

Cloud Bastion Host (CBH)

3.3.54.0

User Guide

Date 2024-05-30

Contents

1 Service Overview	1
1.1 Cloud Bastion Host	1
1.2 Features	2
1.3 Product Advantages	9
1.4 Application Scenarios	10
1.5 Edition Differences	11
1.6 Basic Concepts	16
1.7 Restrictions on Using CBH	17
1.8 Permissions Management of CBH Instances	22
1.9 CBH and Other Services	25
1.10 Personal Data Protection Mechanism	26
1.11 Security Statement	28
2 Instances	30
2.1 Permissions Management	30
2.1.1 Creating a User and Granting Permissions for CBH Instances to It	30
2.1.2 Creating Custom Policies for CBH Instances	31
2.1.3 Managing CBH Instance Permissions and Supported Actions	33
2.2 Checking CBH Instance Details	34
2.3 Resetting the Login Method for User admin	36
2.4 Resetting the Password of User Admin	36
2.5 Upgrading the CBH System Version	37
2.6 Starting a CBH Instance	38
2.7 Stopping a CBH Instance	39
2.8 Restarting a CBH Instance	39
2.9 Changing a VPC for a CBH Instance	40
2.10 Changing Security Groups	41
2.11 Binding an EIP to a CBH Instance	41
2.12 Unbinding an EIP from a CBH Instance	42
2.13 Key CBH Instance Operations Recorded by CTS	43
2.13.1 CBH Operations Supported by CTS	43
2.13.2 Viewing CTS Traces	44
3 Logging In to the CBH System	46

3.1 Overview.....	46
3.2 Using a Web Browser to Log In to a CBH System.....	49
3.3 Using a Client to Log In to a CBH System.....	55
3.4 Configuring Multifactor Verification.....	58
3.4.1 Configuring SMS Login Authentication.....	58
3.4.2 Configuring Mobile OTP Login Authentication.....	60
3.4.3 Configuring USB Key Login Authentication.....	62
3.4.4 Configuring OTP Token Login Authentication.....	63
3.5 Managing Login Security.....	64
3.5.1 Configuring User Login Lockout.....	64
3.5.2 Configuring the Login Password Policies.....	66
3.5.3 Configuring Login Timeout and Login Authentication.....	67
3.5.4 Updating a System Web Certificate.....	70
3.5.5 Configuring the Mobile OTP Type.....	71
3.5.6 Configuring the USB Key Vendor.....	72
3.5.7 Configuring Policies to Disable Zombie Users (Available in V3.3.30.0 and Later Versions).....	73
3.5.8 Configuring the RDP Resource Client Proxy (Available in 3.3.26.0 and Later Versions).....	73
3.5.9 Enabling API Configuration (Included in V3.3.34.0 and Later Versions Only).....	74
3.5.10 Configuring Automatic Inspection (Available in V3.3.36.0 and Later).....	74
3.5.11 Configuring a Resource Account.....	75
3.5.12 Configuring Client Login.....	75
3.5.13 Configuring a User Expiration Reminder.....	76
3.5.14 Configuring Session Limit.....	76
4 Dashboard of the CBH System.....	78
4.1 Dashboard.....	78
4.2 Profile.....	88
4.2.1 Viewing Your Profile.....	88
4.2.2 Editing Basic Information in Profile.....	92
4.2.3 Managing Mobile OTP Application for Login Authentication.....	94
4.2.4 Managing SSH Public Keys.....	95
4.3 Tasks.....	98
4.4 Messages.....	99
4.4.1 Managing Messages.....	99
4.4.2 Creating a CBH System Notice.....	102
4.5 Download Center.....	104
5 Department.....	105
5.1 Overview.....	105
5.2 Creating a Department.....	105
5.3 Deleting a Department.....	106
5.4 Viewing and Editing Department Information.....	108
5.5 Querying Configurations of a Department.....	109

6 User	110
6.1 Overview	110
6.2 User Management	110
6.2.1 Creating a User and Assigning a Role to the User	110
6.2.2 Enabling or Disabling a User	116
6.2.3 Deleting a User	117
6.2.4 Configuring User Login Restrictions	117
6.2.5 Querying and Editing User Information	121
6.2.6 Changing User Login Passwords	123
6.2.7 Exporting User Information	124
6.2.8 Adding Users to a User Group	125
6.3 User Role Management	126
6.3.1 Overview	126
6.3.2 Creating a Custom Role	127
6.3.3 Deleting a Role	127
6.3.4 Querying and Editing Role Information	128
6.4 User Group Management	129
6.4.1 Overview	129
6.4.2 Creating a User Group	130
6.4.3 Deleting a User Group	130
6.4.4 Querying and Editing User Group Information	131
6.5 Remote Authentication Management	132
6.5.1 Configuring Remote AD Authentication	132
6.5.2 Configuring Remote LDAP Authentication	134
6.5.3 Configuring Remote RADIUS Authentication	138
6.5.4 Configuring Remote Azure AD Authentication	139
6.5.5 Configuring Remote SAML Authentication	140
6.6 USB Key Management	142
6.7 OTP Token Management	144
7 Resource	147
7.1 Overview	147
7.2 Managing Host Resources Using CBH	148
7.3 Managing Application Servers Using CBH	156
7.4 Adding Accounts of Managed Host or Application Resources into CBH	161
7.5 Resource Management	167
7.5.1 Verifying Managed Resource Accounts	167
7.5.2 Deleting Managed Resources from the CBH System	169
7.5.3 Querying and Editing Managed Resource Configurations	170
7.5.4 Exporting Resource Information	175
7.5.5 Adding a Resource Account to an Account Group	177
7.6 Account Group	178
7.6.1 Overview	178

7.6.2 Creating an Account Group.....	179
7.6.3 Deleting an Account Group.....	179
7.6.4 Querying and Editing Account Group Information.....	180
7.7 Managing Resource Labels.....	181
7.7.1 Overview.....	181
7.7.2 Creating a Resource Label.....	182
7.7.3 Deleting a Resource Label.....	183
7.8 Customizing OS Types.....	183
7.9 Creating a Proxy Server.....	185
8 Policy.....	186
8.1 ACL Rules.....	186
8.1.1 Creating an ACL Rule and Associating It with Users and Resource Accounts.....	186
8.1.2 Setting Two-person Authorization.....	189
8.1.3 Querying and Editing an ACL Rule.....	190
8.2 Command Rules.....	192
8.2.1 Creating a Command Rule.....	192
8.2.2 Querying and Editing a Command Rule.....	195
8.2.3 Managing Command Sets.....	197
8.2.4 Defining Custom Related Commands.....	199
8.3 Database Rules.....	200
8.3.1 Creating a Database Rule.....	200
8.3.2 Querying and Editing a Database Rule.....	202
8.3.3 Managing Regulation Sets.....	203
8.4 Password Rules.....	205
8.4.1 Creating a Password Rule.....	205
8.4.2 Querying and Editing a Password Rule.....	209
8.4.3 Managing Password Logs.....	210
8.5 Account Synchronization Rules.....	211
8.5.1 Creating a Synchronization Rule.....	211
8.5.2 Querying and Editing a Synchronization Rule.....	214
8.5.3 Managing Synchronization Execution Logs.....	215
9 Ticket.....	217
9.1 Ticket Configuration Management.....	217
9.1.1 Configuring the System Ticket Modes.....	217
9.1.2 Configuring the Ticket Approval Process.....	219
9.2 ACL Ticket.....	221
9.3 Command Approval Ticket.....	223
9.4 Database Approval Ticket.....	225
9.5 Ticket Approval.....	226
9.6 Ticket Application Examples.....	228
10 Operation.....	231

10.1 Host Operation.....	231
10.1.1 Viewing the Host Resource List and Setting Resource Labels.....	231
10.1.2 Logging In to Managed Resources Using a Web Browser for O&M.....	232
10.1.3 Logging In to Resources Using an SSH Client for O&M.....	238
10.1.4 Logging In to File Transfer Resources Using an FTP or SFTP Client.....	240
10.1.5 Logging In to Hosts in Batches for O&M.....	241
10.1.6 File Transmission.....	242
10.1.7 Cooperation.....	250
10.1.8 Enabling Forcible RDP Connections.....	252
10.2 Application Operation.....	253
10.2.1 Viewing the Application Resource List and Setting Resource Labels.....	253
10.2.2 Logging In to Application Resources Using a Web Browser for O&M.....	254
10.3 Script Management.....	258
10.3.1 Creating a Script.....	258
10.3.2 Viewing and Editing Script Information.....	260
10.3.3 Downloading a Script.....	261
10.3.4 Deleting a Script.....	262
10.4 Fast O&M.....	262
10.4.1 Managing Command Operation Tasks.....	262
10.4.2 Managing Script Operation Tasks.....	264
10.4.3 Managing File Transfer Tasks.....	266
10.4.4 Managing Fast Operation Task Execution Logs.....	269
10.5 OM Task.....	270
10.5.1 Creating an OM Task.....	270
10.5.2 Querying and Modifying OM Tasks.....	272
10.5.3 Managing OM Task Execution Logs.....	273
11 Audit.....	275
11.1 Live Session.....	275
11.1.1 Viewing Live Sessions.....	275
11.1.2 Monitoring Live Sessions.....	276
11.1.3 Interrupting a Live Session.....	276
11.2 History Session.....	277
11.2.1 Viewing History Sessions.....	277
11.2.2 Exporting History Session Records.....	281
11.2.3 Managing Session Videos.....	281
11.3 System Logs.....	283
11.3.1 Querying System Logs.....	283
11.3.2 Exporting System Logs.....	284
11.4 Operation Report.....	286
11.4.1 Viewing Operation Reports.....	286
11.4.2 Pushing Operation Reports.....	290
11.5 System Report.....	293

11.5.1 Viewing System Reports.....	293
11.5.2 Pushing System Reports.....	296
12 System Management.....	299
12.1 Sysconfig.....	299
12.1.1 System Configuration Overview.....	299
12.1.2 Network.....	299
12.1.2.1 View Network Configurations.....	299
12.1.2.2 Adding a Static Route to the CBH System.....	300
12.1.3 HA.....	301
12.1.3.1 Enabling HA.....	301
12.1.4 Port.....	303
12.1.4.1 Configuring the Operation Ports.....	303
12.1.4.2 Configuring the Web Console Port.....	304
12.1.4.3 Configuring the SSH Console Port.....	304
12.1.5 Outgoing.....	305
12.1.5.1 Configuring the Outgoing Mail Server.....	305
12.1.5.2 Configuring the Outgoing SMS Gateway.....	306
12.1.5.3 Configuring LTS.....	307
12.1.6 Alarm.....	308
12.1.6.1 Configuring Alarm Channels.....	308
12.1.6.2 Configuring Alarm Levels.....	309
12.1.7 Theme.....	309
12.1.7.1 Changing the System Theme.....	309
12.2 Data Maintenance.....	310
12.2.1 Viewing System Memory.....	310
12.2.2 Configuring the Netdisk Capacity.....	311
12.2.3 Deleting System Data.....	312
12.2.4 Creating a Local Data Backup.....	314
12.2.5 Configuring the Syslog Server for Remote Backup.....	315
12.2.6 Configuring an FTP/SFTP Server for Remote Log Backup.....	316
12.2.7 Configuring OBS Buckets for Remote Log Backup.....	318
12.3 System Maintenance.....	320
12.3.1 Viewing System Status.....	320
12.3.2 System Mgmt.....	322
12.3.3 System Configuration Backup and Restoration (Backup&Restore).....	324
12.3.4 License.....	326
12.3.5 Network Diagnosis.....	327
12.3.6 System Diagnosis.....	328
12.4 About System.....	329
13 FAQs.....	331
13.1 Product Consulting.....	331
13.1.1 What Are the Differences Between a CBH Instance and a CBH System?.....	331

13.1.2 Which Security Hardening Measures Does CBH Provide?.....	331
13.1.3 What Is the Number of Assets?.....	332
13.1.4 What Is the Number of Concurrent Requests?.....	332
13.1.5 Does CBH Support IAM Fine-Grained Management?.....	332
13.1.6 Can I Use a CBH System to Centrally Manage My Cloud ERP or SAP Services?.....	333
13.1.7 What Does Automatic O&M Include?.....	333
13.1.8 How Do I Obtain an Enterprise Agreement Number?.....	333
13.1.9 How Can I Configure Ports for a CBH Instance?.....	334
13.1.10 Can CBH Manage Resources Under Multiple Subnets?.....	335
13.1.11 Which Types of Databases Can I Manage in a CBH System?.....	335
13.2 About Instance Request.....	337
13.2.1 About Instance Request and Deployment.....	337
13.2.2 What Are the Editions of the CBH Service?.....	338
13.2.3 How Do I Configure a Security Group for a CBH Instance?.....	339
13.3 About File Transfer.....	341
13.3.1 What File Transfer Methods Can be Used in a CBH System?.....	341
13.3.2 How Do I Use FTP/SFTP to Transfer Files to or From an SSH Host?.....	342
13.3.3 How Do I Upload or Download Files When I Log In to Managed Hosts Using a Web Browser?....	342
13.3.4 What Is the Netdisk of a CBH System?.....	345
13.3.5 Why Does File Upload to or Download from a Managed Host Fail?.....	345
13.3.6 How Do I Clear the Personal Net Disk Space?.....	348
13.3.7 Why Is File Transfer Not Supported When I Use a Web Browser for Resource O&M?.....	349
13.3.8 Why Does the File List Cannot Be Loaded After I Click File Transfer When I Log In to CBH Through a Web Browser?.....	350
13.3.9 How Do I Configure File Management Permissions?.....	350
13.3.10 Does CBH Check Security of Uploaded Files?.....	352
13.4 About CBH System Login.....	352
13.4.1 Login Methods and Password Issues.....	352
13.4.1.1 Can I Use a Domain Name to Log In to a CBH System?.....	352
13.4.1.2 What Login Methods Does CBH Provide?.....	352
13.4.1.3 Which Login Authentication Methods Are Available in a CBH System?.....	352
13.4.1.4 What Is the Initial Password for Logging In to a CBH System?.....	355
13.4.1.5 How Do I Reset the User Password for Logging In to the CBH System?.....	355
13.4.1.6 How Do I Use IAM to Log In to a CBH Instance?.....	358
13.4.2 Multifactor Verification.....	358
13.4.2.1 How Can I Install an OTP Authentication Application on the Mobile Phone?.....	358
13.4.2.2 Why Does the Mobile OTP Application Binding Operation Fail?.....	359
13.4.2.3 How Do I Enable Mobile SMS Authentication For Logging In to the CBH System?.....	359
13.4.2.4 How Do I Cancel Mobile SMS Authentication?.....	360
13.4.2.5 How Can I Cancel Mobile OTP Authentication If No Mobile OTP Application is Bound to My Account?.....	361
13.4.2.6 Why Does Login Fail When an Account That Has Mobile OTP Application Bound Is Used to Log In?.....	361

13.4.3 Login Security Management.....	362
13.4.3.1 How Do I Set a Security Lock for Logging In to the CBH System?.....	362
13.4.3.2 How Do I Unlock a User or IP Address Locked During the Login to a CBH Instance?.....	363
13.5 User, Resource, and Policy Configuration in a CBH System.....	364
13.5.1 Users.....	364
13.5.1.1 Why Cannot I Select a Superior Department When Creating a User or Resource?.....	364
13.5.1.2 How Do I Change a Mobile Number Bound to a CBH System User?.....	364
13.5.1.3 How Many Users Can Be Created in a CBH System?.....	365
13.5.2 Adding Resources to a CBH System.....	365
13.5.2.1 How Do I Change the Password of a Managed Resource Account?.....	365
13.5.2.2 How Do I Set a Sudo Privilege Escalation Account for the Managed Resource?.....	366
13.5.2.3 How Do I Add a Label to Resources Managed in a CBH System?.....	367
13.5.2.4 How Do I Import or Export Information of Host Resources in Batches?.....	368
13.5.2.5 What Are the AK and SK of an Imported Host? How Can I Obtain Them?.....	369
13.5.2.6 What Are the Statuses of a Managed Resource Account in a CBH System?.....	369
13.5.2.7 Can I Share Labels of Managed Resources with Other System Users?.....	370
13.5.2.8 Can I Manually Enter a Password to Log In to a Managed Resource Through the CBH System?	370
13.5.2.9 Why Does the CBH System Fail to Identify Hosts Imported in Batches?.....	370
13.5.2.10 How Do I Access Services Provided by the Intranet Through a CBH Instance?.....	370
13.5.2.11 How Do I Add a Server with an IPv6 Address to a CBH Instance?.....	371
13.5.2.12 What is an Empty Account?.....	371
13.5.3 System Configuration.....	371
13.5.3.1 How Do I Configure an SSH Key for Logging In to a Managed Host?.....	371
13.5.3.2 How Do I Set the Personal Net Disk Capacity?.....	373
13.5.3.3 How Do I Send More SMS Messages Than the Limit Allowed by CBH.....	374
13.6 Resources Managed in a CBH System.....	374
13.6.1 Operation Management.....	374
13.6.1.1 Can CBH Support GUI-Based O&M for Linux Hosts?.....	374
13.6.1.2 Does CBH Support Mobile App O&M?.....	374
13.6.1.3 How Do I Configure the SSO Tool?.....	375
13.6.1.4 Does CBH Allow Multiple Users to Log In to the Same Resource Concurrently?.....	375
13.6.1.5 Which Algorithms Are Supported by CBH in SSH O&M Mode.....	376
13.6.2 O&M Operations.....	377
13.6.2.1 What Login Methods Does CBH Provide?.....	377
13.6.2.2 How Do I Create a Collaborative O&M Session?.....	378
13.6.2.3 How Do I Use Resource Labels in the CBH System?.....	379
13.6.2.4 How Do I Set the Resolution of the O&M Session Window When I Use a Web Browser for O&M?	380
13.6.2.5 How Can I Use Shortcut Keys to Copy and Paste Text When a Web Browser Is Used for O&M?.....	381
13.6.2.6 What Are the Shortcut Keys for O&M in CBH?.....	382
13.7 O&M Log Audit.....	382
13.7.1 What Audit Logs Does CBH Provide?.....	382

13.7.2 Can I Download Operation Recordings?.....383

13.7.3 Can I Delete CBH O&M Data for a Specific Day?..... 384

13.7.4 Can I Back Up System Audit Logs to an OBS Bucket?.....384

13.7.5 How Long Can I Store Audit Logs in the CBH System?..... 384

13.7.6 How Are Audit Logs in the CBH System Processed?..... 384

13.7.7 Can I Audit User Operations If a User Logs In to Server A Through the CBH System and Then Logs In to Server B from Server A?..... 385

13.7.8 Why Is the Playable Duration Shorter Than the Total Duration of a Session?..... 385

13.7.9 Why Is There No Login Record in History Sessions While I Received a Resource Login Message?. 385

13.8 Troubleshooting..... 385

13.8.1 CBH System Login Failures.....386

13.8.1.1 How Do I Handle Login Exceptions?..... 386

13.8.1.2 Why Is the IP Address or MAC Address Blocked When I Log In to the CBH System?.....386

13.8.1.3 Why Am I Seeing Error Code 404 When I Log In to the CBH System?..... 387

13.8.1.4 Why Am I Seeing Error Code 499 When I Log In to the CBH System?..... 387

13.8.1.5 What Are Possible Faults If I Log In to the CBH System as an Intranet User?..... 388

13.8.1.6 Why Is a Host Inaccessible Through CBH?..... 388

13.8.1.7 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..... 389

13.8.2 CBH Managed Resource Login Failures..... 389

13.8.2.1 Why Does an Exception Occur When I Log In to My Resources Managed in CBH?..... 389

13.8.2.2 Why Am I Seeing Login Errors of Code: T_514 When I Use a Web Browser for Resource O&M? 390

13.8.2.3 Why Am I Seeing Login Errors of Code: T_1006 When I Use a Web Browser for Resource O&M? 392

13.8.2.4 Why Am I Seeing Login Errors of Code: C_515 When I Use a Web Browser for Resource O&M?393

13.8.2.5 Why Am I Seeing Login Errors of Code: C_519 When I Use a Web Browser for Resource O&M?395

13.8.2.6 Why Am I Seeing Login Errors of Code: C_769 When I Use a Web Browser for Resource O&M?397

13.8.2.7 Why Cannot I See the Accessible Resources in the Resource List?..... 398

13.8.2.8 Why Does the Session Page Fail to Load When I Log In to the Managed Host Using a Web Browser?..... 399

13.8.2.9 Why Is the Application Resource Inaccessible through CBH?.....400

13.8.2.10 Why Are Databases Managed in CBH Inaccessible with an SSO Tool?.....401

13.8.2.11 Why Does the Number of Concurrent Sessions Reach the Limit When I Use CBH to Log In to a Host Resource?..... 402

13.8.2.12 Why a Black Block Is Displayed on the Mouse When the MSTSC Client Is Used to Access a Server Resource?..... 402

13.8.3 Maintenance Issues.....403

13.8.3.1 Why Does SMS Verification Code Fail to Send When I Log In to a CBH Instance?..... 403

13.8.3.2 Why Does Verification of An Account for a Managed Host Fail?..... 404

13.8.3.3 Why Am I Seeing Garbled Characters When I Open a System Data File?.....405

13.8.3.4 Why Does Login Timeout Frequently Occur During an O&M Session?..... 405

13.8.3.5 Why Does the PL/SQL Client Display Garbled Characters During Application O&M?.....406

13.8.3.6 Why Is the Requested Session Denied After I Log In to a Managed Host?.....406

13.8.3.7 Why Does the CBH Traffic Bandwidth Exceed the Threshold?.....407

13.8.3.8 Why Text Cannot Be Copied When I Perform O&M Through a Web Browser?.....	407
13.8.3.9 Which Types of Failures May Occur During the O&M?.....	408
13.8.3.10 What Do I Do If an Exception Occurs When I Enter Chinese Characters Using WPS During the O&M of a Windows Server?.....	413
A Change History.....	414

1 Service Overview

1.1 Cloud Bastion Host

Cloud Bastion Host (CBH) is a unified security management and control platform. It provides account, authorization, authentication, and audit management services that enable you to centrally manage cloud computing resources.

A CBH system has various functional modules, such as department, user, resource, policy, operation, and audit modules. It integrates functions such as single sign-on (SSO), unified asset management, multi-terminal access protocols, file transfer, and session collaboration. With the unified O&M login portal, protocol-based forward proxy, and remote access isolation technologies, CBH enables centralized, simplified, secure management and maintenance auditing for cloud resources such as servers, cloud hosts, databases, and application systems.

Service Features

- A CBH instance maps to an independent CBH system. You can configure a CBH instance to deploy the mapped CBH system. A CBH system environment is managed independently to ensure secure system running.
- A CBH system provides a single sign-on (SSO) portal, making it easier for you to centrally manage large-scale cloud resources and safeguard accounts and data of managed resources.
- CBH helps you comply with security regulations and laws, such as Cybersecurity Law, and audit requirements in different standards, including the following:
 - Technical audit requirements in the *Sarbanes-Oxley Act* and *Classified Information Security Protection* standard
 - Technical audit requirements stated by the financial supervision departments
 - O&M audit requirements in relevant laws and regulations, such as *Sarbanes-Oxley Act*, Payment Card Industry (PCI) standards, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27001, and other internal compliance regulations

1.2 Features

CBH enables common authentication, authorization, account, and audit (AAAA) management. Users can obtain O&M permissions by submitting tickets and can invite O&M engineers to perform collaborative O&M.

Credential Authentication

CBH uses multi-factor authentication and remote authentication technologies to enhance O&M security.

- **Multi-factor authentication:** CBH authenticates users by mobile one-time passwords (OTPs), SMS messages, USB keys, and/or OTP tokens. This allows you to mitigate O&M risks caused by leaked credentials.
- **Remote authentication:** CBH interconnects with third-party authentication services or platforms to perform remote account authentication, prevent credential leakage, and ensure secure O&M. Currently, Active Directory (AD), Remote Authentication Dial-In User Service (RADIUS), Lightweight Directory Access Protocol (LDAP), and Azure AD remote authentication are available. CBH allows you to synchronize users from the AD domain server without modifying the original user directory structure.

Account Management

With a CBH system, you can centrally manage system user accounts and managed resource accounts, and establish a visible, controllable, and manageable O&M system that covers the entire account lifecycle.

Table 1-1 Account management

Feature	Description
System user accounts	<p>CBH enables you to grant a unique account with specific permissions to each system user based on their responsibilities. This eliminates security risks resulting from the use of shared accounts, temporary accounts, or privilege escalation.</p> <ul style="list-style-type: none">• Batch importing CBH enables you to synchronize users from a third-party server or import users in batches, eliminating the need to create users repeatedly.• User groups CBH allows you to add users of the same type in a group and assign permissions by user group.• Batch management CBH enables you to manage user accounts in batches, including deleting, enabling, and disabling user accounts, resetting user passwords, and modifying basic user configurations.

Feature	Description
Managed resource accounts	<p>With a CBH system, you can centrally manage accounts of resources managed in the CBH system through the entire account lifecycle, log in to managed resources by using SSO portal, and seamlessly switch between resource management and O&M.</p> <ul style="list-style-type: none"> ● Resource types <p>CBH supports management of a wide range of resource types, including host (such as Windows and Linux hosts) and database (such as MySQL and Oracle) resources.</p> <ul style="list-style-type: none"> - Host resources of the client-server architecture, including hosts configured with the Secure Shell (SSH), Remote Desktop Protocol (RDP), Virtual Network Computing (VNC), Telnet, File Transfer Protocol (FTP), SSH File Transfer Protocol (SFTP), DB2, MySQL, SQL Server, Oracle, Secure Copy Protocol (SCP), or Rlogin protocol. - Application resources of the browser-server architecture or the client-server architecture, including more than 12 types of browser- and client-side Windows applications, such as Microsoft Edge, Google Chrome, and Oracle tools. ● Resource management <ul style="list-style-type: none"> - Batch importing <p>CBH enables quick auto-discovery, synchronization, and batch importing of cloud resources, such as Elastic Cloud Server (ECS) and Relational Database Server (RDS) DB instances on the cloud for centralized O&M.</p> - Account group management <p>CBH manages resource accounts by group. By placing resource accounts of the same attribute in the same group, you can assign permissions on a group basis and let accounts inherit the permissions directly from the group to which they belong.</p> - Password autofill <p>CBH uses the Advanced Encryption Standard (AES) 256-bit encryption technology to encrypt managed resource accounts and uses the password auto-filling technology to encrypt shared accounts, preventing data leakage.</p> - Automatic password change of managed resource accounts <p>CBH supports password change policies so that you can periodically change account passwords to keep managed accounts secure.</p> - Automatic synchronization of managed resource accounts <p>CBH allows you to configure account synchronization policies so that you can periodically check and synchronize account information between the CBH system and the managed host resources. When you create, modify, or delete an account on a host, the same operation is performed in CBH.</p> - Batch management

Feature	Description
	<p>CBH allows you to batch manage information and accounts of managed resources, including deleting a resource, adding a resource label, modifying resource information, verifying a managed account, and deleting a managed account.</p>

Permissions Management

CBH supports fine-grained permission management so that you have complete control over which user can access the CBH system and which managed resources can be accessed by a specific system user, enabling you to safeguard both the CBH system and managed resources.

Table 1-2 Permissions management

Function	Description
<p>CBH system access permission</p>	<p>You can assign permissions to a system user to log in to a CBH system and use different functional modules in the CBH system according to the user's responsibilities.</p> <ul style="list-style-type: none"> ● System user roles CBH supports role-based and module-based permission management so that you can allow a system user to access specific functional modules based on the user's responsibilities. You can use default user roles or create custom roles by adding various functional modules. ● Departments CBH enables department-based system user management, allowing you to specify departments of different levels for each system user. There are no limits on the number of department levels. ● Login restrictions CBH controls system user logins from many dimensions, including login validity period, login duration, multi-factor verification, IP addresses, and MAC addresses.

Function	Description
Managed resource access permission	<p>You can assign permissions for resources by user, user group, account, and account group.</p> <ul style="list-style-type: none">• Access control You can control resource access by resource access validity period, access duration, and IP address. CBH also allows you to assign permissions to users for uploading and downloading files, transferring files, and using the clipboard. When an O&M initiates an O&M session, the watermark indicating their identity will be displayed in the background of the session window.• Two-person authorization You can configure multi-level authorization for users, allowing them to access to a specific resource, and thereby safeguard sensitive and mission-critical resources.• Command interception You can set command control policies or database control policies to forcibly block sensitive or high-risk operations on servers or databases, generate alarms, and review such operations. This gives you more control over key operations.• Batch authorization You can grant permissions for multiple resources to multiple users by user group or account group.

Operation Audit

In a CBH system, each system user has a unique identifier. After a system user logs in to the CBH system, the CBH system logs their operations and monitors and audits their operations on managed resources based on the unique identifier so that any security events can be discovered and reported in real time.

Table 1-3 Operation audit description

Function	Description
System operation audit	<p>All operations in a CBH system are recorded, and alarms are reported for misoperations, malicious operations, and unauthorized operations.</p> <ul style="list-style-type: none">• System logon logs Details about a login, including the login mode, system user, source IP address, and login time, are recorded. System login logs can be exported with just a few clicks.• System operation logs All system operation actions are recorded. System operation logs can be exported with just a few clicks.• System reports CBH displays all operation details of users in one place, including user statuses, user and resource creation, login methods, abnormal logins, and session controls. System reports can be exported with just a few clicks and periodically reported by email.• Alarm notification You can configure different alarm reporting methods and alarm severity levels for system operation and your application environment so that the CBH system sends alarm notifications by email or system messages as soon as it determines system exceptions and abnormal user operations.

Function	Description
Resource O&M audit	<p>A CBH system records user operations throughout the entire O&M process and supports multiple O&M auditing techniques. It audits user operations, identifies O&M risks, and provides the basis for tracing and analyzing security events.</p> <ul style="list-style-type: none"> ● Auditing techniques <ul style="list-style-type: none"> - Linux command audits For command operations through character-oriented protocols (such as SSH and Telnet), a CBH system records the entire O&M process, parses operation commands, reproduces operation commands, and quickly locates and replays operations using keywords in input and output results. - Windows operation audits For operations on terminals and applications through graphics protocol (such as RDP and VNC), the CBH system records all remote desktop operations, including keyboard actions, function key operations, mouse operations, window instructions, window switchover, and clipboard copy. - Database command audit For command operations through database protocols (such as DB2, MySQL, Oracle, and SQL Server), the CBH system records the entire process from single sign-on (SSO) to database command operations, parses database operation instructions, and reproduces all operating instructions. - File transfer audits For file transfer operations through file transfer protocols (such as FTP, SFTP, and SCP), the CBH system audits the entire file transfer process on web browsers or clients, and records the names and destination paths of transferred files. ● O&M audit methods <ul style="list-style-type: none"> - Real-time monitoring Ongoing O&M sessions can be monitored, viewed, and terminated. - History logs All O&M operations are recorded and history session logs can be exported with just a few clicks. - Session videos Linux commands and Windows operations can be recorded by video. Video files can be downloaded with just a few clicks. - Operation reports CBH uses various reports to display O&M statistics in one place, including O&M action distribution over time, resource access times, session duration, two-person authorization, command interception, number of commands, and number of transferred files.

Function	Description
	<p>Operation reports can be exported with just a few clicks and periodically sent by email.</p> <ul style="list-style-type: none"> - Log backup CBH allows you to back up history session logs to a remote Syslog server, FTP/SFTP server, and OBS bucket for disaster recovery.

O&M Functions

CBH supports multiple architectures, tools, and methods to manage a wide range of resources.

Table 1-4 Efficient O&M functions

Function	Description
O&M using a web browser	<p>By leveraging HTML5 for remote logins, O&M engineers can implement O&M operations such as real-time operation monitoring and file uploading and downloading, without installing a client.</p> <ul style="list-style-type: none"> ● One-stop O&M O&M engineers can complete remote O&M anytime anywhere through Microsoft Edge, Google Chrome, or Mozilla Firefox browsers on Windows, Linux, Android, and iOS operating systems without installing plug-ins. ● Batch login CBH supports one-click login to multiple authorized resources, enabling O&M engineers to manage the resources on the same tab page of a browser. ● Collaborative session Allows multiple O&M engineers to perform O&M through a shared O&M session. The user who initiates the O&M session can invite other O&M personnel or experts to join the on-going session and locate problems. This greatly improves O&M efficiency when multiple O&M engineers work together. ● File transmission CBH uses the WSS-based file management technology to upload, download, and manage files online, enabling file sharing among several hosts. ● Command group-sending CBH supports the group sending function for multiple Linux resources. With this function enabled, when a command is executed in a session window, the same operation is performed in other session windows.

Function	Description
Third-party client O&M	<p>CBH enables one-click interconnection with multiple O&M tools, enabling you to perform O&M without changing client usage habits.</p> <ul style="list-style-type: none"> • O&M tools SecureCRT, Xshell, Xftp, WinSCP, Navicat, and Toad for Oracle • SSH clients For host resources with character protocols configured, O&M engineers can log in to them through SSH clients. • Database clients For database-deployed host resources, O&M engineers can log in to databases using configured SSO tools. • File transfer clients For host resources with file transfer protocols configured, O&M engineers can log in to them through FTP or SFTP client.
Automatic O&M	<p>CBH enables automated O&M to simplify online complex operations, eliminating repetitive manual effort and improving efficiency.</p> <ul style="list-style-type: none"> • Script management CBH manages offline scripts, including Shell and Python scripts. • O&M tasks CBH automatically executes one or more preset O&M tasks, such as command execution, script execution, and file transfer tasks.

O&M Ticket Application

During the O&M, if a system user does not have the required permissions for a certain resource, they can submit a ticket to apply for the permissions.

- O&M personnel can:
 - Manually or automatically trigger the ticket system and submit access approval tickets, command approval tickets, and database approval tickets.
 - Submit, query, cancel, and delete tickets.
- System administrators can:
 - Customize approval processes, including multi-level approval processes.
 - Approve one or more tickets at a time, as well as reject, cancel, query, and delete tickets.

1.3 Product Advantages

HTML5 One-stop Management

CBH makes it possible for users to perform O&M anytime, anywhere on any terminal using mainstream browsers (including mobile app browsers) without installing clients or plug-ins.

With an easy-to-use HTML5 UI, CBH gives you the ability to centrally manage users, resources, and permissions. It also enables batch creation of user accounts, batch import of resources, batch authorization of O&M operations, and batch logins to managed resources.

Precise Interception of Commands

CBH presets standard Linux command library or allows you to customize commands, so the CBH system can precisely intercept O&M operation instructions and scripts when corresponding command control rules are triggered. In addition, CBH uses the dynamic approval mechanism to dynamically control sensitive operations in on-going O&M sessions, preventing dangerous and malicious operations.

Multi-level Approval

With CBH, you can enable the multi-level approval mechanism to monitor O&M operations on sensitive and mission-critical resources, improving data protection and management capabilities and keeping data of critical assets secure.

Unified Application Resource Management

CBH gives you the ability to use a unified access entry to manage different application resources, such as databases, web applications, and client programs. It also supports OCR technology, enabling you to convert operations on graphical applications into text files and simplify O&M audits.

Database O&M Audits

For cloud databases such as DB2, MySQL, SQL Server, and Oracle, CBH supports unified resource O&M management and one-click login to the database through SSO portal. To enable efficient audit operations on database resources, CBH records the entire database operation process, parses operation instructions, and reproduces all operation instructions.

Automatic O&M

CBH also gives you the ability to automate complex, repetitive, and large-quantity O&M operations by configuring unified rules and tasks, free O&M personnel from repetitive manual effort, and improve O&M efficiency.

1.4 Application Scenarios

A secure O&M management and audit service is a must-have for any enterprises. CBH is an ideal choice for you. CBH is applicable to various O&M scenarios of enterprise businesses, especially scenarios involving a large number of enterprise employees, a large amount of complex assets, sophisticated O&M personnel construction and permissions, or diversified O&M patterns.

Strict Compliance Audit

Some enterprises, such as enterprises in the insurance and finance industries, have a large amount of personal information data, financial fund operations, and third-

party organization operations. There are big risks of illegal operations, such as violation of regulations and abuse of competence.

CBH gives the ability to those enterprises to establish a sound O&M audit system so that they can comply with industry supervision requirements. With CBH deployed on the cloud, an enterprise can centrally manage accounts and resources, isolate department permissions, configure multi-level review for operations on mission-critical assets, and enable dual-approval for sensitive operations.

Efficient O&M

Some enterprises, such as fast-growing Internet enterprises, have a large amount of sensitive information, such as operations data, exposed on the public networks. Their services are highly open. All these increase data leakage risks.

During the remote O&M, CBH hides the real IP addresses of your assets to protect asset information from disclosure. In addition, CBH provides comprehensive O&M logs to effectively monitor and audit the operations of O&M personnel, reducing network security accidents.

A Large Number of Assets and O&M Staff

As an increasing number of companies move businesses to the cloud, the number of cloud accounts, servers, and network devices also doubles. Many companies outsource system O&M workloads to system suppliers or third-party O&M providers to reduce human resource costs. However, this often involves more than one supplier or agent and increases instability of O&M staff. As a result, risks are increasingly prominent if the monitoring over O&M is not in place.

CBH provides a system to manage a large number of O&M accounts and a wide range of resources in a secure manner. It also allows O&M personnel to access resources using single sign-on (SSO) tools, improving the O&M efficiency. In addition, CBH uses fine-grained permission control so that all operations on a managed resource are recorded and operations of all O&M staff are auditable. Any O&M incidents are traceable, making it easier to locate the operators. Additionally, the CBH system displays the on-going O&M sessions and receives abnormal behavior alarm notifications to ensure that O&M engineers cannot perform unauthorized operations.

1.5 Edition Differences

Currently, CBH provides standard and professional editions. The standard edition provides the following asset specifications: 10, 20, 50, 100, 200, 500, 1,000, 5,000, and 10,000. The professional edition provides the following asset specifications: 10, 20, 50, 100, 200, 500, 1,000, 5,000, and 10,000.

Differences on Specifications

CBH provides the following asset specifications: 10, 20, 50, 100, 200, 500, 1,000, 5,000, and 10,000. For details about specifications, see [Table 1 Configuration of different specifications](#).

Table 1-5 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
500	500	8 cores	16 GB	100 GB	2,000 GB
1,000	1,000	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 1-5](#) 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.

Edition Difference

Both editions provide identity authentication, permission control, account management, and operation audit. Apart from those functions, the enhanced edition also provides automatic O&M and database O&M audit.

For details about functions supported by different editions, see [Table 2 Functions of different editions](#).

Table 1-6 Functions of different editions

Function	Description	Standard edition	Professional edition
Identity authentication	Two-factor authentication for user accounts CBH allows you to configure multi-factor authentication, such as mobile phone one-time passwords (OTPs), mobile phone SMS messages, USB keys, and dynamic OTP tokens to authenticate user identities.	Supported	Supported
	Remote authentication for user accounts CBH also allows you to authenticate user identities through AD, RADIUS, LDAP, Azure AD, and SAML remote authentication.	Supported	Supported
Permission control	System access permission CBH allows you to configure department- and role-based permission control so that you can allow a specific system user to access a specific module in a given CBH system.	Supported	Supported
	Resource access permission CBH allows you to configure resource access control policies based on users, user groups, managed accounts, and account groups to limit what resources can be assessed. You can also configure two-person authorization policies and command control policies to limit what operations are allowed on a certain resource.	Supported	Supported
	Two-person authorization CBH allows you to configure two- or multi-person authorization for core sensitive resources.	Supported	Supported
	Character command interception CBH allows you to configure command control policies to dynamically authorize key operations on character protocol resources.	Supported	Supported
	Database command interception CBH allows you to configure database control policies to precisely restrict and re-review sensitive and risky database operations. NOTE This function applies to cloud databases as well as self-built databases.	Not supported	Supported

Function	Description	Standard edition	Professional edition
Account management	User lifecycle management <ul style="list-style-type: none"> CBH allows you to create a single user account, import user accounts in batches, manage user accounts in batches, and manage user groups. 	Supported	Supported
	Resource account lifecycle management <ul style="list-style-type: none"> CBH allows you to add resources and their accounts one by one or in batches, and classify added accounts into different groups for management. 	Supported	Supported
	Host resource management <ul style="list-style-type: none"> CBH allows you to manage Linux or Windows hosts with the SSH, RDP, VNC, Telnet, FTP, SFTP, DB2, MySQL, SQL Server, Oracle, SCP, or Rlogin protocol configured. 	Supported	Supported
	Application resource management <ul style="list-style-type: none"> If you set Server type to Windows: By default, 14 types are supported, including MySQL Tool, Microsoft Edge, Mozilla Firefox (for Windows servers), Oracle Tool, Google Chrome, VNC Client, SQL Server Tool, SecBrowser, vSphere Client, Radmin, dbisql, Navicat for MySQL, Navicat for PostgreSQL and Other. If you set Server type to Linux: Supported types: DM Tool, KingbaseES Tool, Mozilla Firefox for Linux, and GBaseDataStudio for GBase8a. 	Supported	Supported
	Database resource management <ul style="list-style-type: none"> CBH allows you to manage DB2, MySQL, SQL Server, and Oracle databases. 	Not supported	Supported
	Automatic password change for managed accounts <ul style="list-style-type: none"> CBH allows you to configure password change policies to let the system periodically change passwords of managed accounts. 	Supported	Supported
	Automatic synchronization of managed resource accounts <ul style="list-style-type: none"> CBH allows you to configure account synchronization policies to let the system detect zombie accounts or unmanaged accounts in a timely manner. 	Not supported	Supported

Function	Description	Standard edition	Professional edition
Operation audit	System login and operation logging <ul style="list-style-type: none"> CBH allows you to export system logs, generate system reports, and configure alarm notifications. 	Supported	Supported
	Resource O&M audit <ul style="list-style-type: none"> CBH allows you to audit the entire O&M process through multiple audit methods, such as monitoring on-going sessions, generating videos for history sessions, exporting text reports, and remote log backup. 	Supported	Supported
	Database operation audit <ul style="list-style-type: none"> CBH allows you to audit the entire database O&M process based on operation commands. 	Not supported	Supported
Efficient O&M	One-stop web browser O&M <ul style="list-style-type: none"> CBH allows you to remotely log in to resources without having to install a client with integrated functions, such as batch login, collaborative session, file transfer, and command group sending. 	Supported	Supported
	Third-party client O&M <ul style="list-style-type: none"> CBH can interconnect with multiple O&M tools with just a few clicks, including SSH, FTP, and SFTP client. 	Supported	Supported
	Database O&M <ul style="list-style-type: none"> CBH allows you to log in to the target databases using the single sign-on (SSO) tool with just a few clicks. 	Not supported	Supported
	Automatic O&M <ul style="list-style-type: none"> CBH allows you to manage scripts online and let the system periodically execute preset O&M tasks. 	Not supported	Supported
Ticket application	Access and command authorization ticket application <ul style="list-style-type: none"> CBH allows you to obtain the resource control permissions by manually or automatically triggering a system ticket and submitting the ticket to the system administrator for approval. 	Supported	Supported

Function	Description	Standard edition	Professional edition
	Database authorization ticket application <ul style="list-style-type: none"> • CBH automatically generates an authorization ticket for each sensitive operation from a system user. The system user then needs to submit the ticket to the administrator for approval. The sensitive operation can be resumed only after the application is approved. 	Not supported	Supported

1.6 Basic Concepts

CBH Instance

A CBH instance is an independent CBH system. Users can log in to the CBH console to buy and manage CBH instances. A user can log in to a CBH system to perform secure O&M management and auditing only after the user has purchased a CBH instance.

Single Sign-On

Single sign-on (SSO) is an authentication scheme that allows a user to use a single ID and password to log in to any of several related, yet independent, software systems. After logging in to one of these application systems, the user can access all other related application systems without using other credentials.

Number of Assets

The number of assets refers to the number of resources running on each host managed by CBH. One host may have multiple resources, including protocols and applications running on it.

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

Concurrent Requests

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

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.

1.7 Restrictions on Using CBH

To improve the stability and security of the CBH system, there are some restrictions on the use of CBH instances and their mapped CBH systems.

Network Access Restrictions

- Cross-region resource management is not supported.

A CBH instance and resources (such as ECSs and cloud databases) managed in the mapped CBH system must be in the same region.

Although some services such as Cloud Connect (CC) and Virtual Private Network (VPN) can be used to establish VPCs in different regions, using CBH to manage resources across regions is still not recommended because the cross-region network is less stable.
- Cross-VPC resource management is not supported.

A CBH instance and resources (such as ECSs and cloud databases) managed in the mapped CBH system must be in the same VPC so that the CBH system can communicate the managed resources directly.

If they are in different VPCs, use a VPC peering connection to connect two VPCs.
- Communication between the CBH instance security group and managed resource security group must be allowed.

The managed resources must be accessible through the security group to which the CBH instance belongs, and the security group to which the resources belong must allow access from the private IP address of the CBH instance.

If a CBH instance and its managed resources belong to different security groups, no communication between them is established by default. To establish a connection, add an inbound rule to the CBH instance security group.

The default ports of the security group are ports 443 and 2222, which can be accessed through a web browser or SSH client by default. To use other access methods, manually add the destination port.

For details, see [Table 1-7](#).
- A CBH system can be logged in only through IP address and port number.

Table 1-7 Inbound and outbound rule configuration reference

Scenario Description	Direction	Protocol/ Application	Port
Accessing CBH through a web browser (HTTP and HTTPS)	Inbound	TCP	80, 443, and 8080

Scenario Description	Direction	Protocol/ Application	Port
Accessing a CBH system through Microsoft Terminal Services Client (MSTSC)	Inbound	TCP	53389
Accessing a CBH Instance Through an SSH Client	Inbound	TCP	2222
Accessing CBH instances through FTP clients	Inbound	TCP	20~21
Remotely accessing Linux ECSs of CBH instances over SSH clients	Outbound	TCP	22
Remotely accessing Windows ECSs of CBH instances over the RDP Protocol	Outbound	TCP	3389
Accessing Oracle databases through CBH instances	Inbound	TCP	1521
Accessing Oracle databases through CBH instances	Outbound	TCP	1521
Accessing MySQL databases through CBH instances	Inbound	TCP	33306
Accessing MySQL databases through CBH instances	Outbound	TCP	3306
Accessing SQL Server databases through CBH instances	Inbound	TCP	1433
Accessing SQL Server databases through CBH instances	Outbound	TCP	1433
Accessing DB databases through CBH instances	Inbound	TCP	50000
Accessing DB databases through CBH instances	Outbound	TCP	50000
Accessing GaussDB databases through CBH	Inbound	TCP	18000
Accessing GaussDB databases through CBH	Outbound	TCP	18000
License servers	Outbound	TCP	9443
Cloud services	Outbound	TCP	443
Accessing a CBH system through the SSH client in the same security group	Outbound	TCP	2222

Scenario Description	Direction	Protocol/ Application	Port
SMS service	Outbound	TCP	10743 and 443
Domain name resolution service	Outbound	UDP	53
Accessing PGSQL databases through CBH	Inbound	TCP	15432
Accessing PGSQL databases through CBH	Outbound	TCP	5432

Supported Resources

- Supported host types
CBH allows you to manage Linux or Windows hosts with the SSH, RDP, VNC, Telnet, FTP, SFTP, SCP, or Rlogin protocol configured.
- Supported database types
 - Databases on Elastic Cloud Servers (ECSs)
- Supported database versions

Table 1-8 Supported database versions

Database Engine	Engine Version
MySQL	MySQL 5.5, 5.6, 5.7, and 8.0
Microsoft SQL Server	2014, 2016, 2017, 2019, and 2022
Oracle	10g, 11g, 12c, 19c, and 21c
DB2	DB2 Express-C
PostgreSQL	11, 12, 13, 14, and 15
GaussDB	2 and 3

- Supported application server types and versions
Only applications on Windows servers and Linux servers can be managed. [Table 1-9](#) lists the supported operating system versions.

Table 1-9 Supported application server types and versions

OS Type	Version
Windows	Windows Server 2008 R2 or later
Linux	CentOS7.9

 **NOTE**

Currently, application O&M is available only on the x86 CBH instances.

Supported Third-Party Clients

To perform secure O&M management through CBH, use a third-party client to log in to the CBH system.

Table 1-10 Clients and versions supported for logging in to the CBH system

Login Type	Supported Client	Version
Logging in to a CBH system from a web browser	Edge	Microsoft Edge 44 or later NOTE When you use Microsoft Edge, the maximum size of a file that can be uploaded to a host is 4 GB.
	Google Chrome	Google Chrome 52.0 or later
	Safari	Safari 10 or later
	Mozilla Firefox	Mozilla Firefox 50.0 or later
Login using an SSH client	SecureCRT	SecureCRT 8.0 or later
	Xshell	Xshell 5 or later
	Mac Terminal	Mac Terminal 2.0 or later

Table 1-11 Clients that can be invoked during operation

Operation Method	Resource Protocol Type/Application Type	Supported Client
Database operation (in the Host Operations module)	MySQL	Navicat 11, 12, 15, and 16 MySQL Administrator 1.2.17 MySQL CMD DBeaver 22 and 23
	SQL Server	Navicat 11, 12, 15, and 16 SSMS 17

Operation Method	Resource Protocol Type/Application Type	Supported Client
	Oracle	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
	DB2	DB2 CMD command line 11.1.0
File Transfer	SFTP	Xftp, WinSCP, and FlashFXP
	FTP	Xftp, WinSCP, FlashFXP, and FileZilla
Application operation	MySQL Tool	MySQL Administrator
	Oracle Tool	PL/SQL Developer
	SQL Server Tool	SSMS
	dbisql	dbisql
	Google Chrome	Google Chrome
	Edge	Edge
	Mozilla Firefox	Mozilla Firefox
	VNC Client	VNC Viewer
	SecBrowser	SecBrowser
	vSphere Client	vSphere Client
	Radmin	Radmin

Other Constraints

- The maximum number of resources that can be managed by CBH cannot exceed the number of assets allowed by the instance edition.
- The maximum number of resources that can be concurrently logged in to through CBH cannot exceed the number of concurrent requests allowed by the CBH instance edition.

NOTE

The number of assets refers to the number of resources running on a cloud host managed by CBH. One cloud host may have multiple resources, including protocols and applications running on it.

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

For more details, see [Basic Concepts](#).

1.8 Permissions Management of CBH Instances

If you need to assign different permissions to employees in your enterprise to access your CBH instances, IAM is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you securely manage access to your cloud resources.

With IAM, you can create IAM users under your account for your employees, and assign permissions to the users to control their access to specific resource types. For example, you can create IAM users for the software developers and assign specific permissions to allow them to only use CBH instances but not to create, change specifications of, or upgrade CBH instances.

If your account does not need individual IAM users for permissions management, then you may skip over this section.

IAM is free. You pay only for the resources in your account. For more information about IAM, see IAM Service Overview.

CBH Instance Permissions

By default, new IAM users do not have any permissions assigned. You can add a user to one or more groups to allow them to inherit the permissions from the groups to which they are added.

CBH is a project-level service deployed and accessed in specific physical regions. To assign CBH permissions to a user group, specify the scope as region-specific projects and select projects for the permissions to take effect. If **All projects** is selected, the permissions will take effect for the user group in all region-specific projects. When accessing a CBH instance, switch to a region where they have been authorized to use the CBH instance.

You can grant users permissions by using roles and policies.

- **Roles:** A type of coarse-grained authorization mechanism that defines permissions related to users responsibilities. Only a limited number of service-level roles for authorization are available. You need to also assign other dependent roles for the permission control to take effect. Roles are not ideal for fine-grained authorization and secure access control.
- **Policies:** A fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions. This mechanism allows for more flexible policy-based authorization and meets secure access control requirements. For example, you can grant CBH users only the permissions for managing a certain type of resources.

Table 1-12 lists all the system-defined roles and policies supported by CBH instances.

Table 1-12 System permissions for CBH instances

Role/Policy Name	Description	Type	Dependency
CBH FullAccess	All permissions (except the payment permission) on CBH instances	System-defined policy	None
CBH ReadOnlyAccess	Read-only permissions for CBH instances. Users who have read-only permissions granted can only view CBH instances but not configure services.	System-defined policy	None

 **NOTE**

To use all CBH functions on the CBH console, you need to have the CBH FullAccess role assigned at the enterprise project level and the CBH ReadOnlyAccess role assigned at the IAM project level.

Table 1-13 lists the common operations for each system-defined policy or role of CBH instances. Select the policies or roles as required.

Table 1-13 Common operations for each system-defined policy or role of CBH

Operation	CBH FullAccess	CBH ReadOnlyAccess
Creating a CBH instance	√	x
Changing CBH instance specifications (changing specifications)	√	x
Querying the CBH instance list	√	√
Upgrading the CBH system version	√	x
Querying total ECS quota	√	x
Binding or unbinding an EIP	√	x
Restarting a CBH instance	√	x
Starting a CBH instance	√	x
Stopping a CBH instance	√	x
Querying the AZ of a CBH instance	√	x
Checking whether an IPv6 CBH instance can be created	√	x

Operation	CBH FullAccess	CBH ReadOnlyAccess
Checking network connection between the CBH instance and the license center	√	x
Modifying the network of the CBH instance to ensure that the CBH instance can communicate with the license center	√	x

CBH FullAccess Policy Content

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cbh:*",
        "vpc:subnets:get",
        "vpc:publicIps:list",
        "vpc:vpcs:list",
        "vpc:securityGroups:get",
        "vpc:firewallGroups:get",
        "vpc:firewallPolicies:get",
        "vpc:firewallRules:get",
        "vpc:ports:get",
        "vpc:publicIps:update",
        "vpc:securityGroups:create",
        "vpc:firewallRules:create",
        "vpc:firewallPolicies:addRule",
        "ecs:cloudServerFlavors:get",
        "evs:types:get"
      ]
    }
  ]
}
```

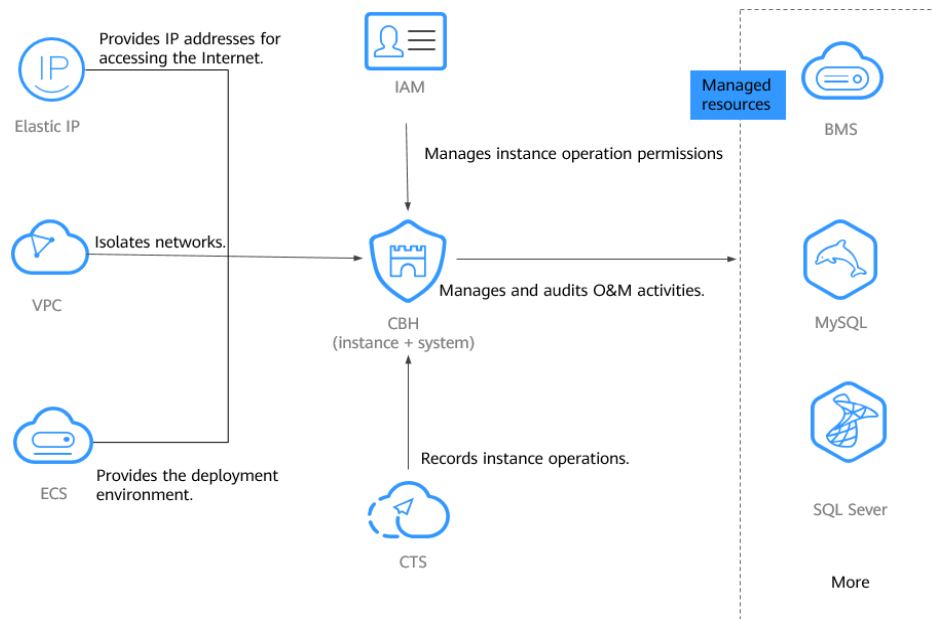
CBH ReadOnlyAccess Policy Content

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cbh:*:list*",
        "vpc:publicIps:list",
        "vpc:vpcs:list",
        "vpc:securityGroups:get",
        "vpc:subnets:get"
      ]
    }
  ]
}
```

1.9 CBH and Other Services

CBH needs to work with other cloud services. **Figure 1-1** shows the dependencies between CBH and other cloud services.

Figure 1-1 CBH and other services



VPC

Virtual Private Cloud (VPC) provides a virtual network environment for you to configure security groups, subnets, and Elastic IP Addresses (EIPs) for your CBH instances. This allows you to manage and configure internal networks. You can also customize access rules for security groups to enhance security.

ECS

Elastic Cloud Server (ECS) provides a deployment environment for CBH instances, and CBH provides security management services for resources on ECSs.

- ECSs are used to deploy the CBH background environment, which uses the EulerOS operating system.
- You can log in to resources, such as servers and databases, on ECSs through CBH to manage those resources and login credentials and audit O&M sessions in a more secure way.

EIP

Elastic IP Address (EIP) provides independent public network IP addresses and egress bandwidths. Each public EIP can be used by only one cloud resource at a time. With an EIP bound to a CBH instance, users can access the Internet through the mapped CBH system. You can adjust the EIP bandwidth at any time to meet your business traffic changes.

CTS

Cloud Trace Service (CTS) generates traces to enable you to get a history of operations performed on CBH instances, allowing you to query, audit, and backtrack resource operation requests initiated from the management console as well as the responses to those requests.

CTS records operations on CBH instances for later query, auditing, and backtracking. For details, see [CBH Operations Supported by CTS](#).

IAM

Identity and Access Management (IAM) helps you to manage permissions and identity authentication for users of CBH instances. For more details, see [Permissions Management](#).

1.10 Personal Data Protection Mechanism

No personal data is gathered by a CBH instance. After an instance is created, you need to create a user account for logging in to the CBH system. Creating a user account for logging in to the system requires personal data.

To ensure that your personal data, such as the username, password, and mobile phone number for logging in to a CBH system, will not be obtained by unauthorized or unauthenticated entities or people and to prevent data leakage, CBH encrypts your personal data before storing it to control access to the data and records logs for operations performed on the data.

Personal Data to Be Collected

[Table 1-14](#) lists the personal data generated or collected by CBH.

Table 1-14 Personal data

Item	Type	Collection Method	Can Be Modified	Mandatory
CBH instances	Login name	Login name configured by the system administrator during user creation	No	Yes Login names are used to identify users.

Item	Type	Collection Method	Can Be Modified	Mandatory
	Password	<ul style="list-style-type: none"> • Password configured by the system administrator during user creation or password resetting • Password reset by a user when they log in to a CBH system for the first time or password changed by a user after the user logs in to the CBH system 	Yes	Yes This password is used by the user to log in to a CBH system.
	Email	<ul style="list-style-type: none"> • Email address configured by the administrator during user creation • Email address entered by a user after the user logs in to the CBH system 	Yes	Yes This email address is used to receive notifications sent by the CBH system.
	Mobile number	<ul style="list-style-type: none"> • Mobile phone number configured by the administrator during user creation • Mobile phone number entered by a user after the user logs in to the CBH system 	Yes	Yes <ul style="list-style-type: none"> • This mobile phone number is used to receive SMS notifications from the CBH system. • This mobile phone number is also used to receive verification codes sent by the CBH system during password resetting.

Storage Mode

CBH uses encryption algorithms to encrypt users' sensitive data and stores encrypted data.

- Login names are not sensitive data and stored in plaintext.

- Passwords, email addresses, and mobile numbers are encrypted for storage.

Access Permission Control

Your personal data is encrypted for storage in CBH. A security code is required for the system administrators and upper-level administrators when they attempt to view your mobile number and email addresses. However, passwords of all users are invisible to all.

Two-factor Authentication

After multi-factor authentication is configured for a user, the user needs to be authenticated twice when logging in to the CBH system. The secondary authentication includes SMS message, mobile OTP, USB key, and dynamic token modes. This effectively protects sensitive user information.

Logging

The CBH system records audit logs for all operations on users' personal data, including adding, modifying, querying, and deleting data. The logs can be backed up to a remote server or local computer. Users with the audit permission can view and manage logs of user accounts in lower-level departments. The system administrator **admin** has the highest permissions and can view and manage operation records of all user accounts used to log in to the CBH system.

1.11 Security Statement

Before using CBH, read this security statement carefully and perform accordingly to avoid network security issues.

Managing Accounts

The default account **admin** is the default administrator of a CBH system. The password of **admin** user is the password you set during purchase of the CBH instance.

Change the password as prompted upon your first login to the CBH system. Otherwise, the CBH system page cannot be reached.

Managing Passwords

To ensure security, you are advised to set passwords according to the following rules:

- Change the password and configure phone number as prompted after you log in to the CBH system. Otherwise, the requested CBH system cannot be reached.
- The complexity of a password must meet the following security policies:
 - Contain 8 to 32 characters.
 - Contain at least three of the following character types: uppercase letters (A to Z), lowercase letters (a to z), digits (0 to 9), and special characters.

- Cannot contain the username or the username spelled backwards.
- It is recommended that you periodically change your password for account security.

Feature Statement

- The purchased products, services and features are stipulated by the contract made between us. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope.
- 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.
- CBH supports the HTTPS protocol but not the HTTP protocol.
- Make sure CBH is used in compliance with laws and regulations.

Third-Party Software

CBH uses the following third-party software:

- Browsers and versions for logging in to a CBH system. For details, see [Table 1-15](#).

Table 1-15 Recommended browsers and versions

Browser	Version	Description
Edge	44 or later	Upload restriction: On the H5 O&M page, the maximum size of a single uploaded file is 4 GB.
Chrome	52.0 or later	None
Safari	10 or later	None
Firefox	50.0 or later	None

Such software can be downloaded in either of the following ways:

- Log in to the CBH system as a system administrator. On the page that is displayed, click the download icon in the upper right corner. On the displayed **Download Center** page, download the required software.
- Log in to the CBH system as an O&M user. On the page that is displayed, click the download icon in the upper right corner. On the displayed **Download Center** page, download the required software.

2 Instances

2.1 Permissions Management

2.1.1 Creating a User and Granting Permissions for CBH Instances to It

To implement fine-grained permissions control for your CBH resources, Identity and Access Management (IAM) is exactly what you need. With IAM, you can:

- Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has their own security credentials, providing access to CBH resources.
- Grant only the permissions required for users to perform a task.
- Entrust an account or cloud service to perform professional and efficient O&M on your CBH resources.

If your account does not require individual IAM users, skip over this section.

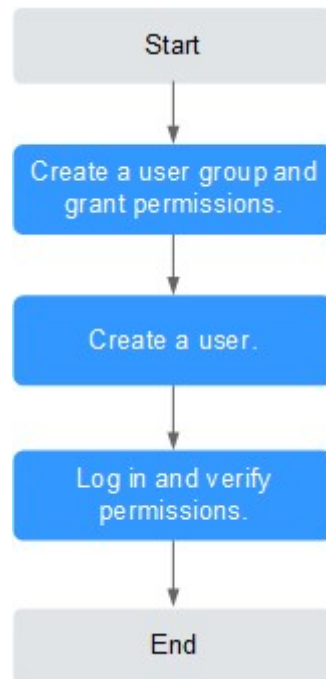
This section describes the procedure for granting permissions. [Figure 2-1](#) shows the process.

Prerequisites

Learn about the permissions supported by CBH and choose policies or roles based on your requirements. For more details, see [Permissions Management of CBH Instances](#).

Authorization Process

Figure 2-1 Process for granting permissions



1. Create a user group and assign permissions.
Create a user group on the IAM console, and attach the **CBH ReadOnlyAccess** policy to the group.
2. Creating an IAM User.
Create a user on the IAM console and add the user to the group created in **1**.
3. Log in and verify permissions.
Log in to the CBH console by using the created user, and verify that the user only has read permissions for CBH.
 - Choose **Service List > Cloud Bastion Host**. On the displayed page, click **Purchase CBH Instance**. If a message is displayed indicating that you do not have the permission to purchase the CBH instance (assume that the current permission contains only CBH ReadOnlyAccess), the CBH ReadOnlyAccess policy has taken effect.
 - Choose any other service in **Service List**. (Assume that the current permission contains only CBH ReadOnlyAccess). If a message appears indicating that you have insufficient permissions to access the service, the CBH ReadOnlyAccess policy has already taken effect.

