

Cloud Bastion Host (CBH)

FAQs

Issue 05
Date 2025-01-15



Copyright © Huawei Technologies Co., Ltd. 2025. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: <https://www.huawei.com>

Email: support@huawei.com

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:

<https://www.huawei.com/en/psirt/vul-response-process>

For vulnerability information, enterprise customers can visit the following web page:

<https://securitybulletin.huawei.com/enterprise/en/security-advisory>

Contents

1 Product Consulting	1
1.1 What Are the Differences Between a CBH Instance and a CBH System?	1
1.2 Which Security Hardening Measures Does CBH Provide?	1
1.3 What Is the Number of Assets?	2
1.4 What Is the Number of Concurrent Requests?	2
1.5 Does CBH Support IAM Fine-Grained Management?	2
1.6 Can I Use a CBH System to Centrally Manage My Cloud ERP or SAP Services?	3
1.7 What Does Automatic O&M Include?	3
1.8 How Do I Obtain an Enterprise Agreement Number?	4
1.9 How Can I Configure Ports for a Bastion Host?	4
1.10 Can CBH Manage Resources Under Multiple Subnets?	6
1.11 Which Types of Databases Can I Manage in a CBH System?	6
2 Regions and AZs	9
2.1 Can I Use CBH to Manage Resources Under Other Accounts?	9
2.2 Can CBH Manage Hosts in Regions or VPCs Different from that of the CBH Instance?	9
2.3 Can CBH Be Used on DeC?	9
3 About Purchase	11
3.1 About Purchase	11
3.2 What Are the Editions of the CBH Service?	12
3.3 How Do I Configure a Security Group for a CBH Instance?	13
4 License	16
4.1 Does CBH Provide a Third-Party License?	16
4.2 What Can I Do If the CBH System License Is About to Expire or Has Expired?	16
5 About Backup, Specification Change, and Upgrade	18
5.1 Which Types of System Data Can Be Backed Up in the CBH System?	18
5.2 How Do I Back Up Data in a CBH System Before Upgrading the System Version?	21
5.3 Will Audit Data Be Lost If I Change Instance Specifications or Upgrade a CBH Instance?	23
5.4 Why Does FTP/SFTP Remote Backup Fail?	24
5.5 How Do I Import Backup Data to a Primary/Standby CBH Instance?	25
6 About File Transfer	26
6.1 What File Transfer Methods Can be Used in a CBH System?	26

6.2 How Do I Use FTP/SFTP to Transfer Files to or From an SSH Host?.....	27
6.3 How Do I Upload or Download Files When I Log In to Managed Hosts Using a Web Browser?.....	28
6.4 What Is the Netdisk of a CBH System?.....	36
6.5 Why Does File Upload to or Download from a Managed Host Fail?.....	37
6.6 How Do I Clear the Personal Net Disk Space?.....	40
6.7 Why Is File Transfer Not Supported When I Use a Web Browser for Resource O&M?.....	42
6.8 Why Does the File List Cannot Be Loaded After I Click File Transfer When I Log In to CBH Through a Web Browser?.....	43
6.9 How Do I Configure File Management Permissions?.....	43
6.10 Does CBH Check Security of Uploaded Files?.....	44
7 Billing, Renewals, and Unsubcriptions.....	46
7.1 How Do I Renew a CBH Instance and Update the Mapped System Authorization?.....	46
7.2 How Is CBH Billed?.....	47
7.3 Can I Unsubscribe from a CBH Instance?.....	48
7.4 How Is a CBH Instance Billed After I Change Specifications of the Instance?.....	49
7.5 Will I Be Billed for Upgrading the CBH Software Version?.....	49
7.6 How Do I Increase the CBH Instance Quota?.....	49
7.7 How Do I Purchase a CBH Instance When the System Prompts that Resources Are Sold Out?.....	50
8 About CBH System Login.....	52
8.1 Login Methods and Password Issues.....	52
8.1.1 Can I Use a Domain Name to Log In to a CBH System?.....	52
8.1.2 What Login Methods Does CBH Provide?.....	52
8.1.3 Which Login Authentication Methods Are Available in a CBH System?.....	52
8.1.4 What Is the Initial Password for Logging In to a CBH System?.....	55
8.1.5 How Do I Reset the User Password for Logging In to the CBH System?.....	55
8.2 Multifactor Verification.....	58
8.2.1 How Can I Install an OTP Authentication Application on the Mobile Phone?.....	58
8.2.2 Why Does the Mobile OTP Application Binding Operation Fail?.....	58
8.2.3 How Do I Enable Mobile SMS Authentication For Logging In to the CBH System?.....	59
8.2.4 How Do I Cancel Mobile SMS Authentication?.....	60
8.2.5 How Can I Cancel Mobile OTP Authentication If No Mobile OTP Application is Bound to My Account?.....	60
8.2.6 Why Does Login Fail When an Account That Has Mobile OTP Application Bound Is Used to Log In?.....	61
8.3 Login Security Management.....	61
8.3.1 How Do I Set a Security Lock for Logging In to the CBH System?.....	61
8.3.2 How Do I Unlock a User or IP Address Locked During the Login to a CBH Instance?.....	63
9 User, Resource, and Policy Configuration in a CBH System.....	64
9.1 Users.....	64
9.1.1 Why Cannot I Select a Superior Department When Creating a User or Resource?.....	64
9.1.2 How Do I Change a Mobile Number Bound to a CBH System User?.....	64
9.1.3 How Many Users Can Be Created in a CBH System?.....	65

9.2 Adding Resources to a CBH System.....	66
9.2.1 How Can I Start Database Maintenance in a CBH System?.....	66
9.2.2 How Do I Use CBH to Manage RDS Databases?.....	68
9.2.3 How Do I Change the Password of a Managed Resource Account?.....	72
9.2.4 How Do I Set a Sudo Privilege Escalation Account for the Managed Resource?.....	73
9.2.5 How Do I Add a Label to Resources Managed in a CBH System?.....	74
9.2.6 How Do I Import or Export Information of Host Resources in Batches?.....	75
9.2.7 What Are the AK and SK of an Imported Host? How Can I Obtain Them?.....	75
9.2.8 What Are the Statuses of a Managed Resource Account in a CBH System?.....	76
9.2.9 Can I Share Labels of Managed Resources with Other System Users?.....	76
9.2.10 Can I Manually Enter a Password to Log In to a Managed Resource Through the CBH System?.....	77
9.2.11 Why Does the CBH System Fail to Identify Hosts Imported in Batches?.....	77
9.2.12 How Do I Access Services Provided by the Intranet Through a CBH Instance?.....	77
9.3 Policy Management.....	77
9.3.1 What Is Dynamic Approval and How Does It Work?.....	77
9.4 System Configuration.....	78
9.4.1 How Do I Configure an SSH Key for Logging In to a Managed Host?.....	79
9.4.2 How Do I Set the Personal Net Disk Capacity?.....	81
9.4.3 How Do I Send More SMS Messages Than the Limit Allowed by CBH.....	81
9.4.4 How Do I Connect CBH to a Third-Party Email Server?.....	82
10 Resources Managed in a CBH System.....	83
10.1 Operation Management.....	83
10.1.1 Can CBH Support GUI-Based O&M for Linux Hosts?.....	83
10.1.2 Does CBH Support Mobile App O&M?.....	83
10.1.3 How Do I Configure the SSO Tool?.....	84
10.1.4 Does CBH Allow Multiple Users to Log In to the Same Resource Concurrently?.....	84
10.1.5 Which Algorithms Are Supported by CBH in SSH O&M Mode.....	85
10.2 O&M Operations.....	86
10.2.1 What Login Methods Does CBH Provide?.....	86
10.2.2 How Do I Create a Collaborative O&M Session?.....	87
10.2.3 How Do I Use Resource Labels in the CBH System?.....	88
10.2.4 How Do I Set the Resolution of the O&M Session Window When I Use a Web Browser for O&M?	89
10.2.5 How Can I Use Shortcut Keys to Copy and Paste Text When a Web Browser Is Used for O&M?.....	90
10.2.6 What Are the Shortcut Keys for O&M in CBH?.....	91
10.2.7 Why Is the File List Not Displayed During O&M Using a Web Browser?.....	92
11 O&M Log Audit.....	93
11.1 What Audit Logs Does CBH Provide?.....	93
11.2 Can I Download Operation Recordings?.....	94
11.3 Can I Delete CBH O&M Data for a Specific Day?.....	95
11.4 Can I Back Up System Audit Logs to an OBS Bucket?.....	95
11.5 How Long Can I Store Audit Logs in the CBH System?.....	95

11.6 How Are Audit Logs in the CBH System Processed?.....	96
11.7 Why Is the Playable Duration Shorter Than the Total Duration of a Session?.....	96
11.8 Why Is There No Login Record in History Sessions While I Received a Resource Login Message?.....	97
12 Troubleshooting.....	98
12.1 CBH System Login Failures.....	98
12.1.1 How Do I Handle Login Exceptions?.....	98
12.1.2 Why Is the IP Address or MAC Address Blocked When I Log In to the CBH System?.....	100
12.1.3 Why Am I Seeing Error Code 404 When I Log In to the CBH System?.....	100
12.1.4 Why Am I Seeing Error Code 499 When I Log In to the CBH System?.....	101
12.1.5 What Are Possible Faults If I Log In to the CBH System as an Intranet User?.....	101
12.1.6 Why Is a Host Inaccessible Through CBH?.....	102
12.1.7 Why Does CBH Login Fail Through an ECS in a New VPC Connected with the VPC Where CBH Is via VPN or a VPC Peering Connection.....	102
12.2 CBH Managed Resource Login Failures.....	103
12.2.1 Why Does an Exception Occur When I Log In to My Resources Managed in CBH?.....	103
12.2.2 Why Am I Seeing Login Errors of Code: T_514 When I Use a Web Browser for Resource O&M?...	104
12.2.3 Why Am I Seeing Login Errors of Code: T_1006 When I Use a Web Browser for Resource O&M?.	107
12.2.4 Why Am I Seeing Login Errors of Code: C_515 When I Use a Web Browser for Resource O&M?...	108
12.2.5 Why Am I Seeing Login Errors of Code: C_519 When I Use a Web Browser for Resource O&M?...	110
12.2.6 Why Am I Seeing Login Errors of Code: C_769 When I Use a Web Browser for Resource O&M?...	112
12.2.7 Why Cannot I See the Accessible Resources in the Resource List?.....	114
12.2.8 Why Does the Session Page Fail to Load When I Log In to the Managed Host Using a Web Browser?.....	115
12.2.9 Why Is the Application Resource Inaccessible through CBH?.....	116
12.2.10 Why Are Databases Managed in CBH Inaccessible with an SSO Tool?.....	117
12.2.11 Why Does the Number of Concurrent Sessions Reach the Limit When I Use CBH to Log In to a Host Resource?.....	118
12.2.12 Why a Black Block Is Displayed on the Mouse When the MSTSC Client Is Used to Access a Server Resource?.....	118
12.2.13 Why Am I Seeing User Creation Failure Message When Accessing a Windows Application Publishing Server?.....	119
12.3 Maintenance Issues.....	119
12.3.1 Why Does SMS Verification Code Fail to Send When I Log In to a CBH Instance?.....	119
12.3.2 Why Am I Seeing a Message Indicating that the Number of Resources Has Reached the Limit When I Add a Resource to CBH?	121
12.3.3 Why Does Verification of An Account for a Managed Host Fail?.....	121
12.3.4 Why Am I Seeing Garbled Characters When I Open a System Data File?.....	122
12.3.5 Why Does Login Timeout Frequently Occur During an O&M Session?.....	122
12.3.6 Why Does the PL/SQL Client Display Garbled Characters During Application O&M?.....	123
12.3.7 Why Is the Requested Session Denied After I Log In to a Managed Host?.....	123
12.3.8 Why Does the CBH Traffic Bandwidth Exceed the Threshold?.....	124
12.3.9 Why Text Cannot Be Copied When I Perform O&M Through a Web Browser?.....	124
12.3.10 Which Types of Failures May Occur During the O&M?.....	125

12.3.11 What Do I Do If an Exception Occurs When I Enter Chinese Characters Using WPS During the O&M of a Windows Server?.....	130
12.3.12 I Mapped My CBH Instance IP Address to a Domain Name, and Added the Domain Name to WAF. Why Does the Domain Name Become Inaccessible?.....	130
12.3.13 Why Is LTS Still Disabled After It Is Configured for a CBH Instance?.....	131
12.3.14 Why My Certificate Becomes Abnormal After a Cross-Version Upgrade?.....	131
12.4 SSO O&M Faults.....	132
12.4.1 Configuring a Customized Driver for DBeaver to Connect to GaussDB Databases.....	132
12.4.2 Configuring the Connection Between DBeaver and GaussDB.....	134
12.4.3 Message "1251-lost connection to mysql server during query" Displayed While Backing Up MySQL Database Tables.....	134
12.4.4 Message "1251-Client does not support authentication protocol requested by server" Reported While Managing MySQL Database Through Host Operation.....	135
12.4.5 Error Message "2013-Lost connection to MySQL server at waiting for initial communication packet', system error:0" Reported While Connecting to MySQL Databases.....	135
12.4.6 Error Message "ORA-12537_TNS_Connection closed" Reported While Connecting to Oracle Databases.....	136
12.4.7 Error Message "ORA-12637_Packet Receive Failed" Reported While Connecting to Oracle Databases.....	136
12.4.8 Error Message "ORA 12170 TNS Connect Timeout" Reported While Connecting Oracle Databases through Host Operation in the Bastion Host.....	138
12.4.9 Failed to Establish a Connection between DBeaver and PostgreSQL Databases.....	139
12.4.10 SSO Failed as JRE Is Missing in the Running Environment.....	139

1 Product Consulting

1.1 What Are the Differences Between a CBH Instance and a CBH System?

A CBH instance maps to an independently running CBH system.

To purchase and manage CBH instances, log in to the management console and choose **Security & Compliance > Cloud Bastion Host**.

A CBH system that is mapped to a CBH instance is the core component for secure O&M. A CBH system uses the EulerOS operating system and provides a wide range of functional modules, including user management, resource management, policy, audit, and ticket modules. After you log in to a CBH system, you can perform security management and control protection for your Windows and Linux hosts managed in this system.

1.2 Which Security Hardening Measures Does CBH Provide?

CBH has a complete security lifecycle management, covering security coding specifications during system development, security tests such as strict security vulnerability scanning and penetration testing, and security supervision by public security departments. It complies with laws and regulations such as the *Cyber Security Law*, meets compliance review requirements, and earns the classified information security level 3 certification.

System Data Security

- Login security: Image encryption, SSH remote login security hardening, kernel parameter security hardening, strong passwords for system accounts, and lockout of login after three consecutive login failures
- Data security: Encrypted sensitive information and independently and dynamically generated system root key
- Application security: Protection from SQL injection attacks, CSV injection attacks, and XSS attacks, and API authentication mechanism

System Security

- Automatic system installation and Linux Unified Key Setup (LUKS) disk encryption
- Built-in firewall function to prevent common network attacks, such as brute force cracking
- Unified HTML5 access APIs with only one system web access port opened to reduce the attack surface
- SSH login hardening parameters to improve security of SSH login systems

1.3 What Is the Number of Assets?

Assets are resources managed with a CBH system. The number of resources is the number of protocols you configure for and applications run on each cloud server managed with a CBH system. You can view the number of different types of assets on the [Dashboard](#).

The total number of resources managed in a CBH system cannot exceed the number of assets allowed by the CBH edition you are using.

The number of assets is calculated based on the number of resources on the managed hosts instead of the number of managed hosts. A host may have multiple types of resources, including different protocols and applications running on the host.

For example, after a host is added to a CBH system, if two RDP, one Telnet, and one MySQL host resources and one Google Chrome browser application resource are added, the number of managed assets is 5 instead of 1.

1.4 What Is the Number of Concurrent Requests?

The number of concurrent requests indicates the number of connections established between managed resources and a CBH system over all protocols at the same time.

The CBH system does not limit the number of system users. You can create as many users as you need. However, the total number of protocol connections of different users at the same time cannot exceed the maximum number of concurrent requests supported by the current CBH edition.

For example, if 10 O&M engineers use a CBH system at the same time and each engineer generates five protocol connections (such as remote connections through SSH or MYSQL client), the number of concurrent requests is 50.

1.5 Does CBH Support IAM Fine-Grained Management?

Yes.

Identity and Access Management (IAM) is a basic service for permission management. By default, new IAM users do not have any permissions. You need to grant different permissions to IAM users based on their duties. IAM fine-grained permission management has been enabled for the CBH service. With IAM

permission management, you can perform fine-grained authorization for key operations, such as purchasing, upgrading, and changing specification of CBH instances.

You can configure user login restrictions and access control policies based on user duties in the CBH system to manage user access and O&M operations in a fine-grained manner. However, this function is a permission management function of the CBH system, not offered by the IAM service.

1.6 Can I Use a CBH System to Centrally Manage My Cloud ERP or SAP Services?

Yes.

CBH allows you to install application publishing servers and use the remote desktop service of the Windows system to access applications, databases, or web pages of typical ERP and SAP systems, such as ERP production systems, ERP DR systems, SAP production systems, SAP development/test systems, SAP Router, and SAP Hybris. In this way, your ERP and SAP cloud services are audited and recorded as web pages or applications in a CBH system. Be sure the network between your service system and the CBH system is well connected.

1.7 What Does Automatic O&M Include?

CBH professional editions support automatic O&M, making complex O&M precise and efficient. Automatic O&M includes account synchronization, online script management, fast O&M of multiple resources, and multi-step automatic O&M.

- **Account synchronization:** You can effectively monitor accounts on hosts, detect zombie accounts or unmanaged accounts in a timely manner, and enhance asset management and control.
For details, see [Account Synchronization Rules](#).
- **Online script management:** You can import or edit scripts online to centrally manage and run scripts in the CBH system. Python and Shell script formats are supported.
- **Fast O&M of multiple resources:** Commands or scripts can be quickly executed on multiple resources through the SSH protocol. The execution results are returned based on the initiated commands and scripts. In addition, one or more files can be uploaded to multiple resources and the upload result can be returned.
- **Multi-step automatic O&M:** Multiple O&M operations can be performed step by step on multiple resources concurrently through the SSH protocol. The O&M operations include command execution, script execution, and file transfer. After an O&M task is submitted, the system automatically performs operations in sequence and returns the execution result.

1.8 How Do I Obtain an Enterprise Agreement Number?

You need to enter the enterprise agreement number for authorization when configuring the remote desktop service during creation of an application publishing server. The enterprise agreement number is not a free suite.

You need to apply for or buy the enterprise agreement number at your cost. The application publishing server is a third-party management plug-in. CBH does not provide an enterprise agreement number. For example, when you apply for or buy a Windows OS, the Office suite is not free and you need to buy it at additional cost.

1.9 How Can I Configure Ports for a Bastion Host?

To properly use a bastion host, configure the instance and resource security group ports by referring to [Table 1-1](#).

CAUTION

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

Table 1-1 Inbound and outbound rule configuration reference

Scenario Description	Direction	Protocol/ Application	Port
Accessing a bastion host through a web browser (HTTP and HTTPS)	Inbound	TCP	80, 443, and 8080
Accessing a bastion host through Microsoft Terminal Services Client (MSTSC)	Inbound	TCP	53389
Accessing a bastion host through an SSH client	Inbound	TCP	2222
Accessing a bastion host through FTP clients	Inbound	TCP	20~21
Remotely accessing Linux ECSs of a bastion host over SSH clients	Outbound	TCP	22

Scenario Description	Direction	Protocol/ Application	Port
Remotely accessing Windows ECSs of a bastion host over the RDP Protocol	Outbound	TCP	3389
Accessing Oracle databases through a bastion host	Inbound	TCP	1521
Accessing Oracle databases through a bastion host	Outbound	TCP	1521
Accessing MySQL databases through a bastion host	Inbound	TCP	33306
Accessing MySQL databases through a bastion host	Outbound	TCP	3306
Accessing SQL Server databases through a bastion host	Inbound	TCP	1433
Accessing SQL Server databases through a bastion host	Outbound	TCP	1433
Accessing DB databases through a bastion host	Inbound	TCP	50000
Accessing DB databases through a bastion host	Outbound	TCP	50000
Accessing GaussDB databases through a bastion host	Inbound	TCP	18000
Accessing GaussDB databases through a bastion host	Outbound	TCP	18000
License servers	Outbound	TCP	9443
Cloud services	Outbound	TCP	443
Accessing a bastion host system through the SSH client in the same security group	Outbound	TCP	2222
SMS service	Outbound	TCP	10743 and 443
Domain name resolution service	Outbound	UDP	53
Accessing PGSQL databases through a bastion host	Inbound	TCP	15432
Accessing PGSQL databases through a bastion host	Outbound	TCP	5432

1.10 Can CBH Manage Resources Under Multiple Subnets?

Yes.

If your CBH instance and the resources you want to manage with CBH are in the same VPC, the CBH system can directly manage resources in multiple subnets in the VPC as subnets in the same VPC can communicate with each other.

Therefore, a CBH instance and the host resources you want to manage with CBH must be in the same VPC in the same region. If your CBH instance and the resources you want to manage with CBH are in two subnets in different VPCs, a cross-VPC connection must be established to enable communications between the two subnets as subnets in different VPCs cannot directly communicate with each other. While this method is not recommended as cross-VPC connections are not stable enough.

1.11 Which Types of Databases Can I Manage in a CBH System?

In CBH, you can manage a variety of databases in the **host O&M** module (**Host Operation**) or **application O&M** module (**Application Operation**). In the host operation module, you can audit database operations, such as adding, deleting, modifying, and querying database operations. In the application operation module, you can audit operation sessions through videos.

NOTE

- In CBH standard editions, directly managing databases is not available. To manage databases, an application publish server must be set up.
- In CBH professional editions, directly managing databases is available in the host operation and application operation modules.

Managing Databases in the Host Operation Module

In the **Host Operation** module, you can manage MySQL, SQL Server, Oracle, DB2, PostgreSQL, and GaussDB databases. For the database types, versions, and client software versions supported by CBH, see **Table 1-2**.

Table 1-2 Supported database types, versions, and clients

Database Type	Version	Supported Client
MySQL	MySQL 5.5, 5.6, 5.7, and 8.0	Navicat 11, 12, 15, and 16 MySQL Administrator 1.2.17 MySQL CMD DBeaver 22 and 23 (supported by CBH V3.3.48.0 and later versions)

Database Type	Version	Supported Client
Microsoft SQL Server	2014, 2016, 2017, 2019, and 2022	Navicat 11, 12, 15, and 16 SQL Server Management Studio (SSMS) 17.6
Oracle	10g, 11g, 12c, 19c, and 21c	Toad for Oracle 11.0, 12.1, 12.8, and 13.2 Navicat 11, 12, 15, and 16 PL/SQL Developer 11.0.5.1790 DBeaver 22 and 23 (supported by CBH V3.3.48.0 and later versions)
DB2	DB2 Express-C	DB2 CMD command line 11.1.0
PostgreSQL	11, 12, 13, 14, and 15	DBeaver 22 and 23
GaussDB	2 and 3	DBeaver 22 and 23

Managing Databases in the App Operation Module

You can use CBH to manage following versions of databases in the application O&M module:

- Windows Server 2008 R2 or later

You need to deploy the database client on a Windows operating system that supports remote desktop. Then, you can use a web browser to remotely log in to the Windows desktop through CBH, invoke the database client, and implement O&M on database applications.

Table 1-3 lists the database clients that are deployed on Windows servers and can be directly configured and called by CBH. If you want to manage other types of database applications on Windows servers, set the application server type to **Other**.

Table 1-3 Supported Windows database clients

Application Type	Supported Client
MySQL Tool	MySQL Administrator
Oracle Tool	PL/SQL Developer
SQL Server Tool	SSMS
dbisql	dbisql
PostgreSQL	Navicat for PostgreSQL

- For Linux servers, only database applications running on Linux CentOS 7.9 servers can be managed.

 **CAUTION**

Linux servers support only Dameng database V8 applications.

Table 1-4 lists the database clients that are deployed on Linux servers and can be directly configured and called by CBH.

Table 1-4 Supported Linux database clients

Application Type	Supported Client
Dameng Database	Dameng management tool V8

2 Regions and AZs

2.1 Can I Use CBH to Manage Resources Under Other Accounts?

Yes.

CBH can directly manage resources in the same VPC as that of the CBH instance. You can establish a [VPC peering connection](#) to enable communication between two VPCs of different accounts.

But, using CBH across different accounts is unstable as network connection across VPCs may be unstable in some cases.

2.2 Can CBH Manage Hosts in Regions or VPCs Different from that of the CBH Instance?

Yes.

CBH can only directly manage resources in the same VPC as that of the CBH instance.

Although you can establish cross-region or cross-VPC network connections between a CBH instance and resources, such connections may be not stable enough for using the CBH system. If you really need to use CBH for cross-VPC or cross-region resource management, you can:

- Use a [VPC peering connection](#) to connect two VPCs.
- Use a [Cloud Connect \(CC\)](#), [Virtual Private Network \(VPN\)](#), or the like, to establish a cross-region network connection.
- Direct Connect does not support dual-stack networks, and virtual IP addresses cannot be connected.

2.3 Can CBH Be Used on DeC?

Yes.

Dedicated Cloud (DeC) is an integrated solution that provides computing, storage resource pools, networks, and multi-level control and isolation for enterprises, governments, and finance customers. DeC provides physically isolated resource pools on the cloud for exclusive use of each customer, meeting requirements for specific performance, business applications, and security compliance.

3 About Purchase

3.1 About Purchase

Can I Scale Down CBH Specification When I Make a Purchase?

Rollback or scale-down of CBH instance specifications is not supported.

For details, see [Changing Specifications of a CBH Instance](#).

How Do I Select a Region and AZ for a CBH Instance?

A region is a geographic area. Multiple data centers are required across regions to provide large bandwidth. Different regions are available for a service. It is recommended that you select the region nearest to your end users.

CBH allows you to directly manage resources in the same VPC and region. Resources in the same VPC and region can directly communicate with each other.

VPCs in different regions or different VPCs in the same region cannot communicate with each other through the intranet. Therefore, when purchasing a CBH instance, you are advised to configure the CBH instances and related resources such as ECSs in the same VPC and region. In addition, you are advised to select the same region and AZ as those of the selected VPC when configuring the AZ for the instance to reduce network latency.

If you cannot select an AZ when purchasing a CBH instance, you can select another AZ in the same region. For example, if AZ1 in the **CN-Hong Kong** region is not available, you can select AZ2 in the **CN-Hong Kong** region.

Can I Change the Security Group After a CBH Instance Is Created?

No. To modify VPC configurations, unsubscribe from the CBH instance and buy another one.

Can I Change the VPC and Its CIDR Blocks After a CBH Instance Is Created?

No. To modify VPC configurations, unsubscribe from the CBH instance and buy another one.

Can I Delete the admin Account After a CBH Instance Is Created?

User **admin** is the CBH system administrator and has the highest operation permissions so it cannot be deleted.

- However, the admin account can be locked out. For details, see [How Do I Set a Security Lock for Logging In to the CBH System?](#)

3.2 What Are the Editions of the CBH Service?

Currently, CBH provides standard and professional editions. The standard edition provides the following asset specifications: 50, 100, 200, 500, 1,000, 2,000, 5,000, and 10,000. The professional edition provides the following asset specifications: 100, 200, 500, 1,000, 2,000, 5,000, and 10,000.

NOTE

- CBH does not support the customization of asset specifications. You can only select the default specifications in a certain edition.
- If you have purchased the CBH instances of history editions, you can continue to use them.

CBH Instance Editions

Table 3-1 Functions of different editions

Edition	Description
Standard edition	Basic functions: identity authentication, permission control, account management, and security audit
Professional edition	Basic functions: identity authentication, permission control, account management, and security audit Enhanced functions: cloud service O&M, automated O&M, and database O&M audits

Table 3-2 Configuration of different specifications

Asset Quantity	Max. Concurrent Connections	CPUs	Memory	System Disk	Data Disk
10	10	4 cores	8 GB	100 GB	200 GB
20	20	4 cores	8 GB	100 GB	200 GB
50	50	4 cores	8 GB	100 GB	500 GB
100	100	4 cores	8 GB	100 GB	1000 GB
200	200	4 cores	8 GB	100 GB	1000 GB

Asset Quantity	Max. Concurrent Connections	CPUs	Memory	System Disk	Data Disk
500	500	8 cores	16 GB	100 GB	2,000 GB
1,000	1,000	8 cores	16 GB	100 GB	2,000 GB
2,000	1,500	8 cores	16 GB	100 GB	2,000 GB
5,000	2,000	16 cores	32 GB	100 GB	3,000 GB
10,000	2,000	16 cores	32 GB	100 GB	4,000 GB

NOTICE

The number of concurrent connections in [Table 3-2](#) includes only connections established by O&M clients that use character-based protocols (such as SSH or MySQL client). Connections established by O&M clients that use graphic-based protocols (such as H5 web and RDP client) is not included, which is only one-third of this number.

3.3 How Do I Configure a Security Group for a CBH Instance?

Background

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

To ensure CBH instance security and reliability, configure security group rules to allow specific IP addresses and ports to access the resources.

