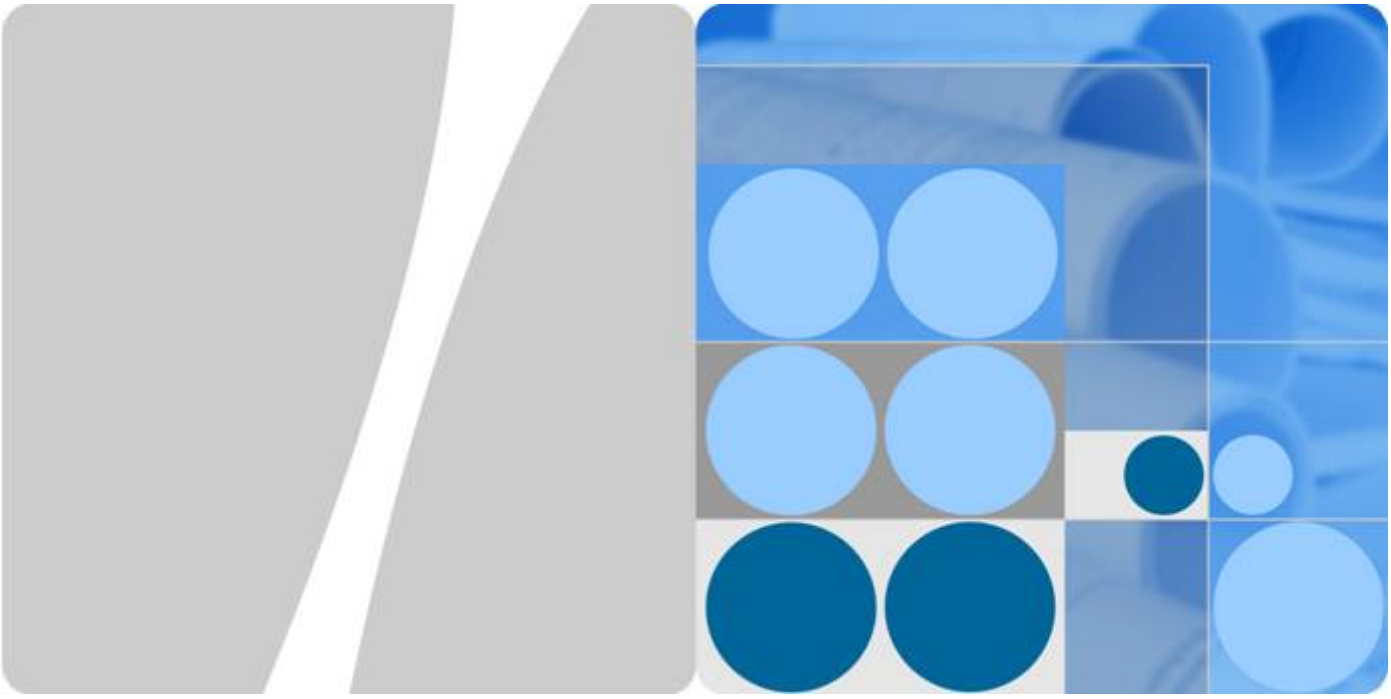


Cloud Bastion Host

Quick Start

Date 2022-12-01

Contents

1 Before You Start..... 1
2 Step 1: Log In to a CBH System..... 4
3 Step 2: Create a CBH System User..... 10
4 Step 3: Add Resources to the CBH System..... 13
5 Step 4: Configure O&M Permissions..... 18
6 Step 5: Log In to a Resource You Want to Manage..... 20
7 Step 6: Audit O&M Sessions..... 21

1 Before You Start

This document provides instructions for getting started with Cloud Bastion Host (CBH). CBH gives you the ability to:

- Log in to the CBH system using a web browser or SSH client, create system users, add resources, configure permission policies, and grant O&M permissions to system users based on their responsibilities.
- Log in to the managed resources within granted permissions.
- Audit O&M sessions, logins, and system operations by resource and/or user.

Figure 1-1 shows how to configure a CBH instance and use the mapped CBH system for secure O&M.