2.1.2 Creating Custom Policies for CBH Instances

Custom policies can be created to supplement the system-defined policies of CBH. For the actions that can be added to custom policies, see [CBH Permissions and Supported Actions](#).

You can create custom policies in either of the following ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

For details, see *Creating a Custom Policy in Identity and Access Management User Guide*. The following section contains examples of common custom policies for CBH instances.

Example Custom Policies

- Example 1: Allowing users to change CBH instance specifications and upgrade CBH instance version.

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cbh:instance:upgrade",
        "cbh:instance:alterSpec"
      ]
    }
  ]
}
```

- Example 2: Denying a user request of restarting a CBH instance

A deny policy must be used together with other policies. If the policies assigned to a user contain both Allow and Deny actions, the Deny actions take precedence over the Allow actions.

The following method can be used to create a custom policy to disallow users who have the **CBH FullAccess** policy assigned to restart a CBH instance. Assign both **CBH FullAccess** and the custom policies to the group to which the user belongs. Then the user can perform all operations on CBH except restarting a CBH instance. The following is an example of a deny policy:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cbh:instance:reboot"
      ]
    }
  ]
}
```

- Example 3: Defining permissions for multiple services in a policy

A custom policy can contain the actions of multiple services that are of the global or project-level type. The following is an example policy containing actions of multiple services:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cbh:instance:create"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [

```

