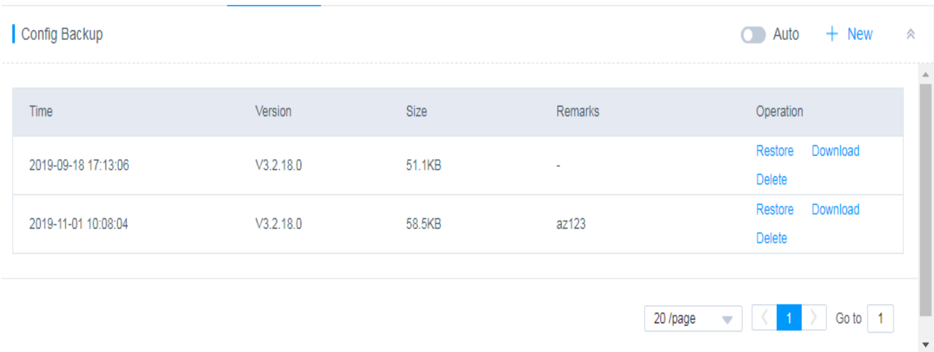
Step 1 Log in to the CBH system.

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.

Figure 11-64 Backup file list



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

11.3.4 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.

This topic walks you through how to view system license.

Prerequisites

You have the management permissions for the **System** module.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **System** > **System Maintain** > **License** and view the current license information.

