Cloud Bastion Host

Best Practices

Issue	04
Date	2025-07-18

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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

Notice

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

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

Contents

1 Change CBH Instance Specifications

1.1 Before You Start

Application Scenarios

You can change specifications of a CBH instance to meet your business needs.

This document applies to specification changes of a single-node CBH instance on Huawei Cloud.

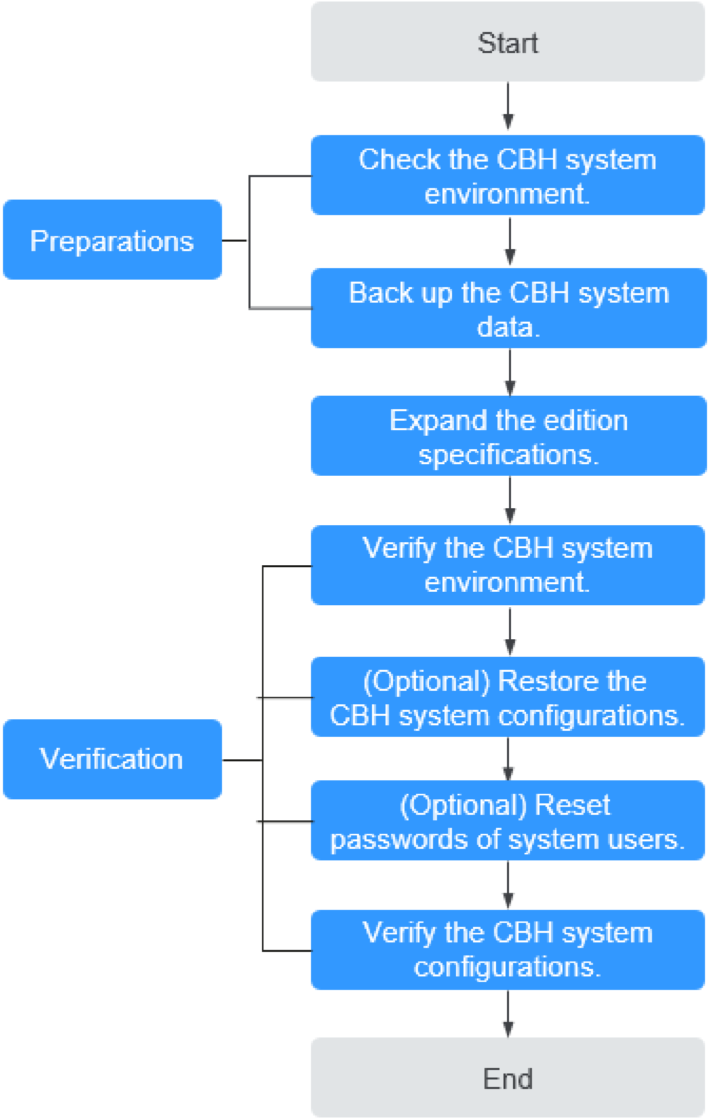
NOTE

To change specifications of a CBH instance in two-node cluster mode, click **Service Tickets** in the Huawei Cloud management console and submit a service ticket for technical support.

Change Process

This document provides guidance for the system administrator **admin** to change specifications of a CBH instance. The general steps are as follows: Back up the CBH system data before the change; change the instance specifications; restore the CBH system configurations; and verify that the configurations for the original and new CBH systems are consistent.

Figure 1-1 Specification change process


Start
Check the CBH system environment.
Preparations
Back up the CBH system data.
Expand the edition specifications.
Verify the CBH system environment.
(Optional) Restore the CBH system configurations.
Verification
(Optional) Reset passwords of system users.
Verify the CBH system configurations.
End

Restrictions on Changing Specifications

Changing specification includes changing the edition and asset specifications of a CBH instance.

- Edition: The edition of a CBH instance can only be changed from the standard to the professional, but cannot be changed from the professional to the standard.
- Asset specifications: include assets, concurrent requests, CPU, memory, and data disks. Asset specifications can only be scaled up.

NOTE

- Changing specifications has no impact on the bandwidth and traffic of the EIP bound to the instance.
- The default capacity of the system disk is 100 GB. Changing specifications does not affect the system disk but expands data disk capacity.
- CBH historical edition provides only functions of the standard edition. To change its specifications, click **Service Tickets** in the upper right corner of the Huawei Cloud management console and submit a service ticket for technical support.
- Change rules:

  Standard edition: A standard edition can be changed to another standard edition as long as the new one has a larger asset quota than the original. A standard edition can also be changed to a professional edition as long as the professional edition has an asset quota no less than the original edition does.

  Professional edition: A professional edition can be changed to another professional edition as long as the new one has a larger asset quota than the original.

Table 1-1 Edition change

Before the Change	After the Change
50 Assets | Standard	100 Assets | Standard or Professional 200 Assets | Standard or Professional 500 Assets | Standard or Professional 1000 Assets | Standard or Professional 2000 Assets | Standard or Professional 5000 Assets | Standard or Professional 10,000 Assets | Standard or Professional
50 Assets | Professional	100 Assets | Professional 200 Assets | Professional 500 Assets | Professional 1000 Assets | Professional 2000 Assets | Professional 5000 Assets | Professional 10,000 Assets | Professional
100 Assets | Standard	100 Assets | Professional 200 Assets | Standard or Professional 500 Assets | Standard or Professional 1000 Assets | Standard or Professional 2000 Assets | Standard or Professional 5000 Assets | Standard or Professional 10,000 Assets | Standard or Professional

Before the Change	After the Change
100 Assets | Professional	200 Assets | Professional 500 Assets | Professional 1000 Assets | Professional 2000 Assets | Professional 5000 Assets | Professional 10,000 Assets | Professional
200 Assets | Standard	200 Assets | Professional 500 Assets | Standard or Professional 1000 Assets | Standard or Professional 2000 Assets | Standard or Professional 5000 Assets | Standard or Professional 10,000 Assets | Standard or Professional
200 Assets | Professional	500 Assets | Professional 1000 Assets | Professional 2000 Assets | Professional 5000 Assets | Professional 10,000 Assets | Professional
500 Assets | Standard	500 Assets | Professional 1000 Assets | Standard or Professional 2000 Assets | Standard or Professional 5000 Assets | Standard or Professional 10,000 Assets | Standard or Professional
500 Assets | Professional	1000 Assets | Professional 2000 Assets | Professional 5000 Assets | Professional 10,000 Assets | Professional
1000 Assets | Standard	1000 Assets | Professional 2000 Assets | Standard or Professional 5000 Assets | Standard or Professional 10,000 Assets | Standard or Professional
1000 Assets | Professional	2000 Assets | Professional 5000 Assets | Professional 10,000 Assets | Professional
2000 Assets | Standard	2000 Assets | Professional 5000 Assets | Standard or Professional 10,000 Assets | Standard or Professional

Before the Change	After the Change
2000 Assets | Professional	5000 Assets | Professional 10,000 Assets | Professional
5000 Assets | Standard	5000 Assets | Professional 10,000 Assets | Standard or Professional
5000 Assets | Professional	10,000 Assets | Professional

Precautions for Changing Specifications

- **Software version**

  To make the functions of the profession edition take effect, the CBH system software version must be V3.2.16.0 or later, or the CBH system cannot be upgraded even the specifications are changed.

  If the software version is earlier than V3.2.16.0, **upgrade the system version** first.

- **System data backup and restoration**

  Before you change specifications, back up important system data to prevent system data loss caused by change failures.

  After the specifications are changed, reload the backup data to the system to quickly restore the system configurations.

- **Specification change time**

  The entire specification change process includes preparation, background upgrade, and verification after the change. The process takes about 60 minutes. It takes about 30 minutes to change the backend specifications. During this period, close the CBH system, which will interrupt the CBH system service.

  To reduce the impact on the system running, change specifications during off-peak hours.

1.2 Preparations

1.2.1 Checking the System Environment

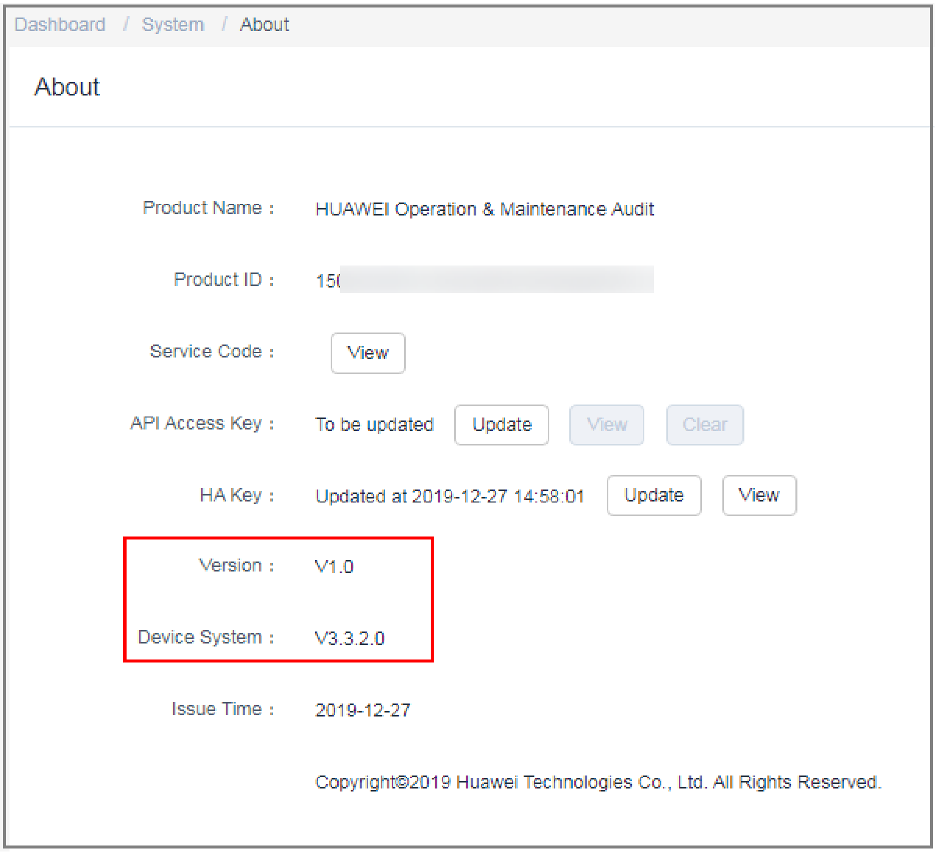
Before the change, query and record the instance version and specifications, including **Version**, **Device System**, **Max Resources**, and **Max Concurrent Conns**.

Step 1 Log in to the CBH system.

Step 2 Confirm and record the instance version.

1. In the navigation pane on the left, choose **System** > **About** to view the instance version.

Figure 1-2 Checking the instance version



About

Product Name : HUAWEI Operation & Maintenance Audit

Product ID : 15[redacted]

Service Code : View

API Access Key : To be updated Update View Clear

HA Key : Updated at 2019-12-27 14:58:01 Update View

Version : V1.0

Device System : V3.3.2.0

Issue Time : 2019-12-27

Copyright©2019 Huawei Technologies Co., Ltd. All Rights Reserved.

2. Record information about **Version** and **Device System**.

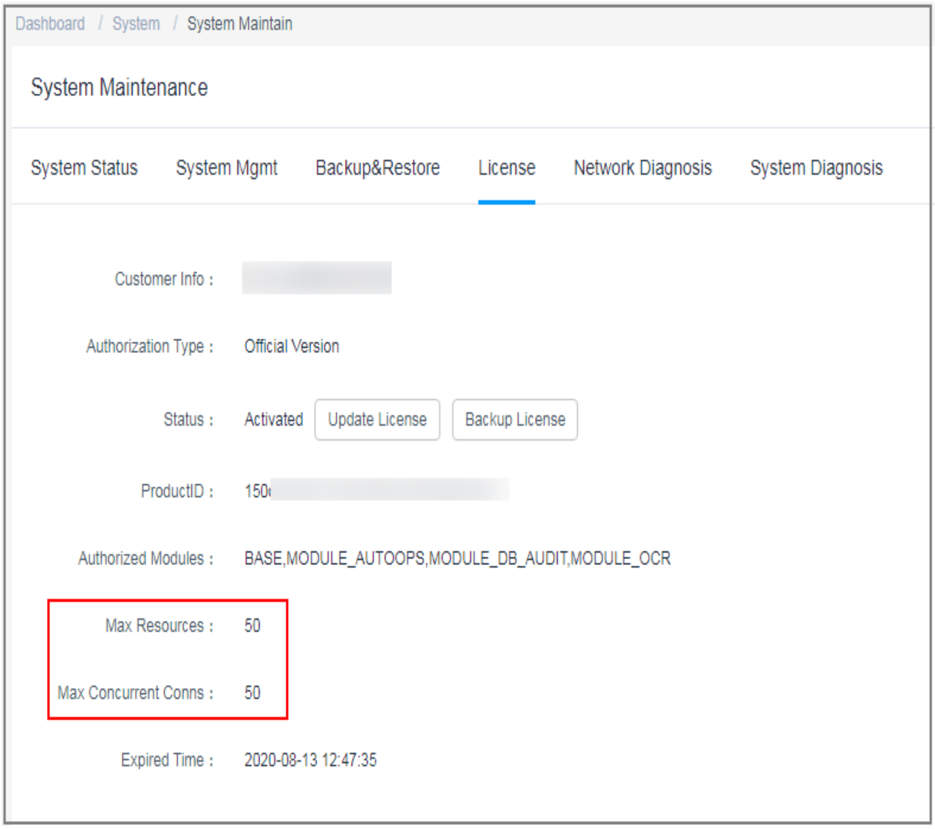
NOTE

The device system version must be V3.2.16.0 or later, or the change does not take effect. **Upgrade the system software** first if needed.

Step 3 Confirm and record the authorization configuration.

1. Choose **System** > **System Maintain** > **License** to view the authorization information.

Figure 1-3 Viewing license



Customer Info : [redacted]

Authorization Type : Official Version

Status : Activated

ProductID : 150[redacted]

Authorized Modules : BASE,MODULE_AUTOOPS,MODULE_DB_AUDIT,MODULE_OCR

Max Resources : 50

Max Concurrent Conns : 50

Expired Time : 2020-08-13 12:47:35

2. Record the number of authorized resources in **Max Resources** and the number of concurrent connections of authorized resources in **Max Concurrent Conns**.

----End

1.2.2 Backing Up the CBH System Data

To prevent system data loss caused by possible change failures, back up important system data, including system configurations, resource accounts, and audit logs, before the change.

Backing Up System Configuration Data

You can back up CBH system configuration data and load it to the new CBH system, eliminating the need to repeat manual configurations.

The system configuration data contains all configuration data of the department, user, resource, policy, ticket, operation, audit, and system modules.

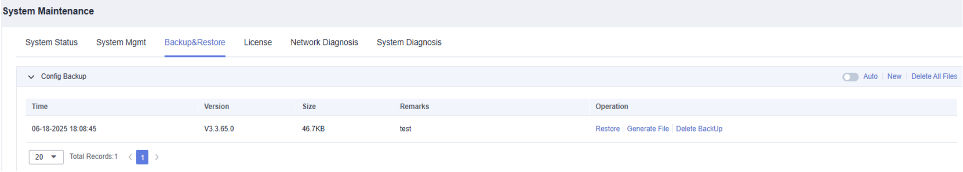
Step 1 Log in to the CBH system.

Step 2 Choose **System** > **System Maintain** > **Backup&Restore**.

Step 3 Click **New**, enter remarks, and click **OK**.

You can go to the task center page to check the task result. If the task is complete, go to the **Backup&Restore** page and check the generated backup file displayed in the backup list according to the task time.

Figure 1-4 Backup task completed



System Maintenance

System Status | System Mgmt | Backup&Restore | License | Network Diagnosis | System Diagnosis

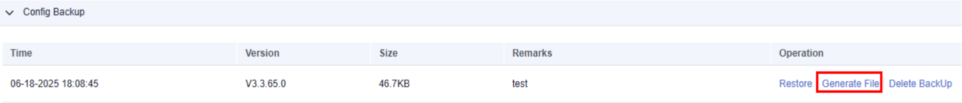
Config Backup — Auto | New | Delete All Files

Time	Version	Size	Remarks	Operation
06-18-2025 18:08:45	V3.3.65.0	46.7KB	test	Restore | Generate File | Delete BackUp

20 Total Records: 1 < 1 >

Step 4 Click **Generate File** in the row corresponding to the task time.

Figure 1-5 Generate File



Config Backup

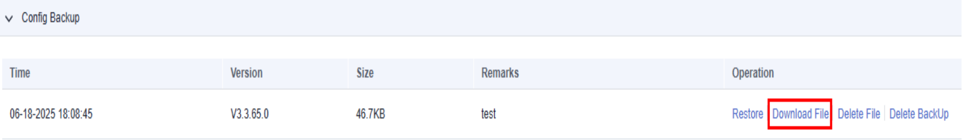
Time	Version	Size	Remarks	Operation
06-18-2025 18:08:45	V3.3.65.0	46.7KB	test	Restore | Generate File | Delete BackUp

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

- Set the encryption password: Specify an encryption password for the backup file. In this way, the backup file cannot be accessed unless the password is provided.
- User password: Enter the password for logging in to the bastion host.

Step 6 Go to the **Backup&Restore** page and click **Download File**.

Figure 1-6 Download File



Config Backup

Time	Version	Size	Remarks	Operation
06-18-2025 18:08:45	V3.3.65.0	46.7KB	test	Restore | Download File | Delete File | Delete BackUp

Step 7 Select a local path and save the backup configuration file.

----End

Backing Up Managed Accounts

The authentication keys of different CBH systems are different. After the specification change, the managed accounts imported using the configuration file may fail to be used for system login. You are advised to back up managed accounts to prevent account information loss in case of specification change failure.

A managed account file contains all data of each account, including the username, password, login methods, sudo account, and names and addresses of associated resources.