```

        "vpc:subnets:get"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "ecs:cloudServerFlavors:get"
    ]
  }
]
}

```

2.1.3 Managing CBH Instance Permissions and Supported Actions

This section describes fine-grained permissions management for your CBH. If your account does not need individual IAM users, then you may skip over this section.

By default, new IAM users do not have any permissions assigned. You need to add a user to one or more groups, and assign permissions policies to these groups. Users inherit permissions from the groups to which they are added and can perform specified operations on cloud services based on the permissions.

Permissions are classified into roles and policies based on the authorization granularity. Roles: A type of coarse-grained authorization mechanism that defines permissions related to user responsibilities. Policies: A type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions.

Supported Actions

CBH provides system-defined policies that can be directly used in IAM. You can also create custom policies and use them to supplement system-defined policies, implementing more refined access control.

- Permission: A statement in a policy that allows or denies certain operations.
- Action: Specific operations that are allowed or denied.

Table 2-1 Supported Actions

Permission	Action
Querying the AZ of a CBH instance	cbh:instance:getAvailableZones
Checking whether an IPv6 CBH instance can be created	cbh:instance:checkIpv6
Checking network connection between the CBH instance and the license center	cbh:network:check
Querying total ECS quota	cbh:instance:getEcsQuota
Stopping a CBH instance	cbh:instance:stop
Starting a CBH instance	cbh:instance:start

Permission	Action
Modifying the network of the CBH instance to ensure that the CBH instance can communicate with the license center	cbh:network:change
Changing the VPC a CBH instance belongs to	cbh:instance:switchVpc
Upgrading the CBH system version	cbh:instance:upgrade
Logging in to a CBH instance as user admin	cbh:instance:loginInstanceAdmin
Modifying the CBH configuration	cbh:instance:modify
Logging n to a CBH instance	cbh:instance:login
Obtaining the CBH O&M Link	cbh:instance:getOmUrl
Changing the type of a single-node CBH instance	cbh:instance:changeInstanceType
Enabling expert O&M service	cbh:expert:create
Changing the password of the admin user for a CBH instance	cbh:instance:resetPassword
Creating a CBH instance	cbh:instance:create
Changing the VPC a CBH instance belongs to	cbh:instance:switchInstanceVpc
Creating a CBH agency	cbh:agency:authorize
Restarting a CBH instance	cbh:instance:reboot
Binding or unbinding an EIP	cbh:instance:eipOperate
Changing the VPC a CBH instance belongs to	cbh:instance:switchInstanceVpcTest
Expanding a CBH instance edition	cbh:instance:alterSpec
Changing the type of a single-node CBH instance	cbh:instance:changeInstanceTypeTest
Logging in to a CBH instance as user admin	cbh:instance:loginInstanceAdminTest
Querying the CBH instance list	cbh:instance:list
Querying the O&M expert service list	cbh:expert:list


2.2 Checking CBH Instance Details

Each CBH instance maps to an independently running CBH system.

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

Checking CBH Instance Information

Step 1 Log in to the management console.

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

Step 3 Click the instance and check the instance details.

Table 2-2 Instance parameters



Parameter	Description
Instance Name	Instance name you specify. It cannot be modified after the instance is created.
Billing Mode	Billing mode of the current instance
VPC	VPC the instance belongs to
Server ID	ID of the server housing the current instance. The ID of the server for the standby node is included.
Security group	Virtual network security rule.
Instance Type	Instance type you select.
Subnet	Subnet of the VPC.
Standby Instance Status	Status of the standby node.
Virtual IP Address	Floating IP address of the current instance.
Specifications	Edition you select for your instance.
Upon Expiration	If an instance expires, it enters a grace period. You can check details about the grace period rules.
Private IP Address	Private IP address of the instance, including the IP address of the standby node.
Instance Version	Version of the instance.
Enterprise Project	Enterprise project that the instance belongs to.

----End

2.3 Resetting the Login Method for User admin

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

Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation pane on the left, click  and choose **Security & Compliance > Cloud Bastion Host** to go to the CBH console.
- Step 4** Locate the row containing the instance for which you want to reset login passwords. In the **Operation** column, choose **More > Reset > Reset Login Method for Admin**.
- Step 5** In the displayed dialog box, click **OK** to reset the login method for user **admin**.

NOTE



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

----End

2.4 Resetting the Password of User Admin

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

Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation pane on the left, click  and choose **Security & Compliance > Cloud Bastion Host** to go to the CBH console.
- Step 4** Locate the row containing the instance you want to restart. In the **Operation** column, choose **More > Reset > Reset Admin Password**.
- Step 5** In the dialog box displayed, reset the password of the admin account.
- Step 6** Click **OK**.

----End

2.5 Upgrading the CBH System Version

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

Precautions

- Before the upgrade
 - Back up data to ensure a quick rollback in case of upgrade failures.
- During the upgrade

The version upgrade takes about 30 minutes. Although the CBH system is unavailable during this period, there is no impacts on host resources managed on the instance. However, to prevent important data loss, do not log in to the CBH system during the version upgrade.
- After the upgrade

The CBH instance automatically restarts after the upgrade completes. You can then use the mapped CBH system.

After the upgrade, you can use the configuration and storage data of the original CBH system. Version upgrading does not affect the original configuration and storage data of the CBH system.
- Rolling Back the Upgrade

After the version upgrade is complete or during the cross-version upgrade, you can roll back the upgrade on the bastion host details page. After the rollback starts, the status of the bastion host changes to **Rolling back edition**.

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

Constraints


- In the new version of CBH, the application publish function is optimized. After the upgrade, to use the application O&M functions as usual, install the required plug-in on the application publish server as prompted.
- To upgrade version 3.3.40.0 and 3.3.41.0, synchronize the time of OBS buckets first.


Prerequisites

- The CBH system data has been backed up.

Procedure

Step 1 Log in to the management console.

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

- Step 3** In the navigation pane on the left, click  and choose **Security & Compliance > Cloud Bastion Host** to go to the CBH console.
- Step 4** Locate the row containing the instance you want to upgrade. In the **Operation** column, choose **More > Upgrade > Upgrade Edition**.
- Step 5** In the displayed dialog box, select the schedule upgrade time and enter **UPGRADE** to confirm. To cancel the upgrade schedule, enter **CANCEL** in the dialog box. You can also change the upgrade schedule you set before.

 **NOTE**

Upgrade types:

- During a minor version upgrade, the CBH instance you are using will be interrupted. It takes about 15 to 30 minutes to complete the upgrade.
- During the cross-version upgrade, a new CBH instance will be created, and the CBH instance you are using will be interrupted. It takes about 30 minutes to 2 hours to complete the upgrade. During the cross-version upgrade, the instance status changes to **Upgrading** first, and then to **Migrating data, Configuring HA**, and to **Running**.

- Step 6** Wait for the upgrade to complete. It takes about 15 minutes to 2 hours for the upgrade to finish at the backend. The actual upgrade time varies depending on the upgrade type. Once the upgrade starts, the instance status changes to **Upgrading**.
- Step 7** When the CBH instance status changes to **Running**, the CBH system is available.

 **NOTE**

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



----End

2.6 Starting a CBH Instance

The instance needs to be started in the following scenarios:

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

Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation pane on the left, click  and choose **Security & Compliance > Cloud Bastion Host** to go to the CBH console.
- Step 4** Locate the row containing the instance you want to start. In the **Operation** column, click **Start**.

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

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


----End

2.7 Stopping a CBH Instance

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

Procedure

Step 1 Log in to the management console.

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

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

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

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

NOTE

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

----End


2.8 Restarting a CBH Instance


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

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

Procedure

Step 1 Log in to the management console.

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

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

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

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

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

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

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

 **NOTE**

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

----End

2.9 Changing a VPC for a CBH Instance


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


Constraints

- The CBH instances must be in the **Running** status.
- At least three IP addresses are required in the VPC subnet you will use.
- The CBH instance version must be V3.3.52.0 or later.

Procedure

Step 1 Log in to the management console.

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

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

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

Step 5 In the dialog box displayed, specify **VPC** and **Subnet**.

 **NOTE**

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

----End

2.10 Changing Security Groups

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


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


Constraints

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

Procedure

Step 1 Log in to the management console.

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

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

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

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

Step 6 Click **Yes**.

----End

2.11 Binding an EIP to a CBH Instance

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

- Log in to the CBH system using a web browser. URL: `https:// EIP of the CBH instance`, for example, `https://10.10.10.10`.

- If the mobile SMS login is configured, you need to obtain the verification code through the mobile phone. If the EIP is not configured, you cannot receive SMS messages.
- Interconnect with LTS to send logs. For details, see [Configuring LTS](#).
- In V3.3.2.0 and earlier versions, if no EIP is bound to a CBH instance, operations such as changing the version specifications, upgrading the version, starting or restarting the instance, and renewing the instance will fail.

Constraints

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

Prerequisites


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


CAUTION

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

Procedure

Step 1 Log in to the management console.

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

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

Step 4 Locate the row containing the instance to which you want to bind an EIP. In the **Operation** column, choose **More > Configure Network > Bind EIP**.

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



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

----End

2.12 Unbinding an EIP from a CBH Instance

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

Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation pane on the left, click  and choose **Security & Compliance > Cloud Bastion Host** to go to the CBH console.
- Step 4** Locate the row containing the instance from which you want to unbind an EIP. In the **Operation** column, choose **More > Configure Network > Unbind EIP**.
- Step 5** In the displayed dialog box, click **OK**.

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

----End

2.13 Key CBH Instance Operations Recorded by CTS

2.13.1 CBH Operations Supported by CTS

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

After CTS is enabled, the system starts to record CBH operations. You can view operation records generated in the latest seven days on the CTS console. [Table 2-3](#) lists the CBH instance operations that can be recorded by CTS.

Table 2-3 CBH instance operations



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

Operation	Resource Type	Trace Name
Upgrading a CBH instance	cbh	upgradeInstance
Changing specifications of a CBH instance	cbh	alterInstanceSpec
Rolling back a CBH instance	cbh	rollbackInstance
Resetting the Admin password	cbh	resetPassword
Resetting login method for user Admin	cbh	resetLoginMethod
Changing network settings for a CBH Instance	cbh	changeNetworkOfCBH

2.13.2 Viewing CTS Traces

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

Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and project.
- Step 3** In the navigation pane on the left, click  and choose **Management & Deployment > Cloud Trace Service**.
- Step 4** On the left navigation pane, choose **Trace List**.
- Step 5** Specify the filters used for querying traces. The following filters are available:
 - **Trace Source, Resource Type, and Search By**
 - Select a search criteria from the drop-down list box. For example, choose **CBH > cbh > Trace Name > createInstance**, and click **Query** to query all instance creation operations.
 - **Trace Name:** Select a trace name, for example, **createInstance**.
 - **Resource ID:** Select or manually enter the ID of a CBH instance whose logs are to be viewed.
 - **Resource Name:** Select or manually enter the name of a CBH instance whose logs are to be viewed.
 - **Operator:** Select a specific operator (a user rather than tenant).
 - **Trace Status:** Available options include **All trace statuses, normal, warning, and incident**. You can only select one of them.

- You can specify start time and end time query traces during a time period.

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

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

----End

3 Logging In to the CBH System

3.1 Overview

Port Requirements

To use the CBH system for resource management, ensure that the communication between the CBH system and the managed resources is enabled. Before you start, check whether your network ACL configuration allows access to CBH and configure the security group of the mapped CBH instance by referring to [Table 3-1](#).

Table 3-1 Inbound and outbound rule configuration reference

Scenario Description	Direction	Protocol/ Application	Port
Accessing CBH through a web browser (HTTP and HTTPS)	Inbound	TCP	80, 443, and 8080
Accessing a CBH system through Microsoft Terminal Services Client (MSTSC)	Inbound	TCP	53389
Accessing a CBH Instance Through an SSH Client	Inbound	TCP	2222
Accessing CBH instances through FTP clients	Inbound	TCP	20~21
Remotely accessing Linux ECSs of CBH instances over SSH clients	Outbound	TCP	22
Remotely accessing Windows ECSs of CBH instances over the RDP Protocol	Outbound	TCP	3389
Accessing Oracle databases through CBH instances	Inbound	TCP	1521

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

Verification Type

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

Table 3-2 Authentication methods

Verification Type	Authentication Description
Local Authentication	<p>Static passwords configured for the CBH system are used for identity verification.</p> <ul style="list-style-type: none"> • Multifactor verification can be configured for users authenticated by static password. • You can reset or change the static passwords through CBH. If you forgot this password, you can find it back through email.
AD domain authentication	<p>The passwords of users on the AD server are used for identity verification.</p> <ul style="list-style-type: none"> • Multifactor verification can be configured for users authenticated by static password. • Passwords cannot be changed through the CBH system.
RADIUS Authentication	<p>The passwords of users on the RADIUS server are used for identity verification.</p> <ul style="list-style-type: none"> • Multifactor verification can be configured for users authenticated by static password. • Passwords cannot be changed through the CBH system.
LDAP Authentication	<p>The passwords of users on the LDAP server are used for identity verification.</p> <ul style="list-style-type: none"> • Multifactor verification can be configured for users authenticated by static password. • Passwords cannot be changed through the CBH system.
Azure AD authentication	<p>The passwords of Microsoft accounts are used for identity verification.</p> <p>The login page is redirected to the Microsoft Azure login page for you to provide credentials.</p> <ul style="list-style-type: none"> • Multifactor verification cannot be configured for users authenticated by the Azure AD server. • Passwords cannot be changed through the CBH system.

Logon Type

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

Table 3-3 Login method description

Logon Type	Login Description
Password	Enter the username and password of your CBH system account.

Logon Type	Login Description
Mobile SMS Authentication	Enter the username and password of your CBH system account, click Send Code , and enter the SMS verification code you will receive.
Mobile OTP	Enter the username and password first, and then enter the mobile one-time password (OTP).
USBKey	Insert your USB key into your terminal device, select the issued USB key, and enter the corresponding personal identification number (PIN).
One-time Passwords (OTPs)	Enter the username and password first, and then enter the verification code displayed on your OTP token device.

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

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

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

NOTE

- First-time login users are required to bind a mobile number for password resetting.

Prerequisites

An EIP has been bound to the CBH instance.

Procedure

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

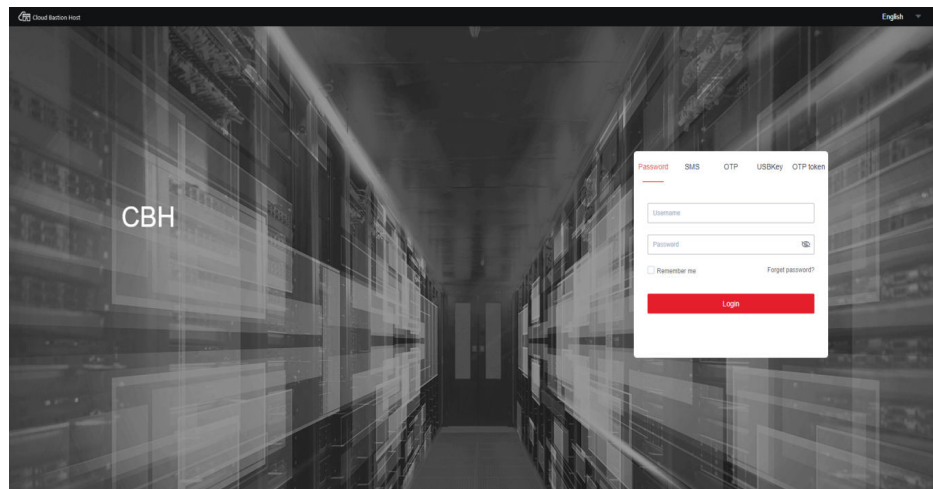
URL: `https:// EIP of PBH`, for example, `https://10.10.10.10`.

NOTE

Use supported browsers to access CBH. In an incompatible browser, the login verification message may fail to be sent to you, or exceptions may occur after you log in.

- Step 2** Select a login authentication method.

Figure 3-1 CBH system login page



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

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

----End

Using Static Passwords for Logging

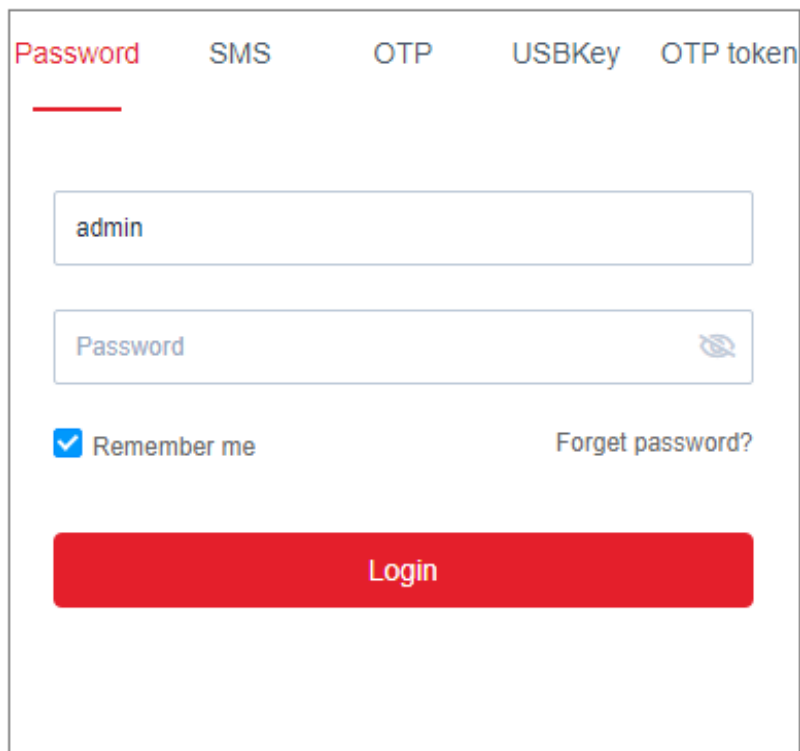
Step 1 Select **Password**.

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

Step 3 Click **Login**.

----End

Figure 3-2 Password authentication



The screenshot shows a login interface with five tabs: Password, SMS, OTP, USBKey, and OTP token. The 'Password' tab is selected and underlined in red. Below the tabs are two input fields: the first contains the username 'admin', and the second is labeled 'Password' with a red eye icon for toggling visibility. Below the password field is a checked checkbox labeled 'Remember me' and a link labeled 'Forget password?'. At the bottom is a large red button labeled 'Login'.

Using SMS Verification for Logging

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

- Step 1** Select **SMS**.
- Step 2** Enter the username and password of your PBH account.
- Step 3** Click **Send code** and enter the 6-digit OTP token in the received SMS message.
- Step 4** Click **Login**.

----End

Figure 3-3 SMS authentication

The screenshot shows a login interface with five tabs: Password, SMS, OTP, USBKey, and OTP token. The 'SMS' tab is selected and highlighted with a red underline. Below the tabs are several input fields and buttons: a text box containing 'admin', a password field with a toggle icon, an 'SMS verification code' field, a red 'Send code' button, a checked 'Remember me' checkbox, a 'Forget password?' link, and a large red 'Login' button at the bottom.

Using Mobile OTPs for Logging

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

NOTICE

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

It is recommended that you save the QR code image when applying for a mobile phone token. If the preceding situation occurs, scan the QR code again.

- Step 1** Select **OTP**.
- Step 2** Enter the username and password of your CBH account.
- Step 3** Start the token client on your mobile phone, obtain the 6-digit OTP, and enter it in the **OTP** text box.
- Step 4** Click **Login**.

----End

Figure 3-4 OTP authentication

The screenshot shows a login form with five tabs at the top: Password, SMS, OTP, USBKey, and OTP token. The 'OTP' tab is selected and underlined with a red line. Below the tabs are four input fields: a username field containing 'admin', a password field with a masked character and an eye icon, an empty OTP field, and a 'Remember me' checkbox which is checked. To the right of the 'Remember me' checkbox is a 'Forget password?' link. At the bottom of the form is a large red button labeled 'Login'.

Login Through USB Key Authentication

Step 1 Select **USBKey**.

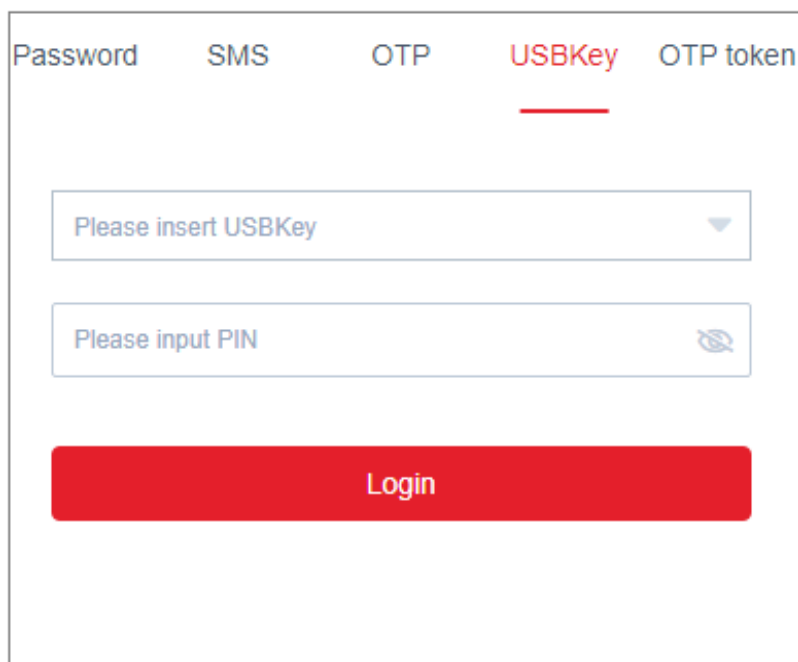
Step 2 Insert your USB key. The CBH system automatically identifies the issued USB key.

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

Step 4 Click **Login**.

----End

Figure 3-5 USB key authentication



Password SMS OTP **USBKey** OTP token

Please insert USBKey

Please input PIN

Login

Using OTP Tokens for Logging

- Step 1** Select **OTP token**.
 - Step 2** Enter the username and password of your CBH account.
 - Step 3** Obtain the 6-digit OTP from the issued hardware token and enter it in the **OTP token** text box.
 - Step 4** Click **Login**.
- End

Figure 3-6 OTP token authentication

The screenshot shows a login form with five tabs at the top: Password, SMS, OTP, USBKey, and OTP token. The 'OTP token' tab is selected and highlighted with a red underline. Below the tabs are three input fields: the first contains 'admin', the second is labeled 'Password' with a visibility icon, and the third is labeled 'OTP token'. Below these fields are two options: a checked checkbox for 'Remember me' and a link for 'Forget password?'. At the bottom is a large red 'Login' button.

3.3 Using a Client to Log In to a CBH System

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

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

Using an SSH Client to Log In to a CBH System

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

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

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

Step 2 Configure user session connection.

- Method 1

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

- Method 2
In the newly opened blank session window, run a command in the following format: **Protocol type User login name@System login IP address Port number**, for example, `ssh admin@10.10.10.10 2222`.
- Method 3
In the live session window of a Linux host, run a command in the following format: **Protocol type User login name@System login IP address-p Port number**, for example, `ssh admin@10.10.10.10 -p 2222`.

 **NOTE**

The **system login IP address** is the CBH IP address, which can be the private IP address or an EIP. The network connection between the local PC and the IP address is normal.

Instance Name	Status	Instance Type	Private IP Address	EIP
CBH-1b4c-test31	Running	Single-node	1[redacted]6	[redacted]
CBH-cjg-1ec2	Running	Single-node	1[redacted]2	[redacted]

Step 3 Authenticate user identities.

Enter your identity credentials as prompted.

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

Table 3-4 SSH client login authentication

Authentic Method	Login Description	Configuration Description
Password	Enter the username and password of your CBH system user account.	Default login mode. The login passwords in the AD, RADIUS, LDAP, or Azure AD authentication are the passwords of users on the remote server.
SSH Pubkey	Enter the private key and private key password for login authentication. After the login authentication is successful, next time the user can log in to the system over the SSH client without entering the password.	You need to generate a public and private key pair for login verification and add the SSH public key to the CBH system in the Profile center.

Authentic ation Method	Login Description	Configuration Description
SMS	In SMS authentication, enter the Password or SSH Pubkey and the SMS verification code you will receive to complete the login authentication.	An available phone number has been configured for the account.
Mobile OTP	In Mobile OTP authentication, enter the Password or SSH Pubkey and the OTP token to complete the login authentication. NOTE Ensure that the CBH system time is the same as the mobile phone time (accurate to the second). Otherwise, a message indicating that the verification code is incorrect will be reported.	Bind your system user account to a mobile OTP and contact the administrator to configure multi-factor authentication for this account.
OTP token	After the Password or SSH Pubkey login is authenticated, select OTP token and enter the verification code.	An OTP token has been issued to the user.

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

 **NOTE**

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

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

----End

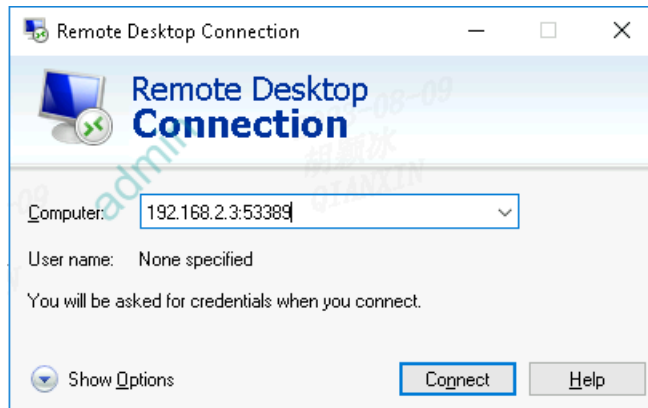
Accessing a CBH system through Microsoft Terminal Services Client (MSTSC)

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

Step 1 Open the MSTSC dialog box.

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

Figure 3-7 Configuring the computer



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

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

NOTE

The *Windows host resource account* must be a resource account that has been added to CBH and the login mode must be automatic login, or the resource account cannot be identified and O&M audit files cannot be generated. Real-time session O&M is not supported.

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

----End

3.4 Configuring Multifactor Verification

3.4.1 Configuring SMS Login Authentication

You can configure a mobile phone to receive a 6-digit code for login identity verification. In SMS authentication method, both the static login password and a 6-digit SMS verification code are required for login.

Constraints

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

Step 1: Bind a Phone Number

The phone number bound to a user account must be valid and can receive SMS messages.

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

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

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

Step 3 In the displayed **Profile** management page, click **Edit**.

Figure 3-8 Binding a phone number

Edit Basic Info ×

* Name
1-255 length of chars, including letter, digit, "@", ".", "_", or "-"

Mobile

Email

Cancel OK

NOTE

The phone number must be in the "+ Country code + Phone number" format.

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

Step 5 Click **OK**.

----End

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

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

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

Step 3 Select a user and click its **LoginName**.

Step 4 On the displayed page, click **Edit** in the **Basic Info** area.

Step 5 Enter a valid phone number in the **Mobile** text box.

Step 6 Click **OK**.

----End

Step 2: Configure SMS Authentication as the Administrator

- Step 1** Log in to a CBH system as the administrator.
- Step 2** Choose **User > User** to go to the **User** management page.
- Step 3** Select a user and click its **LoginName**.
- Step 4** In the **User Setting** area, click **Edit**.
- Step 5** In the displayed **Edit user setting** dialog box, select **Mobile SMS** for **Multifactor Verification**.
- Step 6** Click **OK**.

The next time the user logs in to the CBH system, they will have to provide an SMS code.

----End

3.4.2 Configuring Mobile OTP Login Authentication

A mobile OTP is a mobile application that can generate a dynamic password for identity verification. In mobile OTP verification method, both your static login password and a 6-digit one-time password are required for login.

NOTICE

If you want to enable MFA for the **admin** account, you need to configure the mobile phone token first, or the **admin** account cannot log in to the system in MFA mode.

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

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

Constraints

Ensure that your CBH system and mobile phone have the same system time, accurate to the seconds. Otherwise, the system may prompt that the mobile OTP fails to be bound.

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

Step 1: Bind a Mobile OTP as a Common User

- Step 1** Log in to the CBH system using your static password.
- Step 2** On the **Dashboard** page, click the user name in the upper right corner and choose **Profile**.

- Step 3** On the displayed **Profile** page, click the **Mobile OTP** tab.
On the displayed page, follow the instructions to bind a mobile OTP.

Figure 3-9 Mobile OTP configuration



NOTE

If you do not have the WeChat app, use the Google verification code program to scan the second QR code.

Step 4 (Optional) To unbind the mobile OTP, click **Unbind** on the **Mobile OTP** tab.

----End

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

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

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

Step 3 Select a user having mobile OTP bound and click its **LoginName**.

Step 4 In the **User Setting** area, click **Edit**.

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

Step 6 Click **OK**.

The next time the user logs in to the CBH system, they will have to provide a mobile OTP.

----End

3.4.3 Configuring USB Key Login Authentication

USB token is a one-time password technology implemented based on USB keys. In USB key authentication method, you will need to insert the USB key into your local host for login. The system login page then automatically identifies the inserted USB key and requires you to enter the corresponding PIN to pass identity authentication.

Constraints

- USB keys from different vendors cannot identify each other for login authentication. Configure your vendor before enabling this authentication method. For details, see [Configuring USB Keys](#).
- A USB key can be issued to one user only.

Prerequisites

You have obtained a USB key and installed the USB key driver locally.

Step 1 Configure USB Key Authentication

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

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

Step 3 Select a user and click its **LoginName**.

Step 4 In the **User Setting** area, click **Edit**.

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

Step 6 Click **OK**.

----End

Step 2: Issue the USBKey

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

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

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

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

Table 3-5 Parameters for issuing a USB key

Parameter	Description
USBKey	Specifies the USB key ID.
Relate User	Specifies the user to which the USB key is related. USB key in multifactor verification must be enabled for such users.
PIN	Specifies the personal identification number (PIN) uniquely corresponding to the USB key. It is provided by the USB key vendor.

Step 5 Click **OK**. You can then view the newly issued USB key in the USB key list.

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

----End

3.4.4 Configuring OTP Token Login Authentication

An OTP token is a security hardware device that generates one-time passwords. You can use event-based OTP tokens for CBH. In OTP token authentication method, both your static login password and a 6-digit one-time password generated by your hardware are required for login.

Constraints

- A hardware OTP token can be issued only to one user.

Prerequisites

You have obtained a hardware token.

Step 1: Configure OTP Token Authentication

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

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

- Step 3** Select a user and click its **LoginName**.
 - Step 4** In the **User Setting** area, click **Edit**.
 - Step 5** In the displayed **Edit user setting** dialog box, select **OTP token** for **Multifactor Verification**.
 - Step 6** Click **OK**.
- End

Step 2: Issue an OTP Token

- Step 1** Log in to a CBH system as the administrator.
- Step 2** Choose **User > OTP token** in the navigation pane.
- Step 3** Click **Issue** to issue an OTP token.
- Step 4** Enter the required token information.

Table 3-6 Parameters for issuing an OTP token

Parameter	Description
Token ID	Specifies the OTP token ID.
Key	Specifies the key uniquely corresponding to the OTP token. It is provided by the OTP token vendor.
Relate User	User who the OTP token is related to.

- Step 5** Click **OK**. You can view the newly issued OTP token in the OTP token list.
- In the OTP token authentication method, the login name, static password, and the dynamic password on the OTP token are required for login.
- End

3.5 Managing Login Security

3.5.1 Configuring User Login Lockout

For login security purposes, the source IP address or user account will be locked out if the number of consecutive invalid password attempts exceeds the configured threshold.

This topic describes how to configure the user login lockout, including changing the lockout method, lockout duration, and maximum login attempts.

Prerequisites

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

Procedure

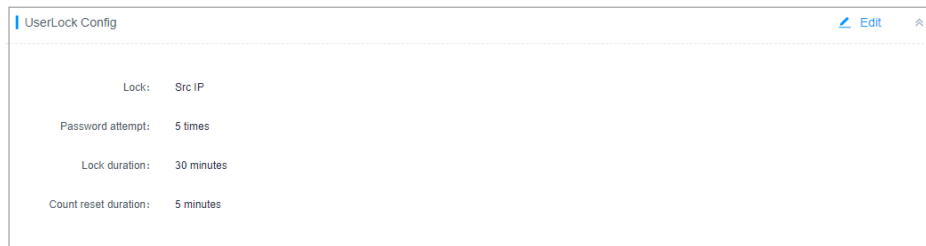
- Step 1** Log in to the CBH system.
- Step 2** Choose **System > Sysconfig > Security**.
- Step 3** In the **UserLock Config** area, click **Edit**.
Complete configurations as prompted.

Table 3-7 Parameters for configuring user lockout

Parameter	Description
Lock	User lock mode. You can select User , or Source IP . <ul style="list-style-type: none"> • User: If the number of consecutive failed password attempts exceeded the upper limit, the user is blocked by the CBH system. • Source IP: If the number of consecutive failed password attempts exceeded the upper limit, the source IP address is blocked by the CBH system.
Password attempt	Allowed maximum number of consecutive failed password attempts. <ul style="list-style-type: none"> • Default value: 5 • Value range: 0 to 999 • If this parameter is set to 0, the user account will not be locked out even if the password is incorrect.
Lock duration	Lockout duration <ul style="list-style-type: none"> • Default value: 30 minutes • Value range: 0 to 10080, in minutes • If this parameter is set to 0, the user account or source IP address will be locked out unless the administrator unlocks it.
Count reset duration	Duration after which the number of login failures is reset to 0 . <ul style="list-style-type: none"> • Default value: 5 minutes • Value range: 1 to 10080, in minutes

- Step 4** Click **OK**. You can then check the lockout configuration of the current system user on the **Security** tab.

Figure 3-10 UserLock Config



----End

3.5.2 Configuring the Login Password Policies

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

Prerequisites







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

Procedure

- Step 1** Log in to the CBH system.
- Step 2** Choose **System > Sysconfig > Security**.
- Step 3** In the **Password Config** area, click **Edit**.

Complete configurations as prompted.

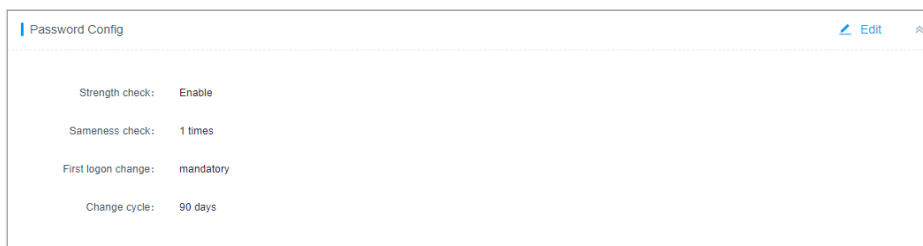
Table 3-8 Parameters for configuring a password policy

Parameter	Description
Strength check	<p>Checks password strength. It is enabled () by default.</p> <ul style="list-style-type: none"> •  : disabled •  : The password can contain 8 to 32 characters and must contain at least three types of the following characters: uppercase letters, lowercase letters, digits, and special characters <code>!@\$%^&^_+=+[{]}:./?~#*</code>.
First logon change	<p>Forces a user to change password upon first login to the CBH system. It is enabled () by default.</p> <ul style="list-style-type: none"> •  : disabled. •  : enabled.

Parameter	Description
Sameness check	Prohibits the reuse of the latest <i>N</i> passwords. <ul style="list-style-type: none"> • The password used for initial login is not counted. • Default value: 5 • Value range: 1 to 30
Change cycle	Password validity period. Users will be forced to change their passwords upon expiry. <ul style="list-style-type: none"> • Default value: 30 days • Value range: 0 to 90, in days • If the value is 0, the password never expires.

Step 4 Click **OK**. You can then check the password policy of the current system user on the **Security** tab.

Figure 3-11 Password Config



----End

3.5.3 Configuring Login Timeout and Login Authentication

This topic describes how to configure the timeout and authentication settings for logins through web browsers, including login timeout duration, SMS verification code validity period, graphic verification code, SSH public key login, and SSH password login.

Prerequisites




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

Configuring Web Login Requirements

- Step 1** Log in to the CBH system.
- Step 2** Choose **System > Sysconfig > Security**.
- Step 3** In the **Web Login Config** area, click **Edit**.

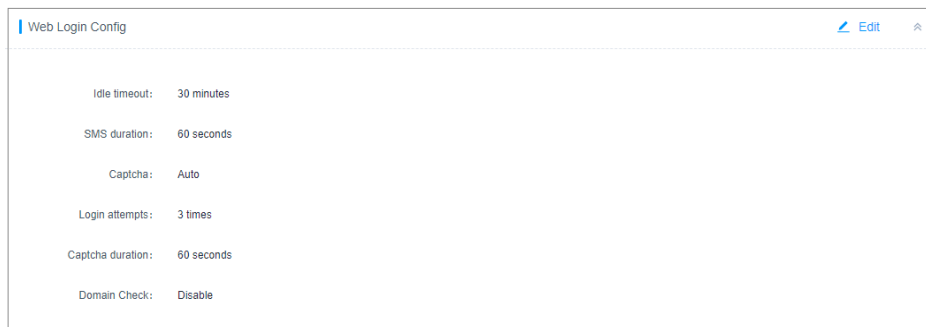
Complete configurations as prompted.

Table 3-9 Parameters for configuring web login

Parameter	Description
Idle timeout	<p>Duration to wait before an inactive user is logged out.</p> <p>After a system user logs in to the CBH system through a web browser, if they have no operations for a period longer than the configured idle timeout, they will be logged out.</p> <ul style="list-style-type: none"> • Default value: 30 minutes • Value range: 1 to 43200, in minutes
SMS duration	<p>SMS verification code validity period.</p> <ul style="list-style-type: none"> • Default value: 60 seconds • Value range: 15 to 3600, in seconds • If the value is 0, the SMS verification code never expires.
Captcha	<p>Whether to use the CAPTCHA technology for graphic verification. The options are Enable, Disable, and Auto.</p> <ul style="list-style-type: none"> • Enable: A graphic verification code is required for every login. • Disable: No graphic verification code is required for logins. • Auto: A graphic verification code is required when the number of consecutive failed password attempts exceeds the configured login attempts.
Login attempts	<p>If the number of consecutive failed password attempts exceeds the login attempts, the graphic verification is automatically enabled.</p> <ul style="list-style-type: none"> • This parameter is mandatory if Captcha is set to Auto. • Default value: 3 • Value range: 1 to 30
Captcha duration	<p>Validity period of a CAPTCHA.</p> <ul style="list-style-type: none"> • Default value: 60 seconds • Value range: 15 to 3600, in seconds • If the value is 0, the graphic verification code never expires.
Domain Check	<p>Whether to check domain. This option is disabled by default (.</p> <ul style="list-style-type: none"> • : enabled. If you select the AD domain authentication, you are required to download an SSO client and use the same login name as that registered with the AD domain server to log in to the CBH system. • : disabled

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

Figure 3-12 Web Login Config



----End

Configuring Login Using a Client

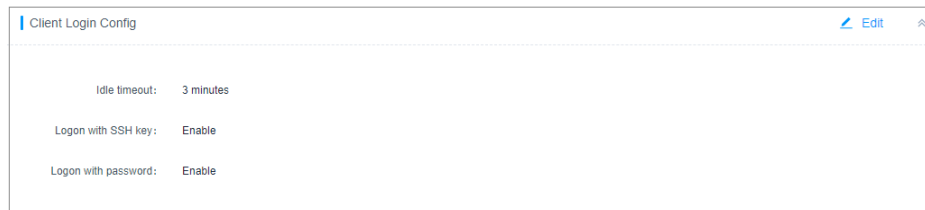
- Step 1** Log in to the CBH system.
- Step 2** Choose **System > Sysconfig > Security**.
- Step 3** In the **Client Login Config** area, click **Edit**.
Complete configurations as prompted.

Table 3-10 Parameters for configuring client login

Parameter	Description
Idle timeout	Duration to wait before an inactive user is logged out of the CBH SSH client. <ul style="list-style-type: none"> • Default value: 30 minutes • Value range: 1 to 43200, in minutes
Logon with SSH key	Whether to enable SSH key login authentication (Default: <input checked="" type="checkbox"/>). <ul style="list-style-type: none"> • <input checked="" type="checkbox"/>: enabled. If you have configured an SSH public key, you can log in to the CBH system using the SSH client without providing passwords. • <input type="checkbox"/>: disabled.
Logon with password	Whether to enable SSH password login authentication (Default: <input type="checkbox"/>). <ul style="list-style-type: none"> • <input checked="" type="checkbox"/>: enabled • <input type="checkbox"/>: disabled • If both Logon with SSH key and Logon with password are enabled, the SSH key login authentication is preferentially performed.

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

Figure 3-13 Client Login Config



----End

3.5.4 Updating a System Web Certificate

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

A secure self-issued certificate is configured for each CBH system by default, but this certificate takes effect only within certain scope and period. You can replace it with your own certificate.

This topic describes how to update the system certificate if it expires or fails a security check.

Prerequisites

- You have purchased and downloaded an SSL certificate.
- The domain name the uploaded certificate is used for has been resolved to the EIP bound to the CBH instance.
- You have the management permissions for the **System** module.

Constraints

- Currently, the CBH system supports only the Java Keystore certificate file of Tomcat, that is, the certificate file in .jks.
- A certificate file cannot exceed 20 KB and must contain a certificate password. When you upload an SSL certificate, provide its password for verification, or the upload will fail.

Procedure

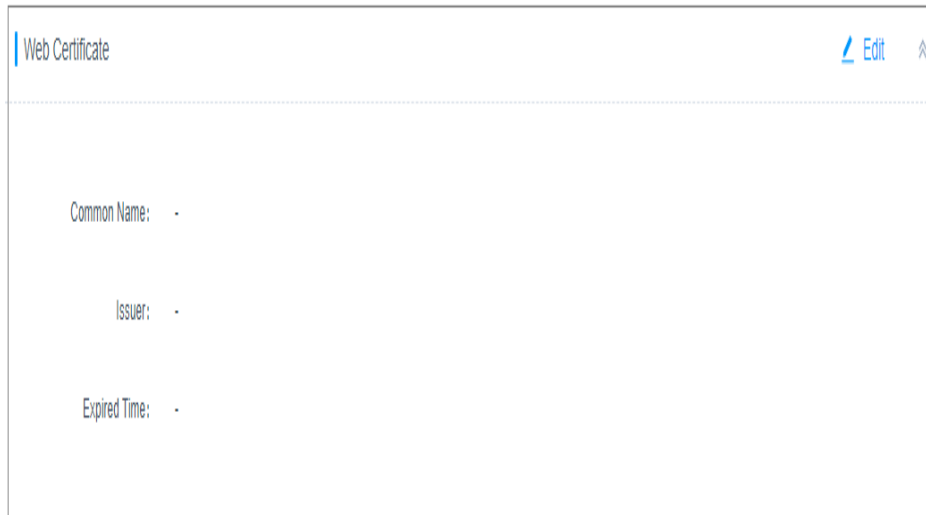
- Step 1** Log in to the CBH system.
- Step 2** Choose **System > Sysconfig > Security**.
- Step 3** In the **Web Certificate** configuration area, click **Edit**.
- Step 4** Upload the certificate file downloaded in your computer.
- Step 5** After the certificate file is uploaded, enter the Keystore password to verify the certificate.
- Step 6** Click **OK**. You can then check the web certificate configuration of the current system user on the **Security** tab.

Step 7 Restart the CBH system for the updated certificate to take effect.

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

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

Figure 3-14 System web certificate information



----End

3.5.5 Configuring the Mobile OTP Type

A mobile OTP application is a software token application used to generate a dynamic password on a bound mobile phone. In mobile OTP verification method, a password and a 6-digit mobile OTP verification code are required for logging in to the CBH system.

This topic describes how to set the mobile OTP type.

Constraints

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

Prerequisites

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

Procedure

- Step 1** Log in to the CBH system.
- Step 2** Choose **System > Sysconfig > Security**.
- Step 3** In the **Mobile Token Settings** area, click **Edit**.
- Step 4** In the displayed **Mobile Token Settings** dialog box, select a mobile OTP type.
- Step 5** Click **OK**. You can then check the mobile token settings of the current system user on the **Security** tab.

Figure 3-15 Viewing mobile token settings



----End

3.5.6 Configuring the USB Key Vendor

This topic describes how to configure the USB key vendor.

Constraints

- If you change the vendor of a USB key, the issued USB key cannot be identified by the CBH system.

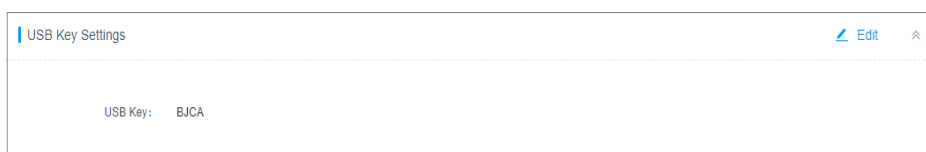
Prerequisites

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

Procedure

- Step 1** Log in to the CBH system.
- Step 2** Choose **System > Sysconfig > Security**.
- Step 3** In the **USB Key Settings** area, click **Edit**.
- Step 4** In the displayed dialog box, select a vendor.
- Step 5** Click **OK**. You can then check the USB key settings of the current system on the **Security** tab.

Figure 3-16 Viewing the USB Key vendor



----End

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

The zombie user policy function allows you to identify zombie users and customize a threshold time range. If a user does not log in to the CBH system within the configured threshold time range, the system marks the user as zombie and disables the user. Only the administrator can enable the zombie user. The default threshold is 30 days. If the threshold is set to 0, all users are disabled immediately.

Prerequisites


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

Procedure

Step 1 Log in to the CBH system.

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

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

- **Disable zombie users:** By default, this function is disabled. After this function is enabled, the status is .
- **Determines the zombie user time:** The value ranges from 0 to 10,080. The default value is 30 days. If the value is set to 0, all users are disabled immediately until the administrator cancels the disabling. For details about how to enable users, see [Enabling or Disabling a User](#).

Step 4 Click **OK**.

----End

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

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

Prerequisites

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

Procedure

Step 1 Log in to the CBH system.

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

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

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

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

----End

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

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

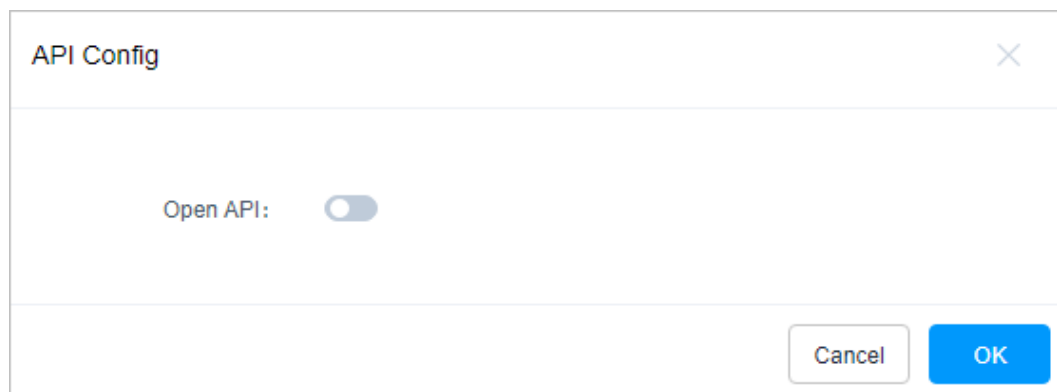
Prerequisites


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

Procedure

- Step 1** Log in to the CBH system.
- Step 2** Choose **System** > **Sysconfig** > **Security**.
- Step 3** In the **API Config** area, click **Edit**.

Figure 3-17 API Config



- Step 4** Click  .
- Step 5** Click **OK**.

----End

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

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

Prerequisites


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

Procedure

- Step 1** Log in to the CBH system.

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

Step 3 In the **Auto Inspect Config** area, click **Edit**.

Step 4 By default, automatic inspection is enabled. You can click  to disable it.

Step 5 Click **OK**.

----End

3.5.11 Configuring a Resource Account


If you enable resource accounts, the Empty account is automatically added.

Procedure

Step 1 Log in to the CBH system.

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

Step 3 On the right of resource account configuration, click **Edit** to go to the configuration page.

Step 4 The **Empty** account is automatically added and enabled by default (). You can disable it if needed.

Step 5 Click **OK**.

----End

3.5.12 Configuring Client Login

You can set an idle limit to trigger automated logout. If a user does not perform any actions within the idle limit, the user will be logged out.

Procedure



Step 1 Log in to the CBH system.

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

Step 3 On the right of the **Client Login Config** bar, click **Edit**. The **Client Login Config** dialog box is displayed.

Step 4 Enter a timeout for logging out idle users and select the SSH login mode. [Table 3-11](#) describes the parameters.

Table 3-11 Configuring Client Login

Parameter	Description	Example Value
Idle timeout	Duration to wait before an inactive user is logged out. Value range: 1 to 43,200 After a system user logs in to the CBH system through a web browser, if they have no operations for a period longer than the configured idle timeout, they will be logged out. The default value is 30 minutes.	30
Logon with SSH key	Whether to enable SSH key login authentication for users that have been logged out after idle timeout. This function is enabled by default.	
Logon with password	Whether to enable SSH password authentication for users that have been logged out after idle timeout. This function is enabled by default.	

Step 5 Click **OK**.

----End

3.5.13 Configuring a User Expiration Reminder


You can configure a user validity period reminder. Then, the system will send an email reminder every day before the user validity period actually expires.

Procedure

Step 1 Log in to the CBH system.

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

Step 3 On the right of **User Expiration Countdown Settings**, click **Edit** to go to the configuration page.

Step 4 Set **User Password** and enable **User Expiration Countdown** ()


Step 5 Click **OK**.

----End

3.5.14 Configuring Session Limit

You can enable session limit to deny new sessions when the CPU and memory usage exceeds the server configuration.

Procedure

- Step 1** Log in to the CBH system.
- Step 2** Choose **System > Sysconfig > Security**.
- Step 3** Click **Edit** on the right of **Session Limit Settings** to go to the configuration page.
- Step 4** Set the status of **Session Limit** to , and set a threshold for CPU and memory usage. When the CPU or memory usage triggers the threshold, no new sessions will be established.
- Step 5** Click **OK**.

----End

4 Dashboard of the CBH System

4.1 Dashboard

In the CBH system, the **Dashboard** page presents the CBH system information, system user actions, and host and application operations. The **Dashboard** module consists of a basic statistic area and 17 graph panels, including **Focus Resources, Online User, Tickets To Approve, Host Statistics, Application Statistics, Alive Sessions, Today Spawned Sessions, Logon Statistics, Operation Statistics, Top 5 of Operation User, Top 5 of Operation Host, System Status, System Info, Recently Logged Hosts, Recently Logged Apps, My Hosts, and My Apps.**

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

Procedure

- Step 1** Log in to the CBH system.
- Step 2** In the navigation tree on the left, choose Desktop. The Desktop Dashboard page is displayed.
- Step 3** View different panels based on your needs. For details about the functions of each panel, see the following topics.

----End

Focus Resources

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

To view basic statistics, obtain the management permissions for **User, Host, Application, and Application Server** modules and the role management permissions. Otherwise, this panel will be invisible for you. In the basic statistics area, you can view:

- **User information**
Displays the number of user accounts that can be managed. You can click this module to go to the user list page and manage the users.
- **Hosts**
Displays the number of host resources that can be managed. You can click this module to go to the host list page and manage the host resources.
- **Application**
Displays the number of application resources that can be managed. You can click this module to go to the application resource list page and manage the application resources.
- **AppServer**
Displays the number of application servers that can be managed. You can click this module to go to the application server list page and manage the application servers.
- **Alert**
Displays the number of unprocessed alarms. You can click this module to go to the message center page and manage messages.

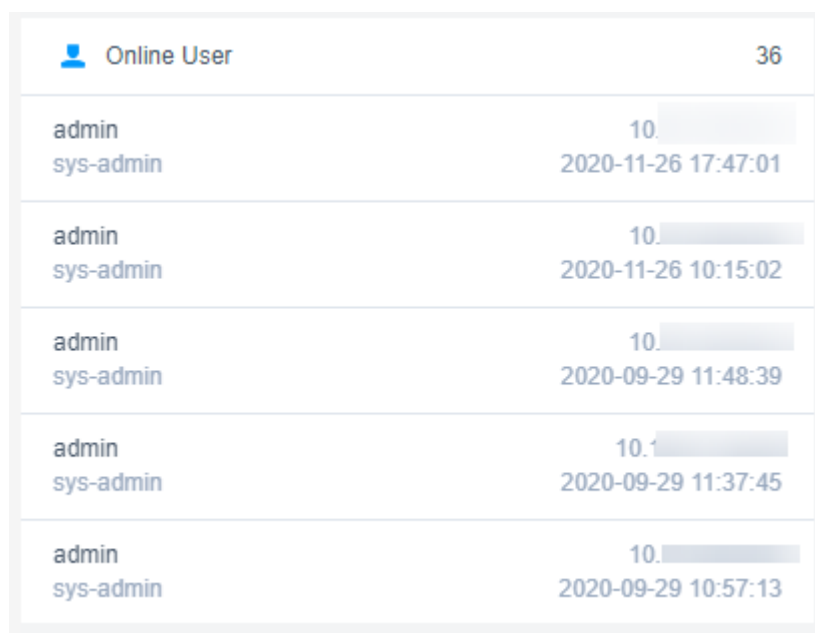
Online User

Displays the online users and historical login users you can manage.

To view the statistics of online users, obtain the management permission of the **User** module and the role management permission.

Click a username in the list to go to the user details page. On this page, you can view and manage user information.

Figure 4-1 Online User



Online User		36
admin sys-admin	10. [redacted] 2020-11-26 17:47:01	
admin sys-admin	10. [redacted] 2020-11-26 10:15:02	
admin sys-admin	10. [redacted] 2020-09-29 11:48:39	
admin sys-admin	10. [redacted] 2020-09-29 11:37:45	
admin sys-admin	10. [redacted] 2020-09-29 10:57:13	

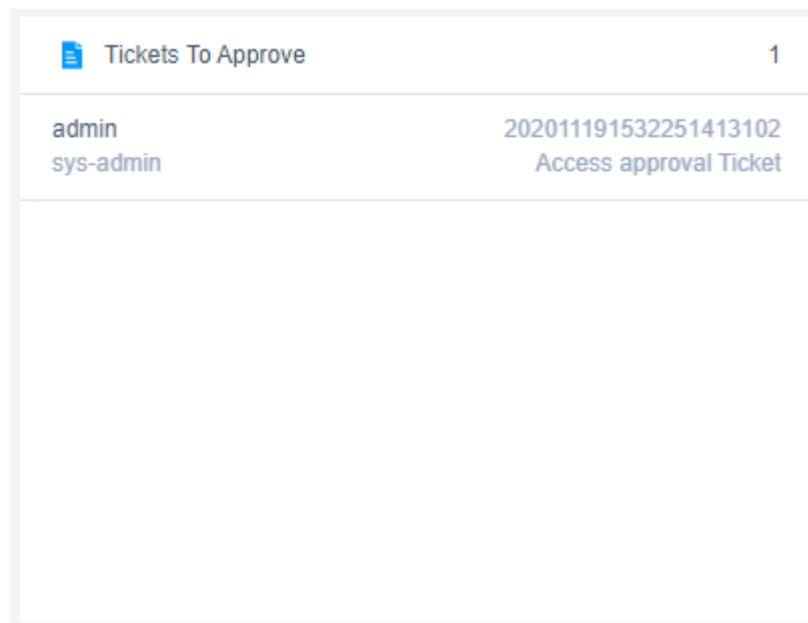
Tickets to Approve

Displays the tickets to be approved.

To view the tickets to be approved, obtain the management permission of the **Ticket Approval** module and the role management permission.

Click a ticket in the list to go to the ticket details page. On this page, you can view the ticket information and approve it with just one click.

Figure 4-2 Tickets to Approve



Tickets To Approve		1
admin sys-admin	202011191532251413102 Access approval Ticket	

Host Statistics

Displays the statistics on hosts you can manage.

To view the statistics of hosts, obtain the management permission of the **Host** module and the role management permission.

- Different color represents different host type. Move your cursor over a color block in the circle to view the number of hosts of a certain type.
- Click a color block to go to the corresponding host list page.

Figure 4-3 Host Statistics

Host Statistics



Application Statistics

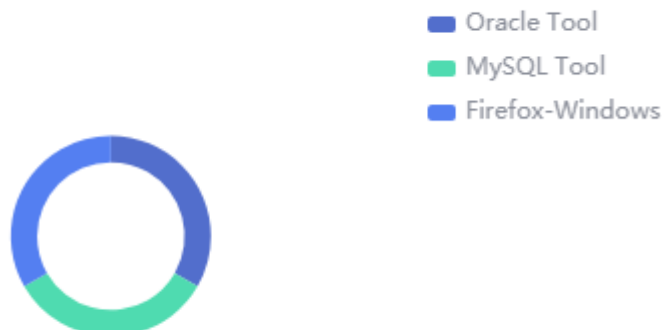
Displays the statistics on application types you can manage.

To view the statistics of application resources, obtain the management permission of the **Application** module and the role management permission.

- Different color represents different host type. Move your cursor over a color block in the circle to view the number of application resources of a certain type.
- Click a color block to go to the corresponding application list page.

Figure 4-4 Application Statistics

Application Statistics



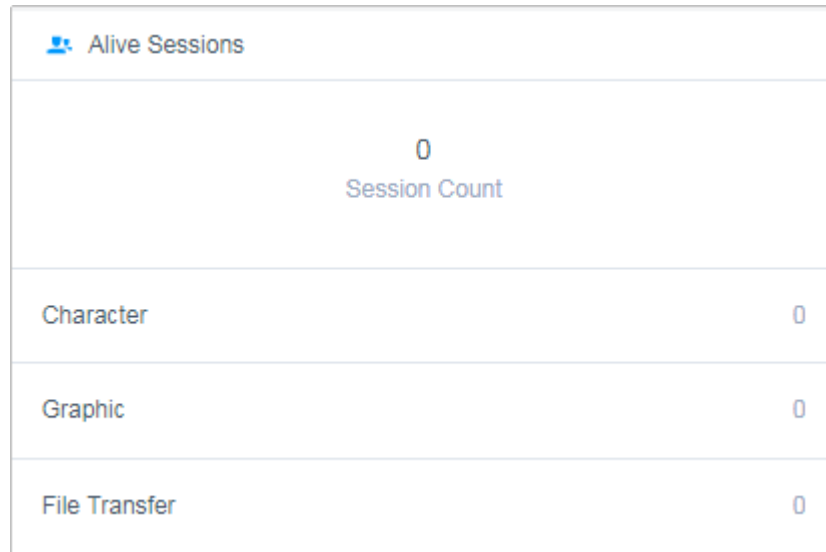
Alive Sessions

Displays the statistics on sessions you can manage.

To view the statistics of live sessions, obtain the management permission of the **Live Session** module and the role management permission.

You can click a live session type to go to the corresponding live session list page and monitor the session in real time.

Figure 4-5 Alive Sessions



Alive Sessions	
0 Session Count	
Character	0
Graphic	0
File Transfer	0

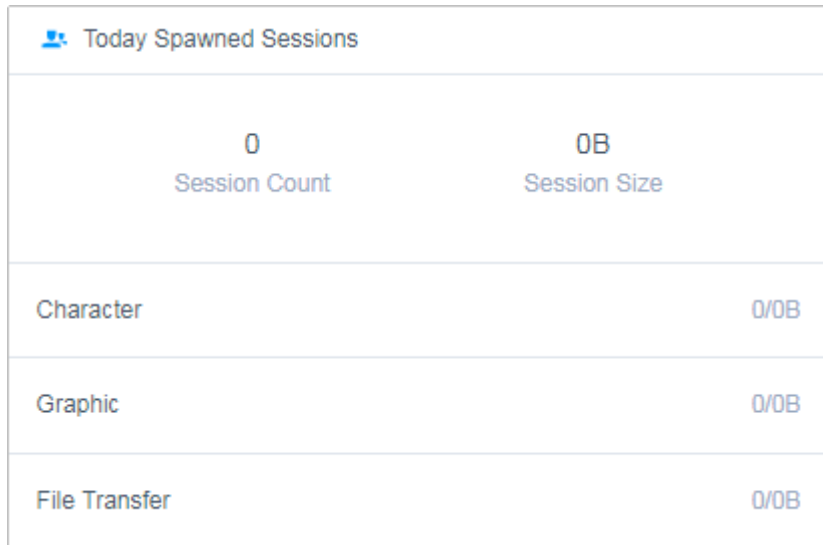
Today Spawned Sessions

Displays the statistics on historical sessions you can manage.

To view the statistics of historical sessions, obtain the management permission of the **History Session** module and the role management permission.

You can click a history session type to go to the corresponding historical session list page and view historical sessions.

Figure 4-6 Today Spawned Sessions



Today Spawned Sessions	
0 Session Count	0B Session Size
Character	0/0B
Graphic	0/0B
File Transfer	0/0B

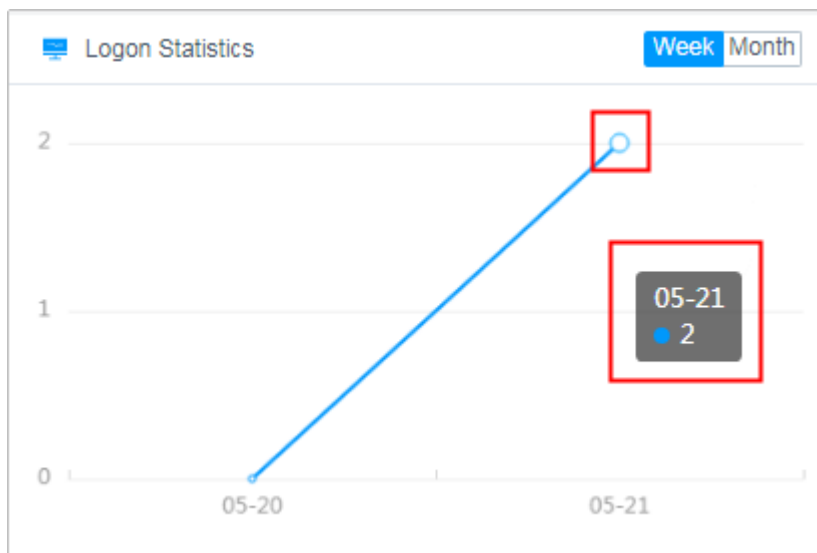
Logon Statistics

Displays the trend chart of the number of logins to the CBH system by system users under your management. You can view the trend charts of the current week and month.

To view the statistics on logins, obtain the management permission of the **User** module and the role management permission.

- To view how many times the CBH system is logged in within a certain day, move your cursor over the corresponding date.

Figure 4-7 Logon Statistics



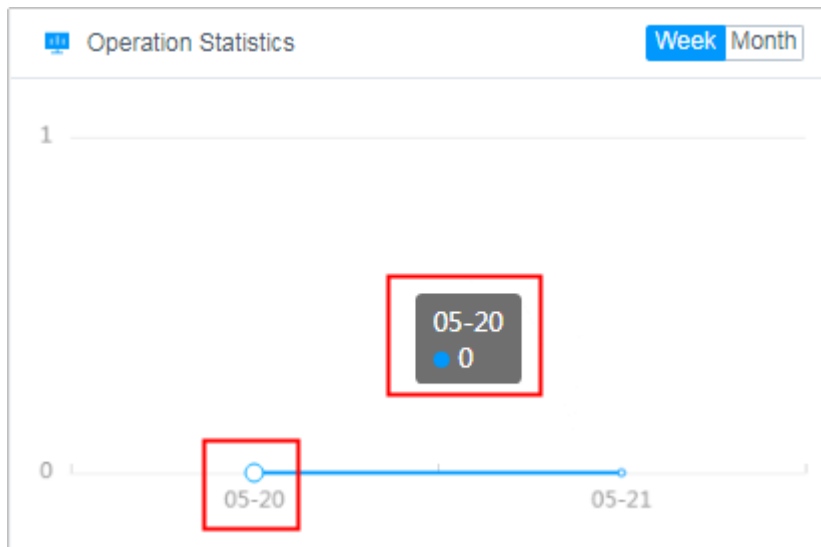
Operation Statistics

Displays the trend chart of the number of logins to managed resources by system users under your management. You can view the trend charts of the current week and month.

To view the statistics on logins to resources, obtain the management permission of the **History Session** module and the role management permission.

To view how many times authorized resources are accessed through the CBH system within a certain day, move your cursor over the corresponding date.

Figure 4-8 Operation Statistics



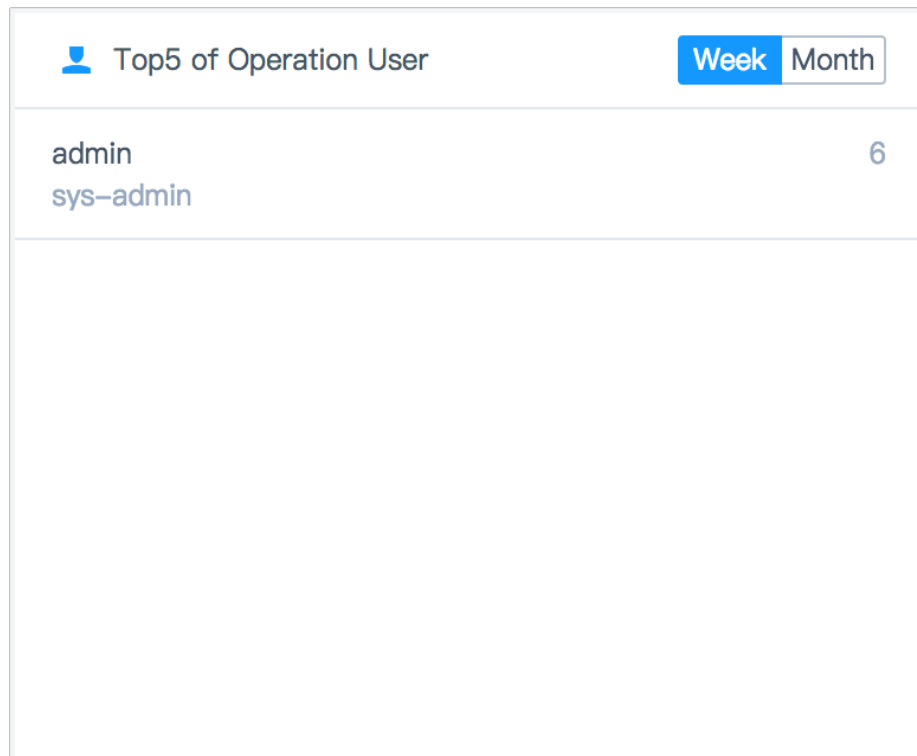
Top 5 of Operation User

Displays top 5 system users with most login times to managed resources. You can view the trend charts of the current week and month.

To view the statistics on user login times to the managed resources, obtain the management permission of the **History Session** module and the role management permission.

Click a user in the list to go to the user details page. On this page, you can view and manage user information.

Figure 4-9 Top 5 of Operation User



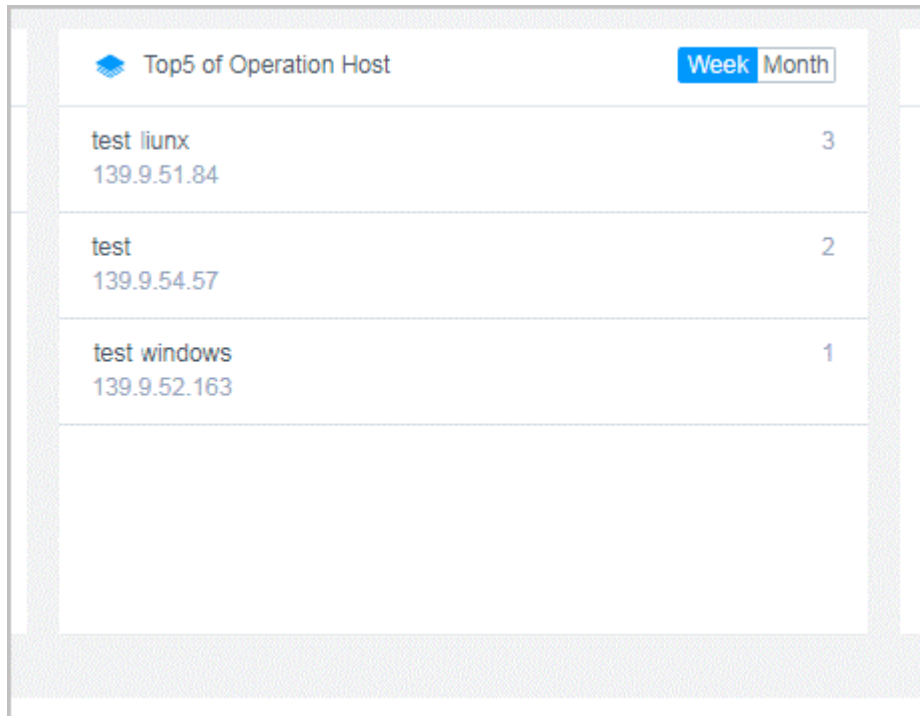
Top 5 of Operation Host

Displays top 5 mostly accessed resources. You can view the trend charts of the current week and month.

To view the statistics on managed resources, obtain the management permission of the **History Session** module and the role management permission.

Click a host resource in the list to go to the details page. On this page, you can view and manage resource information.

Figure 4-10 Top 5 of Operation Host

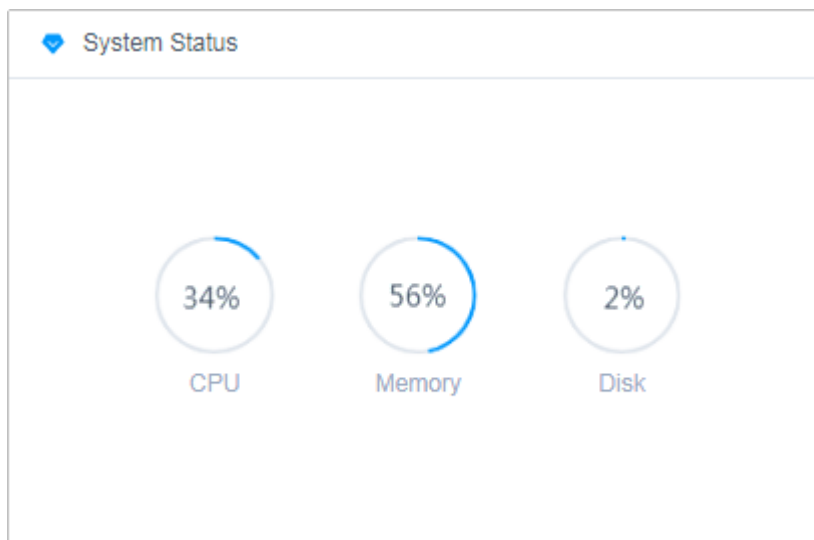


System Status

Displays the CPU, memory, and disk usage of the current system.

To view the statistics on system status, obtain the management permission of the **System** module and the role management permission.

Figure 4-11 System Status



System Info

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

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

Recently Logged Host

Lists the host resources you have logged in recently.

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

- To view details about a host, click the host name in the list to go to the details page.
- To quickly log in to a host resource, click **Login** in the host row.

Figure 4-12 Recently Logged Host

Host Name	Host Addr	Protocol	Label	Account	Operation
192.168.1.62	192.168.1.62:22	SSH		root	Login
SSH	192.168.1.144:22	SSH	1241	root	Login

Recently Logged Application

Lists the application resources you have logged in recently.

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

- To view details about an application, click the application name in the list to go to the details page.
- To quickly log in to an application resource, click **Login** in the application row.

Figure 4-13 Recently Logged Application

App Name	Param	Protocol	Label	Account	Operation
No Data					

My Hosts

Displays host resources you are authorized to log in.

To view hosts that you can log in for operations, obtain the management permissions for the **Host Operations** module.

- To view details about a host, click the host name in the list to go to the details page.
- To quickly log in to a host resource, click **Login** in the host row.

Figure 4-14 My Hosts

Host Name	Host Addr	Protocol	Label	Account	Operation
No Data					

My APPs

Displays the application resources that you are authorized to log in to.

To view application resources that you can log in for operations, obtain the management permissions for the **App Operations** module.

- To view details about an application, click the application name in the list to go to the details page.
- To quickly log in to an application resource, click **Login** in the application row.

Figure 4-15 My APPs

App Name	APP Address	Protocol	Label	Account	Operation
No Data					

4.2 Profile

4.2.1 Viewing Your Profile

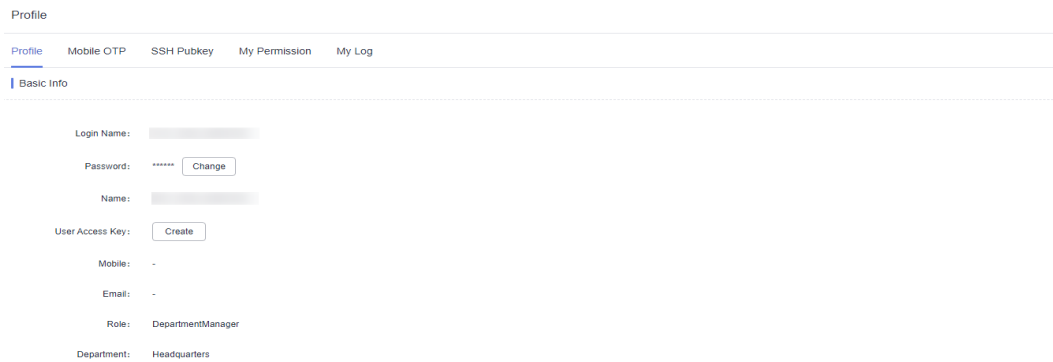
On the **Profile** page, tabs **Profile**, **Mobile OTP**, **SSH Pubkey**, **My Permission**, and **My Log** are available for you to configure basic user information, user permissions, system usage logs, mobile one-time passwords (OTPs), and SSH public keys.

This topic walks you through how to view your profile.

Procedure

- Step 1** Log in to the CBH system.
- Step 2** On the **Dashboard** page, click the user name in the upper right corner and choose **Profile**.

Figure 4-16 Profile



Step 3 Click each tab to view the corresponding information.

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

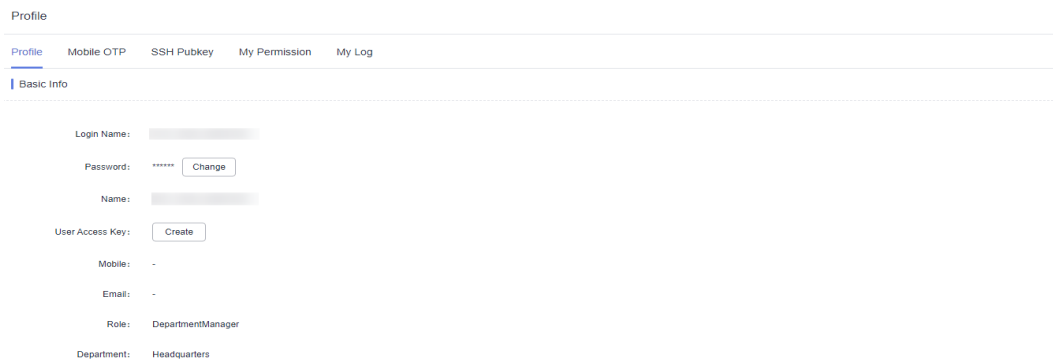
----End

Basic Info

Click the **Profile** tab to view basic user information, including the login name, ciphertext password, name, mobile number, email address, role, and department.

To change the mobile number, email address, and password, see [Editing Basic Information in Profile](#).

Figure 4-17 Profile

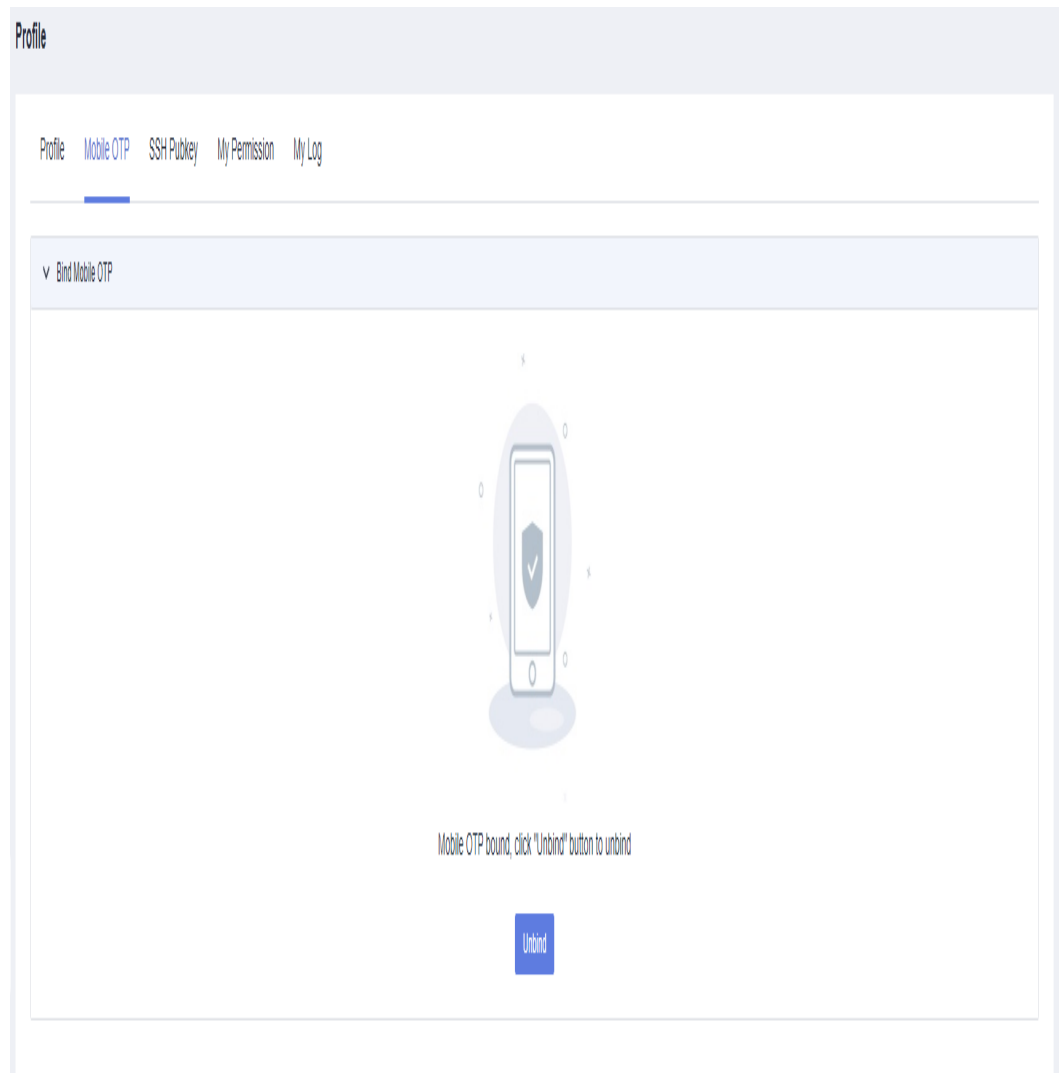


Mobile OTP

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

For more details about how to bind or unbind a mobile phone token, see [Managing Mobile OTPs](#).

Figure 4-18 Mobile OTP

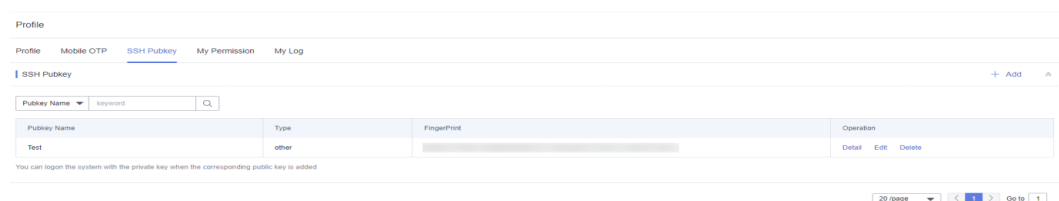


SSH Public Key

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

For details about how to add, modify, and delete a public key, see [Managing SSH Public Keys](#).

Figure 4-19 SSH Pubkey



My Permission

To view the personal system permissions and check whether the administrator permission is enabled, click the **My Permission** tab.

Log in to the CBH system as system administrator **admin**.

Figure 4-20 Permissions of user **admin**

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

My Log

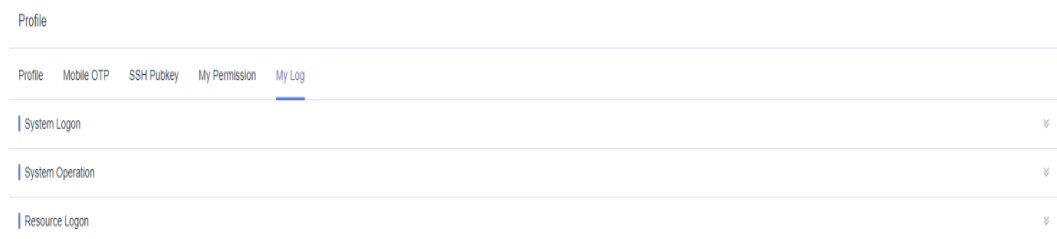
To view logs, click the **My Log** tab. You can then view **System Logon**, **System Operation**, and **Resource Logon** logs.

NOTE

Logs can be managed only by users with the system management permission. Individual users cannot clear their logs. For details, see [Data Maintenance](#).

- System logon logs
A system logon log includes the login time, source IP address of the login user, login method, and login result.
- System operation logs
A system operation log includes the operation time, source IP address of the operation user, operation module, operation content, and operation result.
- Resource logon logs
A resource logon log includes the resource name, protocol type, account, source IP address of the login user, login start and end time, and session duration.

Figure 4-21 My Log



4.2.2 Editing Basic Information in Profile

Basic information of a user profile includes the login name, ciphertext password, name, mobile number, email address, role, and department.

- In the Profile area, you can change your password, name, mobile number, and email address.
- The value of **Login Name** must be unique in the CBH system and cannot be changed once it is created.
- Role and department information can be managed only by users with the user management permission and cannot be modified by common individual users. For more details, see [Querying and Modifying User Information](#).

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

Changing Your Password

Step 1 Log in to the CBH system.

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

Figure 4-22 Profile

The screenshot shows the 'Profile' page with a navigation bar containing 'Profile', 'Mobile OTP', 'SSH Pubkey', 'My Permission', and 'My Log'. The 'Basic Info' section is active and displays the following fields: 'Login Name' (text input), 'Password' (masked with asterisks and a 'Change' button), 'Name' (text input), 'User Access Key' (with a 'Create' button), 'Mobile' (dash), 'Email' (dash), 'Role' (DepartmentManager), and 'Department' (Headquarters).

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

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

The new password must:

- Contain 8 to 32 characters.
- Contain at least three of the following types of characters: uppercase letters (A to Z), lowercase letters (a to z), digits (0 to 9), and following special characters: !@\$%^&*_+[]{}:;./?~#*
- Cannot contain the username or the username spelled backwards.

Step 5 Click **OK**.

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

----End

Modifying Basic Information

Step 1 Log in to the CBH system.

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

Figure 4-23 Profile

This screenshot is identical to Figure 4-22, showing the 'Profile' page with the 'Basic Info' section active. It displays fields for Login Name, Password (with a 'Change' button), Name, User Access Key (with a 'Create' button), Mobile, Email, Role (DepartmentManager), and Department (Headquarters).

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

Step 4 In the displayed dialog box, enter the user name, mobile number, or email address into the **Name**, **Mobile**, and **Email** text boxes, respectively.

Step 5 Click **OK**.

The new user name, mobile number, and email address take effect upon the completion of editing.

----End

4.2.3 Managing Mobile OTP Application for Login Authentication

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

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

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

NOTICE

- Ensure that your CBH system and mobile phone have the same system time, accurate to seconds. Otherwise, the mobile OTP application may fail to be bound to the user account.
- If the mobile OTP fails to be bound, change the CBH system time to be the same as the mobile phone time. After this, refresh the page to generate a new quick response (QR) code for binding.

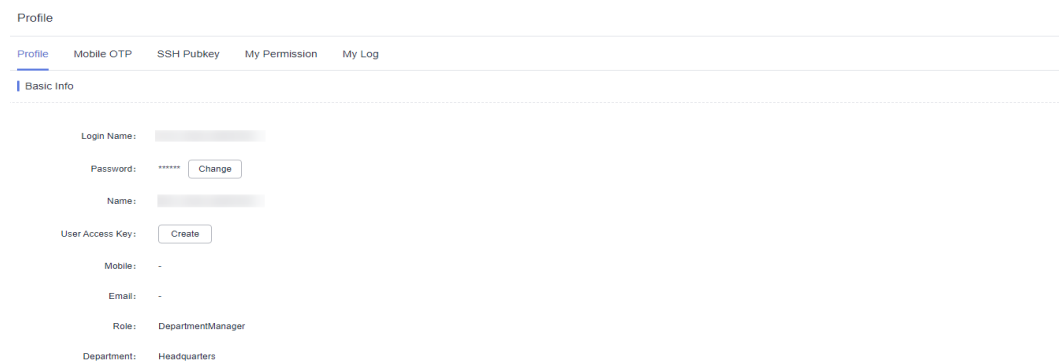
This topic describes how to bind and unbind a mobile OTP application.

Binding a Mobile OTP application to a User

Step 1 Log in to the CBH system.

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

Figure 4-24 Profile



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

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

1. WeChat applet access token

Start WeChat on the mobile phone, obtain the dynamic password for binding according to the operation guide, and enter the 6-digit dynamic password. After the verification, the mobile OTP application is bound.

2. App-based mobile OTP

Start the installed mobile OTP application, scan the QR code in step 2 to obtain a dynamic password, and enter the 6-digit dynamic password. After the verification, the mobile OTP application is bound to you.

Step 5 Refresh the page.

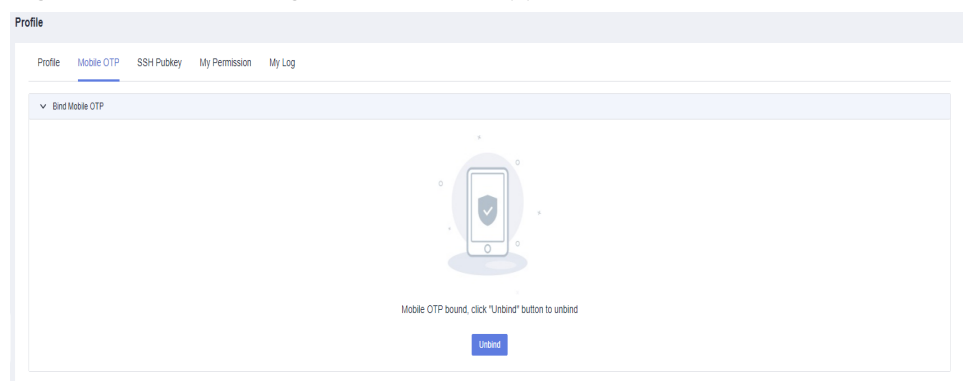
----End

Unbinding a Mobile OTP Application

Click **Unbind** on the **Mobile OTP** tab to unbind the mobile OTP application.

After the unbinding, refresh the page.

Figure 4-25 Unbinding a mobile OTP application



4.2.4 Managing SSH Public Keys

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

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

Constraints

Only OpenSSH public keys are supported.

Adding an SSH Public Key

Step 1 Log in to the CBH system.

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

Figure 4-26 Profile

The screenshot shows the 'Profile' page with the 'Basic Info' tab selected. The page contains the following fields and controls:

- Profile: Mobile OTP, SSH Pubkey, My Permission, My Log
- Basic Info
- Login Name: [Text Input]
- Password: [Text Input] [Change]
- Name: [Text Input]
- User Access Key: [Create]
- Mobile: -
- Email: -
- Role: DepartmentManager
- Department: Headquarters

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

Step 4 Click **Add** in the **SSH Pubkey** area.

Step 5 In the displayed **Add SSH Pubkey** dialog, specify the public key name and enter the SSH public key.

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

----End

Deleting an SSH Public Key

Step 1 Log in to the CBH system.

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

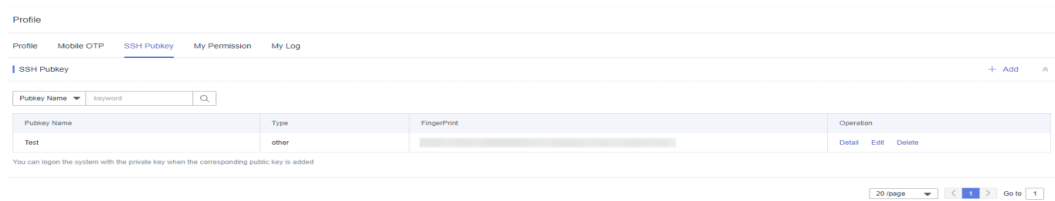
Figure 4-27 Profile

The screenshot shows the 'Profile' page with the 'Basic Info' tab selected. The page contains the following fields and controls:

- Profile: Mobile OTP, SSH Pubkey, My Permission, My Log
- Basic Info
- Login Name: [Text Input]
- Password: [Text Input] [Change]
- Name: [Text Input]
- User Access Key: [Create]
- Mobile: -
- Email: -
- Role: DepartmentManager
- Department: Headquarters

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

Figure 4-28 SSH Pubkey



Step 4 In the **Operation** column of the SSH public key you want to delete, click **Delete**.

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

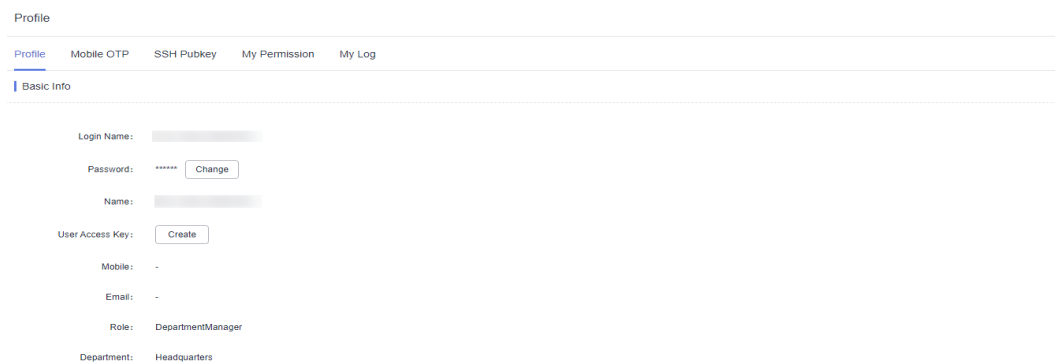
----End

Editing an SSH Public Key

Step 1 Log in to the CBH system.

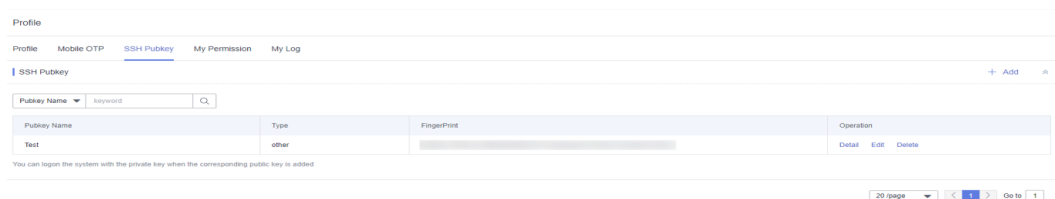
Step 2 On the **Dashboard** page, click the user name in the upper right corner and choose **Profile**.

Figure 4-29 Profile



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

Figure 4-30 SSH Pubkey



Step 4 In the **Operation** column of the SSH public key you want to modify, click **Edit**.

Step 5 In the displayed **Edit SSH pubkey** dialog box, edit the public key name and the public key.

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

----End

4.3 Tasks


The task center is the task management center that displays the task receiving status.

- Task types: importing a user, host, cloud server, application, application server, and an account, changing the password of an account, synchronizing users from the AD Domain server, PBH system maintenance (including upgrade and restoration), generating an O&M video, account synchronization, account verification, configuring backup mechanism, automatic O&M, importing dynamical OTPs, and installing Agent.
- The task status can be **Executing**, **Finished**, or **Stop**.

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

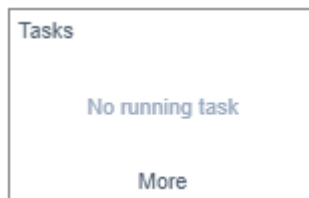
Procedure

Step 1 Log in to the CBH system.

Step 2 Click  in the upper right corner of the page to show the small task center window.

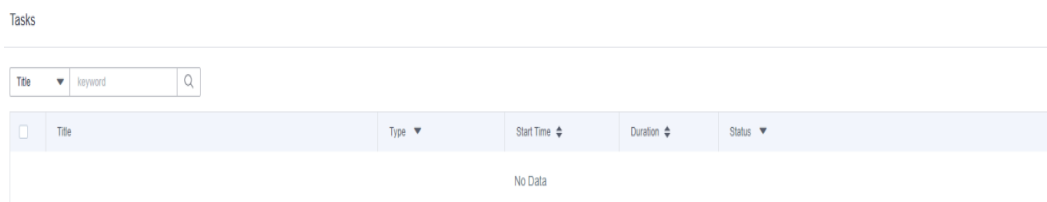
You can view the latest three tasks that are being executed.

Figure 4-31 Small task center window



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

Figure 4-32 Viewing a task list



Step 4 Query tasks.

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

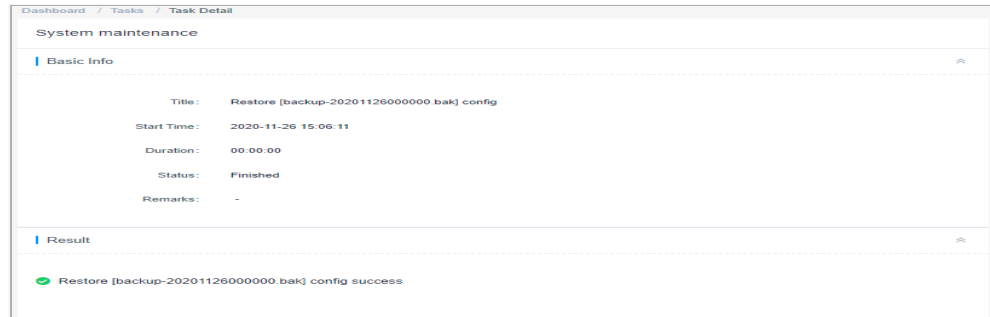
Step 5 View the tasks.

On the **Tasks** page, you can view all running tasks, finished tasks, and stopped tasks.

Step 6 View task details.

1. Click the name of a task.
2. View the basic information and execution result of the task.

Figure 4-33 View task details.



----End

4.4 Messages

4.4.1 Managing Messages


The message center receives system messages. The latest three unread messages are displayed in the small message center window. After a task is complete, you can view messages about all tasks in the task center.

- There are five types of messages, including system messages, service messages, task messages, command alarms, and ticket messages.
- All messages are classified in to three levels by importance, **High**, **Medium**, or **Low**.

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

Viewing Messages

Step 1 Log in to the CBH system.

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

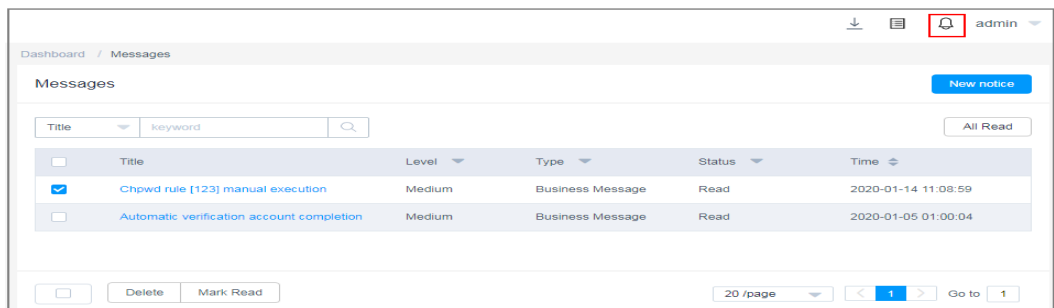
The following figure shows an example.

Figure 4-34 Small message center window



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

Figure 4-35 Message list



Step 4 Query messages.

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

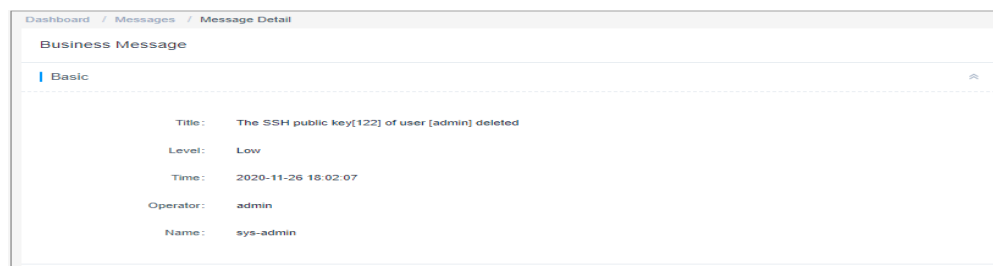
Step 5 View the search results.

Messages are sorted in descending order by time. You can view all read and unread messages.

Step 6 Viewing message details.

1. Click the name of the message to go to the details page.
2. View basic information of the message.


Figure 4-36 Message details



----End

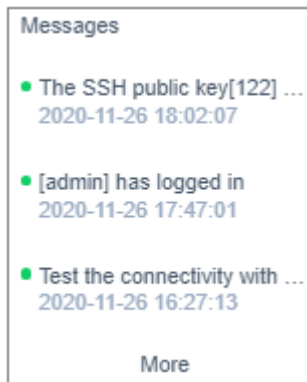
Deleting a Message

Step 1 Log in to the CBH system.

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

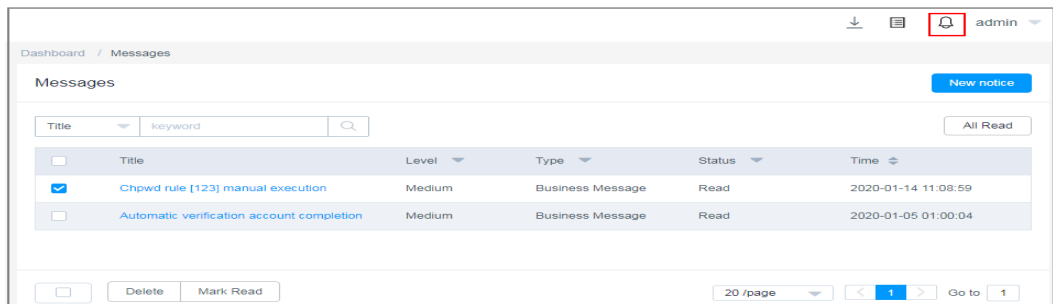
The following figure shows an example.

Figure 4-37 Small message center window



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