- A CBH instance and its managed resources can share the same security group and use their own security group rules.
- The default security group **Sys-default** is created for each user. You can select **Sys-default** and add security group rules as needed. Alternatively, you can create another security group and add security group rules to meet your business needs.
- After a CBH instance is created, its security groups can be modified. You can configure up to five security group rules for it. For details, see [Changing Security Groups](#).
- For CBH to access resources it manages, configure the security group rules for resources such as ECSs and RDS DB instances to enable the necessary gateway IP address and port and allow the private IP address of CBH. For details, see [ECS Security Group Configuration](#).

- The CBH instance is running properly. For details about how to configure the instance and resource security group ports, see [How Can I Configure Ports for a Bastion Host?](#)

Configuring a Security Group for a CBH Instance

Step 1 Log in to the management console and switch to the CBH console.

Step 2 Click **Purchase CBH Instance** to go to the **Purchase CBH Instance** page.

Step 3 Click **Manage Security Groups** on the right of **Security Group**. On the displayed page, create a security group and add security group rules.

NOTE

You can also select a security group from the **Security Group** drop-down list.

Step 4 On the displayed page, click **Create Security Group** and create a security group. For details, see [Creating a Security Group](#).

Step 5 After the security group is created, on the displayed **Security Groups** page, locate the row where the created security group resides and click **Manage Rule** in the **Operation** column. For details, see [Adding a Security Group Rule](#).

Step 6 On the displayed page, select the **Inbound Rules** tab, and then click **Add Rule**. Similarly, you can add outbound rules.

Configure security rules based on the networking scenario of CBH. For details, see [Table 1-1](#).

Step 7 After the security group rules are configured, return to the **Purchase CBH Instance** page, select a security group, and specify other required parameters.

----End

Faults Caused by Improper Security Group Configurations

Improper security group configurations can lead to the following faults:

1. Instance license authentication failure
 - The instance fails to be created, and a message is displayed indicating that the license fails to be activated. The possible cause is that the outbound TCP port 9443 is not configured. As a result, the network is disconnected and the license authentication cannot be obtained.
 - When a user logs in to a CBH instance, the system displays a message indicating that the license has expired. This is because the outbound TCP port 9443 is not configured. As a result, the network is disconnected and the license authentication cannot be obtained.
2. CBH system login failure
 - The CBH login page fails to be loaded, and a message is displayed indicating that the server response time is too long. The possible cause is that the inbound TCP port 443 is not enabled.
 - The CBH system page cannot be displayed properly. The possible cause is that the inbound TCP port 443 is not enabled. As a result, the CBH system cannot be logged in to through a web browser.

3. Host verification failure
 - The system displays a message indicating that the host is unreachable when a host resource is added in to the CBH system. The possible cause is that the inbound TCP port 3389 is not enabled. As a result, the host cannot be remotely connected.
 - The system displays a message indicating that the host is unreachable during the account and password verification. The possible cause is that the inbound Internet Control Message Protocol (ICMP) is not configured. As a result, the host cannot be pinged from the external network.
4. Errors in Accessing Resources from CBH
 - A connection failure occurs during login. The possible cause is that the inbound TCP port 3389 is not configured. As a result, the host cannot be remotely connected.
 - A black screen is displayed during host login. The possible cause is that the inbound TCP port 3389 is not configured. As a result, the host cannot be remotely connected.
 - If error T_514 is reported when a CBH instance is running, TCP port **2222** may not be enabled in the inbound rules. Error 514 indicates that the connection is disconnected because the server does not respond for a long time and the system asks you to check your network connection and try again.

4 License

4.1 Does CBH Provide a Third-Party License?

No.

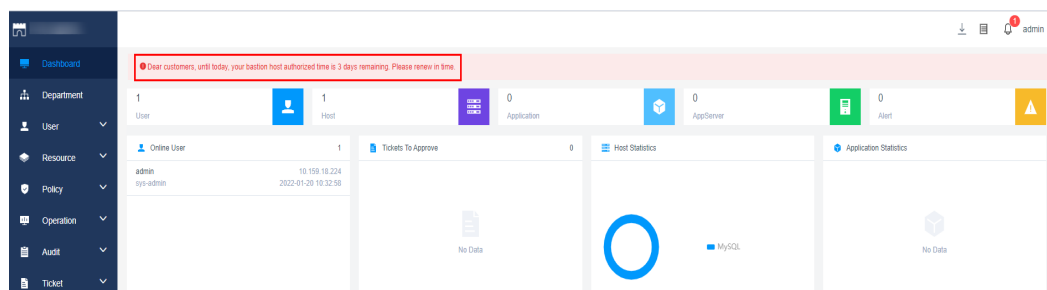
CBH provides functions related to third-party plug-ins such as Navicat but not provides license for them. For example, if you use third-party plug-in Navicat to manage assets such as databases, you need to contact Navicat to apply for a license.

4.2 What Can I Do If the CBH System License Is About to Expire or Has Expired?

If a CBH instance is about to expire or has expired, renew the instance on the console first. Then, update the license file with the one you obtain after the renewal.

Symptom

Symptom 1: The CBH instance is about to expire.



Symptom 2: The CBH instance has expired.

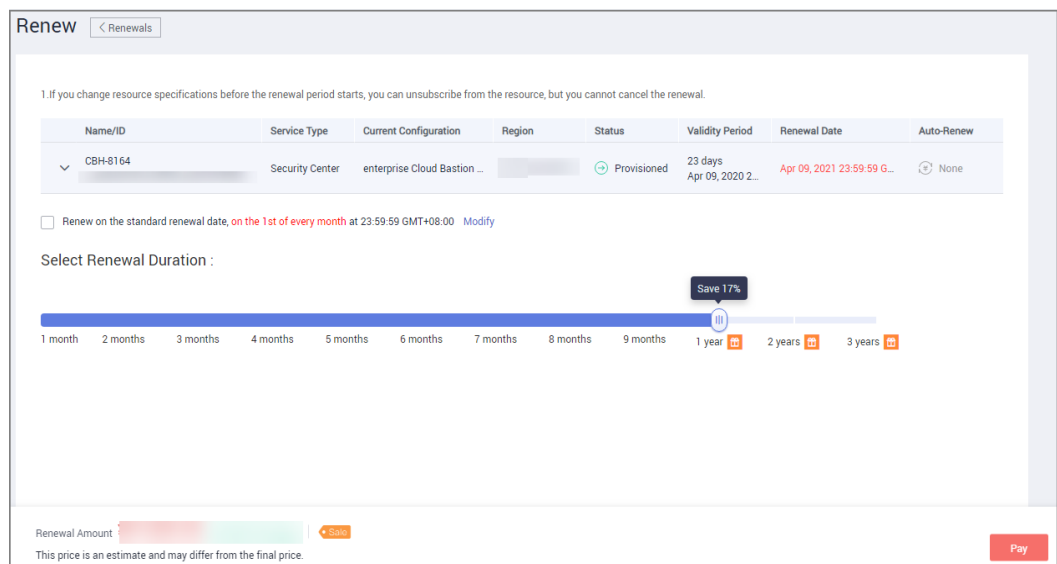
Prerequisites

- You have the CBH operation permissions.
- Access to port 9443 is allowed by the firewall rules and in the outbound direction of the security group to which your CBH instance belongs. Otherwise, the renewal may fail.
- If your CBH instance version is V3.3.2.0 or earlier, [bind an EIP to the CBH instance](#). Otherwise, the renewal may fail.

Procedure

- Step 1** Log in to the management console.
- Step 2** Choose **Security & Compliance > Cloud Bastion Host**.
- Step 3** Click the instance to be renewed and choose **More > Renew** in the **Operation** column to go to the page for renewal.
- Step 4** Select the renewal duration as needed.

Figure 4-1 Renewal configuration



- Step 5** Click **Pay** and complete the payment.
- Step 6** Return to the CBH instance list page and check the latest expiration time in the **Billing Mode** column. You can log in to the CBH system in about 5 minutes.

NOTE

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

----End

5 About Backup, Specification Change, and Upgrade

5.1 Which Types of System Data Can Be Backed Up in the CBH System?

CBH supports manual backup and automated backup to enhance audit data security, system scalability, and data discovery management. For details, see [Manual Backup](#) and [Automated Backup](#).

Before upgrading the system version, back up data in the CBH system by referring to [How Do I Back Up Data in a CBH System Before Upgrading the System Version?](#)

Manual Backup

You can manually export or download data files of each functional module to a local computer. For details about how to manually back up logs, see [Table 5-1](#).

NOTE

Garbled characters may be displayed when a CSV file exported from the system is opened using Excel. If garbled characters are displayed, change the file encoding format and open the file again. For details, see [Why Are Garbled Characters Displayed When I Open a CBH Data File in Excel?](#)

Table 5-1 Data that can be exported or downloaded

Data	Export	Download	Format	Description
User information	Supported	-	CSV	User passwords, mobile numbers, and email addresses cannot be exported.

Data	Export	Download	Format	Description
One-time Passwords (OTPs)	Supported	-	CSV	-
Hosts	Supported	-	CSV	-
Application publishing servers	Supported	-	CSV	-
Application publishing	Supported	-	CSV	-
Accounts	Supported	-	CSV	-
ACL Rules	Supported	-	CSV	-
Password Change Rules	-	Supported	CSV	After the password is verified, you can download the execution logs of a single password change rule.
Account synchronization rules	-	Supported	CSV	CBH professional editions allow you to download the execution logs of a single account synchronization rule.
Fast O&M	Supported	-	CSV	CBH professional editions allow you to export a single fast O&M execution log.
O&M tasks	Supported	-	CSV	CBH professional editions allow you to export a single O&M task execution log.
History sessions	Supported	Supported	CSV or MP4	You can export multiple historical sessions and generate and download a video of a single session.
System logs	Supported	-	CSV	-

Data	Export	Download	Format	Description
O&M reports	Supported	-	PDF, DOC, XLS, or HTML	O&M reports can be exported in text format.
System reports	Supported	-	PDF, DOC, XLS, or HTML	System reports can be exported in text format. System permission configuration reports cannot be exported.
System configuration	-	Supported	bak	<ul style="list-style-type: none"> You can back up and restore the current system configuration. The downloaded backup file can be used only to restore the current system configuration. System permission configuration data cannot be exported. Automatic backup is supported. The system configuration of the previous day is backed up at 00:00 every day.

Automated Backup

You can also configure log backup. After log backup is configured, you can compress login and key operation logs into .tar files and remotely back up the files to the Syslog, FTP, or SFTP server or to an OBS bucket. For details, see table "Data that supports backup configuration".

Table 5-2 Data that supports backup configuration

Backup Method	Data	Description
Local download and backup	System login logs, resource login logs, command operation logs, file operation logs, and two-person authorization logs	You can select a time range to back up logs and download the logs to a local computer.

Backup Method	Data	Description
Remote backup to the Syslog server	System login logs, resource login logs, command operation logs, file operation logs, and two-person authorization logs	After the Syslog server is configured successfully, all historical logs are backed up remotely. When a new log is recorded, the backup is triggered in real time.
Remote backup to the FTP or SFTP server	System configuration and session playback logs	<ul style="list-style-type: none"> After the FTP or SFTP server is successfully configured, log data of the previous day is backed up at 00:00 every day. In addition, you can select a date to back up data to the server immediately.
Remote backup to an OBS bucket	System configuration and session playback logs	<ul style="list-style-type: none"> After the remote backup to an OBS bucket is enabled, logs of the previous day are backed up at 00:00 every day. In addition, you can select a date to back up data to the OBS bucket immediately.

5.2 How Do I Back Up Data in a CBH System Before Upgrading the System Version?

If a new version of the CBH system is available, upgrade your CBH system to use the optimized or new system functions. For details, see [Upgrading the Version of a CBH System](#).

Data to Be Backed Up

You need to manually back up the system data before the upgrade and import the backup data after the upgrade to reuse the data in the new CBH system.

You need to export or import data based on the data type to back up all data.

Table 5-3 Data to be backed up before the upgrade


Data Source	Export	Import	Description
User information	√	√	User passwords cannot be exported. After the upgrade is complete, you can reset the user password.

Data Source	Export	Import	Description
Accounts	√	√	To prevent account information loss, you are advised to back up and restore account files separately.
Audit data	√	×	You need to back up all audit data, including history sessions, session videos, system login logs, system operation logs, O&M reports, and system reports, because audit data cannot be imported to the new CBH system. <ul style="list-style-type: none"> • Operation and maintenance reports and system reports can be exported in text format. • History session videos can be exported in MP4 format.
System configuration	√	√	The system configuration information includes all system configuration data.

Backup Operation Example

As an example, the following operations describe how to back up managed account data.

Step 1 Log in to the management console.

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

Step 3 In the row containing the instance you want to perform a backup, click **Login** in the **Operation** column to log in to the CBH system.

Step 4 Export the system data before the upgrade.

On the **Account** page, click **Export** to export all user information to an Excel file.

NOTE

- If you select specific data and click **Export**, the specified data is exported. If no account is not selected, all data is exported.
- When you export information about a host, all information about the host and its managed accounts will be exported together.
- When you export information about an application, all information about the application and its managed accounts will be exported together.

Step 5 Upgrade the CBH edition.

Step 6 Compare the Excel template.

Log in to the new CBH system. On the **Account** page, click **Import**. On the displayed page, click **Download** to download the Excel template of the new CBH system.

Compare the Excel files before and after the upgrade and check whether they are consistent. If they are inconsistent, modify the Excel file exported before the upgrade.

Step 7 Import the modified Excel file.

On the **Account** page, click **Import**. On the **Import** page, click **Upload** to import the modified Excel file to the new CBH system.

 **NOTE**

- If the **Department** information has been configured in the system before the upgrade, configure the same department structure in the new system before importing the data.
- To restore the system configuration, you can directly upload the original system backup file without having to modify the system configuration file.

Step 8 Refresh the **Account** page and view the information about the imported data.

----End

5.3 Will Audit Data Be Lost If I Change Instance Specifications or Upgrade a CBH Instance?

In normal cases, the audit data will not be lost when you change specifications of a CBH instance or upgrade the system of a CBH system.

Back up data before changing specifications of a CBH instance or upgrading a CBH instance to prevent data loss in case such operations fail.

Precautions for Changing Specifications

- Before specifications change
Data must be backed up before you change CBH specifications. For details, see [How Do I Back Up Data in a CBH System Before Upgrading the System Version?](#)
Ensure that the current CBH system is version 3.2.16.0 or later if you want to change specifications to professional editions. Otherwise, the enhanced functions remain unavailable after specification change. If the CBH system version is earlier than 3.2.16.0, [upgrade the system version](#) first. For details about how to view the CBH system version, see [About System](#).
- During specification change
It takes about 30 minutes for the instance specifications to be changed. During this period, the CBH system is unavailable, but services running on the managed hosts are not affected. To avoid data loss, do not log in to the CBH instance for any operations during this period.
- After specification change
Only the data disk specifications are changed. The system disk specifications are not affected. The CBH system changes the CPU, memory, and bandwidth for you, which does not affect the use of the original EIP.

Precautions for Upgrading CBH

- Before the upgrade
Back up CBH system data to prevent the upgrade failure from affecting services.
- During the upgrade
The version upgrade takes about 30 minutes. Although the CBH system is unavailable during this period, there is no impacts on host resources managed on the instance. However, to prevent important data loss, you are not advised to log in to the CBH system during the version upgrade.
- After the upgrade
The CBH instance automatically restarts after the upgrade completes. You can then use the mapped CBH system.
After the upgrade, you can use the configuration and storage data of the original CBH system. Version upgrading does not affect the original configuration and storage data of the CBH system.

Helpful Links

- [Which Types of System Data Can Be Backed Up in the CBH System?](#)
- [How Do I Back Up Data in a CBH System Before Upgrading the System Version?](#)

5.4 Why Does FTP/SFTP Remote Backup Fail?

Symptoms

- FTP/SFTP remote backup is configured in the CBH system. An error message is displayed, indicating that the server password or network connection is incorrect and the remote backup cannot be started.
- When you back up logs of a specific day, the system displays a message indicating that the backup is being performed, but the remote server does not receive the backup file.

Possible Causes

Cause 1: The username or password configured in the CBH system for logging in to the FTP/SFTP server is incorrect.

Cause 2: The network connection between the CBH system and the FTP/SFTP server is interrupted.

Cause 3: The FTP/SFTP server restricts user directory upload.

Cause 4: A large number of O&M logs are generated on that specific day. The backup transmission rate is low and the backup takes a long time to complete. As a result, backup files cannot be displayed on the remote server immediately.

Solutions

Solution to cause 1

- Log in to the ECS management console, log in to a Linux host using VNC, log in to the FTP/SFTP server from the Linux host, and verify the server username and password. After verifying the username and password, reconfigure the remote backup username and password of the FTP/SFTP server and try to back up data.

Solution to cause 2

- Log in to the CBH system and check the network connection between the CBH system and the FTP/SFTP server by network diagnosis.
 - If the network connection is normal, check other possible causes.
 - If the network connection is abnormal, check whether port **22** is enabled in the security group of the CBH instance and FTP/SFTP server. Check whether port **22** is enabled and whether the public IP address (EIP) of the CBH instance is allowed in the ACL rule of the FTP/SFTP server.

Solution to cause 3

- Grant the upload permission on the user directory.
- Log in to the CBH system, choose **System > Data Maintenance > Log Backup**, and reconfigure the storage path of the FTP/SFTP server.

NOTE

If the storage path is left blank, the backup content is stored in the home directory of the FTP/SFTP server, for example, the absolute path **/home/user name**. The path must start with a period (.). For example, if the path is **./test/abc**, the absolute path is **/home/user name/test/abc**.

Solution to cause 4

- View the backup file on the server the day after the backup starts.

If the problem persists, click **Service Tickets** in the upper right corner of the management console and submit a service ticket.

5.5 How Do I Import Backup Data to a Primary/Standby CBH Instance?

Currently, CBH does not support importing backup data to a primary/standby CBH instance.

This function will be updated later.

6 About File Transfer

6.1 What File Transfer Methods Can be Used in a CBH System?

You can transfer files and audit transferred files in a CBH system. The file transfer methods on Linux and Windows hosts are different.

Transferring Files To or From a Managed Linux Host

To upload files to or download files from a Linux host, web browsers or FTP/SFTP clients are recommended for logging in to the CBH system. For details, see [Uploading Files to and Downloading Files from a Managed Linux Host](#).

- O&M Using a Web Browser

You need to configure the SSH protocol for the Linux host before the file transfer.

After logging in to the target Linux host through a web browser, you can upload or download files in the **File Transfer** tab in the session window to directly transfer files between your local PC and the target host. Alternatively, you can use the personal net disk to store files temporarily and complete file transfer between the target host and other managed hosts.

NOTE

The **rz** or **sz** command cannot be used to upload or download files during web-based O&M.

- O&M Using an FTP/SFTP Client

You need to configure FTP/SFTP protocol for the Linux host before the file transfer.

Log in to the target Linux host with a client tool and run the **rz** or **sz** command in the session window to transfer files.

Transferring Files To or From a Managed Windows Host

To transfer files on a Windows host managed in a CBH system, you can log in to the Windows host using only a web browser.

You need to configure RDP protocol for the Windows host before the file transfer.

Log in to the target Windows host using a web browser. In the **File transfer** tab in the session window, use the personal net disk to temporarily store files for uploads and downloads on disk **G** in the Windows host.

 **NOTE**

The default path of the personal net disk on a Windows host is NetDisk **G**.

For details about file transfer, see the following topics:

- [How Do I Upload or Download Files During Web-Based O&M?](#)
- [How Do I Use FTP/SFTP to Transfer Files to or From an SSH Host?](#)

6.2 How Do I Use FTP/SFTP to Transfer Files to or From an SSH Host?

The O&M engineer **admin_A** needs to use the FTP/SFTP client to transfer files to the SSH host **HOST_A** managed by a CBH instance.

Prerequisites

- OS requirement: The target device must support SFTP/FTP.
- Firewall requirements: Port 2222 (for SFTP) and port 2121 (for FTP) must be enabled.

Configuring **HOST_B** Resources

The CBH administrator assigns the O&M permissions of **HOST_B** to the O&M engineer **admin_A**.

Step 1 Choose **Resource > Host**.

Step 2 Click **New** to create FTP/SFTP host **HOST_B**.

- Select **FTP** or **SFTP** for **Protocol**. For security purposes, you are advised to select **SFTP**.
- Set **Host Address** to the IP address of **HOST_A**.
- Set other parameters according to the configuration of **HOST_A**. **HOST_A** and **HOST_B** point to the same host, but the protocol type is different.

Step 3 Choose **Policy > ACL Rules**, and assign the newly created host **HOST_B** to **admin_A**.

----End

Transferring files using SFTP/FTP clients

The following describes how the O&M engineer **admin_A** logs in to the CBH instance and transfers files using **HOST_B**.

Step 1 Choose **Operation > Host Operations**.

Step 2 Click **Login** in the row where **HOST_B** locates.

Step 3 Start the local FTP/SFTP client and enter the required login information in the displayed dialog box.

Step 4 After engineer **admin_A** logs in to **HOST_B**, files can be transferred.

 **NOTE**

- The FTP/SFTP client login password is the password used by **admin_A** to log in to the CBH system.
- For details about the login precautions, see [Using the FTP/SFTP/SCP Client for Logging In](#).

----End

6.3 How Do I Upload or Download Files When I Log In to Managed Hosts Using a Web Browser?

During web-based O&M, you can upload or download files in **File Transfer** tab. This feature enables file transfer between a local computer and managed host and between different managed hosts. The CBH system records the entire file transfer process in detail, making it easier to audit file upload and download operations.

Netdisk is a personal net disk in a CBH system, which is preset for each system user. A user can temporarily store files on it for file transfer between managed hosts. The file content in the personal net disk is visible only to users who creates the file.

Netdisk is directly associated with each system user. If a user is deleted, the files on the personal net disk are cleared and the personal net disk space is released.

Constraints

- For Linux servers, only SSH host resources support uploading and downloading files through web O&M.
- For Windows servers, only RDP host resources support uploading and downloading files through web O&M.
- During web-based O&M, users cannot upload files to or download files from managed hosts by running the **rz** or **sz** command but only through **File transfer**.

 **NOTE**

For Linux hosts, users can transfer files by running commands on the SSH client. For example, users can run the **rz** or **sz** command on the SSH client to upload or download files. However, the CBH system cannot record such file upload and download data, and the purpose of security audit cannot be met.

- Web-based O&M allows you to download one or more files but not folders.
- Resumable download is not supported. Do not stop or pause the file upload or download process.
- The size of the file to be transferred cannot exceed 1 GB. It is recommended that large files be split and transferred in several batches.

Prerequisites

- You have the permissions to upload and download host resource files.
- You have the host O&M permissions and can log in to the managed host using a web browser.

Uploading Files to and Downloading Files from a Managed Linux Host

Files can be directly transferred between a Linux host and a local computer without having to use the personal net disk. A personal net disk can be used to transfer files from other managed hosts.

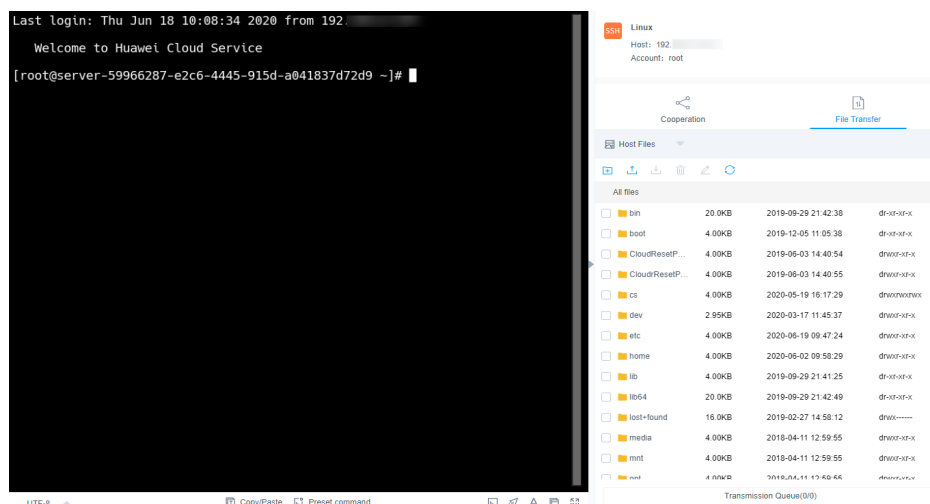
Step 1 Log in to the CBH system.

Step 2 Choose **Operation > Host Operation** and locate the target Linux host.

Step 3 Click **Login** to open the Linux host O&M session.

Step 4 Click **File Transfer** to list the Linux host files.

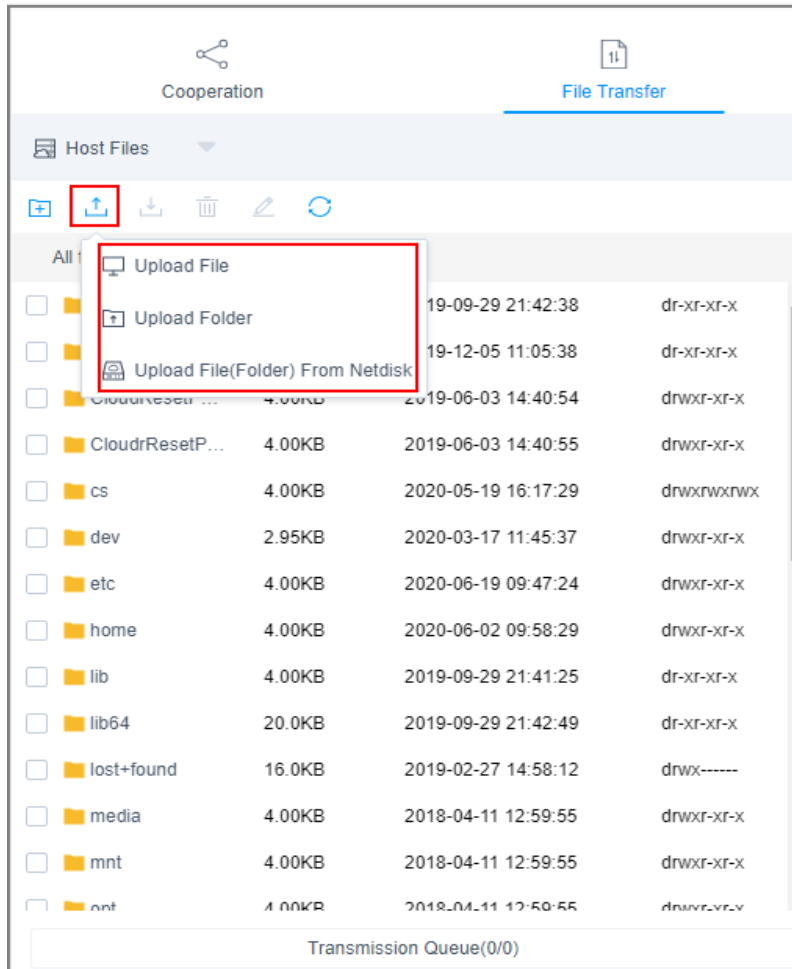
Figure 6-1 File Transfer session page on a Linux host



Step 5 Upload files to the Linux host.

You can click the upload icon and choose **Upload File**, **Upload Folder**, or **Upload File (Folder) from Netdisk** to upload one or more local files, local folders, or net disk files or folders to the Linux host.

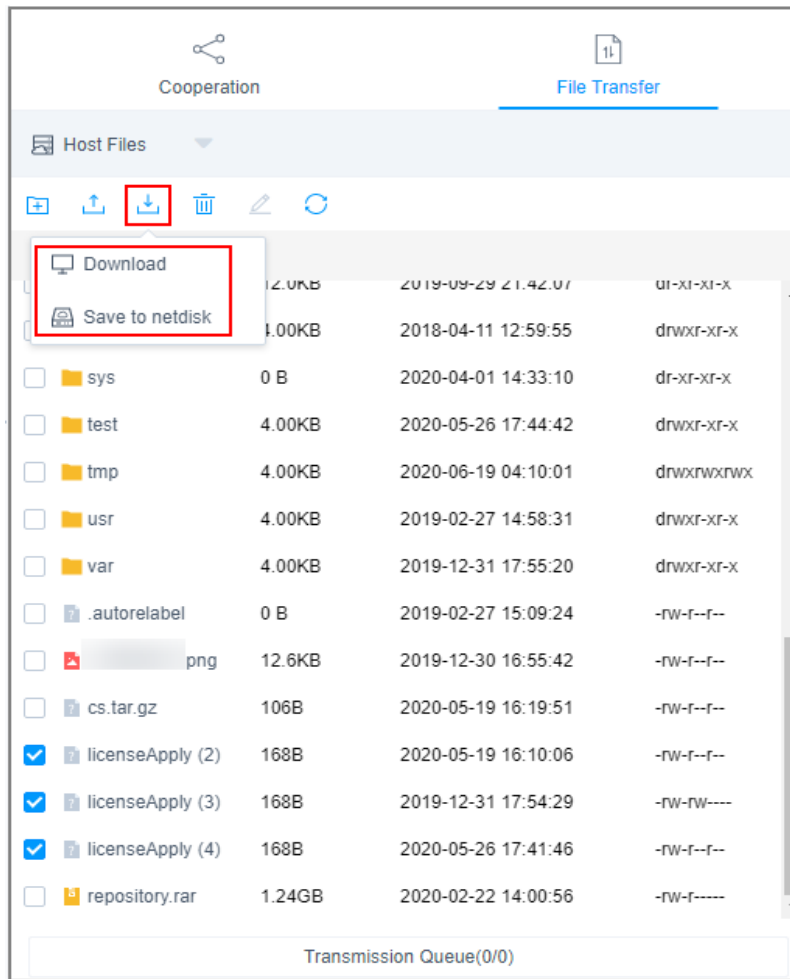
Figure 6-2 Uploading files to a Linux host



Step 6 Download files from the Linux host.