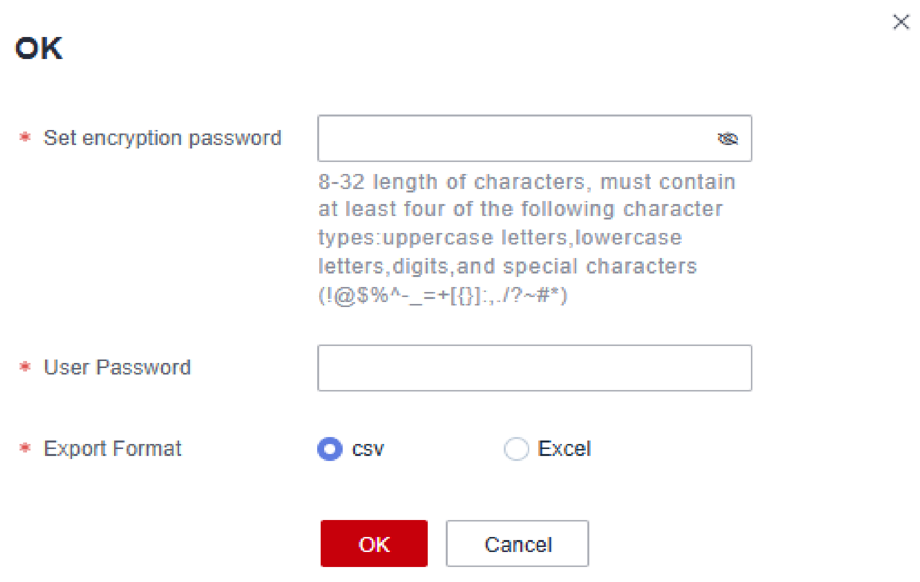
Step 1 Log in to the CBH system.

Step 2 Choose **Resource** > **Account** and click ↗ in the upper right corner of the resource account list.

Step 3 Configure the password and export format, and click **OK**.

You can go to the task center to check whether the task is complete.

Figure 1-7 Configuring a password



OK

×

* Set encryption password

8-32 length of characters, must contain at least four of the following character types:uppercase letters,lowercase letters,digits,and special characters (!@$%^-_=+[{}]:,./?~#*)

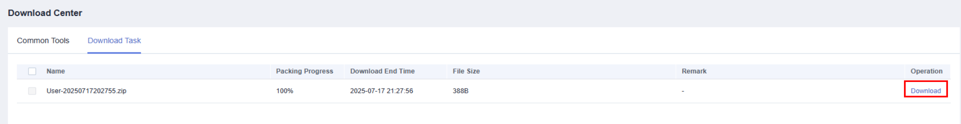
* User Password

* Export Format ● csv ○ Excel

Step 4 If the resource account export task is complete, click ⤓ in the upper right corner to go to the download center.

Step 5 On the **Download Task** page, click **Download** in the row where the target task is located.

Figure 1-8 Downloading the exported account file



Download Center

Common Tools | Download Task

□	Name	Packing Progress	Download End Time	File Size	Remark	Operation
□	User-20250717202755.zip	100%	2025-07-17 21:27:56	388B	-	Download

Step 6 Select a local path and save the exported resource account information file.

----End

Backing Up Audit Logs

CBH does not support migration of history audit logs. You need to back up system audit logs before the change.

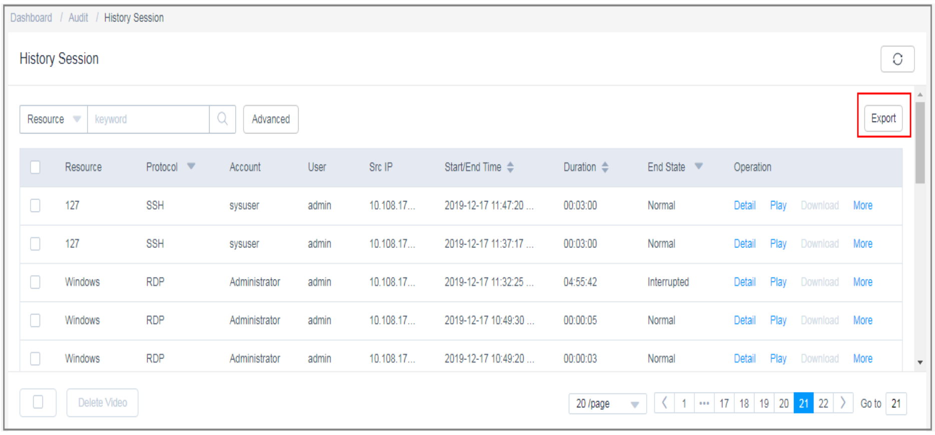
Audit logs include history session records, session videos, system login logs, system operation logs, password change logs, and account synchronization logs.

Step 1 Log in to the CBH system.

Step 2 Export history session records.

1. Choose **Audit** > **History Session**.
2. Select all history sessions, click **Export**, and save exported text records locally.

Figure 1-9 Exporting history session records



Resource	Protocol	Account	User	Src IP	Start/End Time	Duration	End State	Operation
127	SSH	sysuser	admin	10.108.17...	2019-12-17 11:47:20 ...	00:03:00	Normal	Detail Play Download More
127	SSH	sysuser	admin	10.108.17...	2019-12-17 11:37:17 ...	00:03:00	Normal	Detail Play Download More
Windows	RDP	Administrator	admin	10.108.17...	2019-12-17 11:32:25 ...	04:55:42	Interrupted	Detail Play Download More
Windows	RDP	Administrator	admin	10.108.17...	2019-12-17 10:49:30 ...	00:00:05	Normal	Detail Play Download More
Windows	RDP	Administrator	admin	10.108.17...	2019-12-17 10:49:20 ...	00:00:03	Normal	Detail Play Download More

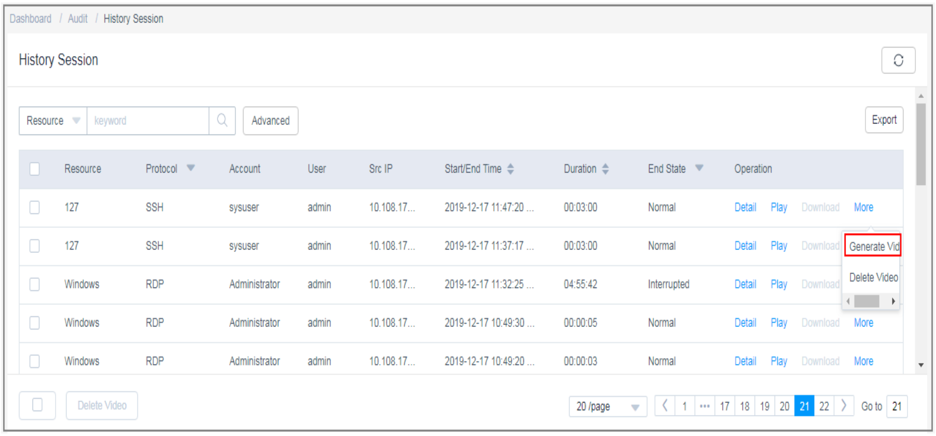
Step 3 Download a session video.

NOTE

Session videos cannot be generated or downloaded in batches. Only one video can be generated or downloaded at a time.

1. Choose **Audit** > **History Session**.
2. Choose **More** > **Generate Video** in the **Operation** column of the target session row.

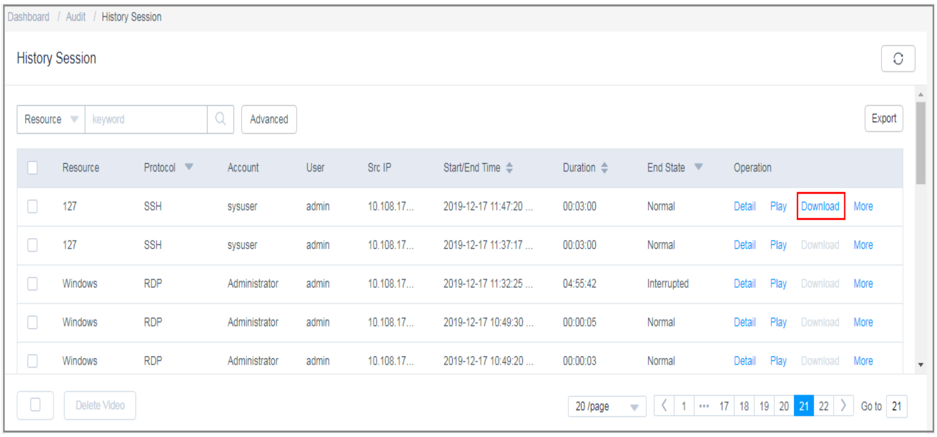
Figure 1-10 Generating a video



Resource	Protocol	Account	User	Src IP	Start/End Time	Duration	End State	Operation
127	SSH	sysuser	admin	10.108.17...	2019-12-17 11:47:20 ...	00:03:00	Normal	Detail Play Download More
127	SSH	sysuser	admin	10.108.17...	2019-12-17 11:37:17 ...	00:03:00	Normal	Detail Play Download
Windows	RDP	Administrator	admin	10.108.17...	2019-12-17 11:32:25 ...	04:55:42	Interrupted	Detail Play Download
Windows	RDP	Administrator	admin	10.108.17...	2019-12-17 10:49:30 ...	00:00:05	Normal	Detail Play Download More
Windows	RDP	Administrator	admin	10.108.17...	2019-12-17 10:49:20 ...	00:00:03	Normal	Detail Play Download More

3. After the video is generated, click **Download** and save the video locally.

Figure 1-11 Downloading a video

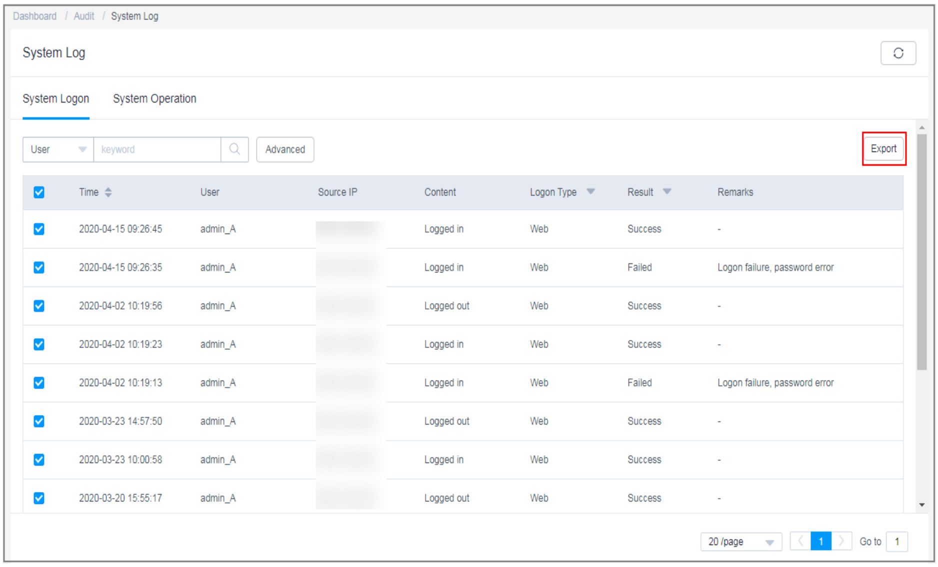


□	Resource	Protocol	Account	User	Src IP	Start/End Time	Duration	End State	Operation
□	127	SSH	sysuser	admin	10.108.17...	2019-12-17 11:47:20 ...	00:03:00	Normal	Detail Play Download More
□	127	SSH	sysuser	admin	10.108.17...	2019-12-17 11:37:17 ...	00:03:00	Normal	Detail Play Download More
□	Windows	RDP	Administrator	admin	10.108.17...	2019-12-17 11:32:25 ...	04:55:42	Interrupted	Detail Play Download More
□	Windows	RDP	Administrator	admin	10.108.17...	2019-12-17 10:49:30 ...	00:00:05	Normal	Detail Play Download More
□	Windows	RDP	Administrator	admin	10.108.17...	2019-12-17 10:49:20 ...	00:00:03	Normal	Detail Play Download More

Step 4 Export system login logs.

1. Choose **Audit** > **System Log** > **System Logon** to switch to the system log page.
2. Select all login logs, click **Export**, and save the exported text records locally.

Figure 1-12 Exporting system login logs

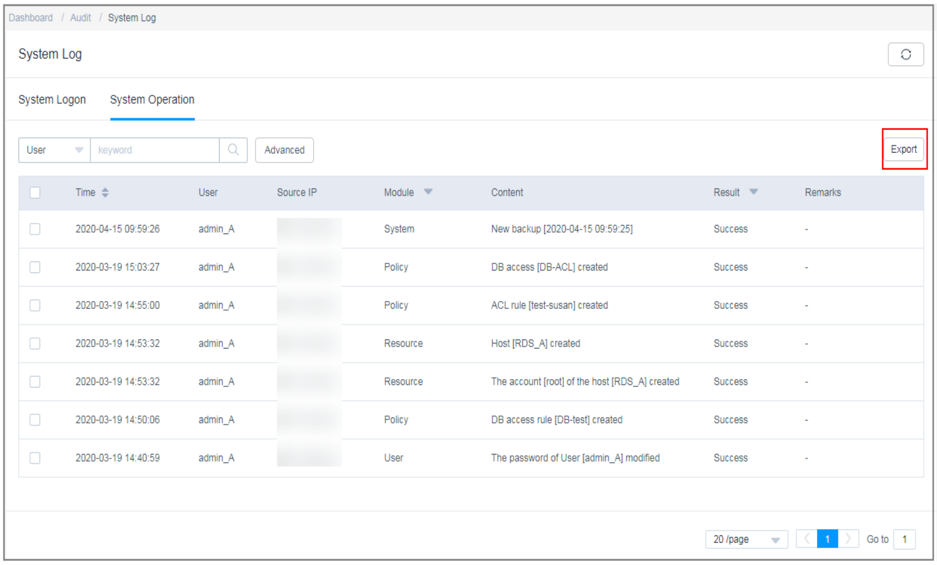


☑	Time	User	Source IP	Content	Logon Type	Result	Remarks
☑	2020-04-15 09:26:45	admin_A	[redacted]	Logged in	Web	Success	-
☑	2020-04-15 09:26:35	admin_A	[redacted]	Logged in	Web	Failed	Logon failure, password error
☑	2020-04-02 10:19:56	admin_A	[redacted]	Logged out	Web	Success	-
☑	2020-04-02 10:19:23	admin_A	[redacted]	Logged in	Web	Success	-
☑	2020-04-02 10:19:13	admin_A	[redacted]	Logged in	Web	Failed	Logon failure, password error
☑	2020-03-23 14:57:50	admin_A	[redacted]	Logged out	Web	Success	-
☑	2020-03-23 10:00:58	admin_A	[redacted]	Logged in	Web	Success	-
☑	2020-03-20 15:55:17	admin_A	[redacted]	Logged out	Web	Success	-

Step 5 Export system operation logs.

1. Choose **Audit** > **System Log** > **System Operation** to switch to the system log page.
2. Select all operation logs, click **Export**, and save the exported text records locally.

Figure 1-13 Exporting system operation logs



Dashboard / Audit / System Log

System Log

System Logon | System Operation

User | keyword | Advanced | Export

	Time	User	Source IP	Module	Content	Result	Remarks
□	2020-04-15 09:59:26	admin_A	[redacted]	System	New backup [2020-04-15 09:59:25]	Success	-
□	2020-03-19 15:03:27	admin_A	[redacted]	Policy	DB access [DB-ACL] created	Success	-
□	2020-03-19 14:55:00	admin_A	[redacted]	Policy	ACL rule [test-susan] created	Success	-
□	2020-03-19 14:53:32	admin_A	[redacted]	Resource	Host [RDS_A] created	Success	-
□	2020-03-19 14:53:32	admin_A	[redacted]	Resource	The account [root] of the host [RDS_A] created	Success	-
□	2020-03-19 14:50:06	admin_A	[redacted]	Policy	DB access rule [DB-test] created	Success	-
□	2020-03-19 14:40:59	admin_A	[redacted]	User	The password of User [admin_A] modified	Success	-

20 /page | 1 | Go to 1

----End

1.3 Changing Specifications of a CBH Instance

Prerequisites

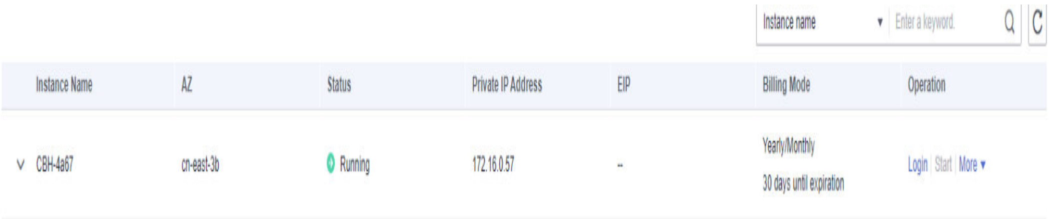
- You have obtained credentials for logging in to the management console.
- An EIP has been bound to the CBH instance.
- You have backed up system data by referring to **Backing Up the CBH System Data**.
- You have disabled the CBH system and terminated all other operations in the CBH system.

Procedure

Step 1 Log in to the management console.

Step 2 In the **Operation** column of the target instance, choose **More** > **Change Edition**.

Figure 1-14 Instances



Instance name | Enter a keyword.

Instance Name	AZ	Status	Private IP Address	EIP	Billing Mode	Operation
CBH-4a67	cn-east-3b	Running	172.16.0.57	--	Yearly/Monthly 30 days until expiration	Login | Start | More

Step 3 Select an edition you want.

Select an **Edition** and click **Next** to go to the **Details** page.

Step 4 Confirm and pay the order.

After confirming the order details, click **Submit**. On the payment page, finish the payment.

Step 5 The specifications are automatically changed in the background.

It takes about 30 minutes for the change to take effect.

During the change, the instance status changes from **Upgrading** to **Restarting**. After the CBH system is restarted, the instance status changes to **Running**.

Step 6 The specifications are changed in the background.

If the instance status changes to **Running** and the instance details are updated, the backend change is completed.

You can then log in to the CBH system and start to verify the change.