Figure 1-1 Process

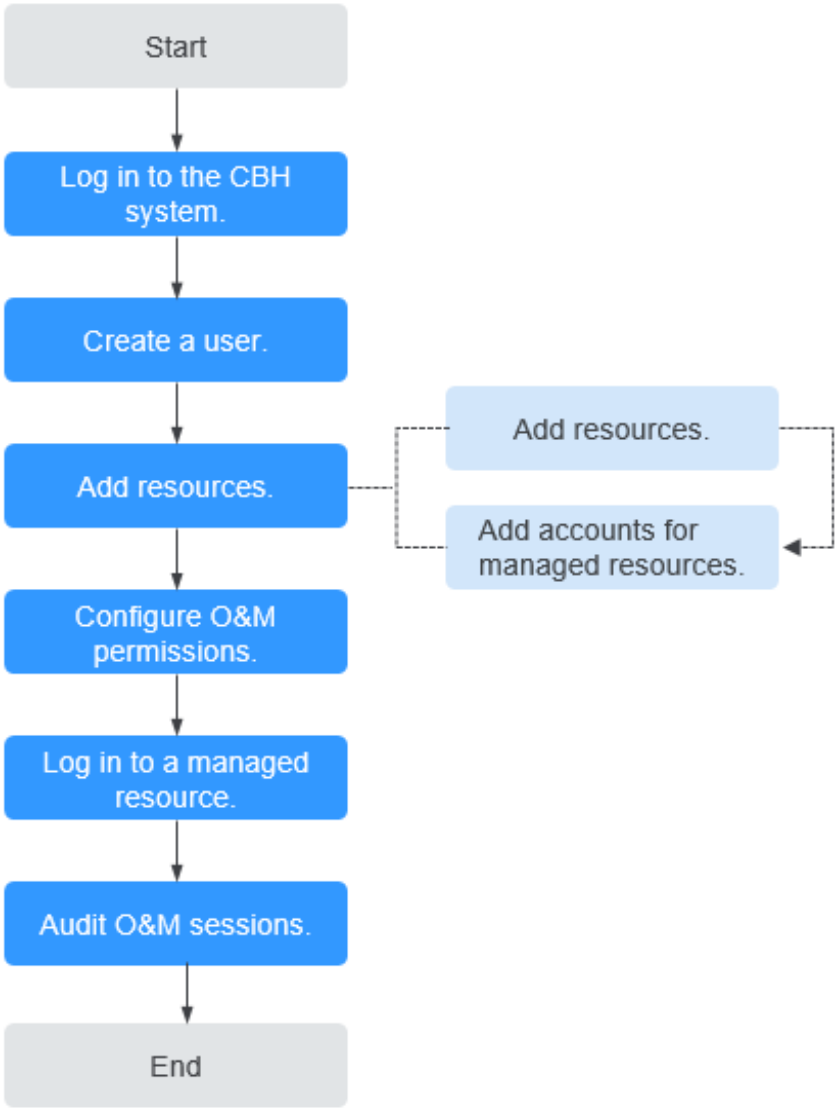


Table 1-1 Process overview

Procedure	Description
Logging in to a CBH system	After you enable a CBH instance, obtain the IP address to log in to the CBH system that maps to the CBH instance. The **admin** user is the first user that can log in to the CBH system. The password of the **admin** user is the one you set when you purchase the CBH instance.
Creating a user	Create a CBH system user. Each user corresponds to an account for logging in to the CBH system.

Procedure	Description
Adding resources	Add resources and their accounts to the CBH system. • Linux hosts, Windows hosts, databases, and applications can be added. • After you add resources to CBH, add the accounts of the added resources to the CBH system so that you can directly access the managed resources through CBH for O&M.
Configuring O&M permissions	Create access control rules. You can grant permissions to each system user based on their responsibilities to determine which users can perform O&M on a specific resource.
Logging in to a managed resource	Multi-factor authentication can be configured for different types of resources.
Auditing O&M sessions	You can audit logins, operations on managed resources, and O&M sessions in the CBH system.

2 Step 1: Log In to a CBH System

Scenarios

You can log in to your CBH system through a web browser, MSTSC client, or SSH client.