Figure 11-65 License

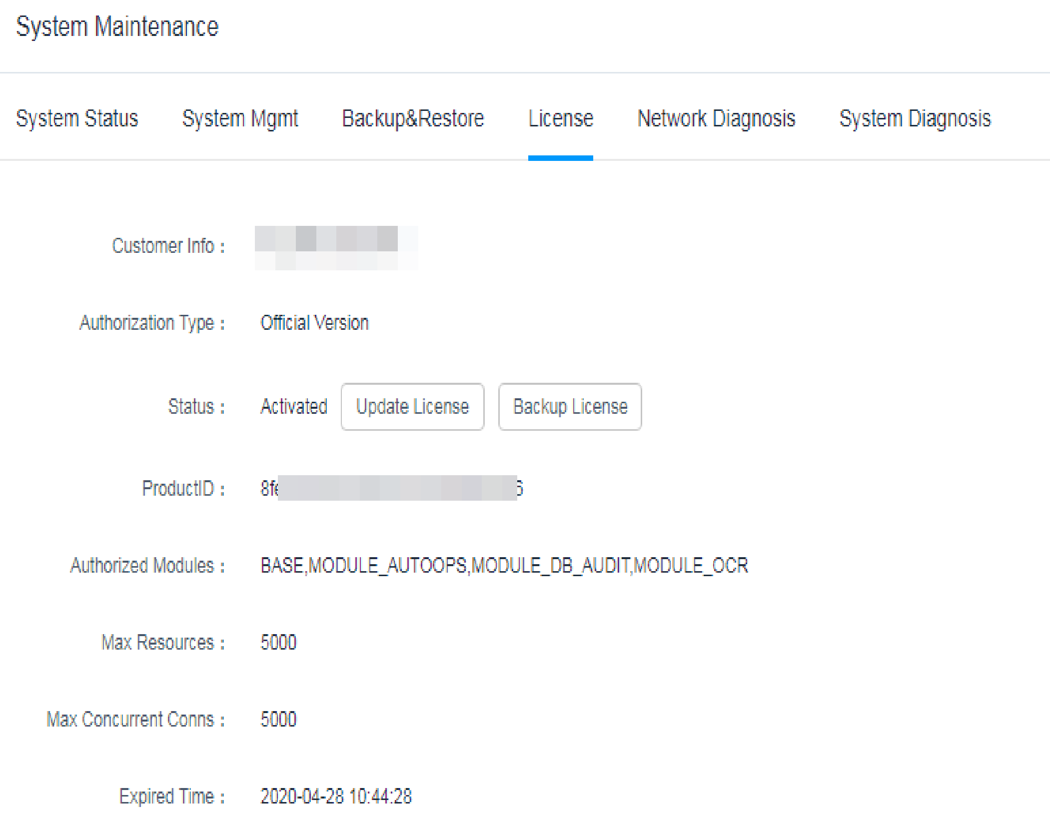


Table 11-9 License parameters

Parameter	Description
Customer Info	Region and AZ where the system is used
Authentication Type	By default, **Official Version** is set for **Authentication 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 the CBH system.
Product ID	Product ID of the current system
Authorized Modules	Supported function modules. The function modules available depend on the edition you are using. CBH has standard editions and professional editions. ● CBH standard editions: include only basic modules. ● CBH professional editions: include basic modules, **automatic O&M**, and **database audit**. – Automatic O&M includes the **Sync Rules**, **Script**, **Fast Ops**, 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 the CBH system and install local database tools for the CBH system to access databases.
Max Resources	Maximum number of resources that can be added to the CBH system (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.
Expired Time	Time when the system license expires

----End

11.3.5 Network Diagnosis

With network diagnosis, you can quickly check whether the network between the CBH system and a managed host is connected if the managed host fails to be logged in. CBH can use any of the following methods to check the connectivity:

- Ping the host IP address to check whether the CBH system communicates with the host over the ICMP protocol.
- Perform route tracing on the host address to check whether the route between the CBH system and the host is reachable.
- Perform the TCP port test on the host IP address to check whether the CBH system is connected to the TCP port on the 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

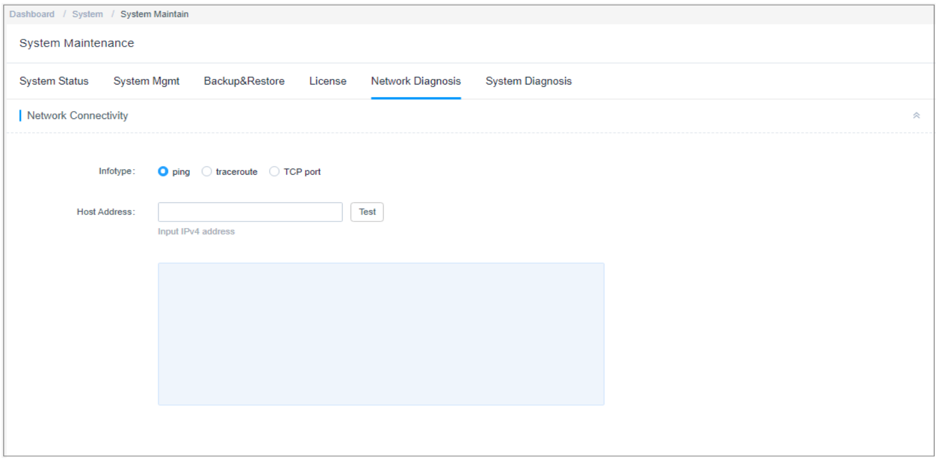
You have the management permissions for the **System** module.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **System** > **System Maintain** > **Network Diagnosis**.

Figure 11-66 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 **traceroute**.
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

11.3.6 System Diagnosis

With system diagnosis, you can easily obtain information about the current system, including comprehensive information and details about system load, kernel, memory, network interface card (NIC), disk usage, routes, and ARP.

This topic describes how to obtain the system background information.

Prerequisites

You have the management permissions for the **System** module.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **System** > **System Maintain** > **System Diagnosis**.