1. Select one or more files to be downloaded.
2. You can click the download icon to download one or more files to the local computer or the personal net disk.

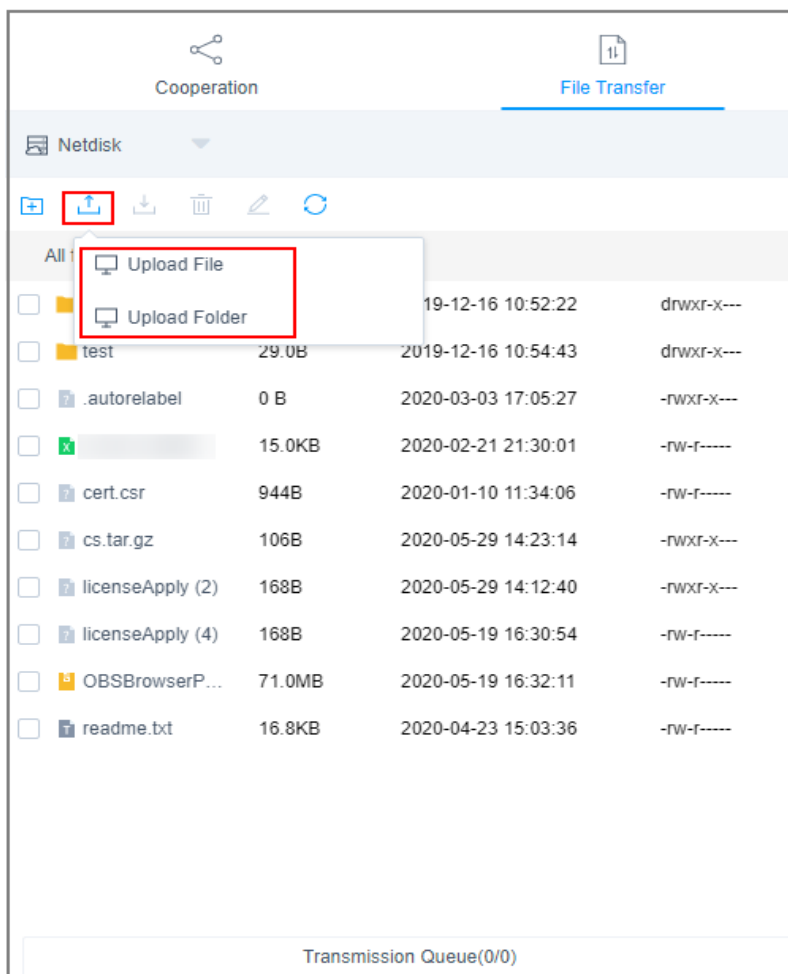
Figure 6-3 Downloading files from a Linux host



Step 7 Upload files to the personal net disk

1. Click **Host File** and select **Netdisk** to switch to the personal net disk file list.
2. Click the upload icon and upload one or more local files or folders.

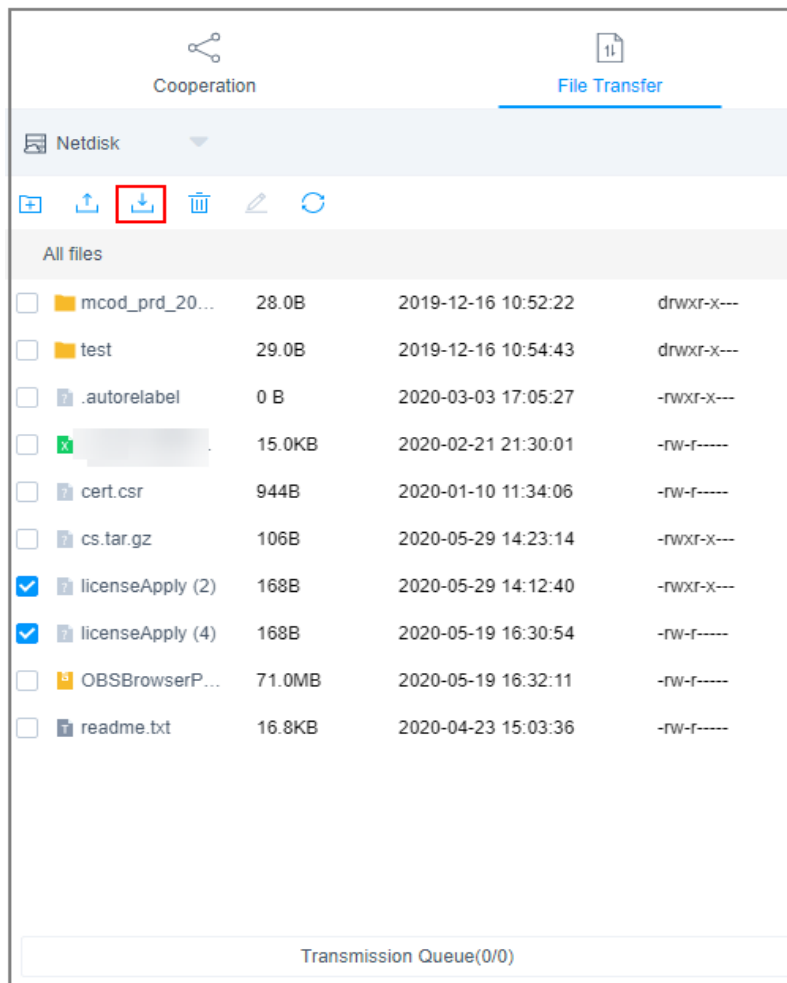
Figure 6-4 Uploading files to the personal net disk



Step 8 Download files from the personal net disk.

1. Select one or more files to be downloaded.
2. Click the download icon to download one or more files to the local computer.

Figure 6-5 Downloading files from the personal net disk



----End

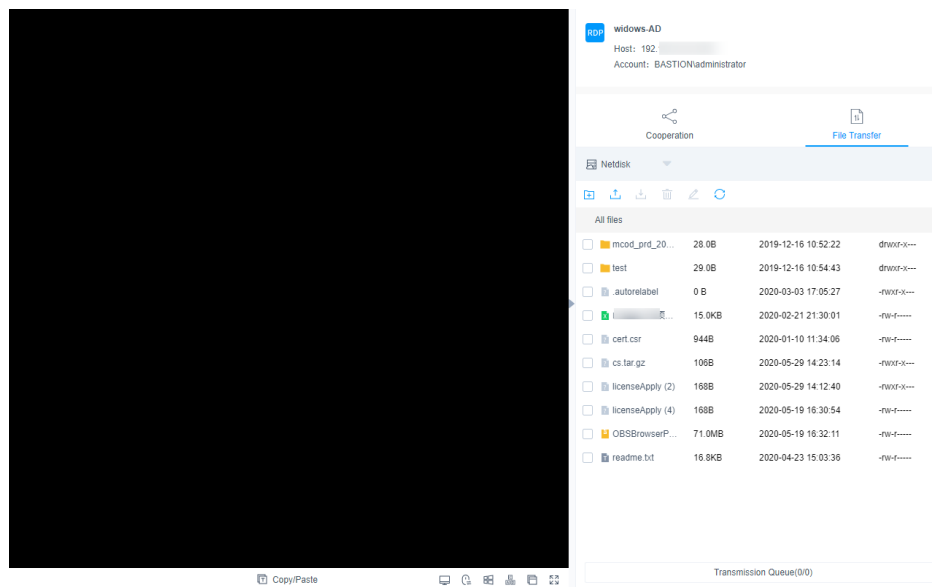
Uploading Files to and Downloading Files from a Managed Windows Host

For Windows hosts managed in a CBH system, the default path for storing files is **NetDisk G**. The disk is the personal net disk of the current user.

Files on a Windows host cannot be directly transferred between the host and a local computer. They can be transferred only through the personal net disk.

- Step 1** Log in to the CBH system.
- Step 2** Choose **Operation > Host Operation** and locate the target Windows host.
- Step 3** Click **Login** to open the Windows host O&M session.
- Step 4** Click **File Transfer** to list of host files on the personal net disk.

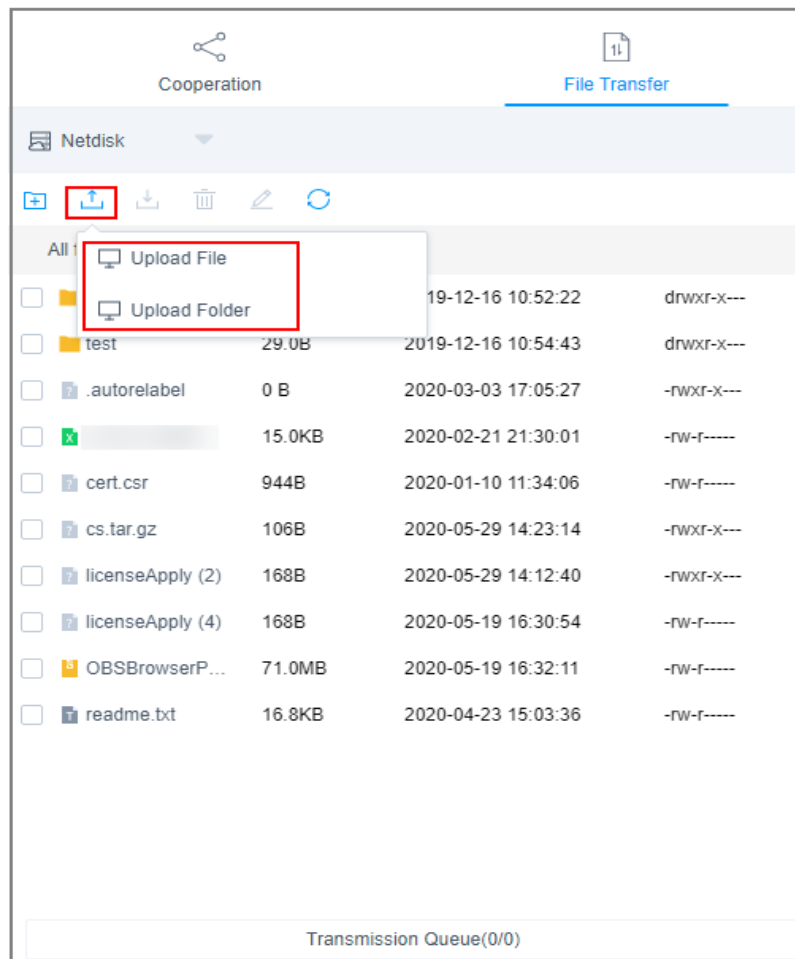
Figure 6-6 File Transfer session page on a Windows host



Step 5 Upload files to the Windows host.

1. Click the upload icon and choose one or more local files or folders.
2. Open the disk directory of the Windows host and search for **Netdisk** on drive G.
3. Open **Netdisk**, right-click the file or folder to be uploaded, copy and paste it to the target directory on the Windows host.

Figure 6-7 Uploading files to the personal net disk



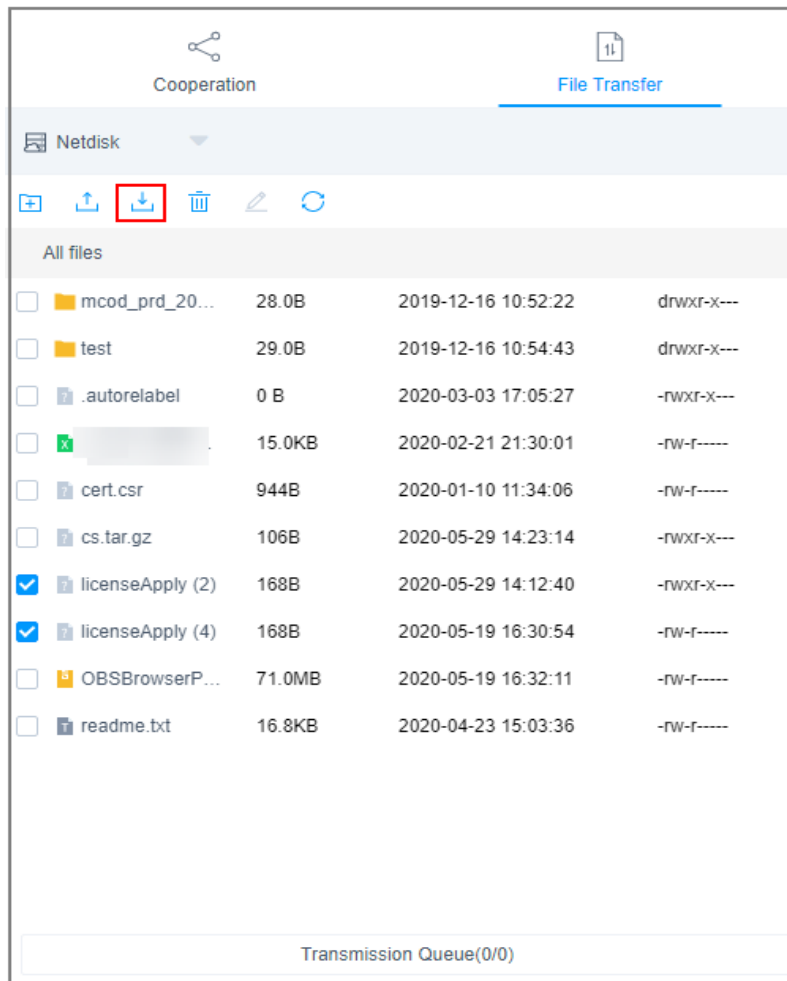
Step 6 Download files from the Windows host.

1. Open the Windows host disk directory, right-click the file or folder to be download, and copy it.
2. Open the **Netdisk** disk directory, right-click and paste the file or folder to the personal net disk on the Windows host.

Step 7 Download files from the personal net disk.

1. Select one or more files to be downloaded.
2. Click the download icon to download one or more files to the local computer.

Figure 6-8 Downloading files from the personal net disk



----End

Handling File Upload/Download Failures

For details, see [Why Does File Upload to or Download from a Managed Host Fail?](#)

6.4 What Is the Netdisk of a CBH System?

The host net disk **Netdisk** of a CBH system is a personal net disk of system users. It can be used as a file transfer station for users to temporarily store uploaded or to-be-downloaded files. A host net disk is:

- A private personal net disk. The data on a net disk is visible only to the user who creates the disk.
- Directly associated with the system users. After a user is deleted, the data on the personal net disk is cleared and its memory is released.
- The available memory space is the capacity of **Personal Netdisk** configured in the CBH system.

The total used space of a personal web disk cannot exceed the capacity configured for **Total Netdisk**.

Usage Restrictions

- Only the system administrator can set the **Personal Netdisk** and allocate the same size of the space to each system user.
For details, see [How Do I Set the Personal Net Disk Capacity?](#)
- The used space of a personal net disk cannot be queried.
- You can only manually delete files to free up space.

For details about how to use the **Netdisk** in the CBH system, see [How Do I Upload or Download Files During Web-Based O&M](#)

6.5 Why Does File Upload to or Download from a Managed Host Fail?

File Upload or Download Failures During Web-Based O&M

Symptoms

- When you attempt to transfer a **Host File** to **Personal Netdisk**, an error message is displayed indicating that the download failed.
- You cannot upload files and error the message "/3.0/h5FileService/upload-403: Service error. Please try again later." is displayed.
- When you attempt to upload a file from a local host to **Netdisk**, or **Personal Netdisk**, the system displays a message indicating that the **Personal Netdisk** space is insufficient.
- You cannot upload or download large files.
- The customer fails to upload files using the Debian+RDP protocol.
- The customer fails to upload files using the ZOC client.

Solutions

Figure 6-9 Mind map for troubleshooting



Table 6-1 Solutions

Troubleshooting Procedure	Possible Causes	Solution
Check whether the CBH system version is the latest.	The CBH system version is too old.	Upgrade CBH by referring to Upgrading the Version of a CBH System .
Check whether the files to be uploaded or downloaded are compressed.	In CBH, file folders must be compressed into packages for uploading and downloading.	Compress the folder into a package and upload or download the package.
Check whether the upload/download permission is obtained.	The resource file management permission is not enabled, and the user is not authorized to upload or download files.	<ol style="list-style-type: none"> Enable permissions to manage files for a certain resource. Grant file upload and download permissions to users.
Check the cache space of the browser.	The browser cache space is insufficient.	Clear the browser cache and upload the file again.

Troubleshooting Procedure	Possible Causes	Solution
Check whether the personal net disk has available storage space.	The Personal Netdisk works as a disk and cannot be automatically cleared. The Personal Netdisk space is insufficient, or the available disk storage space of the system is insufficient.	<ul style="list-style-type: none"> • Delete files from your personal net disk to release space. • Contact the administrator to set the personal net disk capacity. For details, see How Do I Set the Personal Net disk Capacity? • If the size of the file to be uploaded or downloaded is greater than the remaining Data Partition, contact the administrator to clear the system space or change specifications of a CBH instance.
Check the file is too large to be uploaded or downloaded.	The file has reached the maximum size allowed.	<ul style="list-style-type: none"> • Split the large file into several small files of about one GB and upload or download the small files in batches. • If the size of the file to be uploaded or downloaded is greater than the remaining Data Partition, contact the administrator to clear the system space or change specifications of a CBH instance.
Check whether the web login timeout period is appropriate.	Uploading or downloading large files takes a long time, and the web login connection times out. As a result, uploading or downloading large files fails.	<ul style="list-style-type: none"> • During the upload or download process, check the upload or download page irregularly to avoid system timeout. • Ask the administrator to change the web login timeout interval. • Ask the administrator to set the personal net disk capacity. For details, see How Do I Set the Personal Net disk Capacity?
Check whether the protocol and upload tool used by the client are compatible with CBH.	CBH does not support file upload or download using the Debian+RDP protocol or the ZOC tool.	<p>Use the protocols supported by CBH and the corresponding client tools to upload or download files.</p> <ul style="list-style-type: none"> • SFTP: Xftp 6 or later, WinSCP 5.14.4 or later, and FlashFXP 5.4 or later • FTP: Xftp 6 or later, WinSCP 5.14.4 or later, FlashFXP 5.4 or later, and FileZilla 3.46.3 or later

Troubleshooting Procedure	Possible Causes	Solution
Check whether the SCP command on the host is available.	SCP is not installed.	You need to install SCP on the ECS server.

File Upload or Download Failures During SSH Client O&M

Symptoms

If you use the Xshell client to log in to the hosts configured with the SSH protocol, the Xftp client cannot be called to transfer files.

Possible Causes

File transfer and transferred file auditing are disabled by the CBH system for O&M using an SSH client.

Solutions

- Configure the FTP/SFTP protocol for the host with the same IP address and use the FTP/SFTP client to transfer files.
For example, you can configure the SFTP for the host and assign access control permissions for the host. Then, you can directly log in to the host on the Xftp client to upload or download files.
- Log in to the host configured with the SSH protocol using a web browser to upload and download files.

For more information about file transfer in web-based O&M, see [How Do I Upload or Download Files During Web-Based O&M?](#)

For details about how to transfer files of host configured with the SSH protocol, see [How Do I Use the FTP/SFTP Client to Transfer Files to and from an SSH Host?](#)

If the problem persists, click **Service Tickets** in the upper right corner of the management console and submit a service ticket.

6.6 How Do I Clear the Personal Net Disk Space?

The **Netdisk** of a CBH system is a personal net disk for system users and cannot be automatically cleared up.

User admin can manually delete expired or discarded files to free up the personal net disk.

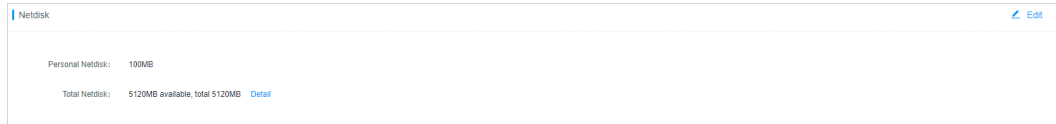
Clear the Net Disks of a Specific User

Step 1 Log in to the CBH system.

Step 2 Choose **System > Data Maintain > Storage Mgmt.**

Step 3 Expand the net disk space to view the capacity configured for **Personal Netdisk** and **Total Netdisk**.

Figure 6-10 Total Netdisk



Step 4 Click **Detail**.

Step 5 In the row containing the net disk, click **user.button.deleteNetDiskData** in the **Operation** column.

 **NOTE**

You can also select all net disks from which you want to delete data and click **user.button.deleteNetDiskData** to clear the disks together.

----End

Clearing Part of the Netdisk Capacity

Transferring Files To or From a Managed Linux Host


Step 1 Log in to the CBH system.

Step 2 Choose **Operation > Host Operation** and locate the target Linux server.

Step 3 Click **Login** to open the operation session for a Linux server.

Step 4 Click **File Transfer** to list the host files on a Linux server.

Step 5 Click **Host File** and select **Netdisk** to switch to the personal net disk file list.

Step 6 Select one or more files or folders and click  to delete them.

----End


Transferring Files To or From a Managed Windows Host

Step 1 Log in to the CBH system.

Step 2 Choose **Operation > Host Operation** and locate the target Windows host.

Step 3 Click **Login** to open the Windows host operation session.

Step 4 Click **File Transfer** to list of host files on the personal net disk.

Step 5 Select one or more files or folders and click  to delete them.

----End

Related Questions

- [How Can I Modify Net Disk Capacity?](#)
- [What Is the Netdisk in a CBH System?](#)

6.7 Why Is File Transfer Not Supported When I Use a Web Browser for Resource O&M?

Symptom

When you perform O&M of Linux host resources through a web browser, the **File Transfer** function is unavailable and a message is displayed indicating that the host does not support file transfer and the file directory cannot be viewed.

Possible Cause

The systemd-logind service of the Linux host is abnormal, affecting the SSH service. As a result, the file transfer function cannot be identified.

Solution

Step 1 Check whether the SSH service is normal.

In the O&M session window, run the **systemctl status sshd.service** command to check the service status.

- If the following information is displayed, the systemd-logind service is abnormal. Go to [2](#).

```
pam_systemd sshd:session:Failed to create session :Activation of org.....
```

- If other information is displayed, contact technical support.

Step 2 Restart the systemd-logind service on the Linux host.

In the O&M session window, run the **systemctl restart systemd-logind.service** command to restart the login service.

Step 3 Restart the SSH service on the Linux host.

In the O&M session window, restart the SSH service.

- CentOS 6
service sshd restart
- CentOS 7
systemctl restart sshd

Step 4 Log out of the system, log in to the Linux host again through CBH, and open the O&M session window.

----End

If the problem persists, click **Service Tickets** in the upper right corner of the management console and submit a service ticket.

6.8 Why Does the File List Cannot Be Loaded After I Click File Transfer When I Log In to CBH Through a Web Browser?

Symptoms

After a user logs in to a CBH instance through a web browser and tries to manage a Linux server, the file list cannot be loaded when the user clicks **File Transfer**.

Possible Causes

Files or folders in the directory of the Linux server contain special characters (garbled characters).

Solutions

Check whether the directory on the Linux server contains files or folders containing garbled characters. You can rename the file or folder that contains garbled characters. Otherwise, the directory list cannot be loaded.

6.9 How Do I Configure File Management Permissions?

You can use the file management function in a CBH system to manage files or folders of managed resources.

- To add, delete, modify, and query files, enable the file management permissions of the resources and ACL rules.
- If you need to upload or download files, you need to have the file upload and download permissions. These permissions can be enabled by the Admin user or the CBH policy administrator.

Constraints

Currently, file management is available only for SSH, RDP, and VNC host resources and application resources.

Prerequisites

Only users with the resource and ACL rule management permissions can configure file management permissions.

Step 1: Enable the file management permissions.

Both host and application resources support the file management function. The following describes how to add the file management permission for host resource *ECS1*.

Step 1 Log in to the CBH system.

Step 2 Choose **Resource > Host > Host Mgmt.** On the displayed page, click the name of **ECS1** or **Manage**. The ECS1 details page is displayed.

Step 3 Click **Edit** in the **Basic Info** area. The **Edit Basic Info** dialog box is displayed.

Step 4 Select **File Manage** in the **Options** row and click **OK**.

----End

Step 2: Authorize the file management permission to users.

Configure an ACL rule to grant O&M permissions to users. The following uses O&M user **User1** as an example to describe how to obtain the file management permissions of **ECS1**.

Step 1 Choose **Policy > ACL Rules** and click **New** in the upper right corner of the displayed **Rule Name** page. The **New ACL Rule** page is displayed.

Step 2 Configure basic information and enable the file management permission.

- (Optional) Select **Upload** or **Download** in the **File Transmission** row.
- (Mandatory) Select **File Manage** in the **Options** row.

Step 3 Click **Next** and relate **User1** to **ECS1**.

Step 4 Click **OK**.

----End

Permission Authentication

As an example, the following describes how to log in to **ECS1** as **User1** using a web browser and configure file management permission.



Step 1 Log in to a CBH system as **User1**.

Step 2 Choose **Operation > Host Operations**. In the row of **ECS1**, click **Login**.

Step 3 On the displayed page, click **File Transfer** to view files on the host web disk or cloud host.

NOTE

- Cloud hosts are resources managed by the CBH systems. You can manage files or folders in the managed host.
- **Netdisk** is a personal net disk for CBH system users. Users can use the personal net disk to manage file transfer between managed hosts.

Step 4 If you have the upload or download permission on a managed host, click  to upload a file to the managed host or click  to download host files.

----End

For details about file management operations, see [O&M Using a Web Browser](#).

6.10 Does CBH Check Security of Uploaded Files?

No.

CBH is an O&M security management and audit platform and does not support the inspection of uploaded files.

If the file fails to be uploaded, refer to [Why Does File Upload to or Download from a Managed Host Fail?](#)

7 Billing, Renewals, and Unsubscriptions

7.1 How Do I Renew a CBH Instance and Update the Mapped System Authorization?

To ensure that you can use CBH properly, renew the CBH license before it expires or within the retention period.

- If your CBH instance is about to expire, you can renew it so that you can continue to use it.
- If your CBH instance fails to be renewed before it expires, there is a retention period for you. During the retention period, the CBH instance is frozen. As a result, you cannot log in to or use the mapped CBH system. If your subscription is still not renewed within the retention period, your data stored in the CBH system will be deleted, and the resource will be released.

Application Scenario

- The CBH instance has expired or is about to expire.
- The message center of the CBH system prompts that the authorized license is about to expire and you need to update the license in a timely manner.
- The CBH system cannot be logged in to, and a message is displayed indicating that the license needs to be updated.

Prerequisites

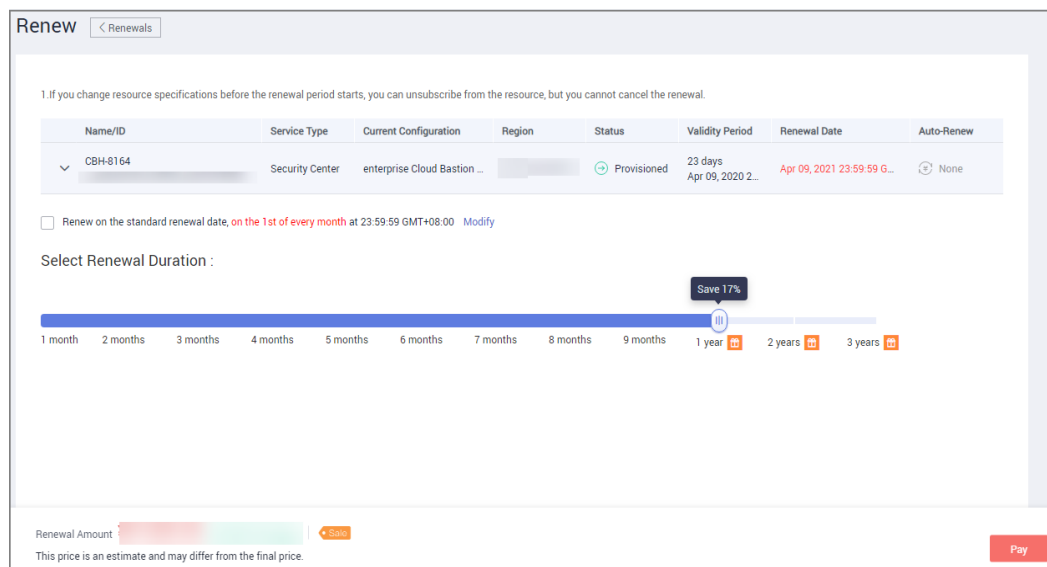
- You have the CBH operation permissions.
- Access to port 9443 is allowed by the firewall rules and in the outbound direction of the security group to which your CBH instance belongs. Otherwise, the renewal may fail.
- If your CBH instance version is V3.3.2.0 or earlier, [bind an EIP to the CBH instance](#). Otherwise, the renewal may fail.

Manual Renewal

Step 1 Log in to the management console.