- Web browser login: In this method, you can use the system management and resource O&M modules in CBH. This method is recommended for system user **admin** or administrators to manage the CBH system and audit authorization.
- SSH client login: You can use an SSH client to directly log in to the authorized resources for O&M without changing your original login methods.
- MSTSC client login: With CBH, your current MSTSC-based O&M experience is still useful. You can use an MSTSC client to directly log in to the CBH system for resource O&M.

Prerequisites

- You have purchased a CBH instance. If you want to access the CBH instance over the public network, bound an EIP to it. For details, see **Purchasing a CBH Instance**.
- The CBH instance is in the **Running** state, and the CBH system is within the authorization period.
- You have obtained the address and credentials for logging in to the CBH system.

Using a Web Browser to Log In to a CBH System

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

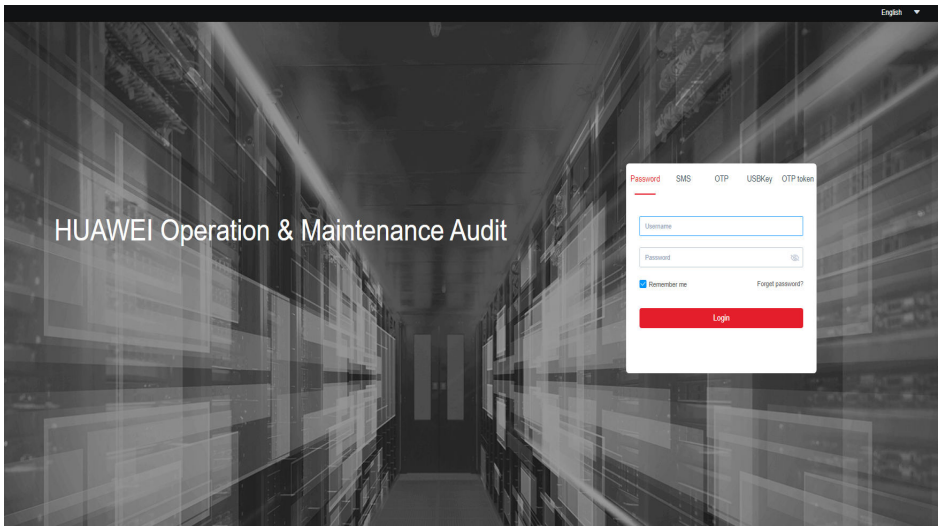
URL: https:// *EIP or private IP address of the CBH instance*, for example, *https://10.10.10.10*.

NOTE

- If no EIP is bound to your CBH instance, use the private network IP address to log in to the CBH system. Ensure that your local network and the private network of the CBH system are connected.
- If a browser incompatible with the CBH system is used, the login verification message may fail to be sent to you, or exceptions may occur after the login. For recommended browsers, see **Restrictions on Using CBH**.

Step 2 Select a login authentication method.

Figure 2-1 CBH system login page



- Multi-factor Authentication (MFA) can be enabled for all CBH users. CBH supports **SMS**, **OTP**, **USBKey**, and **OTP Token**. For details, see **Configuring Multifactor Verification**.
- After multi-factor authentication is configured, **Password** authentication becomes invalid.

Table 2-1 Web browser login authentication

Authentication Method	How to Log In	Configuration Description
Password	Enter the username and password of your CBH system user account.	Default login method. The login passwords in the **AD**, **RADIUS**, **LDAP**, or **Azure AD** authentication are the passwords of users on the remote server. For details, see **System Configuration Overview**.

Authentication Method	How to Log In	Configuration Description
SMS	Enter the username and password, click **Send code**, and enter the SMS verification code you will receive.	A valid phone number has been configured for the account.
OTP	Enter the username and password and enter the mobile phone one-time password (OTP), which changes periodically. **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**.
USBKey	Insert and select an issued USB key and enter the corresponding PIN.	A USB key has been issued to the user. For details, see **Issuing a USB Key**.
OTP token	Enter the username and password, and enter the dynamic password of the OTP device, which changes periodically.	An OTP token has been issued to the user. For details, see **Issuing an OTP Token**.

Step 3 Click **Login** to log in to the CBH system for O&M.