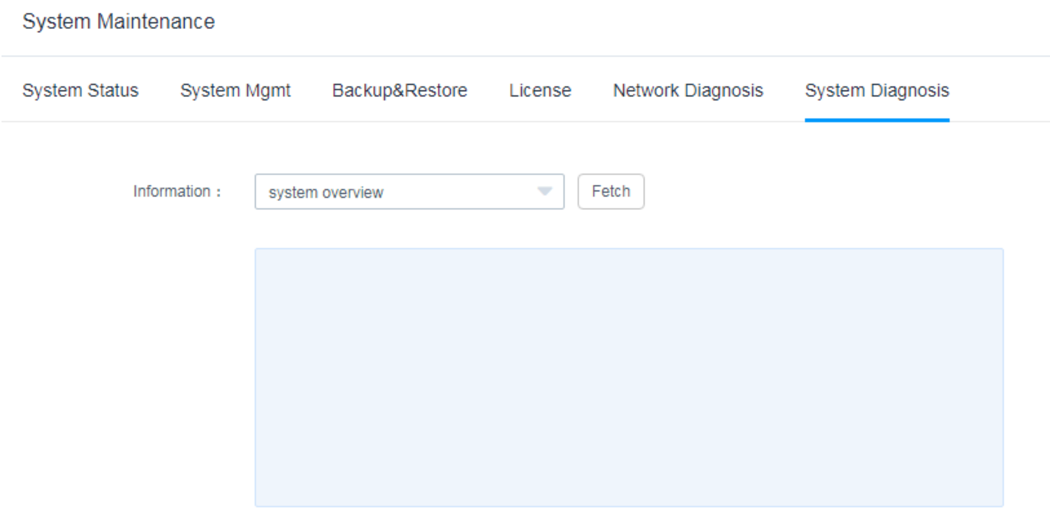
Step 3 Select an information type and then click **Fetch** to view the details.

Table 11-10 System diagnosis parameters

Parameter	Description
system overview	Obtains overview information about the CBH system, including memory, I/O, and CPU.
system load	Obtains information about the CBH system load.
system kernel	Obtains information about the CBH system kernel.
memory summary	Obtains information about the CBH system memory.
network interfaces	Obtains information about the CBH system NIC.
disk usage	Obtains information about the disk usage of the CBH system.
route table	Obtains route information about the CBH system.

Parameter	Description
ARP table	Obtains ARP information about the CBH system.

Figure 11-67 System Diagnosis



----End

11.4 About System

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 the CBH system.

Step 2 On the left navigation pane, choose **System** > **About**.

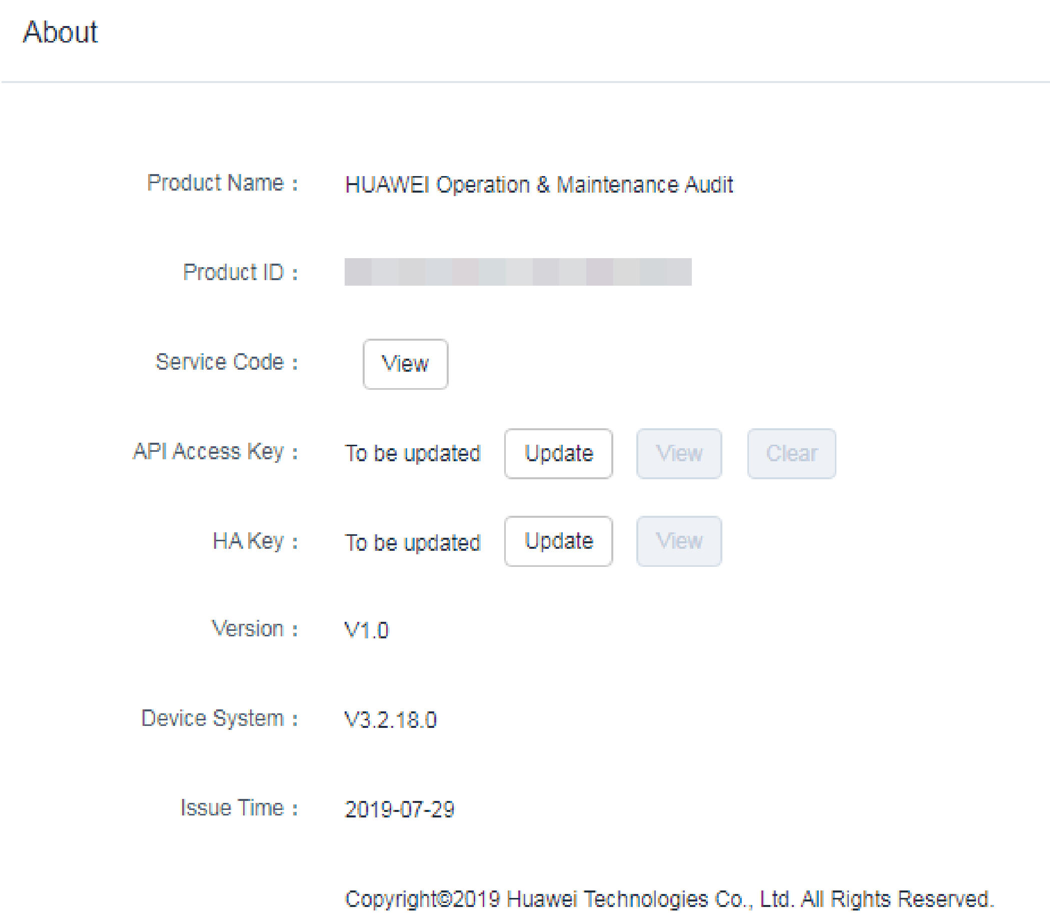
Step 3 View basic system information.