- Step 2** Choose **Security & Compliance > Cloud Bastion Host**.
- Step 3** Click the instance to be renewed and choose **More > Renew** in the **Operation** column to go to the page for renewal.
- Step 4** Select the renewal duration as needed.

Figure 7-1 Renewal configuration



- Step 5** Click **Pay** and complete the payment.
- Step 6** Return to the CBH instance list page and check the latest expiration time in the **Billing Mode** column. You can log in to the CBH system in about 5 minutes.

NOTE

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

----End

7.2 How Is CBH Billed?

CBH instances can be billed on a yearly/monthly or pay-per-use basis.
CBH instances require elastic IP addresses, which are billed separately.

NOTICE

Currently, the pay-per-use billing mode applies only to the government cloud zone.

7.3 Can I Unsubscribe from a CBH Instance?

If you do not need to use CBH instances anymore, or the configured VPC or security group information for an instance is incorrect, you can unsubscribe from the CBH instance.

You can unsubscribe from a purchased cloud service and apply for a full refund unconditionally within five days of the purchase. Each account can request five-day unconditional full refund for 10 times in a year. Handling fees are required if you unsubscribe from a service over 5 days after it is purchased.

Prerequisites

- You have the CBH operation permissions.
- You have stopped all operations in the mapped CBH system and unbind the EIP from the CBH instance.

Unsubscription Process

To prevent data loss, unsubscribe from a CBH instance by performing the following operations:

1. Before the unsubscription, back up the system configurations by referring to [Backing Up and Restoring System Configurations](#).
2. Unsubscribe from the CBH instance. For details, see [Procedure](#).
3. (Optional only when you have purchased another CBH instance of the same edition as the one you unsubscribed) Restore the new CBH system with system configurations you backed up. For details, see [Restoring System Configurations](#).

NOTE

After you unsubscribe from a bastion host, the residual resources will be automatically cleared at 03:00 the next day. If you want to delete a security group, wait until the residual resources are cleared.

Procedure

- Step 1** Log in to the management console.
- Step 2** Choose **Security & Compliance > Cloud Bastion Host**.
- Step 3** Locate the row where the instance you want to unsubscribe from resides, and click **More > Unsubscribe** in the **Operation** column.
- Step 4** In the **Unsubscribe Instance** dialog box, click **OK**.
- Step 5** Complete the unsubscription.

NOTE

- The EIP can only be unbound when the instance is unsubscribed. If you want to release the EIP, go to the EIP console and release it manually.

----End

7.4 How Is a CBH Instance Billed After I Change Specifications of the Instance?

You can directly change your CBH instance specifications.

The price you need to pay after specification change is the price for the new instance specifications minus the remaining fees for the original instance specifications.

After enabling the specification change function for the CBH instance and backing up system data, you can perform the change as follows: Log in to the CBH management console, choose **More > Change Specifications** in the **Operation** column in the row where the target instance locates. On the displayed page, select the target instance edition and complete the payment. For details, see [Changing Specifications of a CBH Instance](#).

7.5 Will I Be Billed for Upgrading the CBH Software Version?

No.

Upgrading the CBH software version is free, but you will be billed for the extra specifications you obtained by changing specifications.

Log in to the CBH console. In the **Operation** column of the target instance, choose **More > Upgrade**. Upgrade the software version after confirming the instance upgrade message. For details about how to upgrade the version, see [Upgrading a CBH Instance Version](#).

After the software version is upgraded, restart the instance and change the instance specifications as required. For details, see [Changing Specifications of a CBH Instance](#).

7.6 How Do I Increase the CBH Instance Quota?

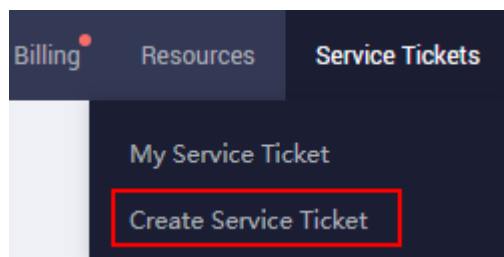
Currently, the default quota of each HUAWEI CLOUD account contains five CBH instances.

If your quota is insufficient during purchase, submit a service ticket to apply for increasing your quota.

Submitting a Service Ticket

Step 1 [Log in to the management console](#).

Step 2 In the upper right corner of the page, choose **Service Tickets > Create Service Ticket**.



Step 3 In the **Products** area, choose **More Products**, and click **Cloud Bastion Host** under **Security & Compliance**.

Step 4 Select a subtype, and click **Create Service Ticket**, and fill in required information.

In the **Problem Description** area, describe what you want and why, provide the **Project ID** of the corresponding region and the number of CBH instance quotas you want to increase.

 **NOTE**


For details about how to obtain the information of **Project ID**, see [My Credentials](#).

Step 5 After all mandatory parameters are configured, select **I have read and agree to the Tenant Authorization Letter** and click **Submit**.

----End

7.7 How Do I Purchase a CBH Instance When the System Prompts that Resources Are Sold Out?

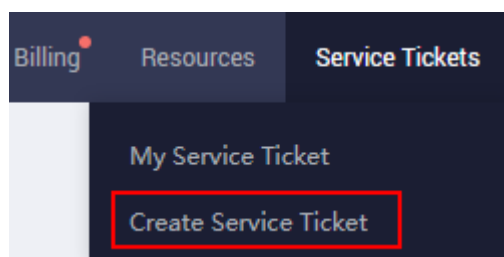
When you are prompted that resources are sold out during purchase a CBH instance, you can perform either of the following methods to solve the problem.

- Click  in the upper left corner of the management console and try another region or an AZ where you can find available instances.
- You can also submit a service ticket.

Submitting a Service Ticket

Step 1 [Log in to the management console](#).

Step 2 In the upper right corner of the page, choose **Service Tickets** > **Create Service Ticket**.



Step 3 In the **Products** area, choose **More Products**, and click **Cloud Bastion Host** under **Security**.

Step 4 Select a subtype, and click **Create Service Ticket**, and fill in required information.

In the **Problem Description** area, describe what you need and why.

Step 5 After all mandatory parameters are configured, select **I have read and agree to the Tenant Authorization Letter** and click **Submit**.

----End

8 About CBH System Login

8.1 Login Methods and Password Issues

8.1.1 Can I Use a Domain Name to Log In to a CBH System?

Yes.

Generally, the EIP bound to the CBH instance is used to log in to the CBH system. If you expect to use a unified domain for logins, use Domain Name Service (DNS) to resolve the domain to an EIP and then bind the EIP to your CBH instance. You can then enter the domain in the address box of a browser to log in to the CBH system.

8.1.2 What Login Methods Does CBH Provide?

You can log in to a CBH system using a web browser or an SSH client.

When you use a web browser, all configuration and management functions of the CBH system are available to you. When you use an SSH client, you can manage authorized host resources through shortcut keys and system commands. You can use the SSH client that you have get used to. It is recommended that the system administrator use the web browser to grant permissions to you. Then, you can log in to the CBH system by using the SSH client to perform O&M.

For details about how to log in to a CBH system using a web browser, see [Logging In to a CBH Instance Using a Web Browser](#).

For details about how to log in to a CBH system using an SSH client, see [SSH Client O&M](#).

8.1.3 Which Login Authentication Methods Are Available in a CBH System?

A CBH system supports local authentication, multi-factor authentication, and remote authentication. Multi-factor authentication includes mobile one-time password (OTP), mobile SMS, USB key, and OTP token methods. Remote authentication includes Active Directory (AD) domain, Remote Authentication

Dial-In User Service (RADIUS), Lightweight Directory Access Protocol (LDAP), and Azure AD methods.

 **NOTE**

- After a multi-factor authentication method is enabled, the local authentication becomes invalid. The CBH system can be logged in through the enabled multi-factor authentication method instead of usernames and passwords.
- If more than one multi-factor authentication methods are enabled for a system user, they can log in to the CBH system using any of the methods.

Local Authentication

The local authentication method is the default verification method. In this method, the CBH system authenticates user's identity through username and password.

Mobile OTP Authentication

In mobile OTP authentication, the CBH system authenticates user's identity through username, password, and mobile OTP.

For mobile OTP authentication to take effect, users need to log in to the CBH system using the username and password and bind the mobile OTP application to their account. After that, the administrator of the CBH system can log in to the CBH system and configure **Mobile OTP** for the system users.

Mobile SMS Authentication

In mobile SMS authentication, the CBH system authenticates user's identity through username, password, and SMS message.

Users need to configure an active mobile number for their account first, following which the administrator can configure **Mobile SMS** for the users.

USB Key Authentication

In USB key authentication, a USB key and its personal identification number (PIN) code are used to authenticate user's identity.

For USB key authentication to take effect, a valid USB key needs to be bound to a user.

OTP Token Authentication

In OTP token authentication, the CBH system authenticates user's identity through username, password, and OTP token.

For OTP authentication to take effect, an OTP application must be bound to a user.

AD Domain Authentication

After an administrator configures the AD authentication, the administrator creates AD domain authentication users or synchronizes users from the AD domain server.

The Windows AD domain server authenticates user's identity through the username and password.

Basic principles: The AD domain system terminal agent uses a third-party library to authenticate user identity.

- **IP:** IP address of the AD domain server
- **Port:** Set the port based on site requirements. The default value is **389**.
- **Domain:** Name of the AD domain

RADIUS Authentication

The administrator configures the RADIUS authentication mode and creates RADIUS authentication users. A third-party authentication server authenticates user identity through the username and password over the RADIUS protocol.

Basic principle: In RADIUS authentication, the client/server model is used to complete authentication by exchanging information between the user who accesses the device through a remote network and the server that contains user authentication and configuration information.

- **IP:** IP address of the RADIUS server
- **Port:** Set the port based on site requirements. The default value is **1812**.
- **Password:** authentication password of RADIUS
- **Test validity:** Test using the RADIUS account and password

LDAP Authentication

The administrator configures the Lightweight Directory Access Protocol (LDAP) authentication and creates LDAP authentication users. A third-party authentication server authenticates user identity in password login mode through the username and password over the LDAP protocol.

Basic principle: LDAP is a directory access protocol based on the TCP/IP protocol suite. It is a common access protocol for directory services on the Internet. It is a tree-like directory database.

- **IP:** IP address of the LDAP server
- **Port:** Set the port based on site requirements. The default value is **389**.
- **User OU:** Organization unit information in the LDAP tree structure. A distinguished name (DN) resembles a path-like structure starting at the directory root. **Base_DN** indicates the DN where the LDAP server starts searching for the user organization unit data in the directory database. For example: If the organization unit of the DN to be searched for is **ou1**, the value of **Base_DN** is **ou=ou1, o=O**.

Azure AD Authentication

To enable Azure AD authentication, the administrator creates an enterprise application on the Azure platform and adds platform users to the enterprise application. The administrator then configures Azure AD authentication in the CBH system and adds those platform users to the CBH system. After Azure AD authentication is enabled, when you log in to the CBH system as a system user, the Azure login page is displayed. You need to enter the username and password on this page. Your login is then authenticated by the Azure AD platform.

Basic principles: Azure AD authentication uses the SAML protocol. You need to configure the CBH system as an application on the Azure AD platform for identity authentication.

8.1.4 What Is the Initial Password for Logging In to a CBH System?

- For system administrator **admin**: When you buy a CBH instance, you are required to configure a password for the instance. This password is the default password for you to log in to the mapped CBH system for the first time.
- For other CBH system users: CBH system users are created by the system administrator **admin**. The passwords specified by the administrator during user creation are used by the system users for first-time logins.

8.1.5 How Do I Reset the User Password for Logging In to the CBH System?

When logging in to a CBH system for the first time, all users need to bind a mobile number as prompted for password resetting.

- If you forget the password of user **admin**, see [Resetting the Password of the admin User](#).
- You have logged in to CBH and forgot the password of the account configured with a mobile number. For details, see [Resetting Passwords on the Login Page](#).
- If a common user forgets the password and does not remember the configured mobile number, the system administrator **admin** or a user with the user management permission can reset the password of the common user. For more details, see [Batch Resetting Passwords of Common Users](#).
- For details about how to periodically change the password of a logged-in user, see [Modifying a Password](#).

Constraints

- Password resetting is not allowed during the user account lockout. You can reset the password after the account is unlocked.
- As a system user, if AD domain or RADIUS authentication is configured for you, you need to reset the password or change the password on the AD domain or RADIUS server. With AD or RADIUS authentication configured, the CBH system does not support your password management operations such as resetting the password or setting the password validity period.

Resetting the Password of the admin User

For details, see [Resetting the Password of User admin](#).

Resetting Passwords on the Login Page

The following describes how to reset a password when you have logged in to the CBH system but forgot the mobile phone number.

Step 1 On the CBH login page, click **Forgot Password?** to go to the page for resetting the password.

Step 2 On the displayed page, complete required information as instructed. Confirm the account information, and enter the login name, mobile number, and SMS verification code. Ensure that the entered mobile number must be the same as the mobile number bound to your account.

Step 3 Confirm the identity for password resetting.

Enter the mobile number bound to the user as prompted and verify the identity using the SMS verification code.

If you forget the mobile number, click **Can't get verification code?** and provide required information as prompted to find your password back.

Step 4 Reset and confirm the password as required.

 **NOTE**

The password must contain 8 to 32 characters. The password must contain uppercase letters (A to Z), lowercase letters (a to z), digits (0 to 9), and special characters. Spaces are not allowed.

Step 5 After the new password is set, return to the login page and enter the username and password to log in to the CBH system.

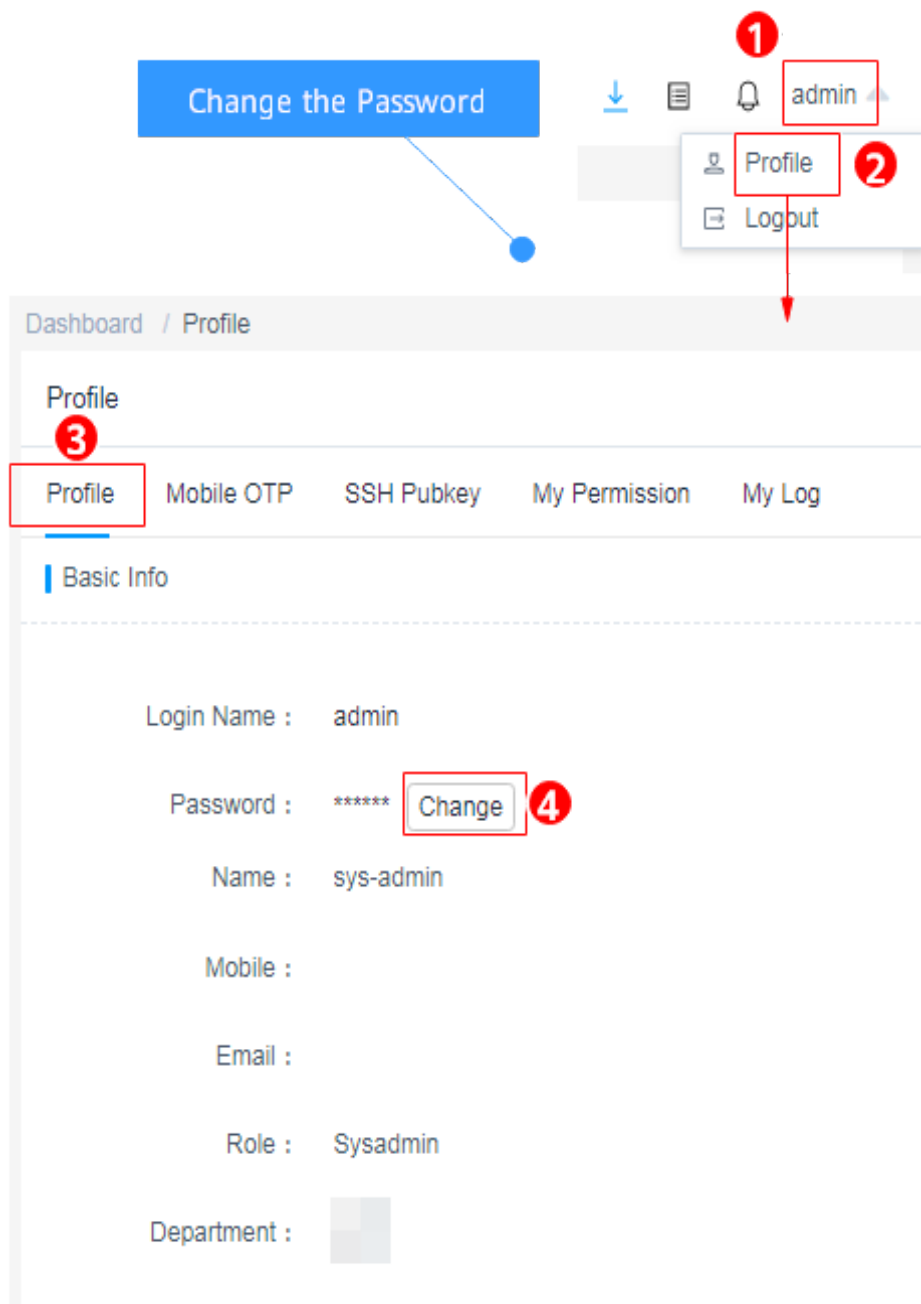
----End

Modifying a Password

If you have logged in to the CBH system, you can periodically change the login password as required.

Step 1 Go to the basic information tab by following the path shown in [Figure 8-1](#) and click **Password** to go to the **Change Password** dialog box.

Figure 8-1 Changing the password of a CBH system



Step 2 Enter the current password for verification, enter the new password as prompted, and confirm the new password.

Step 3 After the new password is set, you need to log out of the system and return to the login page to log in to the CBH system again.

----End

Batch Resetting Passwords of Common Users

The system administrator **admin** or a user who has the user management permission can reset passwords for other users in batches.

- Step 1** Log in to the CBH system.
- Step 2** Choose **User > User** in the navigation pane.
- Step 3** Select the users whose passwords are to be reset and click **More > Reset Password** to go to the page for resetting passwords.
- Step 4** Set a password.
- Step 5** Click **OK** to distribute the new password to the target users.

 **NOTE**

- It is recommended that the users whose passwords are reset in batches change the password upon logging in to the system because the reset passwords for all the target users are the same.
- Other users cannot reset the password of the system administrator **admin**.
- You can change only the passwords of other users in batches.
- After the password is reset, it cannot be viewed or exported in plaintext.

----End

8.2 Multifactor Verification

8.2.1 How Can I Install an OTP Authentication Application on the Mobile Phone?

To enable mobile OTP authentication, ensure that the OTP authentication application has been installed on your mobile phone and the administrator has configured mobile OTP as the multi-factor authentication method for you.

 **NOTE**

- If you are user **admin** and have mobile OTP authentication configured but have no OTP authentication application installed on your mobile phone, go to the management console, click **Service Tickets**, and submit a service ticket to contact technical support for login method resetting.
- If you are a common user and have no OTP authentication application installed on your mobile phone, you cannot log in to the CBH system through mobile OTP authentication. In this case, contact the department administrator to cancel **Mobile OTP** authentication.

8.2.2 Why Does the Mobile OTP Application Binding Operation Fail?

Symptom

When you enter the verification code obtained by scanning the QR code displayed on the login page and attempt to bound the mobile OTP application to your mobile phone, a message is displayed indicating that the mobile OTP application binding failed.

Possible Causes

The time of the CBH system is inconsistent with that of the mobile phone. In mobile OTP authentication, the CBH system time must be consistent with the mobile phone time, accurate to seconds.

Solution

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

Step 1 Log in to the CBH system.

Step 2 Choose **System > System Maintain > System Mgmt > System Time** to view the system time configuration.

Step 3 In the **System Time** area, modify the current system time or use the NTP server to synchronize the current system time.

If you use the NTP server to synchronize the system time, you can select the default NTP server of the system, or specify an NTP server.

Step 4 Click **Sync** to complete time synchronization.

Step 5 Choose **Profile > Mobile OTP** and bind the mobile OTP application again.

Step 6 Delete the bound mobile OTP application, scan the QR code again, and re-bind.

----End

8.2.3 How Do I Enable Mobile SMS Authentication For Logging In to the CBH System?

Prerequisites

- You have configured an active mobile number for the user account.
- You have enabled the SMS gateway IP address and port 10743 and port 443 for the security group of the bastion host instance, and the bastion host system can access the SMS gateway.
- The number of times the SMS verification code is sent does not exceed the maximum allowed limit.

NOTE

If you have configured the SMS gateway as a built-in gateway in the CBH system, the limitations for sending SMS verification codes to an individual account are as follows.

- A maximum of one SMS message can be sent within 1 minute.
- A maximum of 5 SMS messages can be sent within an hour.
- A maximum of 15 SMS messages can be sent within 24 hours.

Configuring Mobile SMS Authentication

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

Step 2 Choose **User > User**.

- Step 3** Click the login name of the user whose information you want to change, or click **Manage** in the row of the user in the **Operation** column.
 - Step 4** Click **Edit** in the **User Setting** area to modify the login configuration of the user.
 - Step 5** Select **Mobile SMS** for **Multifactor verification**.
 - Step 6** Click **OK**.
- End

Mobile SMS Authentication Login

After the authentication configuration is modified, go to the CBH system login page through a web client or an SSH client, select the mobile SMS authentication, and enter the login name and the bound mobile number to obtain the SMS verification code for the login.

For details, see [Using a Web Browser to Log In to a CBH System](#) and [Using an SSH Client to Log In to a CBH System](#).

8.2.4 How Do I Cancel Mobile SMS Authentication?

You can cancel SMS authentication at any time for certain reasons, such as SMS gateway faults.

NOTE

If the **admin** user cannot log in to the CBH system through **Mobile SMS** authentication, submit a service ticket.

Prerequisites

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

Procedure

- Step 1** Log in to the CBH system.
 - Step 2** Choose **User** > **User** in the navigation pane.
 - Step 3** Select the user accounts you want to edit and click **More** in the lower left corner to expand the batch operation buttons.
 - Step 4** Click **Edit multifactor**.
 - Step 5** Deselect **Mobile SMS** multi-factor authentication.
 - Step 6** Click **OK**.
- End

8.2.5 How Can I Cancel Mobile OTP Authentication If No Mobile OTP Application is Bound to My Account?

- If no mobile OTP application has been bound to your account and you are the **admin** user, submit a service ticket and ask the technical support to reset the

login authentication method of **admin** to the initial state. This will not change other system configurations.

- If no mobile OTP application has been bound to your account and you are not the **admin** user, contact the **admin** user to cancel mobile OTP authentication.

8.2.6 Why Does Login Fail When an Account That Has Mobile OTP Application Bound Is Used to Log In?

Symptom

When you log in to a CBH system using an account bound with a mobile OTP, the message "You cannot log in to the system using the mobile token. Try other login methods" is displayed.

Possible Cause

Mobile OTP has not been selected for **Multifactor Verification**.

Solution

A user needs to bind a mobile OTP application to their account on the **Profile** page. The administrator then logs in to the system and enables **Mobile OTP** for **Multifactor Verification** for the user.

Step 1 Log in to the CBH system as user **admin**.

Step 2 Choose **User > User**, locate the target user, and click **Manage**. The **User Details** page is displayed.

Step 3 Click **Edit** in the **User Setting** area. The **Edit user setting** dialog box is displayed.

Step 4 Select **Mobile OTP** for **Multifactor Verification**.

Step 5 Click **OK**.

----End

After the configuration completes, the user can select the mobile OTP method to log in to the CBH system.

8.3 Login Security Management

8.3.1 How Do I Set a Security Lock for Logging In to the CBH System?

Scenario

- An account can be used to log in to CBH from different browsers on the same PC.
- A user account cannot be used to log in to a CBH system from different device at the same time. If it does, the source IP address will be locked out.

- A user account can only be used by a specific user for secure O&M.

Symptom

To secure CBH system, the source IP address or user account will be locked out after the number of consecutive invalid password attempts reached the configured upper limit.

Procedure

- Step 1** Log in to the CBH system.
- Step 2** Choose **System > Sysconfig > Security** and view the current configuration in the **UserLock Config** area.
- Step 3** Click **Edit** in the **UserLock Config** area.
- Step 4** Set parameters as required. For details about the parameters, see [Table 8-1](#).

Table 8-1 Parameters for configuring lockout parameters

Parameter	Description
Lock	<p>You can select User or Source IP.</p> <ul style="list-style-type: none"> • If you select User, the user account will be locked after the number of consecutive incorrect password attempts exceeds the configured threshold. • If you select Source IP, the local source IP address of the user is locked and the IP addresses in the same network segment in the LAN are locked after the number of consecutive invalid password attempts exceeds the configured threshold.
Password attempt	Threshold on consecutive invalid password attempts for all users to log in to a CBH system
Lock duration	<p>Duration for locking out a user after the number of consecutive incorrect password attempts exceeds the configured threshold, in minutes.</p> <ul style="list-style-type: none"> • The default value is 30 minutes. • The value of 0 indicates that the account or source IP address will be locked out until an administrator unlock it manually.
Count reset duration	Amount of the time the account or source IP address will remain locked out after the consecutive incorrect password attempts exceeds the configured threshold

- Step 5** Click **OK**.

----End

8.3.2 How Do I Unlock a User or IP Address Locked During the Login to a CBH Instance?

CBH enables account lockout by **User**, **Source IP**, and **User + Source IP**. To change the lockout mode, refer to **Security Configuration > UserLock Config**.

Unlocking an IP Address

When you log in to the CBH system, the system displays a message indicating that the IP address has been locked and you need to try again 30 minutes later. In this case, your source IP address has been locked by the CBH service and you cannot log in to the CBH system using the IP address within the specified period.

The solution is as follows:

- Wait until the lockout duration expires and try again.
- Submit a service ticket to contact technical support and provide the locked IP addresses for them.

Unlocking a User

If the CBH system displays a message indicating that the user account has been locked and you need to try again 30 minutes later, the user account cannot be used to log in to the CBH system within the specified period. The solution is as follows:

- Wait until the lockout duration expires and try again.
- If a system user account is locked, log in to the CBH system as the **admin** user and choose **User > User**. On the displayed page, select the locked user and click **Enable** to unlock the user account.

NOTE

The **admin** account has the highest operation permissions. If the **admin** account is locked, you can perform operations only after the lockout duration expires.

9 User, Resource, and Policy Configuration in a CBH System

9.1 Users

9.1.1 Why Cannot I Select a Superior Department When Creating a User or Resource?

The role of the account you used to create new users or resources is not configured with management permissions. As a result, when you create a user or resource, the department to which the new user or resource belongs cannot be the superior department of the current account.

For more information about department management and role management, see [Department](#) and [Role](#).

9.1.2 How Do I Change a Mobile Number Bound to a CBH System User?

The mobile number of a CBH system is important for user login verification, password resetting, and receiving dynamic system information.

- For the **admin** user, its mobile number is bound during the first login.
- For other users, the mobile number is bound when they are created by the **admin** user or when they log in to the CBH system for the first time.

The mobile number of a system user account can be modified by the system user or the **admin** user. The admin user can batch modify mobile numbers of other system users.

Changing the Mobile Number as a System User

Step 1 Log in to the CBH system.

Step 2 On the **Dashboard** page, click **Profile** in the upper right corner to enter the **Profile** management page.

Step 3 In the **Basic Info** area, click **Edit** to go to the **Edit Basic Info** dialog box.

Step 4 Configure a new mobile number.

Step 5 Click **OK**.

----End

Changing the Mobile Number for a System User as User admin

The system administrator **admin** or a user who has permissions for the **User** module can reset a mobile number for other users one by one.

Step 1 Log in to the CBH system.

Step 2 Choose **User > User** to go to the **User** management page.

Step 3 Select the desired user and click the user name or **Manage** in the **Operation** column.

Step 4 Click **Edit** in the **Basic Info** area.

Step 5 Configure a new mobile number.

Step 6 Click **OK**.

----End

Changing the Mobile Number for System Users in Batches by admin

The system administrator **admin** or a user who has permissions for the **User** module can reset a mobile number for other users in batches.

Step 1 Log in to the CBH system.

Step 2 Choose **User > User** to go to the **User** management page.

Step 3 Export user information.

Select the all desired user and click **Export** to save the user information file locally.

Step 4 Change the mobile number of users.

Manually change the mobile number as needed and save the file.

Step 5 Export user information.

1. Go back to the **User** page and click **Import**.
2. Click **Upload** and select the modified user information file.
3. After the upload is complete, choose **More > Override existing accounts**.
4. Click **OK**.

----End

9.1.3 How Many Users Can Be Created in a CBH System?

There is no limit.

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

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

For details, see [Creating a User](#).

9.2 Adding Resources to a CBH System

9.2.1 How Can I Start Database Maintenance in a CBH System?

In CBH, you can manage a variety of databases in the **host O&M** module (**Host Operation**) and **application O&M** module (**Application Operation**). For details, see [Which Types of Databases Can I Manage in a CBH System?](#). In the host operation module, you can audit database operations, such as adding, deleting, modifying, and querying database operations. In the application operation module, you can audit operation sessions through videos.

NOTE

- In CBH standard editions, directly managing databases is not available. To manage databases, an application publish server must be set up.
- In CBH professional editions, directly managing databases is available in the host operation and application operation modules.