----End

1.4 Verification After the Change

1.4.1 Checking the System Environment

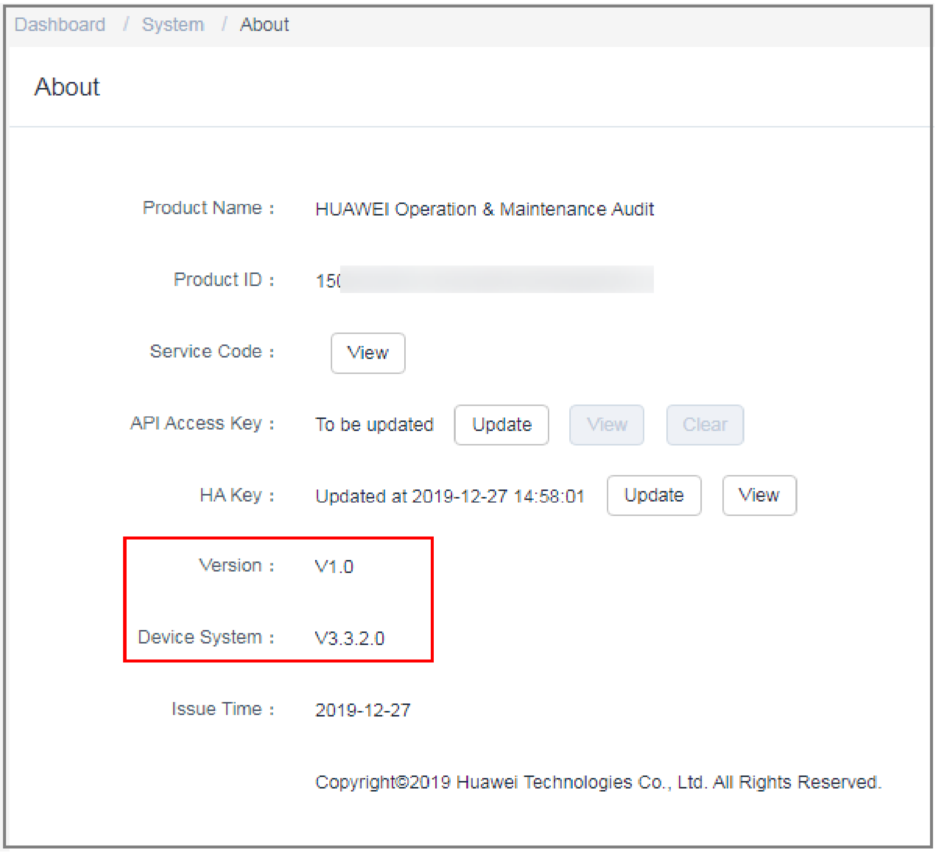
After the change, verify that the settings of **Version**, **Device System**, **Max Resources**, and **Max Concurrent Conns** are the same as that of the new CBH edition.

Step 1 Log in to the CBH system.

Step 2 Check the new instance version.

1. In the navigation pane on the left, choose **System** > **About** to check the instance version.
2. Check the information of **Version** and **Device System**.

Figure 1-15 Checking the instance version



About

Product Name : HUAWEI Operation & Maintenance Audit

Product ID : 15[redacted]

Service Code :

API Access Key : To be updated

HA Key : Updated at 2019-12-27 14:58:01

Version : V1.0

Device System : V3.3.2.0

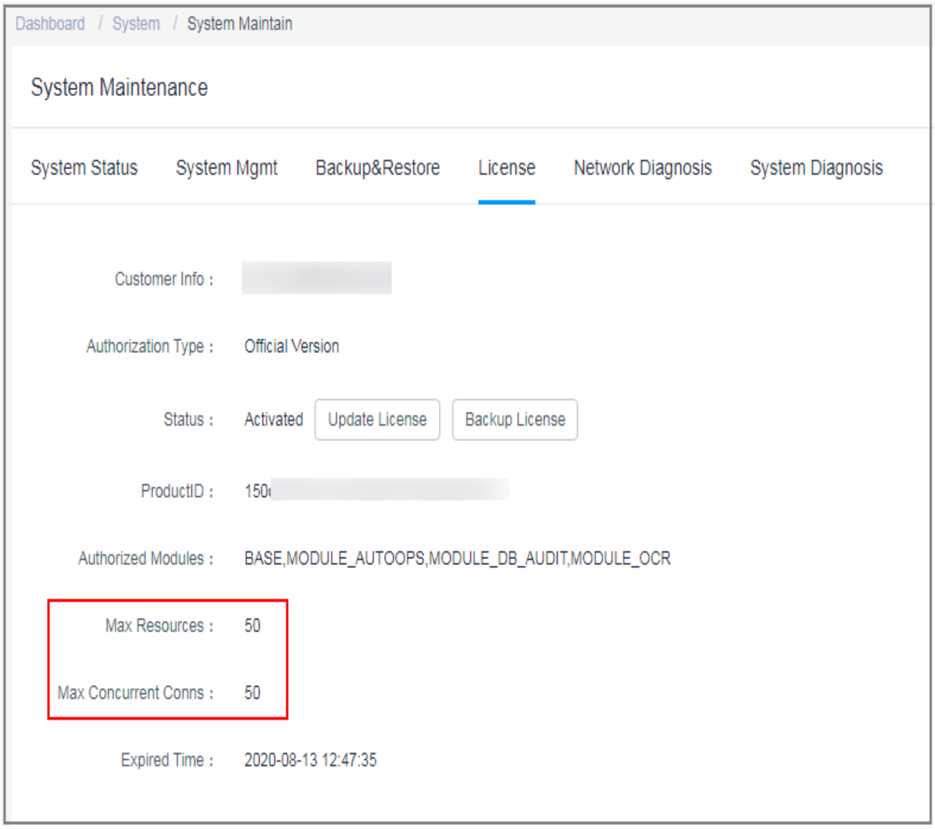
Issue Time : 2019-12-27

Copyright©2019 Huawei Technologies Co., Ltd. All Rights Reserved.

Step 3 Check whether the original and new CBH systems have the consistent authorization information.

1. Choose **System** > **System Maintain** > **License** to view the authorization information.

Figure 1-16 Viewing license



Customer Info : [redacted]

Authorization Type : Official Version

Status : Activated

ProductID : 150[redacted]

Authorized Modules : BASE,MODULE_AUTOOPS,MODULE_DB_AUDIT,MODULE_OCR

Max Resources : 50

Max Concurrent Conns : 50

Expired Time : 2020-08-13 12:47:35

2. Check whether the authorization information is consistent with that of the new CBH edition.
   - If they are consistent, the specification change is successful.
   - If no, contact technical support.

----End

1.4.2 (Optional) Restoring CBH System Configurations

After the change is completed, the number of system assets, number of concurrent requests, CPU, and data disks are upgraded accordingly, which does not affect system data.

If system data is lost due to a change failure, you can import the backup files, such as system configuration files and resource account files, and restore the system configurations.

Importing the Backup File of the CBH System Configurations

You can reuse the system configuration data of the original CBH system in the new CBH system by uploading the system configuration back file to the new system.

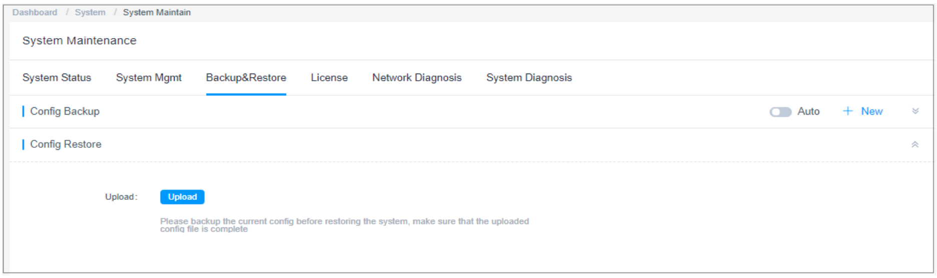
The system configuration data contains all configuration data of the department, user, resource, policy, ticket, operation, audit, and system modules.

Step 1 Log in to the CBH system.

Step 2 Choose **System** > **System Maintain** > **Backup&Restore**.

Step 3 In the **Config Restore** area, click **Upload**, select the configuration file exported from the original CBH system, and upload it.

Figure 1-17 Uploading the backup configuration file



Please backup the current config before restoring the system, make sure that the uploaded config file is complete

Step 4 Click **OK**.

It takes about 5 minutes for the imported configuration data to take effect. It may take a longer time if there is a large amount of system configuration data.

----End

Importing the Backup File of Managed Accounts

The authentication keys of different CBH systems are different. After the change, the managed accounts imported using the configuration file may fail to be used for system login. To ensure the availability of the managed accounts, you are advised to import the backup file of the managed accounts.

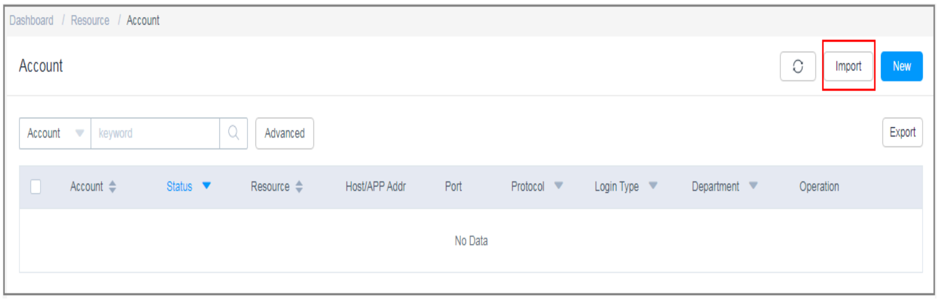
A managed account backup file contains all data of each account, including the username, password, login methods, sudo account, and names and addresses of associated resources.

Step 1 Log in to the CBH system.

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

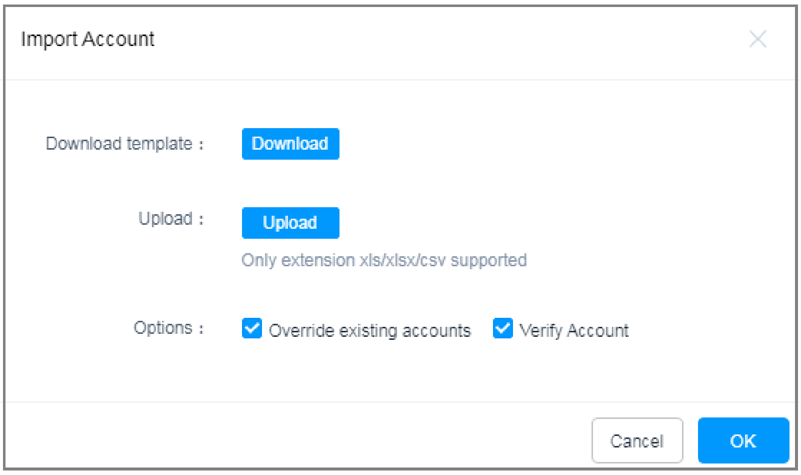
Step 3 Click **Import** to go to the **Import Account** page.

Figure 1-18 Account



Step 4 On the **Import Account** page, click **Upload**, select the account file exported from the original CBH system, and upload it.

Figure 1-19 Import Account



Import Account

Download template :

Upload :

Only extension xls/xlsx/csv supported

Options : ☑ Override existing accounts ☑ Verify Account

Step 5 After the upload is complete, choose **More** > **Override existing accounts** or **Verify Account**.

Step 6 Click **OK**.

----End

1.4.3 (Optional) Resetting the Passwords of System Users

After the specifications of a CBH instance are changed, you are advised to reset the system user passwords to enhance the password security and availability.

You can let the system generate a new password for users in batches or manually reset different passwords for system users.

Step 1 Log in to the CBH system.

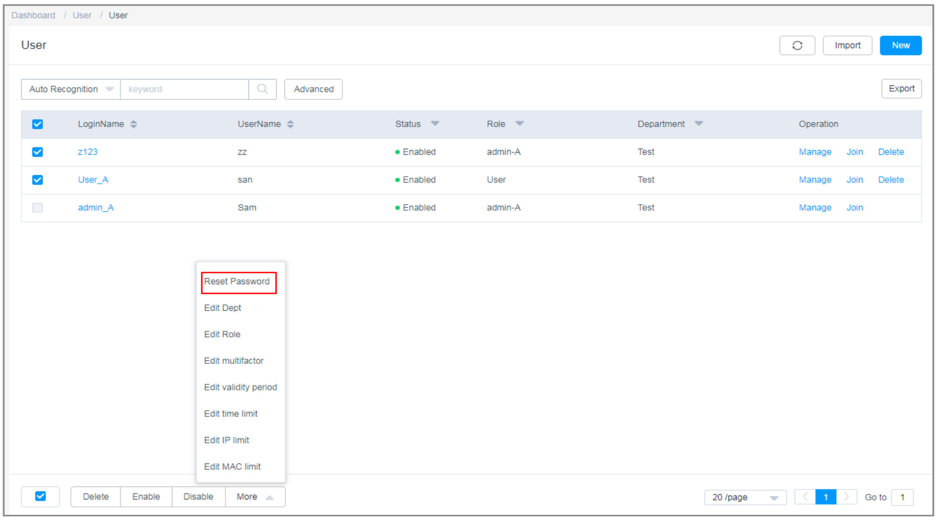
Step 2 Choose **User** > **User** in the navigation pane.

- To reset passwords for a batch of users, go to **Step 3**.
- To manually reset a password, go to **Step 4**.

Step 3 Reset the same login password of multiple system users.

1. Select the users whose passwords need to be reset.

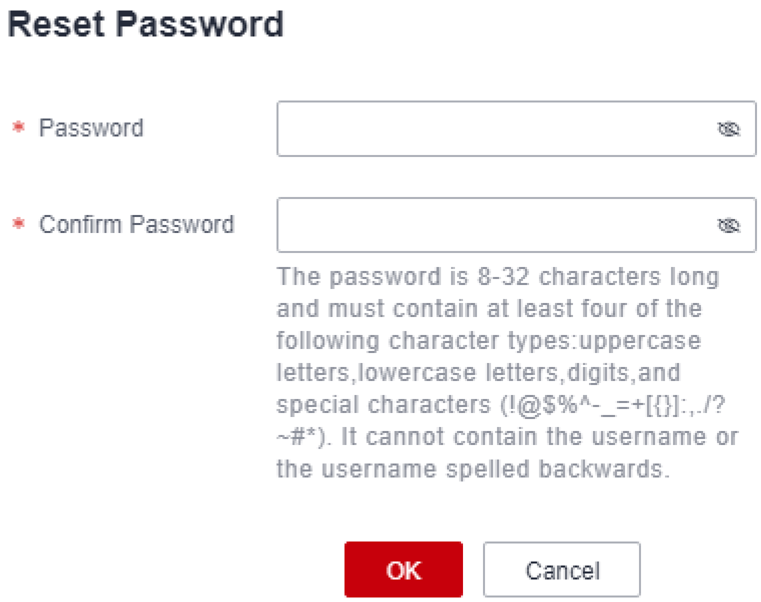
Figure 1-20 Resetting a user's password



☑	LoginName	UserName	Status	Role	Department	Operation
☑	z123	zz	● Enabled	admin-A	Test	Manage Join Delete
☑	User_A	san	● Enabled	User	Test	Manage Join Delete
□	admin_A	Sam	● Enabled	admin-A	Test	Manage Join

2. Choose **More** > **Reset Password** to go to the password resetting dialog box.

Figure 1-21 Reset Password



Reset Password

* Password

* Confirm Password

The password is 8-32 characters long and must contain at least four of the following character types:uppercase letters,lowercase letters,digits,and special characters (!@$%^-_=+[{}]:,./?~#*). It cannot contain the username or the username spelled backwards.

3. Reset the password and click **OK**.

NOTE

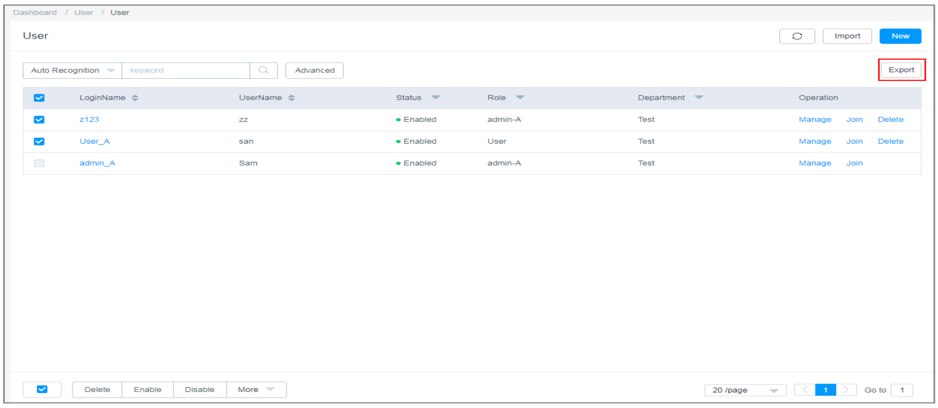
If you batch reset the passwords for system users, these users need to use the reset password to log in to the CBH system. For security purposes, CBH asks each system user to change the password upon the first login.

Step 4 Manually reset different passwords for system users.

1. Export the user list template.

   Select the users you want to export and click **Export** in the upper right corner. If no users are selected, information about all users is exported by default.

Figure 1-22 Exporting information about all users

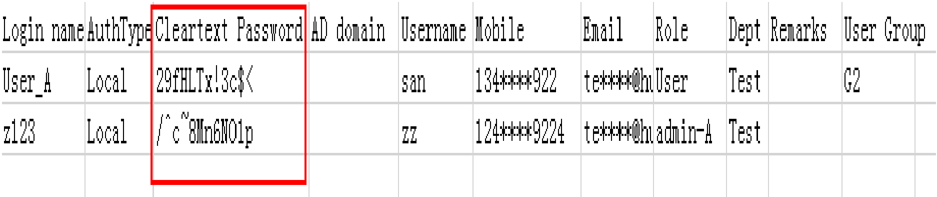


☑	LoginName	UserName	Status	Role	Department	Operation
☑	z123	zz	● Enabled	admin-A	Test	Manage Join Delete
☑	User_A	san	● Enabled	User	Test	Manage Join Delete
□	admin_A	Sam	● Enabled	admin-A	Test	Manage Join

2. Configure user passwords.

   Save the exported user information file locally, change the plaintext password in the **Cleartext Password** row corresponding to the user **Login Name** as needed, and save the file.

Figure 1-23 Changing a password

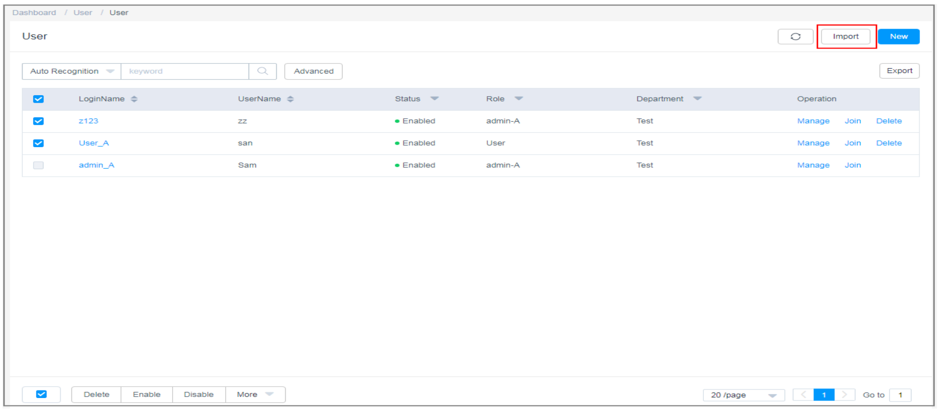


Login name	AuthType	Cleartext Password	AD domain	Username	Mobile	Email	Role	Dept	Remarks	User Group
User_A	Local	29fHLTx!3c$<		san	134****922	te****@h	User	Test		G2
z123	Local	/^c~8Mn6NO1p		zz	124****9224	te****@h	admin-A	Test		

3. Import the user list.

   a. On the **User** page, click **Import**.