Table 11-11 System parameters

Parameter	Description
Product Name	CBH
Product ID	Unique authentication code of a product

Paramete r	Description
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 current system
Device System	Version of the current system software
Issue Time	Release date of the current system

Figure 11-68 About



----End

12 Installing an Application Server

12.1 Installing a Windows Server 2019 Application Server

12.1.1 Adding Roles and Features

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

12.1.2 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.

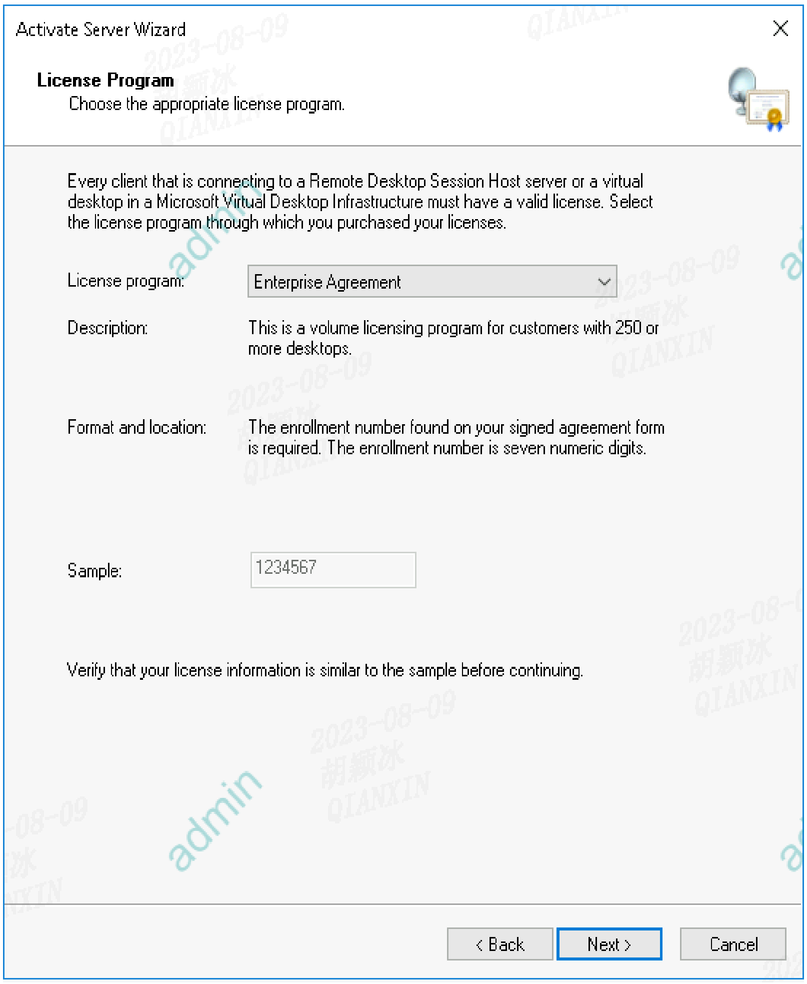
Step 6 Enter the information about your company and user name.