Figure 4-38 Message list



Step 4 Select one or more messages and click **Delete** in the lower left corner.

Step 5 In the confirmation dialog box, click **OK** to delete the selected messages immediately.


 **CAUTION**

Deleted messages cannot be restored. Exercise caution when performing this operation.

----End

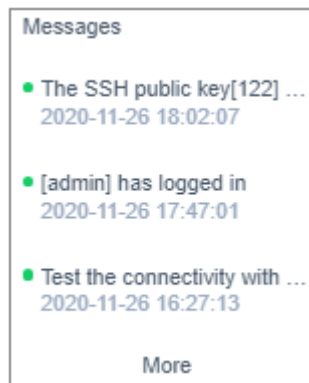
Marking a Message

Step 1 Log in to the CBH system.

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

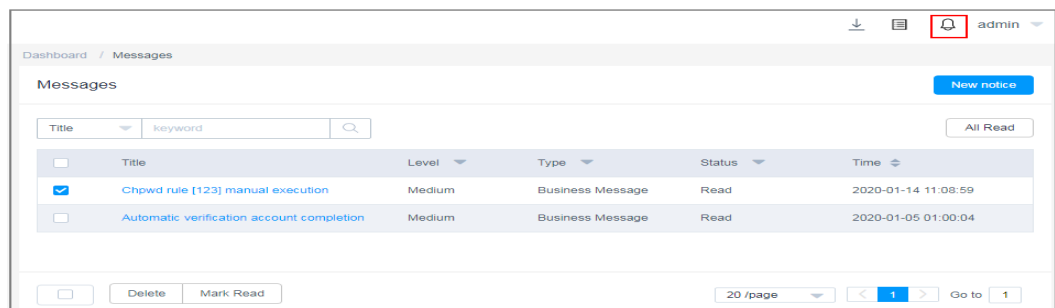
The following figure shows an example.

Figure 4-39 Small message center window



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

Figure 4-40 Message list



Step 4 Marks one or more messages.

1. Select one or more messages and click **Mark Read** in the lower left corner.
2. In the displayed confirmation dialog box, click **OK**. The status of the target message changes to **Read**.

Step 5 Mark all messages.

1. Click **All Read**.
2. In the displayed confirmation dialog box, click **OK**. The status of the all messages changes to **Read**.

----End

4.4.2 Creating a CBH System Notice

A system notice is used to notify system users of major changes in the system. After a system notice is created, the notice content is displayed on the top of page for each system user.

As an individual system user, to let the system notice not show again, click **Read** on the left of the notice.


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

Constraints

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

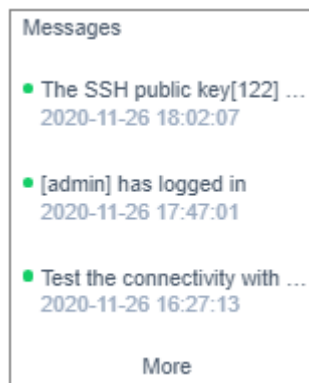
Procedure

Step 1 Log in to the CBH system.

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

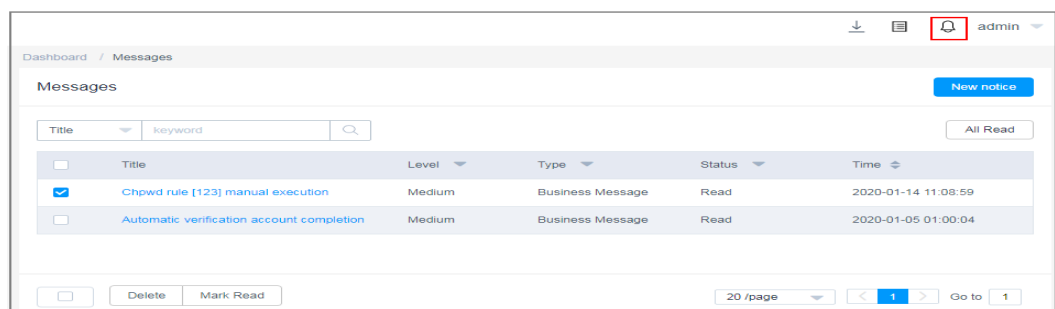
The following figure shows an example.

Figure 4-41 Small message center window



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

Figure 4-42 Message list

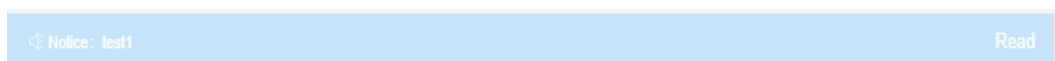


Step 4 Click **New notice**.

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

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

Figure 4-43 Example notice



----End


4.5 Download Center


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

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

Procedure

Step 1 Log in to the CBH system.

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

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

----End

5 Department

5.1 Overview

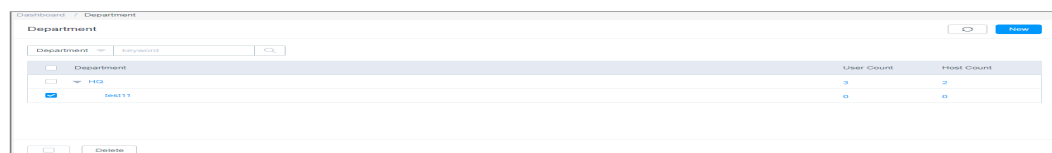
The **Department** module works as an organization that is used to group organization structure and identify users and resources. A CBH system has a default department named **HQ**. The **HQ** department cannot be deleted. Other departments can be created only under the **HQ** department.

Users in lower-level departments cannot view superior department information, including the organization structure, users, host resources, application resources, application publish servers, resource accounts, and policies and operation audit data configured by superior departments.

For users in different departments, they can be managed by administrators of their own department and superior department only.

Only system administrator **admin** or users with the management permissions for the **Department** module can manage the department organization structure, including creating, editing, deleting, and querying a department, querying users in a certain department, and querying resources in a certain department.

Figure 5-1 Department management



5.2 Creating a Department

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

Prerequisites

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

Procedure

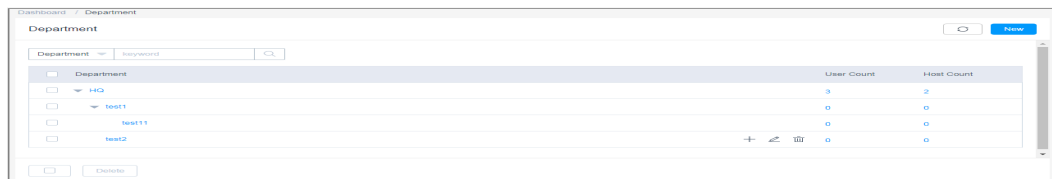
- Step 1** Log in to the CBH system.
- Step 2** In the navigation pane on the left, select **Department**.
- Step 3** On the displayed page, click **New** in the upper right corner of the page to open the **New Department** dialog box.
- Step 4** Select a superior department for **Superior Dept**, enter a name of the department to be created in the **Department** field, and enter the description in the **Remarks** area if necessary.

NOTE

- The department name defined in a CBH system must be unique.
- The superior department can be selected only from the existing department directory tree.

- Step 5** Click **OK**. You can then view the new department on the department management page.

Figure 5-2 Creating a department



----End

How to Create a Department Quickly

- Step 1** Log in to the CBH system.
- Step 2** Select **Department** in the navigation pane on the left.
- Step 3** In the column of the corresponding superior department, click **+** to create a lower-level department.
- Step 4** Change the department name.

----End

5.3 Deleting a Department

The default department **HQ** is the top department in a CBH system and cannot be deleted. When a superior department is deleted, all its lower-level departments are deleted automatically.

Prerequisites

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

Procedure

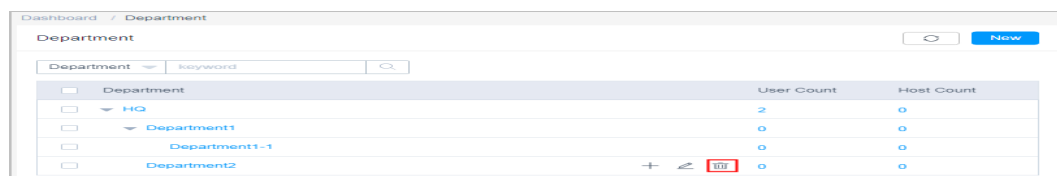
- Step 1** Log in to the CBH system.
- Step 2** Select **Department** in the navigation pane on the left.
- Step 3** Delete a department.

Move the cursor over the row where the department to be deleted locates to let the operation icons appear. Click then the deletion icon to delete the department.

NOTE

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

Figure 5-3 Deleting a department

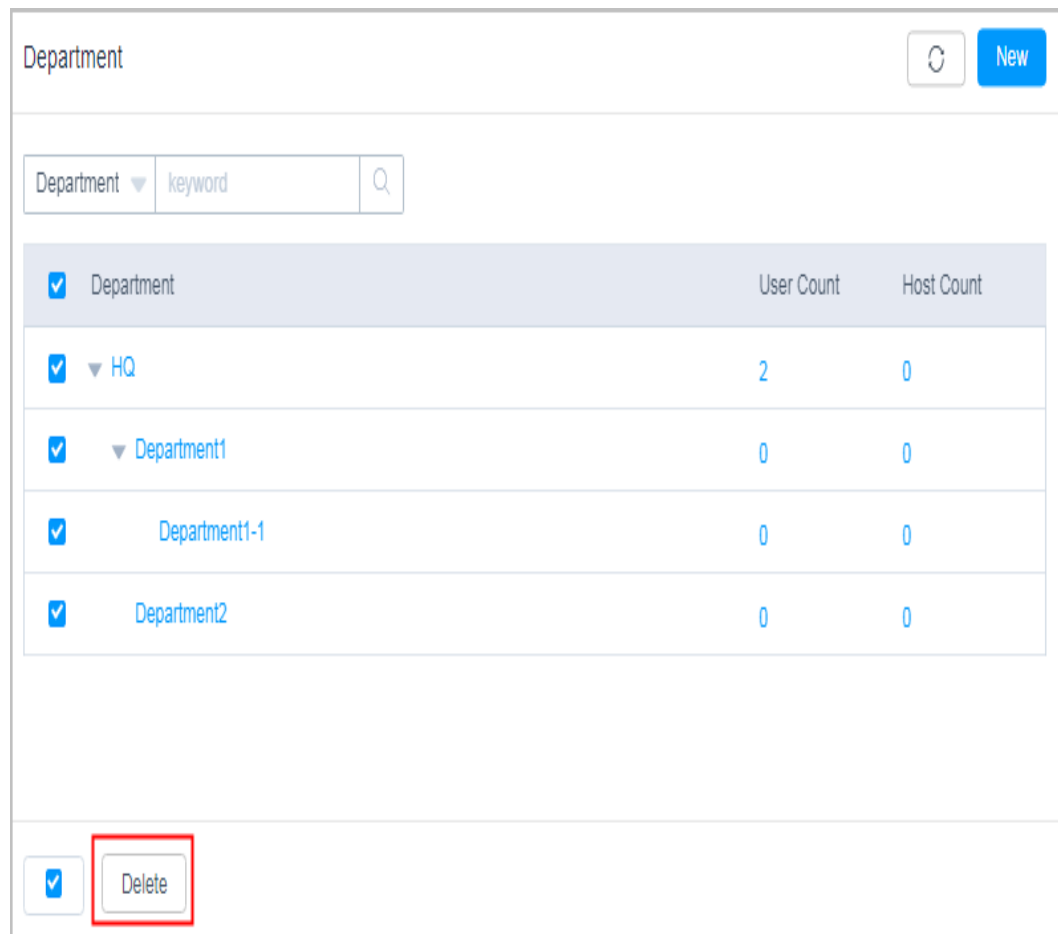


Department	User Count	Host Count
HQ	2	0
Department1	0	0
Department1-1	0	0
Department2	0	0

- Step 4** Delete departments in batches.

Select the ones you want and click **Delete** at the bottom of the list to delete all selected departments together.

Figure 5-4 Batch deleting departments



----End

5.4 Viewing and Editing Department Information

You can change department name and superior department a department belongs to.

After a department is moved from one superior department to another, resources and users in the department are automatically moved accordingly.

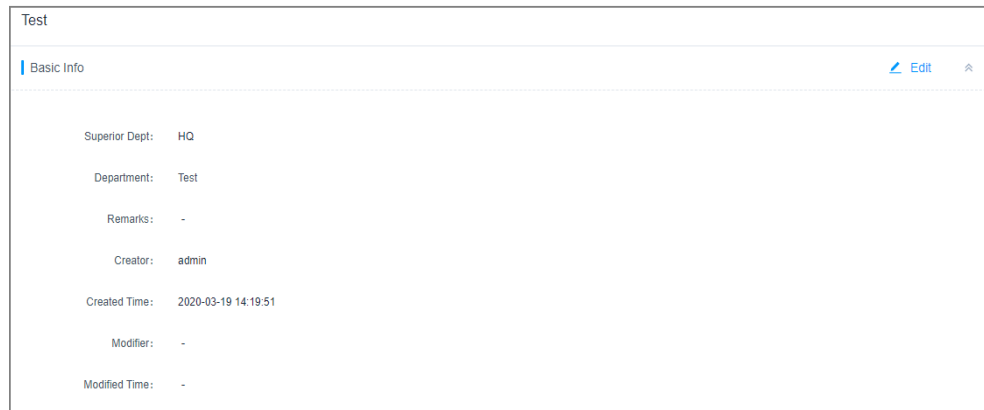
Prerequisites

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

Procedure

- Step 1** Log in to the CBH system.
- Step 2** Select **Department** in the navigation pane on the left.
- Step 3** Click the name of the department to be edited.

Figure 5-5 Basic department information



Step 4 In the **Basic Info** area, view the detailed information about the department.
Click **Edit** and edit basic information.

----End

5.5 Querying Configurations of a Department

CBH collects statistics on the number of users and hosts under each department. You can query the user and host asset configurations of a department on the department management page. Application resources and application publish servers are not included in the statistics.

Prerequisites

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

Procedure

- Step 1** Log in to the CBH system.
- Step 2** Select **Department** in the navigation pane on the left.
- Step 3** Enter a department name in the search box to query the superior department tree to which the department belongs.
- Step 4** View the number of users or hosts in the **User Count** or **Host Count** column in each department in the department tree.
- Step 5** Click a specific number to go to the **User** or **Host** page, respectively, and then view the department configuration.

----End

6 User

6.1 Overview

A CBH system allows you to centrally manage users. Creating a CBH system user is to create an account for logging in to the CBH system. The system administrator **admin** is the first account for users to log in to a CBH system for the first time. The **admin** user has the highest operation permissions and such permissions cannot be deleted or changed.

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

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

6.2 User Management

6.2.1 Creating a User and Assigning a Role to the User

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

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

Constraints

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

Prerequisites

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

Creating a User

Step 1 Log in to the CBH system.

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

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

Table 6-1 Parameters for creating a user

Parameter	Description
LoginName	Specifies the username for logging in to the CBH system. The LoginName must be unique in a CBH system and cannot be changed once created.
Verification Type	Specifies how the user is verified for logging in to the CBH system. <ul style="list-style-type: none"> • Local: (default method) The user is verified against the account management system of the CBH system. • AD: The user is verified against the Windows AD domain server. • LDAP: The user is verified against the third-party authentication server through the LDAP protocol. • RADIUS: The user is verified against the third-party authentication server through the RADIUS protocol. • Azure AD: The user is verified against the Azure platform based on Security Assertion Markup Language (SAML) configuration. <p>NOTE If you want to verify the user against a remote AD domain, LDAP, or RADIUS servers or verify the user against the Azure AD service, configure the remote authentication server in the CBH system. For details, see Authentication Configuration.</p>
Domain name	This parameter is mandatory if you select Azure AD for Verification Type . Provide the suffix you registered with the Azure platform.
Password/Confirm Password	A password must be configured for the user to log in to the CBH system if you select Local for Verification Type .
Authentication server	An authentication server must be configured if you select AD or LDAP for Verification Type .

Parameter	Description
UserName	Specifies the user-defined user name. This name indicates the name of the person who uses the account so that CBH system users can be distinguished from each other.
Mobile	Specifies the mobile number of the user. This number is used for SMS authentication logins and password resetting.
Email	Specifies the email address of the user. The CBH system sends notifications to this email address.
Role	Specifies the role to be assigned to the user. Only one role can be assigned. By default, system roles include DepartmentManager , PolicyManager , AuditManager , and User . <ul style="list-style-type: none"> • DepartmentManager: responsible for managing departments. Except the User and Role modules, this role has the configuration permissions for all other modules. • PolicyManager: responsible for configuring policy permissions. This role has the configuration permissions for the User Group, Account Group, and ACL Rules modules. • AuditManager: responsible for auditing system and maintenance data. This role has the configuration permission for Live Session, History Session, and System Log modules. • User: common system users and resource operators. This role has the permissions for the Host Operations, App Operations, and Ticket approval modules. • User-defined role: Only the admin user can customize a new role or edit permissions of a default role. For details, see Role Overview.
Department Name	Specifies the department to which the user belongs. For details about how to create a department in a CBH system, see Creating a Department .
Remarks	(Optional) Provides supplementary information about the user.


Step 4 Click **OK**.

----End

Batch Importing Users

Step 1 Log in to the CBH system.

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

Step 3 Click  in the upper right corner.

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

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

Table 6-2 Template parameters

Parameter	Description
LoginName	(Mandatory) Specifies the username for the user to log in to the CBH system.
Verification Type	(Mandatory) Specifies the authentication method. Only one authentication method can be entered. You can select Local , RADIUS , AD Domain , LDAP , Azure AD , or IAM .
Password	(Mandatory) Specifies the user-defined login password. This parameter is required when Verification Type is set to Local .
Authentication server/ Domain name	(Mandatory) Specifies the authentication server. This parameter is required if Verification Type is set to AD , LDAP , or Azure AD . Note that the value must be entered in required format. <ul style="list-style-type: none"> For AD domain authentication, the value must be in the format of <i>IP:PORT</i>, for example, <i>10.10.10.10:389</i>. For LDAP authentication, the value must be in the format of <i>IP:PORT/ou=test,dc=test,dc=com</i>, for example, <i>10.10.10.10:389/ou=test,dc=com</i>. For Azure AD authentication, provide the domain name.
UserName	Enter the name of a system user.
Mobile	Enter the mobile number of a system user.
Email	(Mandatory) Enter the email address of a system user.
Role	(Mandatory) Enter the system role of the user. <ul style="list-style-type: none"> Only one role type can be entered. There are four default roles for your choice: DepartmentManager, PolicyManager, AuditManager, and User. Only the role that has been created in the CBH system can be entered.
Department Name	(Mandatory) Enter the department to which the user belongs. The department structure must be complete. <ul style="list-style-type: none"> Only one department structure can be entered, and a user can belong to only one department. By default, the department can be set to HQ. Use a comma (,) to separate a department and its lower-level department. Only the department that has been created in the CBH system can be entered.

Parameter	Description
Remarks	Provides supplementary information about the user account.
User Groups	<p>Specifies the user group that a user belongs to.</p> <ul style="list-style-type: none"> A user account can belong to multiple user groups in the same department. Use a comma (,) to separate every two user groups. Only the user group that has been created in the CBH system can be entered.

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

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

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

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

----End

Synchronizing AD Domain Users

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

Step 1 Log in to the CBH system.

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

Figure 6-1 Configuring remote authentication



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

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

Table 6-3 AD settings for synchronizing users

Parameter	Description
Server	Specifies the IP address of the AD domain server.

Parameter	Description
Status	<p>Specifies whether to enable AD domain remote authentication. AD domain remote authentication is enabled by default.</p> <ul style="list-style-type: none"> • Enabled: AD domain authentication is enabled. If the configuration information is valid, AD domain authentication is enabled or AD domain users are synchronized to the CBH system when the user logs in to the CBH system. • Disabled: AD domain authentication is disabled.
SSL	<p>Specifies whether to enable SSL encryption. SSL encryption is disabled by default.</p> <ul style="list-style-type: none"> • Disabled: SSL encryption is disabled. • After SSL encryption is enabled, data transmitted by synchronized users or authenticated users is encrypted.
Mode	Specifies the working mode of AD domain. Select Sync Mode .
Port	Specifies the access port of the remote server of AD domain. The default port number is 389.
LoginName	Specifies the username of the account for logging in to the AD domain server.
Password	Specifies the password of the account for logging in to the AD domain server.
Domain	Specifies the domain of the AD service.
Base DN	Specifies the base DN for the remote AD domain server.
Dept Filter	Specifies the departments to be filtered out for the remote AD domain server.
User Filter	Specifies the users to be filtered out for the remote AD domain server.
Login Name Filter	Specifies the login name to be filtered out. Separate multiple login names with vertical bars ().
UserName	Specifies the attribute name of user names on the remote AD domain server, for example, name.
Email	Specifies the attribute name of the user mailbox on the AD domain remote server, for example, mail.
Mobile	Specifies the attribute name of user's mobile phone on the AD domain remote server, for example, mobile.

Parameter	Description
Sync	<p>Specifies the AD user synchronization method. The options include Manual and Auto.</p> <ul style="list-style-type: none"> • Manual: After you complete required configurations, manually synchronize the user information from the AD server. • Auto: After you complete required configurations, user information is automatically synchronized. You are also required to configure Start time of sync, Duration, and End time for auto synchronization.
Department	<p>Specifies the department to which the synchronized user account belongs.</p>
Options	<p>Override existing</p> <ul style="list-style-type: none"> • Selected: If an existing user account and the user account being imported have the same LoginName, the existing one will be overwritten. The user account information in CBH is updated accordingly. • Deselected: If an existing user account and the user account being imported have the same LoginName, the existing one will be skipped and kept unchanged.

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

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

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

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

----End

6.2.2 Enabling or Disabling a User

CBH allows you to batch **Enable** or **Disable** other users and change the user account status with just a few clicks.

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

- Enable
 - The default user status is **Enabled**. Enabled users can use the CBH system within the permission scope.
- Disable

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

Prerequisites

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

Procedure

Step 1 Log in to the CBH system.

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

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

----End

6.2.3 Deleting a User

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

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

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

Prerequisites

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

Procedure

Step 1 Log in to the CBH system.

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

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

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

----End

6.2.4 Configuring User Login Restrictions

Overview

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

- Multifactor verification: authenticates user login by SMS, OTP token, or USB key as well as password.

- **Period of validity:** determines the validity period of a user account for logging in to the CBH system.
- **Login limit by time:** allows or forbids a user account to log in to the CBH system at the specified duration.
- **Login limit by IP address:** allows or forbids only users from specified IP addresses to log in to the CBH system.
- **Login limit by MAC address:** allows or forbids only users with specified MAC addresses on a LAN to log in to the CBH system.

Constraints

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

Prerequisites

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

Procedure

- Step 1** Log in to the CBH system.
- Step 2** Choose **User > User** in the navigation pane.
- Step 3** Click the login name of the user whose information you want to change, or click **Manage** in the row of the user in the **Operation** column.
- Step 4** Click **Edit** in the **User Setting** area.

Table 6-4 User login limit parameters

Parameter	Description
Multifactor Verification	<p>Specifies the authentication methods for users to log in to the CBH system. The options are Mobile SMS, Mobile OTP, USBKey, and OTP token.</p> <ul style="list-style-type: none"> • By default, all options are deselected. If no options are selected, only the local password is used for identity authentication. • Mobile SMS: Mobile SMS can be enabled in multifactor verification only after a mobile number is bound to the user account for receiving SMS messages. • Mobile OTP: To make the mobile OTP authentication take effect, bind a mobile OTP to the user account in Profile first. • USBKey: To make the USBKey multifactor verification take effect, relate the user account to an issued USB Key. For details, see Issuing a USB Key. • OTP token: To make the OTP token authentication take effect, relate the user account to an OTP token. For details, see Issuing an OTP Token.
IAM Login	If you enable this, you can directly log in to the CBH instance from IAM.
Period of validity	Specifies the validity period of the user account.
Logon Time Limit	Specifies the allowed or forbidden login time range. The time limit is set by the day and the hour.
Edit IP limit	<p>Specifies the IP address or IP address range to be blacklisted or whitelisted.</p> <ul style="list-style-type: none"> • Blacklist: forbids all user logins from the specified IP address or IP address range. • Whitelist: allows only user logins from the specified IP address or IP address range. • Blacklist-Multifactor Verification for within the List: allows you to configure the IP address or IP address range for the blacklist. Users whose IP addresses or IP address ranges are in the blacklist are allowed to log in to the CBH system only when multifactor verification is configured for them. • Blacklist-Multifactor Verification for beyond the List: allows you to configure the IP address or IP address range for the whitelist. Users whose IP addresses or IP address ranges are not in the whitelist are allowed to log in to the CBH system only when multifactor verification is configured for them. • If no IP address is specified, there is no IP-based login limit.

Parameter	Description
MAC Limit	<p>Specifies the MAC address or address range to be blacklisted or whitelisted.</p> <ul style="list-style-type: none">• Blacklist: forbids all users from configured MAC addresses to log in to the CBH system.• Whitelist: allows only users from configured MAC addresses to log in to the CBH system.• If no MAC address is specified, there is no login limit by MAC address.

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

----End

Batch Changing User Login Configurations

Step 1 Log in to the CBH system.

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

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

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

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

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

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

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

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

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

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

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

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

----End

6.2.5 Querying and Editing User Information

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

CBH allows you to query, view, and edit user information, including basic user and user group information, login restrictions, authorized resource accounts, multifactor verification methods, and the validity period of user accounts.

Prerequisites

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

Querying a User

Step 1 Log in to the CBH system.

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

Step 3 Quick search

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

Step 4 Advanced search

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

----End

Viewing and Editing User Information

Step 1 Log in to the CBH system.

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

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

Figure 6-2 User details



Step 4 Edit basic information.

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

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

Figure 6-3 Basic user information

| Basic Info

LoginName:	admin
Verification Type:	Local
UserName:	sys-admin
Mobile:	1****
Email:	-
Role:	Sysadmin
Department:	Headquarters
Remarks:	-
Creator:	-
Created Time:	2017-10-11 09:00:00
Modifier:	admin
Modified Time:	2023-02-02 16:05:58
LastLoginTime:	2023-02-02 19:06:54

Step 5 Edit user login configurations.

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

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

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

Step 7 View the authorized accounts and resources.

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

Figure 6-4 Authorized Account

Account	Status	Resource	Host/APP Addr	Port	Protocol	Login Type	Department
root	N/A	RDS_A	192.168.1.1	3306	MySQL	Auto Login	Test

----End

Batch Editing User Information

Step 1 Log in to the CBH system.

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

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

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

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

Step 5 Edit role of several users at a time.

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

----End

6.2.6 Changing User Login Passwords

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

Constraints

- You are not allowed to change the password of system administrator **admin**. It can only be changed in the **Profile** module as user **admin**.
- If your password is changed by batch resetting, change the password when the first time you log in to the CBH system after password resetting. This is because the same password is generated for all selected users during password batch resetting.
- After you log in to a CBH system, only the passwords of other users can be batch reset.
- Plaintext passwords cannot be viewed or exported.
- For users with remote authentication enabled, their passwords can be changed only on the remote authentication server instead of CBH.

Prerequisites

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

Procedure

Step 1 Log in to the CBH system.

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

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

Step 4 Click **Reset Password**.

Step 5 Set the password.

Step 6 Click **OK**.

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

----End

6.2.7 Exporting User Information

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

Constraints

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

Prerequisites

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

Procedure

Step 1 Log in to the CBH system.

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

Step 3 Select the user accounts you want to export.

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

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

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

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

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

----End

6.2.8 Adding Users to a User Group

This topic describes how to add a user to a user group. A user can be added to multiple user groups.

Constraints

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

Prerequisites

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

Adding a User to a User Group

Step 1 Log in to the CBH system.

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

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

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

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

----End

Adding Multiple Users to a User Group

Step 1 Log in to the CBH system.

- Step 2** In the navigation pane on the left, choose **User > User Group** to go to the user group list page.
 - Step 3** In the **Operation** column of the user group you want to add users to, click **Member**.
 - Step 4** In the displayed **Edit UserGroup** dialog box, select multiple user accounts and add them to the user group.
 - Step 5** Click **OK**. You can view the added members on the **User Group** page.
- End

6.3 User Role Management

6.3.1 Overview

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

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

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

Table 6-5 Default roles

Parameter	Description
DepartmentManager	Specifies the operation administrator of the department, who manages the CBH system. DepartmentManager has the configuration permissions for all other modules except User and Role modules.
PolicyManager	Specifies the user permission policy administrator. This role manages host operation permissions. It has the permissions for configuration of the user management, resource group management, and access policy management modules.
AuditManager	Specifies the O&M result audit administrator. This role queries and manages system audit data. This role has the configuration permissions for real-time session, historical session, and system logs modules.
User	Specifies common users and operators. This role has the permissions for O&M of resources, such as host and application resources, and service ticket authorization management.

6.3.2 Creating a Custom Role

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

Constraints

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

Creating a Role

Step 1 Log in to the CBH system.

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

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

Table 6-6 Parameters for creating a role

Parameter	Description
Role	Specifies the role name. The value of Role must be unique in a CBH system and cannot be changed after it is created.
Managing Permission	Specifies whether to enable permission management for the role. Users assigned with management permissions can select a superior department when they create a resource or user. <ul style="list-style-type: none"> • Enable: The role has the management permissions and users with this role granted can view the data of their departments and lower-level departments. • Disable: The role has no management permissions.
Remarks	(Optional) Provides supplementary information about the role.

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

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

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

----End

6.3.3 Deleting a Role

This topic describes how to delete a role.

Constraints

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

Procedure

Step 1 Log in to the CBH system.

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

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

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

----End

6.3.4 Querying and Editing Role Information

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

Constraints

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

Procedure

Step 1 Log in to the CBH system.

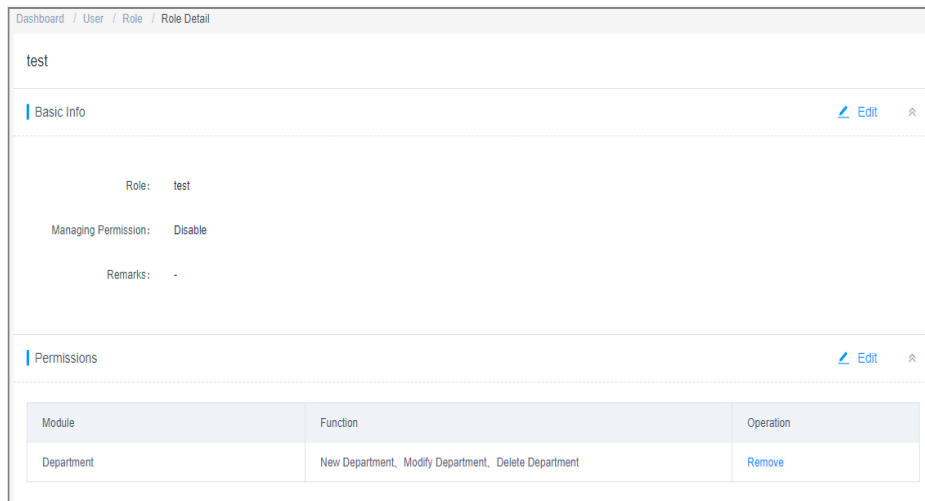
Step 2 In the navigation pane on the left, choose **User > Role** to go to the role list page.

Step 3 Query a role.

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

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

Figure 6-5 Role Detail



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

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

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

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

----End

6.4 User Group Management

6.4.1 Overview

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

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

A user group is associated with a department and does not belong to an individual user. By default, a user group created by the current login user belongs to the department of the user. The department cannot be changed. Users who have the user group permissions can only view the information about all the user groups of their departments and lower-level departments.

 **NOTE**

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

6.4.2 Creating a User Group

This section describes how to create a user group.

Prerequisites

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

Procedure

- Step 1** Log in to the CBH system.
- Step 2** In the navigation pane on the left, choose **User > User Group** to go to the user group list page.
- Step 3** Click **New**. In the **New UserGroup** dialog box displayed, configure basic information about the group.

Table 6-7 Creating a User Group

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

- Step 4** Enter a user group name and descriptions in the **Group** and **Remarks** fields, respectively. The user group name in a CBH system must be unique.
- Step 5** Click **OK**. You can then view the newly created user group in the user group list and add members to it. For details, see [Adding Users to a User Group](#).

----End

6.4.3 Deleting a User Group

CBH allows you to delete user groups. After a user group is deleted, the resource permissions the group members have been granted through the user group become invalid.

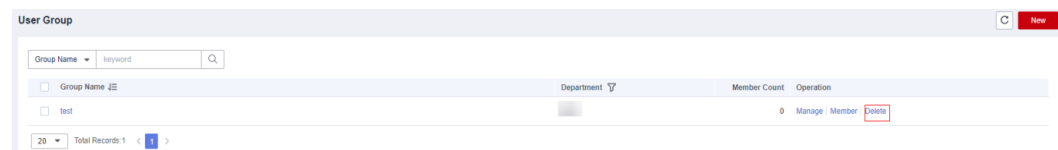
Prerequisites

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

Procedure

- Step 1** Log in to the CBH system.
- Step 2** Choose **User > User Group** in the navigation pane.
- Step 3** To delete a single user group, click **Delete** in the **Operation** column of the user group.

Figure 6-6 Deleting a user group



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

----End

6.4.4 Querying and Editing User Group Information

CBH allows you to view and edit basic information and members of a user group.

Constraints

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

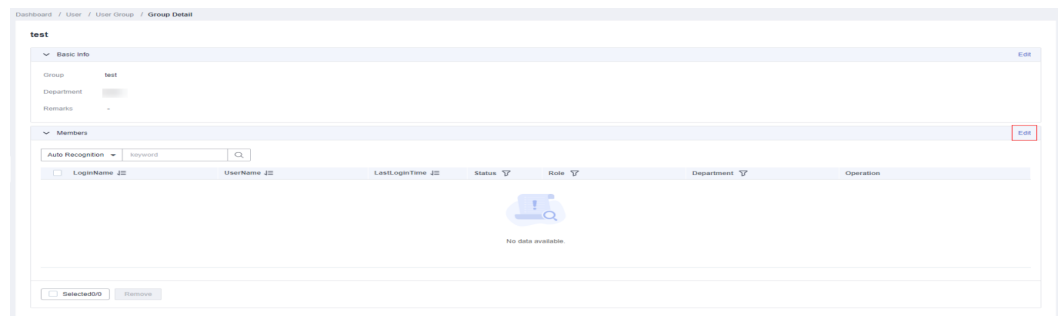
Prerequisites

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

Procedure

- Step 1** Log in to the CBH system.
- Step 2** Choose **User > User Group** in the navigation pane.
- Step 3** Query a user group.
Enter a keyword in the search box and search for a user group by name.
- Step 4** Click the name of the user group you want to edit or click **Manage** in the row of the user group in the **Operation** column.

Figure 6-7 User group details



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

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

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

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

----End

6.5 Remote Authentication Management

6.5.1 Configuring Remote AD Authentication

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

- **Auth Mode**
If this mode is selected, CBH does not synchronize user information from the AD domain server. The administrator needs to manually create users of the CBH system. When a user logs in to a CBH system, the user identify is authenticated by the AD domain server.
- **Sync Mode**
If this mode is selected, CBH synchronizes user information from the AD domain server. Therefore, the administrator does not need to create users of the CBH system. When a user logs in to a CBH system, the user identify is authenticated by the AD domain server. For details, see [Synchronizing AD Domain Users](#).

This topic describes how to configure the AD authentication mode.

Prerequisites

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

Procedure

Step 1 Log in to the CBH system.

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







Figure 6-8 Configuring remote authentication



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

Step 4 Select **Auth** for **Auth Mode** and configure other parameters as shown in [Table 6-8](#).

Table 6-8 AD authentication parameters

Parameter	Description
Server	Specifies the IP address of the AD domain server.
Status	Specifies the status of remote AD authentication (default: ). <ul style="list-style-type: none"> : AD domain authentication is enabled. If the configuration information is valid, AD domain authentication is enabled or AD domain users are synchronized to the CBH system when the user logs in to the CBH system. : AD authentication is disabled.
SSL	Specifies the status of SSL encryption (default: ). <ul style="list-style-type: none"> : SSL encryption is disabled. : SSL encryption is enabled. After SSL encryption is enabled, data transmitted by synchronized users or authenticated users is encrypted.
Mode	Specifies the working mode of AD domain. Select Auth Mode .
Port	Specifies the access port of the remote server of AD domain. The default port number is 389.
Domain	Specifies the domain of the AD service.

Step 5 Click **OK**. You can then view AD authentication configurations in the AD server list.

----End

Follow-up Operations

- To view details of the configured AD authentication, click **Details** in the **Operation** column.

- To modify or disable AD authentication, or change the authentication mode, click **Edit** in the **Operation** column and reconfigure the AD authentication in the displayed dialog box.
- If the AD authentication is no longer required, click **Delete** in the **Operation** column to delete it. Deleted authentication information cannot be recovered. Exercise caution when performing this operation.

6.5.2 Configuring Remote LDAP Authentication

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

This topic describes how to configure the LDAP authentication mode.

Constraints

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

Prerequisites

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

Procedure

Step 1 Log in to the CBH system.

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

Figure 6-9 Configuring remote authentication









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

LDAP supports the two authentication modes:

- If you select **Auth** for **Auth Mode**, configure the parameters by referring to [Table 6-9](#).

Table 6-9 LDAP authentication parameters

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

Parameter	Description
Status	<p>Specifies whether to enable remote LDAP authentication. Remote LDAP authentication is enabled by default (.</p> <ul style="list-style-type: none"> - : LDAP authentication is enabled. Remote LDAP authentication is enabled when the user logs in to the CBH system. - : LDAP authentication is disabled.
SSL	<p>Specifies whether to enable SSL encryption. SSL encryption is disabled by default (.</p> <ul style="list-style-type: none"> - : SSL encryption is disabled. - : SSL encryption is enabled. After SSL encryption is enabled, data transmitted by synchronized users or authenticated users is encrypted.
Port	<p>Specifies the access port of the remote LDAP server. The default port number is 389.</p>
Mode	<p>Select Auth Mode or Sync Mode.</p> <ul style="list-style-type: none"> - Auth Mode: The bastion host is interconnected with the AD server. To add a domain user, you need to manually select LDAP authentication on the user management page. - Sync Mode: After the bastion host is connected to the AD server, you can choose Systemconfig > Authenticate and synchronize users under the corresponding OU to the bastion host.
User OU	<p>Specifies the user organization unit (OU) on the LDAP server.</p>
User Filter	<p>Specifies the users to be filtered out on the LDAP server.</p>

- Select **Auth** for **Auth Mode** and configure the parameters by referring to [Table 6-10](#).

Figure 6-10 Inquire

X

LDAP Settings

Status

* Server
IP address or domain

SSL

* Port
Digits of 1-65535

Mode Auth Mode Sync Mode







Auth Mode Auth Inquire

* User OU

* User Filter

Table 6-10 LDAP inquiring mode parameters

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

Parameter	Description
Status	<p>Specifies whether to enable remote LDAP authentication. Remote LDAP authentication is enabled by default (.</p> <ul style="list-style-type: none"> : LDAP authentication is enabled. Remote LDAP authentication is enabled when the user logs in to the CBH system. : LDAP authentication is disabled.
SSL	<p>Specifies whether to enable SSL encryption. SSL encryption is disabled by default (.</p> <ul style="list-style-type: none"> : SSL encryption is disabled. : SSL encryption is enabled. After SSL encryption is enabled, data transmitted by synchronized users or authenticated users is encrypted.
Port	Specifies the access port of the remote LDAP server. The default port number is 389.
Mode	<p>Select Auth Mode or Sync Mode.</p> <ul style="list-style-type: none"> The CBH instance is interconnected with the AD server. To add a domain user, you need to manually select LDAP authentication on the user management page. After the CBH instance is connected to the AD server, you can choose Systemconfig > Authenticate and synchronize users under the corresponding OU to the bastion host.
Base DN	Base DN of the LDAP server.
Administrator DN	Administrator DN.
Administrator Password	Password of the administrator.
User OU	Specifies the user organization unit (OU) on the LDAP server.
User Filter	Specifies the users to be filtered out on the LDAP server.

Step 4 Click **OK**. You can then view LDAP authentication configurations in the LDAP server list.

----End

Follow-up Operations

- To view details of the configured LDAP authentication, click **Details** in the **Operation** column.

- To modify or disable LDAP authentication, click **Edit** in the **Operation** column and reconfigure LDAP authentication in the displayed dialog box.
- If the LDAP authentication is no longer required, click **Delete** in the **Operation** column to delete it. Deleted authentication information cannot be recovered. Exercise caution when performing this operation.

6.5.3 Configuring Remote RADIUS Authentication

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

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

Prerequisites

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

Procedure

Step 1 Log in to the CBH system.




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

Figure 6-11 Configuring remote authentication



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

Table 6-11 RADIUS authentication parameters

Parameter	Description
Server	Specifies the IP address of the RADIUS server.
Status	Specifies the status of remote RADIUS authentication (default: ). <ul style="list-style-type: none"> •  : RADIUS authentication is enabled. Remote RADIUS authentication is enabled when the user logs in to the CBH system. •  : RADIUS authentication is disabled.
Port	Specifies the access port of the remote RADIUS server. The default port number is 1812.
Protocol	Specifies the remote authentication protocol. This parameter can be set to PAP or CHAP .

Parameter	Description
Password	Specifies the authentication key of the remote RADIUS server.
Timeout	Specifies the timeout for remote RADIUS authentication.
Username	Specifies the username on the RADIUS server to test whether the RADIUS server information is correct.
Password	Specifies the password of username on the RADIUS server to test whether the RADIUS server information is correct.
Test validity	You can click Test validity to test whether the RADIUS server is configured properly.

Step 4 Click **OK**. You can then view RADIUS authentication configurations in the RADIUS server list.

----End

Follow-up Operations

To modify or disable RADIUS authentication, click **Edit** in the **Operation** column and reconfigure RADIUS authentication in the displayed dialog box.

6.5.4 Configuring Remote Azure AD Authentication

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

This topic describes how to configure the Azure AD authentication.

Prerequisites

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

Procedure

Step 1 Log in to the CBH system.




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

Figure 6-12 Configuring remote authentication



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

Table 6-12 Azure AD authentication parameters

Parameter	Description
Status	Specifies the status of remote Azure AD authentication (default: ). <ul style="list-style-type: none">  : Azure AD authentication is enabled. Remote Azure AD authentication is enabled when the user logs in to the CBH system.  : Azure AD authentication is disabled.
Entity ID	Specifies the enterprise name or URL.
Reply URL	Specifies the reply URL. This parameter is automatically set to the URL of the current CBH system. If the IP address or domain name of the CBH system is changed, change the IP address or domain name in the URL.
Apply federation metadata URL	Specifies the application federation metadata URL generated after SAML signature certificate is configured in Microsoft Azure.
Logon URL	Specifies the login URL generated after SAML single sign-on is configured in Microsoft Azure.
Azure AD ID	Specifies the Azure AD ID generated after SAML single sign-on is configured in Microsoft Azure.

Step 4 Click **OK**. You can then view Azure AD authentication configurations in the Azure AD server list.

NOTICE

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

----End

Follow-up Operations

- To modify or disable Azure AD authentication, click **Edit** in the **Operation** column and reconfigure Azure AD authentication in the displayed dialog box.
- After Azure AD authentication is configured, you are required to create a user who has been added to the enterprise application or created on the Azure platform. For details, see [Creating a User](#).

6.5.5 Configuring Remote SAML Authentication

CBH interconnects with the SAML platform to authenticate CBH system user logins.

This topic describes how to configure the SAML authentication mode.

Prerequisites

- You have obtained the permission to manage the **System** module in the CBH system.
- You have created a user on the SAML platform and obtained related configurations on the SAML platform.

Procedure

Step 1 Log in to the CBH system.

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

Figure 6-13 Configuring remote authentication



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

Figure 6-14 Configuring SAML authentication

SAML config

Status

* Identifier (entity ID)

* NameIdFormat




* Signature certificate

* Login URL

* Logout URL

* Reply URL

Table 6-13 SAML authentication parameters

Parameter	Description
Status	Specifies the status of remote SAML authentication (default: ). <ul style="list-style-type: none"> : SAML-based authentication is enabled. Remote SAML authentication is enabled when the user logs in to the CBH system. : SAML-based authentication is disabled.
Entity ID	Obtain the metadata from IdP (Shibboleth IDP, which is configured in the C:\Program Files (x86)\Shibboleth\IdP\metadata directory by default). Identifier: Enter the following part of EntityID .
NameIdFormat	Obtain the metadata from IdP (Shibboleth IDP, which is configured in the C:\Program Files (x86)\Shibboleth\IdP\metadata directory by default). NameIdFormat: The value urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified is recommended.
Signature certificate	Enter the signing certificate of FrontChannel displayed in the IdP.
Logon URL	Enter the location address of SingleSignOnService displayed in the HTTP-Redirect .
Logout URL	Enter the location address of SingleLogoutService displayed in the HTTP-Redirect .
Reply URL	The default value of Host is the IP address of Localhost . Set this parameter based on the site requirements, for example, the domain name.

Step 4 Click **OK** to submit the configuration data. You can view and manage SAML authentication configurations.

----End

6.6 USB Key Management

USB keys can only be issued to user accounts with USB key authentication enabled in multifactor verification.

Before using a USB key for second authentication, prepare USB keys and install the USB key driver on the local computer. A USB key from a vendor cannot be identified by other vendors for login authentication. So, the vendor must be specified for each USB key. For details, see [Configuring USB Keys](#).

Prerequisites

- You have obtained a USB key.
- You have the management permissions for the **User** module.
- You have the management permissions for the **USBKey** module.

Procedure

One USB key can be issued to one user only.

Step 1 Log in to the CBH system.

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

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

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

Table 6-14 Parameters for issuing a USB key

Parameter	Description
USBKey	Specifies the USB key ID.
Relate User	Specifies the user to which the USB key is related. USB key in multifactor verification must be enabled for such users.
PIN	Specifies the personal identification number (PIN) uniquely corresponding to the USB key. It is provided by the USB key vendor.

Step 5 Click **OK**. You can then view the newly issued USB key in the USB key list.

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

----End

Revoking a USB Key

Step 1 Log in to the CBH system.

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

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

Step 4 To revoke multiple USB keys at a time, select the ones you want and click **Revoke** at the bottom of the USB key list to revoke the selected USB keys together.

----End

6.7 OTP Token Management

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

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

Prerequisites

- You have obtained a hardware token.
- You have the management permissions for the **User** module.
- You have the management permissions for the **OTP** module.

Issuing an OTP Token

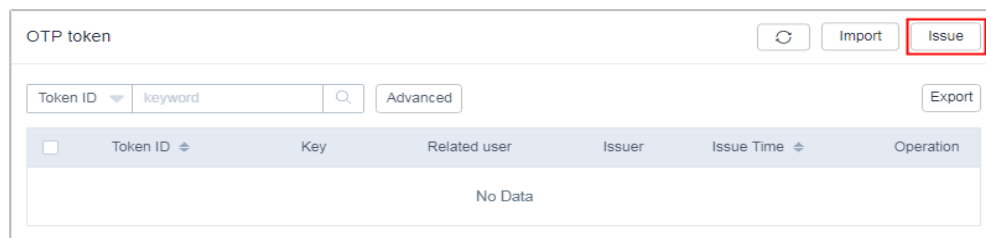
One OTP token can be issued only to one user.

Step 1 Log in to the CBH system.

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

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

Figure 6-15 New OTP token



Step 4 Enter the required token information.

Table 6-15 Parameters for issuing an OTP token

Parameter	Description
Token ID	Specifies the OTP token ID.
Key	Specifies the key uniquely corresponding to the OTP token. It is provided by the OTP token vendor.
Related User	Specifies the user to whom the OTP token is related. OTP token must be enabled in multifactor verification for such users.

Step 5 Click **OK**. You can view the newly issued OTP token in the OTP token list.

For users with OTP token enabled, they need to enter the username, password, and the dynamic password on the OTP token to log in to the CBH system.

----End

Importing an OTP Token

Step 1 Log in to the CBH system.

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

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

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

Step 5 Enter the configuration information of the OTP tokens to be imported according to the configuration requirements of the template.

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

- You can upload files in CSV, XLS, or XLSX format.
- **Override existing OTP token**
 - Selected: The token ID will be overwritten if two tokens have the same key and related user configured, and the information of the existing token will be updated but the token is not deleted.
 - Not selected: The system skips the tokens with duplicate keys and related users.

Step 7 Click **OK**. You can then view the imported OTP tokens in the token list.

----End

Exporting an OTP Token

Step 1 Log in to the CBH system.

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

Step 3 Select the OTP token to be exported.

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

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

----End

Revoking an OTP Token

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

Step 1 Log in to the CBH system.

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

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

Step 4 In the OTP token list, you can select multiple OTP tokens and click **Revoke** at the bottom of the list to revoke the selected tokens together.

----End

7 Resource

7.1 Overview

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

- Resource types

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

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

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

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

- Batch management

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

7.2 Managing Host Resources Using CBH

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

This topic describes how to add a host resource, import host resources from a file, import host resources from a cloud platform, automatically discover host resources, and clone host resources to CBH for centralized management.

Constraints

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

Prerequisites

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

Adding a Host Resource

Step 1 Log in to the CBH system.

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

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

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

Table 7-1 Host resource network parameters

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

Parameter	Description
Protocol	<p>Type of the protocol configured for the host.</p> <ul style="list-style-type: none"> In the CBH professional editions, you can configure SSH, RDP, VNC, Telnet, FTP, SFTP, DB2, MySQL, SQL Server, Oracle, SCP, Rlogin, and DM for a host. In the CBH standard editions, you can configure SSH, RDP, VNC, Telnet, FTP, SFTP, SCP, Rlogin, and DM for a host.
Host Address	<p>Host IP address that can be used to establish connection with the CBH system.</p> <ul style="list-style-type: none"> Select the EIP or private IP address of the host. Private IP addresses are recommended. By default, the IPv4 address of the host is used. After an IPv6 address is enabled for a host, select either the IPv4 address or IPv6 address. <p>NOTE It is recommended that you set Host Address to a private IP address on the same VPC network. This is because CBH manages host resources on the same VPC network based on network stability and proximity. The external access port of the private IP address is not restricted by the network security (security group and ACL) policies. While the EIP of the host is an independent elastic IP address. The port for external access over an EIP is restricted by network security policies. As a result, you may fail to log in to the host from the CBH system. So we recommend private IP addresses.</p>
Port	Port number of the host.
OS Type	<p>(Optional) Type of the host OS or device OS.</p> <ul style="list-style-type: none"> This parameter is automatically set by the CBH system. 14 OS types are supported. In addition, system administrator admin can customize OS types. For details, see OS Types.
Terminal Speed	If you select Rlogin for Protocol , you can select different terminal speed.
Encode	<p>If you select SSH or TELNET for Protocol, the Chinese character can be used on the O&M page.</p> <p>The options are UTF-8, Big5, and GB18030.</p>
Terminal Type	<p>If you select SSH or TELNET for Protocol, you can specify the O&M terminal you want.</p> <p>The options are Linux and Xterm.</p>

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

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

Table 7-2 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.
Login Type	<p>Login method. You can select Auto Login, Manual Login, Sudo Login, or CSMS Credentials 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. • If you select CSMS Credentials Login, make sure you have available credentials. • If you select Sudo Login, a password is mandatory.
Account	<p>Account username of the managed host.</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>

Parameter	Description
Password	<p>Password of the account being added.</p> <p>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"> • Verification succeeded. 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.
SSH Key	<p>Authentication method that can be configured for host resources using the SSH protocol.</p> <p>After the configuration, an SSH key is preferentially used to log in to a related host resource.</p>
Passphrase	<p>Private key sequence corresponding to the SSH key. This parameter is optional.</p> <ul style="list-style-type: none"> • You do not need to enter the password for logging in to the host when no private key password is generated. • You need to enter the private key password each time you log in to the host when the private key password is generated.
Description	Brief description of the account.

 **NOTE**

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

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

----End

Importing Host Resources from a File

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

Step 1 Log in to the CBH system.

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

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

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

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

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

Table 7-3 Template parameters

Parameter	Description
Name	(Mandatory) a user-defined host resource name.
IP address/ domain name	(Mandatory) IP address or domain name of a host.
Protocol	(Mandatory) Select the protocol type of the host resource. Only one protocol type can be selected for a certain type of host resource. <ul style="list-style-type: none"> In the CBH professional editions, you can configure SSH, RDP, VNC, Telnet, FTP, SFTP, DB2, MySQL, SQL Server, Oracle, SCP, and Rlogin for a host. In the CBH standard editions, you can configure SSH, RDP, VNC, Telnet, FTP, SFTP, SCP, and Rlogin for a host.
Port	(Mandatory) Enter the host port number.
OS Type	Enter the operating system type of the host.
Department Name	(Mandatory) the department to which the host resource belongs. The department structure must be complete. <ul style="list-style-type: none"> Only one department structure can be entered, and a resource can belong to only one department. By default, the department can be set to HQ. Use a comma (,) to separate a department and its lower-level department. Only the department that has been created in the CBH system can be entered.
Label	Label of the host resource. <ul style="list-style-type: none"> You can enter multiple labels and separate them with commas (,).
Remarks	Provides supplementary information about the host resource.
Account	Account of the host resource. <ul style="list-style-type: none"> If this parameter is left blank, no Empty account will be generated.
Logon Type	Method to log in to the host resource. <ul style="list-style-type: none"> This parameter can be set to Auto Login, Manual Login, or Sudo Login.

Parameter	Description
IS Sudo	Whether to set the account as a sudo account. <ul style="list-style-type: none"> This parameter can be set to Yes or No.
Password	Password of the account for logging in to the resource.
SSH Key	Authentication method that can be configured for SSH hosts. After the configuration, an SSH key is preferentially used to log in to a related host resource.
passphrase	Private key sequence mapped to the SSH key. You need to enter the private key password each time you log in to the host when the private key password is generated.
Oracle Param	This parameter is mandatory for Oracle hosts. <ul style="list-style-type: none"> This parameter can be set to SERVICE_NAME or SID. Separate multiple parameter values with commas (,).
SERVICE_NAME or SID	This parameter is mandatory for Oracle hosts. <ul style="list-style-type: none"> Separate multiple parameter values with commas (,).
Login Role	This parameter is mandatory for Oracle hosts. <ul style="list-style-type: none"> This parameter can be set to normal, sysdba, or sysoper. Separate multiple parameter values with commas (,).
Database Name	This parameter is mandatory for the DB2 databases. <ul style="list-style-type: none"> Select the database name or instance name. Separate multiple parameter values with commas (,).
Instance Name	This parameter is mandatory for the DB2 databases. <ul style="list-style-type: none"> Select the database name or instance name. Separate multiple parameter values with commas (,).
Switch From	For a host resource using the SSH protocol, enter its account username and set it to a sudo account.
Switch command	The command to switch over between accounts.
Description	Brief description of the managed resource account.
Account Group	The account group to which the managed resource account belongs. <ul style="list-style-type: none"> A managed resource account can belong to multiple account groups in the same department. Use a comma (,) to separate every two account groups. Only the account group that has been created in the CBH system can be entered.

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

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

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

Step 9 Click **OK**.

 **NOTE**

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

----End

Importing Hosts from a Cloud Platform

Step 1 Log in to the CBH system.

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

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

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

Table 7-4 Parameters for importing host resources from a cloud platform

Parameter	Description
Cloud Vendor	Cloud platform from which the host resources are imported. Currently, CBH supports importing of cloud host resources from multiple platforms.
Access Key ID	To get the access key ID, click the information icon on the right of the text box.
Access Key Secret	To get access key secret, click the information icon on the right of the text box of Access Key ID .
Priority of IP imported	You can select Public or Internal .

Parameter	Description
Options	<p>(Optional) Configure Override existing hosts, which is not selected by default.</p> <ul style="list-style-type: none"> Selected: An existing host resource will be overwritten when the existing host resource and the one being imported have the same <i>protocol type@host address:port</i> information. Deselected: An existing host resource will be skipped when the existing host resource and the one being imported have the same <i>protocol type@host address:port</i> information.
Department Name	Department to which the imported host resources belong.
Label	Label attached to the imported host resources.
Import Area	Regions supporting host resource importing.
Operating Environment	Running environment of the imported host resources. Currently, this parameter is required only for cloud hosts on the Azure cloud platform.

Step 5 Click **OK**.

----End

Auto Discovery of Host Resources

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

NOTE

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

Step 1 Log in to the CBH system.

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

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

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

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

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

Step 6 Select the host resources to be imported.

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

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

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

----End

Cloning Host Resources

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

Step 1 Log in to the CBH system.

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

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

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

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

Step 5 Click **OK**.

----End

7.3 Managing Application Servers Using CBH

CBH allows you to manage application resources and application accounts on Windows or Linux servers that support remote desktops. To do so, you only need to install clients and browsers on those servers.

After you obtain the permission for application resources, the CBH system allows you to access client-based application resources and browser-based application resources without manually entering usernames and passwords. This is because the CBH system automatically provides the credentials. In addition, the CBH system records all operations by video. In this way, remote application accounts security is under control, and remote application operations can be auditable.

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

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

Constraints

- The total number of host and application resources to be added cannot exceed the number of assets.
- For Windows servers, only applications running on Windows Server 2008 R2 or later can be managed.

- For Linux servers, only applications running on Linux CentOS 7.9 servers can be managed.
- Port 2376 and ports 35000 to 40000 must be enabled between a Linux server and CBH. The port cannot be changed once it is enabled.
- Contact technical support to obtain the password for logging in to a Linux server.
- Before you add an application resource, ensure that an application server has been added.
- Automatic login accounts cannot be configured for Microsoft Edge application resources.

Prerequisites

- You have purchased resources, such as Windows servers, Linux servers, images, enterprise authorization codes, and client licenses, for deploying an application publishing server.
- You have obtained the permission to manage the **AppServer** and **Application** tabs under the **Application Publish** module.

Adding an Application Server

Step 1 Log in to the CBH system.

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

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

Table 7-5 New AppServer parameters

Parameter	Description
Server Type	<ul style="list-style-type: none">• Windows• Linux
Server Name	Specifies the name of the application server. The server name must be unique in the CBH system.
Server	Specifies the IP address or domain name of the application server.

Parameter	Description
Type	<p>Specifies the type of the browser or client tool used to access the application.</p> <ul style="list-style-type: none"> If you set Server type to Windows: By default, 14 types are supported, including MySQL Tool, Microsoft Edge, Mozilla Firefox (for Windows servers), Oracle Tool, Google Chrome, VNC Client, SQL Server Tool, SecBrowser, vSphere Client, Radmin, dbisql, Navicat for MySQL, Navicat for PostgreSQL and Other. If you set Server type to Linux: Supported types: DM Tool, KingbaseES Tool, Mozilla Firefox for Linux, and GBaseDataStudio for GBase8a. <p>By default, each application resource type corresponds to an application program. You can obtain the application name from the default Program Path.</p>
Port	<p>Enter the port number for accessing the application publish server. The default port 3389 is used for a Windows server and default port 2376 is used for a Linux server.</p>
Account	<p>This parameter is mandatory if Server type is set to Windows. Specifies the server account used to access the application.</p> <p>If AD domain is configured, the server account is in the format of <i>AD domain name\account name</i>, for example, <i>ad\administrator</i>.</p>
Password	<ul style="list-style-type: none"> If you set Server type to Windows, enter the password of the server account used to access the application. If you set Server type to Linux, contact technical support to obtain the password.
Department Name	<p>Specifies the department of the application server.</p>
Program Path	<p>This parameter is mandatory if Server type is set to Windows. Specifies the path of the application resource on the application server.</p> <ul style="list-style-type: none"> Each program type has a default startup path. You can also customize a startup path. For example, to allow a system user to access only Google Chrome from the application server, set Program Path to C:\DevOpsTools\Chrome\chrome.exe. If you select Other, manually configure the corresponding program path.
Remarks	<p>(Optional) Provides the description of the application server.</p>

Step 4 Click **OK**.

----**End**

Importing Application Servers from a File

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

- Step 1** Log in to the CBH system.
 - Step 2** Choose **Resource > Application > AppServer**.
 - Step 3** Click **Import** in the upper right corner of the page.
 - Step 4** Click **Download** to download the template if no template is available locally.
 - Step 5** Enter the configuration information of application servers to be imported according to the configuration requirements in the template file.
 - Step 6** Click **Upload** and select the completed template.
 - Step 7** (Optional) Configure **Override existing appservers**. This option is deselected by default.
 - If you select this option, an existing application server information will be overwritten by the one being imported when both application servers have the same name.
 - If you deselect this option, an existing application server information will be skipped when the one being imported and the existing one have the same name.
 - Step 8** Click **OK**.
- End

Adding an Application Resource

- Step 1** Log in to the CBH system.
- Step 2** Choose **Resource > Application > Application**.
- Step 3** Click **New**. In the displayed **New application** dialog box, complete required parameters.

Table 7-6 Parameters for adding a new application resource

Parameter	Description
App Name	Specifies the name of an application resource to be added. The App Name of an application resource must be unique in the CBH system. NOTE The application name must be unique in the CBH system. This means it cannot be the same as the name of any managed hosts or other application resources.
AppServer	Select a created application publishing server.
Department Name	Specifies the department of the application.

Parameter	Description
APP Address	(Optional) Specifies the address of the application. The value can be an IP address or domain name. <ul style="list-style-type: none"> • If the application is released as a browser, enter the URL of the web page. If the address has a corresponding port, enter the address in the format of <i>URL:Port number</i>. • If the application is released as a database or client, enter the address of the database server.
APP Port	(Optional) Enter the application access port. <ul style="list-style-type: none"> • If the application is released as a database or client, enter the database access port. • Leave this parameter blank if the application is released in other formats except databases.
Param	(Optional) Set application parameters. <ul style="list-style-type: none"> • Enter the database instance name if the application is released as a database. • Leave this parameter blank if the application is released in other formats except databases.
Options	(Optional) Select File Manage , Uplink Clipboard , Downlink Clipboard , and/or Keyboard Audit .
Label	(Optional) You can customize a label or select an existing one.
Remarks	(Optional) Provides the description of the application resource.

Step 4 Click **Next**.

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

Parameter	Description
Add Account	<ul style="list-style-type: none"> • If you select Rightnow, configure Logon Type and then Account. • If you select Afterward, no further configuration is required on the page. You can add the account information later in the resource list or on the resource details page. In this situation, when you click OK, account [Empty] is automatically created. Only one [Empty] account is created for an application resource.
Logon Type	<ul style="list-style-type: none"> • If you select Auto Login, Account and Password must be provided. • If you select Manual Login, Account and Password are optional. If no application account is set, the [Empty] account is automatically created.

Parameter	Description
Account	Account to access the application
Password	Password of the application account
AD Domain	For Radmin application resources, enter the AD domain server address.
Description	Brief description of the account.

 **NOTE**

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

Step 5 Click **OK**.

----End

Importing Application Resources from a File

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

Step 1 Log in to the CBH system.

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

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