NOTE

- The **admin** user is a system administrator account that is used to log in to the CBH system for the first time. The **admin** account has the highest level of authority. Permissions for the **admin** account cannot be modified. Keep the account information secure.
- After you log in to the CBH system for the first time, change the passwords and configure the phone number as prompted. Otherwise, the system cannot be further loaded. The phone number can be changed on the profile page in the **Dashboard** module.

----End

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

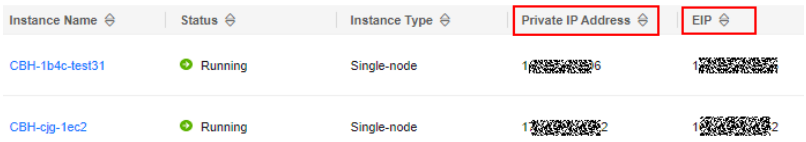
  In the newly opened blank session window, run a command in the following format: ***Protocol type User login name@System login IP address Port number***, for example, ssh admin@10.10.10.10 2222.

- 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.

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 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 2-2 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

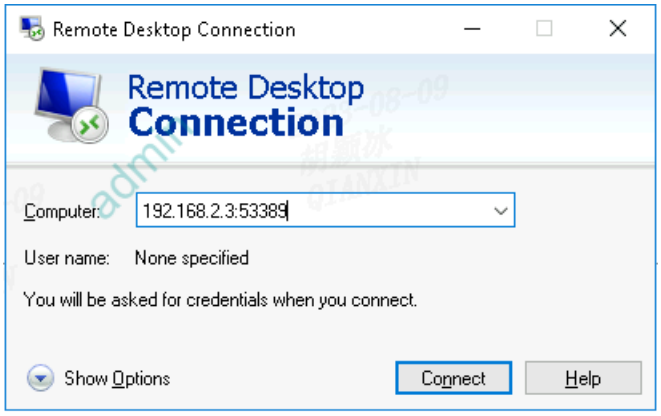
Accessing a CBH system through Microsoft Terminal Services Client (MSTSC)

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 2-2 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

3 Step 2: Create a CBH System User

Scenarios

Before using the CBH system, administrators need to create system users in the CBH system and assign different system roles to them based on their responsibilities.

System users then can access the modules within the permissions.

Only the **admin** user has the permissions to manage system roles.

Procedure

Table 3-1 Different user creation methods

Creation Method	Description
Creating a User	Create system users one by one. This method applies to create an administrator.
Batch Importing Users Using an Excel File	Configure user information in the Excel template and import the generated Excel file to the CBH system. This feature enables you to add system users in batches.
Synchronizing AD Domain Users	Synchronize system users from the AD domain server. You can use the username and password of a user synchronized from the AD domain to log in to the CBH system, and the login is authenticated by the AD domain server.

Configuration Description

Table 3-2 User information description

Parameter	Description
LoginName	Specifies the username for system users to log in to the CBH system. The **LoginName** must be unique in the CBH system and cannot be changed after it is created.
Verification Type	Specifies the identity authentication methods 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.
Password/ Confirm Password	Specifies the password for the user to log in to the CBH system.
UserName	Specifies the user-defined name used to differentiate CBH system users.
Mobile	Specifies the phone number of the user. This phone number is used by the user to receive SMS messages for identity authentication or get the password back.
Email	Specifies the email address of the user. This email address can be used to receive system notifications.

Parameter	Description
Role	Specifies the role to be assigned to the user. Only one role can be selected for each user. Only the **admin** user can customize roles or edit the permissions granted to default roles. By default, system roles include **DepartmentManager**, **PolicyManager**, **AuditManager**, and **User**. ● **DepartmentManager**: responsible for managing the department system. This role has permissions to configure all modules except the **User** and **Role** 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.
Department	Specifies the department to which the user belongs.
Remarks	(Optional) Provides supplementary information about the user.

4 Step 3: Add Resources to the CBH System

Scenarios

The CBH system allows you to centrally manage cloud resources as well as their accounts and permissions. Before you start, ensure resources are added to the CBH system for centralized O&M management.

A host or application resource may have multiple accounts for login. CBH allows you to log in to managed resources through managed accounts without having to repeatedly enter the usernames and passwords.

The default account for each managed resource is **Empty**. If you use the **Empty** account, enter the account username and password for accessing the host resource.