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**.

Figure 12-1 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

12.1.3 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

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 the CBH system.

----End

12.1.4 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 ***RemoteaProxyInstaller_xxx.zip*** (xxx is the version number) package.

Download the required software package at:

- **RemoteaProxyInstaller_v3.3.26.0 to v3.3.37.0 and later**
- **RemoteaProxyInstaller_v3.3.38.0 and later**
- **RemoteaProxy1.1.19.0 download link** (adapts to all bastion host versions)

NOTE

The server must have an EIP bound.

Step 3 Decompress **RemoteaProxyInstaller_*xxx*.zip** (*xxx* indicates the version number).

Step 4 Double-click **RemoteaProxyInstaller_*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

12.2 Installing a Windows Server 2016 Application Server

12.2.1 Adding Roles and Features

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

12.2.2 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.

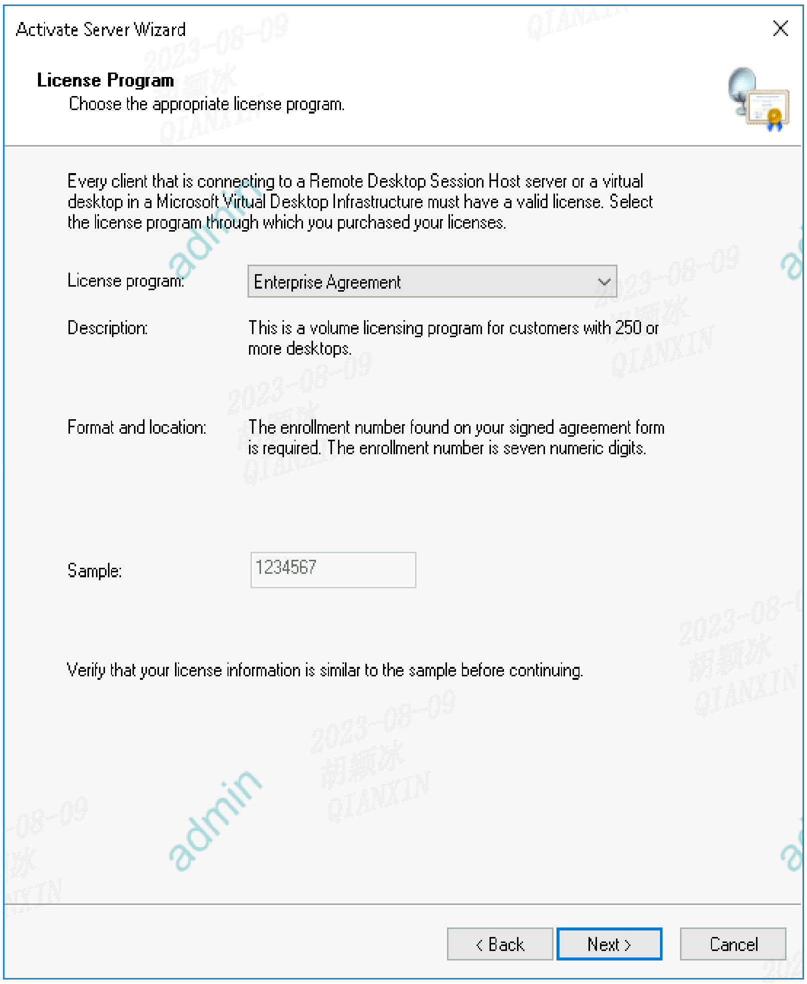
Step 6 Enter the information about your company and user name.