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

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

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

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

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

Step 8 Click **OK**.

----End

7.4 Adding Accounts of Managed Host or Application Resources into CBH

A host or application resource may have multiple accounts configured. Each account of a managed host or application resource is considered as a managed

resource account. You do not need to enter the username or password when you log in to a managed host using its managed resource accounts.

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

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

Constraints

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

Prerequisites

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

Adding an Account for a Resource

Step 1 Log in to the CBH system.

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

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

Table 7-8 Parameters for new managed resource accounts

Parameter	Description
Resource	Host or application resource to be related to the account.
Logon Type	<p>Login mode. You can select Manual Login, Auto Login, or Sudo Login.</p> <ul style="list-style-type: none"> • If you select Auto Login, Account and Password are mandatory. • If you select Manual Login, you can configure Account. • If you select CSMS Credentials Login, you can configure CSMS Credentials and Remarks. • If you select Sudo Login, a password is mandatory. • Sudo Login is valid only for SSH hosts. If Sudo Login is selected, Switch From and Switch Command are mandatory.

Parameter	Description
Accounts	Account name of the managed resource. The value of Account must be unique in a CBH system and cannot be changed after it is created. If you select IS sudo , the account is identified as a sudo account for managing resources and has the password change permission.
Password	Password of the account being added By default, Verify is selected. After the account is added, the system automatically verifies the status of the account. <ul style="list-style-type: none"> • After the account is verified, the resource information is saved. • If the verification fails, modify the configuration as prompted. If the system prompts that the account verification times out, modify the resource configuration. If the system prompts that the account password is incorrect, return to the configuration window and change the account password.
SSH Key	Authentication method that can be configured for host resources using the SSH protocol. After the configuration, an SSH key is preferentially used to log in to a related host resource.
Passphrase	Private key corresponding to the SSH key configured for an SSH host.
CSMS Credentials	(This parameter is available only when login mode is CSMS credential login.) Select the CSMS credential to be managed.
Switch From	For an SSH host, select a configured account and set it to a sudo account.
Switch command	Switchover command for an SSH host, for example, su root .
Description	Brief description of the account.

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

----End

Batch Importing Accounts of Managed Resources into CBH

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

Step 1 Log in to the CBH system.

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

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

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

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

Table 7-9 Template parameters

Parameter	Description
Account	(Mandatory) Enter the username of the managed resource account.
Logon Type	Method to log in to the resource. <ul style="list-style-type: none"> This parameter can be set to Auto Login, Manual Login, or Sudo Login.
IS Sudo	Whether to set the account as a sudo account. <ul style="list-style-type: none"> This parameter can be set to Yes or No.
Password	Password of the account for logging in to the resource.
SSH Key	Authentication method that can be configured for SSH hosts. After the configuration, an SSH key is preferentially used to log in to a related host resource.
Passphrase	Private key sequence mapped to the SSH key.
Oracle Param	This parameter is mandatory for Oracle hosts. <ul style="list-style-type: none"> This parameter can be set to SERVICE_NAME or SID. Separate multiple parameter values with commas (,).
SERVICE_NAME or SID	This parameter is mandatory for Oracle hosts. <ul style="list-style-type: none"> Separate multiple parameter values with commas (,).
Login Role	This parameter is mandatory for Oracle hosts. <ul style="list-style-type: none"> This parameter can be set to normal, sysdba, or sysoper. Separate multiple parameter values with commas (,).
Database Name	This parameter is mandatory for the DB2 databases. <ul style="list-style-type: none"> Select the database name or instance name. Separate multiple parameter values with commas (,).
Instance Name	This parameter is mandatory for the DB2 databases. <ul style="list-style-type: none"> Select the database name or instance name. Separate multiple parameter values with commas (,).
Switch From	Sudo account of the host resource.
Switch command	The command to switch over between accounts.

Parameter	Description
AD Domain	For Radmin application resources, enter the AD domain address.
Description	Brief description of the managed resource account.
Resource	Enter the name of the resource that has been added to the host list or application list.
IP address/domain name	For associated host resources, enter the IP address or domain name of the host resource.
Type	<p>(Mandatory) Enter the protocol type of the host resource or the application type of the application resource.</p> <ul style="list-style-type: none"> Supported host protocols: SSH, RDP, VNC, Telnet, FTP, SFTP, DB2, MySQL, SQL Server, Oracle, SCP, PostgreSQL, GaussDB, and Rlogin. Supported application types: Microsoft Internet Explore, Mozilla Firefox for Windows, Google Chrome, VNC Client, SecBrowser, vSphere Client, Radmin, dbisql, Mysql Tool, SQLServer Tool, Oracle Tool, Rlogin, Mozilla Firefox for Linux, DM Tool, KingbaseES Tool, GBaseDataStudio for GBase8a, X11, and Other.
Port	This parameter is mandatory for host resources. Enter the IP address or domain name of the host resource.
Account Group	<p>The account group to which the managed resource account belongs.</p> <ul style="list-style-type: none"> A managed resource account can belong to multiple account groups in the same department. Use a comma (,) to separate every two account groups. Only the account group that has been created in the CBH system can be entered.

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

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

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

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

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

Step 9 Click **OK**.

----End

Batch Creating Resource Accounts

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

Step 1 Log in to a CBH system.

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

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

 **NOTE**

Only hosts with the same protocol type are supported.

Step 4 Enter the account information to be added, as shown in [Table 7-10](#).

Table 7-10 Parameters for creating resource accounts in batches

Parameter	Description
Login Type	Select the login mode of the created accounts. <ul style="list-style-type: none"> • Auto Login • Manual Login • CSMS Credentials Login • Sudo Login
Account	Name of the account. You can specify one. If the login mode is set to automatic login, this parameter is mandatory.
Password	Password of the account.
SSH Key	This parameter is mandatory if the current account needs to log in to the system using an SSH key. The RSA private key in PEM or RFC4716 format is supported. After the RSA private key is entered, the SSH key is preferentially used for login.
passphrase	Password of the SSH key. You need to enter the SSH key first. If the SSH key is password-free, you do not need to set this parameter.
CSMS Credentials	This parameter is mandatory only when Login Mode is set to CSMS Credentials Login .
Description	Description of the current account. A maximum of 128 characters can be entered.

Parameter	Description
Options	<p>Select an option.</p> <ul style="list-style-type: none"> • Overwrite existing account: You can select this to overwrite the existing accounts that have the same usernames as that of accounts your are creating. • Verify Account: Check whether the added account can be used to log in to the system. This option can be selected only when the automatic login mode is used.

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

----End

7.5 Resource Management

7.5.1 Verifying Managed Resource Accounts

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

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

NOTE

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

Table 7-11 Resource account status description

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

Constraints

Accounts for application resources cannot be verified online.

Prerequisites

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

Automatic Inspection

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

Real-Time Verification

Step 1 Log in to the CBH system.

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

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

Step 4 Configure **Connect Timeout** and **Done notification**.

- The default **Connect Timeout** interval is **10** seconds. If the network condition is poor, increase the **Connection Timeout** interval.
- By default, no task completion notification is sent.
- To receive notifications, select **Email** or **SMS**. Additionally, you can view the verification results on the [Tasks](#) page.

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

----End

Batch Account Verification

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

Step 1 Log in to the CBH system.

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

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

Step 4 Configure **Connect Timeout** and **Done notification**.

- The default **Connect Timeout** interval is **10** seconds. If the network condition is poor, increase the **Connection Timeout** interval.
- By default, no task completion notification is sent.
- To receive notifications, select **Email** or **SMS**. Additionally, you can view the verification results on the [Tasks](#) page.

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

----End

7.5.2 Deleting Managed Resources from the CBH System

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

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

Prerequisites

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

Deleting One or More Managed Resource Accounts

Step 1 Log in to the CBH system.

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

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

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

----End

Deleting One or More Host Resources

Step 1 Log in to the CBH system.

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

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

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

----End

Deleting One or More Application Servers

Step 1 Log in to the CBH system.

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

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

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

----End

Deleting One or More Application Resources

- Step 1** Log in to the CBH system.
 - Step 2** Choose **Resource > Application > Application**.
 - Step 3** Locate the row where the application you want to delete resides and click **More > Delete** in the **Operation** column to delete the application resource.
 - Step 4** Select multiple application resources and click **Delete** at the bottom of the application list to delete all selected application resources together.
- End

7.5.3 Querying and Editing Managed Resource Configurations

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

Prerequisites

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

Querying and Editing Host Configurations

- Step 1** Log in to the CBH system.
- Step 2** Choose **Resource > Host** in the navigation pane on the left.
- Step 3** Query host resources.
 - Quick search
Enter a keyword in the search box to quickly query host resources by host name, host IP address, and port number.
 - Advanced search
Enter keywords in the corresponding attribute search boxes to search for host resources in exact mode.

Figure 7-1 Advanced search

The screenshot shows a search interface for Host resources. It includes several input fields and dropdown menus for filtering results. The fields are: Host Name, Host Addr, Port, OS Type, Account, Creator, and Modifier. There are also checkboxes for 'Accurate Search' and 'File Manage'. A 'Search' button is located at the bottom right of the form.

- Step 4** Click the name of the host resource you want to edit or click **Manage** in the row of the host in the **Operation** column.
- Step 5** View and edit basic information of the host resource.

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

- You can edit the **Host Name**, **Host Address**, **Port**, **OS Type**, **Department**, and **Remarks**.

- The **Protocol** cannot be modified.

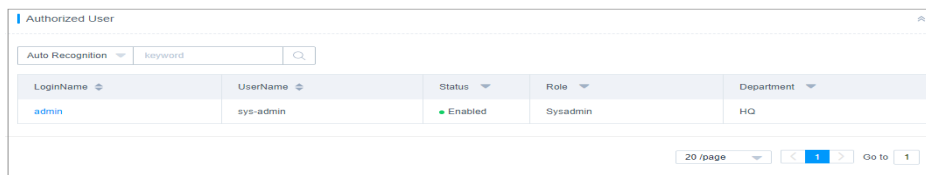
Step 6 View and edit accounts of the host resource.

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

Step 7 View authorized users of the host resource.

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

Figure 7-2 Viewing authorized users of a host resource



LoginName	UserName	Status	Role	Department
admin	sys-admin	Enabled	Sysadmin	HQ

----End

Batch Editing Host Resource Configurations

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

Step 1 Log in to the CBH system.

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

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

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

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

Step 5 Edit options for multiple hosts.

- **File Manage:** This option is supported only by SSH, RDP, and VNC hosts.
 - **Clipboard:** This option is supported only by SSH, RDP, and Telnet hosts.
 - **X11 forward:** This option is supported only by SSH hosts.
 - **Keyboard Audit:** Only RDP, VNC, and protocol hosts can be configured.
1. Click **Edit Option**.
 2. Select **File Manage, Uplink Clipboard, Downlink Clipboard, X11 forward, and/or Keyboard Audit**.
 3. Click **OK**.

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

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

Step 7 Edit OS type of multiple selected hosts.

1. Click **Edit OS Type**.
2. Select an OS type.
3. Click **OK**.

----End

Viewing and Editing Application Server Configurations

Step 1 Log in to the CBH system.

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

Step 3 Query application servers.

- Quick search
Enter a keyword in the search box and search for application servers by server name, server address, or application server account.
- Advanced search
Enter keywords in the corresponding attribute search boxes to search for application servers in exact mode.

Figure 7-3 Advanced search

The screenshot shows the 'Application Publish' interface with the 'AppServer' tab selected. It features several search filters: 'App Name' (text input), 'App Address' (text input), 'AppServer Name' (text input), 'uplink clipboard' (dropdown), 'downlink clipboard' (dropdown), and 'File Manage' (dropdown). Below these are 'Remarks' (text input), 'Account' (text input), 'Creator' (text input), and 'Modifier' (text input). A 'Back to simple search' link is on the left, and 'Reset' and 'Search' buttons are on the right.

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

Step 5 View and edit basic information.

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

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

----End

Batching Editing Application Server Configurations

Batching editing departments of multiple application servers

Step 1 Log in to the CBH system.

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

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

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

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

----End

Viewing and Editing Application Publish Configurations

Step 1 Log in to the CBH system.

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

Step 3 Query application resources.

- Quick search
Enter a keyword in the search box and search for application resources by name.
- Advanced search
Enter keywords in the corresponding attribute search boxes to search for application resources in exact mode.

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

Step 5 View and edit basic information.

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

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

Step 6 View and edit accounts of the application resource.

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

Step 7 View authorized users of the application resource.

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

Figure 7-4 Viewing authorized users of a host resource

Auto Recognition	keyword	LoginName	UserName	Status	Role	Department
		admin	sys-admin	Enabled	Sysadmin	HQ

----End

Batch Editing Configurations of Application Resources

- Batching editing departments of multiple application resources
- Batch editing options, including file management, clipboard, X11 forward, and keyboard audit functions, of multiple application resources

Step 1 Log in to the CBH system.

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

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

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

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

Step 5 Edit options for multiple hosts.

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

----End

Querying and Editing Account Configurations

Step 1 Log in to the CBH system.

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

Step 3 Query application resources.

- Quick search
Enter a keyword in the search box to quickly search for application resources by account, related resource, host address, and privileged account.
- Advanced search
Enter keywords in the corresponding attribute search boxes to search for accounts in exact mode.

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

Step 5 View and edit basic information of the account.

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

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

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

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

Step 7 View authorized users of the account.

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

Figure 7-5 Viewing authorized users of a host resource

LoginName	UserName	Status	Role	Department
admin	sys-admin	Enabled	Sysadmin	HQ

----End

7.5.4 Exporting Resource Information

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

- To enhance information security of resources, CBH allows you to encrypt resource information you export.
- The exported host resource file contains basic information, accounts, and plaintext passwords of managed hosts.
- The exported application server file contains basic information, path, account, and plaintext passwords of application servers.
- The exported application file contains basic information and account information, including plaintext passwords, of managed application resources.
- The exported account file contains basic account information, plaintext passwords, related resources, and related resource addresses.

Prerequisites

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

Batch Editing Host Information

Step 1 Log in to the CBH system.

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

Step 3 Select the hosts you want to export.

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

Step 4 Click **Export**.

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

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

----End

Batch Exporting Application Server Information

Step 1 Log in to the CBH system.

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

Step 3 Select the application servers you want.

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

Step 4 Click **Export**.

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

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

----End

Batch Exporting Application Resource Information

Step 1 Log in to the CBH system.

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

Step 3 Select the application resources you want.

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

Step 4 Click **Export**.

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

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

----End

Batch Exporting Accounts of Resources

Step 1 Log in to the CBH system.

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

Step 3 Select the accounts you want to export.

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

Step 4 Click **Export**.

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

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

----End

7.5.5 Adding a Resource Account to an Account Group

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

Constraints

- The administrator of a superior department can add an account in the superior department to an account group in a lower-level department.
- If you have permissions for the **Account Group** module, you can remove an account of superior department out of the account group. However, as a user in a low-level department, you have no permissions to add those removed accounts back to your current account group.
- An account can be added to multiple account groups.

Prerequisites

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

Adding an Account to an Account Group

Step 1 Log in to the CBH system.

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

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

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

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

----End

Adding Multiple Accounts to an Account Group

Step 1 Log in to the CBH system.

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

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

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

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

----End

7.6 Account Group

7.6.1 Overview

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

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

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

 **NOTE**

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

7.6.2 Creating an Account Group

This section describes how to create an account group.

Prerequisites

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

Procedure

- Step 1** Log in to the CBH system.
- Step 2** Choose **Resource > Account Group** in the navigation pane.
- Step 3** Click **New**. In the dialog box displayed, configure basic information about the group.

Table 7-12 Creating an Account Group

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

- Step 4** Click **OK**. You can then view the newly created account group in the account group list and add account to it. For more details, see [Adding Accounts to an Account Group](#).

----End

7.6.3 Deleting an Account Group

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

Prerequisites

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

Deleting an Account Group

- Step 1** Log in to the CBH system.
 - Step 2** Choose **Resource** > **Account Group** in the navigation pane.
 - Step 3** To delete a single account group, click **Delete** in the **Operation** column of the account group.
 - Step 4** To delete multiple account groups at a time, select the ones you want to delete and click **Delete** at the bottom of the account group list.
- End

7.6.4 Querying and Editing Account Group Information

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

Constraints

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

Prerequisites

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

Procedure

- Step 1** Log in to the CBH system.
- Step 2** Choose **Resource** > **Account Group** in the navigation pane.
- Step 3** Query an account group.
Enter a keyword in the search box and search for an account group by name.
- Step 4** Click the name of the account group you want to edit or click **Manage** in the row of the account group in the **Operation** column.
- Step 5** In the **Basic Info** area, view the detailed information about the account group.
Click **Edit** in the area to modify the name and remarks of the account group.
- Step 6** In the **Members** area, view information about all members in the account group.
 - Click **Add**. In the displayed dialog box, add or remove member of the account group.

- In the row of a specific member, click **Remove** in the **Operation** column to remove the account from the account group.

----End

7.7 Managing Resource Labels

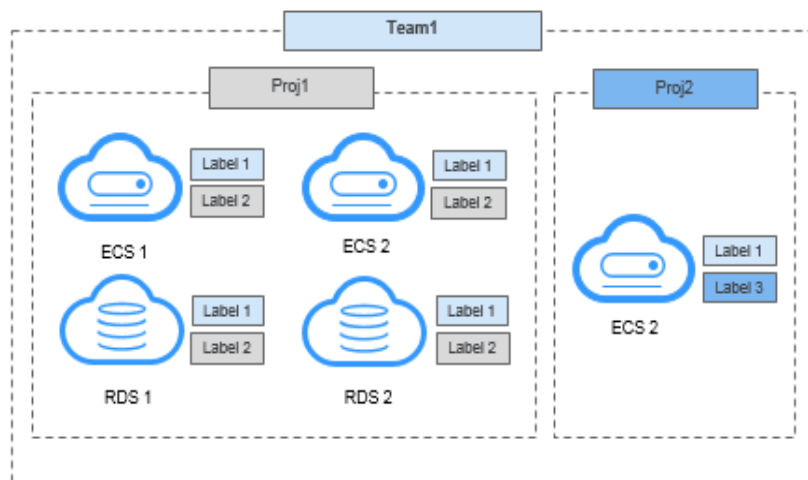
7.7.1 Overview

CBH labels are used to identify managed host and application resources in the CBH system and to identify all resources related to a managed host or application resource.

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

Figure 7-6 shows how labels work. Each managed resource, such as ECSs, is tagged with two labels. **Label 1** is identified by team, and **Label 2** and **Label 3** are identified by project. You can search for resources by label.

Figure 7-6 Examples of labels



After you add labels to resources, you can search for resources by label and manage labels in the CBH system. For more details, see **Table 7-13**.

Table 7-13 Label usage in CBH

Navigation Path	Operation
Dashboard > Recently Logged Host	Search for resources.
Dashboard > Recently Logged Application	Search for resources.

Navigation Path	Operation
Dashboard > My Hosts	Search for resources.
Dashboard > My APPs	Search for resources.
Resource > Host	Add, delete, or edit labels and search for resources by label.
Resource > Application	Add, delete, or edit labels and search for resources by label.
Operation > Host Operation.	Add or delete labels and search for resources by label.
Operation > App Operation	Add or delete labels and search for resources by label.

7.7.2 Creating a Resource Label

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

You can add labels to host or application resources when or after you add host or application resources. A host or application can have a maximum of 10 labels by default.

You can configure labels when you [add host resources](#) or [add application resources](#). This topic describes how to add labels after host and application resources are added to your CBH system. Labels can be added through the resource management or operation modules. As an example, the following content walks you through how to add labels to a host resource in the **Host** module.

Prerequisites

You have obtained the operation permissions for 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 host you want to add a label 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 Operation** page in the **Operation** module to view the new label of the managed host.

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

----End

7.7.3 Deleting a Resource Label

This topic describes how to delete a resource label.

Constraints

- After you confirm the deletion, all labels of the selected resource are deleted.
- If a label is not used by any resources, the system will delete it.

Prerequisites

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

Procedure

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

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

NOTE

Additionally, you can go to the resource list page and click **Manage** in the host or application row. On the displayed page, delete the label of a managed host or application resource.

----End

7.8 Customizing OS Types

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

CBH can manage 14 OS types by default.

Constraints

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

Customizing OS Types

Step 1 Log in to the CBH system.

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

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

Table 7-14 Parameters for creating an OS type

Parameter	Description
OS Type	Specifies the name of the custom OS type.
Chpw Param	Specifies the command of changing the account password and its return value. A maximum of 16 commands can be added. <ul style="list-style-type: none"> ● password indicates the old password. ● new_password indicates the new password. ● change_user indicates the account whose password needs to be changed. ● Brackets are not allowed.
Chpw Param for Sudo Login	Specifies the command of obtaining the permission for changing the account password and its success return. A maximum of 16 commands can be added. <ul style="list-style-type: none"> ● password indicates the old password. ● new_password indicates the new password. ● Brackets are not allowed.
Remarks	Provides brief introduction about the OS type.

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

Step 5 Manage customized OS types.

----End

Other Operations

Step 1 Log in to the CBH system.

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

Step 3 Delete a customized OS type.

- To delete an OS type, click **Delete** in the **Operation** column of the row where the OS type locates.
- To delete multiple OS types, select the ones you want to delete and click **Delete** at the bottom of the OS type list to delete them together.

Step 4 View and edit the customized OS type configurations.

1. Click the name of the OS type you want to edit or click **Manage** in the row of the OS type in the **Operation** column.

2. Click **Edit** in the **Basic Info** area to edit the basic information of the OS type.
- End

7.9 Creating a Proxy Server

You can create a proxy server and use it to manage, operate, and maintain servers.

Prerequisites

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

Procedure

- Step 1** Log in to the CBH system.
- Step 2** Choose **Resource > Host** in the navigation pane on the left.
- Step 3** Click the **Proxy Server** tab and then **New**. In the displayed dialog box, edit the proxy server information.

Table 7-15 Proxy server parameters

Parameter	Description
Server Name	Name of the proxy server. You can enter 1 to 128 characters.
Proxy Type	Select a proxy type. Currently, only SOCKS5 is supported.
Server Address	The private or public IP address of the server that is created as the proxy server. The IP address must be able to communicate with the CBH instance.
Port	Port for the proxy server to access. The default port for SOCKS5 is 1080. If a fixed port is set, enter the fixed port number.
Department	Select a department. If no department is available, create one.
Server Account	Username for the account for logging in to the proxy server.
Password	Password of the account for logging in to the proxy server.
Test connectivity	When creating a server, you can test its connectivity. You are advised to select this option. If this option is not selected, the connectivity of the proxy server cannot be ensured, so the server may fail to manage or maintain resources.

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

8 Policy

8.1 ACL Rules

8.1.1 Creating an ACL Rule and Associating It with Users and Resource Accounts

ACL Rules are used to control users' permissions for accessing resources.

With ACL rules, you can:

- Import rules in batches.
- Sort command rules by priority. The rule in the upper position has the higher priority than the ones in a lower position.
- Control access to managed resources from a wide range of dimensions, including the validity period, login period, user IP address, file transfer permission, file management permission, RDP clipboard function, keyboard audit, and operator watermark display function. ACL Rules are used to control users' permissions for resources.
 - Specify the validity period of the policy.
 - Restrict the time period during which the access is allowed or forbidden.
 - Restrict the users of certain source IP addresses to access managed resources.
 - Enable permissions for file transfer. This means you can enable or disable the function to upload files to managed resources or download files from managed resources.
 - Enable permissions for file management. This means you can enable or disable the function to view, delete, and edit files on the managed resources.
 - Grant permissions to use the RDP clipboard. This means you can enable or disable the RDP clipboard function.
 - Keyboard audit: You can enable this function to let CBH record all keyboard input information.

- Enable or disable watermarks on the web operation background. The watermark content is the login name of the current system user.

Constraints

- To grant the file upload/download permission, enable **File Transmission** and **File Manage**.
- Keyboard audit supports only RDP and VNC protocols.

Prerequisites

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

Procedure

Step 1 Log in to the CBH system.

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

Step 3 On the displayed page, click **New** in the upper right corner of the page.

NOTE

You can also select a rule and choose **More > Insert** to create an ACL rule. After the configuration is complete, a new rule is created.

Step 4 Configure the basic information.

Table 8-1 Basic information about an ACL rule

Parameter	Description
Rule Name	Name of a user-defined ACL rule. The rule name must be unique in the CBH system.
Period of validity	Effective time and expiration time of an ACL rule
File Transmission	Permissions to upload and download files during O&M. <ul style="list-style-type: none"> • If Upload and/or Download are selected, files can be uploaded and/or downloaded. • If Upload and Download are deselected, files cannot be uploaded or downloaded.
Options	Permissions to manage files or file folders, use clipboards on hosts using the RDP protocol, audit keyboard inputs, and display watermarks during O&M. <p>NOTE</p> <ul style="list-style-type: none"> • The file management function is available for managed hosts logged using SSH or RDP. • The file management function is unavailable for managed hosts using VNC. To manage files on such host resources, publish certain applications. • The file management function is unavailable for managed hosts using Telnet.

Parameter	Description
Logon Time Limit	Time period during which managed resources can or cannot be accessed.
IP Limit	<p>Source IP addresses by which users are allowed or forbidden to access resources.</p> <ul style="list-style-type: none"> • Select Blacklist and configure the IP addresses or IP address range to restrict users from these IP addresses from logging in to the resources. • Select Whitelist and configure the IP addresses or IP address range to allow users from these IP addresses to log in to the resources. • If no IP addresses are entered in the field, there is no login restriction on the managed host.

Step 5 Click **Next** and start to relate the command rule to one or more users or user groups.

- You can relate the ACL rule to multiple users or user groups at a time.
- After a user group is related to a command rule, users automatically obtain the permissions of the command rule the instant they are added to the user group.

Step 6 Click **Next** and start to relate the ACL rule to one or more accounts or account groups.

- You can relate an ACL rule to multiple managed resource accounts or account groups at a time.
- After an account group is related to an ACL rule, accounts automatically obtain the permissions of the ACL rule the instant they are added to the account group.

Step 7 Click **OK**. The system switches to the **ACL Rules** list, and you can then view the new ACL rule.

After you relate an ACL rule to users, the authorized users can view and access resources through the **Host Operations** and **App Operations** module.


 **NOTE**

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

----End

Importing ACL Rules in Batches

You can take the following steps to batch import ACL rules:

Step 1 Click  in the upper right corner to download the batch import template and enter the access control policy information.

Step 2 In the dialog box displayed, click **Upload** to upload the completed access control list.

To overwrite the existing rules, select **Overwrite the existing opsStrategy**.

 **NOTE**

Only XLS, XLSX, and CSV files can be uploaded.

Step 3 Click **OK**.

----**End**

Follow-up Operations

CBH gives you the ability to manage all ACL rules on the rule list page, including managing related users or resources, deleting, enabling, or disabling one or more ACL rules, and sorting ACL rules by priority.

- To quickly relate a command rule to more users, user groups, accounts, or account groups, select the rule and click **Relate** in the **Operation** column.
- To delete a command rule, select the rule and click **Delete** in the **Operation** column.
- To disable command rules, select the ones you want to disable and click **Disable** at the bottom of the list. When the status of those rules changes to **Disabled**, they become invalid.
- To change the priority of a command rule, select the rule and drag and drop it to an upper or lower position.
- To manage ACL rules offline, click **Export** to export the details about all ACL rules in CSV format.

8.1.2 Setting Two-person Authorization

Two-person authorization, also known as two-person approval, adds an additional layer of resource security during O&M. After two-person authorization is configured, O&M personnel can access core resources only after being authorized and authenticated by the administrator onsite. Even if the O&M personnel account is lost, the information of business-critical resources will not be disclosed, reducing O&M risks and ensuring the security of critical assets.

Constraints

Only department administrators of the current and superior departments, including the system administrator **admin**, can be selected as the approvers for two-person authorization.

Prerequisites

- You have the operation permissions for the **ACL Rules** module.
- The ACL rule has been related to the system user and managed accounts.

Procedure

- Step 1** Log in to the CBH system.
 - Step 2** Choose **Policy > ACL Rules** to enter the ACL rule list page.
 - Step 3** Select an ACL rule you want to enable two-person approval, choose **More > Approver** in the **Operation** column. The **Edit Approvers** dialog box is displayed.
 - Step 4** Select one or more department administrators and set them as approvers of two-person authorization.
 - Step 5** Click **OK**.
- End

Follow-up Operations

After two-person authorization is successfully configured, double authorization is required when the user related to this rule accesses the resource.

The user needs to select an approver and enter the account password of the approver. The user then can access the resource only after the verification is successful.

8.1.3 Querying and Editing an ACL Rule

CBH allows you to edit ACL rules to meet your changed O&M needs. For example, if your O&M personnel or resource permissions are changed, you can query involved ACL rules and edit their configurations, including basic permissions, related users, user groups, accounts, and account groups, and approvers of two-person authorization.

- A modified database rule takes effect the instant its status changes to **Enabled**.
- If related users have logged in to resources before the modification, those users need to log out and log in again for the modified database rule to take effect.

Prerequisites

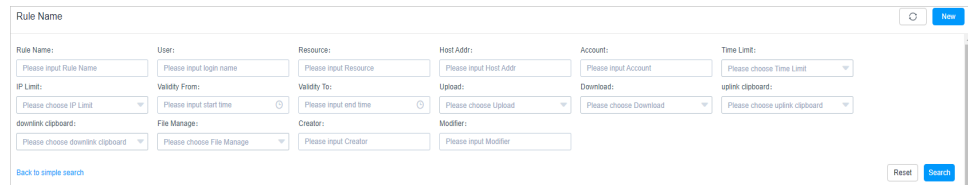
You have the operation permissions for the **ACL Rules** module.

Querying and Editing Database Rule Configurations

- Step 1** Log in to the CBH system.
- Step 2** Choose **Policy > ACL Rules** to enter the ACL rule list page.
- Step 3** Query ACL rules.
 - Quick search
Enter a keyword in the search box to quickly query ACL rules by rule name, user, resource name, host IP address, resource account, time limit, or IP address limit.
 - Advanced search

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

Figure 8-1 Advanced search



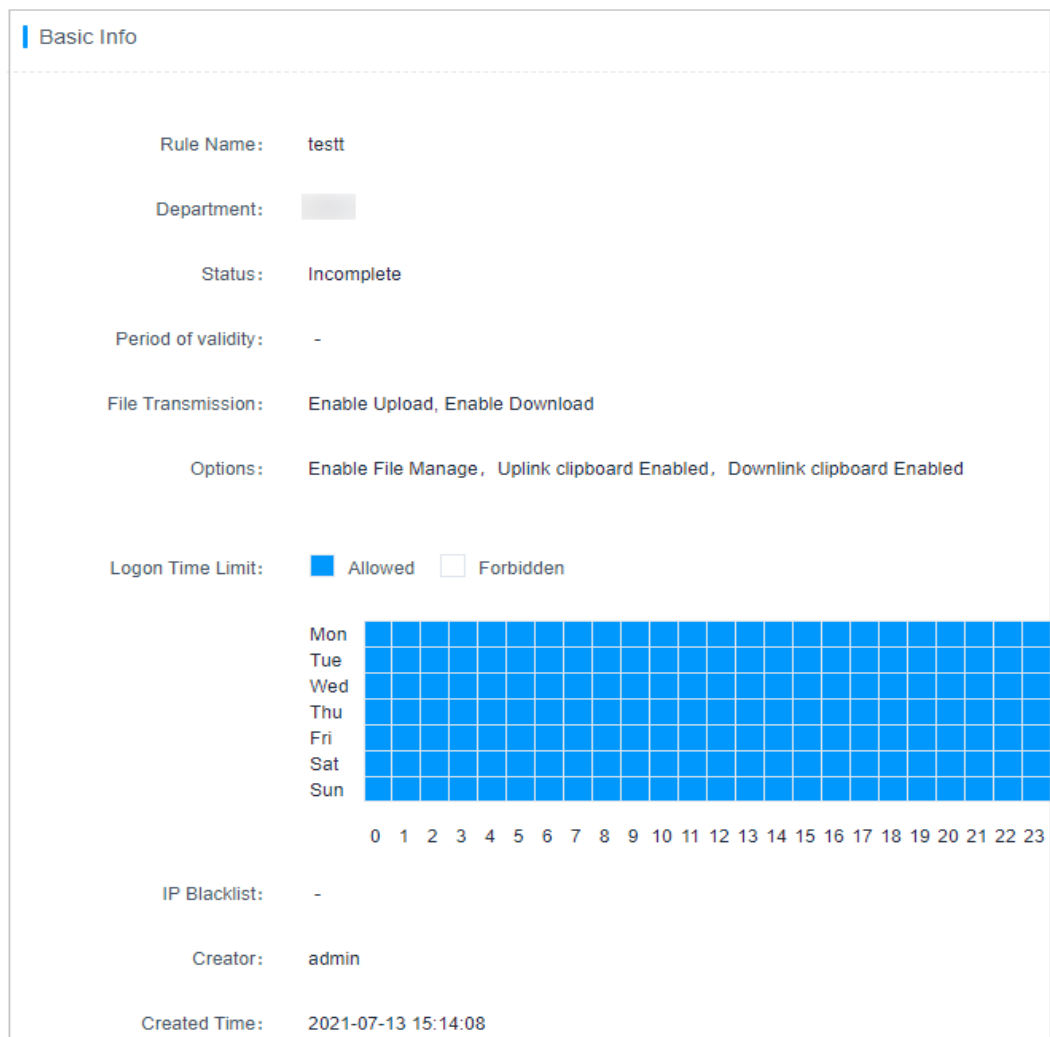
Step 4 Click the name of the database rule that you want to edit or click **Manage** in the row of the rule in the **Operation** column. The details page of the rule is displayed.

Step 5 View and edit basic information.

In the **Basic Info** area, click **Edit**. In the displayed dialog box, edit the database rule details.

You can modify configurations of **Rule Name**, **Period of validity**, **File Transmission**, **File Manage**, **Uplink clipboard**, **Downlink clipboard**, **Logon Time Limit**, **Keyboard Audit**, and **IP Limit**.

Figure 8-2 Viewing the basic information



Rule Name:	testt
Department:	
Status:	Incomplete
Period of validity:	-
File Transmission:	Enable Upload, Enable Download
Options:	Enable File Manage, Uplink clipboard Enabled, Downlink clipboard Enabled
Logon Time Limit:	<input checked="" type="checkbox"/> Allowed <input type="checkbox"/> Forbidden
Calendar:	Mon-Sun grid (all cells blue)
IP Blacklist:	-
Creator:	admin
Created Time:	2021-07-13 15:14:08

Step 6 View and edit users related to the rule.

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

Step 7 View and edit user groups related to the rule.

- To relate a user group to the rule or remove a related user group, click **Edit** in the **User Group** area and complete modifications in the displayed dialog box.
- To only remove a related user group, click **Remove** in the row of the related user group.

Step 8 View and edit accounts related to the database rule.

- To relate an account to the rule or remove a related account, click **Edit** in the **Account** area and complete modifications in the displayed dialog box.
- To only remove a related account, click **Remove** in the row of the related account.

Step 9 View and edit account groups related to the rule.

- To relate an account group to the rule or remove a related account group, click **Edit** in the **Account Group** area and complete modifications in the displayed dialog box.
- To only remove a related account group, click **Remove** in the row of the related account group.

Step 10 View and edit two-person authorization.

- To add or remove an approver, click **Edit** in the **Approver** area and complete modifications in the displayed dialog box.
- To only remove an approver, click **Remove** in the row of the approver.

----End

8.2 Command Rules

8.2.1 Creating a Command Rule

Command rules are used to control permissions for critical O&M operations on managed resources, implementing fine-grained control over the execution of commands on Linux hosts.

For hosts using SSH and Telnet protocols, CBH can record O&M session operations, trigger dynamic authorization, and disconnect connection to an O&M session. The working principles are that CBH uses the guacd proxy to audit and filter the commands executed during O&M based on the rule configured by the administrator. The proxy will return the audited commands, filtering results, and command output content for session operation recording, dynamic authorization, and disconnection.

With command rules, you can:

- Sort command rules by priority. The rule in the upper position has the higher priority than the ones in a lower position.

- Configure four command execution actions, including permitting, rejecting, requiring dynamic approval, and disconnecting the connection.
 - **Permit:** When a command rule is triggered, the system continues to execute the command. By default, all operations are allowed.
 - **Reject command:** After a command rule is triggered, the system rejects to execute the command and displays a message indicating that the command has been intercepted.
 - **Disconnect:** After a command rule is triggered, the system rejects to execute the command and disconnects the O&M session. The system displays a message indicating that the connection is forcibly disconnected by the administrator.
 - **Dynamic approval:** After a command rule is triggered, the system rejects to execute the command. The system displays a message indicating that the command has been intercepted and asking you to submit a command approval ticket. A command approval ticket is automatically generated. The command can be executed only after the ticket is submitted and approved.

Constraints

Command rules apply only to Linux hosts using the SSH or Telnet protocol for fine-grained permission control.

Prerequisites

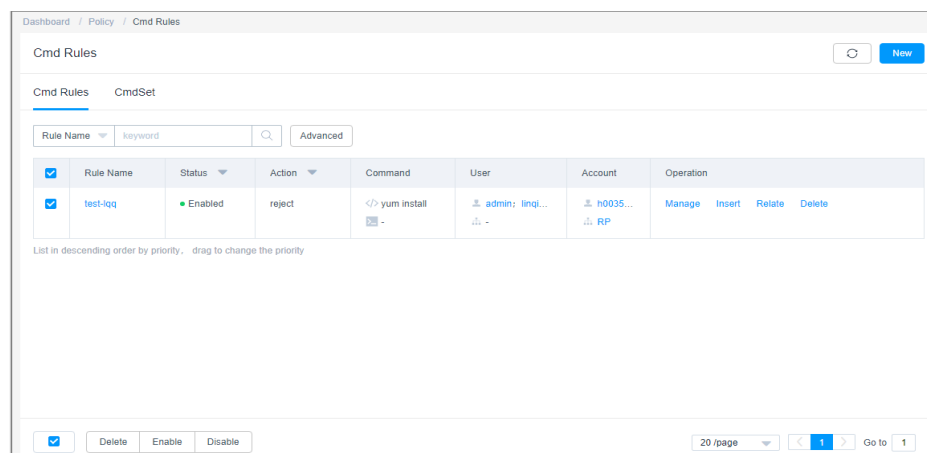
You have obtained the permissions to manage the **Cmd Rules** module.

Creating a Command Rule

Step 1 Log in to the CBH system.

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

Figure 8-3 Cmd Rules



Step 3 Click **New** in the upper right corner of the page to switch to the **New Command Rule** dialog box.

NOTE

You can also select a command rule and choose **More > Insert** to create a command rule. After the configuration is complete, a new rule is created.

Step 4 Configure the basic information.

Figure 8-4 New Command Rule

The screenshot shows a 'New Command Rule' dialog box with the following fields and options:

- Rule Name:** A text input field with a note: "1-64 length of chars, including letters, digit, or '-'".
- Action:** A dropdown menu currently showing "Choose action".
- Period of validity:** Two dropdown menus, one for "Permit" and one for "Forbid".
- Time Limit:** Two radio buttons, "Permit" (selected) and "Forbid".
- Calendar Grid:** A grid showing days of the week (Mon-Sun) and hours (0-23). The "Permit" radio button is selected, and the grid is filled with blue, indicating the rule is active for all days and hours.
- Buttons:** "Cancel" and "Next" buttons at the bottom right.

Table 8-2 Basic information parameters

Parameter	Description
Rule Name	Name of a command rule. The rule name must be unique in the CBH system.
Action	<p>Action executed by the command rule.</p> <p>The options are Disconnect, Reject command, Dynamic approval, and Permit.</p> <ul style="list-style-type: none"> • Disconnect: When a session runs the command to bring the rule into effect, the session is disconnected. • Reject command: When a session runs the command to bring the rule into effect, the command is rejected directly. • Dynamic approval: When a session runs the command to bring the rule into effect, the command is rejected directly. The command must be submitted to the administrator for approval to be executed. • Permit: When a session runs the command to bring the rule into effect, the system runs the command.
Period of validity	Effective time and expiration time of the rule
Time Limit	Validity period of a rule

Step 5 Click **Next** and start to relate the command rule to one or more commands or command sets.

- **Relate Command:** Enter one command in each line. You can enter multiple commands. For more details, see [User-defined Commands That Can be Related to a Command Rule](#).
- **Relate Command Set:** Relate the command rule to a created command set. For details about command sets, see [Managing Command Sets](#).

Step 6 Click **Next** and start to relate the command rule to one or more users or user groups.

- After a user group is related to a command rule, users automatically obtain the permissions of the command rule the instant they are added to the user group.

Step 7 Select a created account or account group.

- After a command rule is related to an account group, accounts automatically obtain the permissions of the rule the instant they are added to the account group.

Step 8 Click **OK**. You can then view the created command rule in the rule list.

During O&M, when a command rule is triggered, the system executes configured actions accordingly.

 **NOTE**

Users in the **Relate User** and **Relate User Group** must have been assigned a role that has ticket approval permissions. Otherwise, users cannot view the command approval ticket module or submit a ticket to obtain required permissions.

----End

Follow-up Operations

CBH gives you the ability to manage all command rules on the rule list page, including managing related users or resources, deleting, enabling, or disabling one or more command rules, and sorting command rules by priority.

- To quickly relate a command rule to more users, user groups, accounts, or account groups, select the rule and click **Relate** in the **Operation** column.
- To delete a command rule, select the rule and click **Delete** in the **Operation** column.
- To disable command rules, select the ones you want to disable and click **Disable** at the bottom of the list. When the status of those rules changes to **Disabled**, they become invalid.
- To change the priority of a command rule, select the rule and drag and drop it to an upper or lower position.

8.2.2 Querying and Editing a Command Rule

This topic describes how to view and edit a command rule. You can view and edit the rule configurations, including the basic settings, related passwords, and related

command sets. You can also edit the users, user groups, accounts, account groups related to the rule.

- A modified database rule takes effect the instant its status changes to **Enabled**.
- If related users have logged in to resources before the modification, those users need to log out and log in again for the modified database rule to take effect.

Prerequisites

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

Querying and Editing Database Rule Configurations

Step 1 Log in to the CBH system.

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

Step 3 Query command rules.

- Quick search
Enter a keyword in the search box to quickly query command rules by rule name, user, resource name, host IP address, resource account, command set, command, or parameter.
- Advanced search
Enter keywords in the corresponding attribute search boxes to search for database rules in exact mode.

Step 4 Click the name of the database rule that you want to edit or click **Manage** in the row of the rule in the **Operation** column. The details page of the rule is displayed.

Step 5 View and edit basic information.

In the **Basic Info** area, click **Edit**. In the displayed dialog box, edit the database rule details.

You can edit **Rule Name**, **Period of validity**, **Action**, and **Time Limit**.

Step 6 View and edit commands related to the rule.

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

Step 7 View and edit command sets related to the command rule.

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

Step 8 View and edit users related to the rule.

- To relate a user to the rule or remove a related user, click **Edit** in the **Users** area and complete modifications in the displayed dialog box.

- To only remove a related user, click **Remove** in the row of the related user.

Step 9 View and edit user groups related to the rule.

- To relate a user group to the rule or remove a related user group, click **Edit** in the **User Group** area and complete modifications in the displayed dialog box.
- To only remove a related user group, click **Remove** in the row of the related user group.

Step 10 View and edit accounts related to the database rule.

- To relate an account to the rule or remove a related account, click **Edit** in the **Account** area and complete modifications in the displayed dialog box.
- To only remove a related account, click **Remove** in the row of the related account.

Step 11 View and edit account groups related to the rule.

- To relate an account group to the rule or remove a related account group, click **Edit** in the **Account Group** area and complete modifications in the displayed dialog box.
- To only remove a related account group, click **Remove** in the row of the related account group.

----End

8.2.3 Managing Command Sets

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

This topic walks you through how to create, view, modify, delete, and batch import command sets.

Prerequisites

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

Creating a Command Set

Step 1 Log in to the CBH system.

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

Step 3 Create a command set.

1. Click **New** in the upper right corner of the page to switch to the **New Command Set** dialog box.
2. Configure the command set name.
The command set name must be unique in the CBH system.
3. Click **OK**. You can then view the new command set on the **CmdSet** tab.

Step 4 Add commands to the command set.

1. In the row of the command set you want to add commands, click **Command** in the **Operation** column. The **Command** dialog box is displayed.

2. Select command sets or a single command.
Currently, common commands for **Linux** and **Network devices** are preset in the CBH system.
3. Click **OK**.

----End

Querying and Editing a Command Set

Step 1 Log in to the CBH system.

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

Step 3 Query a command set.

Quick search: Enter a keyword in the search box to quickly query command sets by command set name, command, and/or parameter.

Step 4 Click the command set name or click **Manage** in the row of the command set in the **Operation** column.

Step 5 View and edit basic information.

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

You can edit **CommandSet Name**. The **Department** cannot be changed.

Step 6 View and edit commands and parameters in the **Command** area.

- To add preset commands or parameters, click **Add** in the **Command** area and select preset commands in the displayed dialog box.
- To delete a command or parameter, locate the row containing the command or parameter you want to delete and click **Remove**.

----End

Deleting a Command Set

Step 1 Log in to the CBH system.

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

Step 3 To delete one command set, click **Delete** in the **Operation** column of the row where the command set locates.


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

----End

Batch Importing Command Sets

Step 1 Log in to a CBH system.

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

Step 3 Click  in the upper right corner. In the displayed dialog box, download the template.

Step 4 Complete the template. Click **Upload** to import the entered command sets to CBH.

You can choose to overwrite existing command sets.

 **NOTE**

Only XLS, XLSX, and CSV files can be uploaded.

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

----End

8.2.4 Defining Custom Related Commands

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

Custom related commands are case-sensitive. If the command to execute is inconsistent with the configured one, the command rule will fail to be triggered. The following examples are for your reference:

- **Single command format**
If you want to configure a rule to deny the **ls** command, set the related command of the rule to **ls**. The rule is triggered when the single command **ls** is executed.
- **Single command and path format**
If you want to configure a rule to dynamically authorize the log query actions, set the related command of the rule to **ls /var/log/**. The rule is triggered when the command **ls /var/log/** is executed. If the **ls /var/log** command is executed, the rule fails to be triggered.
- **Commands that contain the wildcard character (*), which indicates one or more characters.**
If you want to configure a rule to deny all deletion commands, set the related command of the rule to **rm ***. The rule is triggered when the command **rm -rf** is executed; while the rule will fail to be triggered if the **rm** command is executed.
- **Commands that contain the question mark (?), which indicates any single character. The number of entered question marks indicates the number of unknown characters.**
If you want to configure a rule to deny commands that will delete files or file directories containing two certain characters, set the related command to **rm -rf ??**. The rule is triggered when the command **rm -rf ts** is executed. The rule will fail to be triggered if the **rm -rf test** command is executed.
- **Commands that contain a string or any characters enclosed in square brackets ([]) or negated ones in square brackets (using a vertical bar (|) or caret (^) to negate)**
If you want to configure a rule to dynamically approve commands that will delete files or file directories containing any characters in the string "abcd",

set the related command of the rule to **rm -rf [abcd]**. The rule is triggered when the command **rm -rf cloud** is executed. The rule will fail to be triggered if the **rm -rf test** or **rm -rf ABCD** command is executed.

8.3 Database Rules

8.3.1 Creating a Database Rule

Database rules are used to intercept sensitive database session operations, implementing fine-grained control over database operations. When an authorized system user logs in to a database related to a database rule, their sensitive operations will be intercepted once the database rule is triggered.

With database rules, you can:

- Sort command rules by priority. The rule in the upper position has the higher priority than the ones in a lower position.
- Configure four command execution actions, including permitting, rejecting, requiring dynamic approval, and disconnecting the connection.
 - Permit: By default, all operations are allowed. After a database rule is triggered, operations in the related regulation set are allowed.
 - Reject: After a database rule is triggered, the system rejects to execute the operation and displays a message indicating that the operation has been intercepted.
 - Disconnect: After a database rule is triggered, the system rejects to execute the operation and disconnects the O&M session. The system displays a message indicating that the connection is forcibly disconnected by the administrator.
 - Dynamic approval: After a database rule is triggered, the system rejects to execute the operation. The system displays a message indicating that the operation has been intercepted and asking you to submit a database approval ticket. A database approval ticket is automatically generated. The command can be executed only after the ticket is submitted and approved.

Constraints

- The database operation audit is available only in the CBH professional editions.
- Database rules apply only to MySQL, Oracle, PostgreSQL, and GaussDB databases for fine-grained permission control.

Prerequisites

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

Creating a Database Rule

Step 1 Log in to the CBH system.

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

Step 3 In the upper right corner of the page, click **New**.

 **NOTE**

You can also select a database rule and choose **More > Insert** to create a database rule. After the configuration is complete, a new rule is created.

Step 4 Configure the basic information.

Table 8-3 Basic information parameters

Parameter	Description
Rule Name	Name of the database rule. The rule name must be unique in the CBH system.
Action	Action executed by the rule. The options are Disconnect , Reject command , Dynamic approval , and Permit . <ul style="list-style-type: none"> ● Disconnect: When a database rule is triggered, the system automatically disconnects the session. ● Reject command: When a database rule is triggered, the system directly rejects the command. ● Dynamic approval: When a database rule is triggered, the system directly rejects the command and requires an approval from the administrator. To continue the execution of the command, the system user needs to submit a ticket to the administrator for approval. ● Permit: When a database rule is triggered, the system allows the database operation commands to be executed.
Period of validity	Effective time and expiration time of the rule
Time Limit	Validity period of a rule

Step 5 Click **Next** and start to relate the command rule to a rule set.

Select a rule set. For details about command sets, see [Managing Database Rule Sets](#).

Step 6 Click **Next** and start to relate the database rule to one or more users or user groups.

After a user group is related to a command rule, users automatically obtain the permissions of the command rule the instant they are added to the user group.

Step 7 Click **Next** and start to relate the database rule to one or more accounts or account groups.

After a database rule is related to an account group, accounts automatically obtain the permissions of the database rule the instant they are added to the account group.

Step 8 Click **OK**. You can then view the created rule in the rule list.

During O&M, when a command rule is triggered, the system executes configured actions accordingly.

 **NOTE**

Users in the **Relate User** and **Relate User Group** panes must have a role that has database ticket approval permissions assigned to them. Otherwise, users cannot view the database approval ticket module or submit a ticket to obtain required permissions.

----**End**

Follow-up Operations

CBH gives you the ability to manage all database rules on the rule list page, including managing related users or resources, deleting, enabling, or disabling one or more command rules, and sorting command rules by priority.

- To quickly relate a command rule to more users, user groups, accounts, or account groups, select the rule and click **Relate** in the **Operation** column.
- To delete a command rule, select the rule and click **Delete** in the **Operation** column.
- To disable command rules, select the ones you want to disable and click **Disable** at the bottom of the list. When the status of those rules changes to **Disabled**, they become invalid.
- To change the priority of a command rule, select the rule and drag and drop it to an upper or lower position.

8.3.2 Querying and Editing a Database Rule

This topic describes how to view and edit a database rule. You can view and edit rule configurations, including basic settings, related regulation sets, users, user groups, accounts, and account groups.

- A modified database rule takes effect the instant its status changes to **Enabled**.
- If related users have logged in to resources before the modification, those users need to log out and log in again for the modified database rule to take effect.

Prerequisites

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

Querying and Editing Database Rule Configurations

Step 1 Log in to the CBH system.

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

Step 3 Query database rules.

- Quick search

Enter a keyword in the search box to quickly query database rules by rule name, user, resource name, host IP address, resource account, and regulation set name.

- Advanced search

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

Step 4 Click the name of the database rule that you want to edit or click **Manage** in the row of the rule in the **Operation** column. The details page of the rule is displayed.

Step 5 View and edit basic information.

In the **Basic Info** area, click **Edit**. In the displayed dialog box, edit the database rule details.

You can edit **Rule Name**, **Period of validity**, **Action**, and **Time Limit**.

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

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

Step 7 View and edit users related to the rule.

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

Step 8 View and edit user groups related to the rule.

- To relate a user group to the rule or remove a related user group, click **Edit** in the **User Group** area and complete modifications in the displayed dialog box.
- To only remove a related user group, click **Remove** in the row of the related user group.

Step 9 View and edit accounts related to the database rule.

- To relate an account to the rule or remove a related account, click **Edit** in the **Account** area and complete modifications in the displayed dialog box.
- To only remove a related account, click **Remove** in the row of the related account.

Step 10 View and edit account groups related to the rule.

- To relate an account group to the rule or remove a related account group, click **Edit** in the **Account Group** area and complete modifications in the displayed dialog box.
- To only remove a related account group, click **Remove** in the row of the related account group.

----End

8.3.3 Managing Regulation Sets

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

CBH has 29 common database operation commands preset, including **ALTER, TRUNCATE, EXECUTE, INSERT, DELETE, UPDATE, SELECT, GRANT, REVOKE, HANDLER, DEALLOCATE, SET, COMMIT, ROLLBACK, PREPARE, CREATEINDEX, DROPINDEX, CREATEFUNCTION, DROPFUNCTION, CREATEVIEW, DROPVIEW, CREATEDATABASE, DROPDATABASE, CREATEPROCEDURE, DROPPROCEDURE, DROPPROCEDURE, CREATETABLE, DROPTABLE, CALL, and ACCESS.**

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

Prerequisites

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

Creating a Regulation Set

Step 1 Log in to the CBH system.

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

Step 3 Create a regulation set.

1. In the upper right corner of the page, click **New**.
2. Configure the **RegSet name** and specify a protocol.
 - The **RegSet Name** must be unique in the CBH system.
 - Currently, only MySQL, Oracle, PostgreSQL, and GaussDB are supported. The protocol type cannot be changed after being selected.
3. Click **OK**. You can then view new regulation set on the list page.

Step 4 Add database rules.

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

Table 8-4 Parameters for adding regulation

Parameter	Description
Lib	This parameter is optional. It can be set to a regular expression to match the library name. By default, all SQL statements that use this command are intercepted.
Table	This parameter is optional. It can be set to a regular expression to match the table name. By default, all SQL statements that use this command are intercepted.
Cmd	This parameter is mandatory. Select at least one preset command. Currently, 29 commands are available. You can select multiple commands.

3. Click **OK**.

----End

Querying and Editing a Regulation Set

Step 1 Log in to the CBH system.

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

Step 3 Query the regulation sets.

Quick search: Enter a keyword in the search box and search for regulation sets by regulation set name.

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

Step 5 View and edit basic information.

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

You can edit **RegSet name**. The **Protocol** and **Department** cannot be changed.

Step 6 Query and edit a regulation set in the **Regulation** area.

- To add a library, table, or command to a regulation set, click **Add** and then complete modifications in the displayed dialog box.
- To delete a regulation set, locate the row and click **Remove**.

----End

Deleting a Regulation Set

Step 1 Log in to the CBH system.

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

Step 3 To delete one regulation set, click **Delete** in the **Operation** column of the row where the regulation set locates to delete it.

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

----End

8.4 Password Rules

8.4.1 Creating a Password Rule

With password rules, you can let the CBH system periodically change the passwords of multiple managed host resources at a time, improving the managed resource account security.

With password rules, you can:

- Change passwords of managed resource accounts manually, periodically, or at a scheduled time.
- Change the passwords of multiple managed resource accounts to different passwords randomly generated by the system, the same password generated by the system, or the same password you specify.

Constraints

- Password change rules apply only to hosts configured with SSH, MySQL, SQL Server, Oracle, RDP, or Telnet protocols.
- To enable a password change rule for Windows hosts, enable the SMB service and open port 445 in the security group.
- Before relating to an account of a Windows 10 resource, set server parameters by referring to [Setting Parameters of Windows 10 Servers](#).

Prerequisites

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

Creating a Password Change Rule

Step 1 Log in to the CBH system.

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

Step 3 Click **New** in the upper right corner of the page to switch to the **New ChangePassword Rule** dialog box.

Step 4 Configure the basic information.

Table 8-5 Parameter for password change rules

Parameter	Description
Rule Name	Name of a password change rule. The rule name must be unique in the CBH system.
Timing	The options are Manual , Fixed-Time , and Cycle . <ul style="list-style-type: none"> • Manual: Manually trigger the password change rule to change the password of the managed resource account. • Fixed-Time: The password change rule is triggered by the CBH system to change the password of the managed resource account at a fixed time. This type of rule is executed only once. • Cycle: The password change rule is periodically triggered by the CBH system to change the passwords of the managed resource accounts. This type of password change rule is triggered periodically.
Execute Time	Date when the password change rule is executed. The default execution time is at 00:00 every day.

Parameter	Description
Cycle Frequency	<p>Password change interval.</p> <ul style="list-style-type: none"> The unit is day. You need to set the End Time for this type of rules. Otherwise, the rule will be executed indefinitely.
Method	<p>How the password is changed. The options are Generate different passwords, Generate the same password, and Specify the same password.</p> <ul style="list-style-type: none"> Generating a different password: The system randomly generates different passwords for managed resource accounts in compliance with password requirements. Generating the same password: Randomly generate the same password for managed resource accounts in compliance with password requirements. Specifying the same password: You manually change passwords of managed resource accounts to the same preset password you specify. <p>NOTE A password randomly generated by CBH contains 20 characters, including uppercase letters, lowercase letters, digits, and the following special characters %, -, _, and?. A random password must contain at least an uppercase letter, a lowercase letter, and a special character.</p>
Options	<p>The following options are supported:</p> <ul style="list-style-type: none"> Allow to change the sudo account password: To change the password of sudo account, select this option, or the password of the sudo account cannot be changed. This option is not selected by default. Priority use of the sudo account to change password: To let the system automatically search for the corresponding sudo account and use it to change the account password, select this option. If no sudo account is available, the password can be changed using the current account. This option is selected by default.

- Step 5** Click **Next** and start to relate the ACL rule to one or more accounts or account groups.
- After a password change rule is related to an account group, accounts automatically obtain the permissions of the rule the instant they are added to the account group.
 - If a password change rule is related to multiple managed resource accounts, batch changing passwords is available.

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

To obtain the new password of the managed resource accounts, export host resource details by referring to [Batch Editing Host Information](#).

----End

Setting Parameters of Windows 10 Servers

Step 1 Log in to a Windows 10 server.

Step 2 Start the Windows Remote Management (WinRM) service.

1. Search for **Windows Components**.
2. In the navigation pane on the left, choose the local service. In the window displayed on the right, locate **Windows Remote Management(WS-Management)**.
3. Right-click **Windows Remote Management(WS-Management)** and choose **Start** from the shortcut menu.

Step 3 Configure WinRM.

1. Run the **cmd** command as the administrator and run the following command:

```
winrm qc
```
2. Perform twice. After the command output is displayed, enter **y** as prompted.
3. Run the following commands:

```
winrm set winrm/config/service '@{AllowUnencrypted="true"}'
```
4. Run the following commands:

```
winrm set winrm/config/service/auth '@{Basic="true"}'
```

Step 4 (Skip this step if you are already an administrator.) Run the following command to add a user to the user group:

For example, run the following command to add **appuser01** to the user group:

```
net localgroup "Remote Management Users" appuser01 /add
```

Step 5 In the power shell dialog box, run the following command to add a firewall:

```
New-NetFirewallRule -DisplayName "WinRM-5985" -Direction Inbound -LocalPort 5985 -Protocol TCP -Action Allow
```

----End

Follow-up Operations

CBH gives you the ability to manage all password change rules on the rule list page, including managing related resources, deleting, enabling, or disabling one or more password change rules, and immediate execution of a password change rule.

- To quickly relate a synchronization rule to more accounts or account groups, select the rule and click **Relate** in the **Operation** column.
- To delete a command rule, select the rule and click **Delete** in the **Operation** column.
- To disable password change rules, select the ones you want to disable and click **Disable** at the bottom of the list. When the status of those rules changes to **Disabled**, they become invalid.
- To change the password of a managed account immediately, click **Execute** in the **Operation** column.

8.4.2 Querying and Editing a Password Rule

You can edit password rules to meet your changed O&M requirements. For example, you can edit when and how a password rule is executed and which accounts, account groups, and resources a password rule is used for.

A modified database rule takes effect the instant its status changes to **Enabled**.

Prerequisites

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

Querying and Editing Rule Configurations

Step 1 Log in to the CBH system.

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

Step 3 Query password rules.

- Quick search

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

- Advanced search

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

Step 4 Click the name of the rule that you want to edit or click **Manage** in the row of the rule in the **Operation** column. The details page of the rule is displayed.

Step 5 View and edit basic information.

In the **Basic Info** area, click **Edit**. In the displayed dialog box, edit the database rule details.

- You can edit **Rule Name, Timing, Method, and Options**.
- The **Department** cannot be modified.

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

- To relate an account to the rule or remove a related account, click **Edit** in the **Account** area and complete modifications in the displayed dialog box.
- To only remove a related account, click **Remove** in the row of the related account. The rule becomes invalid for the deleted account.

Step 7 View and edit account groups related to the rule.

- To relate an account group to the rule or remove a related account group, click **Edit** in the **Account Group** area and complete modifications in the displayed dialog box.
- To only remove a related account group, click **Remove** in the row of the related account group. The rule becomes invalid for all accounts in the deleted account group.

----End

8.4.3 Managing Password Logs

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

Prerequisites

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

Viewing Log Details

Step 1 Log in to the CBH system.

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

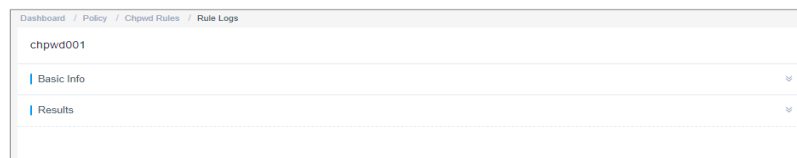
Step 3 Query password change logs.

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

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

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

Figure 8-5 Viewing password log details



----End

Downloading Password Logs

Step 1 Log in to the CBH system.

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

Step 3 Click **Download**.

Step 4 Confirm downloading information.

1. **Set encryption password:** This parameter is optional. If this parameter is not set, the downloaded password change log is an unencrypted CSV file. If you set a password, the downloaded password change log is an encrypted .zip file.
2. **User Password:** This parameter is mandatory. You need to enter the login password of the current user and then the password change log can be downloaded only after the verification is successful. This ensures password security of managed host accounts.
3. Click **OK** to download the file locally.

----End

Deleting Execution Logs

- Step 1** Log in to the CBH system.
 - Step 2** Choose **Policy > Password Rules > Password Log**.
 - Step 3** To delete one execution log, select the one you want and click **Delete** in the **Operation** column to delete it.
 - Step 4** To delete multiple execution logs at a time, select the ones you want and click **Delete** at the bottom of the list to delete all selected logs together.
- End

8.5 Account Synchronization Rules

8.5.1 Creating a Synchronization Rule

Synchronization rules are used to automatically synchronize managed host accounts, making it easier for you to manage accounts of managed hosts, delete zombie accounts, and discover accounts that are not managed in a timely manner. This further strengthens management of resources.

With synchronization rules, you can:

- Synchronize accounts from managed hosts manually, periodically, or at a scheduled time.
- Pull accounts from managed hosts, check the validity of pulled accounts, and update the managed resource account status.
- Update the password of a host account, create a host account, or delete invalid host accounts by pushing managed resource account information to the corresponding hosts.

Constraints

- The account synchronization is available only in CBH professional editions.
- Account synchronization rules apply only to hosts using the SSH protocol.
- Only one managed resource account is allowed to log in to a managed host and pull its account information.

Prerequisites

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

Creating a Synchronization Rule

- Step 1** Log in to the CBH system.
- Step 2** Choose **Policy > Sync Rules > Sync Rules**.
- Step 3** Click **New** in the upper right corner of the **Sync Rule** area to switch to the **New rule** dialog box.

Figure 8-6 New rule

New rule

×

* Rule Name
1-64 length of chars, including letter, digit or "-"

* Timing

Action

Pull Account
Scan all accounts of target hosts and find out all normal and abnormal account.

Push Account
Sync the accounts to the target host, update the password, or create a new account, or delete the illegal account.

Allow update of the account password if inconsistent

Allow creation of the account if not exist on remote host

Allow deletion of the account if not registered in system

* Connect Timeout
Connect timeout, default 10 second

Step 4 Configure the basic information.

Table 8-6 Parameters for configuring an account synchronization rule

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

Parameter	Description
Timing	<p>The options are Manual, Fixed-Time, and Cycle. You need to configure the execution time if Fixed-Time or Cycle is selected.</p> <ul style="list-style-type: none"> • Manual: Manually trigger the rule to change the password of the managed resource accounts. • Fixed-Time: The rule is triggered by the CBH system to change the password of the managed resource account at a fixed time. This type of rule is executed only once. • Cycle: The rule is periodically triggered by the CBH system to change the password of the managed resource account. This type of rule is triggered periodically.
Execute Time	Date when a policy is periodically executed. The default execution time is at 00:00 every day.
Cycle Frequency	<p>Account synchronization frequency.</p> <ul style="list-style-type: none"> • The options are every minute, every hour, every day, every week, and every month. • You need to set the End Time for this type of synchronization rules. Otherwise, the rule will be executed indefinitely.
Action	<p>Synchronization mode. By default, Pull Account is selected.</p> <ul style="list-style-type: none"> • Pull Account: Scans all accounts of a host and collects statistics on all normal and abnormal accounts. • Push Account: Pushes accounts to a host to automatically update account passwords, create accounts, or delete invalid accounts of the host. <p>NOTE When the synchronization mode is set to push account, the following three options are available:</p> <ul style="list-style-type: none"> - If the account and password are inconsistent, the password can be updated. - If the account does not exist, the account can be created. - If a non-managed account exists on the host, the account can be deleted.
Connect Timeout	<p>Timeout interval for connecting to a managed host. If the connection times out, the account synchronization task is interrupted.</p> <ul style="list-style-type: none"> • The default value is 10 seconds.

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

- Only one account can be configured for each host to execute synchronization tasks.

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

To obtain the account synchronization details, [download the synchronization logs](#) after the synchronization.

----End

Follow-up Operations

You can manage all synchronization rules on the rule list page, including managing related resources, deleting, enabling, or disabling one or more synchronization rules, and immediately executing a synchronization rule.

- To quickly relate a synchronization rule to more accounts or account groups, select the rule and click **Relate** in the **Operation** column.
- To delete a command rule, select the rule and click **Delete** in the **Operation** column.
- To disable synchronization rules, select the ones you want to disable and click **Disable** at the bottom of the list. When the status of those rules changes to **Disabled**, they become invalid.
- To execute a synchronization rule immediately, click **Execute** in the **Operation** column.

8.5.2 Querying and Editing a Synchronization Rule

You can edit a synchronization rule to meet your changed requirements. For example, you can edit when and how a synchronization rule is executed and which accounts, account groups, and resources a synchronization rule is used for.

A modified rule takes effect the instant its status changes to **Enabled**.

Prerequisites

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

Querying and Editing Rule Configurations

Step 1 Log in to the CBH system.

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

Step 3 Query account synchronization rules.

- Quick search
Enter a keyword in the search box to quickly query rules by rule name, resource name, and account,
- Advanced search
Enter keywords in the corresponding attribute search boxes to search for rules in exact mode.

Step 4 Click the name of the rule that you want to edit or click **Manage** in the row of the rule in the **Operation** column. The details page of the rule is displayed.

Step 5 View and edit basic information.

In the **Basic Info** area, click **Edit**. In the displayed dialog box, edit the rule details.

- You can edit **Rule Name**, **Timing**, and **Action**.
- The **Department** cannot be modified.

Step 6 View and edit accounts related to the rule.

- To relate an account to the rule or remove a related account, click **Edit** in the **Execute Account** area and complete modifications in the displayed dialog box.
- To only remove a related account, click **Remove** in the row of the related account. The removed account then cannot be used for synchronizing accounts of the corresponding host.

Step 7 View and edit account groups related to the rule.

- To relate an account group to the rule or remove a related account group, click **Edit** in the **Account Group** area and complete modifications in the displayed dialog box.
- To only remove a related account group, click **Remove** in the row of the related account group. Each account in the removed account group cannot be used for synchronizing accounts of the corresponding host.

----End

8.5.3 Managing Synchronization Execution Logs

After a synchronization rule is executed, execution logs are generated accordingly. You can view the account synchronization result in the execution logs, including the synchronized account information, new account information, and deleted account information.

Prerequisites

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

Viewing Log Details

Step 1 Log in to the CBH system.

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

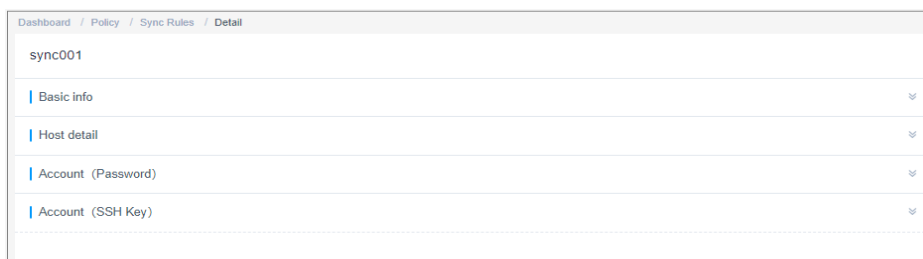
Step 3 Query OM task execution logs.

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

Step 4 Select the execution log and click **Detail**.

You can view the basic information, host details, account list for synchronizing passwords, and account list for synchronizing SSH keys.

Figure 8-7 Viewing the basic information



----End

Downloading OM Task Execution Logs

- Step 1** Log in to the CBH system.
- Step 2** Choose **Policy > Sync Rules > Sync Log**.
- Step 3** Select the execution log and click **Download** to download the log in CSV format.

----End

Deleting Execution Logs

- Step 1** Log in to the CBH system.
- Step 2** Choose **Policy > Sync Rules > Sync Log**.
- Step 3** Select an execution log and click **Delete** in the row to delete it.
- Step 4** To delete multiple execution logs at a time, select the ones you want and click **Delete** at the bottom of the list to delete all selected logs together.

----End

9 Ticket

9.1 Ticket Configuration Management

9.1.1 Configuring the System Ticket Modes

A ticket mode consists a series of ticket settings which restrict the resource scope that can be applied for through an access control ticket and the method a ticket is submitted. There are two modes of ticket settings:

- **Basic Settings:** In this mode, you can restrict the access scope of resources that can be applied for through an access control ticket and specify the way to submit a command control ticket.
- **Advanced Settings:** In this mode, you can restrict the access scope of resources that can be applied for through access control ticket from multiple dimensions, such as the user department, user role, and resource department.
 - After a **User Department** is configured, users in the department form a user pool. Only users in the user pool can apply for resources in the resource pool.
 - If no **User Role** is configured, all users in the user pool can apply for resources in the resource pool.
 - If **User Role** is configured, only users of specified roles in the user pool can apply for resources in the resource pool.
- A user pool is a group of users specified by the user department and user role. After a department or role is associated, users of the department or role can apply for resources in the resource pool.
- A resource pool is a group of resources specified by the resource department. After a department is associated, the resources of the department can be applied for by users in the user pool.

This topic describes how to configure the ticket mode.

Prerequisites

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

Configuring the Basic Ticket Settings

- Step 1** Log in to the CBH system.
- Step 2** Choose **System > Sysconfig > Ticket**.
- Step 3** In the **Basic Settings** area, click **Edit**.

Set the **Application scope** of resources that can be viewed by the user and the **Submission mode** of command approval ticket.

Table 9-1 Parameter description

Parameter	Description
Application scope	<p>Specifies the scope of resources that can be applied for with the access control ticket.</p> <ul style="list-style-type: none"> • The default value is the current department. • This Department: When applying for access control tickets, you can apply for the access control permission on the resources of the current department, excluding the resources of lower-level departments. • This Dept and lower level: When applying for access control tickets, you can apply for access control permissions for resources of the current department and lower-level departments. • All: You can apply for access control permissions for all system resources.
Submission mode	<p>Specifies the way to submit a ticket. The options are Manual and Auto.</p> <ul style="list-style-type: none"> • By default, Manual is selected. • Manual: After a command control ticket is generated, submit the ticket to the administrator for approval. • Auto: After a command control ticket is generated, it is automatically submitted to the administrator for approval.

- Step 4** Click **OK**. You can then view the configured ticket settings.

----End

Configuring the Advanced Ticket Settings

- Step 1** Log in to the CBH system.
- Step 2** Choose **System > Sysconfig > Ticket**.
- Step 3** In the **Advanced Settings** area, click **Edit**.
- Step 4** Configure the user pool.

Select user department or user role.

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

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

----**End**

Follow-up Operations

- To modify the resource pool and user pool in a certain piece of advanced settings, click **Edit** in the corresponding row. In the displayed dialog box, select other user and/or resource departments.
- To delete the restrictions of a certain piece of advanced settings, click **Delete** in the corresponding row. Deleted authentication information cannot be recovered. Exercise caution when performing this operation.

9.1.2 Configuring the Ticket Approval Process

The ticket approval process is the policy that specifies how to approve a system ticket. You can customize the approval process in terms of the approval process mode, approval form, approval node, approval series, and final approval node to enhance the management of the ticket approval process. The following are some major factors in an approval process:

- **Approval process type**
There are two types of application processes, the hierarchical process and fixed process. The hierarchical process is applicable to the approval within a department, and the fixed process is applicable to approval across departments.
- **Approval form**
Approval form is used to specify how a ticket is approved when multiple approvers are involved in the approval process. There are two forms, multiplayer approval and countersign approval. In multiplayer approval form, a ticket is approved as long as it is approved by any of the approvers. In countersign approval form, a ticket is approved only after it is approved by all approvers.
- **Approval node**
Approval node is used to specify attributes of the approver in the approval process, including the department and role attributes. The department administrator who meets the department and role requirements has the approval permission.
- **Approval series**
Approval series refers to the number of approval levels. If you select the hierarchical approval process, the approval series must be specified.
- **Final approval node**
After approvals at other levels complete, **admin** performs the final approval.

This topic describes how to customize a ticket approval process.

Prerequisites

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

Procedure

Step 1 Log in to the CBH system.




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

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

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

Table 9-2 Parameters for configuring ticket approval processes

Parameter	Description
Approval process type	<p>Approval process. The options are Classification for hierarchical process and Regular for fixed process.</p> <p>After the ticket approval process is configured, the ticket goes to each approver in sequence for approval. If there is no qualified approver at one stage, the ticket is approved at this stage by default. Then the ticket is routed to the next stage.</p> <ul style="list-style-type: none"> • By default, the hierarchical process mode is used. • Hierarchical process: Approval is performed level by level based on the approval level. • Fixed process: Approval is performed based on the fixed approval node. <p>NOTE You can send an email to notify the approver of the ticket status in either of the following ways:</p> <ul style="list-style-type: none"> - Set an outgoing email address by referring to Configuring the Outgoing Mail Server and ensure that emails can be sent properly. - On the Ticket tab, set the alarm level to High. For details, see Configuring Alarm Levels.
Approval form	<p>How the approval is performed. The options are Multiplayer and Countersign.</p> <ul style="list-style-type: none"> • The multiplayer approval mode is used by default. • Multiplayer: indicates that an approval from only one approver at each level is required. After the ticket is approved at a certain level, it becomes invisible to other approvers at the same level. If a ticket is rejected by any approver at the same level, the ticket is rejected. • Countersign: A ticket will not be transferred to the next level for approval until all approvers at the same level approve the ticket. If any approvers reject the ticket, the ticket is rejected. • During the approval process, the admin account can review all tickets on any node, and the review result is the final result.

Parameter	Description
Approval node	<p>Set the approver attribute of the node. The department attribute and role attribute must be set.</p> <p>After the setting is complete, the users who meet the department and role requirements automatically become the approvers of the node. If no users meet the department and role requirements, the system automatically searches for qualified users in the superior department until HQ is reached.</p> <ul style="list-style-type: none"> • Department attribute: includes User department and Resource department. • Role attribute: The role must have the administrator and ticket approval permissions. The default role is the department administrator. For example, if you select User department, the administrator of the department to which the ticket applicant belongs is select as the approver. If you select Resource department, the administrator of the department to which the resource belongs is selected as the approver.
Approval series	<p>Number of approval levels. If you select Classification for approval process, this parameter is mandatory.</p> <ul style="list-style-type: none"> • A maximum of five levels of approval series can be set. • The default value is 1, indicating that an approval level is required.
Final approval node	<p>Whether to enable final approval by admin. Final approval is enabled by default (.</p> <ul style="list-style-type: none"> • : indicates that final approval by admin is disabled. • : indicates that final approval by admin is enabled. This means the ticket cannot be approved until all approvers in other levels approve it and the admin user approves it. <p>NOTE If no qualified approvers at all approval levels, the approval from the admin user is required no matter whether the final approval is enabled.</p>

Step 4 Click **OK**. You can then view the configured ticket approval process.

----End

9.2 ACL Ticket

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

This topic describes how to create and manage ACL tickets.

Prerequisites

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

Procedure

Step 1 Log in to the CBH system.

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

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

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

Table 9-3 Parameters for configuring an ACL ticket

Parameter	Description
Operation Time	Specifies the time period for accessing the resource. The start time and end time must be set.
File Transmission	File transfer permissions, including uploading and downloading files.
Options	Whether to enable the functions in the session window when a web browser is used for O&M. <ul style="list-style-type: none"> • File Manage: Permissions to manage files or folders. If Upload or Download is selected for File transfer, File Manage must be enabled. • uplink clipboard and downlink clipboard: Permissions to use the clipboard function on hosts with Protocol set to RDP. • Watermark: Permissions to display the watermark of the user login name in the operation session window.
Remarks	(Optional) Briefly describe the reason for applying for the resource access control permission or other information.

Step 4 Click **Next** and select an account for which the permissions are applied.

Step 5 Click **OK** to submit the ticket.

After the administrator approves the ticket, you obtain the access permission for the resources.

----End

Follow-up Operations

- After a ticket is submitted, the administrator will receive a notification in the message center. They can view the ticket details. The ticket will also display in the ticket approval page. The administrator can choose to approve or reject the ticket.
- To modify a submitted ticket, click **Withdraw** to cancel the ticket. Then, the ticket status changes to **Revoked**.
- To view or modify the ticket information after the ticket is created, click **Manage** to go to the ticket details page.

 **NOTE**

For tickets in the **approving** status, you can only view the details but cannot modify the content. Only the ticket in the **Revoked** or **Not submitted** state can be modified.

- If a submitted ticket has expired, click **Delete** to delete it. You can also select multiple tickets and click **Delete** in the lower left corner to delete them in batches.

 **CAUTION**

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

9.3 Command Approval Ticket

CBH enables dynamic authorization of operations on Linux hosts. This enhances the restriction of key operations.

During O&M on Linux hosts, if an operation command triggers the command rules for dynamical approval, the system automatically intercepts the operation command and generates a command approval ticket. The command approval ticket is sent to the administrator. After it is approved by the administrator, you obtain the permission to run the operation command on the Linux host.

Figure 9-1 Example of command interception