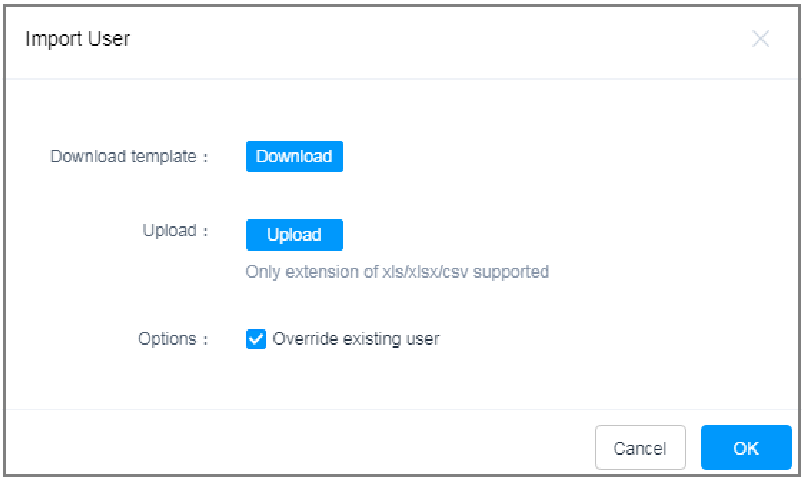
Figure 1-24 Importing the user information file



☑	LoginName	UserName	Status	Role	Department	Operation
☑	z123	zz	● Enabled	admin-A	Test	Manage Join Delete
☑	User_A	san	● Enabled	User	Test	Manage Join Delete
□	admin_A	Sam	● Enabled	admin-A	Test	Manage Join

   b. Click **Upload** and select the modified user information file.

Figure 1-25 Import User



Import User

Download template : Download

Upload : Upload

Only extension of xls/xlsx/csv supported

Options : ☑ Override existing user

Cancel OK

c. Select **Override existing user** for **Options**.

d. Click **OK**.

----End

1.4.4 Verifying the CBH System configurations

After the instance specifications are changed, log in the CBH system as system administrator **admin** to verify system configuration consistence for each module in the navigation pane of the CBH system.

You need to verify system configurations in the department, user, resource, policy, ticket, audit, operation, and system modules. For more details, see **Table 1-2**

Table 1-2 System configuration verification

Level 1 Module	Level 2/3 Module	Verification Item
Department	None	Department level, department name, number of users, and number of hosts.
User	User	Number of users and basic information about each user, such as the login name, user name, status, role, and department.
	User Group	Number of user groups, user group names, and group members.
	Role	Role configuration.
Resource	Host	Number of managed hosts and basic information about each managed host, including the host name, host address, port number, protocol type, OS type, and number of accounts.

Level 1 Module	Level 2/3 Module	Verification Item
	Application Publish	- Number of applications, names, addresses, associated hosts, and department of each application. - Number of application servers, names, addresses, types, and department of each application server.
	Account	- Number of accounts and basic information about each account, including the account name, related resources, host or application address, port number, and department. - Whether accounts can be used. You can select accounts in batches and click **Verify** to check whether the selected accounts can be used to log in to the system.
	Account Group	Number of account groups, account group names, members in an account group, and number of members in an account group.
Operation	Host label	Number of labels of managed hosts, such as the number of labels, names, and labeled hosts.
	Application Label	Verify the configuration information about the number of tags, names, and tagged application resources released by the application.
Policy	ACL Rules	Number of ACL rules and basic information about each ACL rule, such as rule name, status, associated users, and associated accounts.
	Cmd Rules	- Number of policies, policy names, actions, and associated command sets. - Number of command sets, names, commands, and parameters.
	Chpwd Rules	Number of policies and basic information about each policy, such as policy names, status, execution modes, and password change mode.
Audit	System Report	**Auto Send** configuration
	Ops Report	**Auto Send** configuration
Ticket	ACL Ticket	Basic information about the authorization ticket, including ticket number, status, and application time
System	Security	System login security configuration, including user locking, policy password, web login, and SSH client login.

Level 1 Module	Level 2/3 Module	Verification Item
	Outgoing	Email and SMS gateway configuration.
	Authenticate	AD domain, RADIUS, and LDAP authentication configurations.
	Ticket	Basic settings and approval process of tickets.
	Alarm	Alarm channel and alarm severity level.
	Storage Mgmt	Auto deletion.
	Log Backup	Remote backup to the Syslog server and remote backup to the FTP/SFTP server.
	Backup& Restore	Automatic configuration backups.

2 Host and Application Resource Management

2.1 Overview

A bastion host can manage hosts, applications, cloud servers (container resources), and databases. This topic walks you through how to manage hosts, databases, and applications.

A bastion host can manage the following types of hosts, databases, and applications:

- 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.

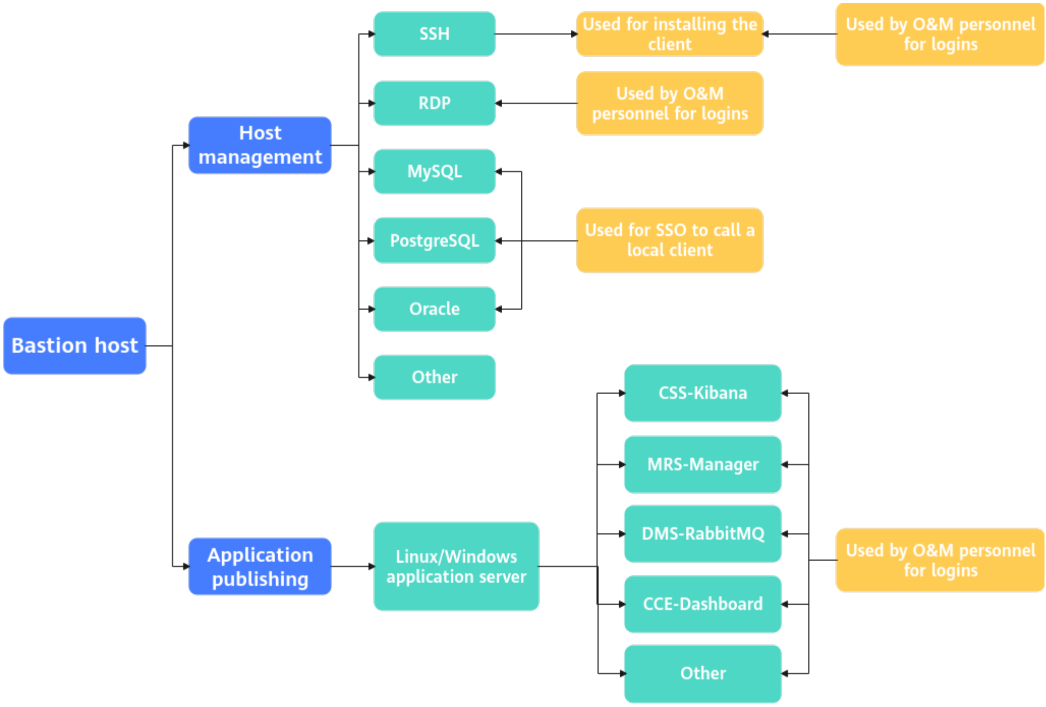
Table 2-1 Types of resources a bastion host can manage

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

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

Figure 2-1 shows the management of common hosts, databases, and application protocols and O&M login methods.

Figure 2-1 Common types of hosts and applications


Bastion host
Host management
SSH
RDP
MySQL
PostgreSQL
Oracle
Other
Used for installing the client
Used by O&M personnel for logins
Used by O&M personnel for logins
Used for SSO to call a local client
Application publishing
Linux/Windows application server
CSS-Kibana
MRS-Manager
DMS-RabbitMQ
CCE-Dashboard
Other
Used by O&M personnel for logins

2.2 Managing Host or Database Resources

This topic describes how to manage hosts or databases through a bastion host.

Figure 2-2 Process of managing hosts or databases

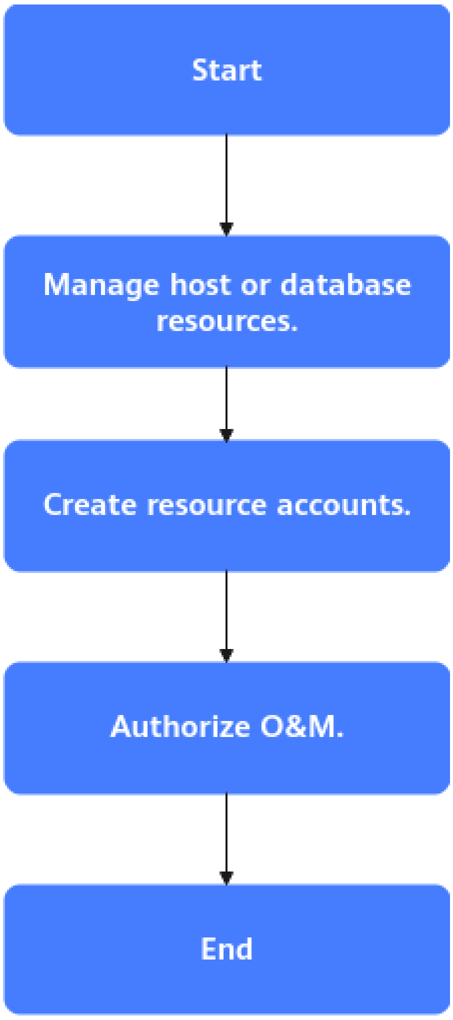


Table 2-2 Process of managing hosts or databases

Step	Description	Reference
Start	Prepare the information about the hosts or databases to be managed by a bastion host.	-

Step	Description	Reference
Manage host or database resources.	Add the information about the prepared hosts or databases to the bastion host for centralized management.	You can select any of the following methods to add the information: - **Adding a Host or Database Resource** - **Importing Host or Database Resources from a File** - **Importing Host or Database Resources from an Account** - **Automatically Discovering Host or Database Resources**
Create resource accounts.	Create login accounts for managed host or database resources. A resource account uniquely identifies a host or database resource managed in a bastion host. You need to create a resource account for each managed host or database resource and associate the resource with the account. O&M personnel can use the account to log in to the host or database resource for O&M operations.	**Creating a Resource Account and Associating It with the Corresponding Resource**
Authorize O&M.	You can configure access control policies and associate the policies with users and resource accounts to control O&M personnel, O&M resources, and O&M operations.	**Creating an ACL Rule and Associating It with Users and Resource Accounts**

Step	Description	Reference
End	Send the user account and bastion host login information to O&M personnel. O&M personnel log in to managed host or database resources in a way based on the host or database protocol type.	- Hosts with SSH, Telnet, and Rlogin protocols configured **Using an SSH Client to Log In to Resources for O&M** - MySQL, SQL Server, Oracle, DB2, PostgreSQL, and GaussDB databases **Using an SSO Client to Log In to Database Resources for O&M** - Hosts with SSH, Telnet, RDP, and VNC protocols configured **Using a Web Browser to Log In to Resources for O&M** - Hosts with FTP and SFTP protocols configured **Using an FTP or SFTP Client to Log In to File Transfer Resources**

2.3 Managing Application Resources

This topic describes how to manage applications through a bastion host.

Figure 2-3 Process of managing applications

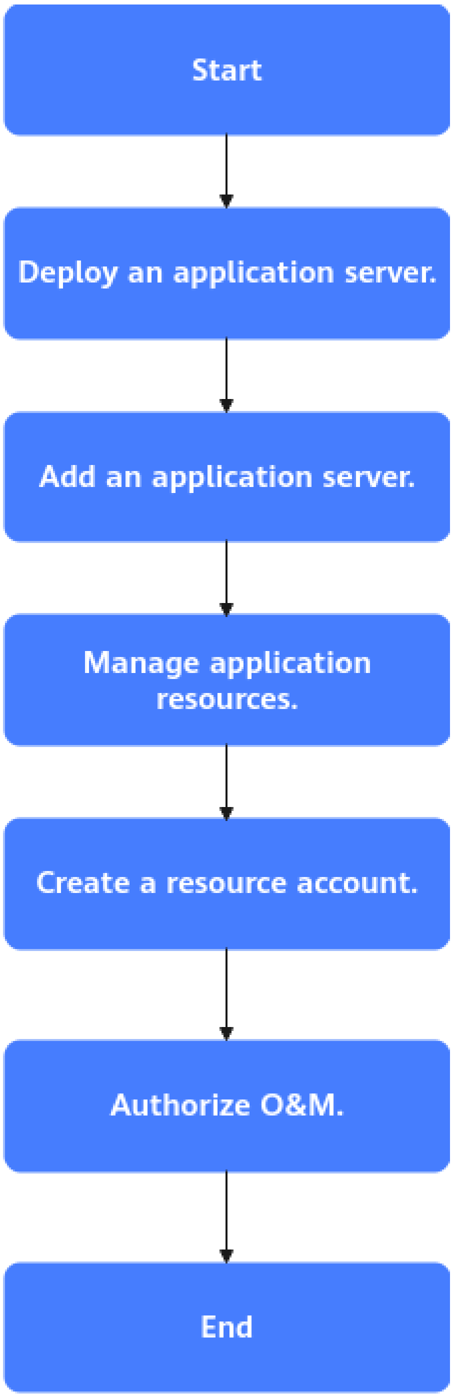

Start
Deploy an application server.
Add an application server.
Manage application resources.
Create a resource account.
Authorize O&M.
End

Table 2-3 Process of managing applications

Step	Description	Reference
Start	- **Prepare a Windows or Linux server as the application server.** You are advised to prepare application servers based on the number of resources to be maintained. For details about the recommended specifications, see **Specifications Selection**. - Prepare information about application resources you want to manage with the bastion host.	-
Deploy an application server.	Deploy related services or applications on the prepared application server. The following lists the services or applications that need to be deployed based on the application server OS. - Windows OSs Deploy Windows Server remote desktop services and RemoteApp. - Linux OSs Deploy the app_publisher component.	**Windows OSs** - **Installing a Windows Server 2019 Application Server** - **Installing a Windows Server 2016 Application Server** - **Installing a Windows Server 2012 R2 Application Server** - **Installing a Windows Server 2008 R2 Application Server** **Linux OSs** **Installing a Linux Application Server**
Add an application server.	Add or import the deployed application server to the bastion host instance to connect the application server to the bastion host instance.	- **Adding an Application Server** - **Importing Application Servers from a File**
Manage application resources.	Add the prepared application resources (client applications or web applications) to the bastion host.	- **Adding an Application Resource** - **Importing Application Resources from a File**

Step	Description	Reference
Create a resource account.	Create a login account for the application. A resource account uniquely identifies an application resource managed in a bastion host. You need to create a resource account for each managed application resource and associate the resource with the account. O&M personnel can use the account to log in to the application resource for O&M operations.	**Creating a Resource Account and Associating It with the Corresponding Resource**
Authorize O&M.	You can configure access control policies and associate the policies with users and resource accounts to control O&M personnel, O&M resources, and O&M operations.	**Creating an ACL Rule and Associating It with Users and Resource Accounts**
End	Send the user account and bastion host login information to O&M personnel. O&M personnel can log in to application resources using a web browser for O&M.	**Using a Web Browser to Log In to Application Resources for O&M**

3 Secondary Authorization for High-Risk Database Operations

With CBH editions, you can delete, modify, and view your database instances by running commands. To secure sensitive database information and prevent key information from being lost or disclosed, CBH gives you the ability to configure an approval process for high-risk database operations and monitor key information.

Use administrator ***admin_A*** as an example to describe how to authorize O&M user ***User_A*** to perform secondary authorization for high-risk operations on MySQL database instance ***RDS_A***.

Application Scenarios

With Cloud Bastion Host (CBH), you can dynamically identify and intercept high-risk commands (including deleting databases, modifying key information, and viewing sensitive information) to interrupt database O&M sessions by setting database control policies and preset command execution policies. In addition, the system automatically generates a database authorization ticket and sends it to the administrator for secondary authorization. O&M users can resume interrupted O&M sessions only after the administrator approves the ticket and authorizes the high-risk operations.

Constraints

Currently, secondary authorization of high-risk operations only applies to the commands executed on the MySQL or Oracle database instances.

Prerequisites

- The security group to which the CBH instance belongs has enabled the database access port, and the network connection between the database and the CBH system is normal.
- Database ***RDS_A*** has been managed as a host resource.
- O&M user ***User_A*** has obtained the access control permission for ***RDS_A***.

Configuring the Secondary Authorization Policy

To approve high-risk operations on database instances, you need to preset command rules on the **DB Rules** page in the **Policy** module and enable **Dynamic approval** in the **Action** field.

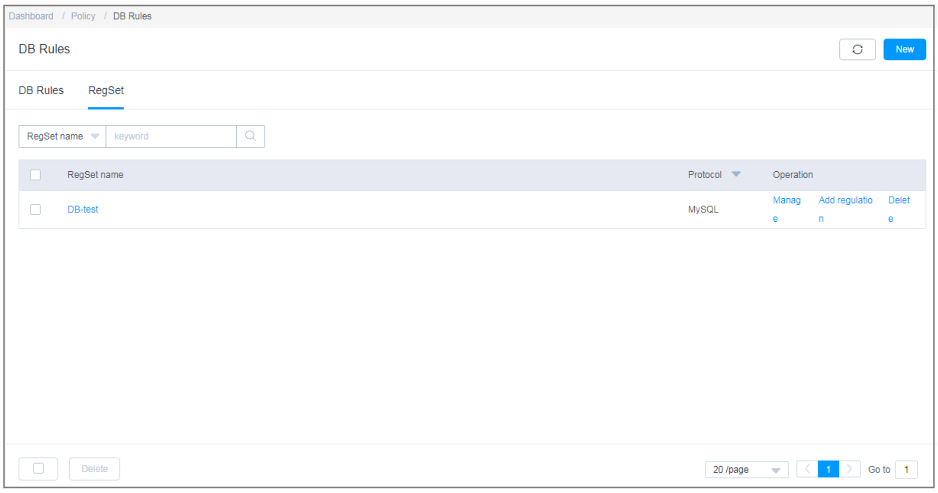
Step 1 Log in to the CBH system as ***admin_A***.

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

Step 3 Configure the database rule set and select the preset high-risk operation commands.