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**.

Figure 12-2 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

12.2.3 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 (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 the CBH system.

----End

12.2.4 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 ***RemoteaProxyInstaller_xxx.zip*** (xxx is the version number) package.

Download the required software package at:

- **RemoteaProxyInstaller_v3.3.26.0 to v3.3.37.0 and later**
- **RemoteaProxyInstaller_v3.3.38.0 and later**
- **RemoteaProxy1.1.19.0 download link** (adapts to all bastion host versions)

NOTE

The server must have an EIP bound.

Step 3 Decompress **RemoteaProxyInstaller_*xxx*.zip** (*xxx* indicates the version number).

Step 4 Double-click **RemoteaProxyInstaller_*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

12.3 Installing a Windows Server 2012 R2 Application Server

12.3.1 Adding Roles and Features

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

12.3.2 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 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.

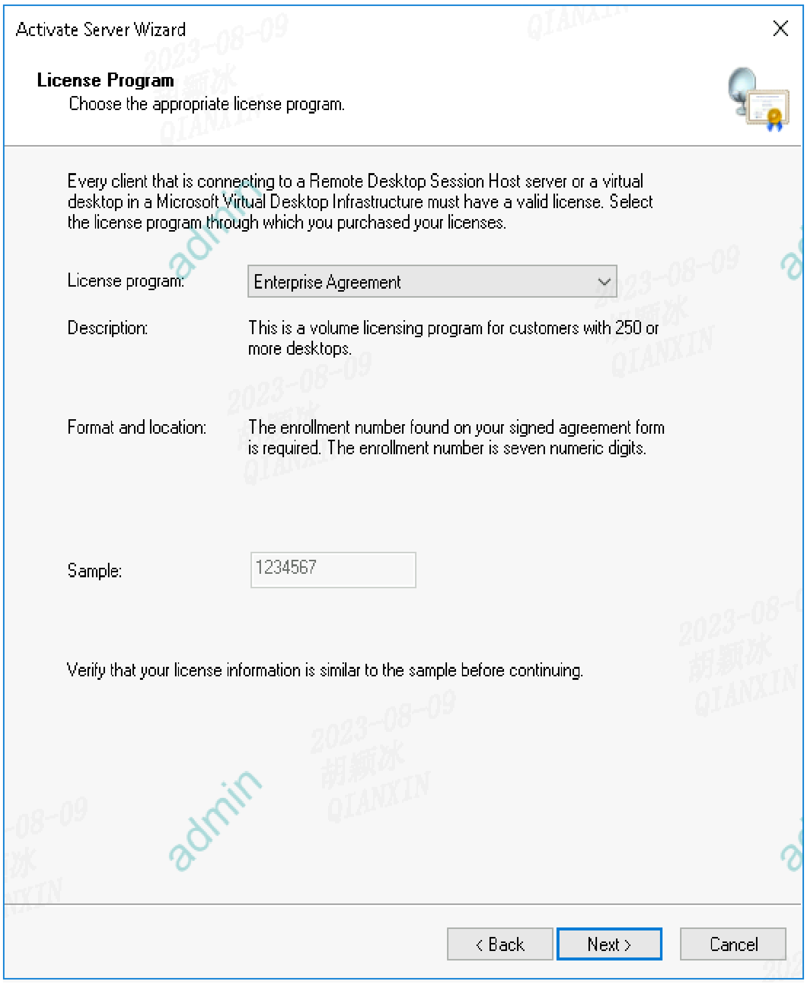
Step 5 Enter the information about your company and user name.