```
Last login: Wed Mar 28 10:04:27 2018 from 192.168.1.66
hello, world!
[root@yabvpn ~]# 11
Command "11" is rejected. Please submit CommandControl authorization ticket
[root@yabvpn ~]# █
```

This topic describes how to manage command approval tickets.

Constraints

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

Prerequisites

- You have the management permissions for the **Command Approval Ticket** module.
- Command interception has been triggered, and a command approval ticket has been generated.

Procedure

Step 1 Log in to the CBH system.

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

Figure 9-2 Command Approval Ticket

Ticket Number	Status	Time	Command	Account	Remarks	Operation
201803281011216191205	Not submitted	-	11	root@192.1...	-	Manage Revoke Submit Delete

Step 3 Submit a ticket.

Command approval tickets can be submitted automatically or manually. For details, see [Configuring Basic Ticket Settings](#).

- If the automatic submission mode is selected, the system automatically submits the ticket to the administrator for approval.
- If the manual submission mode is selected, click **submit** to send it to the administrator for approval in the **Operation** column on the **Command Approval Ticket** list page.
- If the ticket is rejected by the administrator, you can modify the ticket information and submit it again.

Step 4 Withdraw a ticket.

Click **Withdraw** in the **Operation** column of the ticket you want to cancel. The ticket status then changes to **Revoked**.

Step 5 Modify ticket information.

- Click **Manage** to go to the details page.
- Click **Edit** on the details page and modify the authorized operation duration.

NOTE

For tickets in the **approving** status, you can only view the details but cannot modify the content. Only the ticket in the **Revoked** or **Not submitted** state can be modified.

Step 6 Delete a ticket.

- To delete one ticket, in the row of the ticket you want to delete, click **Delete** in the **Operation** column.
- To delete multiple tickets, select the ones you want to delete and click **Delete** at the bottom of the ticket list to delete all selected tickets together.

CAUTION

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

----End

Follow-up Operations

- After a ticket is submitted, the administrator will receive a notification in the message center. They can view the ticket details. The ticket will also display in the ticket approval page. The administrator can choose to approve or reject the ticket.
- After the administrator approves the ticket, you then obtain the command operation permissions within the authorization scope and period.
- After the permission in the ticket is revoked by the administrator, the operation commands will be intercepted again.

9.4 Database Approval Ticket

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

During O&M on databases, if an operation command triggers the database rules for dynamical approval, the system automatically intercepts the operation command and generates a database approval ticket. The command approval ticket is sent to the administrator. After the administrator approves the ticket, you obtain the permission to run the operation command.

This topic describes how to manage database approval tickets.

Constraints

- The database operation audit is available only in CBH professional editions.
- CBH can intercept sensitive operation commands and generate tickets only for MySQL and Oracle databases.
- A database approval ticket cannot be manually created. It is automatically generated when a user attempts to run a command which triggers a database rule.

Prerequisites

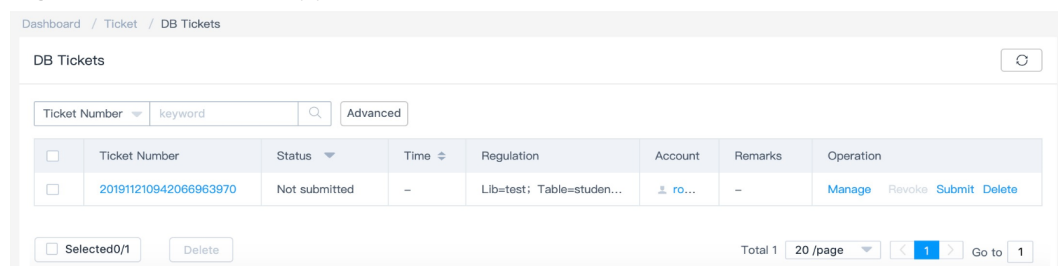
- You have the management permissions for the **DB Tickets** module.
- Operation interception has been triggered, and a database approval ticket has been generated.

Procedure

Step 1 Log in to the CBH system.

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

Figure 9-3 Database approval ticket list



The screenshot shows the 'DB Tickets' interface. At the top, there is a breadcrumb trail: 'Dashboard / Ticket / DB Tickets'. Below this, the title 'DB Tickets' is displayed with a refresh icon. A search bar contains 'keyword' and an 'Advanced' button. The main area features a table with the following columns: Ticket Number, Status, Time, Regulation, Account, Remarks, and Operation. One ticket is listed with the number '201911210942066963970', status 'Not submitted', and regulation 'Lib=test; Table=studen...'. The 'Operation' column for this ticket contains links for 'Manage', 'Revoke', 'Submit', and 'Delete'. At the bottom, there is a 'Selected 0/1' indicator, a 'Delete' button, and pagination controls showing 'Total 1', '20 /page', and 'Go to 1'.

<input type="checkbox"/>	Ticket Number	Status	Time	Regulation	Account	Remarks	Operation
<input type="checkbox"/>	201911210942066963970	Not submitted	-	Lib=test; Table=studen...	ro...	-	Manage Revoke Submit Delete

Step 3 Submit a ticket.

- In the row of the ticket you want to submit, click **Submit** in the **Operation** column to submit the ticket to the administrator for approval.
- If the ticket is rejected by the administrator, you can modify the ticket information and submit it again.

Step 4 Withdraw a ticket.

Click **Withdraw** in the **Operation** column of the ticket you want to cancel. The ticket status then changes to **Revoked**.

Step 5 Modify ticket information.

- Click **Manage** to go to the details page.
- Click **Edit** on the details page and modify the authorized operation duration.

 **NOTE**

For tickets in the **approving** status, you can only view the details but cannot modify the content. Only the ticket in the **Revoked** or **Not submitted** state can be modified.

Step 6 Delete a ticket.

- To delete one ticket, in the row of the ticket you want to delete, click **Delete** in the **Operation** column.
- To delete multiple tickets, select the ones you want to delete and click **Delete** at the bottom of the ticket list to delete all selected tickets together.

 **CAUTION**

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

----End

Follow-up Operations

- After a ticket is submitted, the administrator will receive a notification in the message center. They can view the ticket details. The ticket will also display in the ticket approval page. The administrator can choose to approve or reject the ticket.
- After the administrator approves the ticket, you then obtain the operation permissions within the authorization scope and period.
- After the permission in the ticket is revoked by the administrator, the operation commands will be intercepted again.

9.5 Ticket Approval

After a ticket is created by a system user or generated by the system, the ticket goes to the specified approvers. The approvers receive a ticket approval notification in the message center. They can view tickets to be approved on the **Ticket approval** page.

This topic describes how to manage submitted tickets, including viewing ticket details, approving tickets, rejecting tickets, and revoking ticket.

Prerequisites

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

Procedure

- Step 1** Log in to the CBH system.
- Step 2** Choose **Ticket > Ticket approval**.

Figure 9-4 Ticket approval

<input type="checkbox"/>	Ticket No	Status	Time	Type	Content	Creator	Operation
<input checked="" type="checkbox"/>	2020111915...	approving	2020-11-19 1...	Access appro val	root@...	admin	Manage Approve Reject Revoke
<input type="checkbox"/>	2020111915...	Revoked	2020-11-19 1...	Access appro val	root@f...	admin	Manage Approve Reject Revoke
<input type="checkbox"/>	202003091...	Expired	2020-03-09 1...	Command ap proval	vim test	lyk	Manage Approve Reject Revoke
<input type="checkbox"/>	202001161...	Rejected	2020-02-25 0...	Access appro val	Admini...	admin	Manage Approve Reject Revoke
<input type="checkbox"/>	202002241...	Expired	2020-02-24 1...	Command ap proval	vim test	admin	Manage Approve Reject Revoke
<input type="checkbox"/>	202002162...	Revoked	2020-02-16 2...	Command ap proval	cat test	admin	Manage Approve Reject Revoke

- Step 3** Views details about tickets.

In the row of a ticket you want to manage, click **Manage** in the **Operation** column. On the displayed ticket details page, view the basic information, account list, and approver list of the ticket.

Figure 9-5 Ticket details

202011191532251413102		Approve	Reject
Basic Info	⌵		
Account	⌵		
Approvers	⌵		

- Step 4** Approve the ticket.
 - To approve one ticket, click **Approve** in the **Operation** column of the corresponding row.
 - To approve multiple tickets at a time, select the ones you want and click **Approve** in the lower left corner of the list to approve them together.

Step 5 Reject a ticket.

In the row of the ticket you want to reject, click **Reject** in the **Operation** column.

Step 6 Cancel a ticket.

In the row of the ticket you want to cancel the authorization, click **Cancel** in the **Operation** column.

----End

9.6 Ticket Application Examples

Case 1: Creating a Classification Approval Ticket to Control Resource Requests Based on User Departments

Prerequisites

- You have configured required parameters, including departments, users, roles, and resources. For more details, see [Department](#), [User](#), and [Resource](#).
- The ticket approval process is configured as shown in [Table 9-4](#). For more details about ticket approval process, see [Configuring the Ticket Approval Process](#).

Table 9-4 Parameters for configuring a ticket approval process

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

Approval Process

A user submits a ticket to apply for access permissions for resources based on the department that the user belongs to.

Both user A and user B (lower-level administrators) have the approval right. If either one of them approves, the ticket is approved. If either one of them rejects, the ticket is rejected. After one of the lower-level administrators approves the ticket, the workflow goes to the next stage for user C (middle-level administrator) to review. The rest can be deduced by analogy. After user D (higher-level administrator) approves the ticket, the user obtains the requested permissions. If the ticket is rejected at any stage during the approval, it fails to be approved and the user cannot obtain the permissions.

 **NOTE**

An account with permissions of the admin administrator can approve or reject any ticket on any node, and the result is the final result.

Case 2: Creating a Classification Approval Ticket to Control Resource Requests Based on Resource Departments

Prerequisites

- You have configured required parameters, including departments, users, roles, and resources. For more details, see [Department](#), [User](#), and [Resource](#).
- The ticket approval process is configured as shown in [Table 9-5](#). For more details about ticket approval process, see [Configuring the Ticket Approval Process](#).

Table 9-5 Parameters for configuring a ticket approval process

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

Approval Process

A user submits a ticket to apply for access permissions for resources based on the department that the resource belongs to.

If user D (lower-level administrator) approves the ticket, the workflow goes to the next stage for user E (middle-level administrator) to review. If user D rejects the ticket, the ticket is rejected. The rest can be deduced by analogy. After user F (higher-level administrator) approves the ticket, the user obtains the requested permissions. If the ticket is rejected at any stage during the approval, it fails to be approved and the user cannot obtain the permissions.

NOTE

An account with permissions of the admin administrator can approve or reject any ticket on any node, and the result is the final result.

Case 3: Creating a Ticket with Fixed Approval Process and Countersign Form

Prerequisites

- You have configured required parameters, including departments, users, roles, and resources. For more details, see [Department](#), [User](#), and [Resource](#).
- The ticket approval process is configured as shown in [Table 9-6](#). For more details about ticket approval process, see [Configuring the Ticket Approval Process](#).

Table 9-6 Parameters for configuring a ticket approval process

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

Approval Process

A user submits a ticket to apply for access to resources of a department that the user does not belong to.

Both user B and user C have the approval right. If both of them approve, the ticket is approved. If either one of them rejects, the ticket is rejected. After the engineering department administrators approve the ticket, the workflow goes to the next stage for user D (finance department administrator) to review. The rest can be deduced by analogy. After user E (finance department administrator) approves the ticket, the user obtains the requested permissions. If the ticket is rejected at any stage during the approval, it fails to be approved and the user cannot obtain the permissions.

NOTE

An account with permissions of the admin administrator can approve or reject any ticket on any node, and the result is the final result.

10 Operation

10.1 Host Operation

10.1.1 Viewing the Host Resource List and Setting Resource Labels

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

This topic describes how to view authorized resources and set resource labels.

Constraints

- Labels cannot be shared with others. You can define your own resource labels for your exclusive use.
- Downloading login configuration is supported by only resources managed over SSH.

Prerequisites

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

Procedure


Step 1 Log in to the CBH system.

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

Step 3 Query host resources.

Quick search: Enter a keyword in the search box to quickly query host resources by auto recognition, host name, and host IP address.

Step 4 Add a label to an application resource.

1. Select an application resource you want and click  in the **Label** column.

2. Enter a label type and press **Enter** or select an existing label type.
3. Click **OK**. You can then view the added label on the **Host Operations** page.

Step 5 Add a label for multiple application resources at a time.

1. Select multiple resources and click **Add Label** in the lower left corner of the list.
2. Enter a label type and press **Enter** or select an existing label type.
3. Click **OK**. You can then view the added label on the **Host Operations** page.

Step 6 Delete an application resource label.

1. Select multiple resources and click **Delete Label** in the lower left corner of the list.
2. In the displayed dialog box, confirm the deletion and click **OK**.

----End

10.1.2 Logging In to Managed Resources Using a Web Browser for O&M

After you log in to a host resource using a web browser, the cooperation, file management, file transfer, and command preset functions are available for you. All operations performed on a host resource are recorded by CBH for audit.

- **Cooperation:** This function allows the session initiator to invite other system users to participate the current session by sharing the session link with them, implementing O&M collaboration.
- **File management:** This function allows all session participants to manage files or folders on hosts and host net disk on the pane on the right after they obtain the operation permissions. In addition, they can:
 - Create new folders.
 - Change the name of a file or folder.
 - Delete files or folders in batches.
- **File transfer:** This function allows session participants to download or upload files or folders on the host or host net disk after they obtain the operation permissions. They can:
 - Upload and download files.
 - Upload folders.
 - Upload multiple files on a local server or net disk to a host or download multiple files from a host to a local server or net disk, if **Host Files** is selected as the destination address.
 - Upload multiple files or a folder to a host net disk or download multiple files from a host net disk to a local host, if **Netdisk** is selected as the destination address.

This topic describes how to log in to a host using a web browser and how to perform operations in the session window of the hosts using character or image protocols.

Constraints

- Only hosts using character protocols (SSH and Telnet) or image protocols (RDP and VNC) can be logged in using a web browser.
- The file transfer and management functions are unavailable for hosts using the Telnet protocol.
- Although using a web browser for O&M allows you to copy and paste a large number of characters without garbled characters, a maximum of 80,000 characters can be copied from the local to the remote, and a maximum of 1000,000 of bytes can be copied from the remote to the local.
- If you log in to a CBH system as a non-admin user and want to manage Windows host resources, deselect the admin console. To do so, go to the **Operation > Host Operations** page, click **Web OPS Settings** in the upper right corner, then deselect **admin console**.
- File management
 - Files and folders cannot be edited in batches.
- File Transmission
 - By default, the system supports the upload of a single file with a maximum size of 100 GB. However, the size of a single file to be uploaded is limited by the **Personal Netdisk** space and browser type.
 - Folders cannot be downloaded.
 - For the hosts using the RDP protocol, only **Netdisk** can be select as the destination address.

Prerequisites

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

Procedure

Step 1 Log in to the CBH system.

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

Step 3 Select the host you want and click **Login** in the **Operation** column to open the session.

- [Session Window of Hosts Using the RDP or VNC Protocol](#)
- [Session Window of Hosts Using the SSH or Telnet Protocol](#)

Step 4 Invite other system users to participate in the current session. For details, see [Cooperation](#).

1. Click **Cooperation**. The collaborative session window is displayed.
2. Click **Share**. Complete the information in the displayed **Invite friends** dialog box.

NOTE

- The URL link can be copied and sent to multiple users.
 - Only users with the access permission of the CBH account can access the CBH system. Otherwise, a connection error will be reported, indicating that the connection has been disconnected because the server does not respond for a long time. Check your network settings and try again (Code: T_514).
3. Copy the link and send it to the users whom you want to invite. The users must have the access permission for CBH. Once they receive the link, they can log in to the CBH system, open a web browser, and enter the link to open it in the web browser.
 4. If you are invited, click **Enter** to join the session.

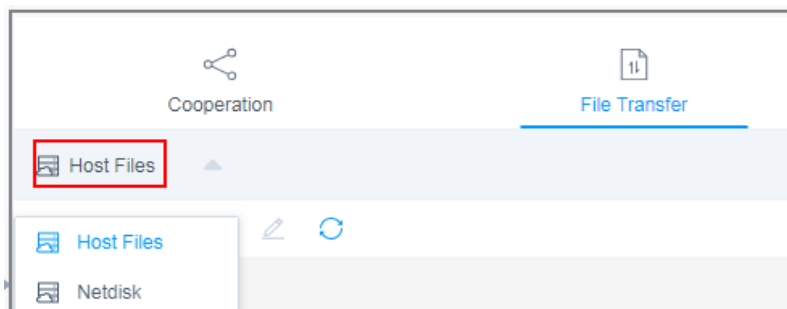
Table 10-1 Parameters for session operation

Parameter	Description
Apply for control	The invited user can apply for control from the invitation sender. Once approved, the invited user can control the current session.
Exit session	Exit the current session.

Step 5 Upload files to or download files from the host or host net disk. For details, see [File Transfer](#).

1. Click **File Transfer**. The **File Transfer** window is displayed.
2. **Host Files** is selected by default. You can click **Host Files** to switch the destination address to **Netdisk**.

Figure 10-1 Switchover of destination address





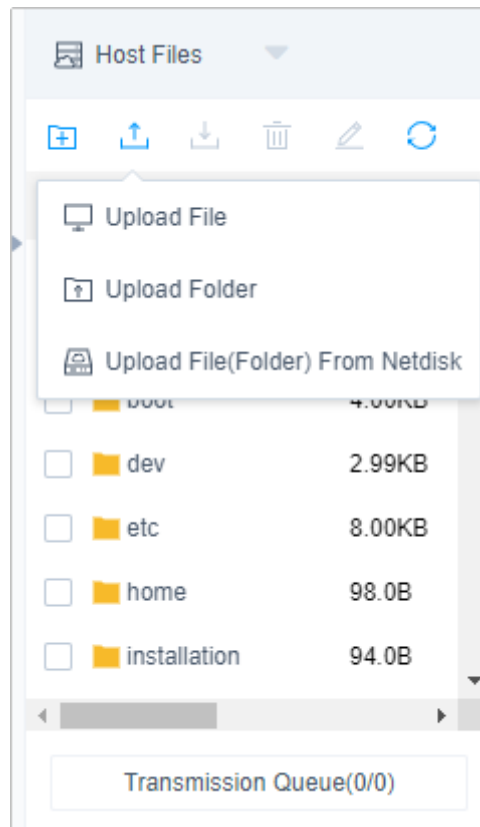
3. Click  to upload a file.
4. Select a file and click  to download a file.

Figure 10-2 Uploading files



NOTE

- **Netdisk** is dedicated for your exclusive use. It cannot be accessed by other users. You can transfer files from **Netdisk** to multiple hosts without worries of data leakage.
- The default file storage path of Windows servers is drive G, and that of Linux servers is the root directory.
- To upload or download files on a Windows server, open the disk directory of the server and copy and paste the file to drive **G** of the Netdisk.

Step 6 In the file management area, manage files or folders on the host or host net disk.


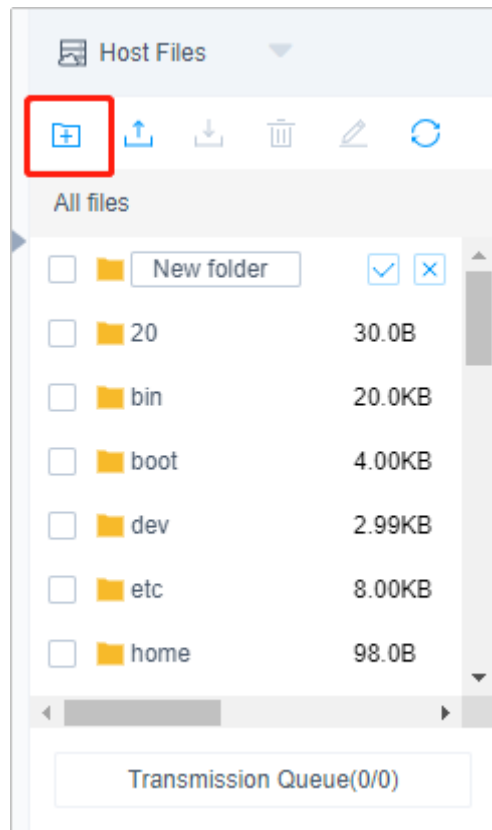



1. Click **File Transfer**. The **File Transfer** window is displayed.
2. Click  to create a folder.

Figure 10-3 New folder



3. Select one or more files or folders and click  to delete them.
4. Select a file or folder and click  to edit its name.
5. Click  to refresh all file directories.

----End

Session Window of Hosts Using the SSH or Telnet Protocol

Table 10-2 Linux host operations

Parameter	Description
Chinese code	The character protocol supports multiple Chinese character encoding formats.
Copy/Paste	Select the characters, press Ctrl+C to copy it, and press Ctrl+V to paste it.
Preset command	You can preset commands that are long and frequently used.
Terminal Type	The character protocol supports terminal type switching, including Linux and Xterm.

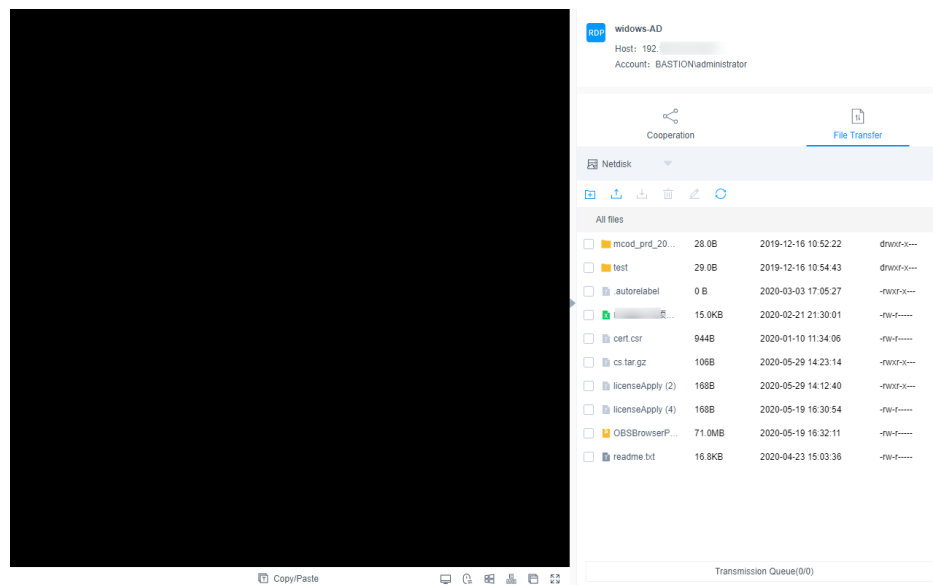
Parameter	Description
Mass sending	When the group sending function is enabled, you can run commands in multiple sessions at the same time.
Font size	There are three types of font sizes: large, medium, and small.
Copy window	You can copy the current session window.
Full screen	Displays the window in full screen.

Session Window of Hosts Using the RDP or VNC Protocol

Table 10-3 Windows host operations

Parameter	Description
Copy/Paste	<p>Remote text: Select the character you want, press Ctrl+C twice to copy the character, and press Ctrl+V to paste the character.</p> <p>Remote machine files: Select a text or image, press Ctrl+B to copy it, and press Ctrl+G to paste it.</p> <p>NOTE Although using a web browser for O&M allows you to copy and paste a large number of characters without garbled characters, a maximum of 80,000 characters can be copied from the local to the remote, and a maximum of 1000,000 of bytes can be copied from the remote to the local.</p>
Resolution	You can switch the resolution of the current operation interface. During the switching, a new connection is created.
Switch to remote mouse	You can switch over between the local mouse and remote mouse.
Windows	This Windows icon can be used for easy access to Windows system functions.
Ctrl+Alt+Delete	Ctrl+Alt+Delete
Copy window	You can copy the current session window.
Full screen	Displays the window in full screen.

Figure 10-4 Session window of hosts using the RDP protocol



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

CBH gives you the ability to use an SSH client to manage your host resources without changing your habits of using your original SSH client. In addition, the command rules and operation audit function are still available.

This topic uses Xshell as an example to describe how to use an SSH client to log in to a resource for O&M and how to download the configuration file of the resource.

Constraints

- Logging using an SSH client is used only for hosts using the SSH, Telnet, or Rlogin protocol. For hosts using the Rlogin protocol, only an SSH client can be used for login.
- Supported SSH clients include SecureCRT 8.0 or later, Xshell 5 or later, PuTTY, and MAC Terminal 2.0 or later.

Prerequisites

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

Procedure

- Step 1** Start the local client tool Xshell and choose **File > New** to create a user session.
- Step 2** Configure session connections.

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

In the newly opened blank session window, run a command in the following format: **Protocol type User login name@System login IP address Port number**, for example, `ssh admin@10.10.10.10 2222`.
- Method 3

In the live session window of a Linux host, run a command in the following format: **Protocol type User login name@System login IP address-p Port number**, for example, `ssh admin@10.10.10.10 -p 2222`.

 **NOTE**

The **system login IP address** is the CBH IP address, which can be the private IP address or an EIP. The network connection between the local PC and the IP address is normal.

Instance Name	Status	Instance Type	Private IP Address	EIP
CBH-1b4c-test31	Running	Single-node	172.31.1.6	172.31.1.6
CBH-cjg-1ec2	Running	Single-node	172.31.1.2	172.31.1.2

Step 3 Verify user identity.

- Select **Password**, enter your password, and click **OK**.
- Select **Public Key**, select a user key from the **Browse** drop-down list, enter the password, and click **OK**.

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

Step 4 Log in to the CBH system.

If an SSH client is used, password, SMS message, mobile token, and OTP can be used for login identity authentication. To use mobile SMS message, mobile OTP, and OTP authentication methods, configure multifactor verification. For details, see [Configuring User Login Restrictions](#).

- Mobile SMS: After logging in to the system using the local password, select **Mobile SMS** for **Multifactor Verification**, and enter the SMS verification code.
- Mobile OTP: After logging in to the system using the local password, select **Mobile OTP** and enter the dynamic password of the mobile phone token.
- One-Time password: After logging in to the CBH system using the local password, select **OTP** and enter the dynamic token verification code.

Step 5 Import multiple accounts of a managed host.

Decompress the configuration file package, open the **readme.txt** file, and import the resource account. For details about how to download the package, see [Downloading Host Configuration File](#).

Step 6 Log in to the managed host using an account.

Select the account to be used for logging, enter the password of the system user, and log in to the host for O&M.

----End

Downloading Host Configuration File

To import host resources in batches using the SSH client, download the configuration files of the hosts to be imported.

- Step 1** Log in to the CBH system using a web browser.
- Step 2** Choose **Operation > Host Operations** to go to the **Host Operations** page.
- Step 3** Click **Export Host Configuration**.
- Step 4** Select the configuration file of the client and click **OK** to download the configuration file.

----End

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

CBH allows you to use file transfer clients to transfer files between authorized managed hosts using the file transfer protocol. This means you can transfer files the way you are used to. All operations performed on a host resource are recorded by CBH for audit.

This topic describes how to obtain client login information and log in to resources that use a file transfer protocol.

Constraints

Only hosts with **Protocol** set to **FTP**, **SFTP**, or **SCP** can be logged in to using a web browser. Client tools must meet the requirements in the following table.

Host Protocol	Client Tool Required
SFTP	Xftp 6 or later, WinSCP 5.14.4 or later, and FlashFXP 5.4 or later
FTP Protocol	Xftp 6 or later, WinSCP 5.14.4 or later, FlashFXP 5.4 or later, and FileZilla 3.46.3 or later

Prerequisites

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

- You have enabled FTP and opened ports 2222 (for SFTP) and 2121 (for FTP). For details, see [Configuring the Operation Ports](#).

Procedure

Step 1 Obtain the login information.

- Log in to the CBH system.
- Choose **Operation > Host Operations** to go to the **Host Operations** page.
- Select an FTP or SFTP host resource, and click **Login**.

Step 2 Log in to the host using a client tool.

- Start the local FTP or SFTP client tool.
- Enter the host address, port number, user name, and login password.

NOTE

CBH allows you to use APIs to log in to hosts using the FTP or SFTP protocol.

Table 10-4 Parameter description

Parameter	Description
Host Addr	IP address for logging in to the CBH system
Port	Port number. The default port number is 2222.
UserName	Username in the configuration information in the format of login name@resource account name@host address, for example, admin@root@192.168.1.1.
Password	Password for the user to log in to the CBH system.

----End

10.1.5 Logging In to Hosts in Batches for O&M

CBH also allows you to batch log in to multiple host resources for operation, including file transfer, file management, and command presetting. All operations performed on a host resource are recorded by CBH for audit.

This section describes how to log in to hosts in batches using a web browser.

Constraints

- Batch login is unavailable for hosts configured with the FTP, SFTP, DB2, MySQL, Oracle, SQL Server, or SCP protocol.
- Manual login and two-person approval accounts cannot be used for batch logging.
- The cooperation session function is unavailable for hosts logged in through batch logging.

Prerequisites

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

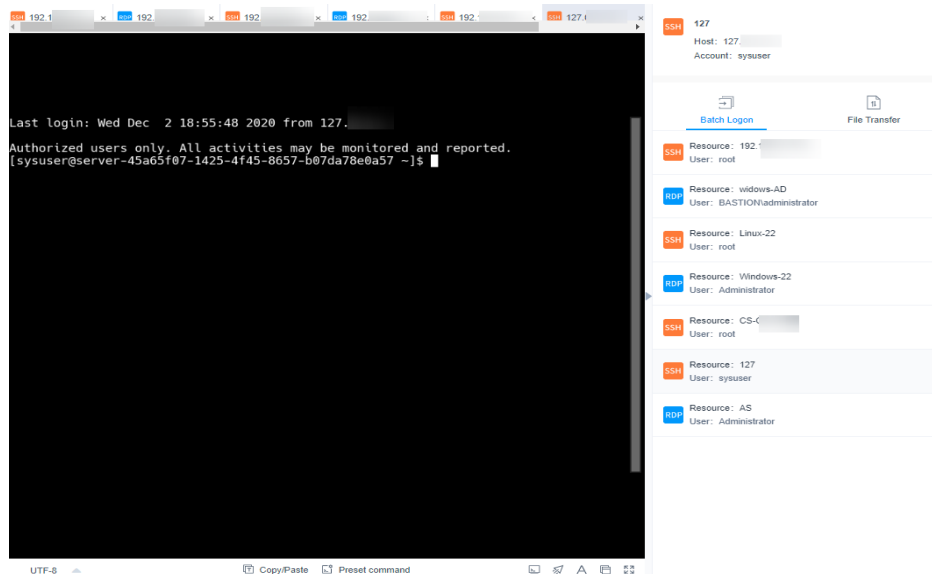
Procedure

Step 1 Log in to the CBH system.

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

Step 3 Select multiple resources and click **Batch Logon**.

Figure 10-5 Batch logon session windows



Step 4 Switch over session windows.

Click the resource name in the batch logon list to switch to the corresponding session window.

Step 5 For details about the operations in the session window, see the following description.

- [Session Window of Hosts Using the RDP or VNC Protocol](#)
- [Session Window of Hosts Using the SSH or Telnet Protocol](#)

Step 6 Upload files to or download files from the host or host net disk. For details, see [File Transfer](#).

Step 7 In the file management area, manage files or folders on the host or host net disk. For details, see [Using a Web Browser for Logging In](#).

----End

10.1.6 File Transmission

When you manage resources through a web browser, you can upload or download files on the **File Transfer** tab. This feature enables file transfer between a local computer and managed host and between different managed hosts. The CBH

system records the entire file transfer process in detail, making it easier to audit file upload and download operations.

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

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

Constraints

- Currently, when you use a web browser for O&M, files can be uploaded or downloaded only on the hosts using the SSH or RDP protocol.
- During web-based O&M, users cannot upload files to or download files from managed hosts by running the **rz** or **sz** command but only through **File transfer**.

NOTE

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

- Web-based O&M allows you to download one or more files but not folders.
- Resumable download is not supported. Do not stop or pause the file upload or download process.
- For a file larger than 1 GB, you can split the file into several small files and then upload or download them in batches or [use the FTP client to transfer the file](#).

Prerequisites

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

Uploading Files to and Downloading Files from a Managed Linux Host

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

Step 1 Log in to the CBH system.

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

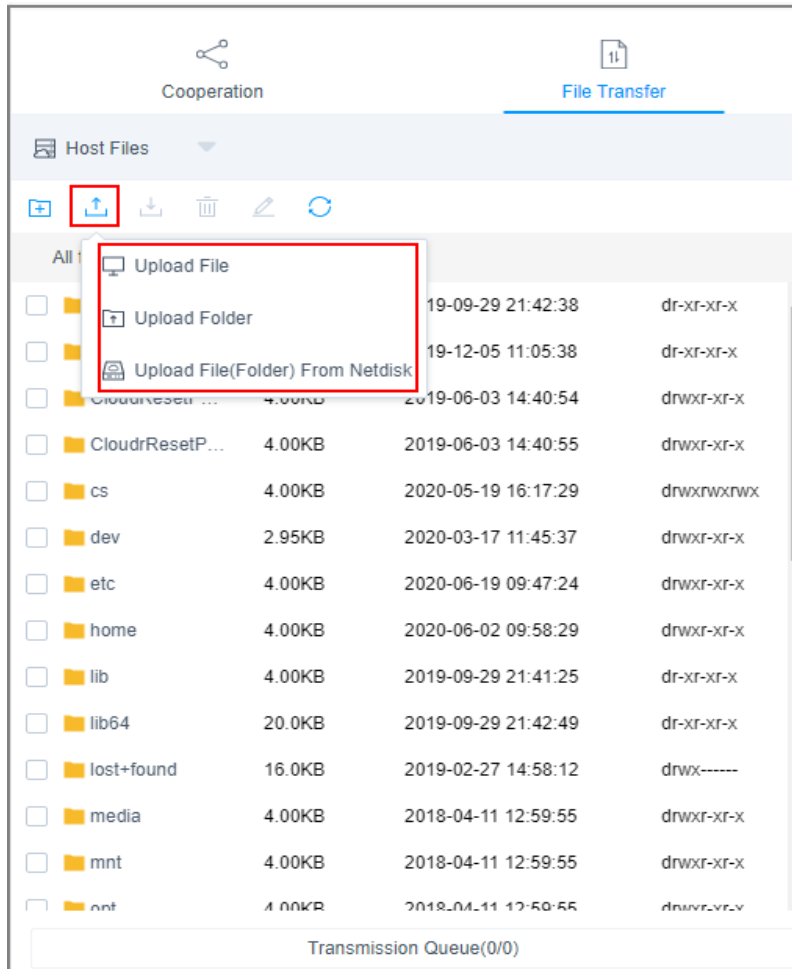
Step 3 Click **Login** to open the Linux host operation session.

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

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.

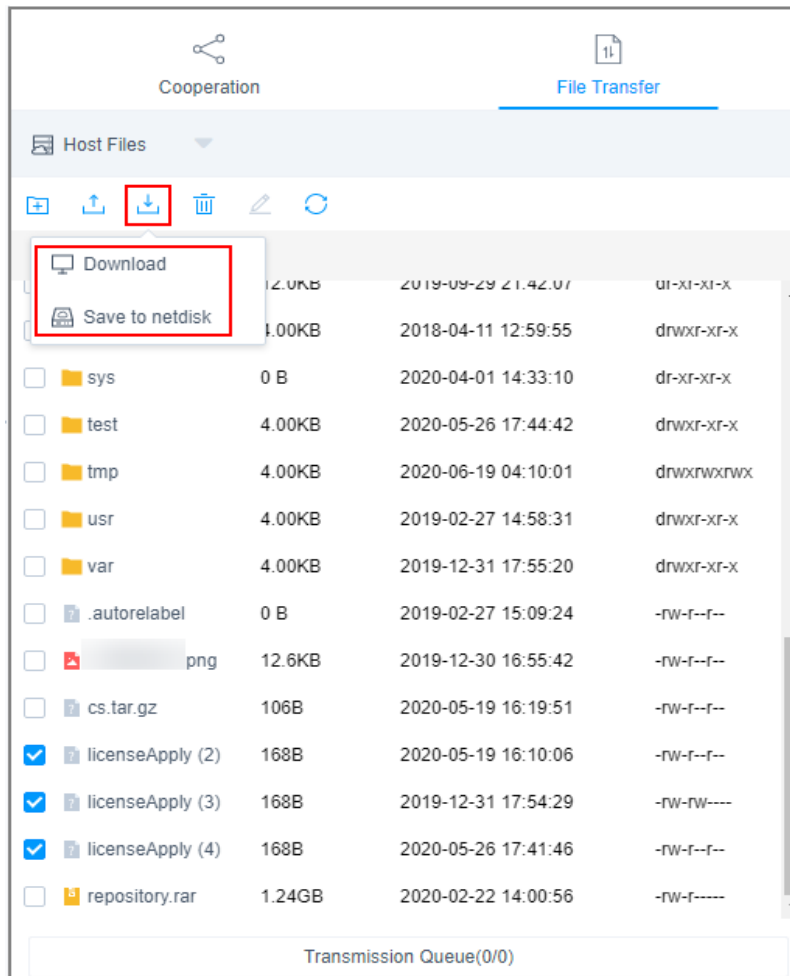
Figure 10-6 Uploading files to a Linux host



Step 6 Download files from the Linux host.

1. Select one or more files to be downloaded.
2. Click **Download** or **Save to netdisk** to download selected files to the local computer or the personal net disk, respectively.

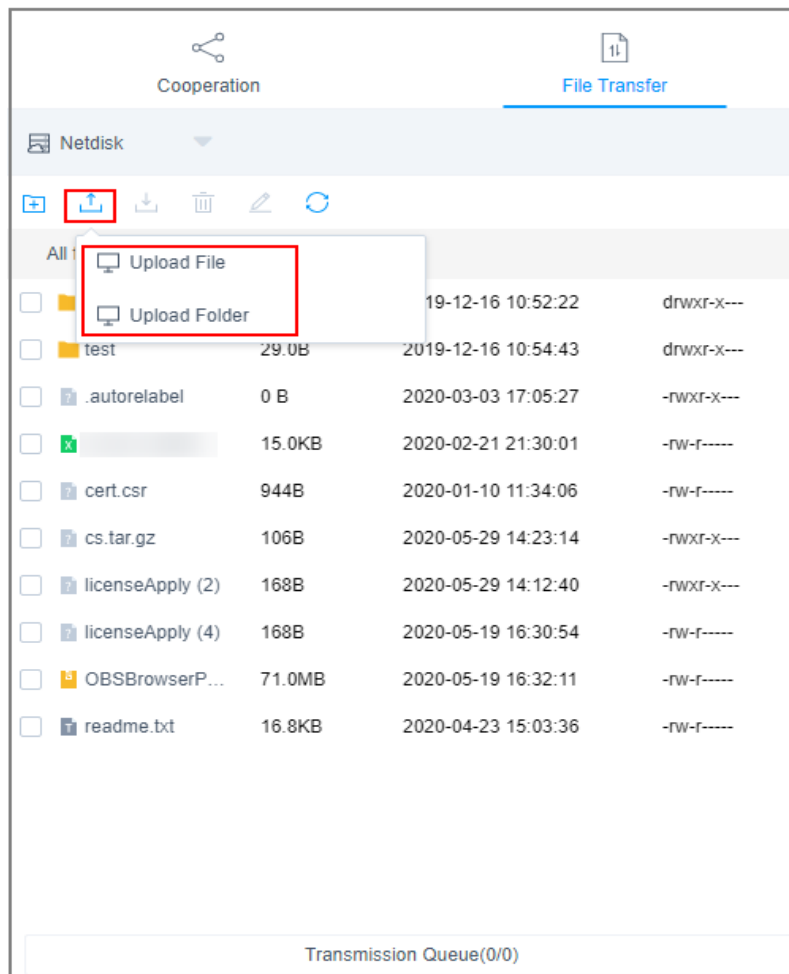
Figure 10-7 Downloading files from a Linux host



Step 7 Upload files to the personal net disk

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

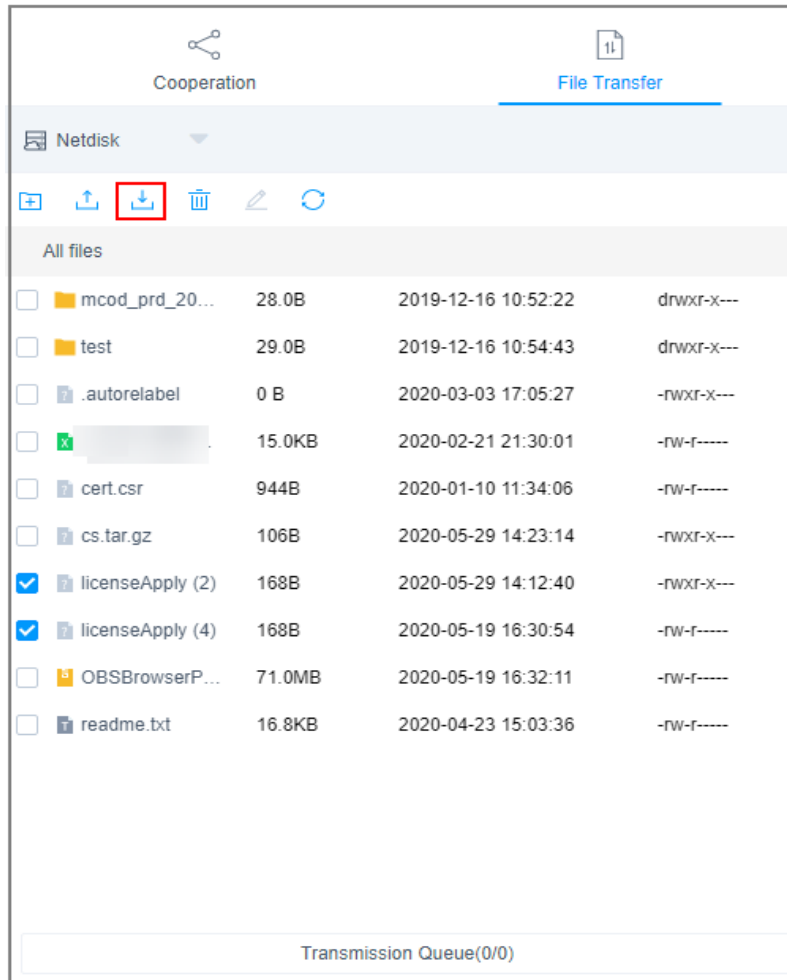
Figure 10-8 Uploading files to the personal net disk



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 10-9 Downloading files from the personal net disk



----End

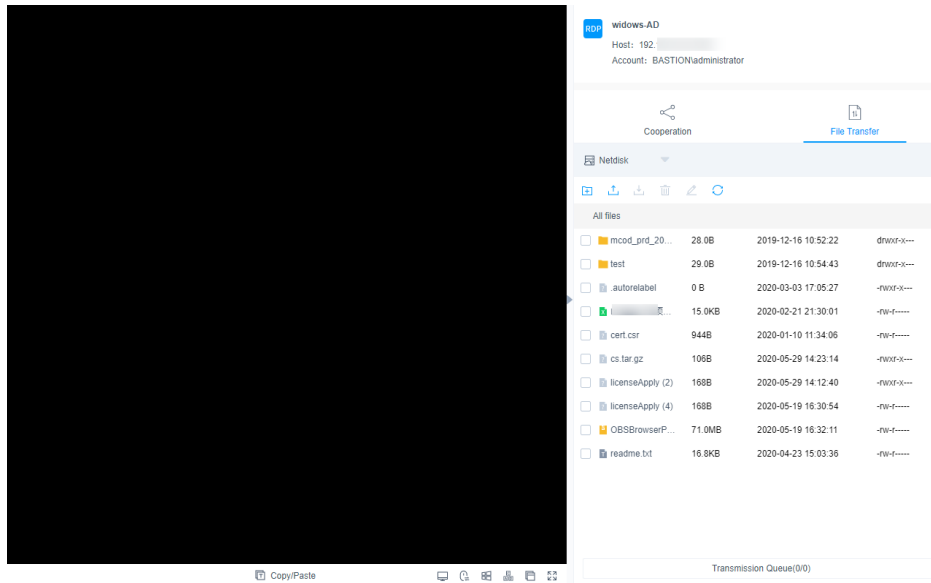
Uploading Files to and Downloading Files from a Managed Windows Host

For Windows hosts managed in a CBH system, the default path for storing files is **NetDisk G**. This disk is your personal net disk.

Files on a Windows host cannot be directly transferred between the 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 operation session.
- Step 4** Click **File Transfer** to list of host files on the personal net disk.

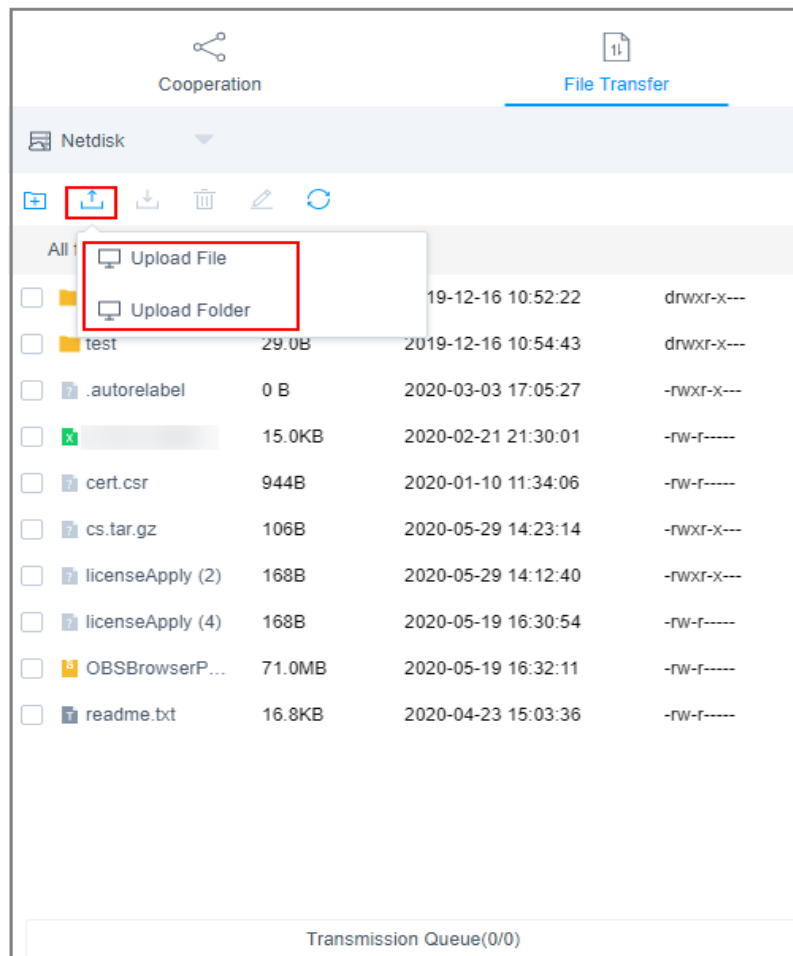
Figure 10-10 Windows host file transfer



Step 5 Upload files to the Windows host.

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

Figure 10-11 Uploading files to the personal net disk



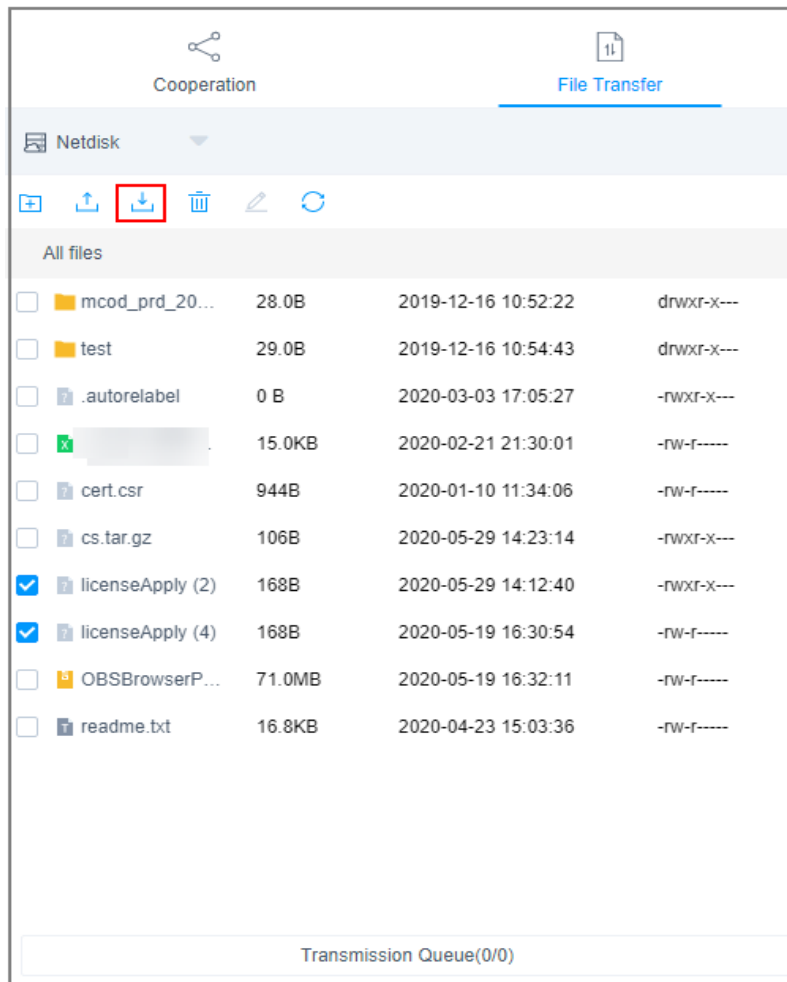
Step 6 Download files from the Windows host.

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

Step 7 Download files from the personal net disk.

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

Figure 10-12 Downloading files from the personal net disk



----End

10.1.7 Cooperation

With the cooperation function, CBH allows a session creator to invite other system users through a URL to join the on-going session. Participants can perform operations on the session after being approved by the session creator. This function can be used in scenarios such as remote demonstration and consultation of difficult O&M problems.

Constraints

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

- The invited user can join the session only before the URL expires or the session ends.

Prerequisites

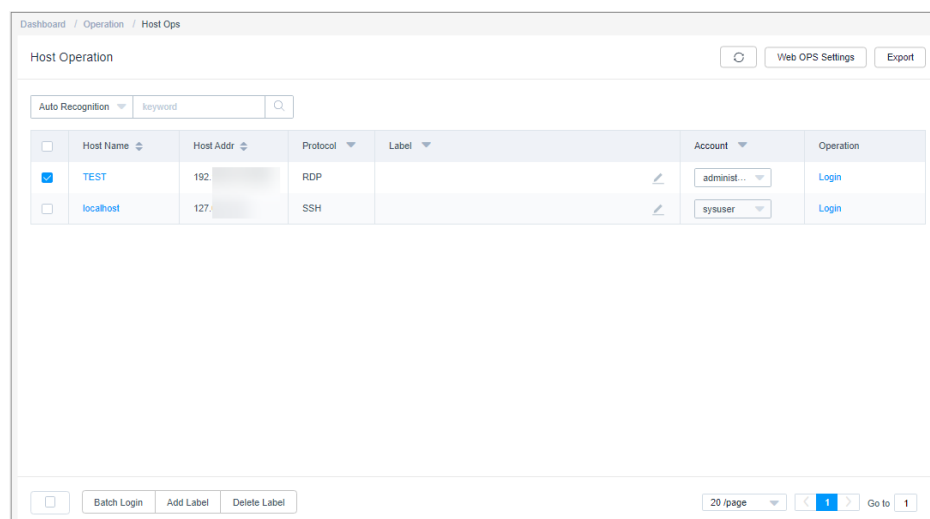
- You have the operation permissions for the host resources.
- You have logged in to the host using a web browser.

Procedure

Step 1 Log in to the CBH system.

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

Figure 10-13 Host Operation



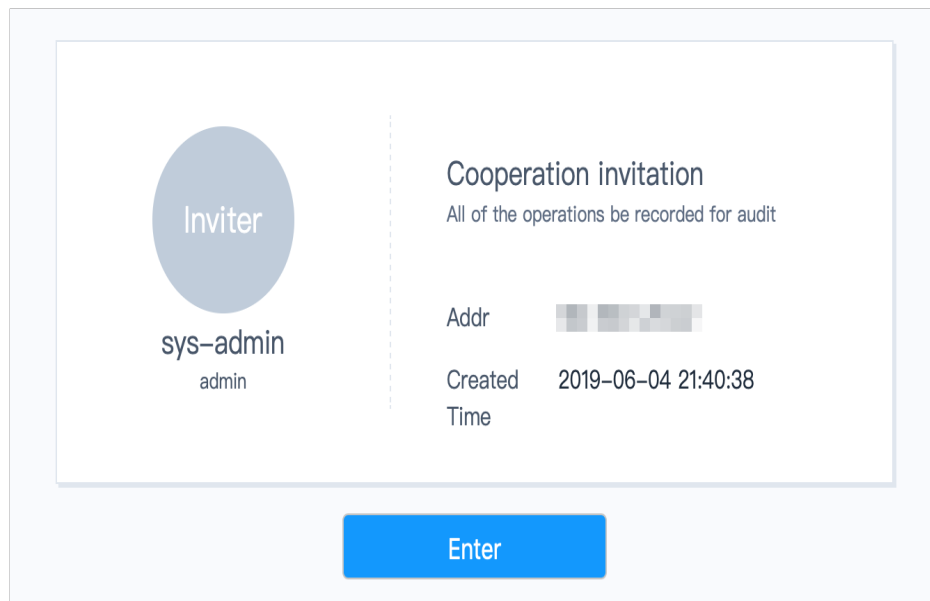
Step 3 Select the host resource you want to operate and click **Login**.

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

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

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

Figure 10-14 Invitation information displayed for the invited users



Step 7 As an invited user, click **Enter** to join the session.

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

Step 8 The creator or the invited user can manage the session.

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

----End

10.1.8 Enabling Forcible RDP Connections

When the number of Windows remote desktop connections exceeds the upper limit, you are not allowed to establish remote connections with the host resources. In this case, you can enable the **admin console** in the CBH system to implement force logins. This means you can force the CBH system to establish login connection by forcibly logging out other logged in users.

This topic describes how to enable the **admin console** configuration for enabling force RDP connections.

Constraints

- This function is available only for hosts using the RDP protocol.

- This function is available to user **admin** only.

Prerequisites

You have the management permissions for the **Host Operations** module.

Procedure

Step 1 Log in to the 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 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, if the number of connections exceeds the upper limit, the user is forced to log in.

----End

10.2 Application Operation

10.2.1 Viewing the Application Resource List and Setting Resource Labels

After obtaining the access permissions for application resources, you can view authorized application resources and set labels for them.

This topic describes how to view authorized resources and set resource labels.

Constraints

Labels cannot be shared with others. You can define your own resource labels for your exclusive use.

Prerequisites

- You have the management permissions for the **App Operations** module.
- You have obtained the access permissions for the resources.

Procedure


Step 1 Log in to the CBH system.

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

Step 3 Query application resources.

Quick search: Enter a keyword in the search box to quickly query application resources by auto recognition, application name, and application IP address.

Step 4 Add a label to an application resource.

1. Select an application resource you want and click  in the **Label** column.
2. Enter a label type and press **Enter** or select an existing label type.
3. Click **OK**. You can then view the added label on the **App Operations** page.

Step 5 Add a label for multiple application resources at a time.

1. Select multiple resources and click **Add Label** in the lower left corner of the list.
2. Enter a label type and press **Enter** or select an existing label type.
3. Click **OK**. You can then view the added label on the **App Operations** page.

Step 6 Delete an application resource label.

1. Select multiple resources and click **Delete Label** in the lower left corner of the list.
2. In the displayed dialog box, confirm the deletion and click **OK**.

----End

10.2.2 Logging In to Application Resources Using a Web Browser for O&M

After you log in to an application resource using a web browser, the cooperation, file management, and file transfer functions are available for you. All operations performed on an application resource are recorded by CBH for audit.

- **Cooperation:** This function allows the session initiator to invite other system users to participate the current session by sharing the session link with them, implementing O&M collaboration.
- **File management:** This function allows all session participants to manage files or folders on hosts and host net disk after they obtain the operation permissions. In addition, they can:
 - Create new folders.
 - Change the name of a file or folder.
 - Delete files or folders in batches.
- **File transfer:** This function allows session participants to download or upload files or folders on the host or host net disk after they obtain the operation permissions. They can:
 - Upload and download files.
 - Upload folders.
 - Upload multiple files or a folder to a host net disk or download multiple files from a host net disk to a local host, if **Netdisk** is selected as the destination address.

This topic describes how to log in to application resources and perform operations through a web browser.

Constraints

- Currently, application operation is available only for the x86 CBH instances.

- Only web browsers can be used to log in to application resources for O&M.
- Although using a web browser for O&M allows you to copy and paste a large number of characters without garbled characters, a maximum of 80,000 characters can be copied from the local to the remote, and a maximum of 1000,000 of bytes can be copied from the remote to the local.
- File management
Files and folders cannot be edited in batches.
- File Transmission
 - By default, the system supports the upload of a single file with a maximum size of 100 GB. However, the size of a single file to be uploaded is limited by the **Personal Netdisk** space and browser type.
 - Folders cannot be downloaded.
 - For application resources, only **Netdisk** can be select as the destination address.

Prerequisites

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

Procedure

Step 1 Log in to the CBH system.

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

Step 3 On the displayed page, select the application resource you want and click **Login** in the **Operation** column to open the session.

Table 10-5 Parameters for session operation

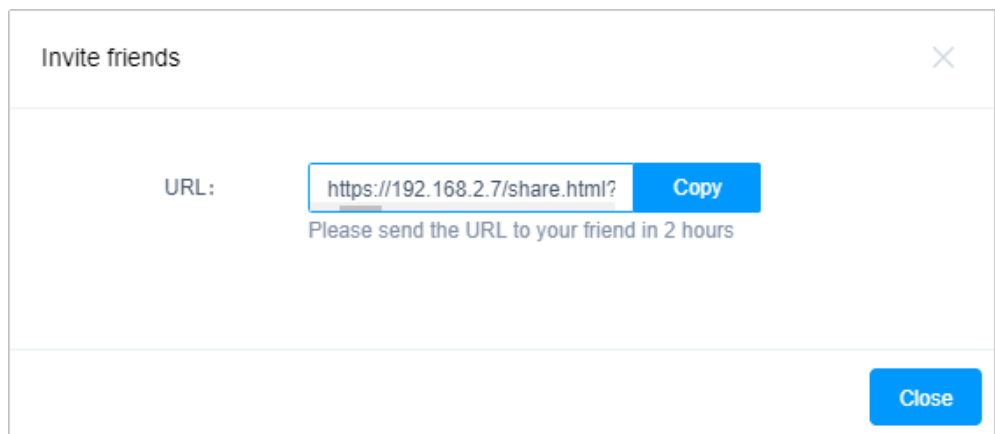
Parameter	Description
Copy/Paste	Remote text: Select the character you want, press Ctrl+C twice to copy the character, and press Ctrl+V to paste the character. Remote machine files: Select a text or image, press Ctrl+B to copy it, and press Ctrl+G to paste it. NOTE Although using a web browser for O&M allows you to copy and paste a large number of characters without garbled characters, a maximum of 80,000 characters can be copied from the local to the remote, and a maximum of 1000,000 of bytes can be copied from the remote to the local.
Resolution	You can switch the resolution of the current operation interface. During the switching, a new connection is created.

Parameter	Description
Switch to remote mouse	You can switch over between the local mouse and remote mouse.
Windows	This Windows icon can be used for easy access to Windows system functions.
Ctrl+Alt+Delete	Ctrl+Alt+Delete
Copy window	You can copy the current session window.
Full screen	Displays the window in full screen.

Step 4 Invite other system users to participate in the current session. For details, see [Cooperation](#).

1. Click **Cooperation**. The collaborative session window is displayed.
2. Click **Share**. Complete the information in the displayed **Invite friends** dialog box.

Figure 10-15 Collaboration session page of the inviter



NOTE

The link can be copied and sent to multiple users.

3. Copy the URL and send it to the user who has permissions for accounts managed in CBH.
4. Log in to the CBH system as the invited user, open a new browser window, and paste the session link.
5. If you are invited, click **Enter** to join the session.

Table 10-6 Parameters for session operation

Parameter	Description
Apply for control	The invited user can apply for control from the invitation sender. Once approved, the invited user can control the current session.
Exit session	Exit the current session.

Step 5 Upload files to or download files from the host or host net disk. For details, see [File Transfer](#).

Click **File Transfer** to manage files or folders on the personal net disk.

Step 6 In the file management area, manage files or folders on the host or host net disk.


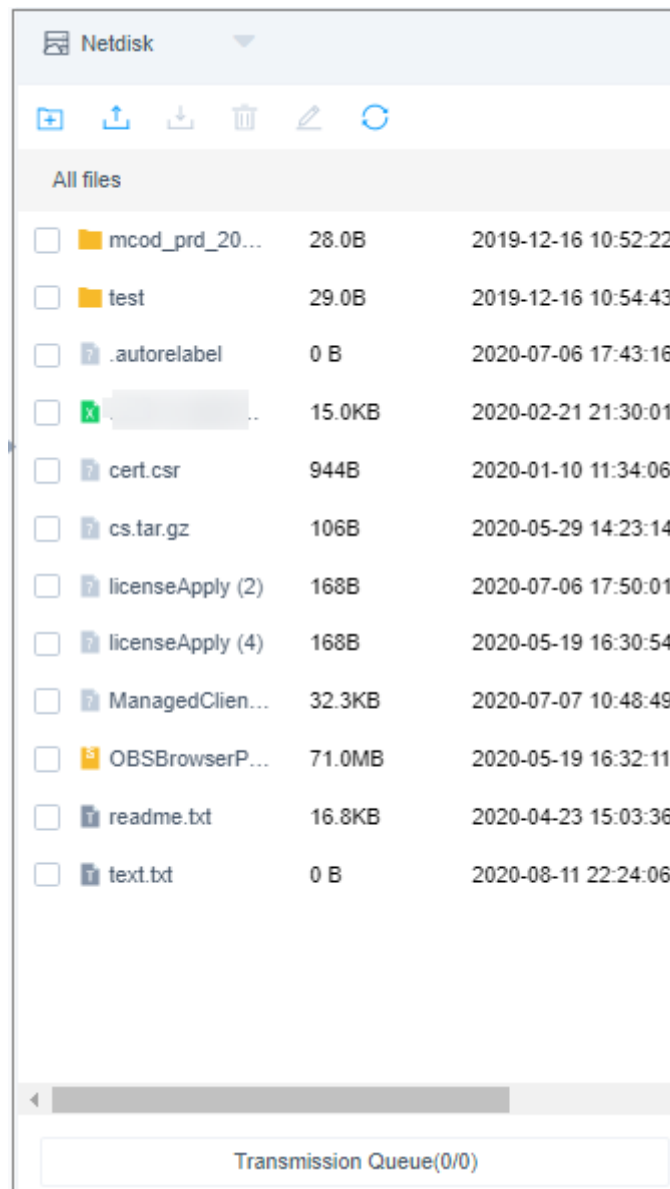



1. Click **File Transfer**. The **File Transfer** window is displayed.
2. Click  to create a folder.

Figure 10-16 New folder



3. Select one or more files or folders and click  to delete them.
4. Select a file or folder and click  to edit its name.
5. Click  to refresh all file directories.

----End

10.3 Script Management

10.3.1 Creating a Script

CBH gives you the ability to manage scripts. You can execute scripts to perform complicated or repetitive operation tasks, improving O&M efficiency. CBH allows you to compile scripts online or import scripts by file.

This topic describes how to create a script.

 **NOTE**

HSS-Agent automatic download and installation scripts have been built-in CBH.

Constraints

- Script management is available only in the CBH professional editions.
- Currently, you can manage Python and Shell scripts with CBH.
- Your scripts can be managed by yourself, administrator, or department administrator.

Prerequisites

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

Procedure

- Step 1** Log in to the CBH system.
- Step 2** Choose **Operation > Script** to go to the script management page.
- Step 3** Click **New** in the upper right corner of the page.
- Step 4** In the displayed **New Script** dialog box, configure the basic information about the script.

Table 10-7 Script information parameters

Parameter	Description
Source	The script content source. This parameter can be set to Edit online or From file . <ul style="list-style-type: none"> • Edit online: indicates that you can edit the script information online to form your script. • From file: indicates that you can import an offline script file to form your script. The file cannot exceed 5 MB in size.
Department Name	Department to which the host resource belongs.
Name	Name of the script. For a user-defined script rule, the script name must be unique in the system. NOTE For the script imported by file, the name is automatically filled based on the name of the imported file.
Remarks	Brief script description

- Step 5** Click **OK**. The system returns to the script list page, and you can view the information about the new script.

----End

Follow-up Operations

After creating an online edited script, you can edit the script online on the script details page. For more details, see [Viewing and Modifying Script Information](#).

10.3.2 Viewing and Editing Script Information

This topic describes how to view and modify script online.

Constraints

If a script exceeds 128 KB, you cannot view the script online. You can download the script to your local PC by referring to [Downloading a Script](#).

Prerequisites

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

Procedure

- Step 1** Log in to the CBH system.
- Step 2** Choose **Operation** > **Script** to go to the script management page.
- Step 3** Query a script.
 - Quick search
Enter a keyword in the search box and search for scripts by name.
 - Advanced search
Enter keywords in the corresponding attribute search boxes to search for scripts in exact mode.
- Step 4** Click the name of the script you want to modify or locate the row where the script locates and click **Manage** in the **Operation** column.

Figure 10-17 Script details page

test	
Basic Info	
Name:	test
Department:	
Size:	0B
Remarks:	-
Creator:	admin
Created Time:	2021-04-26 15:02:04
Modifier:	-
Modified Time:	-
Script content	

Step 5 On the displayed script details page, view and edit basic information of the script.
In the **Basic Info** area, click **Edit**. In the displayed dialog box, edit the script details.
You can edit the script **Name** and **Remarks**.

Step 6 View and modify script content.

In the **Script content** area, click **Edit**. In the displayed dialog box, edit the script content.

----End

10.3.3 Downloading a Script

This topic describes how to download a script for local query and management.

Prerequisites

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

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **Operation > Script** to go to the script management page.

Step 3 Select the script you want to download and click **Download** in the **Operation** column to download the script.

----End

10.3.4 Deleting a Script

This topic describes how to delete an online script and manage the scripts.

Prerequisites

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

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **Operation > Script** to go to the script management page.

Step 3 Delete a department.

1. Select the script you want to delete and click **Delete** in the **Operation** column.
2. In the displayed dialog box, click **OK**.

Step 4 Delete departments in batches.

Select multiple scripts at a time and click **Delete** at the bottom of the script list to delete all selected scripts together.

----End

10.4 Fast O&M

10.4.1 Managing Command Operation Tasks

CBH gives you the ability to manage multiple resources concurrently by executing commands, improving O&M efficiency. You can execute the same command on multiple host resources that use the SSH protocol through one task, and the corresponding execution results are returned accordingly.

This topic describes how to manage command tasks, including creating, executing, and stopping command tasks, and viewing task execution results.

Constraints

- Fast operation is available only in the CBH professional editions.
- Fast operation tasks apply only to Linux hosts using the SSH protocol.
- Currently, Fast operation tasks cannot be performed on Windows host, database, or application resources.

Prerequisites

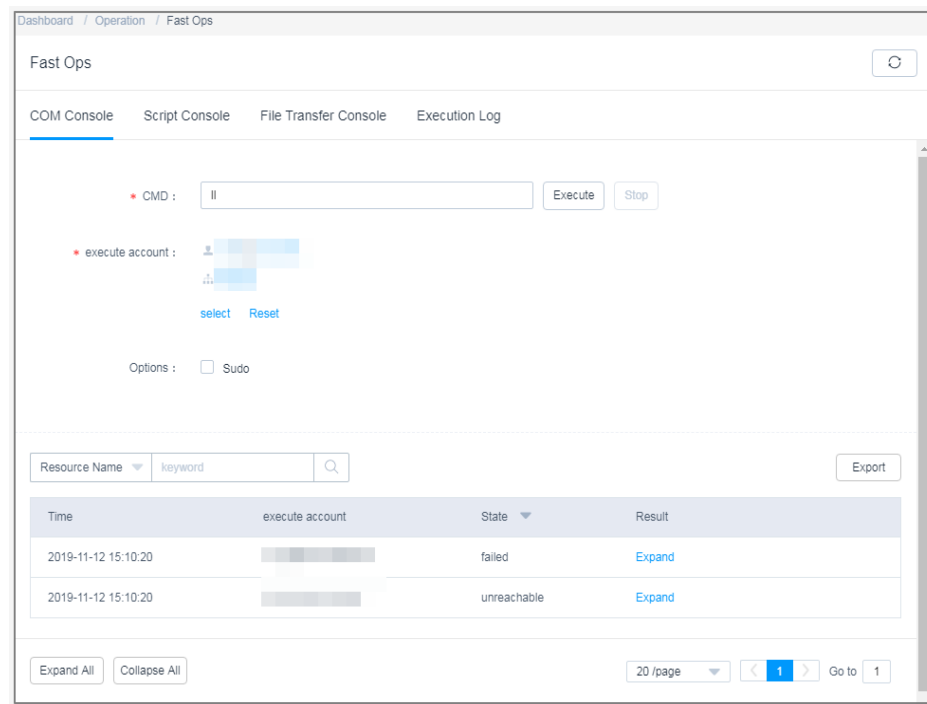
- You have the management permissions for the **Fast Ops** module.
- You have obtained the access permissions for the resources.
- The network connections between the managed hosts and the CBH system are normal.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **Operation > Fast Ops > COM Console** to go to the quick command OM page.

Figure 10-18 Command console



Step 3 Configure fast command operation information.

Table 10-8 Fast command operation parameters

Parameter	Description
CMD	Enter the command to be executed for host resources.

Parameter	Description
execute account	<ul style="list-style-type: none"> The managed resource account allowed to execute the script. You can select a created SSH account or account group. You can also Reset the selected account or account group. <p>NOTE You can select a maximum of one account for each resource.</p>
Options	(Optional) If you have no permissions for the selected accounts, select Sudo to escalate your privilege and execute the task under the sudoers file.

Step 4 Execute the command task.

Click **Execute** next to the **CMD** text box to execute the command operation task.

Step 5 Stop the command operation task.

Click **Stop** to stop the task.

 **NOTE**

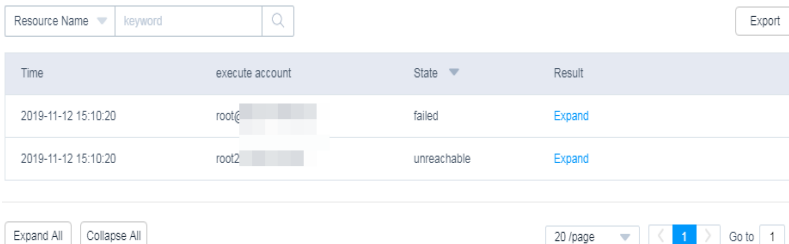
Stopping a task cannot stop the corresponding job that is being executed on a certain resource.

Step 6 View the execution results.

After the command operation task is executed, check the execution results. To view execution results of historical operation tasks, see [Viewing Execution Logs](#)

- In the execution result area, enter a keyword in the search box to quickly query the task execution result by resource name, execution result, or execution account.
- Click **Expand** to view the execution results of the corresponding task.
- Click **Export** to download the corresponding execution logs in CSV format.

Figure 10-19 Command operation task results



Time	execute account	State	Result
2019-11-12 15:10:20	root@	failed	Expand
2019-11-12 15:10:20	root2	unreachable	Expand

----End

10.4.2 Managing Script Operation Tasks

CBH gives you the ability to manage multiple resources concurrently by executing scripts, improving O&M efficiency. You can execute the same script on multiple

host resources that use the SSH protocol through one task, and the corresponding execution results are returned accordingly.

This topic describes how to manage script operation tasks, including creating, executing, and stopping script operation tasks, and viewing task execution results.

Constraints

- Fast operation is available only in the CBH professional editions.
- Fast operation tasks apply only to Linux hosts using the SSH protocol.
- Currently, Fast operation tasks cannot be performed on Windows host, database, or application resources.

Prerequisites

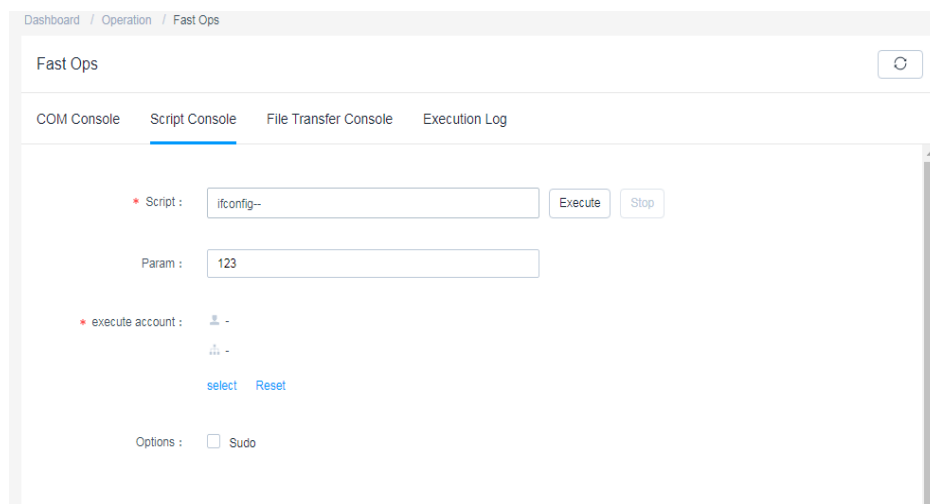
- You have the management permissions for the **Fast Operation** module.
- You have obtained the access permissions for the resources.
- The network connections between the managed hosts and the CBH system are normal.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **Operation > Fast Operation > Script Console** to go to the quick script operation page.

Figure 10-20 Script Console



Step 3 Configure fast script operation information.

Table 10-9 Fast script operation parameters

Parameter	Description
Script	The script to be executed for the host resources. <ul style="list-style-type: none"> You can select the script content in the script management module or upload a new local script file.
Param	(Optional) user-defined script parameter.
execute account	<ul style="list-style-type: none"> The managed resource account allowed to execute the script. You can select a created SSH account or account group. You can also Reset the selected account or account group. <p>NOTE You can select a maximum of one account for each resource.</p>
Options	(Optional) If you have no permissions for the selected accounts, select Sudo to escalate your privilege and execute the task under the sudoers file.

Step 4 Execute the script operation task.

Click **Execute** next to the **Script** text box to execute the script operation task.

Step 5 Stop the script operation task.

Click **Stop** to stop the task.

 **NOTE**

Stopping a task cannot stop the corresponding job that is being executed on a certain resource.

Step 6 View the execution results.

After the script operation task is executed, check the execution results. To view execution results of historical operation tasks, see [Viewing Execution Logs](#)

- In the execution result area, enter a keyword in the search box to quickly query the task execution result by resource name, execution result, or execution account.
- Click **Expand** to view the execution results of the corresponding task.
- Click **Export** to download the corresponding execution logs in CSV format.

----End

10.4.3 Managing File Transfer Tasks

CBH gives you the ability to quickly upload system disk files or local files to paths of multiple managed hosts at a time. You can upload one or more files to multiple hosts with just one file transfer task and the system returns the execution results.

This topic describes how to manage file transfer tasks, including creating, executing, and stopping file transfer tasks, and viewing task execution results.

Constraints

- Fast operation is available only in the CBH professional editions.
- Fast operation tasks apply only to Linux hosts using the SSH protocol.
- Currently, Fast operation tasks cannot be performed on Windows host, database, or application resources.

Prerequisites

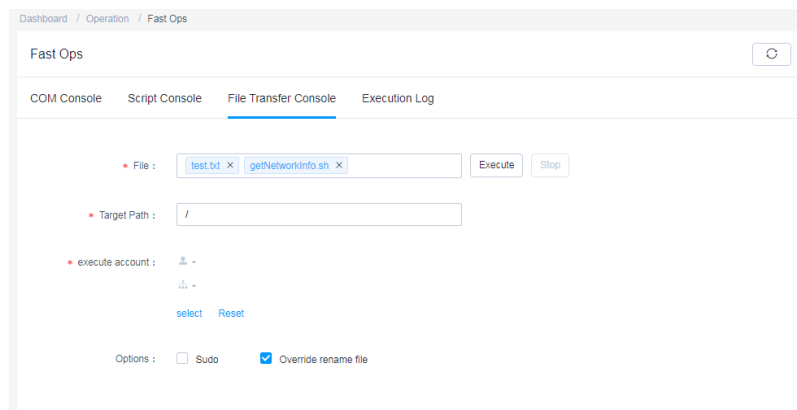
- You have the management permissions for the **Fast Ops** module.
- You have obtained the access permissions for the resources.
- The network connections between the managed hosts and the CBH system are normal.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **Operation > Fast Ops > File Transfer Console** to go to the **File Transfer Console** tab.

Figure 10-21 File Transfer Console



Step 3 Configure fast file transfer information.

Table 10-10 Parameters for fast file transfer

Parameter	Description
File	Files to be transferred. The system disk file is selected by default. You can also upload the local file to the personal net disk and then select the file. A maximum of 10 files can be selected.
Target Path	Absolute path on the host to which files are transferred

Parameter	Description
execute account	<ul style="list-style-type: none"> The managed resource account allowed to execute the script. You can select a created SSH account or account group. You can also Reset the selected account or account group. <p>NOTE You can select a maximum of one account for each resource.</p>
Options	<p>(Optional)</p> <ul style="list-style-type: none"> (Optional) If you have no permissions for the selected accounts, select Sudo to escalate your privilege and execute the task under the sudoers file. Override rename file: If a file with the same name as the file to be uploaded exists in the target path of the destination host, the existing file will be overwritten by the newly uploaded file.

Step 4 Execute the file transfer task.

Click **Execute** next to the **File** text box to execute the file transfer task.

Step 5 Stop the file transfer task.

Click **Stop** to stop the task.

 **NOTE**

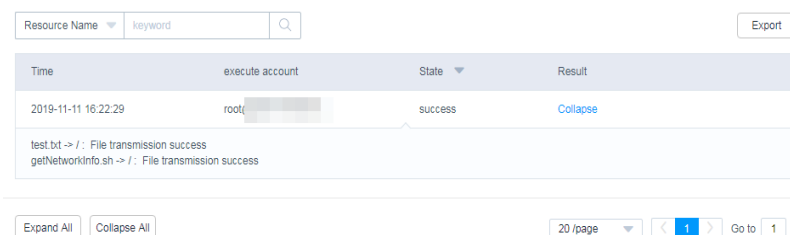
Stopping a task cannot stop the job that is being executed until the job is done.

Step 6 View the execution results.

After the file transfer task is executed, check the execution results. To view execution results of historical operation tasks, see [Viewing Execution Logs](#)

- In the execution result area, enter a keyword in the search box to quickly query the task execution result by resource name, execution result, or execution account.
- Click **Expand** to view the execution results of the corresponding task.
- Click **Export** to download the corresponding execution logs in CSV format.

Figure 10-22 File transfer task results



----End

10.4.4 Managing Fast Operation Task Execution Logs

This topic describes how to manage execution logs after fast operation tasks are executed, including viewing task details, exporting execution logs, and deleting execution logs.

Prerequisites

- You have the management permissions for the **Fast Operation** module.
- Fast operation tasks (including fast command tasks, script tasks, and file transfer tasks) have been executed.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **Operation** > **Fast Operation** > **Execution Log** to go to the **Execution Log** tab.

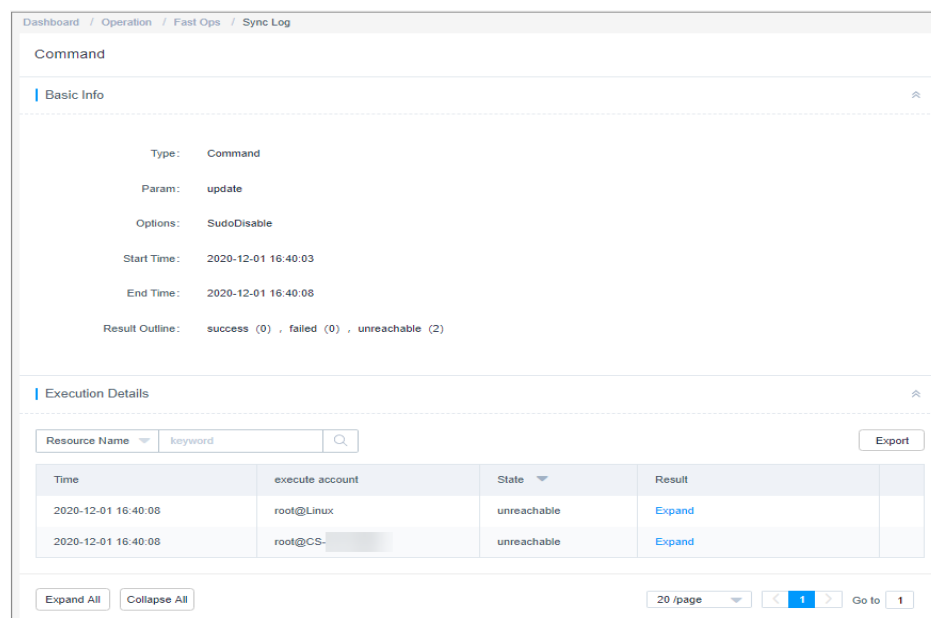
Step 3 Query logs.

Enter a keyword in the search box and search for execution logs by execution parameter.

Step 4 View execution log details.

1. Select the execution log you want to view and click **Detail**.

Figure 10-23 Execution log details



2. In the **Basic Info** area, view the basic information and brief result of the operation task.
3. In the **Execution Details** area, view the detailed execution result of the operation task.
4. In the **Execution Details** area, click **Export** to export the detailed execution result of the operation task.

Step 5 Download execution logs.

Select the execution log and click **Download** in the **Operation** column to download the log in CSV format.

Step 6 Delete execution logs.

- To delete one execution log, select the one you want and click **Delete** in the **Operation** column of the corresponding row to delete it.
- To delete multiple execution logs at a time, select the ones you want and click **Delete** at the bottom of the list to delete the selected logs together.

----End

10.5 OM Task

10.5.1 Creating an OM Task

CBH allows you to create OM tasks that will be automatically executed. After you create an OM task, the system automatically executes the task according to task steps, task types, resources, and execution mode you configure. For example, you can create an OM task to upload system disk files or local files to multiple designation hosts. With the fast OM function, CBH automatically executes OM tasks based on your configured execution period and time. In addition, it can automatically execute multiple types of tasks concurrently on multiple devices, improving the OM efficiency.

- Multiple OM tasks can be concurrently performed step by step on multiple resources that use the SSH protocol, including command, script, and file transfer OM tasks.
- After an operation task is submitted, the system automatically performs operations in sequence and returns the execution result.

Constraints

- Fast operation is available only in the CBH professional editions.
- Automated operation tasks can be executed only on Linux host resources that use the SSH protocol.
- Currently, automated operation tasks cannot be performed on Windows host, database, or application resources.
- Operation tasks created by you can be managed only by yourself and cannot be managed by other system users.

Prerequisites

- You have the management permissions for the **OM Task** module.
- You have obtained the access permissions for the resources.
- The network connections between the managed hosts and the CBH system are normal.

Creating an Automated Operation Task

- Step 1** Log in to the CBH system.
- Step 2** Choose **Operation > OM Task > Task**.
- Step 3** Click **New** in the upper right of the **OM Task** area.
- Step 4** Configure basic information about the task.

Table 10-11 Basic task information parameters

Parameter	Description
Task Name	Name of the task. The value of Task Name must be unique in the system.
Timing	Execution mode of the operation task. The options are Manual , Scheduled , and Cycle . You need to configure the execution time if Fixed-Time or Cycle is selected. <ul style="list-style-type: none"> • Manual: indicates that you need to manually start the task. • Fixed-Time: indicates that the task will start at the specified time. This type of rule is executed only once. • Cycle: indicates that the task will start periodically at the specified interval. This type of password change rule is triggered periodically.
Execute Time	Date when the task is periodically executed. The default execution time is at 00:00 every day.
Cycle Frequency	Task execution frequency. <ul style="list-style-type: none"> • The options are every minute, every hour, every day, every week, and every month. • Set the End Time for this type of tasks. Otherwise, the tasks will be executed periodically forever.
Options	(Optional) If you have no permissions for the selected accounts, select Sudo to escalate your privilege and execute the task under the sudoers file.
Remarks	Brief description of the operation task.

Step 5 Click **Next** and start to configure execution accounts or account groups.

Step 6 Click **Next** and set task steps.

1. Click **Add Step** and select **Command**, **Script**, or **Transfer File**.
2. Select one or more task types and set task parameters.

 **NOTE**

Multiple steps can be added to an operation task.

Step 7 Click **OK**. The system returns to the task list page, and you can view the information about the new operation task.

You can [download the execution logs](#) to obtain the task execution results.

----End

Follow-up Operations

On the **OM Task** page, you can manage all created OM tasks, including managing related execution accounts and deleting, enabling, or disabling OM tasks.

- To quickly relate an OM task to more accounts, select the task and click **Relate** in the **Operation** column.
- To delete an OM task, select the task and click **Delete** in the **Operation** column.
- To disable a periodic OM task, select the enabled ones and click **Disable** at the bottom of the list. When the status of those tasks changes to **Disabled**, they are hibernated.
- To execute an OM task, click **Execute** in the **Operation** column.

NOTE

During the task execution, task steps are performed in sequence. When a task step is interrupted or the selected resource is unreachable, the subsequent task steps will be stopped.

10.5.2 Querying and Modifying OM Tasks

You can edit steps in an OM task anytime you want to meet your changed requirements. You can view and edit task configuration, including the basic task settings, task steps, as well as execution date, period, and account or account group.

Prerequisites

- You have the management permissions for the **OM Task** module.
- You have obtained the access permissions for the resources.

Querying and Editing Task Configurations

Step 1 Log in to the CBH system.

Step 2 Choose **Operation > OM Task > Task**.

Step 3 Query OM tasks.

- Quick search
Enter a keyword in the search box to quickly query tasks by task name, resource name, and execution account.
- Advanced search
Enter keywords in the corresponding attribute search boxes to search for tasks in exact mode.

Step 4 Click the name of the task or click **Manage** in the **Operation** column of the task row.

- Step 5** On the displayed OM task details page, view and edit basic information.
- In the **Basic Info** area, click **Edit**. In the displayed dialog box, edit the details.
- You can edit **Task Name** and **Timing**.
- Step 6** On the displayed OM task details page, view and edit basic information of the execution account.
- To add or delete an execution account, click **Edit** in the **Execute Account** area and complete modifications in the displayed dialog box.
 - To only remove an execution account, click **Remove** in the row of the execution account. The removed account then cannot be to execute the OM tasks on the corresponding host.
- Step 7** In the displayed dialog box, view and edit basic information of the execution account.
- To add or delete an execution account group, click **Edit** in the **Execute Account Group** area and complete modifications in the displayed dialog box.
 - To only remove an execution account group, click **Remove** in the row of the execution account group. Each account in the removed account group cannot be used for executing OM tasks on the corresponding host.
- Step 8** In the displayed OM task dialog box, view and edit task steps.
- In the **Task Step** area, click **Add**. In the displayed **Add Step** dialog box, add one or more task steps as needed.
 - To modify an added task step, click **Edit** in the row of the corresponding step and complete modifications in the then displayed dialog box.
 - To only remove a task step, click **Remove** in the row of the task step. The removed task step will no longer be executed in the OM task.
- Step 9** View the execution history of an OM task in the **History** area.
- To view the execution details of an OM task, click **View** in the **Operation** column of the corresponding row of the OM task.
 - To download execution details, click **Export** in the **Operation** column of the corresponding row of the OM task.

----End

10.5.3 Managing OM Task Execution Logs

After an OM task is executed, an execution log is generated. You can view the task execution result in the log, including the execution results and details.

This topic describes how to manage execution logs, including viewing, downloading, and deleting execution logs.

Prerequisites

You have the management permissions for the **OM Task** module.

Viewing Log Details

- Step 1** Log in to the CBH system.

Step 2 Choose **Operation > OM Task > Execution Log** to go to the task list page.

Step 3 Query OM task execution logs.

Quick search: Enter a keyword in the search box and search for O&M tasks by task name.

Step 4 Select the task you want and click **Detail** in the **Operation** column.

- In the **Basic Info** area, view the basic information and brief result of the operation task.
- In the **Execution Details** area, view and export the detailed execution result of the OM task.

----End

Downloading OM Task Execution Logs

Step 1 Log in to the CBH system.

Step 2 Choose **Operation > OM Task > Execution Log** to go to the task list page.

Step 3 Select the task you want and click **Download** in the **Operation** column to download the execution log in CSV format.

Step 4 Click **View** to go to the task details page.

You can view the basic information and brief execution result of an operation task. In the execution details area, you can view and export the detailed execution result of an operation task.

Step 5 Click **Export** to download the current execution log file in CSV format to the local computer.

Step 6 To delete one execution log, select the one you want and click **Delete** in the **Operation** column to delete it.

To delete multiple execution logs at a time, select the ones you want and click **Delete** at the bottom of the list to delete the selected logs together.

----End

Deleting Execution Logs

Step 1 Log in to the CBH system.

Step 2 Choose **Operation > OM Task > Execution Log** to go to the task list page.

Step 3 To delete on task logs, select the one you want and click **Delete** in the **Operation** column to delete it.

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

----End

11 Audit

11.1 Live Session

11.1.1 Viewing Live Sessions

After a system user logs in to a resource through CBH, you, the audit administrator, will receive session records in real time. It enables you to view and audit live operation sessions to prevent losses caused by violations.

This topic walks you through how to query and view live sessions.

Prerequisites

- You have the management permissions for the **Live Session** module.
- There is at least one live session.

Procedure

Step 1 Log in to the CBH system.

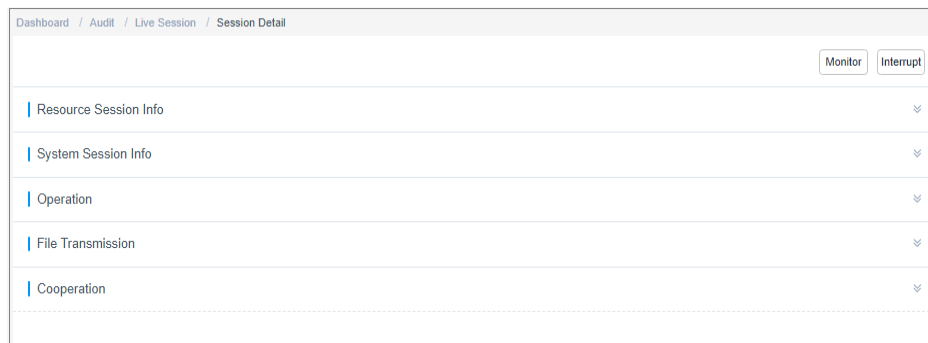
Step 2 Choose **Audit > Live Session**.

Step 3 Query live sessions.

- Quick search
Enter a keyword in the search box to quickly query live sessions by resource name, account, user, or source IP.
- Advanced search
Enter keywords in the corresponding attribute search boxes to search for live sessions in exact mode.

Step 4 Click **Detail** in the **Operation** column of the live session you want to view.

Figure 11-1 Viewing Live Sessions



Step 5 View resource session information, system session information, operation records, file transmission records, and collaborative session records.

----End

11.1.2 Monitoring Live Sessions

After a system user logs in to a resource through CBH, you, the audit administrator, will receive session records in real time. You can monitor live sessions to audit real-time operations of other system users.

This topic describes how to monitor OM operations in live sessions.

Prerequisites

- You have the management permissions for the **Live Session** module.
- There is at least one live session.
- Currently, only H5 O&M sessions and SSH client sessions are supported.

Procedure

Step 1 Log in to the CBH system.

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

Step 3 Click **Monitor** in the **Operation** column of the live session you want to monitor. The OM session window is visible to you.

Step 4 In the displayed session window, view real-time operations, historical OM operations, file transmission records, and participant records of the session.

----End

11.1.3 Interrupting a Live Session

After a system user logs in to a resource through CBH, you, the audit administrator, will receive session records in real time. When discovering violations or high-risk operations, you can interrupt the session to prevent the system user from performing further operations.

This topic describes how to interrupt live sessions.

Prerequisites

- You have the management permissions for the **Live Session** module.
- There is at least one live session.

Procedure

Step 1 Log in to the CBH system.

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

Step 3 Click **Interrupt** in the **Operation** column of the session to forcibly disconnect the session.

After the session is interrupted, the session window is immediately disconnected and the system user receives a message indicating that the session is interrupted.

----End

11.2 History Session

11.2.1 Viewing History Sessions

After an operation ends, you, the audit administrator, will receive history session records. It makes easy for you to query detailed operation records and audit historical sessions online.

Constraints

- Text and video audit are available for operations performed through a web browser.
- For O&M operations, file transfer, and database operations through an SSH client, video audit is unavailable.
- Details about **account verification** for accessing managed resources will not be recorded.
- Only valid session logs can be played. Valid session logs start when you initiate a session and end when the last operation is completed.

Prerequisites

- You have the management permissions for the **History Session** module.
- The OM session has finished.

Viewing History Sessions

Step 1 Log in to the CBH system.

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

Figure 11-2 History Session

Resource	Protocol	Account	User	Source IP	Start/End Time	Duration	End State	Operation
ManageOne-S...	SSH	sopuser	admin	1	03-25-2024 21:20:16 ~ 0...	00:10:03	Normal	Detail Play Download
ManageOne-S...	SSH	sopuser	admin	1	03-25-2024 21:15:53 ~ 0...	00:10:35	Normal	Detail Play Download
ManageOne-S...	SSH	sopuser	admin	1	03-25-2024 21:15:38 ~ 0...	00:00:06	Normal	Detail Play Download
ManageOne-S...	SSH	sopuser	admin	1	03-25-2024 20:25:21 ~ 0...	00:00:01	Normal	Detail Play Download
ManageOne-S...	SSH	sopuser	admin	1	03-25-2024 20:12:22 ~ 0...	00:10:03	Normal	Detail Play Download

NOTE

The **More** operation in the **Details** column is removed from CBH V3.3.42.0 or later versions.

Step 3 Query history sessions.

- Quick search
Enter a keyword in the search box to quickly query history sessions by resource name, account, user, or source IP.
- Advanced search
Enter keywords in the corresponding attribute search boxes to search for history sessions in exact mode.

Step 4 Click **Detail** in the **Operation** column of the history session you want to view.

Figure 11-3 Viewing History Sessions

Linux	
Resource Session Info	⌵
System Session Info	⌵
Operation	⌵
File Transmission	⌵
Session Cooperator	⌵

Step 5 View resource session information, system session information, operation records, file transmission records, and collaborative session records.

For a history session, you can view the resource name, type, host IP address, account, start and end time, session duration, session size, operation user, source IP address and MAC address of the operation user, login mode, operation records, file transfer records, and session collaboration records.

----End

Online Playback of History Session

NOTE

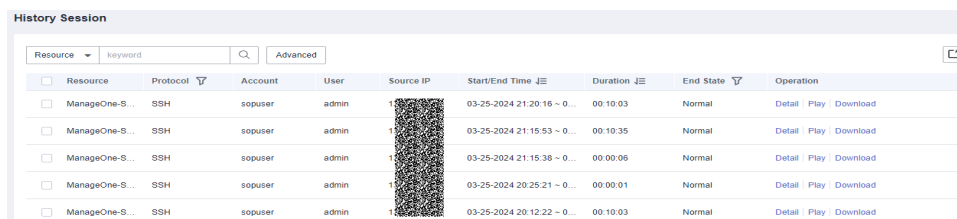
The total duration and playable duration of a downloaded video file may be different because the logout time and last operation time are different.

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

Step 1 Log in to the CBH system.

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

Figure 11-4 History Session



Resource	Protocol	Account	User	Source IP	Start/End Time	Duration	End State	Operation
ManageOne-S...	SSH	sopuser	admin	1	03-25-2024 21:20:16 - 0...	00:10:03	Normal	Detail Play Download
ManageOne-S...	SSH	sopuser	admin	1	03-25-2024 21:15:53 - 0...	00:10:35	Normal	Detail Play Download
ManageOne-S...	SSH	sopuser	admin	1	03-25-2024 21:15:36 - 0...	00:00:05	Normal	Detail Play Download
ManageOne-S...	SSH	sopuser	admin	1	03-25-2024 20:25:21 - 0...	00:00:01	Normal	Detail Play Download
ManageOne-S...	SSH	sopuser	admin	1	03-25-2024 20:12:22 - 0...	00:10:03	Normal	Detail Play Download

NOTE

The **More** operation in the **Details** column is removed from CBH V3.3.42.0 or later versions.

Step 3 Click **Play** in the **Operation** column of the historical session you want to audit.

Step 4 Play the video recording the entire session operation process.

- In the session window, check the total duration and drag the playback progress bar as needed.
- In the right pane of the session window, you can view information such as operation instructions, file transfer records, participants of the session, and join a live session to monitor the participants.

Step 5 Skip idle playback.

- If **Skip Idle** is enabled, only the content containing the session operations is played.
- This function is disabled by default.


Step 6 Control playback speed as needed.

Click **1X** and select a playback speed. You can select **1X**, **2X**, **4X**, **8X**, or **16X**.

Step 7 Take a quick screenshot of the session.

Click  to generate a screenshot in .png format.

Step 8 Query the playlist.

1. Click  to expand the playlist on the right of the session window. Then you can select a history session to play its video.
2. Enter a login name or account name in the search box to search for a historical session.

3. Click the target session to play its video immediately.

Figure 11-5 History session playback list

keyword
Operator: admin Start: 2020-09-29 14:53:53 End: 2020-09-29 14:53:57 Account: root@Linux
Operator: admin Start: 2020-08-05 16:05:29 End: 2020-08-05 17:44:55 Account: root@CS-CHH
Operator: admin Start: 2020-06-17 15:27:43 End: 2020-06-17 16:03:42 Account: root@Linux
Operator: admin Start: 2020-05-25 15:46:34 End: 2020-05-25 18:11:58 Account: root@tank
Operator: admin Start: 2020-05-14 15:09:59 End: 2020-05-14 16:39:28 Account: root@Linux
Operator: admin Start: 2020-05-14 14:31:55 End: 2020-05-14 16:39:28 Account: admin@127
Operator: admin Start: 2019-12-13 09:33:46 End: 2019-12-13 09:42:36 Account: sysuser@127

----End

11.2.2 Exporting History Session Records

CBH allows you to export all history session records for offline audit.

Prerequisites

- You have the management permissions for the **History Session** module.
- The OM session has finished.

Procedure

- Step 1** Log in to the CBH system.
- Step 2** Choose **Audit > History Session**.

Figure 11-6 History Session

Resource	Protocol	Account	User	Source IP	Start/End Time	Duration	End State	Operation
ManageOne-S...	SSH	sopuser	admin	10.0.0.1	03-25-2024 21:20:16 ~ 0...	00:10:03	Normal	Detail Play Download
ManageOne-S...	SSH	sopuser	admin	10.0.0.1	03-25-2024 21:15:53 ~ 0...	00:10:35	Normal	Detail Play Download
ManageOne-S...	SSH	sopuser	admin	10.0.0.1	03-25-2024 21:15:38 ~ 0...	00:00:06	Normal	Detail Play Download
ManageOne-S...	SSH	sopuser	admin	10.0.0.1	03-25-2024 20:25:21 ~ 0...	00:00:01	Normal	Detail Play Download
ManageOne-S...	SSH	sopuser	admin	10.0.0.1	03-25-2024 20:12:22 ~ 0...	00:10:03	Normal	Detail Play Download

NOTE

The **More** operation in the **Details** column is removed from CBH V3.3.42.0 or later versions.

- Step 3** (Optional) Select one or more history session logs.
If no log is selected, all historical session logs are exported by default.
- Step 4** Click **Export** in the upper right corner to download the CSV file.

----End

11.2.3 Managing Session Videos

After an operation ends, you, the audit administrator, will receive history session records. So, you can audit operation commands on Linux hosts and operations on Windows hosts. You can also generate, download, or delete operation videos for different audit purposes.

Constraints

- Text and video audit are available for operations performed through a web browser.
- For O&M operations, file transfer, and database operations through an SSH client, video audit is unavailable.
- Only valid session logs can be played. Valid session logs start when you initiate a session and end when the last operation is completed.
- Session videos are cached in the CBH system space. You are advised to move the video to a local computer in a timely manner and clear the system disk space.

Prerequisites

- You have the management permissions for the **History Session** module.
- The OM session has finished.

Generating Session Videos

Step 1 Log in to the CBH system.

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

Figure 11-7 History Session

Resource	Protocol	Account	User	Source IP	Start/End Time	Duration	End State	Operation
ManageOne-S...	SSH	sopuser	admin	192.168.1.1	03-25-2024 21:20:16 ~ 0...	00:10:03	Normal	Detail Play Download
ManageOne-S...	SSH	sopuser	admin	192.168.1.1	03-25-2024 21:15:53 ~ 0...	00:10:35	Normal	Detail Play Download
ManageOne-S...	SSH	sopuser	admin	192.168.1.1	03-25-2024 21:15:36 ~ 0...	00:00:06	Normal	Detail Play Download
ManageOne-S...	SSH	sopuser	admin	192.168.1.1	03-25-2024 20:25:21 ~ 0...	00:00:01	Normal	Detail Play Download
ManageOne-S...	SSH	sopuser	admin	192.168.1.1	03-25-2024 20:12:22 ~ 0...	00:10:03	Normal	Detail Play Download

NOTE

The **More** operation in the **Details** column is removed from CBH V3.3.42.0 or later versions.

Step 3 In the **Operation** column of a history session, choose **More > Generate Video**. The system starts generating a video for the session.

The task center displays a message indicating that a task is being executed. After the task is finished, a notification is sent to you through the message center indicating that the session video is generated.

NOTE

- If the CBH system storage space is abundant, the video duration and size are not limited.
- If the system storage space is insufficient, the video may fail to be generated.
- Session recordings can be backed up to OBS buckets. For details, see [Configuring OBS Buckets for Remote Log Backup](#).

----End

Downloading a Session Video

After a video is generated, it is cached in the system and occupies the system storage space. To save system storage space, download videos and save them locally.

Step 1 Log in to the CBH system.

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

Figure 11-8 History Session

Resource	Protocol	Account	User	Source IP	Start/End Time	Duration	End State	Operation
ManageOne-S...	SSH	sopuser	admin	10.10.10.10	03-25-2024 21:20:16 ~ 0...	00:10:03	Normal	Detail Play Download
ManageOne-S...	SSH	sopuser	admin	10.10.10.10	03-25-2024 21:15:53 ~ 0...	00:10:35	Normal	Detail Play Download
ManageOne-S...	SSH	sopuser	admin	10.10.10.10	03-25-2024 21:15:36 ~ 0...	00:00:06	Normal	Detail Play Download
ManageOne-S...	SSH	sopuser	admin	10.10.10.10	03-25-2024 20:25:21 ~ 0...	00:00:01	Normal	Detail Play Download
ManageOne-S...	SSH	sopuser	admin	10.10.10.10	03-25-2024 20:12:22 ~ 0...	00:10:03	Normal	Detail Play Download

NOTE

The **More** operation in the **Details** column is removed from CBH V3.3.42.0 or later versions.

Step 3 In the **Operation** column of the history session recording you want to download, click **Download** to download it.

After the video is downloaded, a notification is sent to you through the message center.

NOTE

To playback a session recording in a compressed package, perform the following steps:

1. Download the **local player tool** by referring to [Download Center](#).
2. Open the local player tool and drag the downloaded package to the playback window.

----End

11.3 System Logs

11.3.1 Querying System Logs

After a system user logs in to the CBH system and perform operations such as permission configuration and audit management, you, the audit administrator, will receive system log records. You can query detailed login and operation records in the CBH system and audit system logs online. System logs include system login logs and system operation logs.

Prerequisites

You have the management permissions for the **System Logon** or **System Operation** module under **System Log**.

Querying System Logon Logs

Step 1 Log in to the CBH system.

Step 2 Choose **Audit > System Log > System Logon** to switch to the system log page.

NOTE

In system operation logs, O&M task results record whether O&M tasks are complete. System logs do not include the execution results of specific commands or scripts in an O&M task.

Step 3 Query login logs.

- Quick search
Enter a keyword in the search box to quickly query system logon logs by user, source IP address, start time, end time, and log content.
- Advanced search
Enter keywords in the corresponding attribute search boxes to search for system login logs in exact mode.

Step 4 View the login logs in the search result.

----End

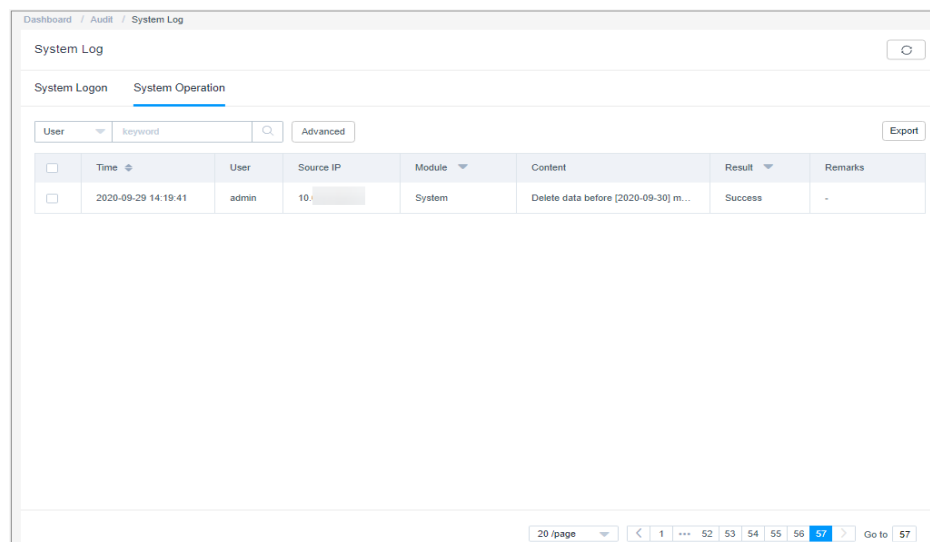
Viewing System Operation Logs

Step 1 Log in to the CBH system.

Step 2 Choose **Audit > System Log** to go to the system log page.

Step 3 Click the **System Operation** tab.

Figure 11-9 System operation logs



The screenshot shows the 'System Log' interface with the 'System Operation' tab selected. It features a search bar with 'keyword' and an 'Advanced' search option. Below the search bar is a table with the following data:

<input type="checkbox"/>	Time	User	Source IP	Module	Content	Result	Remarks
<input type="checkbox"/>	2020-09-29 14:19:41	admin	10.1.1.1	System	Delete data before [2020-09-30] m...	Success	-

At the bottom of the page, there is a pagination control showing '20 /page' and a 'Go to 57' button.

Step 4 Query operation logs.

- Quick search
Enter a keyword in the search box to quickly query operation logs by user, source IP address, start time, end time, and log content.
- Advanced search
Enter keywords in the corresponding attribute search boxes to search for operation logs in exact mode.

Step 5 View the operation logs in the search result.

----End

11.3.2 Exporting System Logs

After a system user logs in to the CBH system and perform operations such as permission configuration and audit management, you, the audit administrator, will

receive system log records. You can query detailed login and operation records in the CBH system and audit system logs online. System logs include system login logs and system operation logs.

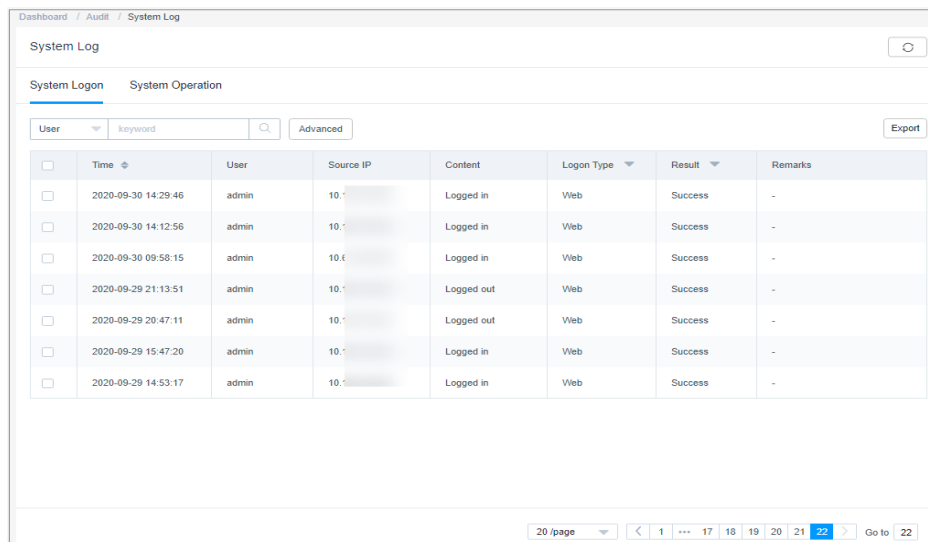
Prerequisites

You have the management permissions for the **System Logon** or **System Operation** module under **System Log**.

Exporting System Logon Logs

- Step 1** Log in to the CBH system.
- Step 2** Choose **Audit > System Log** to go to the system log page.
- Step 3** In the **System Logon** tab, click **Export** in the upper right corner to export system logon logs.

Figure 11-10 System logon logs



The screenshot shows the 'System Log' interface with the 'System Logon' tab selected. It features a search bar with 'User' and 'keyword' dropdowns, an 'Advanced' search option, and an 'Export' button. Below is a table with columns: Time, User, Source IP, Content, Logon Type, Result, and Remarks. The table contains seven rows of logon records for the user 'admin'.

<input type="checkbox"/>	Time	User	Source IP	Content	Logon Type	Result	Remarks
<input type="checkbox"/>	2020-09-30 14:29:46	admin	10.0.0.1	Logged in	Web	Success	-
<input type="checkbox"/>	2020-09-30 14:12:56	admin	10.0.0.1	Logged in	Web	Success	-
<input type="checkbox"/>	2020-09-30 09:58:15	admin	10.0.0.1	Logged in	Web	Success	-
<input type="checkbox"/>	2020-09-29 21:13:51	admin	10.0.0.1	Logged out	Web	Success	-
<input type="checkbox"/>	2020-09-29 20:47:11	admin	10.0.0.1	Logged out	Web	Success	-
<input type="checkbox"/>	2020-09-29 15:47:20	admin	10.0.0.1	Logged in	Web	Success	-
<input type="checkbox"/>	2020-09-29 14:53:17	admin	10.0.0.1	Logged in	Web	Success	-

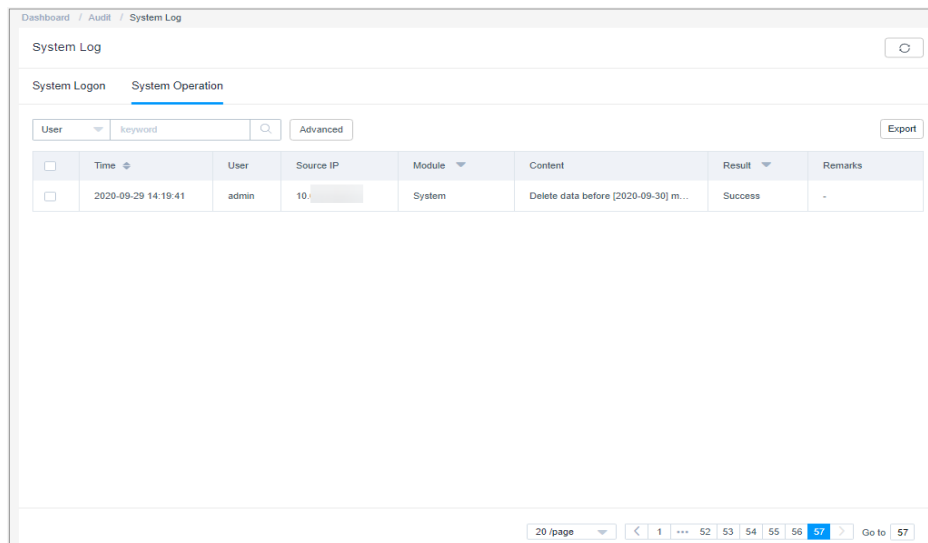
- Step 4** (Optional) Select one or more login logs.
If no log is selected, all login logs are exported by default.
- Step 5** Click **Export** in the upper right corner to download the CSV file.

----End

Exporting System Operation Logs

- Step 1** Log in to the CBH system.
- Step 2** Choose **Audit > System Log** to go to the system log page.