1. Click the **RegSet** tab.

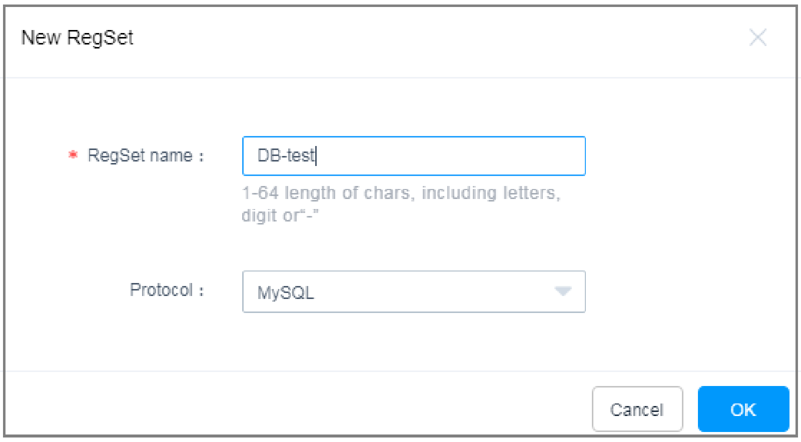
Figure 3-1 RegSet



RegSet name	Protocol	Operation
DB-test	MySQL	Manage Add regulation Delete

2. Click **New** to create a rule set for MySQL databases. Use the ***DB-test*** rule set as an example.

Figure 3-2 New RegSet



* RegSet name : DB-test

1-64 length of chars, including letters, digit or"-"

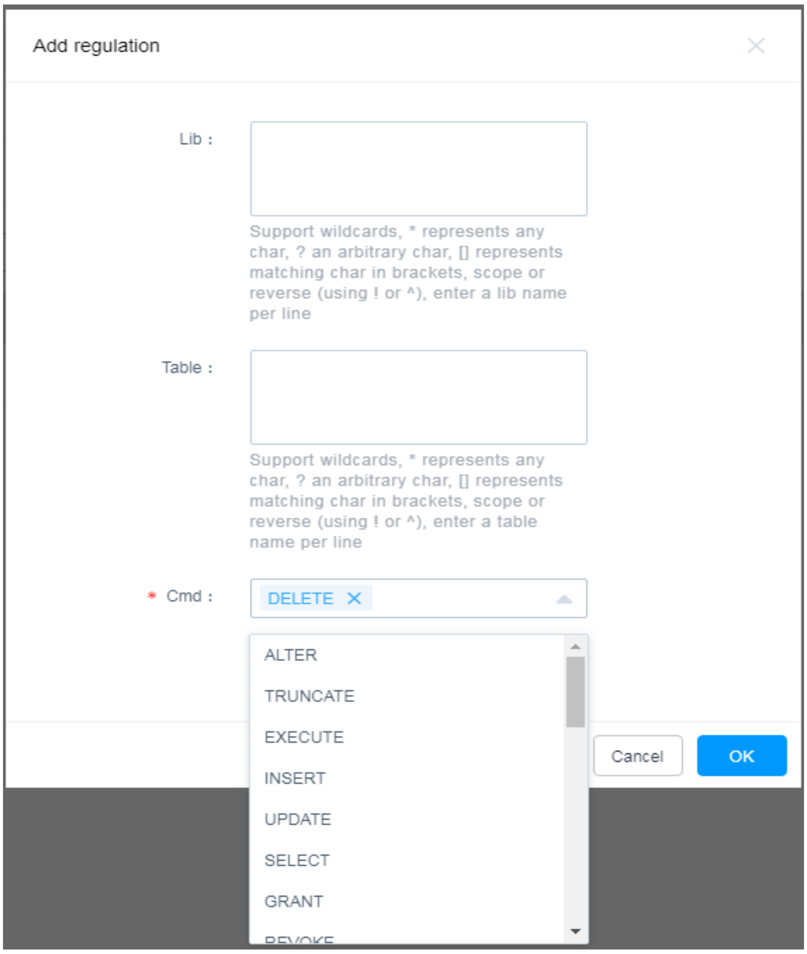
Protocol : MySQL

3. Click **Add Regulation** in the **Operation** column of the ***DB-test*** row to add a library, table, or command rule. The following describes how to add the **DELETE** command for deleting table content.

NOTE

- The **Cmd** field is mandatory. You must select at least one command. You can select multiple commands at a time.
- Set the **Lib** or **Table** field to restrict operation commands on the database library or tables.
- If the **Lib** or **Table** field is left blank, all operation commands in the database are restricted.

Figure 3-3 Add regulation



Add regulation

Lib :

Support wildcards, * represents any char, ? an arbitrary char, [] represents matching char in brackets, scope or reverse (using ! or ^), enter a lib name per line

Table :

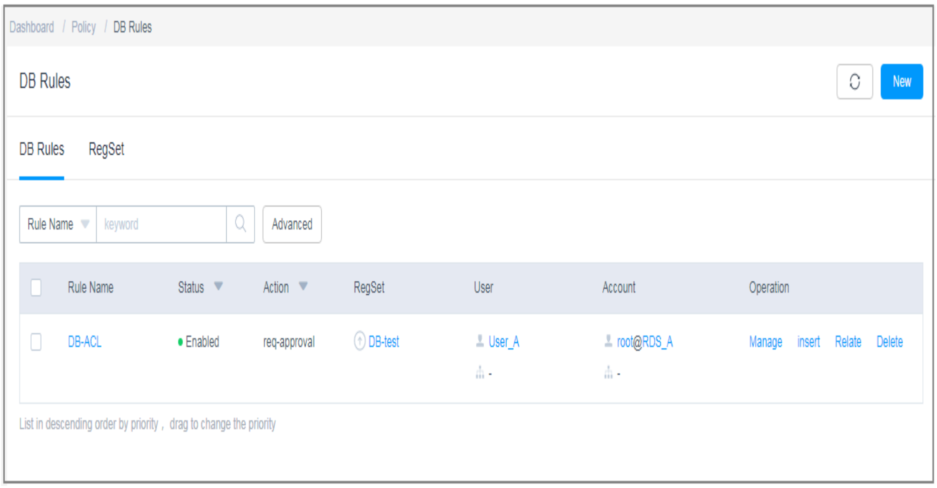
Support wildcards, * represents any char, ? an arbitrary char, [] represents matching char in brackets, scope or reverse (using ! or ^), enter a table name per line

* Cmd : DELETE

Step 4 Configure a DB rule.

1. Click the **DB Rules** tab.

Figure 3-4 DB Rules



Dashboard / Policy / DB Rules

DB Rules

DB Rules RegSet

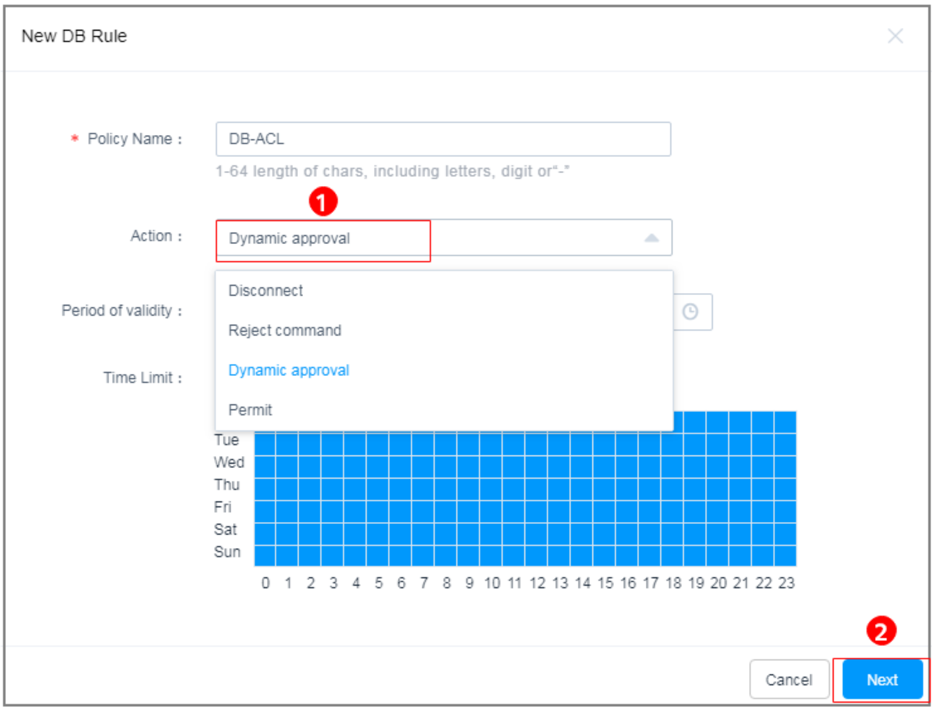
Rule Name keyword

List in descending order by priority , drag to change the priority

	Rule Name	Status	Action	RegSet	User	Account	Operation
□	DB-ACL	● Enabled	req-approval	DB-test	User_A -	root@RDS_A -	Manage insert Relate Delete

2. Click **New** to create a **Dynamic approval** rule for the database. Use database rule ***DB-ACL*** as an example.

Figure 3-5 Configuring dynamic approval



New DB Rule

* Policy Name : DB-ACL

1-64 length of chars, including letters, digit or"-"

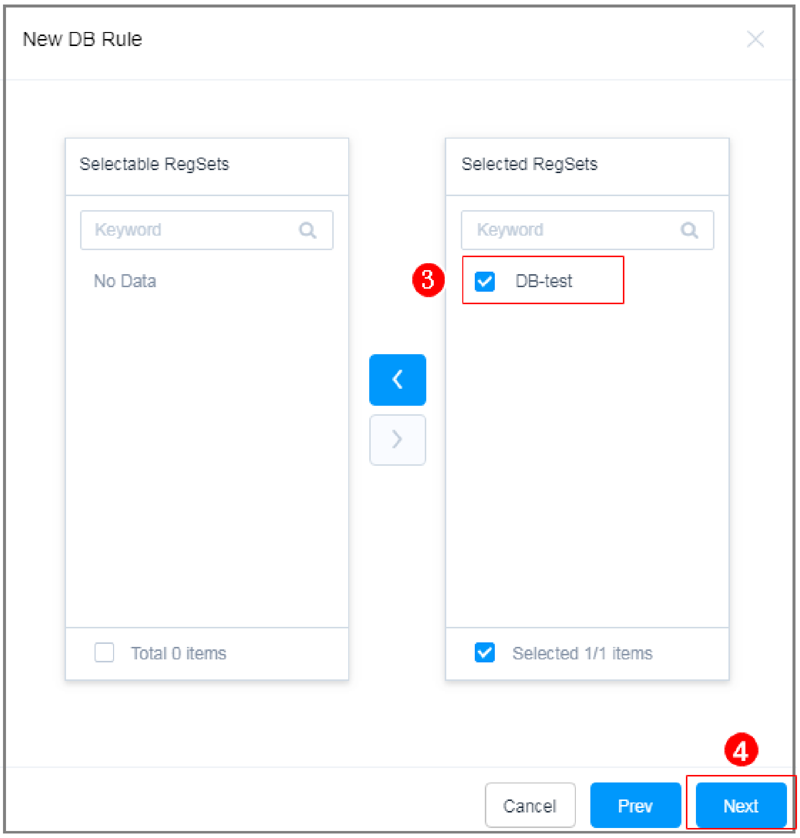
Action : Dynamic approval

Period of validity :

Time Limit :

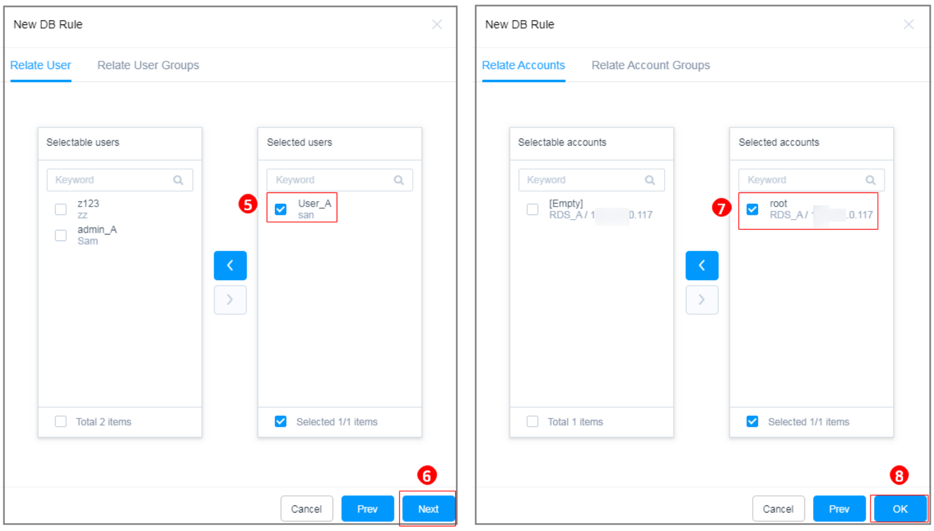
3. Relate the rule to rule set ***DB-test***.

Figure 3-6 Relating a new database rule to a rule set (RegSet)



4. Relate user ***User_A*** to resource ***RDS_A***.

Figure 3-7 Relating users to resources



----End

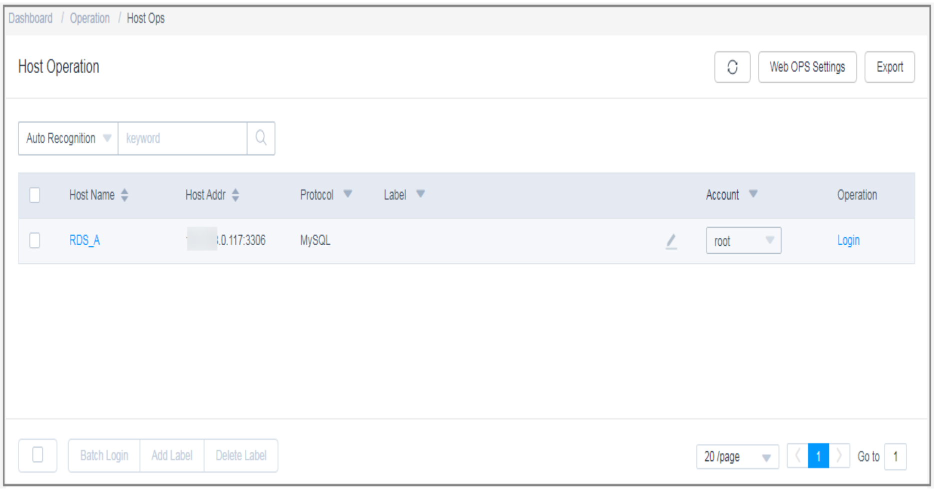
Verifying the Secondary Authorization Policy

An O&M user performs a high-risk operation and applies for operation permissions after the operation is intercepted. The administrator authorizes the high-risk operation after review to strengthen the management and control of core database assets.

Step 1 Log in to ***RDS_A*** as O&M user ***User_A***.

1. Log in to the CBH system.
2. Choose **Operation** > **Host Ops**.
3. Click **Log In** to log in to database resource ***RDS_A*** using an SSO tool.

Figure 3-8 Database login



Dashboard / Operation / Host Ops

Host Operation

Web OPS Settings | Export

Auto Recognition | keyword

□	Host Name	Host Addr	Protocol	Label	Account	Operation
□	RDS_A	[redacted]0.117:3306	MySQL		root	Login

□ Batch Login | Add Label | Delete Label

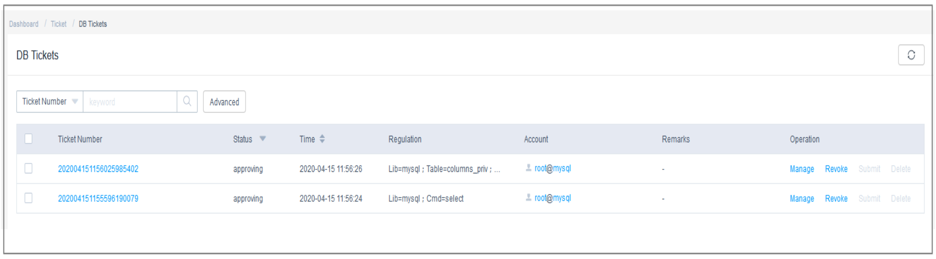
20 /page | 1 | Go to 1

Step 2 Use the Navicat client as an example. O&M user ***User_A*** deletes table content from ***RDS_A***. The **DELETE** command is automatically intercepted, and a message is displayed indicating that ***User_A*** does not have the permission to delete the table content.

Step 3 O&M user ***User_A*** submits a database authorization ticket to administrator ***admin_A*** for approval of the deletion operation.

1. Log in to the CBH system as O&M user ***User_A***.
2. Choose **Ticket** > **DB Tickets** and view the tickets generated due to the interception of the deletion.
3. Click **Submit** to submit the application for granting the required permissions on ***RDS_A***.

Figure 3-9 DB Tickets



Dashboard / Ticket / DB Tickets

DB Tickets

Ticket Number | keyword | Advanced

□	Ticket Number	Status	Time	Regulation	Account	Remarks	Operation
□	202004151156025985402	approving	2020-04-15 11:56:26	Lib=mysql ; Table=columns_priv ; ...	root@mysql	-	Manage Revoke Submit Delete
□	202004151155596190079	approving	2020-04-15 11:56:24	Lib=mysql ; Cmd=select	root@mysql	-	Manage Revoke Submit Delete

Step 4 The ***admin_A*** approves or rejects the O&M operations performed by ***User_A*** based on situation.

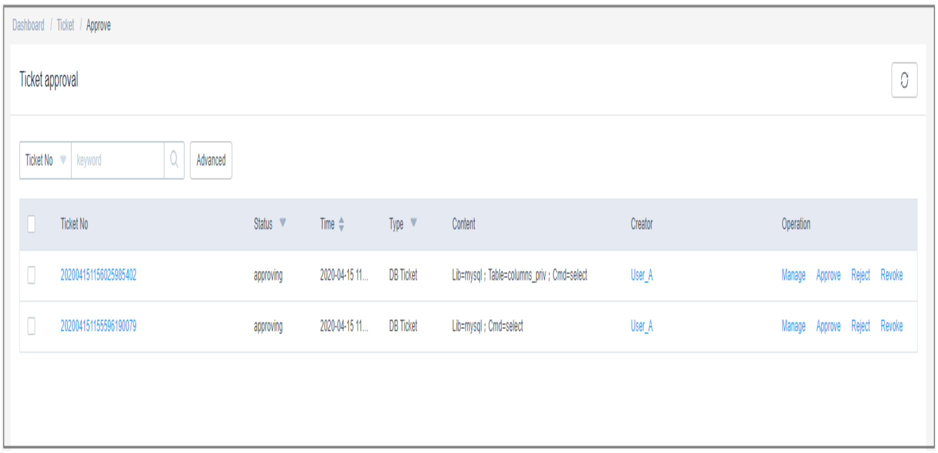
1. Log in to the CBH system as administrator ***admin_A***.