Prerequisites

- You have purchased a CBH instance and the CBH system can be logged in. To manage databases by command, purchase a professional CBH instance. You can then manage databases by command in the host operation module.
- The network connection between the databases and CBH instance is normal. The security group of the CBH instance allows inbound access through port 33306, and the database security group allows access from the IP address of the CBH instance.

Managing Databases in the Host Operation Module

The host O&M module makes it easy for you to maintain MySQL, SQL Server, Oracle, and DB2 databases by Single Sign-On (SSO) authentication.

Step 1 The administrator creates a host resource for databases.

Choose **Resource > Host**, set the **Protocol Type** to **DB2, MySQL, SQL Server**, or **Oracle**, and add or let the system generate a database account. For details about other parameters, see [Creating a Host Resource](#).

Step 2 Assign access control permissions to users as an administrator.

- Choose **Policy > ACL Rules**, grant the database access permissions to users, and relate the users to the account generated in the last step. For details, see [Creating an ACL Rule](#).
- Choose **Policy > Database Control Rules**. For MySQL and Oracle databases, you can configure key operation control rules to perform command interception. For details, see [Database Control Rules](#).

Step 3 Log in to the database as an O&M user.

Choose **Operation > Host Operation** and log in to the database as an authorized user. For details about how to log in to a database as an authorized user, see [Logging In to CBH Using an SSO Client](#).

O&M users can add, delete, modify, and query managed databases, view the commands that are being executed on the [Live Session](#) page, and view history command operation records on the [History Session](#) page.

When an O&M user runs a critical operation command, the system automatically initiates command interception and generates a **database authorization ticket**. To continue the O&M operation, the O&M user needs to submit an application to the administrator for approval.

 **NOTE**

The host O&M module does not support the generation and download of historical database O&M session videos.

----End

Managing Databases in the Application O&M Module

The application O&M module **App Operation** allows you to maintain all types of databases through web sessions and automatically inputs account usernames and passwords of databases. Before managing databases in this module, ensure that the network connection between the database to be managed and the application publishing server is normal and the network connection between the application publishing server and the CBH instance is normal.

Step 1 Create an application for databases to be managed as an administrator.

Choose **Resource > Application Publish**, configure an application of database type, and add or let system generate a database account. For details about other parameters, see [Publishing an Application](#).

Step 2 Assign access control permissions to users as an administrator.

Choose **Policy > ACL Rules**, grant the database access permissions to users, and relate the users to the account generated in the last step. For details, see [Creating an ACL Rule](#).

Step 3 Log in to the database as an O&M user.

Choose **Operation > App Operation** and authorize users to log in to database resources. For details about O&M session operations, see [Application O&M](#).

O&M users can record database O&M sessions by video and download session videos from the [History Session](#) module.

 NOTE

The application O&M module does not support command interception during O&M sessions.

----End

For more information about database O&M, see [Which Types of Databases Can I Manage in a CBH System?](#)

9.2.2 How Do I Use CBH to Manage RDS Databases?

CBH allows you to use CBH to manage RDS databases in the same VPC.

Constraints


Only professional edition CBH can directly manage DB2, MySQL, SQL Server, and Oracle databases.

Prerequisites

- You have purchased a CBH instance and the CBH system can be logged in. To manage databases by command, purchase a professional CBH instance. You can then manage databases by command in the host operation module.
- The network connection between the RDS databases and CBH instance is normal. The security group of the CBH instance allows inbound access through port 33306, and the database security group allows access from the IP address of the CBH instance.

Obtaining the Version, Floating IP Address, Port, and Administrator Account of an RDS DB Instance

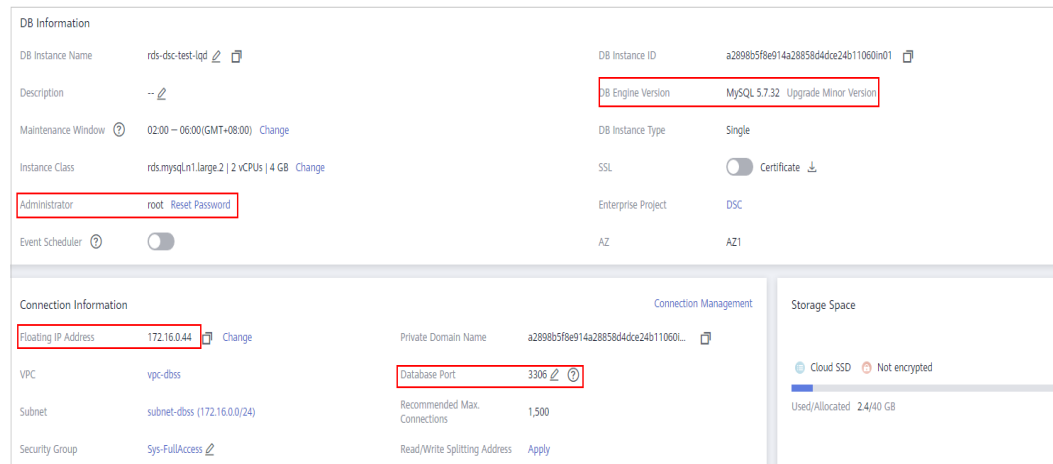
Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, click  and choose **Databases > Relational Database Service** to go to the **Instance Management** page.

Step 4 Click the instance you want to view. On the displayed details page, record details about **DB Engine Version**, **Floating IP Address**, **Database Port**, and **Administrator**.

Figure 9-1 RDS database instance details page



----End

Managing RDS Databases Through CBH

- Step 1** Log in to the CBH system.
- Step 2** Choose **Resource** > **Host** in the navigation pane on the left.
- Step 3** Click **New**. On the displayed dialog box, configure parameters by referring to [Table 9-1](#).

Table 9-1 Parameters for adding RDS instances into CBH

Parameter	Description
Host Name	Custom name of the host resource. The host name must be unique in the CBH system.
Protocol	Select MySQL or SQL Server . Obtain the database types of the RDS instance you want to manage by referring to Obtaining the Version, Floating IP Address, Port, and Administrator Account of an RDS DB Instance .

Parameter	Description
Host Address	<p>Host IP address that can be used to establish connection with the CBH system.</p> <p>For RDS databases, use the floating IP address of the RDS instance as the host address. You can obtain the floating IP address of the RDS instance by referring to Obtaining the Version, Floating IP Address, Port, and Administrator Account of an RDS DB Instance.</p> <p>NOTE It is recommended that you set Host Address to a private IP address in the same VPC. This is because CBH manages host resources in the same VPC based on network stability and proximity. The external access port of the private IP address is not restricted by the network security (security group and ACL) policies. While the EIP of the host is an independent elastic IP address. The port for external access over an EIP is restricted by network security policies. As a result, you may fail to log in to the host from the CBH system.</p> <p>So we recommend private IP addresses.</p>
Port	Database port of the RDS instance, which you can obtain by referring to Obtaining the Version, Floating IP Address, Port, and Administrator Account of an RDS DB Instance .
OS Type	(Optional) Type of the host OS or device OS. This parameter is auto-filled by the CBH system.
Options	<p>(Optional) Select File Manage, X11 forward, uplink clipboard, and/or downlink clipboard.</p> <ul style="list-style-type: none"> • 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 Name	Department to which the host resource belongs.
Label	(Optional) You can customize a label or select an existing one.
Remarks	(Optional) Provides the description of the host resource.

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

Table 9-2 Parameters of managed host accounts

Parameter	Description
Add Account	<p>When to add the account. The options are Rightnow and Afterward.</p> <ul style="list-style-type: none"> If you select Rightnow, continue the configuration on the page to add the account immediately. If you select Afterward, no further configuration is required on the page. You can add the account information later in the resource list or on the resource details page.
Logon Type	<p>Login method of the host resource. The options are Auto Login and Manual Login.</p> <ul style="list-style-type: none"> If you select Auto Login, Account and Password are mandatory. If you select Manual Login, Account and Password are optional.
Account	<p>The administrator account of the RDS instance you obtained in Obtaining the Version, Floating IP Address, Port, and Administrator Account of an RDS DB Instance.</p> <p>NOTE If the AD domain service is installed on the host, the added account is <i>Domain name\Host account name</i>, for example, ad\administrator.</p>
Password	<p>The password of the administrator account of the RDS instance. By default, Verify is selected. After the account is added, the system automatically verifies the status of the account.</p> <p>NOTE</p> <ul style="list-style-type: none"> After the account is verified, the host resource information is saved. Verification failed <ul style="list-style-type: none"> If the system prompts that the verification times out, return to the configuration window and modify the resource information. If the system prompts that the account password is incorrect, return to the configuration window and change the account password.
Remarks	Brief description of the account.

 **NOTE**

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

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

Step 6 In the navigation pane on the left, choose **Policy > ACL Rules** and configure the access control policy of the RDS database.

Step 7 In the navigation pane on the left, choose **Operation > Host Operations**. In the host list, locate the row that contains the RDS database, and click **Login** in the **Operation** column.

Step 8 (Optional) In the displayed dialog box, click **Download the SSO tool** and then install it in the default mode.

 **NOTE**

If the SSO tool has been installed, skip this step.

Step 9 Configure the SSO tool by referring to [How Do I Configure the SSO Tool?](#)

Step 10 After you complete [Step 8](#) to [Step 9](#), click **Login** in the **Operation** column.

 **NOTE**

If an error message is displayed indicating that the database client tool configuration path is incorrect and a reconfiguration is required, perform [Step 9](#) again.

----End

9.2.3 How Do I Change the Password of a Managed Resource Account?

Directly Changing Passwords of Managed Accounts

After the account password of a host or application server is changed, you need to change the password of the account managed by CBH.

Step 1 Log in to the CBH system.

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

Step 3 Click the account whose password is to be changed or click **Manage** to go to the account details page.

Step 4 In the **Basic Info** area, click **Edit**. The **Edit basic info** dialog box is displayed.

Step 5 Enter the new password and select **Verify**. Click **OK** to host the new password of the account.

Step 6 Go to the account list page and view the message in **Tasks** to check whether the new password is correct.

 **NOTE**

You can also go to the **Account** page, select the account whose password has been changed, and click **Test and Verify** at the bottom to verify the new password.

----End

Changing Passwords Through Password Change Rules

You can also change account passwords on managed hosts and applications through creating password change rules on the **Chpwd** page in the **Policy** module and then host the new passwords.

In addition, you can download password change logs or export the managed account list to view the new account password.

 **NOTE**

A password change rule takes effect only for accounts on managed hosts that can be logged in to through passwords. It does not take effect for managed hosts that use SSH keys for login authentication.

9.2.4 How Do I Set a Sudo Privilege Escalation Account for the Managed Resource?

CBH supports adding Sudo login accounts for SSH and Telnet hosts.

Account **test** can be used by the O&M engineer **admin_A** to log in to the target host. However, account **test** has limited permissions. In this case, the CBH system administrator can use the sudo command to escalate the privileges of account **test** for O&M purpose of engineer **admin_A**. After the sudo privilege escalation is configured, the system automatically switches to the Sudo account login page when engineer **admin_A** logs in to the target host using account **test**. The administrator can configure a sudo privilege escalation login account as follows:

- Step 1** Choose **Resource > Host**.
- Step 2** Locate the row where the target host resides and click **More > Add Account** in the **Operation** column.
- Step 3** Select **Sudo Login** for **Login Type**, complete other required information, and click **OK**.

Table 9-3 Parameters for setting a sudo privilege escalation account

Parameter	Description
Login Type	Select Sudo Login .
Password	Enter the login password of an account with the highest level of permissions to the target host. For example, if user root has the highest permission to the managed host, enter the password of user root .
Switch from	Select the account with no sudo permissions configured.
Switch command	Retain the default value of su .

- Step 4** Choose **Resource > Account**. The new Sudo login account is displayed.
- Step 5** Choose **Policy > ACL Rules**, and assign the newly created Sudo login account **[root->su]** to **admin_A**.

----End

9.2.5 How Do I Add a Label to Resources Managed in a CBH System?

Prerequisites

You have the permissions for operations in the **Host**, **Application Publish**, **Host Operations**, and **App Operations** modules.

Adding a Label

- Step 1** Log in to the CBH system.
- Step 2** Choose **Resource** > **Host** in the navigation pane on the left.
- Step 3** Select the target host and click **Add Label**. The **Add Label** dialog box is displayed.
- Step 4** Type label information in the **Label** field and press **Enter** to create a customized label, or select an existing label from the **Label** drop-down list.
- Step 5** Click **OK**. You can go to the **Host** page in the **Resource** module or the **Host Operations** page in the **Operation** module to view the new label of the managed host.
- Step 6** After a label is added, you can select a label from the drop-down list in the **Label** column on a specific resource management page to search for resources.

----End

Deleting Labels

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

- Step 1** Log in to the CBH system.
- Step 2** Choose **Resource** > **Host** in the navigation pane on the left.
- Step 3** Select the target host and click **Delete Label** at the bottom of the host list. In the displayed **Delete Label** dialog box, click **Confirm**. All labels added to the host are deleted.
- Step 4** You can go to the **Host** page in the **Resource** module or the **Host Operations** page in the **Operation** module to view the managed host.

NOTE

- After you confirm the deletion, all labels of the selected resource are deleted.
- If a label is not used by any resources, the system will delete it.
- To delete a single label of a managed host or application, click **Manage** in the host or application resource list. On the displayed page, delete the label as needed.

----End

9.2.6 How Do I Import or Export Information of Host Resources in Batches?

Batch Importing

CBH does not support batch creating of host resources. However, you can batch import host resources by importing an Excel file or through cloud platform.

From file: The Excel file must include the host name, IP address/domain name, protocol type, port, OS type, department, label, host description, host account, login mode, and privileged account.

NOTE

- The **From file** method requires that host information in the Excel file be filled strictly in accordance with the template file format. In addition, the file cannot be encrypted so that it can be opened after the upload. Otherwise, host resources fail to be imported.
- By importing hosts in batches, you can configure automatic login during host information entering to avoid the generation of **Empty** account.

Batch Exporting

CBH also allows you to export information about a batch of host resources. As an authenticated user, you can export information about all managed host with just one click. You can view the latest configuration about accounts of all managed hosts.

The exported Excel file includes the host name, host address, protocol type, port number, OS type, department, label, host description, account name, login mode, and privileged account.

9.2.7 What Are the AK and SK of an Imported Host? How Can I Obtain Them?

An access key comprises an access key ID (AK) and secret access key (SK) pair that is used as identity credentials for users to access cloud resources using development tools. The system uses AKs to identify users and SKs to verify signatures. Encrypted signature verification ensures the confidentiality and integrity of requests and the identity of the requester.

- If you select a cloud platform for **Cloud Vendor** on the **Import Host** page, you can manage your access keys on the **My Credential** page. Perform the following operations to obtain your AK and SK?

Log in to the management console. In the upper right corner of the page, click the username and choose **My Credentials > Access Keys**. The **Access Keys** page is displayed.

- If you select other cloud vendor on the **Import Host** page, click **How to get?** next to the **Access Key ID field** to go to the specific cloud platform and obtain the AK/SK file as instructed.

9.2.8 What Are the Statuses of a Managed Resource Account in a CBH System?

The status of a managed resource account in a CBH system is used to identify whether the password of the account passes verification. The status cannot be manually changed and can be updated through real-time verification and automatic verification.

A managed account can be in the **Normal**, **Abnormal**, or **N/A** status. For details, see [Table 9-4](#).

Table 9-4 Managed account status description

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

NOTE

Automatic verification

The system automatically checks whether the managed accounts can be used for login and marks the account status at 01:00 on the fifth, fifteenth, and twenty-fifth days of each month.

- If the connection is established and the account can be used for login, its status is **Normal**.
- If the connection cannot be established and the account cannot be used for login, its status is **Abnormal**.

9.2.9 Can I Share Labels of Managed Resources with Other System Users?

No.

CBH systems for different users are isolated from each other. Therefore, a resource label can be used only by the user who defines it.

For example, if a resource label is added by system administrator **admin**, this label is invisible to other administrators or O&M personnel.

9.2.10 Can I Manually Enter a Password to Log In to a Managed Resource Through the CBH System?

Yes. Perform the following steps to set the password login method if you do not want to host your managed resource accounts in CBH:

- Step 1** Log in to the CBH system.
- Step 2** Choose **Policy > ACL Rules** to enter the ACL rule list page.
- Step 3** Click **New** or **Relate**.
- Step 4** When configuring **Relate Account**, select **Empty**.
- Step 5** Choose **Operation > Host Operations**. You are required to enter the account username and password to log in to the managed host.

----End

9.2.11 Why Does the CBH System Fail to Identify Hosts Imported in Batches?

If the CBH system version is earlier than V3.3.0.0, the imported cloud hosts may fail to be identified and the host information cannot be obtained.

You can upgrade the system to the latest version and import the cloud host again. You can also keep the cloud host information in an Excel file.

9.2.12 How Do I Access Services Provided by the Intranet Through a CBH Instance?

Perform the following steps:

Procedure

- Step 1** Buy resources required for deploying an application server, including Windows servers, Linux servers, images, enterprise authorization codes, and client licenses.
- Step 2** Install the application server. For details, see [Installing an Application Server](#).
- Step 3** Add application resources. For details, see [Adding an Application Resource](#).

----End

9.3 Policy Management

9.3.1 What Is Dynamic Approval and How Does It Work?

When an authorized user performs a specific O&M operation, the operation triggers a rule set. The system then intercepts character commands or database sessions based on the rule set and generates an authorization ticket. If the authorized user needs to continue the operation, they need to submit the ticket to the administrator for approval.

The following steps show how to configure the dynamic approval function for command control rules.

- Step 1** Log in to the CBH system as an administrator, choose **Policy > Cmd Rules**. On the displayed page, create a character command control rule and command set (SSH or Telnet).

When creating the command rule, set **Action** to **Dynamic approval**.

- Step 2** After the command control rule is set, the authorized user logs in to the CBH system, logs in to the target host, and runs related commands to trigger command interception. The system generates a command authorization ticket.

Figure 9-2 Dynamic interception

```
Last login: Wed May 29 15:25:33 2019 from 192.168.0.106

Welcome to Huawei Cloud Service

[root@ecs-test-zilliao ~]# ls -al
Command "ls" is rejected. Please submit CommandControl authorization ticket
[root@ecs-test-zilliao ~]# █
```

- Step 3** The authorized user chooses **Ticket > Cmd Ticket** to view and submit the ticket.
- Step 4** The administrator or superior department leader can choose **Ticket > Approve** to view and approve the ticket.
- Step 5** After the ticket is approved, the related command can be executed successfully by the authorized user.

Figure 9-3 Obtaining authorization

```
Last login: Wed May 29 15:25:33 2019 from 192.168.0.106

Welcome to Huawei Cloud Service

[root@ecs-test-zilliao ~]# ls -al
Command "ls" is rejected. Please submit CommandControl authorization ticket
[root@ecs-test-zilliao ~]# █
[root@ecs-test-zilliao ~]# ls -al
total 48
dr-xr-x---. 6 root root 4096 May 29 15:01 .
dr-xr-xr-x. 20 root root 4096 May 29 15:01 ..
-rw-r--r--. 1 root root 31 May 29 16:09 .bash_history
-rw-r--r--. 1 root root 18 Dec 29 2013 .bash_logout
-rw-r--r--. 1 root root 176 Dec 29 2013 .bash_profile
-rw-r--r--. 1 root root 176 Dec 29 2013 .bashrc
drwx----- 3 root root 4096 Feb 27 15:16 .cache
-rw-r--r--. 1 root root 100 Dec 29 2013 .cshrc
-rw----- 1 root root 0 Feb 27 15:17 .history
drwxr-xr-x 2 root root 4096 Feb 27 15:17 .oracle_jre_usage
drwxr----- 3 root root 4096 Feb 27 15:12 .pki
drwx----- 2 root root 4096 May 29 15:01 .ssh
-rw-r--r--. 1 root root 129 Dec 29 2013 .tcshrc
[root@ecs-test-zilliao ~]# █
```

----End

9.4 System Configuration

9.4.1 How Do I Configure an SSH Key for Logging In to a Managed Host?

A CBH system allows you to configure SSH keys for logging in to managed hosts. After an SSH key is configured for a host, the SSH keys are verified preferentially.

Generating an SSH Key

Step 1 Generate an SSH authentication key.

Log in to the host and run the following command to generate an SSH key:

```
ssh-keygen -t rsa
```

The command output is as follows:

```
[root@Server ~]# ssh-keygen -t rsa
Generating public/private rsa key pair.
```

You can configure the SSH key file name and password as required. The following is an example of the command output:

Enter file in which to save the key (/root/.ssh/id_rsa): *Leave this parameter blank or enter the name of the file to be generated. The file is saved in the /root/.ssh directory.*

Enter passphrase (empty for no passphrase): *Leave this parameter blank or enter a password as required.*

Enter same passphrase again: *Confirm the password.*

Your identification has been saved in /home/fdipzone/.ssh/id_rsa.

Your public key has been saved in /home/fdipzone/.ssh/id_rsa.pub.

The key fingerprint is: f2:76:c3:6b:26:10:14:fc:43:e0:0c:4d:51:c9:a4:b2 root@Server

The key's randomart image is:

```
+--[ RSA 2048 ]-----+
| .+=*                |
| . += +             |
| o +                |
| E . . o            |
| .S.                 |
| .o.                 |
| .+                  |
| ..                  |
| .+.                 |
+-----+

```

NOTE

-t rsa indicates that the RSA algorithm is used for encryption. DSA algorithm can also be used, and the command is as follows:

```
ssh-keygen -t dsa
```

Step 2 Run the following command to view the SSH key file:

```
cd /root/.ssh (directory for storing files)
```

In the directory where the SSH key file of the current user is stored, view the generated private key file **id_rsa** and public key file **id_rsa.pub**. After the password is configured, you can also view the private key password **key** and public key password **key.pub**.

Information similar to the following is displayed:

```
[root@Server ~]# cd /root/.ssh/
[root@Server ~]# ll
total 16
-rw----- 1 root root  0 Oct 14 15:47 authorized_keys
-rw----- 1 root root 1679 Nov 15 09:45 id_rsa
```

```
-rw----- 1 root root 430 Nov 15 09:45 id_rsa.pub  
-rw----- 1 root root 1766 Nov 15 09:48 key  
-rw----- 1 root root 430 Nov 15 09:48 key.pub
```

Step 3 In the `/.ssh` directory of the current user, run the following command to copy the public key content to the `authorized_keys` file:

```
cat id_rsa.pub >>authorized_keys
```

Step 4 Enable the SSH key login authentication.

1. Run the following command and modify the `sshd_config` configuration file for **RSAAuthentication** and **PubkeyAuthentication** to take effect and authorize SSH key authentication:

```
vim /etc/ssh/sshd_config
```

2. Press **Esc**, enter `:wq!`, and press **Enter** to save the modification and exit.
3. Run the following command to restart the SSHD service:

```
service sshd restart
```

The process is successfully restarted if the following command output is displayed.

```
Redirecting to /bin/systemctl restart sshd.service
```

----End

Configuring SSH Key Information

Step 1 Log in to the CBH system.

Step 2 Choose **Resource** > **Host**. On the displayed page, create a host resource for which an SSH key has been generated.

NOTE

You can click **Manage** to add an account for the managed host on the host details page.

Step 3 Click **New** to create the SSH host resource, and configure the host **Account** and **Password** on the **Add Account** page.

Step 4 Copy the content of the `id_rsa` private key file and the private key password, and configure **SSH Key** and **passphrase**.

NOTE

passphrase is optional. If **passphrase** is not configured:

- You do not need to enter the password for logging in to the host when no private key password is generated.
- You need to enter the private key password each time you log in to the host when the private key password is generated.

Step 5 Click **OK** to add an account with the SSH key configured to the host resource.

NOTE

- When importing host resources in batches, enter the correct SSH key private key and passphrase. Do not enter unnecessary characters or spaces.
- You are advised to configure only the host account and password for host resources to be imported in batches. After the host resources are imported to the CBH system, change the account and add the private key and password.

Step 6 Configure ACL rules.

Grant the host account configured with the SSH key to users.

Step 7 Log in to the host as an authorized user.

----End

9.4.2 How Do I Set the Personal Net Disk Capacity?

The net disk of a CBH system is the personal net disk for users in the CBH system. If the space of a personal net disk is insufficient, the administrator can configure a larger capacity for **Personal Netdisk**.

- After **Personal Netdisk** is set, the CBH system allocates the same personal net disk capacity for each user in the system.
- To use the personal net disk with no space limitations, set both **Personal Netdisk** and **Total Netdisk** to 0.

Prerequisites

You have obtained the permission to manage the **System** module in the CBH system.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **System > Data Maintain > Storage Mgmt** to go to the storage configuration page.

Step 3 Query the configurations of **Personal Netdisk** and **Total Netdisk** in the **Netdisk** area.

The default settings of **Personal Netdisk** and **Total Netdisk** are **100 MB** and **5120 MB**, respectively.

Step 4 Click **Edit** in the **Netdisk** area. The **Edit Netdisk** dialog box is displayed.

Step 5 Change the value of **Personal Netdisk**.

Step 6 Click **OK** and go back and check the change on **Personal Netdisk**.

----End

9.4.3 How Do I Send More SMS Messages Than the Limit Allowed by CBH

CBH provides free SMS message quota for you. The restrictions are as follows:

- You can send a maximum of one SMS message within 1 minute.
- You can send a maximum of five SMS messages within an hour.
- You can send a maximum of 15 SMS messages within 24 hours.

If you want to increase the message quota, customize an SMS gateway.

9.4.4 How Do I Connect CBH to a Third-Party Email Server?

CBH can connect to email servers on the public network.

Procedure

The following uses a 163 email address as an example.

- Step 1** Log in to the 163 website or email box, go to **Settings**, select **POP3/SMTP/IMAP**, and enable the IMAP/SMTP or POP3/SMTP service.
- Step 2** Enable the email service as prompted.
- Step 3** Scan the QR code with your mobile phone and send an SMS message. Then, click the "sent" button.
- Step 4** Save the generated authorization password and click **OK**.
- Step 5** Log in to the web page of the bastion host and choose **System > System Config > Outgoing > Email**.
- Step 6** Enter the SMTP email server address and the authorization password generated in [Step 4](#). If the test email is sent successfully, the interconnection is successful.

----End

10 Resources Managed in a CBH System

10.1 Operation Management

10.1.1 Can CBH Support GUI-Based O&M for Linux Hosts?

Yes.

 **NOTE**

Before using CBH to manage such servers, [test the VNC connection locally](#). CBH is not responsible for the compatibility of third-party VNC software.

CBH can manage resources with the VNC (Virtual Network Computing) protocol configured, making it possible for you to log in to the graphical user interface of Linux hosts for O&M purposes.

To configure VNC for a managed host, select **VNC** for **Protocol** in the **New Host** dialog box.

10.1.2 Does CBH Support Mobile App O&M?

No. CBH does not support mobile app O&M, but you can access the CBH system using a mobile browser.

Step 1 Open the browser on your mobile phone and enter `https://EIP address of your CBH instance` to go to the login page of the CBH system.

Step 2 Enter the username and password for login authentication.

After a successful login, you can manage system data in departments, users, resources, policies, and system configurations, approve work tickets, and download logs.

 **NOTE**

Using of mobile phone browsers to log in to managed resources through the **Host Operation** and **Application Operation** pages is not support.

----End

10.1.3 How Do I Configure the SSO Tool?

The Single Sign On (SSO) tool is used to log in to managed database resources on the **Host Operation** page.

By default, CBH uses SsoDBSettings as its SSO tool. Before logging in to database resources, install SsoDBSettings and the database client tool on the local host and configure the correct path of the database client on SsoDBSettings.

 **NOTE**

Before logging in to a database, enable the service port by referring to [How Do I Configure a Security Group for a CBH Instance?](#)

The following uses the **Navicat** client as an example to describe how to configure the client path.

- Step 1** Start local SSO Tool SsoDBSettings.
- Step 2** Click the path configuration icon next to **Navicat Path**.
- Step 3** Select the .exe file of the Navicat tool based on the absolute path where the Navicat client is installed, and click **Open**.
- Step 4** Go to the SsoDBSettings SSO tool configuration page and view the selected Navicat client path.
- Step 5** Click **Save** to return to the **Host Operation** page of the CBH system. Then, you can log in to the database.

----End

10.1.4 Does CBH Allow Multiple Users to Log In to the Same Resource Concurrently?

CBH allows multiple users to log in to the same resource at the same time. There is no limit on the number of concurrent users who log in to a managed host. However, in some cases, users are not allowed to log in to the same resource concurrently using the same resource account due to the multi-login configurations of the resource.

For example, the number of users who can log in to a Windows host is limited by the concurrent login configuration of the host. By default, a host running Windows Server 2008 or Windows Server 2012 allows only two users to log in to it concurrently. In this case, a maximum of two users can log in to the Windows host managed in CBH concurrently by default.

To enable more users to log in to a resource concurrently, perform the following operations:

- Configure the resource server to allow multiple users to log in. For example, configure the remote desktop session host and the remote desktop authorization on Windows hosts.
- Create multiple accounts on the resource server, manage them in CBH as resource accounts, and grant these resource accounts to users.

10.1.5 Which Algorithms Are Supported by CBH in SSH O&M Mode

Table 10-1 lists the algorithms supported by CBH 3.3.26.0 and later over SSH.