Prerequisites

- The network between the hosts to be added and the CBH is normal.
- Before adding application resources, you need to add application servers to the CBH system. For details, see **Adding an Application Resource to CBH** or **Importing Application Resources from an Excel File**.

Procedure

Table 4-1 Methods of adding resources

Resource Type	How to Add	Description
Host resources	**Adding a Host Resource**	Add host resources one by one. After you add the basic information of the host resource, add accounts to the host resource. If no account is added, account **Empty** is generated for the host resource by default.

Resource Type	How to Add	Description
	Importing Host Resources from an Excel File	Configure basic information as well as accounts of a host based on the Excel template. If an account is configured for a host resource, the CBH system will no longer generate the **Empty** account for the host resource.
	Importing Host Resources from a Cloud Platform	Select a cloud platform that can communicate with the CBH system and import the basic information and account information of the hosts on the cloud platform into the CBH system. All accounts of the hosts in the cloud platform will be imported into the CBH system. The CBH system will no longer generate the **Empty** account.
	Automatic Host Discovery	The CBH system automatically discovers hosts that can communicate with the CBH system through IP addresses or IP address ranges. In this method, only basic information of discovered hosts is added to the CBH system. You are required to add the accounts to them manually.
Application resources	**Adding An Application Resource to CBH**	Add application resources one by one. After you add the basic information of the application resource, add an account to the application resource. If no account is added, Account **Empty** is generated for the application resource by default.
	Importing Application Resources from an Excel File	Configure basic information as well as accounts of application resources using the Excel template. If an account is configured for an application resource, the CBH system will no longer generate the **Empty** account for the application resource.

Configuration Description

The settings of **Protocol** and **Host Address** must be unique. So, the host resource managed in the CBH system must be unique.

Table 4-2 Basic information about managed host resources

Parameter	Description
Host Name	User-specified name of a host resource. The host name must be unique in the CBH system.
Protocol	Type of the protocol used for the host. In 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.
Host Address	Host IP address that can be used to establish connection with the CBH system. • Select the EIP or private IP address of the host. A Private IP address is recommended. • By default, the IPv4 address of a host is required. • You can enter either an IPv4 address or IPv6 address of a host as long as an IPv6 address is enabled for the host and the IPv6 network interface is enabled in **system configuration** in the CBH system. **NOTE** • CBH manages host resources on the same VPC network. Therefore, private IP addresses are not restricted by external security policies or access control policies based on network stability and proximity. It is recommended that you set the **Host Address** to a private IP address on the same VPC network. • Using an EIP of a host may result in login failure because EIP is an independent public IP address, which may be blocked by the access restrictions on the port.
port	Port number of the managed host.
OS Type	(Optional) Type of the host OS or device OS. • The following OS types are supported by default: 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 Type**.
Terminal Speed	Terminal rate. Different terminal speeds can be selected for Rlogin hosts.
Encode	Code used on the host O&M UI. SSH and Telnet hosts support Chinese code. You can select **UTF-8**, **Big5**, or **GB18030**.

Parameter	Description
Terminal Type	Terminal type for O&M. For O&M of SSH and Telnet hosts, different terminal types are available. You can select **Linux** or **Xterm**.
Options	(Optional) You can select **File Manage**, **Clipboard**, or **X11 forward**. • **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.
Department	Department to which the host belongs.
Label	(Optional) You can customize a label or select an existing one.
Remarks	(Optional) Provides the description of the host.

Table 4-3 Basic information about managed application resources

Parameter	Description
App Name	Name of an application resource. The value of **App Name** must be unique in the CBH system.
AppServer	Select a created application publishing server.
Department	Select the department of the application.
APP Address	(Optional) Enter the address of the application. You can enter 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. • If the application is released as other resource types instead of a database, leave this parameter blank.

Parameter	Description
Param	(Optional) Set application parameters. • If the application is released as a database, enter the database instance name. • If the application is released as other resource types instead of a database, leave this parameter blank.
Options	(Optional) You can select **File Manage** or **Clipboard**.
Label	(Optional) You can customize a label or select an existing one.
Remarks	(Optional) Provides the description of the application.

5 Step 4: Configure O&M Permissions

Scenarios

To use CBH to maintain resources, **configure access control policies**, associate users with resources, and assign resource permissions to CBH system users.