2. Choose **Ticket** > **Approve** and review the ticket submitted by ***User_A***.
3. Click **Approve** or **Reject** to approve or reject the ticket.

NOTE

Only after the administrator approves the ticket, the O&M user can resume the intercepted high-risk operations.

Figure 3-10 Ticket approval



□	Ticket No	Status	Time	Type	Content	Creator	Operation
□	202004151156025985402	approving	2020-04-15 11...	DB Ticket	Lib=mysql ; Table=columns_priv ; Cmd=select	User_A	Manage Approve Reject Revoke
□	202004151155596190079	approving	2020-04-15 11...	DB Ticket	Lib=mysql ; Cmd=select	User_A	Manage Approve Reject Revoke

----End

4 CBH for DJCP (or MLPS)

This topic describes which CBH functions are useful for DJCP certification. So that you can use certain functions and provide supporting materials accordingly to win DJCP certification easily.

Articles Related to DJCP Level 3 Certification

The following part focuses on the following DJCP articles:

- Security audit should be performed on network borders and important network nodes. Every user's critical behaviors and security events shall be audited.
- Audit records shall include the event date and time, users, event types, whether the events succeeded, and other related audit information.
- Audit records shall be protected and backed up periodically to avoid unexpected deletion, modification, or overwriting.
- Behavior audit and analyses shall be separately performed for remote access user behaviors and Internet access user behaviors.
- The identity of the login user shall be identified and authenticated. The ID shall be unique, and the identity authentication information shall meet complexity requirements and be changed periodically.
- Response measures to login failures, including stopping sessions, restricting the number of illegal logins, and automatically logging off expired network connections, shall be configured and enabled.
- During remote management, necessary measures shall be taken to prevent authentication information from being intercepted during transmission.
- Two or more authentication methods, including tokens, passwords, and biometric technologies, shall be used to authenticate user identity. Password authentication must be used.
- Appropriate accounts and permissions shall be assigned to login users.
- Default accounts shall be renamed or deleted, and their passwords should be changed.
- Redundant or expired accounts should be deleted or disabled in time to avoid account sharing.
- The minimum permissions shall be granted to management users to implement separation of privilege.

- Access control policies should be configured by the authorization subject, and the access policy should specify the rules for the subject to access the authorized object.
- The security audit function must be provided for each user to audit important security incidents and user behavior.
- Audit records shall include the event date and time, users, event types, whether the events succeeded, and other related audit information.

Prerequisites

You have purchased a later bastion host of the standard edition or later and completed the bastion host configuration.

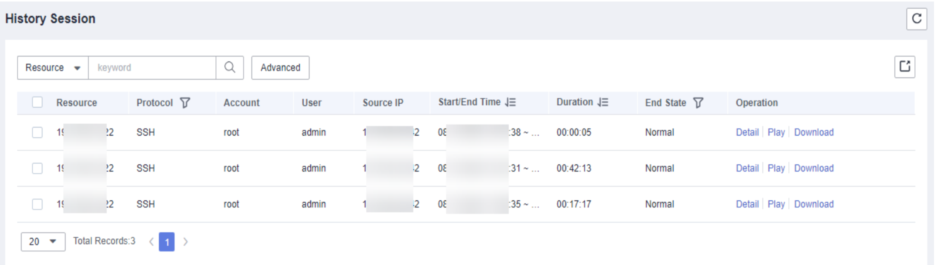
Security Zone Border: Security Audits

- DJCP article: **Security audit should be performed on network borders and important network nodes. Every user's critical behaviors and security events shall be audited.**

  This clause focuses on whether security audit is performed. CBH supports monitoring and security audits for O&M activities on cloud servers.

  - Log in to the CBH system using an account with the permission on the audit module. Choose **Audit** > **History Session**.

    Figure 4-1 Viewing historical sessions

    History Session

    Resource ▾ | keyword | Advanced

□	Resource	Protocol	Account	User	Source IP	Start/End Time	Duration	End State	Operation
□	19[redacted]22	SSH	root	admin	1[redacted]2	08[redacted]:38 ~ ...	00:00:05	Normal	Detail | Play | Download
□	19[redacted]22	SSH	root	admin	1[redacted]2	08[redacted]:31 ~ ...	00:42:13	Normal	Detail | Play | Download
□	19[redacted]22	SSH	root	admin	1[redacted]2	08[redacted]:35 ~ ...	00:17:17	Normal	Detail | Play | Download

    20 ▾ Total Records:3 ‹ 1 ›

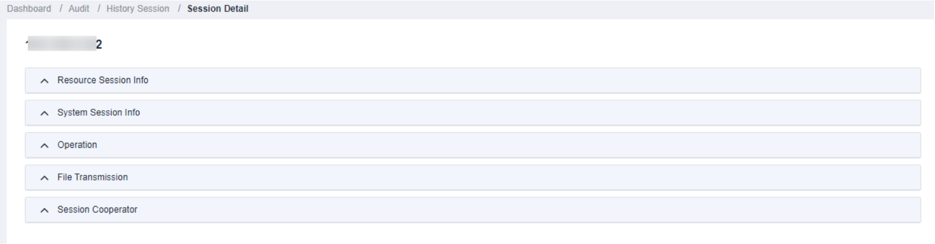
  - On the history session page, you can view resource session information, system session information, operation records, file transmission records, and collaborative session records.

- DJCP article: Audit records shall include the event date and time, users, event types, whether the events succeeded, and other related audit information.

  This article checks whether logs are recorded as required.

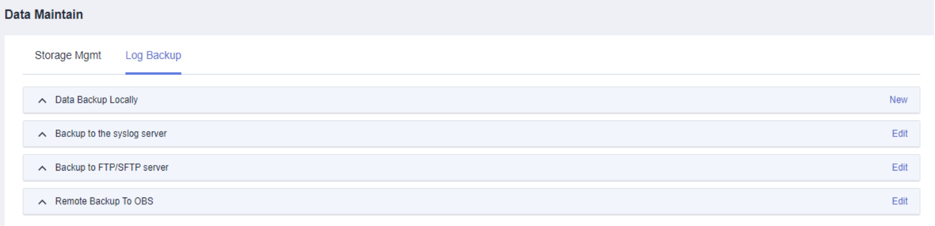
  - Log in to the CBH system using the administrator account. Choose **Audit** > **History Session**.
  - For a history session, you can view the resource name, type, host IP address, account, start and end time, session duration, session size, operation user, source IP address and MAC address of the operation user, login mode, operation records, file transfer records, and session collaboration records.

Figure 4-2 Viewing historical sessions



- Audit records shall be protected and backed up periodically to avoid unexpected deletion, modification, or overwriting.
  - Log in to the CBH system as the administrator, choose **System** > **Data Maintain**, and click **Log Backup** to go to the **Log Backup** page.
  - On the **Log Backup** page, you can create and view log backups, including system login logs, resource login logs, command operation logs, file operation logs, and two-person authorization logs. Data can also be backed up to the Syslog server, FTP server, SFTP server, and an OBS bucket.

Figure 4-3 Creating a database backup



- Behavior audit and analyses shall be separately performed for remote access user behaviors and Internet access user behaviors.

  This article checks whether remote access user activities and log data can be audited and analyzed.

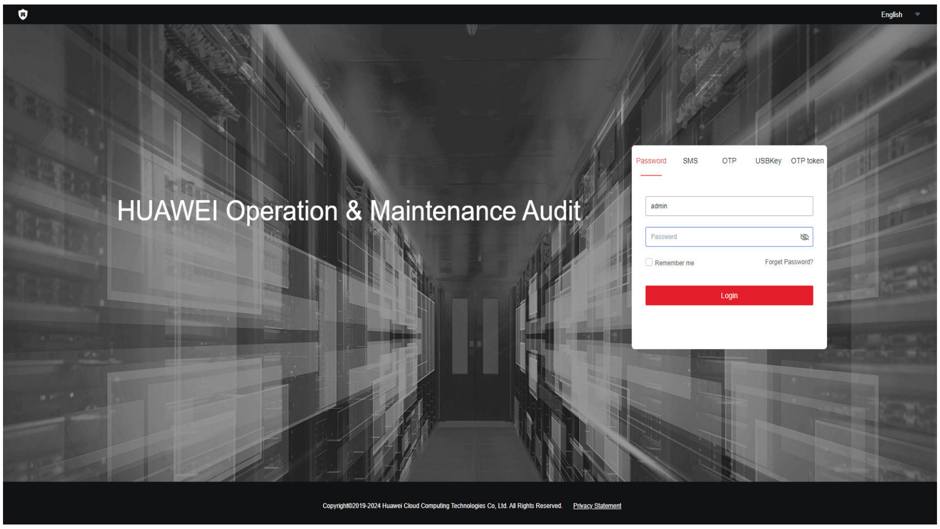
Secure Computing Environment: Identity Authentication

- DJCP article: The identity of the login user shall be identified and authenticated. The ID shall be unique, and the identity authentication information shall meet complexity requirements and be changed periodically.

  This clause focuses on the following three points:

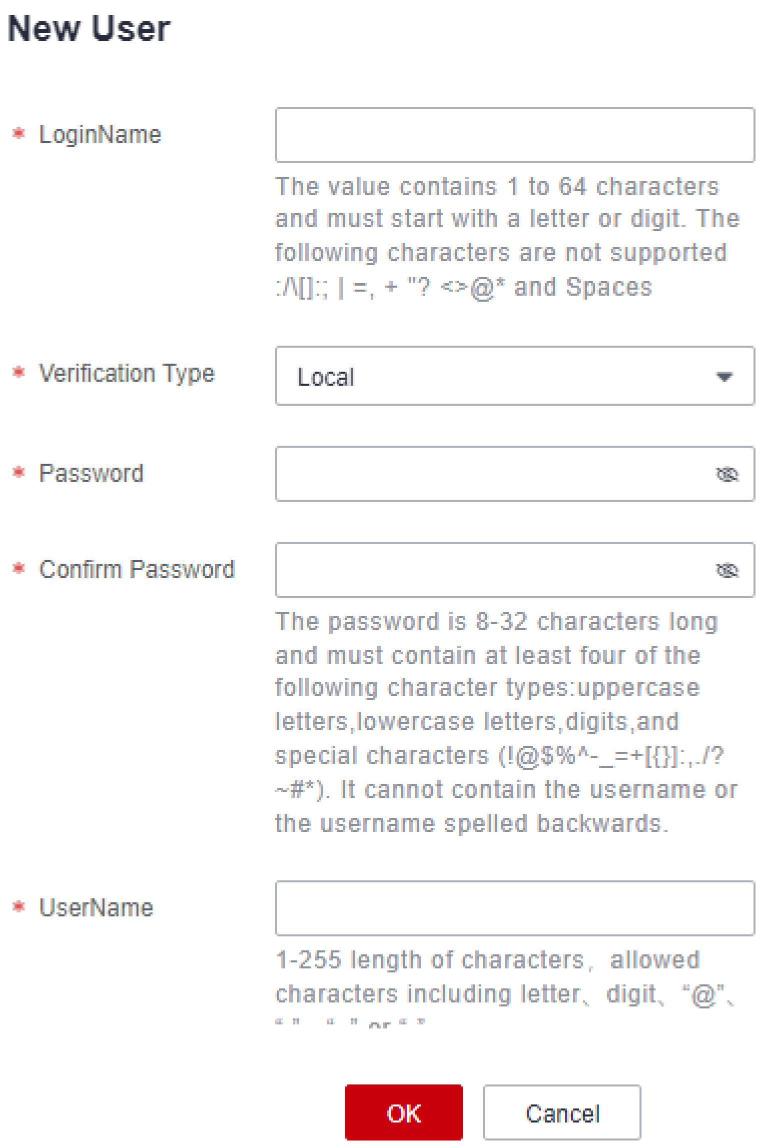
  a. Check whether the login user is identified and authenticated. If the user accesses the bastion host page using a browser, the product functions can be used only after the user identity is authenticated.

Figure 4-4 CBH system login page


English
HUAWEI Operation & Maintenance Audit
Password
SMS
OTP
USBKey
OTP token
admin
Password
Remember me
Forget Password?
Login
Copyright©2019-2024 Huawei Cloud Computing Technologies Co, Ltd. All Rights Reserved.
Privacy Statement

b. Uniqueness: When creating users, the username, mobile number, email address, and role must be unique for each user. Only one role can be configured for a user. For details, see **Creating a CBH System User**.

Figure 4-5 Creating a user



New User

* LoginName

The value contains 1 to 64 characters and must start with a letter or digit. The following characters are not supported :/\[]:; | =, + "? <>@* and Spaces

* Verification Type: Local

* Password

* Confirm Password

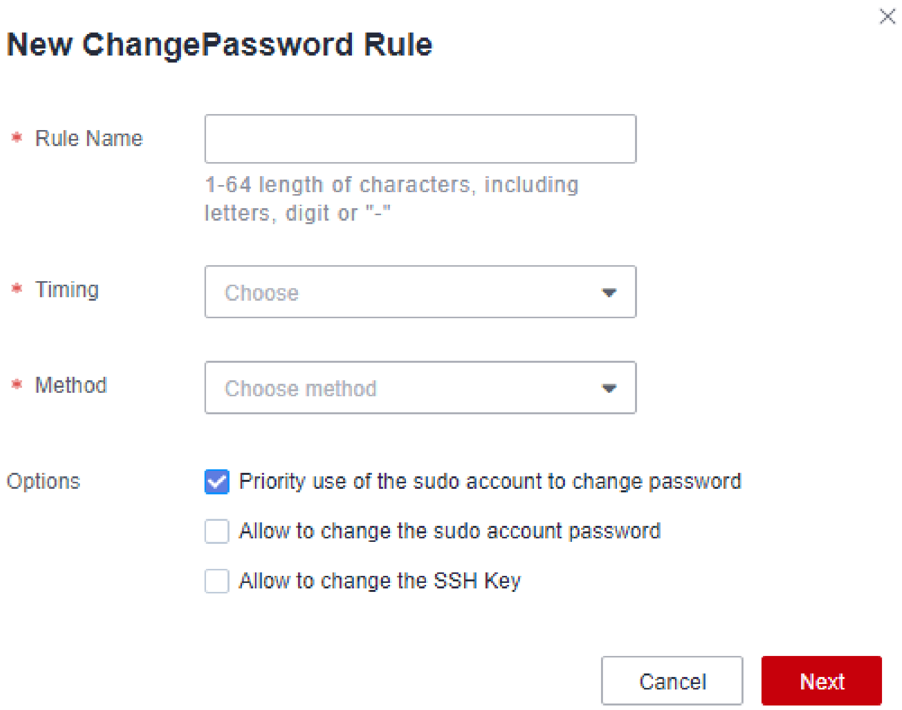
The password is 8-32 characters long and must contain at least four of the following character types:uppercase letters,lowercase letters,digits,and special characters (!@$%^-_=+[{}]:,./?~#*). It cannot contain the username or the username spelled backwards.

* UserName

1-255 length of characters, allowed characters including letter、digit、“@”、

c. Check whether password complexity and periodic change requirements on identity authentication are met. CBH supports manual, scheduled, and periodic password change methods. In addition, CBH supports generating different passwords, generating the same password, and specifying the same password for quickly change passwords for system users. For details, see **CBH Password Change Rules**.

Figure 4-6 Chpwd Rules



New ChangePassword Rule

* Rule Name

1-64 length of characters, including letters, digit or "-"

* Timing: Choose

* Method: Choose method

Options

☑ Priority use of the sudo account to change password

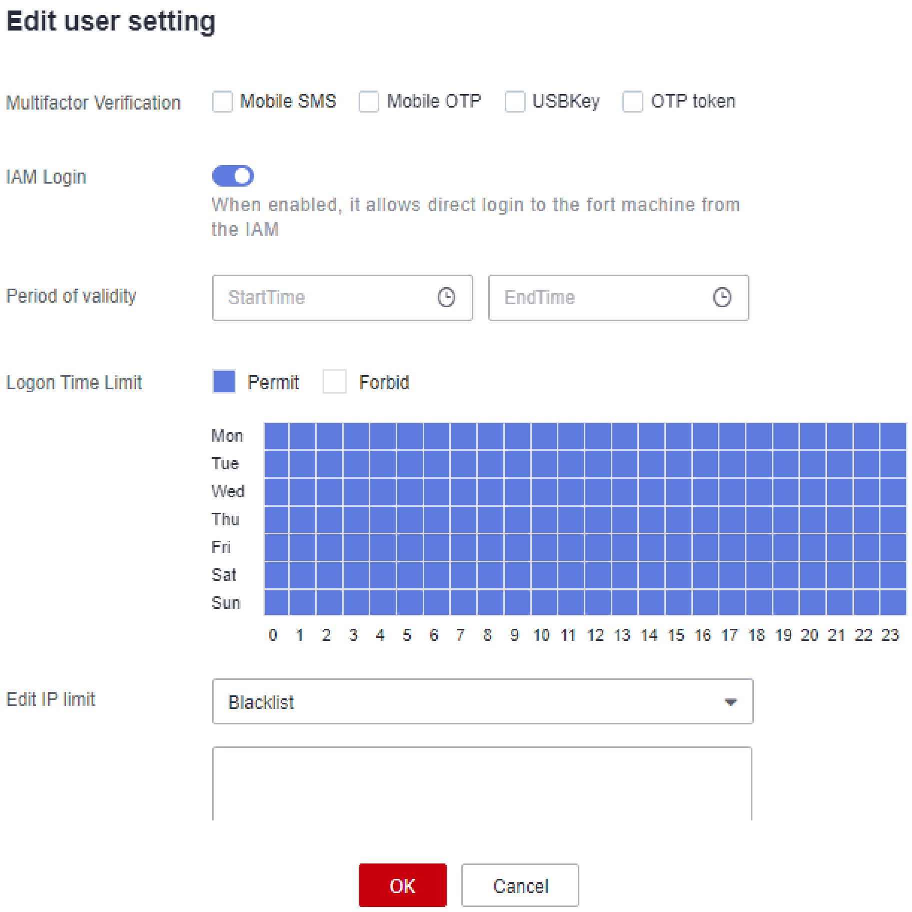
□ Allow to change the sudo account password

□ Allow to change the SSH Key

- DJCP article: Two or more authentication methods, including tokens, passwords, and biometric technologies, shall be used to authenticate user identity. Password authentication must be used.

  CBH uses multi-factor authentication. The login authentication methods include SMS messages, mobile phone tokens, USB keys, and dynamic OTPs.