Table 10-1 Algorithms supported by CBH in SSH mode

Algorithm Type	H5 O&M	Client O&M
Key exchange	diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1	diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 ecdh-sha2-nistp521 ecdh-sha2-nistp384 ecdh-sha2-nistp256
Encryption	aes128-ctr aes192-ctr aes256-ctr aes128-cbc aes192-cbc aes256-cbc 3des-cbc blowfish-cbc arcfour128 arcfour cast128-cbc	aes128-ctr aes192-ctr aes256-ctr aes128-cbc aes192-cbc aes256-cbc 3des-cbc blowfish-cbc arcfour128 arcfour256
HMAC	hmac-md5 hmac-md5-96 hmac-sha1 hmac-sha1-96 hmac-sha2-256 hmac-sha2-512 hmac-ripemd160 hmac-ripemd160@openssh.com	hmac-md5 hmac-md5-96 hmac-sha1 hmac-sha1-96 hmac-sha2-256 hmac-sha2-512

Algorithm Type	H5 O&M	Client O&M
Host key	ssh-rsa ssh-dss	ssh-rsa ssh-dss ecdsa-sha2-nistp256 ecdsa-sha2-nistp384

10.2 O&M Operations

10.2.1 What Login Methods Does CBH Provide?

A CBH system supports automatic login, manual login, and sudo login for managed resources. In addition, CBH supports logging of batches of resources at a time.

Auto Login

When adding a resource to a CBH system, select **Auto Login** and configure the account username and password of the resource to host the account.

With **Auto Login** enabled, O&M personnel can locate the target resource and click **Login** in the **Operation** column on the **Host Operation** or **Application Operation** page to automatically log in to the resource without entering the username and password.

NOTE

- **Auto Login** cannot be configured for applications accessed through Microsoft Edge.
- If an SSH key is configured for an SSH host, the SSH key is preferentially used for login.

Manual Login

If you select manual login or choose to add an account later during resource creation, the system generates the **[Empty]** account for the host or application resource.

O&M personnel need to enter the username and password of the host or application when accessing the resources.

Sudo Login

A sudo account is created for managed resources so that sudo privilege escalation can be configured for common resource accounts.

When O&M personnel access resources using a common account, the CBH system automatically switches to the account with the escalated privileges. In doing this, the common account has the same permissions as those of the account with the escalated privileges.

Batch Login

On the **Host Operation** page, O&M personnel can select multiple host resources and click **Batch Login** in the lower left corner to log in to multiple host resources of different protocol types on one O&M page and manage these resources centrally without repeated logins. This greatly facilitates O&M personnel and improves efficiency.

NOTE

Batch login does not support FTP, SFTP, SCP, DB2, MySQL, Oracle, or SQL Server host resources or host resources configured with manual login or accounts of two-person authorization.

10.2.2 How Do I Create a Collaborative O&M Session?

With the collaborative O&M function, a CBH system allows you to share URLs and invite other users to view the same session during web O&M. Participants can perform operations on the session after being approved by the session creator. This function can be used in scenarios such as remote demonstration and consultation of difficult O&M issues.

NOTE

- Before sharing a collaborative O&M, ensure that the network connection between the CBH system and the managed host is normal. Otherwise, the invited user cannot join the session, and a connection error (code: T_514) is reported on the session page of the creator. The error code T_514 indicates that the server does not respond for a long time and the connection is disconnected, and you need to check your network and try again.
- The invitation URL can be copied and sent to multiple users. Only users with the account permissions of the managed resource can open the invitation URL.
- The invited user can join the session only before the URL expires or the session ends.

Procedure

Step 1 Log in to the CBH system.

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

Step 3 Select the host to be maintained and click **LogIn**.

Step 4 Click **Share** on the right of the dialog box to invite users to join the session.

Step 5 Click **Invite friends** to obtain the invitation URL. Copy the URL and send it to the user who has permissions for account of the managed resource.

Step 6 The invited user then can log in to the CBH system, visit the invitation URL, and view the invitation information.

Step 7 Click **Enter** to join the session.

- Click **Apply for control** to send a request to the current controller to apply for the control permission.
- Click to **Release control** or **Exit session** to hand the session control back to the creator.
- Click **Exit session** to exit the current session. The invited user can join the session again if the invitation URL does not expire and the session remains in progress.

Step 8 The creator and the invited user manage the session together.

- If the creator clicks **Cancel share** or exits the session, the sharing session ends. The invited user is forced to exit the session and cannot access the session again through the URL.
- When an invited user applies for the session control permission, the session creator can click **Agree** to hand over the session control permission or click **Refuse** to reject the application.

----End

10.2.3 How Do I Use Resource Labels in the CBH System?

CBH labels are used to identify managed host and application resources in a CBH system and to identify all resources related to the same managed host or application. After a label is added to a host or application, all resources related to the host or application will be labeled. In this way, you can search for resources by label. A host or application can have a maximum of 10 labels.

Each managed ECS and RDS are tagged with two labels. **Label 1** is identified by team, and **Label 2** and **Label 3** are identified by project. Users can filter resources identified by label.

After adding labels to resources, you can search for resources by label and manage labels in the CBH system. For details, see [Table 10-2](#).

Table 10-2 Label usage in CBH

Entry Path	Operation
Dashboard > Recently Logged Host	Search for resources.
Dashboard > Recently Logged Application	Search for resources.
Dashboard > Recently Logged Host	Search for resources.
Dashboard > Recently Logged Application	Search for resources.
Resource > Host	Add, delete, or edit labels and search for resources by labels.
Resource > Application Publish	Add, delete, or edit labels and search for resources by labels.
Operation > Host Operations.	Add or delete labels and search for resources by labels.
Operation > App Operations.	Add or delete labels and search for resources by labels.

Example of Searching Resources by Label

The following describes how to filter the host resources tagging with label **Proj1** in the host list.

Step 1 Log in to a CBH system.

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

Step 3 Expand the **Label** drop-down list and select the **Proj1** label. You can also search for the label in the search box and select it.

Step 4 In the host list, view the host resources filtered by **Proj1**.

NOTE

You can search for resources by a combination of multiple labels and filter every resource tagged with those labels. For example, if you select labels **Team1** and **Proj1**, hosts with **Team1** and **Proj1** are displayed.

----End

10.2.4 How Do I Set the Resolution of the O&M Session Window When I Use a Web Browser for O&M?

You can adjust the resolution of the O&M session window during the web-based O&M to fit your screen.

Constraints

- This feature is available for Windows hosts and application resources.
- For hosts configured with the VNC protocol, this feature is unavailable.

Prerequisites

- You have obtained the permissions for the **Host Operations** and **App Operations** modules.
- The administrator has authorized the access control permissions to the user account or the permission application ticket has been approved.
- The network connection between the managed host and the system is normal, and the account username and password for logging in to the managed host are correct.

Procedure

As an example, the following describes how to adjust the session window resolution of a Windows host.

Step 1 Log in to the CBH system.

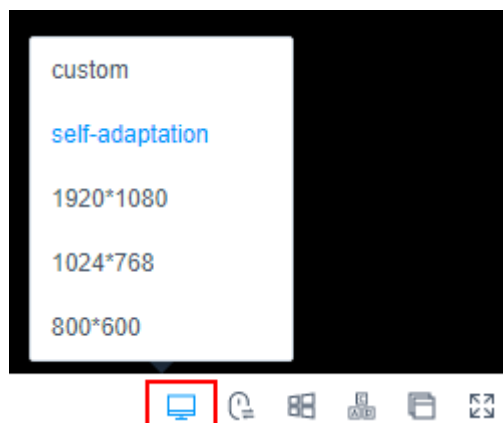
Step 2 Choose **Operation > Host Operations** to go to the **Host Operations** page.

Step 3 Select the target Windows host resource and click **Login** to go to the O&M session window.

Step 4 Click the display icon in the lower right corner of the O&M session window to unfold all resolution options.

Step 5 Select a preset resolution or **self-adaptation**.

- By default, the **self-adaptation** is selected.
- You can set the resolution to **1920 x 1080**, **1024 x 768**, or **800 x 600**.

Figure 10-1 Session window resolution settings**Step 6** Select **Custom**.

1. Click **Custom** to go to the **Resolution** dialog box.
2. Configure the resolution **Width** and **Height**.
3. Click **OK**.

Step 7 After you reselect or customize the resolution, the O&M session window will be reconnected.

After the O&M session window is reconnected, it is displayed at the specified resolution.

----End

10.2.5 How Can I Use Shortcut Keys to Copy and Paste Text When a Web Browser Is Used for O&M?

During the web-based O&M, shortcut keys **Ctrl+C** and **Ctrl+V** are used to copy and paste text. The operations of those shortcut keys vary on the Linux and Windows hosts.

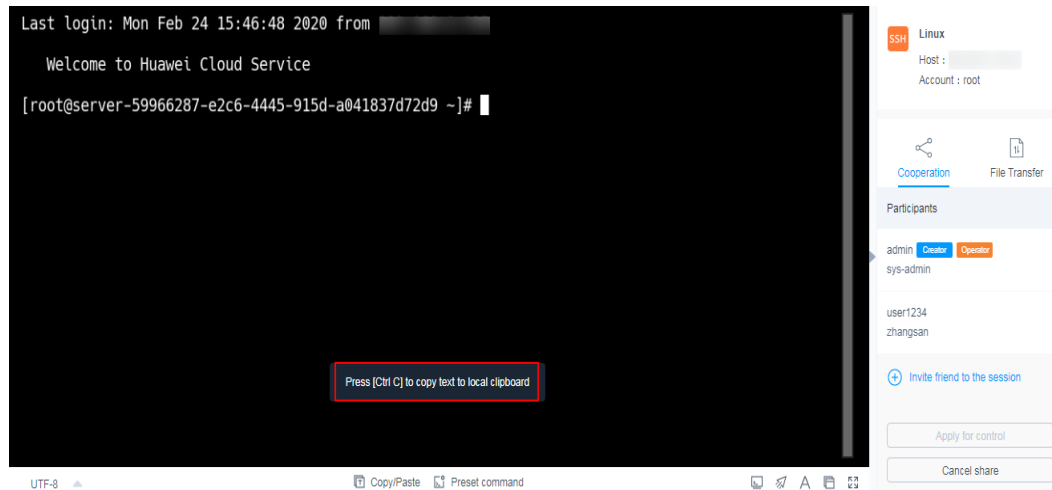
NOTE

- VNC host resources do not support text copy and paste.
- Only SSH, RDP, and Telnet host resources support text copy and paste by pressing **Ctrl+C** and **Ctrl+V**.
- A maximum of 80,000 characters can be copied from a local PC to the CBH system, and a maximum of 1 million characters can be copied from the CBH system to a local computer.
- If only letter **C** is displayed for a replication action, upgrade your CBH to V3.3.40.0 or later.

How to Use Ctrl+C and Ctrl+V in Linux Hosts

Log in to the Linux host to go to the O&M session window. Select the text content, press **Ctrl+C** and then **Ctrl+V** to copy and paste the text.

Figure 10-2 Copying text on a Linux host



How to Use Ctrl+C and Ctrl+V in Windows Hosts

Log in to the Windows host to go to the O&M session window. Select the text content, press **Ctrl+C** twice to copy the text and press **Ctrl+V** to paste the text.

NOTE

Shortcut keys **Ctrl+B** and **Ctrl+G** are used for copying and pasting host files on a Windows host.

10.2.6 What Are the Shortcut Keys for O&M in CBH?

- Shortcut keys used for web O&M are the same as that used in Windows OSs. For example, **Ctrl+C**, **Ctrl+V**, and **Ctrl+X** are used to copy, paste, and cut text in web browser, respectively.
If a web O&M shortcut key conflicts with a browser shortcut key, the browser shortcut key is executed preferentially. You are advised to change the shortcut keys of your browser to avoid such conflicts.
The same web O&M session GUI and shortcut keys are used for application O&M and host O&M.
- For database O&M, the Windows shortcut keys are still applicable because the single sign-on (SSO) tool is used to invoke the local database client.
- Shortcut keys used by the host and client are the same when SSH, FTP, or SFTP client are used for O&M.

10.2.7 Why Is the File List Not Displayed During O&M Using a Web Browser?

Symptoms

When a web browser is used for O&M, the file list is not displayed in some directories in the file transfer area. Other directories can be opened normally.

Solution

CBH cannot identify files with names containing backslashes (\). So, you need to rename these files or folders and make sure no backslashes (/) are included in their names.

11 O&M Log Audit

11.1 What Audit Logs Does CBH Provide?

CBH provides instance and system audit logs.

Instance Auditing

To audit CBH instances, you need to enable Cloud Trace Service (CTS) to record operations on CBH instances. The CTS management console stores the operation records of the last seven days.

For details about instance audit logs, see [CBH Operations Supported by CTS](#).

System Auditing

A CBH system centrally manages user login and provides system logs and system reports. In addition, CBH authorizes users to log in to managed resources and perform O&M operations. CBH provides records of the system and resource O&M, including history sessions and O&M reports. For details, see [Table 2 CBH system logs](#).

Table 11-1 CBH system audit logs

Log Type	Content
History sessions	<ul style="list-style-type: none">O&M session videos: The entire process of O&M sessions is automatically recorded by screencasting. You can play or download the screencasts online.O&M session details: O&M session details generated for different users can be viewed online or exported to an Excel file. Session details include detailed operation records of resource sessions, system sessions, O&M records, file transfer, and collaboration sessions.

Log Type	Content
System logs	<p>CBH displays the number of O&M operations by a specific user over time through line charts and generates comprehensive O&M analysis reports.</p> <p>System logs include 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.</p>
O&M reports	<ul style="list-style-type: none"> 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 reports	<p>CBH collects statistics on user logins and system operations in a bar chart and generates comprehensive system management reports.</p> <p>A system report includes information about user control, user and resource operations, number of user source IP addresses, user login methods, abnormal logins, session control, and user status.</p>

11.2 Can I Download Operation Recordings?

Video files in MP4 format can be downloaded and played on multiple players.

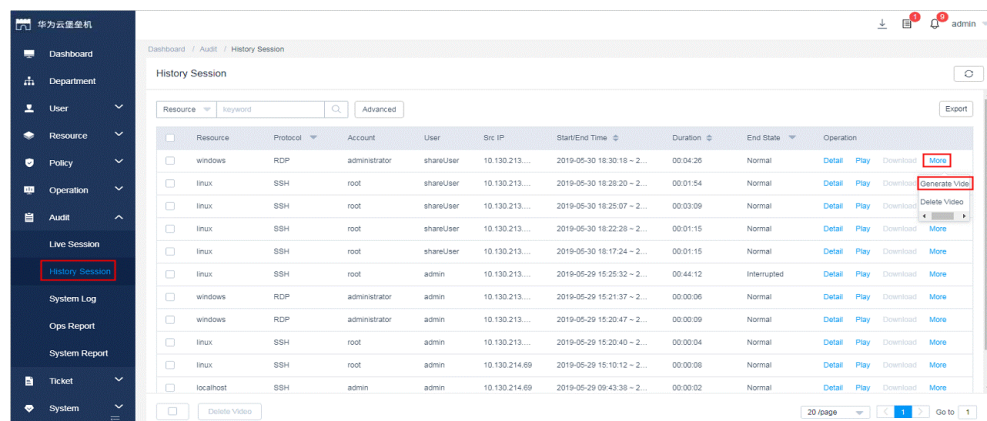
By default, the system does not automatically generate video files for downloading. You can manually generate them. After downloading a video, delete it from the CBH system to avoid occupying too much storage space.

Step 1 Log in to the CBH system.

Step 2 Choose **Audit > History Session**.

Step 3 Click **More** in the **Operation** column and select **Generate Video**.

Figure 11-1 Generating a video



Step 4 After the video is generated, click **Download** in the **Operation** column to save the video to the local computer.

Step 5 After downloading videos, you can delete them from the system cache. To delete a specific video, locate the row where it resides and choose **More > Delete Video** in the **Operation** column. To delete videos in batches, select multiple video files and click **Delete Video** in the lower left corner.

 **NOTE**

The total duration and playable duration of a downloaded video file may be different because the logout time and operation time are different. The total duration refers to the period from the time when a user logs in to a resource to the time when the user logs out of the resource. The playable duration refers to the period from the time when a user logs in to a resource to the time when the user performs the last session operation.

----End

11.3 Can I Delete CBH O&M Data for a Specific Day?

No. You can only delete data generated before a day you specified.

CBH supports automatic deletion and manual deletion of O&M data in the system.

- Automatic deletion: The CBH system automatically deletes the data when the system space usage reaches 90% or data is stored for more than 180 days (maximum default value).
- Manual deletion: You can select a date to delete the data generated before the selected date. You cannot delete the data of a specific day.

 **NOTE**

Data that is not backed up cannot be restored after being deleted. You are advised to back up important data. For details, see [Backing Up System Configurations](#).

11.4 Can I Back Up System Audit Logs to an OBS Bucket?

Yes.

You can back up CBH system audit logs to OBS buckets or cloud servers on the same VPC using an FTP or SFTP server.

For details about how to back up system audit logs, see [Which Types of System Data Can Be Backed Up in the CBH System?](#)

11.5 How Long Can I Store Audit Logs in the CBH System?

If the data disk usage of the CBH system is less than 90%, system audit logs can be stored for up to 180 days by default.

Auto Deletion is enabled in the CBH system by default. The CBH system automatically deletes history logs based on the log storage history and system storage space usage.

You can change the log storage duration in **Auto Deletion** configuration. If the system data disk space is large enough, you can prolong the storage duration of system audit logs or even keep system audit logs for ever.

For more details about system data backup, see [How Can I Back Up CBH System Data?](#)

11.6 How Are Audit Logs in the CBH System Processed?

CBH system audit logs are stored in the system data disk. **Auto Deletion** is enabled by default. Therefore, the CBH system automatically deletes historical logs based on the log storage period and system storage space usage.

The automatic log deletion mechanism is as follows:

- The system automatically deletes historical logs older than 180 days.
- If the system storage space usage is higher than 90%, the system automatically deletes the earliest logs by day until the usage of the system storage space is lower than 90%.
- Audit logs generated on the current day are not deleted.

NOTE

- You can also configure **Manual Deletion** to manually delete historical logs generated on and before a specific day.
- You are not advised to disable the **Auto Deletion** function. If the storage space usage exceeds 95%, the system may be faulty and cannot be used.

11.7 Why Is the Playable Duration Shorter Than the Total Duration of a Session?

In an audit video, CBH logs a session from the time when a user logs in to a resource to the time the last command is executed. No data is recorded for the duration from the completion of the last operation to the close of the session. So, if the logout time and the last operation time are different, the total session duration and playable duration of a video are different.

For example, when you log in to a resource using a web browser, the total session duration is 30 minutes. The last command is executed in the fifth minute, and no operation is performed till the session is closed. The total session duration is still 30 minutes. However, only the first 5 minutes are playable because the last 25 minutes are not recorded.

NOTE

- The total duration starts from the time when a system user logs in to a resource to the time they log out of the resource.
- The playable duration starts from the time a system user logs in to a resource to the time the last session is completed.

11.8 Why Is There No Login Record in History Sessions While I Received a Resource Login Message?

To verify connectivity between CBH and managed hosts, the CBH background system starts automatic inspections by logging in to all managed hosts using the managed host accounts at 01:00 on the fifth, fifteenth, and twenty-fifth days of each month. After the verification completes, the **admin** user will receive a message indicating that resources have been logged in.

However, no task is generated for such logins. Therefore, no login record is generated in historical sessions.

12 Troubleshooting

12.1 CBH System Login Failures

12.1.1 How Do I Handle Login Exceptions?

Symptoms

- The IP address of CBH cannot be connected. As a result, the web page of CBH fails to be displayed and the CBH system cannot be logged in through the Internet.
- The CBH system page cannot be displayed after the login.
- The system displays a message indicating that the authorization fails to take effect.
- The CBH system cannot be logged in by users who are authenticated through the AD domain server.
- The CBH system is inaccessible through password logins and public IP addresses.

Possible Causes

Cause 1: The disk space of the CBH system is insufficient.

Cause 2: The CBH version is not updated to the latest one. As a result, the disk space may be occupied and not released.

Cause 3: The browser you used for logins is incompatible with the CBH system.

Cause 4: An improper security group is configured for the CBH instance.

Cause 5: An inappropriate network ACL rule is configured in the VPC where the CBH instance is deployed, or the IP address for logging in to the CBH system is restricted by the network ACL.

Cause 6: SSL encryption authentication is not disabled when AD domain authentication is configured.

Cause 7: The CBH system version is not the latest one.

Solutions

Solution to cause 1

- Enable **Manual Deletion** and periodically delete historical data such as logs and videos generated before a specified date. Enable **Auto Deletion** to let the system automatically delete logs when the disk space is full to ensure abundant disk space. For details, see [Storage Configuration](#).
- [Change CBH instance specifications](#) to meet the requirements of large-capacity disks.
- You are advised to configure the disk space usage alarm notification. When the disk space usage exceeds the threshold, the system sends an alarm notification. For details, see [Alarm Configuration](#).

Solution to cause 2

- On the CBH console, restart the CBH instance and check whether the fault is rectified. If the problem persists, upgrade the CBH instance to the latest version and change specifications as required.

Solution to cause 3

- Use other browser or upgrade the browser version. The browser of a required version is recommended for web login. For details, see [Logging In to a CBH System](#).

Solution to cause 4

- [Check the security group rules, configure the security group rules](#) based on the CBH suggestions, and log in to the CBH system again.

Solution to cause 5

- [Check the network ACL rule](#). If the ACL configuration is incorrect, enable the inbound and outbound ports by referring to the [CBH security group rule](#) and log in to the CBH system again.
- [Check the network ACL rule](#). If the login IP address of the CBH instance is restricted by the network ACL, reconfigure the ACL rule to allow the elastic IP address of the CBH instance to be accessed.

NOTE

To log in to a CBH instance using a browser, enable TCP port 443 in the inbound direction. To log in to a CBH instance using an SSH client, enable TCP port 2222 in the inbound direction.

Solution to cause 6

- Log in to the CBH system as user **admin**, reconfigure the [AD domain authentication](#), and cancel the SSL encryption authentication.
- Check whether the user's login IP address and MAC address are blacklisted. For details, see [Configuring User Login Restrictions](#).
- Check whether the user login IP address is restricted by ACL rules. For details, see [ACL Rules](#).

Solution to Cause 7:

Upgrade the CBH system version by referring to [Upgrading the Version of a CBH System](#).

If the problem persists, click **Service Tickets** in the upper right corner of the management console and submit a service ticket.

12.1.2 Why Is the IP Address or MAC Address Blocked When I Log In to the CBH System?

Symptoms

- The system prompts that the login IP address is forbidden when a user logs in to the CBH system using a web browser.
- The system prompts that the login MAC address is forbidden when a user logs in to the CBH system using a web browser.

Possible Causes

The CBH system restricts the login with IP addresses or MAC addresses. The IP addresses or MAC addresses are blacklisted.

Solutions

Contact the administrator to check the login IP address restrictions and check whether a blacklist or whitelist is configured for MAC address and IP address restriction.

- If a whitelist is configured, use a server whose IP address or MAC address is whitelisted.
- If a blacklist is configured, use a server whose IP address or MAC address is not restricted.

12.1.3 Why Am I Seeing Error Code 404 When I Log In to the CBH System?

Symptoms

The error message "/3.0/AUTHSERVICE/CONFIG-404 service error occurs" is displayed when a user logs in to a CBH system using a web browser.

Possible Causes

The available data disk space is insufficient.

Solutions

- Add a separate system data disk and restart the CBH system.
- Change the CBH instance specifications to improve the overall system performance.

 NOTE

The existing system disks and data disks cannot be expanded. You can attach additional data disks to the system. New disks are automatically attached after the CBH system restarts.

12.1.4 Why Am I Seeing Error Code 499 When I Log In to the CBH System?

Symptoms

The error message `"/3.0/profileService/freshProfile 499: service error occurs"` is displayed when a user logs in to a CBH system using a web browser.

Possible Causes

The CBH system is unavailable because the mapped CBH instance is in the **Restarting** status.

Solutions

Log in to the CBH system after the CBH instance is restarted.

12.1.5 What Are Possible Faults If I Log In to the CBH System as an Intranet User?

Scenarios

- After you log in to the CBH system on the intranet, a black screen will display and icons are not completely displayed.
- After you log in to the CBH system on the intranet, the network may abruptly disconnect or become unstable.
- When you log in to the CBH system on the intranet, the request is redirected to another link.
- The CBH system cannot be logged in, and the message "Network exception. Check the network configuration." is displayed.

Possible Causes

A proxy server is configured for your company. As a result, the CBH system cannot be connected.

Solution

After a proxy server is configured to block requests, apply for whitelisting the IP address of your CBH system.

12.1.6 Why Is a Host Inaccessible Through CBH?

Symptom

- **Symptom 1:** The managed host resource was inaccessible through the **admin** user in CBH.
- **Symptom 2:** The managed host resource was accessible through the **admin** user but inaccessible through other users in CBH.

Possible Causes

- **Cause of symptom 1:** A non-RDP protocol was configured for the managed host resource while forcible RDP connection was enabled for the host resource (**admin console** was selected for connection mode).
- **Cause of symptom 2:**
 - The number of RDP connections between CBH and the managed host resource has reached the upper limit of the Windows Remote Desktop connections.
 - The logged-in user for managing Windows resources is not user **admin**.

Solutions

- **Solution to symptom 1:** Deselect the **admin console** connection mode by following the instructions provided in "Enabling Forcible RDP Connections."
- **Solution to symptom 2:** Select the **admin console** connection mode by following the instructions provided in "Enabling Forcible RDP Connections."

12.1.7 Why Does CBH Login Fail Through an ECS in a New VPC Connected with the VPC Where CBH Is via VPN or a VPC Peering Connection

Symptom

1. A VPC with a 10.xx.xx.xx CIDR block was selected for a CBH instance.
2. This VPC was connected to another VPC with a 192. xx.xx.xx CIDR block via a VPN or VPC Peering connection.
3. The CBH system can be accessed through the ECSs in the VPC with a 10.xx.xx.xx CIDR block.
4. There is a low probability that the CBH system cannot be accessed through the ECS in the VPC with a 192.xx.xx.xx CIDR block.
5. The route in the red box in the following figure was displayed in the network configurations of the CBH system.

Figure 12-1 Network configuration

Destination	Subnet Mask/Prefix	Next Hop	Route type	Outgoing	Metric	Remarks	Operation
0.0.0.0	0.0.0.0	192.168.0.1	Static	eth1	0	-	Delete
0.0.0.0	0.0.0.0	192.168.0.1	Direct	eth1	101	-	
100.84.0.0	255.192.0.0	172.16.0.1	Static	eth0	1	-	Delete
169.254.169.254	255.255.255.255	172.31.255.254	Direct	eth0	100	-	
172.16.0.1	255.255.255.255	0.0.0.0	Direct	eth0	1	-	
192.168.0.0	255.255.255.0	0.0.0.0	Direct	eth1	101	-	

Possible Causes

The CBH system uses a version earlier than 3.3.26.0. In versions earlier than 3.3.26.0, if a CBH system has a large number of requests, threads may be exceptionally stopped during system status checks. As a result, routes may fail to be refreshed, and request traffic is forwarded to ETH0 and then discarded. Login failures then occur.

Solutions

Upgrade the bastion host version to 3.3.26.0..

12.2 CBH Managed Resource Login Failures

12.2.1 Why Does an Exception Occur When I Log In to My Resources Managed in CBH?

Symptoms

- A black screen is displayed when a user attempts to log in to a managed resource.
- The host fails to be connected or is unreachable when a user attempts to log in to the managed resource.
- Resources managed with CBH cannot be logged in through CBH.

Possible Causes

Cause 1: The managed host responds slowly, and the network connection is abnormal.

Cause 2: The shared bandwidth of CBH does not meet user requirements.

Cause 3: The authorization of the related services on the host expires. For example, the Windows authorization expires, or the 120-day RDP service authorization expires.

Cause 4: The CBH instance and the managed host are not in the same VPC.

Solutions

Solution to cause 1

- Restart the managed host. The network recovers after the managed host is restarted. Log in to the CBH system and [check the network connection](#) between CBH and the managed host.
- If the fault persists after the host is restarted, check based on [ECS Failures or Slow ECS Responses](#).

Solution to cause 2

- Reconfigure the bandwidth of the EIP bound to the CBH instance. It is recommended that the bandwidth be greater than 5 Mbit/s. For details about the EIP bandwidth, see [How Do I Check Whether the Bandwidth Exceeds the Limit?](#)
- Rectify the configuration and restart the CBH system.

Solution to cause 3

Renew the expired services on the managed host to obtain required authorization and log in to the managed hosts through CBH again.

Solution to cause 4

CBH can only directly manage resources in the same VPC as that of the CBH instance.

Although you can establish cross-region or cross-VPC network connections between a CBH instance and resources, such connections may be not stable enough for using the CBH system. If you really need to use CBH for cross-VPC or cross-region resource management, you can:

- Use a [VPC peering connection](#) to connect two VPCs.
- Use a [Cloud Connect \(CC\)](#), [Virtual Private Network \(VPN\)](#), or the like, to establish a cross-region network connection.