- Step 3** Click the **System Operation** tab.

Figure 11-11 System operation logs



The screenshot shows a web interface for viewing system logs. At the top, there are tabs for 'System Logon' and 'System Operation', with 'System Operation' selected. Below the tabs is a search bar with a 'User' dropdown, a 'keyword' input field, and an 'Advanced' button. An 'Export' button is located in the top right corner. The main area contains a table with the following columns: 'Time', 'User', 'Source IP', 'Module', 'Content', 'Result', and 'Remarks'. A single log entry is visible with the following details:

Time	User	Source IP	Module	Content	Result	Remarks
2020-09-29 14:19:41	admin	10....	System	Delete data before [2020-09-30] m...	Success	-

At the bottom of the interface, there is a pagination control showing '20 /page' and a set of page numbers from 1 to 57, with page 57 highlighted.

Step 4 (Optional) Select one or more operation logs.

If no log is selected, all operation logs are exported by default.

Step 5 Click **Export** in the upper right corner to download the CSV file.

----End



11.4 Operation Report

11.4.1 Viewing Operation Reports

As the audit administrator, you can view and export detailed operation reports, including the **Operation Stat**, **Logon Stat**, **Duration Stat**, **SrcIP Stat**, **Cooperation Stat**, **Approval Stat**, **Interception Stat**, **Command Stat**, and **File Stat** graphs.

Constraints

- Operation statistics for a maximum of 180 consecutive days can be viewed.
 - By default, the operation data of the current day is displayed by the hour.
 - If the time range you select falls into a week of a month, the operation data is displayed by the day.
 - If the time range you select falls into a week spanning different months, the operation data can be displayed by the day or by the month.
 - If the time range you select spans different weeks of a month, the operation data can be displayed by the day or by the week.
 - If the time range you select spans different weeks of different months, the operation data can be displayed by the day, by the week, or by the month.
- You can view operation statistics in line, bar, or pie charts.

- : indicates statistics will be displayed in a line chart.
- : indicates that statistics will be displayed in a bar chart.
- Only the command interception trend chart can be displayed in a pie chart.
- By default, the **Operation Stat** trend chart is displayed. It allows you to:
 - View operation statistics trend chart by user. A maximum of five users can be selected.
 - View operation statistics trend chart by resource. A maximum of five resources can be selected.

Prerequisites

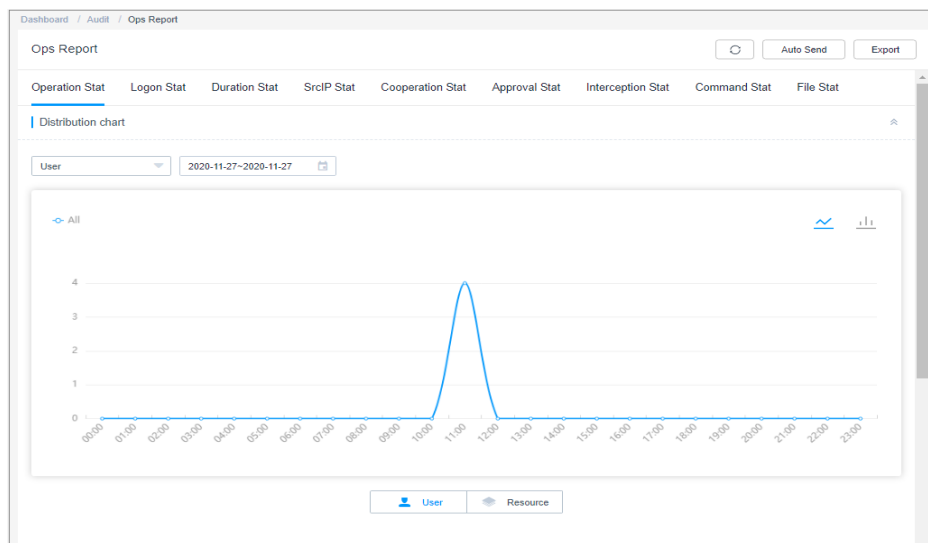
You have the management permissions for the **Operation Report** module.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **Audit > Operation Report**.

Figure 11-12 O&M reports



Step 3 Click each statistics tab and view the details.

The following describes details about each tab.

----End

Operation Stat

Displays the distribution of accessed resources by user or by resource. By default, the statistics of the current day is displayed by the hour.

In the detailed data area, view the session start and end time, user login name, resource name, protocol type, and account.

Figure 11-13 Distribution chart of Operation Stat

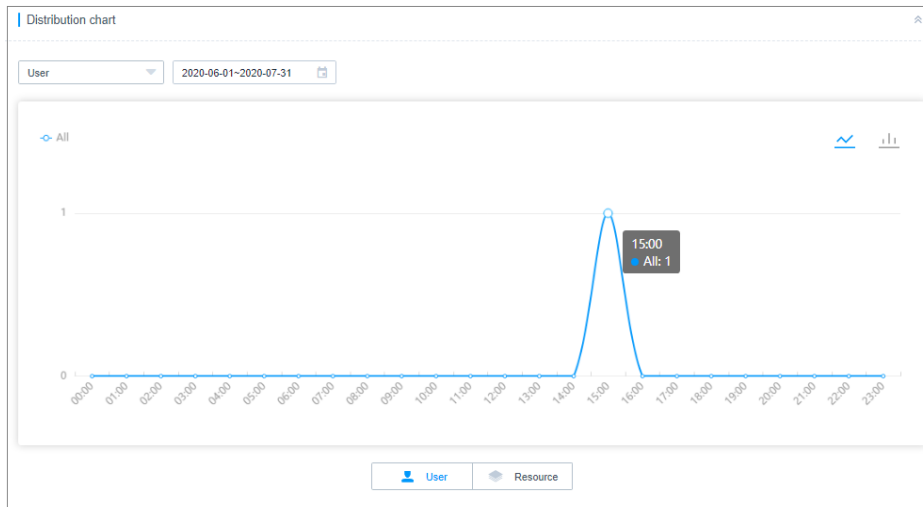


Figure 11-14 Detailed data of Operation Stat

Start/End time	User	Resource	Protocol	Account
2020-06-17 15:27:43-2020-06-17 16:03:42	admin	Linux	SSH	root

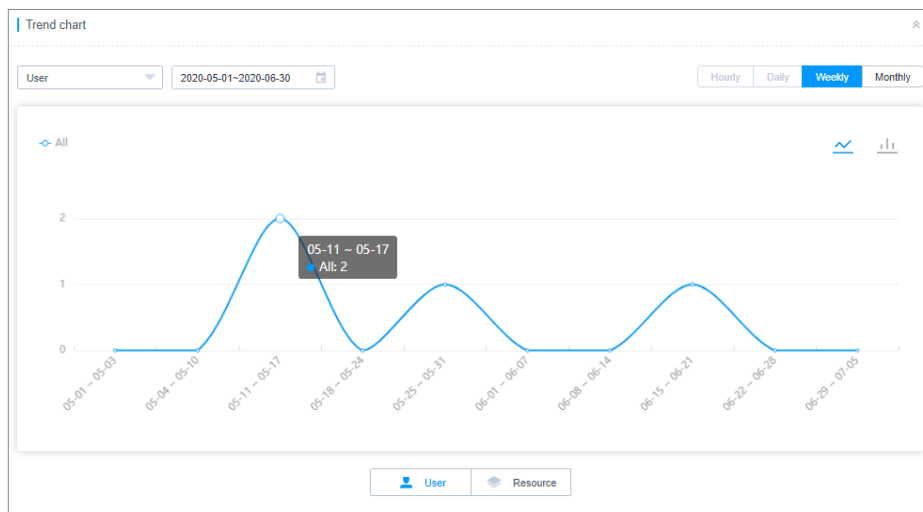
20 /page < 1 > Go to 1

Logon Stat

Displays the number of historical sessions by user or by resource. By default, the statistics of the current day is displayed by the hour.

In the detailed data area, view the session start and end time, user login name, resource name, protocol type, and account.

Figure 11-15 Trend chart of Logon Stat



Duration Stat

Displays the duration of history sessions by user or by resource. By default, the statistics of the current day is displayed by the hour.

In the detailed data area, view the session start and end time, user login name, resource name, protocol type, account, and session duration.

SrcIP Stat

Displays the number of source IP addresses from which sessions are established by user or by resource. By default, the statistics of the current day is displayed by the hour.

In the detailed data area, view the session start and end time, user login name, resource name, protocol type, account, and source IP address.

Cooperation Stat

Displays the number of users participating in a cooperation session by user or by resource. By default, the statistics of the current day is displayed by the hour.

In the detailed data area, view the session start and end time, user login name, resource name, protocol type, account, and login names of session participants.

Two-person authorization

Displays the number of sessions requiring two-person approval by user or by resource. By default, the statistics of the current day is displayed by the hour.

In the detailed data area, view the approval time, user login name, resource name, protocol type, account, and login names of approvers.

Interception Stat

Displays the number of intercepted commands by user or by resource. By default, the statistics of the current day is displayed by the hour.

Intercepting a command includes three actions, disconnecting the session, rejecting the session, or asking dynamical approval.

In the detailed data area, view the operation time, user login name, resource name, protocol type, account, and action.

Command Stat

Displays the number of executed commands by user or resource. By default, the statistics of the current day is displayed by the hour.

In the detailed data area, view the operation time, user login name, resource name, protocol type, account, and operation instructions.

File Stat

Displays the number of files uploaded and downloaded by user or by resource. By default, the statistics of the current day is displayed by the hour.

In the detailed data area, view the file operation time, user login name, resource name, protocol type, account, operation type, and file name.

11.4.2 Pushing Operation Reports

For your convenience of audit, you can manually export the operation reports or enable the auto send function to let CBH push operation reports to you through emails at the interval you select.

- Operation reports can be automatically sent by the day, week, and month.
- The report format can be PDF, DOC, XLS, or HTML.
- An operation report for a maximum of 180 consecutive days can be pushed each time.

Prerequisites

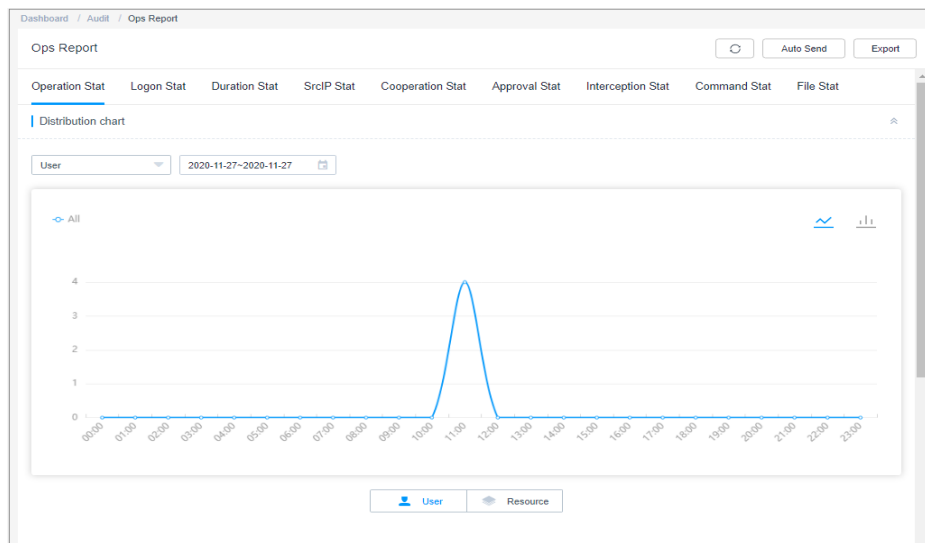
- You have the management permissions for the **Operation Report** module.
- You have completed [Configuring the Outgoing Mail Server](#).

Manually Exporting an Operation Report

Step 1 Log in to the CBH system.

Step 2 Choose **Audit > Operation Report**.

Figure 11-16 O&M reports



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

Step 4 In the displayed **Export** dialog box, configure the method and time to export the report and the report format.

Table 11-1 Parameters for exporting operation reports

Parameter	Description
Granularity	Time granularity for displaying the trend chart of the operation report. The options are Hourly , Daily , Weekly , and Monthly .
Time	Start time and end time to generate the operation report to be exported. <ul style="list-style-type: none"> Start time and end time are mandatory. A maximum of 180 consecutive days are allowed.
Report Type	Type of operation statistics to be included in the operation report.
File format	Format of the report. You can select only one format. <ul style="list-style-type: none"> DOC is selected by default. You can download a report in PDF, DOC, XLS, or HTML.

Step 5 Click **OK** to export the operation report immediately.

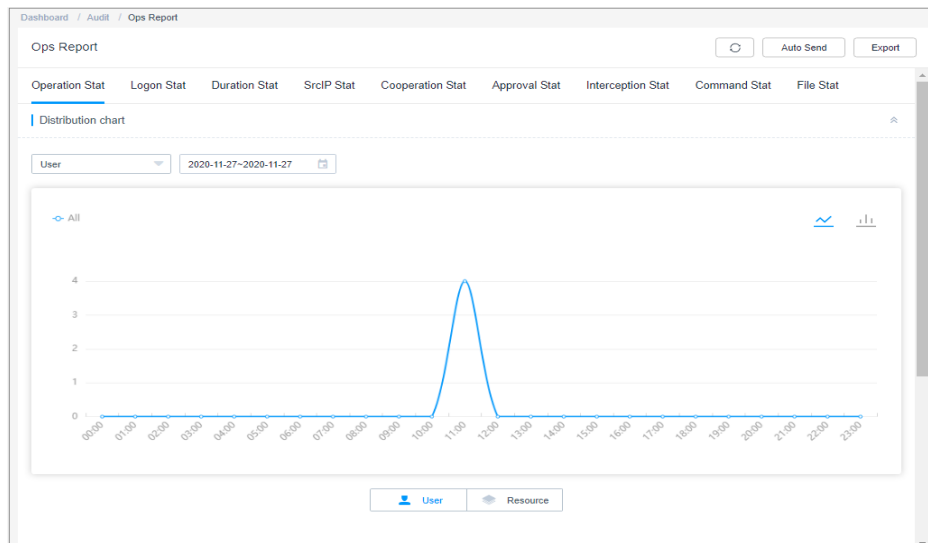
----End

Automatically Pushing a System Report

Step 1 Log in to the CBH system.

Step 2 Choose **Audit > Operation Report**.




Figure 11-17 O&M reports



Step 3 On the displayed page, click **Auto Send** in the upper right corner.

Step 4 In the displayed **Auto Send** dialog box, configure the method and time to push the report and the report format.

Table 11-2 Auto Send

Parameter	Description
Status	<p>Whether to enable the auto send function. This function is disabled by default ().</p> <ul style="list-style-type: none">  : indicates that auto send function is disabled.  : indicates that the auto send function is enabled. The operation report of the previous period will be sent to you through emails.
Send cycle	<p>Interval at which a report is sent.</p> <ul style="list-style-type: none"> By default, the report is sent at 00:00 on the specified date. Reports can be sent by the day, week, or month. Statistics in the daily reports are displayed by the hour. Statistics in the weekly reports are displayed by the day. Statistics in the monthly reports are displayed by the week.
File format	<p>Format of the report. You can select only one format.</p> <ul style="list-style-type: none"> DOC is selected by default. You can download a report in PDF, DOC, XLS, or HTML.

Step 5 Click **OK**.

----End

11.5 System Report

11.5.1 Viewing System Reports

As an audit administrator, you can view the detailed operation data in the system report, including the **UserControl Stat**, **User&Resource Stat**, **SrcIP Stat**, **Logon Stat**, **Exception Stat**, **Supervision Stat**, and **User Status** trend charts.

Constraints

- Each trend chart displays the statistics for a maximum of 180 consecutive days.
 - By default, the operation data of the current day is displayed by the hour.
 - Operation data over 30 days can only be viewed by the week or month.
 - Operation data within 30 days can be viewed by the day, week, or month.
- The trend chart can only be a bar chart.

Prerequisites

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

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **Audit > System Report**.

Step 3 Click each statistics tab and view the details.

----End

UserControl Stat

This area displays the number of disabling and enabling users. By default, the statistics of the current day is displayed.

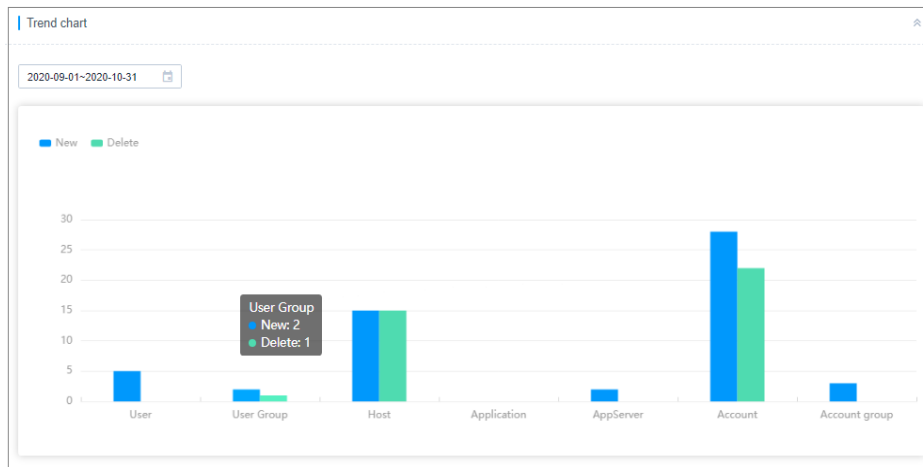
In the detailed data area, view the operation time, user login name, source IP address, operation, and operation results.

User&Resource Stat

This area displays statistics of how many users, user groups, hosts, application resources, application servers, accounts, and account groups are created and deleted. By default, the statistics of the current day is displayed.

In the detailed data area, view the operation time, user login name, source IP address, operation, and operation results.

Figure 11-18 Trend chart of User&Resource Stat



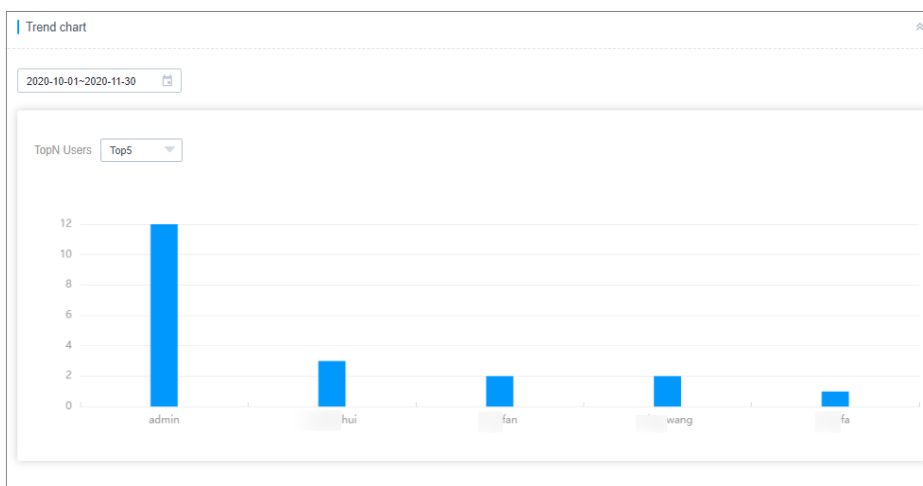
SrcIP Stat

This area displays the number of IP addresses from which users log in to the system. By default, the statistics of the current day is displayed.

You can view top 5, top 10, and top 20 source IP addresses.

In the detailed data area, view the logon time, source IP address, operation, and operation results.

Figure 11-19 Trend chart of SrcIP Stat



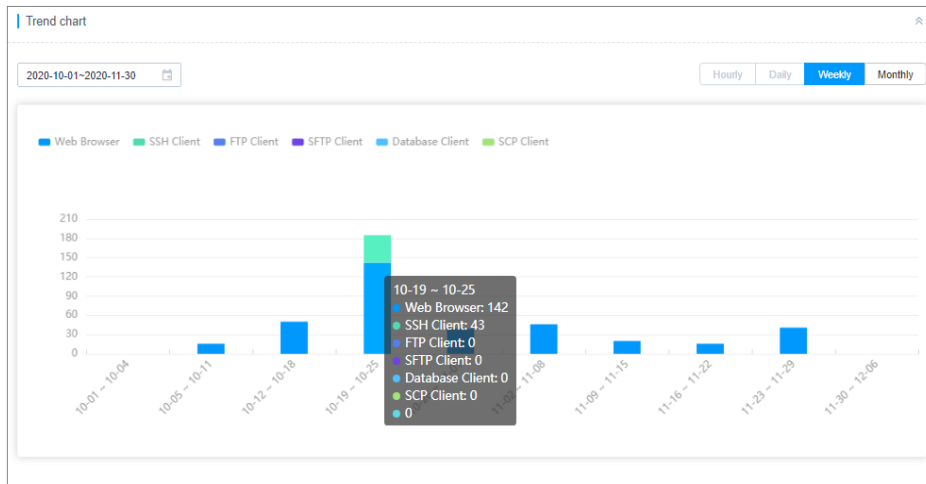
Logon Stat

This area displays the number of logins by login method. By default, the statistics of the current day is displayed.

You can view logins by web browsers and SSH, FTP, and SFTP clients.

In the detailed data area, view the logon time, source IP address, operation, and operation results.

Figure 11-20 Trend chart of Logon Stat



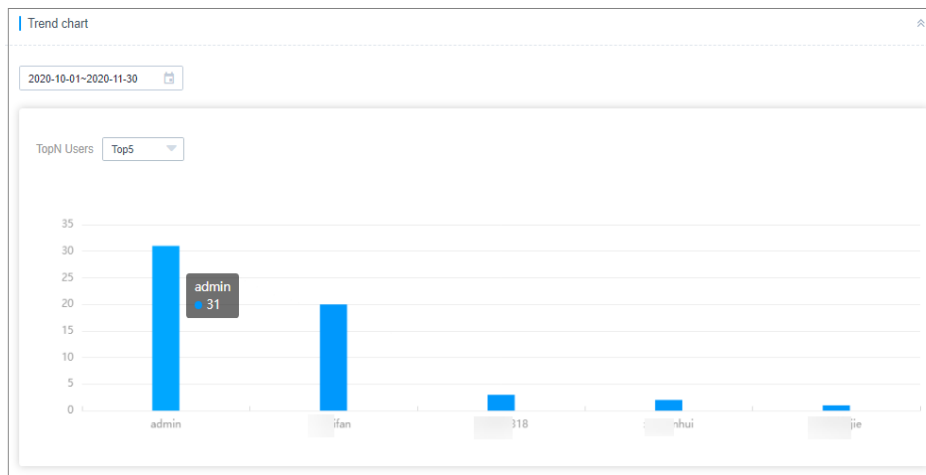
Exception Stat

This area displays the number of login exceptions. By default, the statistics of the current day is displayed.

You can view top 5, top 10, and top 20 login exceptions.

In the detailed data area, view the logon time, source IP address, operation, and operation results.

Figure 11-21 Trend chart of Exception Stat



Supervision Stat

This area displays the number of interrupted sessions and monitored sessions. By default, the statistics of the current day is displayed.

In the detailed data area, view the logon time, source IP address, operation, and operation results.

User Status

This area displays the number of zombie users and the number of users by password strength.

- Zombie users are valid users who have not logged in for more than 14 days. Zombie accounts are counted by the number of days during which they have not logged in.

By default, information about top 5 zombie accounts is displayed. You can view top 5, top 10, and top 20 zombie users.

In the detailed data area, view the time of the last successful login, source IP address, operation, and operation results.

- Password strength is classified into three levels: high, medium, and low. In the detailed data area, you can view the login name of the user who completes the last password change, password strength, and last password change time, which are displayed in ascending order by password strength.

NOTE

Password strength classification criteria:

High: The password contains eight or more characters that include uppercase letters, lowercase letters, digits, and special characters.

Medium: The password contains eight or more characters that include two or three types of the following characters: uppercase letters, lowercase letters, digits, and special characters.

Low: The password contains fewer than eight characters or contains eight or more characters that include one type of the following characters: uppercase letters, lowercase letters, digits, or special character.

11.5.2 Pushing System Reports

For your convenience of audit, you can manually export the system reports or enable the auto send function to let CBH push system reports to you through emails at the interval you select.

- System reports can be automatically sent by the day, week, and month.
- The report format can be PDF, DOC, XLS, or HTML.
- A system report for a maximum of 180 consecutive days can be pushed each time.

Prerequisites

- You have the management permissions for the **System Report** module.
- You have configured an available email address to receive reports.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **Audit > System Report**.

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

Step 4 In the displayed **Export** dialog box, configure the method and time to export the report and the report format.

Table 11-3 Parameters for exporting system reports

Parameter	Description
Granularity	Time granularity for displaying the trend chart of the system report. The options are Hourly , Daily , Weekly , and Monthly .
Time	Start time and end time to generate the report to be exported. <ul style="list-style-type: none"> Start time and end time are mandatory. A maximum of 180 consecutive days are allowed.
Report Type	Type of statistics to be included in the report.
File format	Format of the report. You can select only one format. <ul style="list-style-type: none"> DOC is selected by default. You can download a report in PDF, DOC, XLS, or HTML.

Step 5 Click **OK** to export the system report immediately.

Step 6 Go to your email address to check the system report after you receive the notification in the message center.

----End

Automatically Pushing a System Report




Step 1 Log in to the CBH system.

Step 2 Choose **Audit > System Report**.

Step 3 On the displayed page, click **Auto Send** in the upper right corner.

Step 4 In the displayed **Auto Send** dialog box, configure the method and time to push the report and the report format.

Table 11-4 Parameters for auto-send function

Parameter	Description
Status	Whether to enable the auto send function. This function is disabled by default (). <ul style="list-style-type: none">  : indicates that auto send function is disabled.  : indicates that the auto send function is enabled. The operation report of the previous period will be sent to you through emails.

Parameter	Description
Send cycle	Interval at which a report is sent. <ul style="list-style-type: none">• By default, the report is sent at 00:00 on the specified date.• Reports can be sent by the day, week, or month.• Statistics in the daily reports are displayed by the hour.• Statistics in the weekly reports are displayed by the day.• Statistics in the monthly reports are displayed by the week.
File format	Format of the report. You can select only one format. <ul style="list-style-type: none">• DOC is selected by default.• You can download a report in PDF, DOC, XLS, or HTML.

Step 5 Click **OK**.

----End

12 System Management

12.1 Sysconfig

12.1.1 System Configuration Overview

System configuration includes security, network, port, outgoing, authentication, ticket, alarm, audit, and HA backup. By default, only the system administrator **admin** has permissions to modify system configurations and manage the overall system running status.

- Security configuration: See [Login Security Management](#).
- Network configuration: See [Network](#).
- Port configuration: See [Port](#).
- Outgoing configuration: See [Outgoing](#).

 **NOTE**

User Expiration Countdown Settings: If you configure this, you will receive an email five days before a user expires.

- Authentication configuration: See [Remote Authentication Management](#).
- Ticket configuration: See [Ticket Configuration Management](#).
- Alarm configuration: See [Alarm](#).
- System theme: See [Theme](#).

12.1.2 Network

12.1.2.1 View Network Configurations

This topic describes how to view the system network interface, DNS address, default gateway address, and static routes.

Prerequisites

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

Procedure

Step 1 Log in to the CBH system.

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

Step 3 In the **Network interfaces** area, view the network interface information of the CBH system.

By default, the network interfaces cannot be modified.

Step 4 In the **DNS** configuration area, view the primary and secondary DNS addresses of the CBH system.

By default, the DNS address cannot be changed.

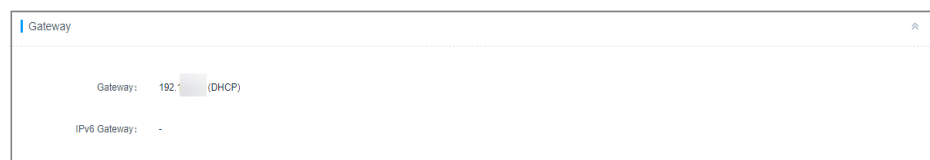
Figure 12-1 System DNS address



Step 5 In the **Gateway** area, view the default gateway of the CBH system.

By default, the DHCP gateway address is identified as the system gateway. The default gateway cannot be changed.

Figure 12-2 System default gateway



Step 6 In the **Static Route** configuration area, view accessible servers in other network segments.

----End

12.1.2.2 Adding a Static Route to the CBH System

After the CBH system restarts, non-static routes may be lost, affecting network availability. To prevent this issue, add static routes to the system.

This topic describes how to add a static route to the CBH system.

Prerequisites

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

CAUTION

Each static route must be correct. If the information is incorrect, you cannot log in to the CBH system.

Procedure

Step 1 Log in to the CBH system.

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

Step 3 In the **Static Route** configuration area, click **Add**.

In the displayed **Add static route** dialog box, configure other parameters.

Step 4 Click **OK**. You can then go to the **Security** configuration page and view the configured static route.

----End

Follow-up Operations

To delete a static route, click **Delete** in the **Operation** column in the corresponding row.

12.1.3 HA

12.1.3.1 Enabling HA

CBH supports the dual-node high availability (HA). After HA is enabled, the secondary node will take over the service if the primary node breaks down.

This topic describes how to enable dual-node HA backup.

Constraints

- The primary node must be configured first. After the primary node is configured and the configuration takes effect, configure the secondary node and ensure that the primary and secondary nodes use the internal network for HA synchronization configuration.
- After the HA configuration on the secondary node is complete, the historical data is cleared regardless of whether there is configuration data on the secondary node, and the configuration data of the primary node is synchronized to the secondary node.

Prerequisites

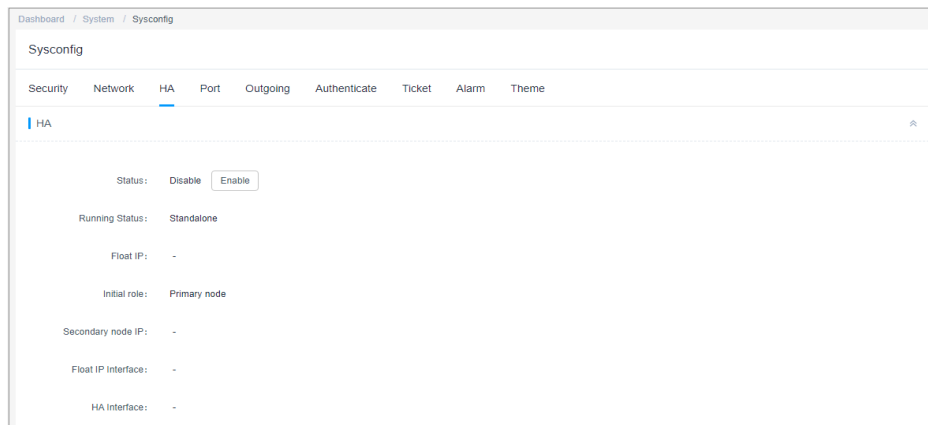
- You have the management permissions for the **System** module.
- You have prepared two CBH systems and authorized the two CBH systems with the same license.

Procedure

Step 1 Log in to the CBH system.

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

Figure 12-3 HA



Step 3 View the HA status. By default, the HA status is **Disabled**.

CAUTION

If you purchase a primary/standby instance, do not disable HA, or logins to the CBH instance will fail.

Step 4 Click **Enable** next to **Status**.

In the displayed **Enable HA** dialog box, configure the network information for the primary and secondary nodes.

Table 12-1 Parameters for enabling the HA function

Parameter	Description
Initial role	The working status of the node. This parameter can be set to Primary node or Secondary node . You must configure the CBH system that functions as the primary node first.
HA cluster authcode	The value is automatically generated by the system and is used for mutual verification between the primary and secondary nodes. <ul style="list-style-type: none"> When configuring HA parameters for the primary node, record the verification key of the HA group and configure the parameters for the secondary node accordingly. The value is a string consisting of 8 to 20 digits or letters.
Secondary node IP	When configuring HA parameters for the primary node, enter the IP address of the CBH system that functions as the secondary node.

Parameter	Description
Primary node IP	When configuring HA parameters for the secondary node, enter the IP address of the CBH system that functions as the primary node.
HA Key	When configuring HA parameters on the primary node, enter the key for mutual authentication between the primary and secondary nodes.
Float IP	Enter an unused IP address that is in the same network range as the fixed IP address of the current CBH instance. A mask must be added to the end of the floating IP address. Logical IP address of the two CBH systems. When you access this IP address, you will automatically log in to one of the CBH systems, usually the primary node.
Float IP Interface	Select the network interface where the fixed IP address of the CBH instance is located.
HA Interface	This interface is the same as that of the floating IP interface.

Step 5 Click **OK** and then restart the system for the configuration to take effect.

----End

Effective Conditions

Restart the primary and secondary nodes for the HA configuration to take effect.

- Before the restart, the **Running Status** is **Standalone**, indicating that the configuration does not take effect.
- After the restart, the HA backup cannot take effect until the primary node discovers the IP address of the secondary node and the **Running Status** of the secondary node changes to **Online**.

Follow-up Operations

To disable the dual-node HA function, click **Disable** next to **Status** in each system.

Save the settings and restart the two CBH systems. HA is disabled after the restart.

12.1.4 Port

12.1.4.1 Configuring the Operation Ports

The operation port is required for accessing managed resources, such as SSH, SFTP, or FTP resources, and logging in to the CBH system through SSH client. Different operation ports may be required for different types of resources. The default operation port is 2222.

If you change the default port, modify the security group configuration of the instance accordingly.

This topic describes how to configure an operation port.

Prerequisites

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

Procedure

Step 1 Log in to the CBH system.

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

Step 3 In the **Operation Port** area, click **Edit**.

- Configure port for SSH/SFTP resources. The default port number is 2222.
- The FTP agent service is disabled by default. Enable the FTP agent service. The default port is 2121.

Step 4 Click **OK** and then restart the system for the configuration to take effect.

----End

12.1.4.2 Configuring the Web Console Port

The web console port is used for logging in to the CBH system through a web browser. The default port is 443.

If you change the default port, modify the port configured in the security group of the instance accordingly.

This topic describes how to configure a web console port.

Prerequisites

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

Procedure

Step 1 Log in to the CBH system.

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

Step 3 In the **Web Console** area, click **Edit**.

In the displayed **Web Console** dialog box, configure the port for accessing the web browser. The default port is 443.

Step 4 Click **OK** and then restart the system for the configuration to take effect.

----End

12.1.4.3 Configuring the SSH Console Port

The SSH console port is required for logging in to the CBH system through an SSH client. The default port is 22.

If you change the default port, modify the port configured in the security group of the instance accordingly.

This topic describes how to configure an SSH console port.

Prerequisites

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

Procedure

Step 1 Log in to the CBH system.

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

Step 3 In the **SSH Console** area, click **Edit**.

In the displayed **SSH Console** dialog box, configure the port for accessing the SSH client. The default port is 22.

Step 4 Click **OK** and then restart the system for the configuration to take effect.

----End

12.1.5 Outgoing

12.1.5.1 Configuring the Outgoing Mail Server

To send email notifications, such as password change plans and alarm messages, configure an outgoing mail server.

- You can set a private mailbox server or public mailbox server as required and test whether the entered server information is valid.
- Currently, two protocols are supported: SMTP and Exchange (only Exchange 2010).

This topic describes how to configure an outgoing mail server.

Prerequisites

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

Procedure

Step 1 Log in to the CBH system.

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

Step 3 In the **Email** area, click **Edit**.

In the displayed **Email** dialog box, set **Protocol** to **SMTP** or **Exchange** and specify other parameters.

Step 4 Click **OK**. You can then view email configuration on the **Outgoing** tab.

----End

12.1.5.2 Configuring the Outgoing SMS Gateway

SMS messages are mainly used to:

- Receive the mobile phone verification code for login authentication.
- Reset the password.
- Receive alarm messages. For details about the alarm scope, see [Alarm](#).

Currently, you can select **Built-in** or **Third-party** SMS gateways. If you select **Third-party**, general **SMS Gateway** and cloud SMS gateway are available.

- If you do not need to push system alarms or send and receive SMS messages to mobile numbers outside the Chinese mainland, you can configure the SMS gateway by referring to [Built-in SMS gateway](#).
- If you need to receive system alarms or send and receive SMS messages to mobile numbers outside the Chinese mainland, configure the SMS gateway by referring to [General Third-party SMS Gateway](#).

This topic describes how to configure an outgoing SMS gateway.

Prerequisites

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

Built-in SMS gateway

- Step 1** Log in to the CBH system.
- Step 2** Choose **System > Sysconfig > Outgoing**.
- Step 3** In the **SMS API** area, click **Edit**.
- Step 4** Select **Built-in** and enter a mobile number to verify the connectivity of the built-in SMS gateway.
- Step 5** Click **OK**. You can then view SMS gateway configuration on the **Outgoing** tab.

CAUTION

- The built-in SMS gateway cannot push CBH system alarm notifications.
 - The built-in SMS gateway cannot send SMS messages to mobile numbers outside the Chinese mainland. If you need to receive SMS messages from mobile numbers outside the Chinese mainland, configure an SMS gateway outside the Chinese mainland.
-

----End

General Third-party SMS Gateway

- Step 1** Log in to the CBH system.
- Step 2** Choose **System > Sysconfig > Outgoing**.

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

Step 4 Select **Third-party** and then select **SMS Gateway** from the **SMS Conf** drop-down list.

In the displayed parameter list, specify other parameters as prompted.

Step 5 Click **OK**. You can then view SMS gateway configuration on the **Outgoing** tab.

Table 12-2 SMS API parameters

Parameter	Description
Method	Request method. The options are POST and GET .
URL	URL of SMS API. You can enter a universal URL or a URL containing parameters. Do not enter MD5-encrypted URLs.
HTTP Header	HTTP request header. Use colons (:) to separate the name and value of the HTTP request header. Only HTTP and HTTPS gateways are supported.
API Params	API parameters of the SMS gateway. Replace keywords <i>\$MOBILE</i> and <i>\$TEXT</i> with the phone number and SMS content.
Encode	Encode method. You can select UTF-8 , Big5 , or GB18030 .
Mobile	Phone number for receiving the SMS messages. Enter an available phone number and verify the SMS message content.

----End

12.1.5.3 Configuring LTS

You can use Log Tank Service (LTS) to manage operation logs in the CBH system.

Prerequisites

- You have the management permissions for the **System** module.
- You have enabled Log Tank Service (LTS).
- An EIP has been bound to the CBH instance.

Constraints

- An EIP must be bound to the CBH instance.
- Log Tank Service (LTS) must be enabled before you configure LTS in CBH.


Procedure

Step 1 Log in to the CBH system.

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

Step 3 On the displayed page, locate the **LTS Config** area and click **Edit**.

Step 4 Click to enable LTS and enter the installation instruction in the **Install Agent** text box.

Click  to view how to obtain the installation instruction.

Step 5 Click **OK**.

----End

12.1.6 Alarm

12.1.6.1 Configuring Alarm Channels

You can enable alarm notification on messages of a certain severity level. There are five types of alarm messages, including system messages, service messages, task messages, command alarms, and ticket messages. All messages are classified into high, medium, and low severity levels.

- Alarm notifications can be sent through message center, emails, or SMS message.
- Whether to report an alarm for a message and which alarm channel is used vary depending on severity level of the message. By default:
 - For messages of low severity, no alarms are sent.
 - For messages of medium severity, alarms are sent through the message center.
 - For messages of high severity, alarms are sent through the message center and emails.

This topic describes how to configure the alarm channels.

Constraints

Alarm notifications can be pushed through SMS messages only after you enable the SMS APIs.

Prerequisites

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

Alarm

Step 1 Log in to the CBH system.

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

Figure 12-4 Alarm



Step 3 In the **Alarm Channel** area, click **Edit**.

In the displayed **Alarm Channel** dialog box, set alarm channels for different message types.

Step 4 Click **OK**. You can then view alarm level configuration on the **Alarm** tab.

----End

12.1.6.2 Configuring Alarm Levels

This topic describes how to configure the alarm levels of messages.

Prerequisites

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

Procedure

Step 1 Log in to the CBH system.

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

Figure 12-5 Alarm



Step 3 In the **Alarm Level** area, click **Edit**.

- In the displayed **Alarm Level** dialog box, configure alarm severity levels for different types of messages in each tab.
- The alarm level can be high, medium, or low.

Step 4 Click **OK**. You can then view alarm level configuration on the **Alarm** tab.

----End

12.1.7 Theme

12.1.7.1 Changing the System Theme

This topic describes how to change the system language and customize system and company logos.

Prerequisites

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

Theme

Step 1 Log in to the CBH system.

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

Step 3 Switch over the system language.

1. On the displayed page, in the **Language settings** area, click **Edit**.
2. Select a language. You can select simplified Chinese or English.
3. Click **OK**.

Then, log out the CBH system, clear cookies, and log in to it again for the specified language to take effect.

 **NOTE**

Changing language in the upper right corner on the login page takes effect immediately.

Step 4 Change the system icon.

1. In the **Logo settings** area, click **Edit**.
2. Click logos under **System logo** and **Company logo**, respectively, open the local path, and select a logo you want to use.
3. Click **OK** and then restart the system for the configuration to take effect.

----End

12.2 Data Maintenance

12.2.1 Viewing System Memory

The storage space of the CBH system consists of system partitions and data partitions. If the idle space of the data partition is insufficient, delete historical system data.

This topic describes how to check the system memory usage.

Prerequisites

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

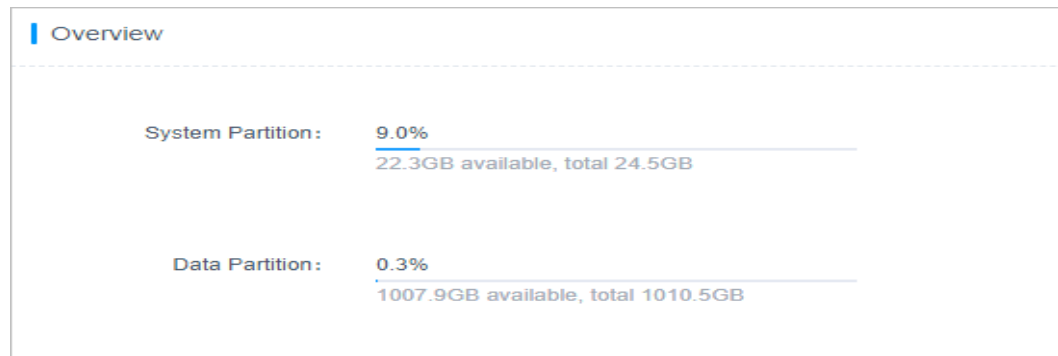
Procedure

Step 1 Log in to the CBH system.

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

Step 3 In the **Overview** area, view the space usage of the system partition and data partition.

Figure 12-6 Storage space overview



----End

12.2.2 Configuring the Netdisk Capacity

The **Netdisk** is used to temporarily store files from managed hosts or the local server for the purpose of file transfer. The **Netdisk** is a personal net disk in the CBH system.

This topic describes how to set the net disk capacity.

Constraints

- The maximum available space of the net disk is the available space of the system data disk.
- After **Personal Netdisk** is set, the CBH system allocates the same personal net disk capacity for each user in the system.
- Files on the **Netdisk** can only be manually deleted. Periodic clearance of personal net disk space is not supported.

Prerequisites

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

Procedure

- Step 1** Log in to the CBH system.
- Step 2** Choose **System > Data Maintain > Storage Mgmt.**
- Step 3** In the **Netdisk** area, click **Edit**. In the displayed dialog box, set the disk size.

Table 12-3 Netdisk parameters

Parameter	Description
Personal Netdisk	A private disk exclusively used by the current user <ul style="list-style-type: none"> • The default value is 100 MB. • To use the personal net disk unlimitedly when the system data disk capacity is allowed, set Personal Netdisk to 0.

Parameter	Description
Total Netdisk	Total netdisk capacity. <ul style="list-style-type: none"> The default value is 5120 MB. To use all space of the total net disk unlimitedly when the system data disk capacity is allowed, set Total Netdisk to 0.

Step 4 Click **OK**. You can then view capacity of the configured **Personal Netdisk** and **Total Netdisk** on the **Storage Mgmt** tab.

Step 5 Click **Detail** and view details about the net disk.

Step 6 In the row containing the net disk, click **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

12.2.3 Deleting System Data

If the system data disk usage is higher than 95%, the system may become unavailable. To ensure that the system data disk can be used properly, you can configure automatic or manual deletion of system data by referring to this section.

The system data that is automatically or manually deleted is mainly the files temporarily stored on the data disk, including large historical session video files, local backup log files, and local backup system configuration files.

 **DANGER**

Deleted system data cannot be restored. Exercise caution when performing this operation.

Constraints

Data of a specific day cannot be deleted through **Manual Deletion**. You can delete the data before the date you select.

Prerequisites

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







Configuring Auto Deletion

Step 1 Log in to the CBH system.

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

Step 3 In the **Auto Deletion** area, click **Edit**. In the displayed dialog box, set related parameters.

Table 12-4 Configuring Auto Deletion

Parameter	Description
Auto Deletion	<p>Status of auto deletion (default: ).</p> <ul style="list-style-type: none"> : Auto deletion is enabled. The system automatically starts the data deletion job when the data storage duration and data disk usage exceeds the limit. : Auto deletion is disabled.
Data life (days)	<p>Data storage duration. The data is automatically deleted when its storage duration exceeds the specified value.</p> <ul style="list-style-type: none"> Default value: 180 days. Value range: 1 to 10000, in days.
Overwrite when full	<p>When the data disk usage exceeds 90%, data on the disk will be automatically deleted.</p> <p>Whether to enable this function (default: ).</p> <ul style="list-style-type: none"> : This function is disabled : This function is enabled. Auto deletion policies: <ul style="list-style-type: none"> The system checks the data disk usage every 30 minutes. When the usage is lower than 90%, the auto deletion stops. By default, the system deletes data generated 180 days earlier than the current day. If the data disk usage is still higher than 90%, the rest data is deleted day by day backwards from the day before the current day until the space usage is lower than 90% Data of the current day cannot be automatically deleted.
Delete Content	<p>The options are as follows:</p> <ul style="list-style-type: none"> System Log Session Log

Step 4 Click **OK**.

----End

Manual Deletion

Step 1 Log in to the CBH system.

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

Step 3 In the **Manual Deletion** area, select a date.

Step 4 Click **Delete**. Data generated before the selected date is deleted.

----End

12.2.4 Creating a Local Data Backup

To enhance data disaster recovery management and improve audit data security and system scalability, CBH enables backup of configuration logs.

This topic walks you through how to create a backup locally.

Constraints

- Supported logs: System login logs, resource login logs, command operation logs, file operation logs, and two-person authorization logs
- After a local backup is created, a log file is generated on the system data disk.

Prerequisites

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

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **System > Data Maintain > Log Backup**.

Step 3 In the **Data Backup Locally** area, click **Add**. In the displayed dialog box, configure backup content and date range.

Table 12-5 Creating a Local Backup

Parameter	Description
Log content	Type of logs to be backed up <ul style="list-style-type: none"> • The options are System Login, Resource Logon, Command log, File log, and Double auth log. • Select at least one log type.
Date Range	Date range to generate logs to be backed up <ul style="list-style-type: none"> • Select at least one day.
Remarks	Brief description. <ul style="list-style-type: none"> • A maximum of 128 characters can be entered.

Step 4 Click **OK**. You can then view the backup information on the **Log Backup** tab.

----End

Follow-up Operations

- To download a local backup to your local server, click **Download** in the **Operation** column of the corresponding row.

- To delete a local backup, click **Delete** in the **Operation** column of the corresponding row.

12.2.5 Configuring the Syslog Server for Remote Backup

To enhance data disaster recovery management and improve audit data security and system scalability, CBH enables backup of configuration logs.

This topic walks you through how to configure the Syslog server for remote log backup.

Constraints

- After remote backup is enabled, the system backs up the system data of the previous day at 00:00 every day by default.
- Logs are automatically backed up on a daily basis and uploaded to the corresponding folder on the Syslog server.
- Supported logs: System login logs, resource login logs, command operation logs, file operation logs, and two-person authorization logs




Prerequisites

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

Procedure

- Step 1** Log in to the CBH system.
- Step 2** Choose **System > Data Maintain > Log Backup**.
- Step 3** In the **Backup to the syslog server** area, click **Edit**. In the displayed dialog box, complete required parameters.

Table 12-6 Parameters for configuring the Syslog server

Parameter	Description
Status	Whether to back up data to the Syslog server (default: ). <ul style="list-style-type: none"> • : This function is enabled. The system automatically starts backup at 00:00 every day. • : This function is disabled.
Sender Identifier	Identifier for connecting the CBH system to the Syslog server. The identifier is used to identify the CBH system from which the logs are received on the Syslog server.
Server IP	IP address of the Syslog server.
Port	Port number of the Syslog server.

Parameter	Description
Protocol	<p>Protocol of the Syslog server.</p> <ul style="list-style-type: none"> • The options are TCP or UDP. • If TCP is selected, click Test connectivity to check whether the server is reachable.
Backup Content	<p>Select at least one type of logs to be backed up.</p> <ul style="list-style-type: none"> • System logon log • Resource logon log • Command operation log • File operation log • Two-person authorization log

Step 4 Click **OK**. You can then view the backup information on the **Log Backup** tab.

After the configuration is complete, the system backs up the data of the previous day at 00:00 every day and uploads the data to the remote Syslog server.

----End

Follow-up Operations

- To disable the Syslog server backup, click **Edit**. In the displayed dialog box, set **Status** to **Disabled**.
- To view or download logs backed up to the Syslog server, log in to the Syslog server.

12.2.6 Configuring an FTP/SFTP Server for Remote Log Backup

To enhance data disaster recovery management and improve audit data security and system scalability, CBH enables backup of configuration logs.

This topic walks you through how to configure the FTP or SFTP server for remote log backup.

Constraints

- After remote backup is enabled, the system backs up the system data of the previous day at 00:00 every day by default.
- Logs are automatically backed up on a daily basis and uploaded to the corresponding folder on the FTP or SFTP server.
- Logs of the same day cannot be backed up repeatedly in the same server path.
- System configuration and session playback logs can be remotely backed up to the FTP or SFTP server.

Prerequisites

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




Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **System > Data Maintain > Log Backup**.

Step 3 In the **Backup to the FTP/SFTP server** area, click **Edit**. In the displayed dialog box, complete required parameters.

Table 12-7 Parameters for configuring the FTP or SFTP server

Parameter	Description
Status	Whether to back up data to the FTP or SFTP server (default: ). <ul style="list-style-type: none"> : Remotely backing up logs to an FTP or SFTP server is enabled. The system automatically starts backup at 00:00 every day. : Remotely backing up logs to an FTP or SFTP server is disabled.
Protocol	Protocol over which logs are transferred for backing up <ul style="list-style-type: none"> The options are FTP and SFTP.
Server IP	IP address of the FTP or SFTP server.
Port	Port number of the FTP or SFTP server.
Username	Username on the FTP or SFTP server to test whether the FTP or SFTP server is reachable.
Password	Password of the username on the FTP or SFTP server to test whether the FTP or SFTP server is reachable.
Storage Path	Path where the logs are stored. <ul style="list-style-type: none"> The path must start with a period (.). For example, if the path is ./test/abc, the absolute path is /home/username/test/abc. If this parameter is left empty, the backup content is stored in the home directory of the FTP or SFTP server user, for example, absolute path /home/username.
Test connectivity	Tests whether the configured FTP or SFTP server is reachable. <ul style="list-style-type: none"> It checks only the network status between the CBH system and the FTP or SFTP server. The user account of the server is not verified.

Parameter	Description
Backup Content	<p>Select at least one type of logs to be backed up.</p> <ul style="list-style-type: none"> • System configuration • Session recording playback log • System logon log • Resource logon log • Command operation log • File operation log • Two-person authorization log

Step 4 Click **OK**. You can then view the backup information on the **Log Backup** tab.

After the configuration is complete, the system backs up the data of the previous day at 00:00 every day and uploads the data to the remote FTP or SFTP server.

----End

Follow-up Operations

- To back up the logs of a certain day immediately, start the remote backup immediately.
In the **Backup to FTP/SFTP server** area, select the date of the logs to be backed up and click **Backup**.
- To disable the FTP or SFTP server backup, click **Edit**. In the displayed dialog box, set **Status** to **Disabled**.
- To view or download logs backed up to the FTP or SFTP server, log in to the FTP or SFTP server.

12.2.7 Configuring OBS Buckets for Remote Log Backup

To enhance data disaster recovery management and improve audit data security and system scalability, CBH enables backup of configuration logs.

This topic walks you through how to set OBS buckets to remotely back up logs.

Constraints

- After remote backup is enabled, the system backs up the system data of the previous day at 00:00 every day by default.
- Logs are automatically backed up on a daily basis and uploaded to the corresponding folder in the OBS bucket.
- Logs of the same day cannot be backed up repeatedly in the same server path.
- System configuration and session playback logs can be remotely backed up to OBS buckets.

Prerequisites

- You have the management permissions for the **System** module.
- You have created an OBS bucket, and the network between the OBS bucket and the CBH system is normal.




Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **System > Data Maintain > Log Backup**.

Step 3 In the **Remote Backup To OBS** area, click **Edit**. In the displayed dialog box, set bucket parameters.

Table 12-8 Parameters for remote backup to OBS

Parameter	Description
Status	Whether to back up logs to an OBS bucket (default: ). <ul style="list-style-type: none"> • : Backing up logs to OBS buckets is enabled. The system automatically starts backup at 00:00 every day. • : Backing up logs to OBS buckets is disabled.
Access Key ID	Specifies the access key ID, which is used to verify the identity of the request sender for accessing the OBS bucket. An access key ID is a unique identifier associated with a secret access key and is used together with the secret access key to sign requests cryptographically.
Secret Access Key	Specifies the secret access key used together with the access key ID. A secret access key works as a cryptographic signature to identify the sender of a request and prevent the request from being tampered with.
EndPoint	Region where the bucket is located.
bucket	Bucket name.
Storage Path	Bucket path or bucket folder path. The path cannot contain three or more consecutive slashes (/). If the OBS bucket does not have the corresponding path, a folder is automatically generated in the bucket. Example: cbh/bastion/.../...
Test connectivity	Tests whether the network between the CBH system and the configured OBS bucket is reachable. The connectivity test checks only the network status between the CBH system and the OBS bucket.

Parameter	Description
Backup Content	<p>Select at least one type of logs to be backed up.</p> <ul style="list-style-type: none"> • System configuration • Session recording playback log • System logon log • Resource logon log • Command operation log • File operation log • Two-person authorization log

Step 4 Click **OK**. You can then view the backup information on the **Log Backup** tab.

After the configuration is complete, the system backs up the data of the previous day at 00:00 every day and uploads the data to the OBS bucket.

----End

Follow-up Operations

- To back up the logs of a certain day immediately, start the remote backup immediately.
In the **Remote Backup To OBS** area, select the date of the logs to be backed up and click **Backup**.
- To disable the remote OBS bucket backup, click **Edit**. In the displayed dialog box, set **Status** to **Disabled**.
- To view or download logs backed up to the OBS bucket, log in to the OBS console and perform operations in the corresponding bucket folder.

12.3 System Maintenance

12.3.1 Viewing System Status

To ensure the healthy running of the CBH system, monitor the CPU, memory, disk, and network bandwidth usage in a timely manner.

This topic describes how to check the system CPU, disk, and network bandwidth usage.

Prerequisites

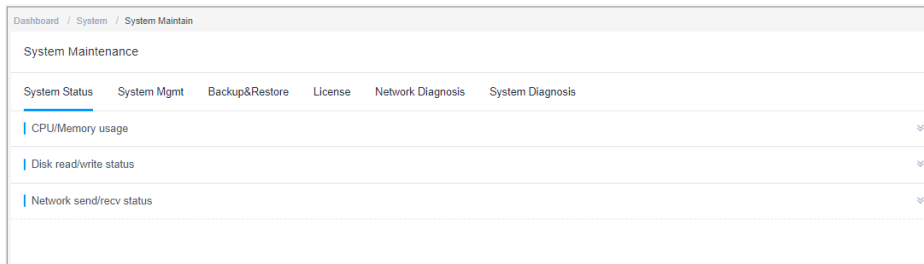
You have the management permissions for the **System** module.

Viewing System CPU and Memory Usage

Step 1 Log in to the CBH system.

Step 2 Choose **System > System Maintain > System Status**.

Figure 12-7 Viewing System Status



Step 3 Expand the **CPU/Memory usage** area and view the CPU or memory usage.

- View CPU or memory usage statistics over the past 5 minutes, 15 minutes, or 1 hour.
- To view CPU or memory usage at a certain moment, move your cursor over the time point.

----End

View Disk Read/write Status

Step 1 Log in to the CBH system.

Step 2 Choose **System > System Maintain > System Status**.

Step 3 Expand the **Disk read/write status** area and view the read/write usage of the system disk.

- View disk read/write statistics over the past 5 minutes, 15 minutes, or 1 hour.
- To view disk read/write speed at a certain moment, move your cursor over the time point.

----End

Viewing Network Sending and Receiving Status

Step 1 Log in to the CBH system.

Step 2 Choose **System > System Maintain > System Status**.

Step 3 Expand the **Network send/rcv status** area and view the system network receiving or sending status.

- View network packet receiving and sending speed over the past 5 minutes, 15 minutes, 1 hour, or 24 hours.
- View the sending and receiving status on the **eth0** and **eth1** network interfaces.
- To view network sending or receiving speed at a certain moment, move your cursor over the time point.

----End

12.3.2 System Mgmt

This topic describes how to update the system IP address, time, and version, how to restart, shut down, and restore the system, and how to manage the basic system information and status.

Prerequisites

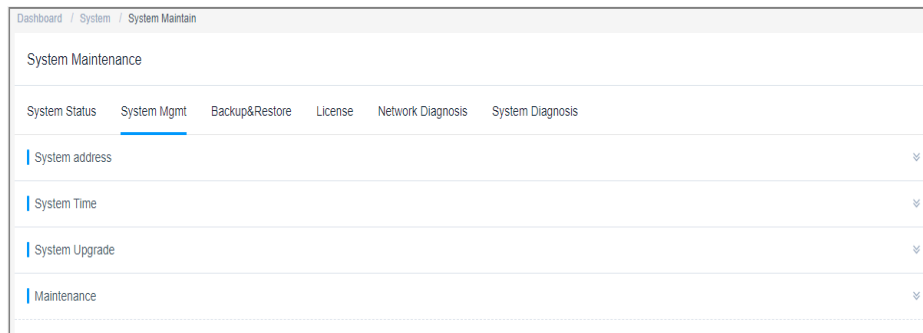
You have the management permissions for the **System** module.

Managing System Addresses

Step 1 Log in to the CBH system.

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

Figure 12-8 System Mgmt

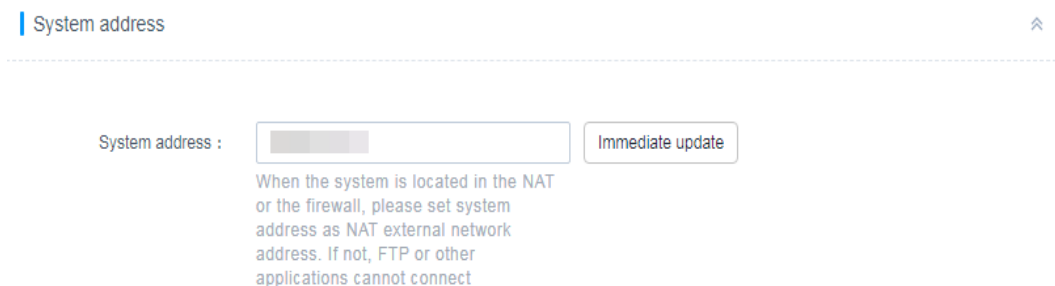


Step 3 Expand the **System address** area.

Step 4 Update the system IP address.

- After the EIP bound to the mapped CBH instance is changed, update the system IP address accordingly.
- The system IP address must be the NAT external network address. Otherwise, application resources such as FTP cannot be connected.

Figure 12-9 System address



----End

Managing System Time

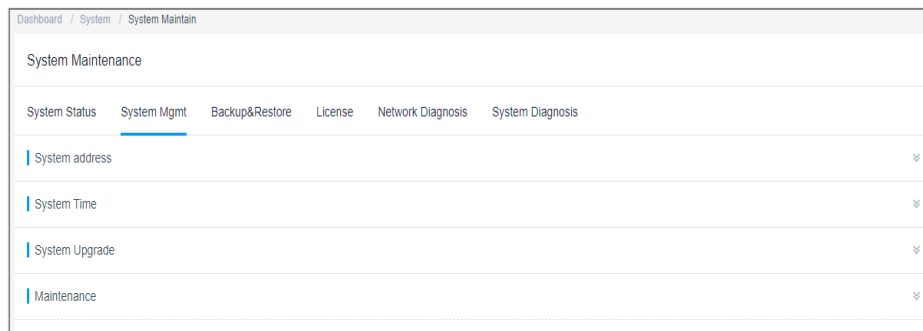
 **NOTE**

Incorrect system time will make policies and tickets ineffective and causes failures in the authentication of the mobile OTP and dynamic OTP token when they bound to the CBH system.

Step 1 Log in to the CBH system.

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

Figure 12-10 System Mgmt



Step 3 Expand the **System Time** area.

Step 4 Update the system time manually.

1. Click **Modify** next to the **Current Time**.
2. In the displayed **Edit System Time** dialog box, specify the date and time.
3. Click **OK**.

Step 5 Synchronize time from the NTP server.

The current system time is synchronized by default.

1. Select the built-in NTP server or enter the IP address of the NTP server.
2. Click **Sync**.

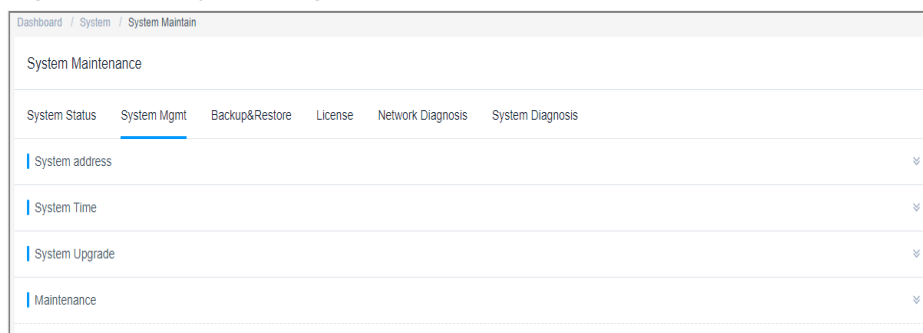
----End

Managing System Tools

Step 1 Log in to the CBH system.

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

Figure 12-11 System Mgmt



- Step 3** Expand the **Maintenance** area. In this area, you can restart and upgrade the system and restore the system to factory settings.
- Restarting the system
 - a. Click **Restart**.
 - b. In the displayed confirmation dialog box, click **OK**.
 - c. Enter the password of system administrator **admin**.
 - d. Click **OK**. After the verification is successful, you can log in to the system.
 - Shutting down the system
 - a. Click **Shutdown**.
 - b. In the displayed confirmation dialog box, click **OK**.
 - c. Enter the password of system administrator **admin**.
 - d. Click **OK**.
 - Restoring factory settings
 - a. Click **Reset to factory defaults**.
 - b. In the displayed confirmation dialog box, click **OK**.
 - c. Enter the password of system administrator **admin**.
 - d. Click **OK**. After the verification is successful, the system is restored to the initial settings, and all system data is cleared.



Do not restore factory settings unless in emergencies. Otherwise, all system data will be lost.

----End

12.3.3 System Configuration Backup and Restoration (Backup&Restore)

To ensure that the system configuration data is not lost, enable the automatic backup function or periodically back up the system configuration data.

This section describes how to back up and restore system configurations and how to manage the backup files

Constraints

- System configuration backup files can be used only for the corresponding CBH system.
- Only system configuration parameters can be backed up. System data generated during O&M cannot be backed up. For details about system data backup, see [Data Maintenance](#)

Prerequisites

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

Backing Up System Configuration Data

Step 1 Log in to the CBH system.

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

Step 3 Enable auto backup.

In the **Config Backup** area, enable **Auto**. The system will automatically back up the configuration at 00:00 every day.

Step 4 Start a backup job immediately.

1. In the **Config Backup** area, click **New**.
2. In the displayed dialog box, enter remarks to distinguish backup files.
3. Click **OK** to start the backup. After the backup is complete, you can view the backup file in the backup list.

----End

Restoring System Configurations

Step 1 Log in to the CBH system.

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

Step 3 Restore the system configuration. Select any of the following methods:

- One-click system configuration restoration
Before your start, ensure that a system configuration backup file is ready.
 - a. In the **Config Backup** area, select the backup file you want to use.
 - b. In the **Operation** column, click **Restore**.
- Using a local backup file to restore system configurations
 - a. In the **Config Restore** area, click **Upload**.
 - b. In the displayed dialog box, select a backup configuration file that has been downloaded.
 - c. After the backup file is uploaded, click **OK**.

Step 4 Refresh the page. After the system is restored, you are required to log in to the system again.

----End

Managing Backup Files

You can download and delete system configuration backup files to save more storage space.

Step 1 Log in to the CBH system.

Step 2 Choose **System > System Maintain > System Status**.

Step 3 Download a backup file.

1. In the **Config Backup** area, select the backup file you want to use.

2. In the **Operation** column, click **Download** to download the backup file.

Step 4 Delete a backup file.

1. In the **Config Backup** area, select the backup file you want to use.
2. In the **Operation** column, click **Delete** to delete the backup file to release storage space.

----End

12.3.4 License

This topic walks you through how to view system license.

Prerequisites

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

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **System > System Maintain > License** and view the current license information.

Table 12-9 License parameters

Parameter	Description
Customer Info	Region and AZ where the system is used
Authentication Type	By default, Official Version is set for Authentication Type .
Status	<p>Activated: The license can be used normally.</p> <ul style="list-style-type: none"> • Click Update License, download the license application file as prompted, and contact the vendor to apply for a license. Import the new license to update the license. • Click Backup License to download the current system license to your PC. <p>NOTE When the numbers of assets, users, and concurrent requests increase, you can update the license to upgrade the system specifications. In this case, adjust the CPU, memory, and bandwidth configurations of the CBH system.</p>
Product ID	Product ID of the current system
Authorized Modules	Supported function modules.
Max Resources	Maximum number of resources that can be added to the CBH system (including host and application resources)

Parameter	Description
Max Concurrent Conns	Maximum number of connections established to host and application resources at the same time over different protocols. This number is the result of the number of logged users multiply by the number of logged in resources.

----End

12.3.5 Network Diagnosis

With network diagnosis, you can quickly check whether the network between the CBH system and a managed host is connected if the managed host fails to be logged in. CBH can use any of the following methods to check the connectivity:

- Ping the host IP address to check whether the CBH system communicates with the host over the ICMP protocol.
- Perform route tracing on the host address to check whether the route between the CBH system and the host is reachable.
- Perform the TCP port test on the host IP address to check whether the CBH system is connected to the TCP port on the host.

 **NOTE**

- If the network is unreachable, rectify the fault.
- If the network connectivity is normal, check whether the username, password, and port number of the host added to the system are correct.

This topic describes how to test the network connectivity.

Prerequisites

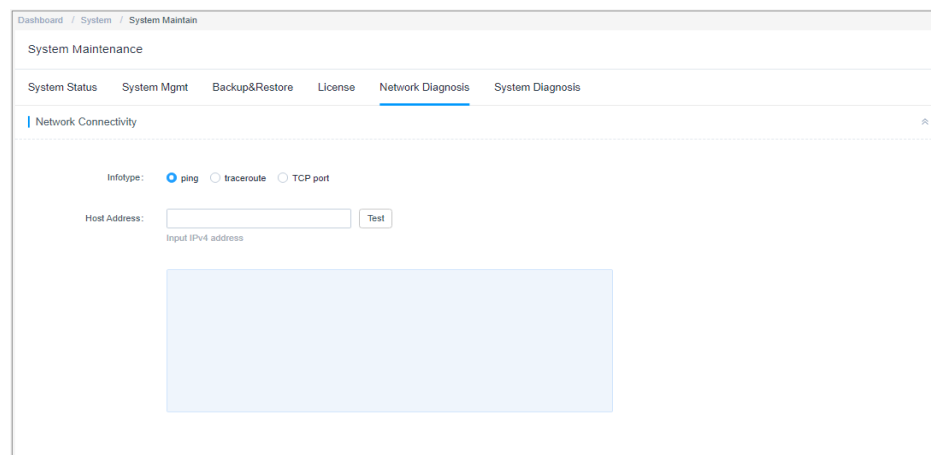
You have the management permissions for the **System** module.

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **System > System Maintain > Network Diagnosis**.

Figure 12-12 Network Diagnosis



Step 3 Ping the IP address of the host to check the network connectivity.

1. Set **Infotype** to **ping**.
2. Enter the host IP address and click **Test** to view the connectivity test result.
3. Check whether the system can communicate with the host using the ICMP protocol.

Step 4 Traceroute the host IP address and check the network connectivity.

1. Set **Infotype** to **traceroute**.
2. Enter the host IP address and click **Test** to view the connectivity test result.
3. Check whether there is a reachable route between the system and the host.

Step 5 Test network connectivity through the TCP port.

1. Set **Infotype** to **TCP port**.
2. Enter the host IP address and port number and click **Test** to view the connectivity test result.
3. Check whether the TCP port between the system and the host is reachable.

----End

12.3.6 System Diagnosis

With system diagnosis, you can easily obtain information about the current system, including comprehensive information and details about system load, kernel, memory, network interface card (NIC), disk usage, routes, and ARP.

This topic describes how to obtain the system background information.

Prerequisites

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

Procedure

Step 1 Log in to the CBH system.

Step 2 Choose **System > System Maintain > System Diagnosis**.

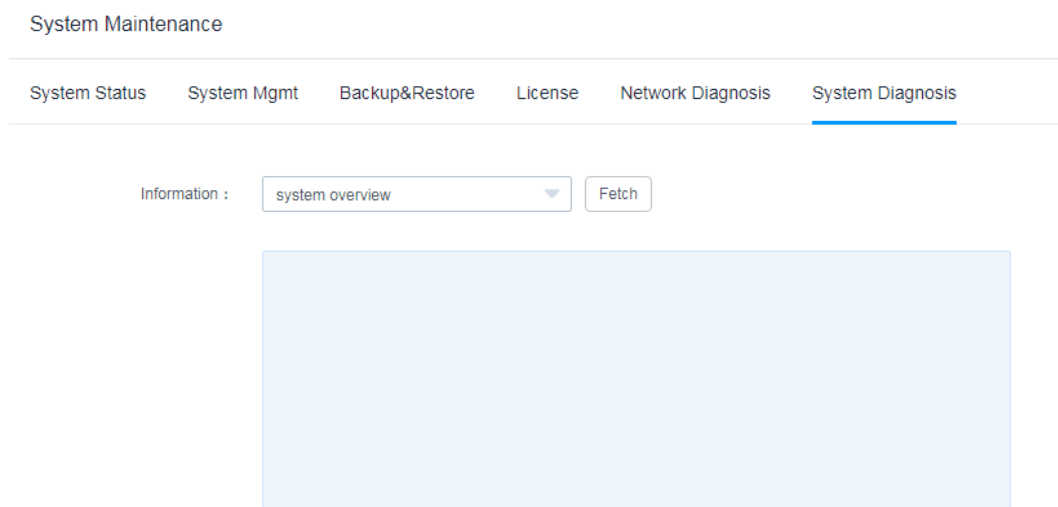
Step 3 Select an information type and then click **Fetch** to view the details.

Table 12-10 System diagnosis parameters

Parameter	Description
system overview	Obtains overview information about the CBH system, including memory, I/O, and CPU.
system load	Obtains information about the CBH system load.
system kernel	Obtains information about the CBH system kernel.
memory summary	Obtains information about the CBH system memory.

Parameter	Description
network interfaces	Obtains information about the CBH system NIC.
disk usage	Obtains information about the disk usage of the CBH system.
route table	Obtains route information about the CBH system.
ARP table	Obtains ARP information about the CBH system.

Figure 12-13 System Diagnosis



----End

12.4 About System

This topic walks you through how to view basic system information.

Prerequisites

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

Procedure

- Step 1** Log in to the CBH system.
- Step 2** On the left navigation pane, choose **System > About**.
- Step 3** View basic system information.

Table 12-11 System parameters

Parameter	Description
Product Name	CBH
Product ID	Unique authentication code of a product
Service Code	<p>This code is used by technical personnel to log in to the system background and manage the background. Click View to obtain the code.</p> <p>After obtaining the service code, keep it secure. Do not send it to the public information platforms.</p> <p>NOTE When technical personnel use the service code to log in to the system backend, a piece of root account login record will be added to the bastion host login log.</p>
API Access Key	<p>Used for node authentication on the unified management platform</p> <ul style="list-style-type: none"> ● View: To view the information, enter the password of the system administrator admin, access key secret, and access key ID. ● Update and Clear: To update or clear the API credentials, enter the password of the system administrator admin. After the password is updated or cleared, the node managed by the unified management platform becomes invalid.
HA Key	<p>Used to configure the HA</p> <p>When configuring the standby node for HA on the web interface, connect the programs on the standby node to the specified active one, perform the validity check based on configuration information, and then modify the configuration on the active node after the validity check is passed.</p>
Version	Version of the current system
Device System	Version of the current system software
Issue Time	Release date of the current system

----End

13 FAQs

13.1 Product Consulting

13.1.1 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.

13.1.2 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

13.1.3 What Is the Number of Assets?

The number of assets indicates the number of resources running on devices such as cloud hosts managed in a CBH system. The number of resources is the total number of protocols and applications that need to be operated and maintained for a cloud host.

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.

13.1.4 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.

13.1.5 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.

13.1.6 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.

13.1.7 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.
- 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.

13.1.8 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.

13.1.9 How Can I Configure Ports for a CBH Instance?

To properly use CBH, configure the instance and resource security group ports by referring to [Table 13-1](#).

Table 13-1 Inbound and outbound rule configuration reference

Scenario Description	Direction	Protocol/ Application	Port
Accessing CBH through a web browser (HTTP and HTTPS)	Inbound	TCP	80, 443, and 8080
Accessing a CBH system through Microsoft Terminal Services Client (MSTSC)	Inbound	TCP	53389
Accessing a CBH Instance Through an SSH Client	Inbound	TCP	2222
Accessing CBH instances through FTP clients	Inbound	TCP	20~21
Remotely accessing Linux ECSs of CBH instances over SSH clients	Outbound	TCP	22
Remotely accessing Windows ECSs of CBH instances over the RDP Protocol	Outbound	TCP	3389
Accessing Oracle databases through CBH instances	Inbound	TCP	1521
Accessing Oracle databases through CBH instances	Outbound	TCP	1521
Accessing MySQL databases through CBH instances	Inbound	TCP	33306
Accessing MySQL databases through CBH instances	Outbound	TCP	3306
Accessing SQL Server databases through CBH instances	Inbound	TCP	1433
Accessing SQL Server databases through CBH instances	Outbound	TCP	1433
Accessing DB databases through CBH instances	Inbound	TCP	50000
Accessing DB databases through CBH instances	Outbound	TCP	50000
Accessing GaussDB databases through CBH	Inbound	TCP	18000

Scenario Description	Direction	Protocol/ Application	Port
Accessing GaussDB databases through CBH	Outbound	TCP	18000
License servers	Outbound	TCP	9443
Cloud services	Outbound	TCP	443
Accessing a CBH system through the SSH client in the same security group	Outbound	TCP	2222
SMS service	Outbound	TCP	10743 and 443
Domain name resolution service	Outbound	UDP	53
Accessing PGSQL databases through CBH	Inbound	TCP	15432
Accessing PGSQL databases through CBH	Outbound	TCP	5432

13.1.10 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.

13.1.11 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 13-2](#).

Table 13-2 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)
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 13-3](#) 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 13-3 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 13-4 lists the database clients that are deployed on Linux servers and can be directly configured and called by CBH.

Table 13-4 Supported Linux database clients

Application Type	Supported Client
Dameng Database	Dameng management tool V8

13.2 About Instance Request

13.2.1 About Instance Request and Deployment

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

No. To modify VPC configurations,

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

No. To modify VPC configurations,

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?](#)

13.2.2 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.

CBH Instance Editions

Table 13-5 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: automatic O&M and database O&M audit

Table 13-6 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
500	500	8 cores	16 GB	100 GB	2,000 GB
1,000	1,000	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 13-6](#) 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.

13.2.3 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 **default** is created for each user. You can select **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 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 CBH Instance?](#)

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 **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 3 On the displayed page, click **Create Security Group** and create a security group.

Step 4 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.

Step 5 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 13-1](#).

Step 6 After the security group rules are configured, 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.

13.3 About File Transfer

13.3.1 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.

- 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?](#)

13.3.2 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.

----End

13.3.3 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.

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.

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.

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.

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.

----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.

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.

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.

----End

13.3.4 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.
- The used space of a personal net disk cannot be queried.
- You can only manually delete files to free up space.

13.3.5 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 13-1 Mind map for troubleshooting



Table 13-7 Solutions

Troubleshooting Procedure	Possible Causes	Solution
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"> 1. Enable permissions to manage files for a certain resource. 2. 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 space cannot be automatically cleared. The Personal Netdisk space is insufficient, or the available system storage space 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?
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.
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

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.

13.3.6 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**.
- 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?](#)

13.3.7 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.

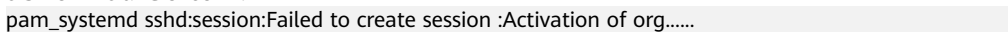
Possible Cause

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](#).

- 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

13.3.8 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.

13.3.9 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

13.3.10 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.

13.4 About CBH System Login

13.4.1 Login Methods and Password Issues

13.4.1.1 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.

13.4.1.2 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.

13.4.1.3 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.

13.4.1.4 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.

13.4.1.5 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.

- 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 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.

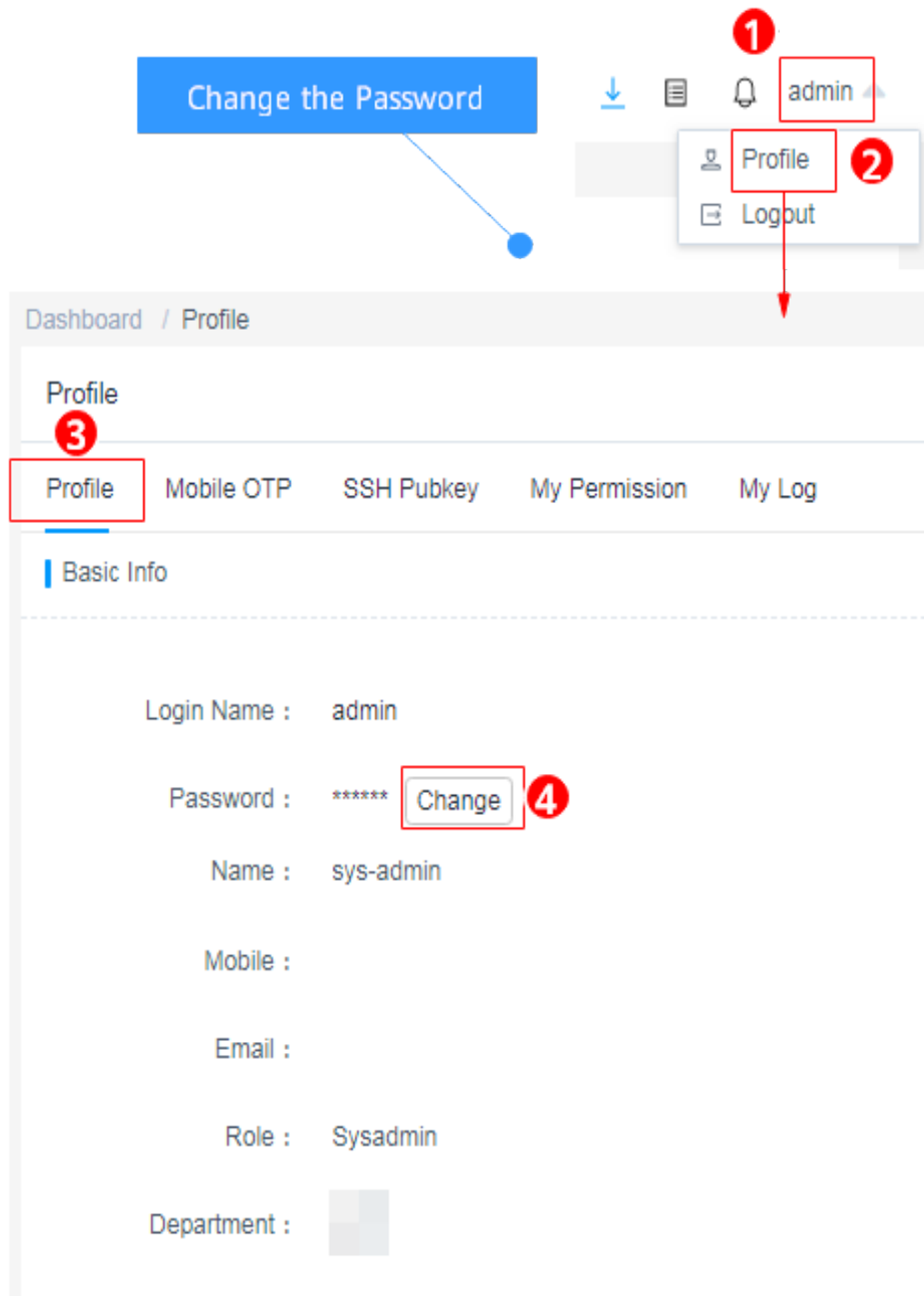
----End

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 13-2](#) and click **Password** to go to the **Change Password** dialog box.

Figure 13-2 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

13.4.1.6 How Do I Use IAM to Log In to a CBH Instance?

Constraints

- Before using an IAM account to log in, the browser cache must be cleared.
- The IAM account must have the `cbh:instance:login` permission.
- The IAM account must have permissions for all resources or at least a specific resource.

Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page, select a region, and choose **Security > Cloud Bastion Host** to go to the CBH instance management page.
- Step 3** Locate the row containing the target instance and click **Remote Login > IAM Login** in the **Operation** column.

----End

13.4.2 Multifactor Verification

13.4.2.1 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.

13.4.2.2 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

13.4.2.3 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 CBH instance, and the CBH 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.

13.4.2.4 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

13.4.2.5 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.

13.4.2.6 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.

13.4.3 Login Security Management

13.4.3.1 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 13-8](#).

Table 13-8 Parameters for configuring lockout parameters

Parameter	Description
Lock	You can select User or Source IP . <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

Parameter	Description
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

13.4.3.2 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.
- 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.

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

13.5.1 Users

13.5.1.1 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.

13.5.1.2 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.

- The CBH does not support mobile numbers outside China.
- 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

13.5.1.3 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**.

13.5.2 Adding Resources to a CBH System

13.5.2.1 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.

13.5.2.2 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 13-9 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

13.5.2.3 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

13.5.2.4 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, privileged account, and password.

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, including new account passwords set after a password change policy is configured.

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

13.5.2.5 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.

13.5.2.6 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 13-10](#).

Table 13-10 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**.

13.5.2.7 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.

13.5.2.8 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 Ops**. You are required to enter the account username and password to log in to the managed host.

----End

13.5.2.9 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.

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

Perform the following steps:

Procedure

- Step 1** Purchase 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.
 - Step 3** Add application resources.
- End

13.5.2.11 How Do I Add a Server with an IPv6 Address to a CBH Instance?

CBH supports servers with IPv6 addresses. You must enable the IPv6 subnet when purchasing the CBH instance.

13.5.2.12 What is an Empty Account?

If no account is added for a host or application resource in your CBH system, the **Empty** account is generated by default. So, when you log in to the host or application resource through CBH, you can use the username and password of **Empty**, or the login will fail.

13.5.3 System Configuration

13.5.3.1 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

13.5.3.2 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

13.5.3.3 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.

13.6 Resources Managed in a CBH System

13.6.1 Operation Management

13.6.1.1 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.

13.6.1.2 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

13.6.1.3 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.

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

13.6.1.4 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.

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

Table 13-11 lists the algorithms supported by CBH 3.3.26.0 and later over SSH.

Table 13-11 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

13.6.2 O&M Operations

13.6.2.1 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.

13.6.2.2 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

13.6.2.3 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 13-12](#).

Table 13-12 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

13.6.2.4 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**.

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

13.6.2.5 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.

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.

13.6.2.6 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.

13.7 O&M Log Audit

13.7.1 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.

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 13-13 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>

13.7.2 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**.

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

13.7.3 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](#).

13.7.4 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.

13.7.5 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.

13.7.6 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.

13.7.7 Can I Audit User Operations If a User Logs In to Server A Through the CBH System and Then Logs In to Server B from Server A?

Yes. All maintenance operations performed by the same user on server A and server B can be audited by video. For Linux servers, even all commands executed on server B can be recorded.

13.7.8 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.

13.7.9 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.

13.8 Troubleshooting

13.8.1 CBH System Login Failures

13.8.1.1 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.

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

13.8.1.2 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.

13.8.1.3 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.

13.8.1.4 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.

13.8.1.5 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.

13.8.1.6 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."

13.8.1.7 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 13-3 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	-	
100.64.0.0	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 CBH system to 3.3.26.0. .

13.8.2 CBH Managed Resource Login Failures

13.8.2.1 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 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.

13.8.2.2 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.

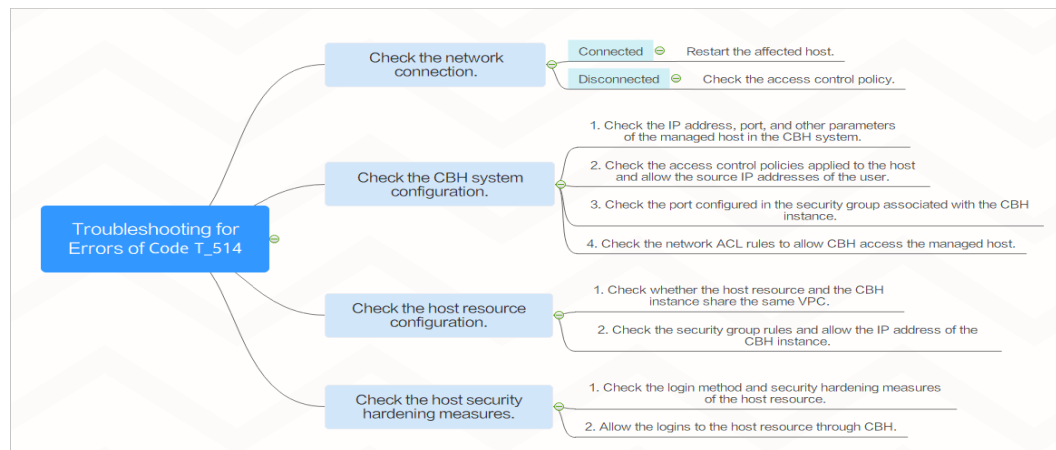
Possible Causes

- 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 13-4 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.
 - 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

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

13.8.2.3 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.

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

13.8.2.4 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 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)

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/ssh.deny.hostguard` file.

1. Log in to the Linux Server as an administrator.
2. Run the following command to query the `/etc/ssh.deny.hostguard` file:
cat /etc/ssh.deny.hostguard
3. Run the following command to open the `/etc/ssh.deny.hostguard` file:
vim /etc/ssh.deny.hostguard
4. Check whether the `/etc/ssh.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

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

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

13.8.2.5 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** 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.

13.8.2.6 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.

----End

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.

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, you are not allowed to establish remote connections with the host resources. In this case, you can enable the **admin console** in the CBH system to implement force logins. This means you can force the CBH system to establish login connection by forcibly logging out other logged in users.

Step 1 Log in to the 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 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, if the number of connections exceeds the upper limit, the user is forced to log in.

----End

13.8.2.7 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.

13.8.2.8 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

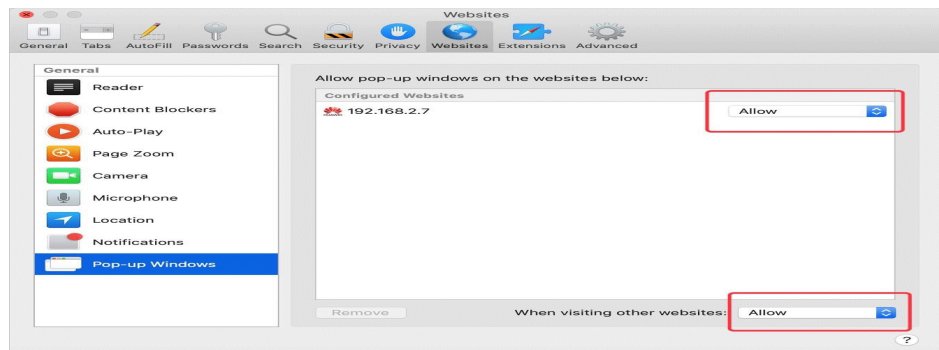
1. Check whether the browser is a recommended one.

Table 13-14 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 Pop-up 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 13-5 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.

13.8.2.9 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 applications that can be called by 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.

13.8.2.10 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.

13.8.2.11 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.

To fix this issue, change your CBH instance specifications to increase the concurrent request quota.

13.8.2.12 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

13.8.3 Maintenance Issues

13.8.3.1 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 13-15](#).

Table 13-15 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.

13.8.3.2 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.

13.8.3.3 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.

13.8.3.4 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
 - Increase the login timeout period.
 - 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.

13.8.3.5 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 search for Chinese contents.

----End

13.8.3.6 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

13.8.3.7 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. It is recommended that the bandwidth be greater than 5 Mbit/s. For details, see "VPC Shared Bandwidth Overview."

----End

13.8.3.8 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.

- The clipboard function is enabled for host resources.
- Grant the clipboard permission to the user.
- 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. The file management function is enabled for host resources.
2. Grant the file management permission to the user.

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

13.8.3.9 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 13-16](#).

Table 13-16 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 Code	Error Message	Troubleshooting
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 <code>/etc/hosts.deny</code> 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 <code>route -n</code> 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_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 Code	Error Message	Troubleshooting
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_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 Code	Error Message	Troubleshooting
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.

13.8.3.10 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

A Change History

Released On	Description
2024-05-30	<p>This issue is the second official release.</p> <p>Optimized:</p> <ul style="list-style-type: none">• Checking CBH Instance Details: Added some instance parameters.• Upgrading the CBH System Version: Added the version description and restrictions.• Configuring SMS Login Authentication, Configuring Mobile OTP Login Authentication, Configuring USB Key Login Authentication, and Configuring OTP Token Login Authentication: Changed some screenshots.• Configuring USB Key Login Authentication: Modified the description of restrictions.• Configuring the Login Password Policies: Updated the description of password strength verification.• Dashboard: Updated the description of the statistics control board.• Creating a User and Assigning a Role to the User: Updated the description of some parameters.• Viewing Operation Reports: Modified the description of restrictions.• Network Diagnosis: Modify TCP port check description.• Logging In to Managed Resources Using a Web Browser for O&M: Optimized the description.• Upgrading the CBH System Version and Overview: Modified the port usage description.• Viewing the Host Resource List and Setting Resource Labels: Added restrictions on login configuration downloads.

Released On	Description
	<ul style="list-style-type: none"> • Logging In to Managed Resources Using a Web Browser for O&M: Added restrictions on Windows resource O&M. • Creating a Script: Modified the description of restrictions. <p>Added:</p> <ul style="list-style-type: none"> • Managing CBH Instance Permissions and Supported Actions: Added actions supported. • CBH Operations Supported by CTS: Added operation items supported. • Overview: Added description of the PGSQL type. • Configuring User Login Lockout: Added the user + source IP address locking mode. • Configuring a Resource Account • Configuring Client Login • Configuring a User Expiration Reminder • Configuring Session Limit • Configuring User Login Restrictions: Added IAM login method. • Creating a Proxy Server • Managing Host Resources Using CBH, Managing Application Servers Using CBH, Querying and Editing Managed Resource Configurations, Creating an ACL Rule and Associating It with Users and Resource Accounts, and Querying and Editing an ACL Rule: Added keyboard audit. • Managing Host Resources Using CBH and Adding Accounts of Managed Host or Application Resources into CBH: Added CSMS credentials login and sudo login modes. • Managing Command Sets: Added description of batch importing command sets.
2023-10-30	This issue is the first official release.