Figure 4-7 Configuring Multifactor Verification



Edit user setting

Multifactor Verification □ Mobile SMS □ Mobile OTP □ USBKey □ OTP token

IAM Login ●

When enabled, it allows direct login to the fort machine from the IAM

Period of validity StartTime EndTime

Logon Time Limit ■ Permit □ Forbid

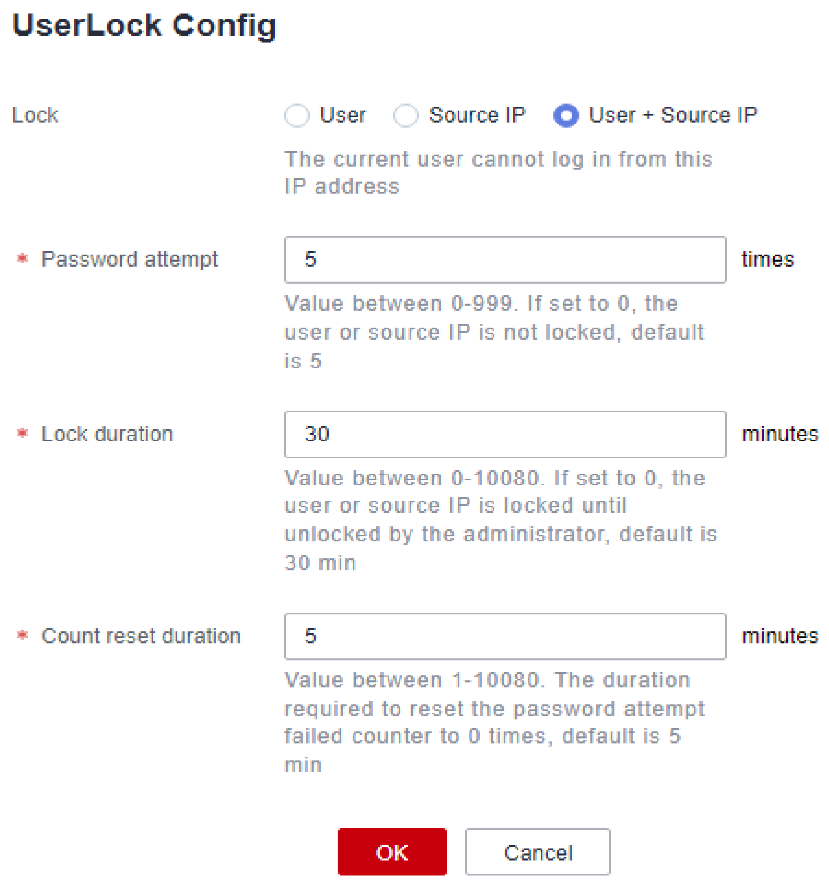
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Mon	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Tue	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Wed	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Thu	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Fri	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Sat	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Sun	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■

Edit IP limit Blacklist

- DJCP article: Response measures to login failures, including stopping sessions, restricting the number of illegal logins, and automatically logging off expired network connections, shall be configured and enabled.

  You can configure a security lock for user login, including the lock mode, lock duration, and maximum number of password attempts.

Figure 4-8 User login lockout



UserLock Config

Lock ○ User ○ Source IP ● User + Source IP

The current user cannot log in from this IP address

* Password attempt: 5 times

Value between 0-999. If set to 0, the user or source IP is not locked, default is 5

* Lock duration: 30 minutes

Value between 0-10080. If set to 0, the user or source IP is locked until unlocked by the administrator, default is 30 min

* Count reset duration: 5 minutes

Value between 1-10080. The duration required to reset the password attempt failed counter to 0 times, default is 5 min

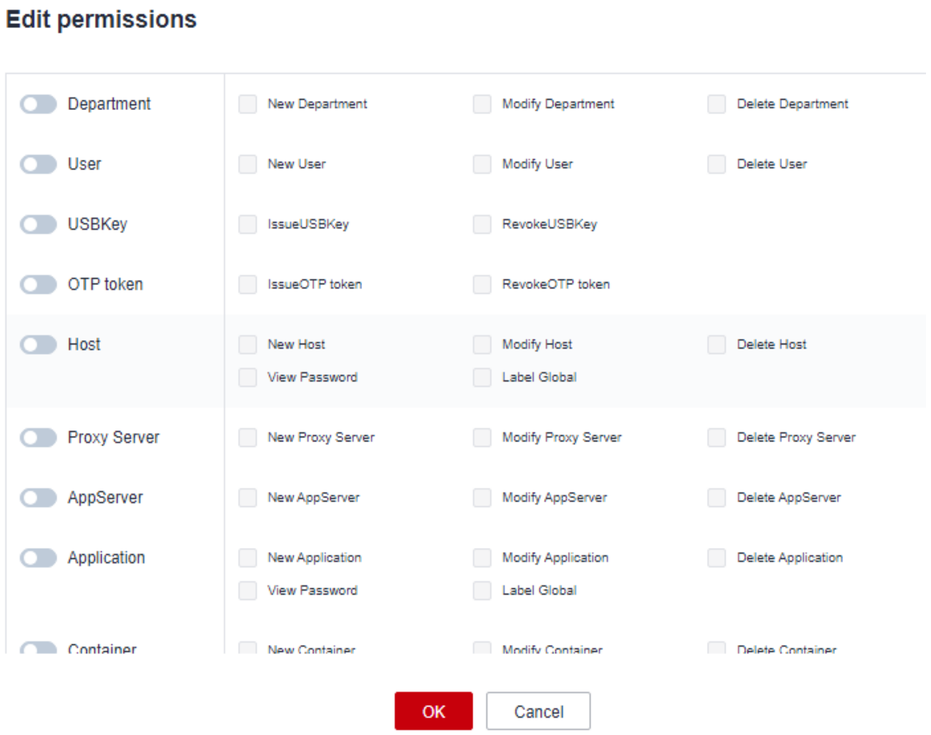
Access Control

- DJCP article: The minimum permissions shall be granted to management users to implement separation of privilege.

  CBH supports three types of user operation permissions: access control, command control, and database control policies.

  a. CBH can control some operation permissions based on login user roles. For example, you can grant the permission to delete and modify proxy servers to the O&M manager account.

Figure 4-9 Fine-grained role permissions

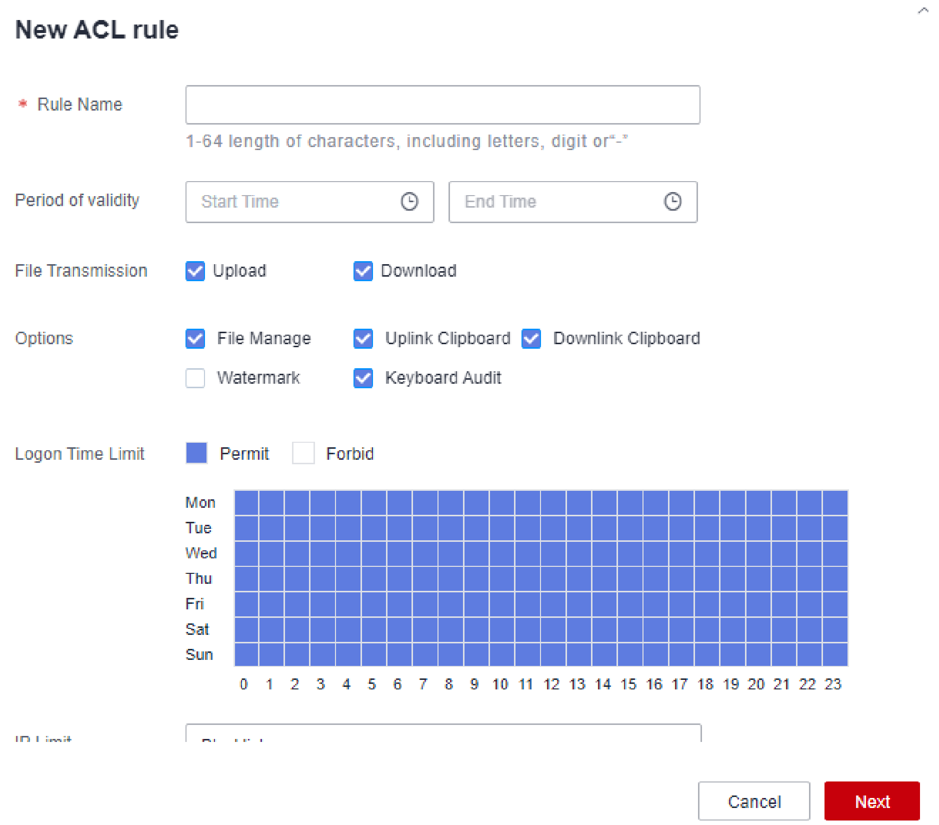


Edit permissions

Department	□ New Department	□ Modify Department	□ Delete Department
User	□ New User	□ Modify User	□ Delete User
USBKey	□ IssueUSBKey	□ RevokeUSBKey	
OTP token	□ IssueOTP token	□ RevokeOTP token	
Host	□ New Host □ View Password	□ Modify Host □ Label Global	□ Delete Host
Proxy Server	□ New Proxy Server	□ Modify Proxy Server	□ Delete Proxy Server
AppServer	□ New AppServer	□ Modify AppServer	□ Delete AppServer
Application	□ New Application □ View Password	□ Modify Application □ Label Global	□ Delete Application
Container	□ New Container	□ Modify Container	□ Delete Container

b. You can control access to specific functions, such file management, upstream clipboard, downstream clipboard, watermark display, login time control, file upload, and file download. You can also allow or block the users of certain source IP addresses to access managed resources.

Figure 4-10 ACL Rules



New ACL rule

* Rule Name

1-64 length of characters, including letters, digit or"-"

Period of validity: Start Time — End Time

File Transmission: ☑ Upload ☑ Download

Options: ☑ File Manage ☑ Uplink Clipboard ☑ Downlink Clipboard □ Watermark ☑ Keyboard Audit

Logon Time Limit: ■ Permit □ Forbid

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Mon	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Tue	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Wed	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Thu	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Fri	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Sat	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Sun	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■

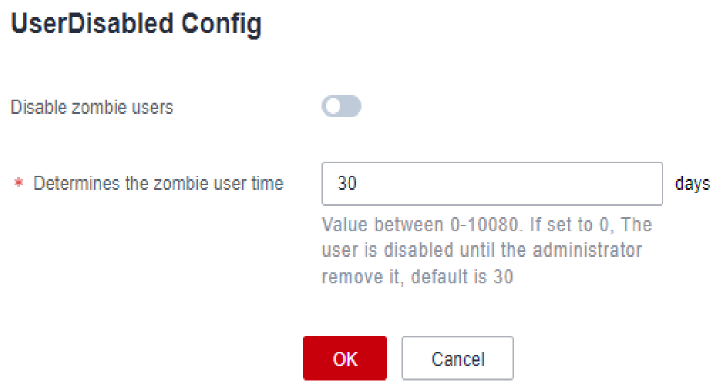
IP Limit

- DJCP article: Appropriate accounts and permissions shall be assigned to login users.

  CBH allows you to assign roles to users and create user groups for users. For details, see *User Role Management* and *CBH User Group Management* in the *Cloud Bastion Host User Guide*.

  Accounts that have not been used for a long time or have expired should be deleted in a timely manner. You can set a validity period for each CBH system user. Once the validity period expires, the corresponding account will be disabled as a zombie user.

Figure 4-11 Zombie user identification rule



UserDisabled Config

Disable zombie users

* Determines the zombie user time: 30 days

Value between 0-10080. If set to 0, The user is disabled until the administrator remove it, default is 30

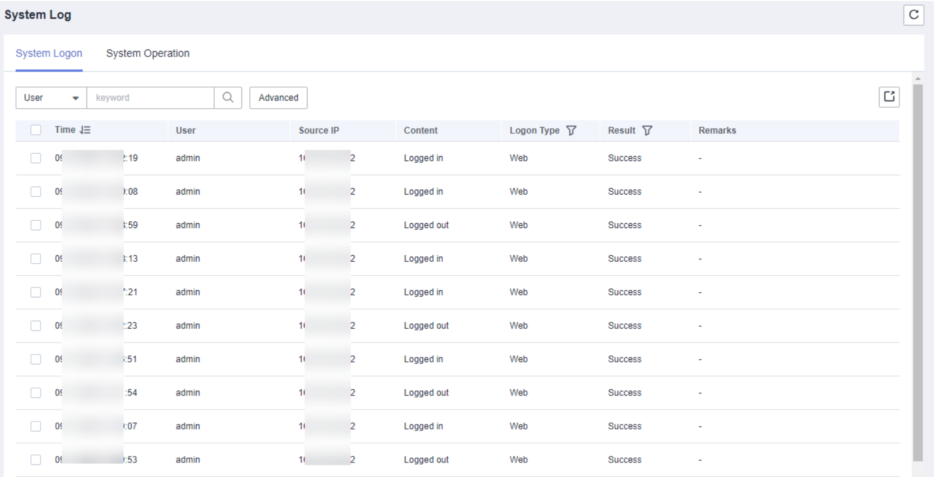
Security Audits

- DJCP article: The security audit function must be provided for each user to audit important security incidents and user behavior.

  CBH allows you to view real-time sessions, historical sessions, and system logs.

  You can view system login logs, including the login time, login user, source IP address, log content, login mode, login result, and remarks.

  Figure 4-12 System logon logs

  System Log

  System Logon | System Operation

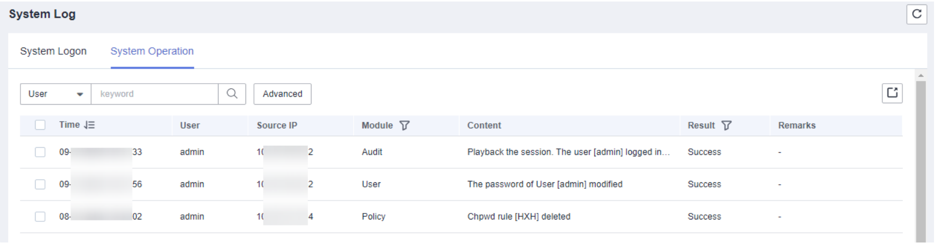
  User | keyword | Advanced

☐	Time	User	Source IP	Content	Logon Type	Result	Remarks
☐	0[redacted]:19	admin	1[redacted]2	Logged in	Web	Success	-
☐	0[redacted]:08	admin	1[redacted]2	Logged in	Web	Success	-
☐	0[redacted]:59	admin	1[redacted]2	Logged out	Web	Success	-
☐	0[redacted]:13	admin	1[redacted]2	Logged in	Web	Success	-
☐	0[redacted]:21	admin	1[redacted]2	Logged in	Web	Success	-
☐	0[redacted]:23	admin	1[redacted]2	Logged out	Web	Success	-
☐	0[redacted]:51	admin	1[redacted]2	Logged in	Web	Success	-
☐	0[redacted]:54	admin	1[redacted]2	Logged out	Web	Success	-
☐	0[redacted]:07	admin	1[redacted]2	Logged in	Web	Success	-
☐	0[redacted]:53	admin	1[redacted]2	Logged out	Web	Success	-

- DJCP article: Audit records shall include the event date and time, users, event types, whether the events succeeded, and other related audit information.

  You can view which accounts performed what operations in system operation logs, including the user, time, source IP address, module, log content, and result.

  Figure 4-13 System operation logs

  System Log

  System Logon | System Operation

  User | keyword | Advanced

☐	Time	User	Source IP	Module	Content	Result	Remarks
☐	09-[redacted]33	admin	1[redacted]2	Audit	Playback the session. The user [admin] logged in...	Success	-
☐	09-[redacted]56	admin	1[redacted]2	User	The password of User [admin] modified	Success	-
☐	08-[redacted]02	admin	1[redacted]4	Policy	Chpwd rule [HXH] deleted	Success	-

5 Cross-Cloud, Cross-VPC O&M for Resources On and Off the Cloud

Application Scenarios

If you have servers deployed across VPCs, in on-premises data centers, and across multiple clouds, CBH is always a good choice for centralized O&M. With CBH, you can manage scattered servers centrally without establishing dedicated lines, making O&M of all workloads efficiently and securely.

This topic describes how to use the CBH system to manage and maintain your resources across VPCs, clouds, and on-premises environments. Before doing this, you need to enable communications between your CBH instance and the network where the resources to be managed with CBH locate. The following walks you through how to configure a proxy server in a target network and connect the proxy server to a CBH system.

Prerequisites and Preparations

- Your CBH instance is running properly.
- You have purchased an ECS, and the ECS is running properly.
- You have obtained a server from the peer network domain as the proxy server.
- An EIP has been bound to the proxy server. For details, see **Binding an EIP to an Instance**.
- The proxy server can communicate with the servers you want CBH to manage.
- You have downloaded **the latest version 3proxy** package.

Setting the Proxy Server

Before managing and maintaining servers across network domains, you need to configure a network proxy server in the peer network domain. Then connect the proxy server to service servers through the intranet, and connect the proxy server to the CBH network. In this way, the CBH system can communicate with the service servers across domains.

This operation is the prerequisite for a bastion host to manage host resources across networks.

- **Enabling the Network Proxy Service for the Proxy Server**

Step 1 Log in to the proxy server and set the proxy server (assume it is named **3proxy**).

> ⚠ CAUTION
>
> The commands in Step 2 to Step 4 are based on CentOS 7. For details about example commands for CentOS 8, see **Example for Configuring a Proxy for CentOS 8**.

Step 2 Upload and decompress the 3proxy package, go to the corresponding directory, and run the following command:

```
bash install.sh
```

Step 3 Enter the following command to add the **3proxy** user:

```
/etc/3proxy/add3proxyuser.sh myuser mypassword
```

Step 4 Restart the proxy service **3proxy**.

```
systemctl restart 3proxy
```

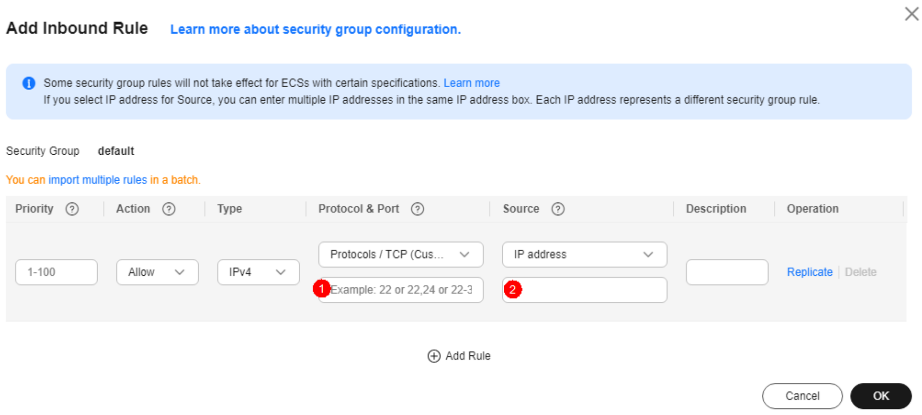
> NOTE
>
> - The SOCKS5 proxy protocol (port: 1080) does not provide the encryption function. If an unencrypted protocol is used for O&M through the proxy server, disable access from unnecessary IP addresses in the security group settings.
> - If encrypted transmission or data security is required, you can select an encrypted protocol when selecting an inbound or outbound rule. The protocol can be SSH, RDP, SFTP, SCP, or Rlogin.