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**.

Figure 12-3 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

12.3.3 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

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 the CBH instance.

----End

12.3.4 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 ***RemoteaProxyInstaller_xxx.zip*** (xxx is the version number) package.

Download the required software package at:

- **RemoteaProxyInstaller_v3.3.26.0 to v3.3.37.0 and later**
- **RemoteaProxyInstaller_v3.3.38.0 and later**
- **RemoteaProxy1.1.19.0 download link** (adapts to all bastion host versions)

NOTE

The server must have an EIP bound.

Step 3 Decompress **RemoteaProxyInstaller_*xxx*.zip** (*xxx* indicates the version number).

Step 4 Double-click **RemoteaProxyInstaller_*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

12.4 Installing a Windows Server 2008 R2 Application Server

12.4.1 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

12.4.2 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*.

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

12.4.3 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

12.4.4 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

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 the CBH instance.

----End

12.4.5 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 ***RemoteaProxyInstaller_xxx.zip*** (xxx is the version number) package.

Download the required software package at:

- **RemoteaProxyInstaller_v3.3.26.0 to v3.3.37.0 and later**
- **RemoteaProxyInstaller_v3.3.38.0 and later**
- **RemoteaProxy1.1.19.0 download link** (adapts to all bastion host versions)

NOTE

The server must have an EIP bound.

Step 3 Decompress **RemoteaProxyInstaller_*xxx*.zip** (*xxx* indicates the version number).

Step 4 Double-click **RemoteaProxyInstaller_*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

12.5 Installing a Linux Application Server

Basic Environment Requirements

- System requirements: CentOS release 7.9 minor
- Network requirements: The server must have an EIP bound.
- Firewall requirements: Port 2376 for Docker services and ports 35000 to 40000 must be allowed.

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 12-1 app_publisher version description

CBH Version	Supported Architecture	app_publisher Version	Download URL
V3.3.26.0	x86 and Arm	V1.0.0	**Software Package**
V3.3.30.0	x86 and Arm	V1.1.0	**Software Package**
V3.3.38.0	X86	V1.2.0_CentOS7	**Software Package**
	ARM	V1.2.0_UOS20	**Software Package**
V3.3.40.0	X86	V1.3.0_CentOS7	**Software Package**
	ARM	V1.3.0_UOS	**Software Package**
V3.3.43.0	X86	V1.4.0_CentOS7	**Software Package**
	ARM	V1.4.0_UOS	**Software Package**
V3.3.46.0	X86	V1.5.0_CentOS7	**Software Package**
	ARM	V1.5.0_UOS	**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

13 Monitoring

13.1 CBH Monitoring Metrics

Description

This topic describes metrics reported by CBH 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 CBH.

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 13-1 CBH metrics

Metric ID	Metric Name	Description	Value Range	Monitored Object	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%	CBH	300s
mem_util	Memory Usage	Memory usage of the monitored object	0%~100%	CBH	300s
disk_util	Disk Usage	Disk usage of the monitored object	0%~100%	CBH	300s
session_count	Session Connections	Number of session connections of the monitored object	≥0	CBH	300s
resource_count	Managed Resources	Total number of resources managed by the monitored object	≥0	CBH	300s

Dimensions

Key	Value
server_id	CBH instance ID

13.2 Configuring Monitoring Alarm Rules

You can set CBH 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 the CBH status in a timely manner.

Prerequisites

A CBH instance has been created.

Procedure

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

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

Step 3 Hover your mouse over in the upper left corner of the page and choose **Management & Governance** > **Cloud Eye**.

Step 4 In the navigation pane on the left, choose **Alarm Management** > **Alarm Rules**.

Step 5 In the upper right corner of the page, click **Create Alarm Rule**.

Step 6 Enter the alarm rule information by referring to **Table 13-2**.