Solutions to Other Errors

- [Why a Login Error \(Code: T_514\) Occurs?](#)
- [Why a Login Error \(Code: C_515\) Occurs?](#)
- [Why a Login Error \(Code: C_519\) Occurs?](#)
- [Why a Login Error \(Code: C_769\) Occurs?](#)

If the problem persists, click **Service Tickets** in the upper right corner of the management console and submit a service ticket.

12.2.2 Why Am I Seeing Login Errors of Code: T_514 When I Use a Web Browser for Resource O&M?

Symptoms

When a user attempts to log in to a resource using a web browser, the login page fails to load. A login error (**Code T_514**) is reported, indicating that the session is

disconnected because the server does not respond for a long time and the user needs to check network and try again.

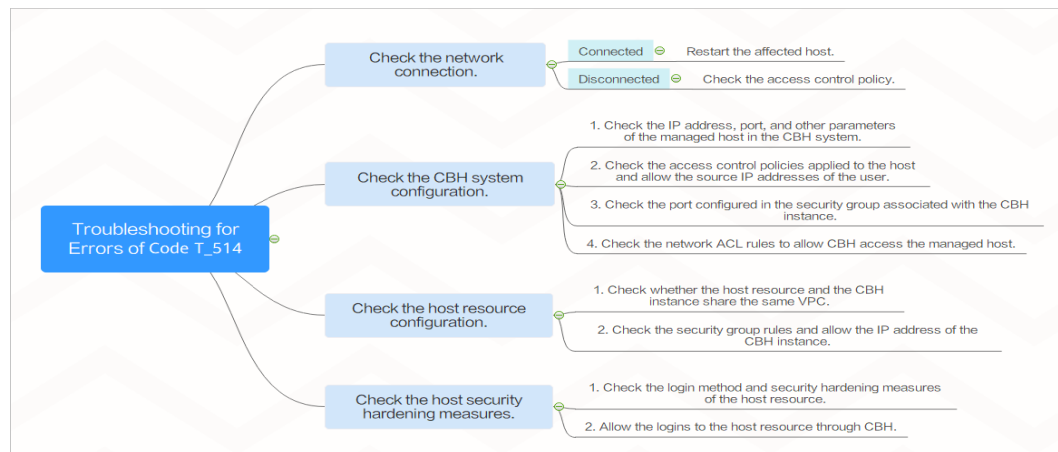
Possible Causes

- The network connection between the CBH system and the managed host is unstable.
- The network between the CBH system and the managed host is blocked.
- The managed host does not respond, leading to network disconnection.

Mind Map for Troubleshooting

Refer to the following map to locate the causes and fix the Code T_514 login error you encountered.

Figure 12-2 Mind map for troubleshooting



Check the Network Connection

Log in to the CBH system, **ping the managed host**, and check whether the network connection is normal.

- If the network connection is normal, the login failure may be caused by unstable connections.
Restart the corresponding managed host. If the network recovers after the host is restarted, no further action is required. If the fault persists after the host is restarted, check by referring to **ECS Failures or Slow ECS Responses**.
- If the network connection is abnormal, the network between the CBH system and the managed host is restricted. Perform the following operations to rectify the fault:
 - a. Check whether the current user is an intranet user and whether the user's access permission is restricted.
For example, intranet users cannot access public network resources. They need to apply for the Internet access permission or WebSocket permission to access managed hosts.
 - b. **Check the CBH System Configuration**

c. [Check the Host Resource Configuration](#)

Check the CBH System Configuration

- Step 1** Log in to the CBH system and check whether the IP address and port number of the managed resource are correct.
- Step 2** Check whether IP address restriction is configured in the access control policy associated with the resource. Modify an ACL Rule to remove the restriction on the source IP address of the user.
- Step 3** Check the security group associated with the CBH instance and check whether the port configuration of the security group is correct. You are advised to configure a security group for a CBH instance based on the recommended CBH ports.

If you log in to the managed host using a web browser, manually add an inbound rule that allows unrestricted access to TCP port 443 in the CBH instance security group.

- Step 4** Check whether the network ACL associated with the CBH instance on the intranet is correctly configured.

Remove the access restriction on the IP address of the CBH instance and add the resource IP address to the destination address to allow the CBH instance to access resources.

- Step 5** After the reconfiguration, log in to the managed host again through the CBH system.

----End

Check the Host Resource Configuration

- Step 1** Log in to the management console of the managed host as the administrator.
- Step 2** Check whether the host resource and the CBH instance are in the same VPC and region. The CBH instance can only directly access resources in the same VPC and region.
- Step 3** Check whether the security group rules associated with the managed host are properly configured.

Remove the access restriction on the IP address of the CBH. Add the IP address of the CBH to the source address to allow CBH to access resources.

- Step 4** After the reconfiguration, log in to the managed host again through the CBH system.

----End

Check the Host Security Hardening Measures

- Step 1** Log in to the managed host as an administrator.
- Step 2** Check the login method and login security hardening measures of the managed host by referring to the following content:

- [Enhancing Security for SSH Logins to Linux ECSs](#)

- [Windows ECS Login Overview](#)
- [Linux ECS Login Overview](#)

Step 3 Remove the login restriction by referring to the following content:

- [Why Cannot I Log In to My Linux ECS?](#)
- [Why Cannot I Log In to My Windows ECS?](#)

Step 4 After removing the security hardening restrictions, log in to the managed host through the CBH system again.

----End

If the problem persists, click **Service Tickets** in the upper right corner of the management console and submit a service ticket.

12.2.3 Why Am I Seeing Login Errors of Code: T_1006 When I Use a Web Browser for Resource O&M?

Symptoms

When a user attempts to log in to a resource using a web browser, a login error (**Code: T_1006**) is reported, indicating that the network connection has been disconnected and the user needs to try again.

Possible Causes

- The network connection between the CBH system and the managed host is unstable.
- The bandwidth of CBH or the managed host exceeds the limit.
- The managed host is slow.

Solution

Log in to the CBH system, [ping the managed host](#), and check whether the network connection is normal.

- If the network connection is still abnormal, the network between the CBH system and the managed host is restricted. Rectify the fault by following [Why a Login Error \(Code: T_514\) Occurs?](#)
- If the network connection is normal, unstable network causes network disconnection.

Restart the managed host. The network recovers after the managed host is logged in again. If the fault persists after the host is restarted, perform the following operations:

- a. Check whether the bandwidth of the CBH instance and host exceeds the upper limit.
- b. Check whether the host resource is slow by referring to [Troubleshooting Slow Linux ECSs](#) or [Troubleshooting Slow Windows ECSs](#).

If the problem persists, click **Service Tickets** in the upper right corner of the management console and submit a service ticket.

12.2.4 Why Am I Seeing Login Errors of Code: C_515 When I Use a Web Browser for Resource O&M?

Symptoms

When a user attempts to log in to a Linux or Windows host using a web browser, a login error (**Code: C_515**) is reported, indicating that an error occurs and the user can try again or contact the administrator.

Possible Causes

- Cause 1: The number of incorrect password attempts exceeds the upper limit for Linux hosts. As a result, the CBH IP address is added to the **/etc/hosts.deny** file.
- Cause 2: Host Security Service (HSS) is enabled on the Linux host. After multiple login attempts with incorrect passwords, the internal IP address of CBH is added to the **/etc/sshd.deny.hostguard** file by HSS.
- Cause 3: CBH does not support the SSH algorithms used by host OSs. (Only for CBH earlier than V3.3.38)
- Cause 4: The firewall is enabled on the Windows host. So the network between the bastion host and the host cannot be connected.

Removing Restriction from /etc/hosts.deny

Step 1 Log in to the Linux Server as an administrator.

Step 2 Run the following command to view the **/var/log/secure** log and check whether the host rejects the IP address of the CBH instance:

```
cat /var/log/secure
```

Step 3 Run the following command to edit the **/etc/hosts.deny** file and delete the IP address of the CBH instance from the file:

```
vim /etc/hosts.deny
```

Step 4 (Optional) Whitelist the CBH IP address.

To use the CBH instance properly, run the following command to edit the **/etc/hosts.allow** file on the Linux host and allow all CBH IP addresses to log in to the host:

```
vim /etc/hosts.allow
```

```
----End
```

Removing IP Address Restrictions from HSS

Step 1 View the **/etc/sshd.deny.hostguard** file.

1. Log in to the Linux Server as an administrator.
2. Run the following command to query the **/etc/sshd.deny.hostguard** file:

```
cat /etc/sshd.deny.hostguard
```

3. Run the following command to open the `/etc/sshd.deny.hostguard` file:
vim /etc/sshd.deny.hostguard
4. Check whether the `/etc/sshd.deny.hostguard` file contains the CBH internal IP address.

Step 2 On the HSS management console, remove the IP address restriction.

1. Log in to the HSS console.
2. Choose **Intrusions > Events**.
3. In the **Alarm Statistics** area, click **Blocked IP Addresses**.
4. Locate and select the row that contains the CBH internal IP address, and click **Unblock** above the upper left corner of the list.

Step 3 (Optional) Whitelist the CBH IP address.

On the HSS console, whitelist the CBH IP address on the Linux server.

----End

 **NOTE**

Using CBH to [manage passwords of host accounts](#) and periodically [synchronize accounts](#) can prevent the CBH IP address from being blacklisted caused by entering incorrect passwords or using of unsynchronized zombie accounts.

Removing SSH Algorithm Restrictions

Step 1 Check the server configuration file `/etc/ssh/sshd_config`.

1. Log in to the Linux Server as an administrator.
2. Run the following command to query the `/etc/ssh/sshd_config` file:
cat /etc/ssh/sshd_config
3. Run the following command to open the `/etc/ssh/sshd_config` file:
vim /etc/ssh/sshd_config

Step 2 Modify the algorithm by adding the following command to the end of the **HostKeyAlgorithms** line:

ssh-rsa,ssh-dss

 **NOTE**

If the **HostKeyAlgorithms** line cannot be found in your default configuration file, use this command instead: **HostKeyAlgorithms ssh-rsa,ssh-dss**.

Step 3 Run the following command to restart the SSH service:

systemctl restart sshd

----End

Whitelisting the IP Address of the Bastion Host

For Windows server login failure caused by firewall settings, whitelist the IP address of the bastion host on the firewall.

12.2.5 Why Am I Seeing Login Errors of Code: C_519 When I Use a Web Browser for Resource O&M?

Symptoms

When a user attempts to log in a managed host using a web browser, a login error (Code: C_519) is reported, indicating that the resource cannot be accessed because the resource connection fails or the resource is unreachable. If the problem persists, contact the system administrator or check the system log.

Possible Causes

- The network is broken because the network connection between the CBH system and the resource server is abnormal.
- The connection is broken because the network between the CBH system and the managed host is blocked.
- The connection is unreachable because the server does not respond.

Check the Network Connection

Log in to the CBH system, [ping the managed host and TCP port](#), and check whether the network connection is normal.

- If the network connection is normal, unstable network causes network disconnection.
Restart the managed host. The network recovers after the managed host is restarted. If the fault persists after the host is restarted, check by referring to [ECS Failures or Slow ECS Responses](#).
- If the network connection is still abnormal, the network between the CBH system and the managed host is restricted. Perform the following operations to rectify the fault:
 - a. Check whether the current user is an intranet user and whether the user's access permission is restricted.
 - b. [Check Whether the CBH System Environment Is Properly Configured](#)
 - c. [Check Whether the Managed Host Is Properly Configured](#)
 - d. [Checking Whether the Managed Host Can Be Accessed by the CBH System](#)

Check Whether the CBH System Environment Is Properly Configured

- Step 1** Log in to the CBH system and check whether the IP address and port number of the managed resource are correct.
- Step 2** Check whether IP address restriction is configured in the access control policy associated with the resource. [Modify ACL rules](#) to remove the restrictions on the source IP address of a user.
- Step 3** Check the security group associated with the CBH instance and check whether the port configuration of the security group is correct. It is recommended that you [configure CBH instance security group](#) based on the recommended CBH ports.

If you log in to the managed host using a web browser, manually add an inbound rule that allows all access to TCP port 443 in the security group to which the CBH instance belongs.

- Step 4** Check whether the network ACL associated with the CBH instance on the intranet is correctly configured.

Remove the access restriction on the IP address of the CBH instance and add the resource IP address to the destination address to allow the CBH instance to access resources.

- Step 5** After the reconfiguration, log in to the managed host again through the CBH system.

----End

Check Whether the Managed Host Is Properly Configured

- Step 1** Log in to the management console of the managed host as an administrator.

- Step 2** Check whether the host resource and the CBH instance are in the same VPC and region. The CBH instance can only directly access resources in the same VPC and region.

- Step 3** Check whether the security group rules associated with the managed host are properly configured.

Remove the access restriction on the IP address of the CBH. Add the IP address of the CBH to the source address to allow CBH to access resources.

- Step 4** After the reconfiguration, log in to the managed host again through the CBH system.

----End

Checking Whether the Managed Host Can Be Accessed by the CBH System

- Step 1** Log in to the managed host as an administrator.

- Step 2** Run the **route -n** command to check whether the CBH route is missing from the routing table.

- Step 3** Check the login method and login security hardening measures of the managed host by referring to the following content:

- [Enhancing Security for SSH Logins to Linux ECSs](#)
- [Windows ECS Login Overview](#)
- [Linux ECS Login Overview](#)

- Step 4** Remove the login restriction by referring to the following content:

- [Why Cannot I Log In to My Linux ECS?](#)
- [Why Cannot I Log In to My Windows ECS?](#)

- Step 5** After removing the security hardening restrictions, log in to the managed host through the CBH system again.

----End

If the problem persists, click **Service Tickets** in the upper right corner of the management console and submit a service ticket.

12.2.6 Why Am I Seeing Login Errors of Code: C_769 When I Use a Web Browser for Resource O&M?

Symptoms

When a user attempts to log in to a managed host resource using a web browser, a login error (**Code: C_769**) is reported, indicating that the account username, password, or key is incorrect.

Checking Managed Host Account Passwords

- Step 1** Log in to the CBH system, select the target Linux host, [export managed accounts](#), and obtain the host account username and password.
- Step 2** Log in to the ECS management console, log in to the Linux host [using VNC](#), and verify the host account username and password.
- If the login fails, the host account password is incorrect. [Change the account password for the Linux host](#), reconfigure the password of the corresponding resource account in CBH, and [verify the account](#).
 - If the login is successful, [Check Whether Two-Factor Authentication Is Enabled on the Linux Host](#) and [Check Whether the Linux Host Rejects the Login of User root](#).

----End

Check Whether Two-Factor Authentication Is Enabled on the Linux Host

When a dynamic password is required for logging in to a Linux host, the two-factor authentication function of Host Security Service (HSS) is enabled on the Linux host.

In this case, disable two-factor authentication for the Linux host by referring to [HSS Two-Factor Authentication](#).

After that, log in to the managed Linux host again through the CBH system.

Check Whether the Linux Host Rejects the Login of User root

In the sshd service configuration file `/etc/ssh/sshd_config`, if `PermitRootLogin` is set to `no`, the user `root` is not allowed to log in to the Linux host.

Step 1 Log in to the Linux host and check the configuration file of the sshd service.

Step 2 In the `/etc/ssh/sshd_config` file, find the `PermitRootLogin` parameter, and check whether the parameter value is `no`. If yes, go to the next step.

Step 3 Modify the `/etc/ssh/sshd_config` file.

Find the `PermitRootLogin` parameter and change its value to `yes` or comment out the line where the parameter is located.

```
#PermitRootLogin no
```


Step 4 Run the following command to restart the SSHD service:

```
systemctl restart sshd
```

----End

After the preceding operations are complete, log in to the Linux host through the CBH system again.

Check Whether the 120-Day Free Trial Period of the Windows Server Expires

Check method: Remotely log in to the target Windows ECS from a Windows ECS on the intranet and check whether the following error message is displayed: "The remote session was disconnected because there are no Remote Desktop License Servers available to provide a license. Please contact the server administrator."

In this case, the 120-day RDS free trial expires. There is a default grace period of 120-day free trial for Windows ECSs. After the free trial period expires, pay for the service. Otherwise, the remote connection will fail.

Solution: Activate and authorize the server again by referring to [activate the server](#).

If the problem persists, click **Service Tickets** in the upper right corner of the management console and submit a service ticket.

Enabling Forcible RDP Connections

When the number of Windows remote desktop connections exceeds the upper limit, no more remote connections with the host resources can be established. In this case, you can enable the **admin console** in the CBH system to implement force logins. This means you can force the CBH system to establish login connection by forcibly logging out other logged in users.

Step 1 Log in to your bastion host.

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

Step 3 Click **Web OPS Settings**. The configuration window is displayed.

Step 4 Select the **admin console** connection mode.

Step 5 Click **OK** to return to the **Host Operations** page.

After the configuration is successful, when a user attempts to log in to an RDP host, even if the number of connections exceeds the upper limit, logins of this user will be successful at the cost of forcible logouts of other users.

----End

Checking the Bastion Host Image Version

Check method: Log in to the bastion host and choose **System > About** and check whether **Device System** is 3.3.54.0.

If yes, the keyboard may be enabled on the server.

Solution

- CentOS: Set **ChallengeResponseAuthentication** in the server configuration file `/etc/ssh/sshd_config` to **no**.
- Ubuntu: Set **KbdInteractiveAuthentication** in the server configuration file `/etc/ssh/sshd_config` to **no**.

Checking Whether the OS of a Resource Is SUSE Linux Enterprise Server (SLES)

Step 1 Check whether the resource OS is SLES.

```
cat /etc/os-release
```

If the following information is displayed, the resource runs SLES.

```
NAME="SLES"  
VERSION="12-SP3"  
ID="sles"  
ID_LIKE="suse opensuse"
```

Step 2 If the resource runs SLES, change the value of **PasswordAuthentication** to **yes** and that of **ChallengeResponseAuthentication** to **no**, save the settings, and exit.

```
/etc/ssh/sshd_config
```

```
----End
```

12.2.7 Why Cannot I See the Accessible Resources in the Resource List?

Symptoms

The managed resources that are listed on the **Host Ops** or **Application Ops** page suddenly becomes invisible.

Possible Causes

- **Period of Validity** is set in the ACL Rule related to the resource. Therefore, users' access permissions become invalid.
- **Logon Time Limit** is set in the ACL rule related to the resource, which specifies the login period. Users cannot view managed resources during the **Forbidden** login period.
- The user or resource related to the ACL rule is removed. As a result, user's access permission is canceled.
- The ACL rule related to the resource is disabled. Therefore, the user loses the access control permission to the resource.
- The ACL rule related to the resource is deleted. Therefore, the user loses the access control permission to the resource.

Solutions

View details about the **ACL Rule** related to the resource. Reconfigure or create an ACL rule based on site requirements.

- Modify the basic information about the ACL rule and reconfigure the **Period of Validity** or **logon Time Limit**.

- Enable the disabled ACL rule.
- Modify the ACL rule details and relate the user or resource to the modified ACL rule again.
- If the ACL rule is deleted, create another ACL rule and relate it to users and resources.

12.2.8 Why Does the Session Page Fail to Load When I Log In to the Managed Host Using a Web Browser?

Symptoms

When a user attempts to log in to a managed resource in CBH, the O&M session page fails to load.

Possible Causes

The browser blocks the request or the system SSL certificate has expired.

Removing the Browser Blocking Restrictions

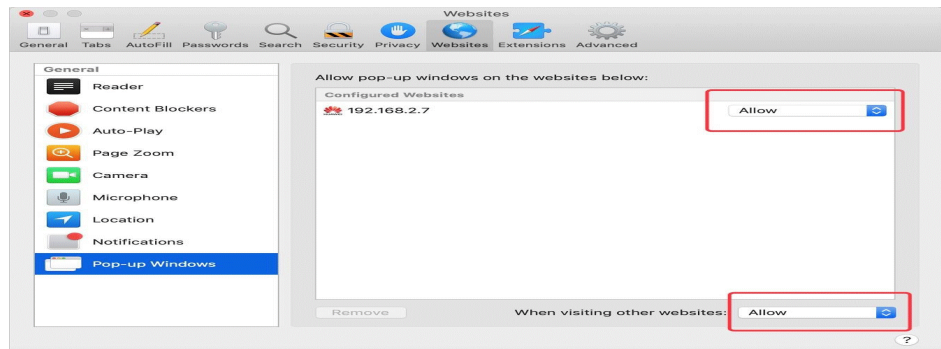
1. Check whether the browser is a recommended one.

Table 12-1 Recommended browsers

Browser	Version
Edge	44 or later
Google Chrome	52.0 or later
Safari	10 or later
Mozilla Firefox	50.0 or later

2. Open the browser, view the messages in the upper right corner of the address bar, and check whether the page is blocked by the browser.
3. Disable the pop-up window blocking.
 - Use Google Chrome browser as an example. In the Windows OS, select **Edit Popup Blocker Options** and deselect **Block Pop-up windows** to log in to the resource.
 - In the macOS, set the preference of the Safari browser. Choose **Websites > Pop-up Windows**. Select **Allow** to allow pop-up windows.

Figure 12-3 Restrictions on Safari



Updating the System SSL Certificate

A CBH system is configured with a secure self-issued certificate by default. There are restrictions on the authentication protection scope and time limit of the self-issued certificate. To better protect your CBH system, you can replace the self-issued certificate with your own SSL certificate. However, if the self-issued certificate expires or fails to pass the security scanning, update it to ensure the CBH system security.

12.2.9 Why Is the Application Resource Inaccessible through CBH?

Incorrect Startup Path of the Application Publish Program

Symptoms

After a user configures an application resource, the user cannot access the resource through the CBH system.

Possible Causes

- Cause 1: The startup path of the application is incorrect.
- Cause 2: The application type is not supported by CBH, so it cannot be called.

Solutions

- Modifying the configured **Program Path**
 - a. Log in to the CBH system. On the application server details page, view the **Program Path** configured for the application server.
 - b. Log in to the Windows application server, query the application installation path, and obtain the exe startup path.
 - c. Ensure that the configured **Program Path** and the queried startup path are the same. If they are different, change the configured **Program Path**.
- Installing an application supported by CBH
 - a. Log in to the Windows application server and install the application that can be called by the CBH system. For details about which types of applications are supported by CBH, see [Restrictions on Using CBH](#).
 - b. Log in to the CBH system and reconfigure the **Program Path** of the application server.

What Can I Do If Applications Cannot Be Called After the Windows Host Is Restarted?

Symptoms

Before the Windows application server system is upgraded, application resources can be properly accessed. After the system is upgraded and restarted, the access to application resources is denied. As a result, the configured application cannot be called, and an error message is displayed, indicating that the initial application program cannot be started.

Possible Causes

After the virus and threat protection function is updated in Windows, Windows Defender automatically prevents all exe programs whose names contain **administrator** from running on your devices. For example, the database application **mysqladministrator.exe** supported by CBH is prevented.

Solutions

- Changing the application name
Change the startup program name of the application on the Windows application server and change the application startup path **Program Path** in the CBH system.
- Disabling Windows Defender
On the control panel of the Windows application server, choose **Settings > Update & Security > Windows Defender** to disable the **Real-time protection** function of Windows Defender.

12.2.10 Why Are Databases Managed in CBH Inaccessible with an SSO Tool?

Database Login Failures After the Instance Edition Upgrade

Symptoms

After the upgrade of CBH, databases managed in your CBH system became inaccessible. The system displayed a message indicating that the SSO tool had been installed. If login failures occurred, retry or install the latest SSO tool.

Possible Causes

After the CBH is upgraded, the SSO tool is not upgraded. As a result, the remote connection fails to be established.

Solution

After each CBH upgrade, uninstall the local SSO Tools in **SsoDBSettings**, download and install the latest SSO tool again, and correctly configure the database client path.

Incorrect Database Client Path

Symptoms

When you log in to the database for the first time, the system displays a message indicating that the path of the database client tool is incorrect and must be reconfigured.

Possible Causes

The database client path configured on the SSO tool is incorrect or not configured.

Solution

Start the SSO tool and verify that the database client path is correct.

12.2.11 Why Does the Number of Concurrent Sessions Reach the Limit When I Use CBH to Log In to a Host Resource?

Symptom

There is a limit on the number of concurrent SSH connections established between CBH and servers it manages. If this limit is reached, no more users can log in to CBH unless a logged-in user logs out.

Possible Causes

There is a limit on how many concurrent connections can be established between CBH and a managed host resource. If multiple users establish concurrent connections to a host resource over SSH, a user will be logged out once the number of concurrent connections reaches the limit.

Solutions

The limit of concurrent requests varies depending on the CBH edition you are using. CBH has two editions that respectively support 50, 100, 200, 500, 1,000, 2,000, 5,000, or 10,000 assets. For details, see [Edition Differences](#).

To fix this issue, [change your CBH instance specifications](#) to increase the concurrent request quota.

12.2.12 Why a Black Block Is Displayed on the Mouse When the MSTSC Client Is Used to Access a Server Resource?

If a black block is displayed when you use the MSTSC client to access server resources, perform the following operations to fix the issue.

Procedure

- Step 1** Log in to your server.
- Step 2** Open **Control Panel** and click **Devices**.
- Step 3** In the navigation tree on the left, click **Mouse** to go to the mouse configuration page.
- Step 4** Click **Mouse Properties** box and then click the **Pointers** tab.

Step 5 Deselect **Enable pointer shadow** and click **OK**.

----End

12.2.13 Why Am I Seeing User Creation Failure Message When Accessing a Windows Application Publishing Server?

Symptoms

When an O&M engineer attempted to log in to a published Windows application, an error message is displayed indicating that the login denied and the user failed to be created.

Possible Causes

- Cause 1: The version of RemoteAppProxy installed on the application publishing server is too low and needs to be upgraded.
- Cause 2: The maximum length of the shadow account username to be created is longer than what the server account allows.

Solution

- Solution 1: Upgrade RemoteAppProxy installed on the application publishing server to **1.1.8.0** or later.
- Solution 2: Log in to the application publishing server, open the **C:\DevOpsTools\RemoteAPPProxy\Application.ini** file, and change the value of **max_user_length** (20 by default) to the maximum length of the shadow account username supported by the server, for example, 15.

NOTE

If you do not want to upgrade RemoteAppProxy, log in to the application publishing server, open the **C:\DevOpsTools\RemoteAPPProxy\Application.ini** file, and disable the shadow account by setting **use_shadow_user** to **0**.

The parameter indicating whether to use the shadow account mode is as follows:

- **1**: enabled.
- **0**: disabled.

12.3 Maintenance Issues

12.3.1 Why Does SMS Verification Code Fail to Send When I Log In to a CBH Instance?

Symptoms

- **Mobile SMS** is selected as multifactor verification for your account. When you attempt to log in to the CBH system through SMS, the system displays a message indicating that the SMS message fails to be sent.
- After the login password is reset, you do not receive the SMS verification code.

Possible Causes

- Cause 1: If the browser you used is incompatible with the CBH system, the login verification SMS fails to be sent.
- Cause 2: The security group denies the IP address of the SMS gateway, or ports 10743 and 443 are not enabled.
- Cause 3: The mobile number is incorrect.
- Cause 4: The SMS service is abnormal.
- Cause 5: No elastic IP address (EIP) is bound to the CBH instance.

Solutions

- Solution to cause 1
Use other browsers or upgrade the browser version. For details, see [Table 12-2](#).

Table 12-2 Recommended browsers and versions

Browser	Version
Edge	44 or later
Google Chrome	52.0 or later
Safari	10 or later
Mozilla Firefox	50.0 or later

- Solution to cause 2
Configure the CBH instance security group to allow access to the SMS gateway IP address and enable ports 10743 and 443.
- Solution to cause 3
If you are a system user, contact the administrator to change the mobile number bound to your account.

 **NOTE**

If you are user **admin**, submit a service ticket to change the mobile number bound to your account.

- Solution to cause 4
Check the status of the SMS service of the bound mobile number from the following aspects:
 - Check if the mobile number is suspended due to arrears.
 - Check if the SMS message is in the spam short messages folder.
 - Check if the mobile communication network is normal.
- Solution to cause 5
An EIP must be bound to a CBH instance for successful logins. An EIP with a bandwidth of 5 Mbit/s or above is recommended.

12.3.2 Why Am I Seeing a Message Indicating that the Number of Resources Has Reached the Limit When I Add a Resource to CBH?

Symptoms

When you add a host or application resource, a message is displayed indicating that the number of resources that can be added has reached the maximum allowed limit.

Possible Causes

The total number of resources that can be added has reached the maximum number allowed by the instance specifications.

Solutions

1. Upgrade the instance specifications. For details, see [Changing Specifications of a CBH Instance](#).
2. Delete idle or zombie resource accounts. For details, see [Resource Management](#).

To strengthen resource management and control, you can [set account synchronization policies](#) to automatically detect and delete zombie accounts.

12.3.3 Why Does Verification of An Account for a Managed Host Fail?

Symptoms

- The system prompts that the account verification has timed out.
- The system prompts that the entered account password is incorrect.
- The task center displays a message indicating that the account failed to be verified because the host is unreachable.
- The task center displays a message indicating that the account failed to be verified because its password is incorrect.

Possible Causes

Cause 1: Incorrect host information. For example, the host IP address or port number is incorrect.

Cause 2: Incorrect account password.

Cause 3: Network delay due to poor connectivity.

Solutions

Solution to cause 1

- Modify the host IP address and port on the **Host** page or host details page in the **Resource** module.

Solution to cause 2

- Change the password of the host resource on the **Host** page or **Account** page in the **Resource** module.