----End

- **Configuring Security Group Rules for the Proxy Server**

Step 1 Configure **inbound rules** to allow the bastion host to access the proxy server.

Figure 5-1 Inbound rule configuration



Add Inbound Rule Learn more about security group configuration.

Some security group rules will not take effect for ECSs with certain specifications. Learn more
If you select IP address for Source, you can enter multiple IP addresses in the same IP address box. Each IP address represents a different security group rule.

Security Group default

You can import multiple rules in a batch.

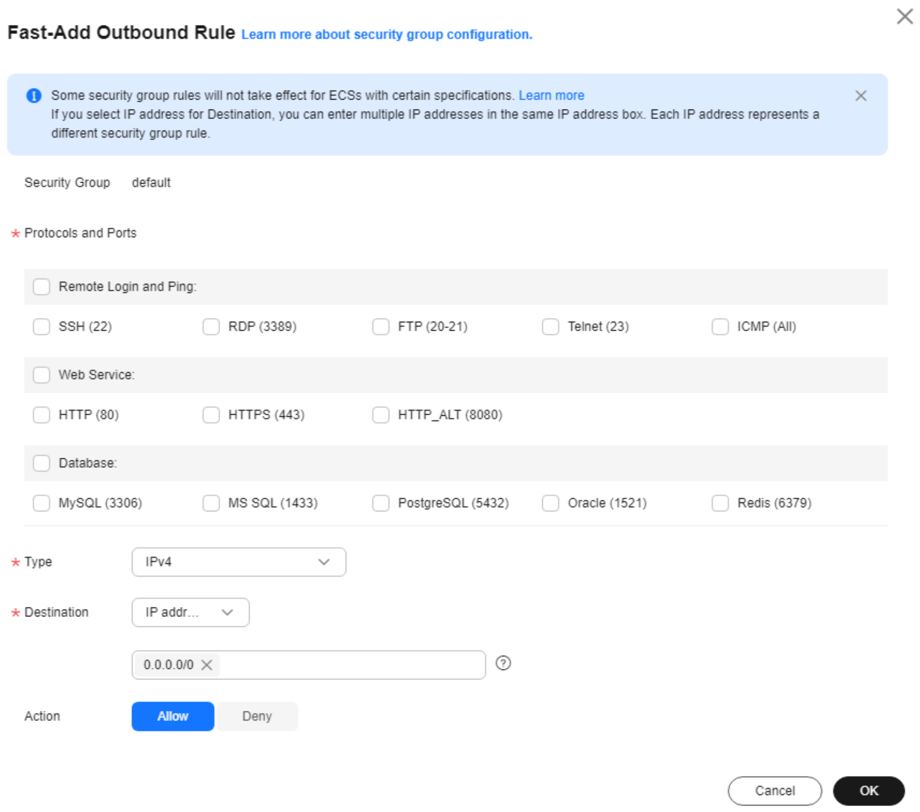
Priority	Action	Type	Protocol & Port	Source	Description	Operation
1-100	Allow	IPv4	Protocols / TCP (Cus... 1 Example: 22 or 22,24 or 22-3	IP address 2		Replicate | Delete

NOTE

- Set **Protocol & Port** to the default port **1080** for the SOCKS5 proxy server.
- Enter the IP address of the bastion host in the **Source** text box.

Step 2 Configure **outbound rules** for the proxy server to allow the proxy server to access the service servers managed with CBH.

Figure 5-2 Outbound rule configuration



Fast-Add Outbound Rule Learn more about security group configuration.

Some security group rules will not take effect for ECSs with certain specifications. Learn more
If you select IP address for Destination, you can enter multiple IP addresses in the same IP address box. Each IP address represents a different security group rule.

Security Group default

* Protocols and Ports

□ Remote Login and Ping:

□ SSH (22) □ RDP (3389) □ FTP (20-21) □ Telnet (23) □ ICMP (All)

□ Web Service:

□ HTTP (80) □ HTTPS (443) □ HTTP_ALT (8080)

□ Database:

□ MySQL (3306) □ MS SQL (1433) □ PostgreSQL (5432) □ Oracle (1521) □ Redis (6379)

* Type IPv4

* Destination IP addr...

0.0.0.0/0

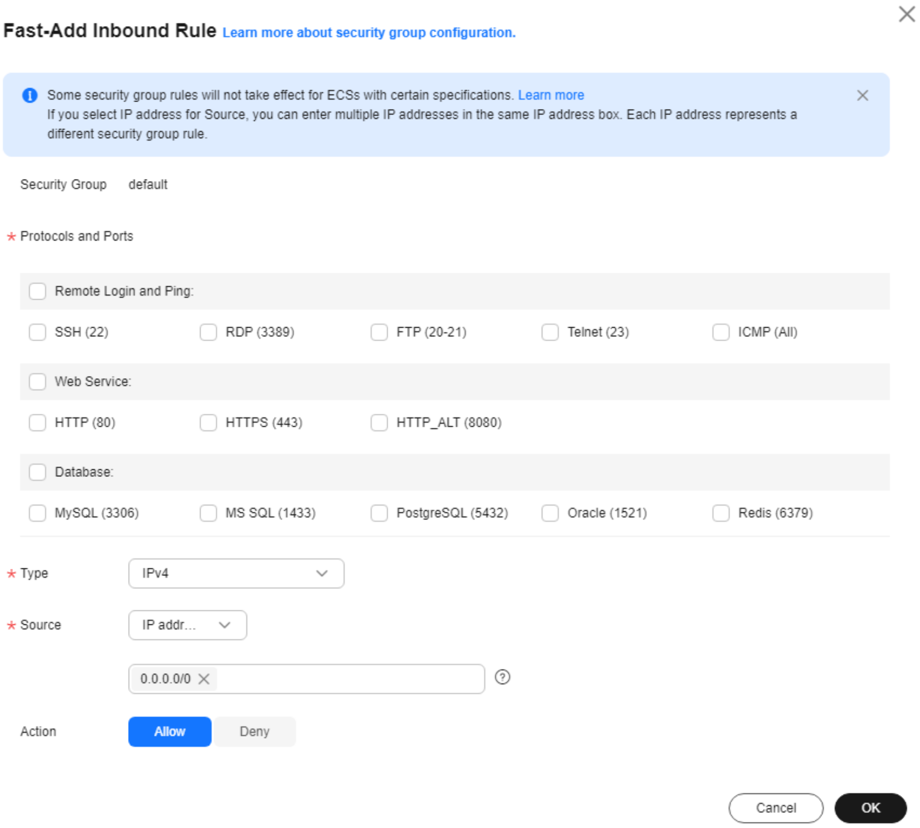
Action Allow Deny

----End

Using CBH to Manage Cross-Domain Service Servers

Step 1 Log in to the network console and choose **Access Control** > **Security Groups**. On the **Security Groups** page, configure the inbound and outbound rules of the security group associated with the CBH instance.

Figure 5-3 Configuring an inbound rule for a CBH instance



Fast-Add Inbound Rule Learn more about security group configuration.

Some security group rules will not take effect for ECSs with certain specifications. Learn more
If you select IP address for Source, you can enter multiple IP addresses in the same IP address box. Each IP address represents a different security group rule.

Security Group default

* Protocols and Ports

□ Remote Login and Ping:

□ SSH (22) □ RDP (3389) □ FTP (20-21) □ Telnet (23) □ ICMP (All)

□ Web Service:

□ HTTP (80) □ HTTPS (443) □ HTTP_ALT (8080)

□ Database:

□ MySQL (3306) □ MS SQL (1433) □ PostgreSQL (5432) □ Oracle (1521) □ Redis (6379)

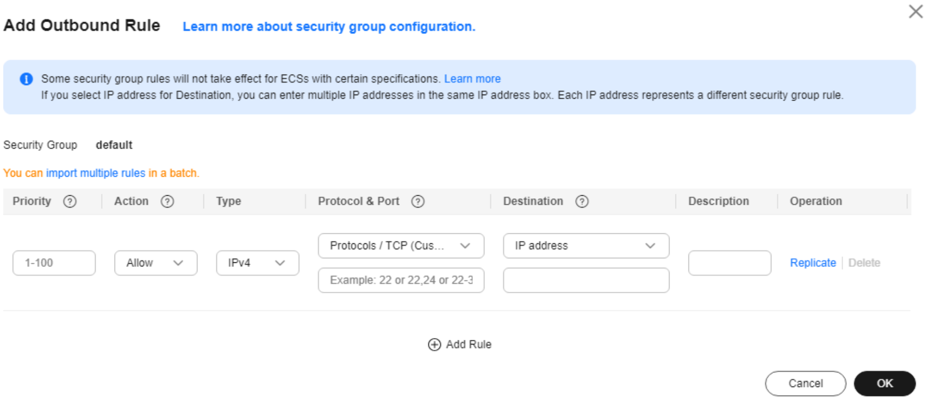
* Type IPv4

* Source IP addr...

0.0.0.0/0

Action Allow Deny

Figure 5-4 Configuring an outbound rule for a CBH instance



Add Outbound Rule Learn more about security group configuration.

Some security group rules will not take effect for ECSs with certain specifications. Learn more
If you select IP address for Destination, you can enter multiple IP addresses in the same IP address box. Each IP address represents a different security group rule.

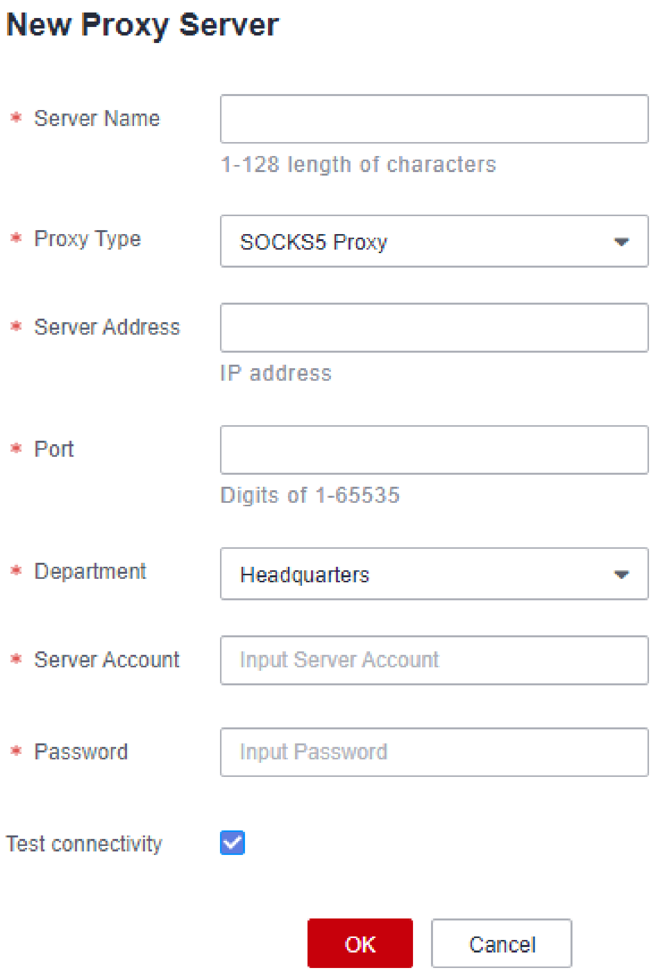
Security Group default

You can import multiple rules in a batch.

Priority	Action	Type	Protocol & Port	Destination	Description	Operation
1-100	Allow	IPv4	Protocols / TCP (Cus... Example: 22 or 22,24 or 22-3	IP address		Replicate | Delete

Step 2 Use CBH to manage proxy servers. Log in to the CBH system and add the proxy server. For details, see **Adding a Host**. On the **Host** page, click the **Proxy Server** tab and then **New**.

Figure 5-5 New Proxy Server



New Proxy Server

* Server Name:
1-128 length of characters

* Proxy Type: SOCKS5 Proxy

* Server Address:
IP address

* Port:
Digits of 1-65535

* Department: Headquarters

* Server Account: Input Server Account

* Password: Input Password

Test connectivity ☑

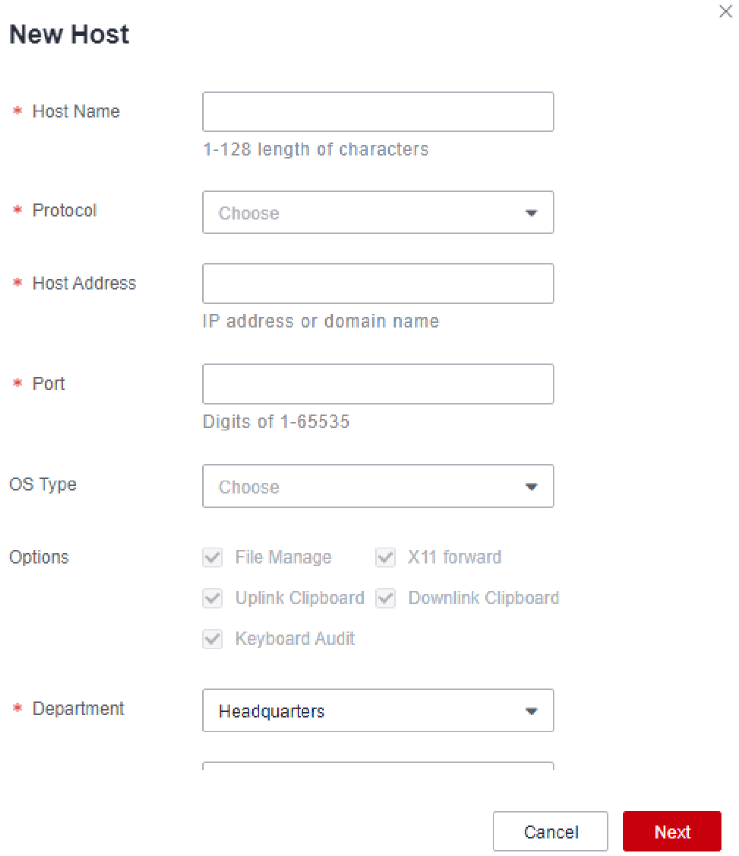
Step 3 Go back to the security group (the one you select in **Step 1**) your service servers belong to. On the **Inbound Rules** tab, click **Fast-Add Rule**.

NOTE

You can also add some outbound rules as required.

Step 4 Use CBH to manage service servers. For details, see **Adding Hosts**.

Figure 5-6 New Host



New Host

* Host Name:
1-128 length of characters

* Protocol: Choose

* Host Address:
IP address or domain name

* Port:
Digits of 1-65535

OS Type: Choose

Options: ☑ File Manage ☑ X11 forward ☑ Uplink Clipboard ☑ Downlink Clipboard ☑ Keyboard Audit

* Department: Headquarters

----End

After the preceding operations are performed, you can perform O&M on the managed hosts across network domains using the host operation function in CBH. Similarly, the preceding methods can be applied to different network environments such as hybrid/heterogeneous clouds and offline IDCs to implement unified online and offline O&M across clouds and VPCs.

Example for Configuring a Proxy for CentOS 8

Step 1 Run the following command to install the 3proxy software package:

```
yum install -y epel-release
```

```
yum install -y 3proxy
```

Step 2 Run the following command to perform simplified configuration:

```
nscache 65536
```

```
timeouts 1 5 30 60 180 1800 15 60
```

# Set the username. Enter the username after the **users** command. Enter the username after the **CL** command. This section uses **test** as an example.

```
users test:CL:test
```

```
daemon
```

```
log /var/log/3proxy/3proxy.log
logformat "- +_L%t.%. %N.%p %E %U %C:%c %R:%r %O %I %h %T"
archiver gz /bin/gzip %F
rotate 30
external 0.0.0.0
internal 0.0.0.0
auth strong
allow test
maxconn 20
socks
flush
```

Step 3 Start the service.

```
systemctl start 3proxy
```

----End

6 How Can We Use CBH to Locate Incident Causes?

As cloud services develop, the number of cloud O&M engineers increases. In this case, security incidents may occur due to negligence. Tradition servers do not provide functions such as command monitoring and operation playback, resulting in incomplete traceability of security events.

CBH can manage and control all operations and log all operations in detail. Audit logs of sessions can be viewed online, recorded and played online, and played offline after being downloaded. CBH allows you to audit operations performed over character protocols (SSH and TELNET), graphics protocol (RDP and VNC), file transfer protocols (FTP, SFTP, and SCP), and database protocols (DB2, MySQL, Oracle, and SQL Server), as well as application publishing. For operations over character and database protocols, their operation instructions can be parsed so that you can know what actions have been done. For file transfer actions, the name and destination path of a transferred file can be logged.

Overview

This topic describes how to use CBH session audit function to trace and investigate security events and determine responsibilities.

Prerequisites

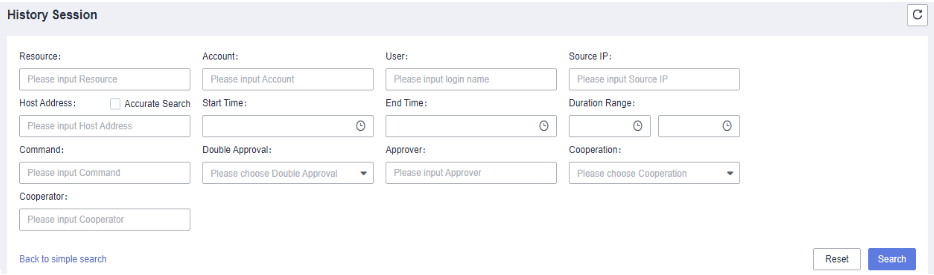
You have purchased a CBH instance and logged in to it using an account that has the audit module permission.

Auditing Historical Sessions

Step 1 Log in to CBH console. Go to the **History Session** page. For details, see **Viewing History Sessions**.

Step 2 Enter the related information in the advanced search box based on your security issues.

Figure 6-1 Advanced search



Step 3 Locate the target security issue, click **Detail** in the **Operation** column to view the historical commands and file transfers.

----End

You can locate the fault based on the commands, ensuring event traceability. You can also use the session playback function to view the specific operations by playing the corresponding O&M video. For details, see **Managing Session Videos**.

NOTICE

CBH also provides real-time session monitoring. This means you can view the O&M page of high-risk operations in real time. If an alarm is reported for an on-going risky command, the corresponding operations can be immediately terminated to ensure service security.