Figure 13-1 Configuring CBH alarm rules

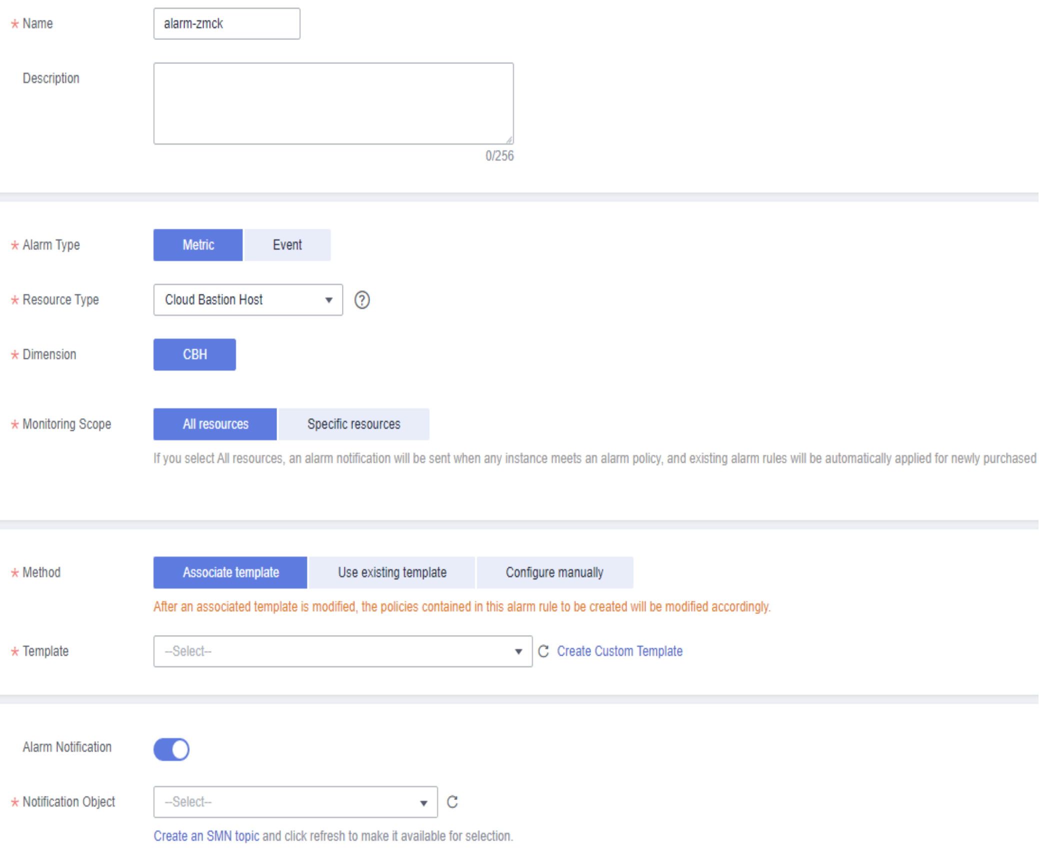


Table 13-2 Parameters for setting CBH alarm rules

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
Resource Type	Select a resource type. Select **Cloud Bastion Host**.	Cloud 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

Parameter	Description	Example Value
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
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

Parameter	Description	Example Value
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 7 Click **Create**. In the displayed dialog box, click **OK**.

----End

13.3 Viewing Metrics

You can view CBH metrics on the management console to learn about the CBH 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 management console**.

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

Step 3 Hover your mouse over in the upper left corner of the page and choose **Management & Governance** > **Cloud Eye**.

Step 4 In the navigation pane on the left, choose **Cloud Service Monitoring** > **Cloud Bastion Host**.

Step 5 In the row containing the target CBH instance, click **View Metric** in the **Operation** column.

----End

A Change History

Released On	Description
2024-03-25	This issue is the second official release. New screenshots are used as a new console style is used.
2022-12-01	This issue is the first official release.