Procedure

Table 5-1 Parameters for configuring ACL rules

Step	Description
New ACL Rule	You can configure the file transfer permission, user login IP address restrictions, user login time restrictions, and policy validity period.
Associate ACL rules with users or user groups.	• Associate a user: Assign the permissions for the **Host Operation** and **App Operation** modules to a system user so that the user can have O&M permissions for resources. • Associate a user group: Assign permissions to all members in the user group in batches. Each user will inherit the permissions granted to the user group when the user is added to the group.
Associate an account or account group with an ACL rule.	• Associate an account: Assign resource access permissions to an account. • Associate an account group: Assign resource access permissions to an account group. Each account will inherit the resource access permissions granted to the account group when the account is added to the group.

Configuration Description

Table 5-2 Basic information about access control policies

Parameter	Description
Rule Name	User-defined name of an ACL rule. The rule name must be unique in the CBH system.
Period of validity	(Optional) Effective time and expiration time of a policy.
File Transmission	(Optional) Permissions to upload and download host 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	(Optional) Permissions to manage host resource files, use RDP clipboards, and displays watermarks during O&M. You can select **File Manage**, **Clipboard**, or **Watermark**. **NOTE** File management is available for the devices using SSH or Remote Desktop Protocol (RDP) protocols. For devices using the Virtual Network Computing (VNC) protocol, file management is available only after the application mapped to this device is released. File management is unavailable for the devices using the Telnet protocol.
Logon Time Limit	(Optional) Time period allowed or forbidden for the user to log in to the host.
IP Limit	(Optional) Restricts or allows users from specified IP addresses to access resources. • Select **Blacklist** and configure the IP addresses or IP address ranges to restrict users from these IP addresses from logging in to the resources. • Select **Whitelist** and configure the IP addresses or IP address ranges 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 resource.

6 Step 5: Log In to a Resource You Want to Manage

Scenarios

After you obtain required permissions, you can log in to a managed resource through the CBH system. The entire O&M process will be monitored and logged.

You can select different login methods based on resource types.

Procedure

Table 6-1 Methods to log in to managed resources

Login Type	Resource Type
Using a Web Browser for Logging In	• Host resources configured with the SSH, RDP, VNC, or Telnet protocol. • All application resources.
Using an SSH Client for Logging In	Host resources configured with the SSH, Telnet, or Rlogin protocol.
Using an FTP/SFTP/SCP Client for Logging In	Host resources configured with any type of transmission protocols. Host resources configured with the FTP or SFTP protocol.
Using an SSO Client for Logging In	Host resources configured with any type of database protocols. • Host resources configured with the MySQL, SQL Server, Oracle, or DB2 protocol.

7 Step 6: Audit O&M Sessions

Scenarios

You can log in to the managed resources, including databases, within the granted permissions for further O&M in the CBH system.

The CBH system makes it easier for the administrators to audit logins, operations on managed resources, and O&M sessions performed by other system users.

Procedure

Table 7-1 Description about the **System** and **Audit** modules

Audit Object	Audit Content
Live Session	Monitor on-going O&M sessions, view the session details of system users and resources, and interrupt sessions with high risks.
History Session	• O&M session videos: The entire process of O&M sessions is automatically recorded by screencasting. You can play the screencasts online or download them. • O&M session details: O&M session details generated for different system users can be viewed online or exported as an Excel file. Session details include detailed operation records of resource sessions, system sessions, O&M records, file transfer, and collaboration sessions.
Operation Report	Display the trend of O&M operations over time in a line chart and generate a comprehensive O&M analysis report. This area includes O&M time distribution, resource access times, session duration, number of access times from source IP addresses, session collaboration, two-person authorization, command interception, number of character commands, and number of transferred files.

Audit Object	Audit Content
System Log	• System login logs: record detailed information about user login to the system. System login logs can be viewed online or exported as Excel files. • System operation logs: record detailed system operations. System operation logs can be viewed online or exported as an Excel file.
System Report	Collect statistics on user logins and system operations in a bar chart and generate a comprehensive system management analysis report. This area includes information about user control, user and resource operations, number of user source IP addresses, user login mode, abnormal login, session control, and user status.