Solution to cause 3

- Restart the host resource and check the network status.

12.3.4 Why Am I Seeing Garbled Characters When I Open a System Data File?

Symptom

When you export the CBH system data as a CSV file and open the file with Excel, the data in the file is displayed as garbled characters.

Possible Cause

The CSV file exported from the CBH system uses the UTF-8 encoding format. However, when the file is opened in Excel, the ANSI encoding format is used. As a result, data cannot be identified and garbled characters are displayed.

Solutions

Use a text editor, such as Notepad, to open the CSV file and save it as an ANSI file.

After the file is saved successfully, use Excel to open the file again. The file information will be displayed properly.

12.3.5 Why Does Login Timeout Frequently Occur During an O&M Session?

Symptoms

- On the web-based O&M session page, the login times out and the O&M connection is disconnected. A message is displayed indicating that the session has ended because no operation has been performed for a long time.
- The CBH system does not log you out but the host is disconnected from the O&M session.

Possible Causes

- Cause 1: The default login **Lockout Duration** is 30 minutes. If you do not perform any operation in the O&M session for more than 30 minutes, the CBH system will log you out and the O&M session will be disconnected.
- Cause 2: A small value is configured for the system idle time or lock screen timeout of the host. As a result, the host system logs you out due to timeout.

Solutions

- Solution to cause 1

- Set the login **Lockout Duration** to a larger value. For details, see [Web Login Configuration](#).
- Ensure that the CBH O&M session is in the running state.
- Solution to cause 2
 - Set the idle time **TMOUT** of the Linux host to a larger one.
 - Set the value of lock screen timeout for the Windows host to a larger one.

12.3.6 Why Does the PL/SQL Client Display Garbled Characters During Application O&M?

Symptom

The PL/SQL Developer client for Oracle databases is managed as an application resource. When you attempt to log in to an application resource using a web browser, garbled characters are displayed on the PL/SQL client.

Possible Cause

The encoding format of the Oracle database is different from that of the PL/SQL client, which uses English encoding format. As a result, the PL/SQL client is incompatible with the Oracle database and garbled characters are displayed.

Solutions

Step 1 Query the character set of the Oracle database.

Run the following command on the PL/SQL client to check the encoding format of the Oracle database:

```
select userenv('language') from dual;
```

Obtains the default encoding value **SIMPLIFIED CHINESE_CHINA.ZHS16GBK**.

Step 2 Change the encoding format of the PL/SQL client.

On the server where the application is published, create the system environment variable **NLS_LANG** and set its value to **SIMPLIFIED CHINESE_CHINA.ZHS16GBK**.

Step 3 Restart the PL/SQL client and verify the search content.

----End

12.3.7 Why Is the Requested Session Denied After I Log In to a Managed Host?

Symptom

After you log in to a host using a web browser, a message is displayed, indicating that the requested session is denied and the O&M session cannot be performed.

Possible Cause

The **admin console** connection mode is enabled in the CBH system. When the number of remote desktop login users reaches the upper limit, new users can forcibly log in to the host using the RDP protocol. As a result, logged-in users are forcibly logged out and cannot continue O&M sessions.

Solutions

- Step 1** Log in to a CBH system.
- Step 2** Choose **Operation > Host Operations** to go to the **Host Operations** page.
- Step 3** Click **Web OPS Settings**. The configuration window is displayed.
- Step 4** Deselect the **admin console** connection mode.
- Step 5** Click **OK** and go to the **Host Operations** page and log in to the host again.

----End

12.3.8 Why Does the CBH Traffic Bandwidth Exceed the Threshold?

Symptoms

An error is reported indicating that the traffic bandwidth exceeds the threshold. As a result, the CBH system cannot be used and managed resources cannot be accessed through CBH.

Possible Causes

The traffic bandwidth used by CBH exceeds the maximum shared bandwidth or dedicated bandwidth of the bound EIP.

Solution

- Step 1** Log in to the management console and verify the EIP bandwidth limit. For details, see "How Do I Check Whether the Bandwidth Exceeds the Limit?"
- Step 2** Reconfigure the bandwidth of the EIP bound to the CBH instance. A bandwidth larger than 5 Mbit/s is recommended. For details, see "VPC Shared Bandwidth Overview."

----End

12.3.9 Why Text Cannot Be Copied When I Perform O&M Through a Web Browser?

Text Cannot Be Copied or Pasted

Symptoms

You cannot use the copy and paste functions on the **Host Operation** session page.

Possible Causes

- Cause 1: The permission for clipboard is not enabled for you or the host resource.
- Cause 2: The clipboard program on the Windows host is faulty or suspended.

Solution

- Solution to cause 1
The clipboard function of the host must be enabled, and you must have been granted the permission to use the clipboard.
 - To enable the clipboard function for host resources, see [Modifying Host Configuration](#).
 - To obtain the permission to use the clipboard, see [Editing an ACL Rule](#) or [ACL Ticket](#).
- Solution to cause 2
Reload or restart the clipboard program `rdpclip.exe` on the Windows host.

Unable to Copy Extra-long Text to a Windows Host

Symptoms

When you attempt to copy a text from a local computer to a managed Windows host, a message is displayed indicating that the text is too long and the file management function is recommended.

Possible Causes

Text with more than 80,000 characters cannot be copied or pasted from a local PC to a managed host in the CBH system.

Solution

- Step 1** Enable the file management function and obtain file management permission.
1. To enable the file management function on a host resource, see [Modifying Host Configuration](#).
 2. To obtain the file management permission, see [Modifying an ACL Rule](#) or [ACL Ticket](#).
- Step 2** Copy your text file to a local disk and upload the file to the **Personal Netdisk**. Go to the `G:\` directory on the Windows host and obtain the text content in the file.

----End

For more details about copy/paste, see [How Do I Use Shortcut Keys to Copy/Past Text During Web-based O&M?](#)

12.3.10 Which Types of Failures May Occur During the O&M?

After a user logs in to a managed host through the CBH system and starts operation, if an error occurs during this period, an error code and its description will be returned.

For details about common CBH error codes and troubleshooting methods, see [Table 12-3](#).

Table 12-3 Common O&M Error Codes

Error Code	Error Message	Troubleshooting
ERROR_CLIENT_514	Code: C_514 The file transfer response time is too long. Please try again or contact the system administrator.	<ol style="list-style-type: none"> 1. Check whether packet loss occurs on the network between the CBH system and the FTP server. 2. Log in to the FTP server and check whether files can be uploaded. 3. Check whether the native network restricts the size of the file to be uploaded. 4. Submit a service ticket to contact technical support.
ERROR_CLIENT_515	Code: C_515 An error occurs during O&M. Please try again or contact the system administrator.	<ol style="list-style-type: none"> 1. Log in to the faulty host locally or try to log in to another host in the same network segment. 2. Check whether /etc/hosts.deny file blacklists the IP address of the CBH system. For details, see What Should I Do If a Login Error (Code: C_515) Occurs? 3. Check whether the IP address of the CBH system is blocked by network protocols between the CBH system and faulty host. 4. Submit a service ticket to contact technical support.
ERROR_CLIENT_519	Code: C_519 The managed host cannot be accessed because the resource is disconnected or unreachable. If the problem persists, contact the system administrator or check system logs.	<ol style="list-style-type: none"> 1. Check whether the network connection between the CBH system and the managed host is normal. 2. Log in to the managed host locally and run the route -n command to check whether the CBH route is missing from the routing table. 3. Submit a service ticket to contact technical support. For details, see What Should I Do If a Login Error (Code: C_519) Occurs?

Error Code	Error Message	Troubleshooting
ERROR_CLIENT_520	Code: C_520 The managed host cannot be accessed because the RDP rejects the connection or an error occurs during waiting for response data. If the problem persists, contact the system administrator or check system logs.	<ol style="list-style-type: none"> 1. Check whether the remote desktop is enabled on Windows host. 2. Log in to the managed host in local MSTSC mode and check whether the login is successful. 3. Submit a service ticket to contact technical support.
ERROR_CLIENT_521	Code: C_521 Connection conflict occurs due to login of other users. Please try again later.	<ol style="list-style-type: none"> 1. Log in to the Windows host locally and run the gpedit.msc command to set the maximum number of connections and change the maximum number of enabled connections. Alternatively, disable the restriction that each user can have only one session. 2. Submit a service ticket to contact technical support.
ERROR_CLIENT_522	Code: C_522 The connection has been disconnected because the RDP session exceeds the time limit. To restore the connection, contact the system administrator or check the system settings.	<ol style="list-style-type: none"> 1. Log in to the Windows host locally and run gpedit.msc command to set the time for the disconnected session. 2. Log in to the host in local MSTSC mode and check whether the RDP timeout error occurs. 3. Submit a service ticket to contact technical support.

Error Code	Error Message	Troubleshooting
ERROR_CLIENT_523	Code: C_523 The connection has been disconnected because the administrator has disconnected the connection, the account has been logged out, or the host login duration has reached the upper limit. To restore the connection, contact the system administrator or check system logs.	<ol style="list-style-type: none"> 1. Check whether the RDP connection is forcibly disconnected by the administrator. 2. Check whether the system user is logged out by the server administrator. 3. Check whether the login duration exceeds the limit.
ERROR_CLIENT_769	Code: C_769 Login failed. The account username, password, or key is incorrect. Please try again.	<ol style="list-style-type: none"> 1. Log in to the faulty host locally and check whether the managed host account username and password are correct. 2. Check whether two-factor authentication is enabled for the managed host. 3. Check whether the managed host rejects the login of user root. 4. Submit a service ticket to contact technical support. For details, see What Should I Do If a Login Error (Code: C_769) Occurs?
ERROR_CLIENT_771	Code: C_771 Contact the administrator to grant account access permission or check your system settings.	Check whether the remote login permission of the target account is enabled for the managed host.

Error Code	Error Message	Troubleshooting
ERROR_CLIENT_776	<p>Code: C_776</p> <ul style="list-style-type: none"> • This error code is returned when the connection has been interrupted because the browser does not respond for a long time. Please check your network and try again. • This error code is returned when the connection has been interrupted because the browser does not respond for a long time. Check the outbound access policy of the security group that the application server belongs and allow access to the CBH instance IP address over port 443. 	<p>Check the running status of the local browser. The Google Chrome browser is recommended.</p>
ERROR_CLIENT_797	<p>Code: C_797</p> <p>The number of connections exceeds the upper limit. Close one or more connections and try again.</p>	<p>Log in to the Windows host locally and run the gpedit.msc command to set the maximum number of connections.</p>

Error Code	Error Message	Troubleshooting
ERROR_T UNNEL_5 14	Code: T_514 The connection has been disconnected because the server does not respond for a long time. Please check your network and try again.	<ol style="list-style-type: none">1. Check whether the network between the CBH system and the managed host is stable.2. Check whether the network connection between the CBH system and the managed host is normal.3. Submit a service ticket to contact technical support. For details, see What Should I Do If a Login Error (Code: T_514) Occurs?
ERROR_T UNNEL_5 20	Code: T_520 The proxy server of H5 server is rejecting the connection. Please check your network and try again.	<ol style="list-style-type: none">1. Check whether the IP address or port number of the managed host are correct.2. Check whether the guacd service is enabled on the managed host.3. Check whether host guacd service can be accessed by the IP address of the CBH system.4. Submit a service ticket to contact technical support.

12.3.11 What Do I Do If an Exception Occurs When I Enter Chinese Characters Using WPS During the O&M of a Windows Server?

During the O&M of a Windows server, when the WPS software is used to enter characters, duplicate characters are displayed.

Solutions

Step 1 Set the input method of the local computer to English.

Step 2 Set the input method of the Windows server to be operated and maintained to Chinese.

----End

12.3.12 I Mapped My CBH Instance IP Address to a Domain Name, and Added the Domain Name to WAF. Why Does the Domain Name Become Inaccessible?

After a domain name mapped to CBH instance IP address were added to WAF, the domain name became inaccessible. An error message is displayed indicating that there are too many redirections.

Solution

- Step 1** Disable the function of checking source IP addresses on the bastion host. For details, see [Configuring Web Login Requirements](#) .
- Step 2** Choose **System > System Maintain > System Mgmt**, add the system address under the **System address**, and click **Immediate update**.

----End

12.3.13 Why Is LTS Still Disabled After It Is Configured for a CBH Instance?

Symptom

After Log Tank Service (LTS) is configured for a CBH instance, the system displays a message indicating that the LTS service is disabled.

Solution

The command for installing ICAgent starts with the curl command. If the **set +o history**; field exists before the curl command, delete it and interconnect ICAgent with the bastion host. The parameters for installing ICAgent are as follows:

```
curl http://icagent-{region}.obs.{region}.myhuaweicloud.com.ICAgent_linux/  
apm_agent_install.sh > apm_agent_install.sh && REGION=[region] bash  
apm_agent_install.sh -ak [ak] sh [sk] -region [region] -projectid [projectid] -  
accessip [accessip] -obsdomain [obsdomain] -accessdomain [accessdomain] ;
```

NOTICE

- For bastion host versions earlier than 3.3.42.0, parameter **accessdomain** is not required, and the parameters do not end with spaces or semicolons (;).
- For bastion host version 3.3.42.0 or later, parameter **accessdomain** is required, and the parameters do not end with spaces or semicolons (;).
- For bastion host version 3.3.46.0 or later, parameter **accessdomain** is optional, and the parameters do not end with spaces or semicolons (;).

12.3.14 Why My Certificate Becomes Abnormal After a Cross-Version Upgrade?

If a cross-version upgrade is performed for CBH, you need to upload the certificate after the upgrade. You can also upgrade CBH version by version in sequence.

Possible Causes

- The original certificate may expire.
- If a cross-version upgrade is performed before the certificate status becomes abnormal, the certificate and manually added routes might be affected after the upgrade. In this case, you need to synchronize the certificate again.

Solution

Certificate expiry

You need to purchase a new commercial certificate and replace the expired one with the new one in CBH. For details, see [Replacing Certificates](#).

Cross-version upgrade

- Step 1** Log in to the CBH system.
- Step 2** Choose **System > Sysconfig > Security**.
- Step 3** In the **Web Certificate** configuration area, click **Edit**.
- Step 4** Upload the certificate file you download earlier.
- Step 5** After the certificate file is uploaded, enter the Keystore password to verify the certificate.
- Step 6** Click **OK**. You can then check the web certificate configuration of the current system user on the **Security** tab.

NOTE

To ensure certificate update, restart the CBH instance on the management console or through the system tool in the CBH system.

- Step 7** Check the certificate information.

----End

12.4 SSO O&M Faults

12.4.1 Configuring a Customized Driver for DBeaver to Connect to GaussDB Databases

GaussDB databases can be connected through the custom driver configured on DBeaver.

Version Requirements

3.3.52.0 or later.

Network Requirements

- PC to bastion host: 18000
- Port for connections between the bastion host and GaussDB databases: The default port is 8000.

Configuration on the Bastion Host

- Step 1** Log in to the web page of the bastion host, click **Download Center** in the upper right corner, and download **SSOTool Windows**.

Step 2 Choose **Resource > Host** and add a GaussDB protocol host.

Step 3 Then, choose **Policy > ACL Rule** to associate the user with the access permission for the GaussDB host.

----End

Configuring the DBeaver Client

Step 1 Start the DBeaver client, choose **Database > Driver Manager**, and click **New**.

Table 12-4 Parameter descriptions

Parameter	Description
Driver Name	Set a name that is easy to identify, for example, GaussDB.
Driver Type	Select Generic .
Class Name	org.postgresql.Driver
URL Template	jdbc:postgresql://{host}[:{port}]/[{database}]
Default Port	Port of the database to be connected. Default port: 8000

Step 2 Click the **Libraries** tab, click **Add File**, and add **gsjdbc4.jar**.

Download the **gsjdbc4.jar** file. The driver package file is compatible with the database version.

- Download the [3.X driver package](#).
- Download the [2.X driver package](#).

Decompress the package, go to the **GaussDB_driver\GaussDB_driver\Centralized\Euler2.5_x86_64** directory, and decompress the JDBC package.

Step 3 Click **OK**, edit the corresponding driver again, and click **Find Class**.

Step 4 Open the DBeaver client and directly connect to the target GaussDB database. Select the driver file created in [Step 1](#).

Step 5 Click **OK**. After the connection is successful, open the **C:\sso\SsoTool\DBeaver\General\DBeaver\data-sources.json** file, verify that the corresponding connection is generated, and open the **C:\sso\SsoTool\ssotool.conf** file.

Add the **C:\sso\SsoTool\DBeaver\General\DBeaver\data-sources.json** parameter to the **C:\sso\SsoTool\ssotool.conf** file, uncomment the corresponding line in the **ssotool.conf** file, and save the file.

Step 6 Choose **Operation > Host Operations** and access the host using the corresponding protocol.

----End

12.4.2 Configuring the Connection Between DBeaver and GaussDB

Version Requirements

3.3.50.0 or later

Network Requirements

- Port for connections between your PC and the bastion host: 18000
- Port for connections between the bastion host and GaussDB databases: The default port is 8000.

Configuring the DBeaver Client

Step 1 Use DBeaver to directly connect to GaussDB databases. Select PostgreSQL. During the connection, the system prompts you to download the driver. Download the driver and connect to the database.

Step 2 Configure the DBeaver driver and obtain the GaussDB driver package. The driver package version is the same as the GaussDB database version.

- Download the [3.X driver package](#).
- Download the [2.X driver package](#).

Decompress the package, go to the **GaussDB_driver\GaussDB_driver\Centralized\Euler2.5_x86_64** directory, and decompress the JDBC package.

Step 3 Start the DBeaver client, choose **Database > Driver Manager > PostgreSQL**, and click **Edit**. Then, select **Libraries**, delete the original driver from the library, and import **gsjdbc4.jar**.

Step 4 After the import, click **OK**. Edit the postgresql driver again and click **Find Class**.

Step 5 Enable SSL for GaussDB and disable SSL in DBeaver.

Start the DBeaver client, choose **Database > Driver Manager > PostgreSQL**, click **Edit**, select **Connection properties**, and add the **sslmode** property. Set its value to **disable**.

Step 6 Configure the workspace.

Choose **File > Switch Workspace** and select **C:\sso\SsoTool\DBeaver**.

----End

12.4.3 Message "1251-lost connection to mysql server during query" Displayed While Backing Up MySQL Database Tables

Symptoms

The message "lost connection to mysql server during query" was displayed while backing up MySQL database tables.

Check the proxy log in the background. A message is displayed, indicating that a memory overflow occurred.

Solution

This problem has been resolved in the 3.3.34 image version. Upgrade the image to this version.

12.4.4 Message "1251-Client does not support authentication protocol requested by server" Reported While Managing MySQL Database Through Host Operation

Symptoms

The message "1251-Client does not support authentication protocol requested by server" was reported while managing MySQL databases through host operation in a bastion host.

Possible Causes

The IP address of the bastion host may be restricted.

Solution

Log in to the database and run the following command to check whether the host value of the corresponding user restricts the IP address of the bastion host. If yes, remove the restriction.

```
select * from user
```

NOTE

You can log in to the bastion host and choose **System** > **System Config** > **Network** to check the IP address of the bastion host, or log in to the cloud console and check the IP address of the corresponding bastion host instance.

12.4.5 Error Message "2013-Lost connection to MySQL server at waiting for initial communication packet', system error:0" Reported While Connecting to MySQL Databases

Symptoms

The message "2013-Lost connection to MySQL server at waiting for initial communication packet', system error:0" was reported while connecting to MySQL databases added as host resource.

Possible Causes

- Port 33306 or 3306 may not be enabled.
- There are multiple NICs for domain name resolution.

Solution

- Enable the communication between the local PC and the bastion host over port 33306 and communication between the bastion host and the data base server over port 3306.

- To address the issue of multiple NICs:
Log in to the bastion host background and run the following command and add the domain name: *Domain name=IP address of the bastion host*.
`vim /usr/local/yunanbao/apache-tomcat-7.0.82/webapps/ROOT/WEB-INF/classes/domain.properties`

12.4.6 Error Message "ORA-12537_TNS_Connection closed" Reported While Connecting to Oracle Databases

Symptoms

The error message "ORA-12537_TNS_Connection closed" is reported while connecting to Oracle databases.

Possible Causes

Port 1521 may not be enabled.

Solution

Enable the communication between the local PC and the bastion host over port 1521 and communication between the bastion host and the data base server over port 1521.

12.4.7 Error Message "ORA-12637_Packet Receive Failed" Reported While Connecting to Oracle Databases

Symptoms

After the bastion host is upgraded to 3.3.26.0, error message "ORA-12637_Packet Receive Failed" was reported while connecting to Oracle databases with PL/SQL clients.

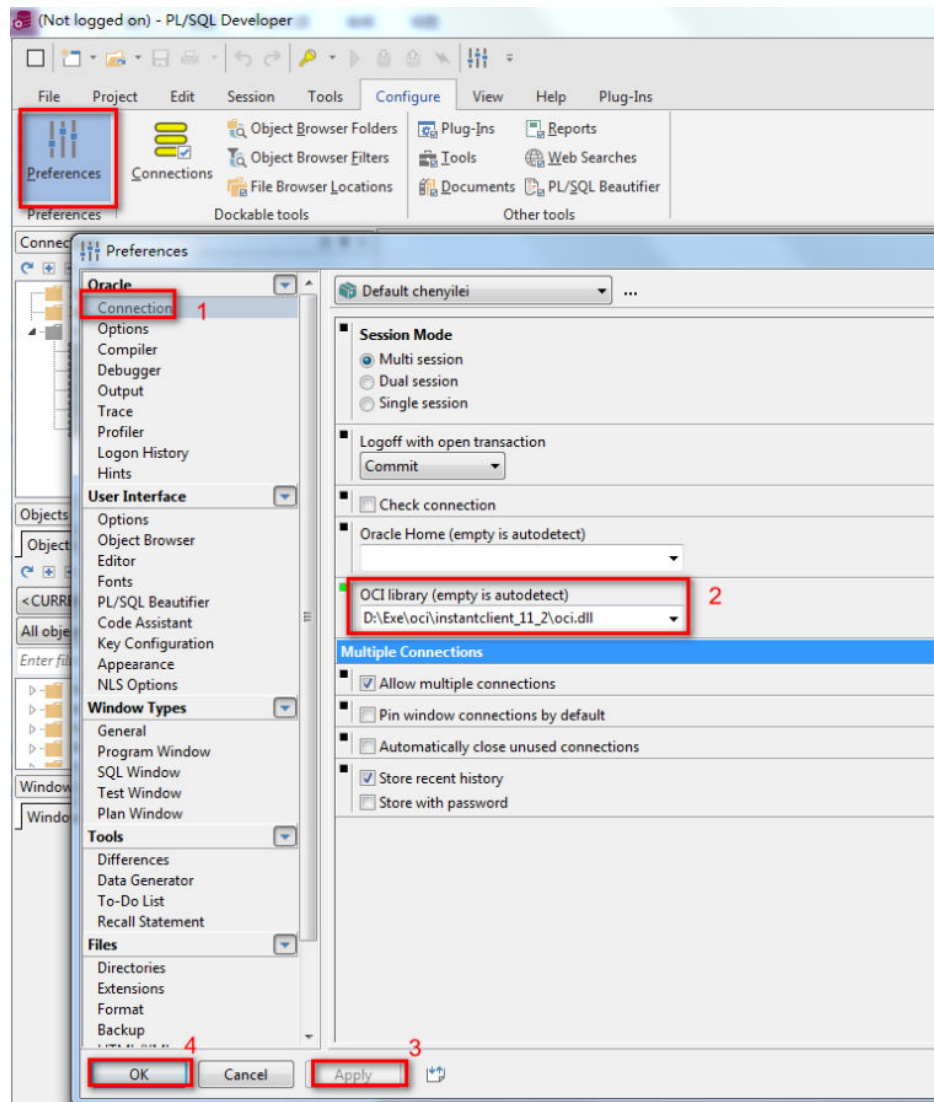
Possible Causes

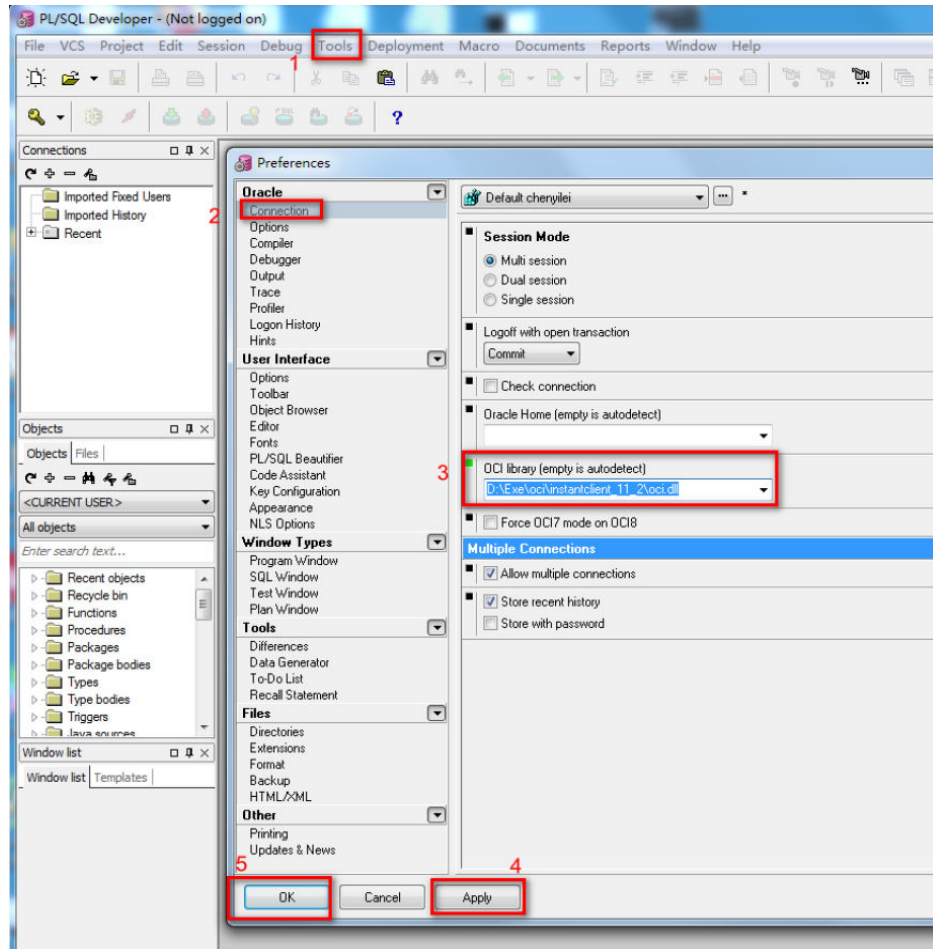
The configuration file **oci.dll** is missing.

Solution

- Step 1** Download the **oci.dll** file. The number of oci bits depends on the number of PL/SQL bits.
- Step 2** Decompress the downloaded package and verify that the **oci.dll** file is in the decompressed directory.
- Step 3** Configure the **oci.dll** file in PL/SQL Developer. The configuration takes effect only after the program is closed.

Figure 12-4 Configuration file





----End

12.4.8 Error Message "ORA 12170 TNS Connect Timeout" Reported While Connecting Oracle Databases through Host Operation in the Bastion Host

Symptoms

Error message "ORA:12170 TNS Connect Timeout" was reported while connecting to Oracle databases through host operation in the bastion host.

Possible Causes

The network between the client and the virtual IP address is disconnected.

Solution

Step 1 Check the network communication.

- Port for connections between your PC and the bastion host: 1521
- Port for connections between the bastion host and the database: port 1521 used for Oracle databases by default

Step 2 If the network communication is normal, capture packets on the bastion host and check whether the database IP address managed by the bastion host is the actual IP address of the database node instead of the virtual IP address of the Oracle database.

----End

12.4.9 Failed to Establish a Connection between DBeaver and PostgreSQL Databases

Symptoms

When a user tried to use host operation in the bastion host to manage PostgreSQL databases, the connection between DBeaver and PostgreSQL databases was not established.

Possible Causes

The network is inaccessible.

Solution

Step 1 Check whether the network communication is normal.

- Port for connections between your PC and the bastion host: 15432
- Port for connections between the bastion host and the managed database: PostgreSQL database port

Step 2 If the communication is normal, ensure that SSL is enabled for PostgreSQL and disabled in DBeaver.

Start the DBeaver client, choose **Database > Driver Manager**, click **Edit**, select **Connection properties**, and add the **sslmode** property. Set its value to **disable**.

----End

12.4.10 SSO Failed as JRE Is Missing in the Running Environment

Symptoms

The SSO client fails to start the database client. When trying to start host operations, a message is displayed, indicating that the JRE is missing in the running environment.

Possible Causes

The image version corresponding to the process or listening port is incorrect.

Solution

- After performing an operation on database through the host operation function, check whether there is a **YabLocalAgent.exe** process. If the bastion

host version is 3.3.56.0 or later, check whether there is a **LocalAgent.exe** process.

- Make sure that the listening port of the LocalAgent main process exists. For versions earlier than 3.3.56.0, the listening port is 7001. For 3.3.56.0 and later versions, the listening port is 9010. Note that the O&M PC you use does not have conflict ports.

```
netstat -ano |findstr 7001
```

```
netstat -ano |findstr 9010
```