

# Cloud Bastion Host (CBH)

## Service Overview

**Issue** 01  
**Date** 2022-12-01



**Copyright © Huawei Technologies Co., Ltd. 2024. All rights reserved.**

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

## **Trademarks and Permissions**



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

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

## **Notice**

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

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

## **Huawei Technologies Co., Ltd.**

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

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

Email: [support@huawei.com](mailto:support@huawei.com)

# Security Declaration

## Vulnerability

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

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

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

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

---

# Contents

---

<b>1 Cloud Bastion Host.....</b>	<b>1</b>
<b>2 Features.....</b>	<b>2</b>
<b>3 Product Advantages.....</b>	<b>11</b>
<b>4 Application Scenarios.....</b>	<b>13</b>
<b>5 Edition Differences.....</b>	<b>15</b>
<b>6 Basic Concepts.....</b>	<b>20</b>
<b>7 Pricing Details.....</b>	<b>21</b>
<b>8 Security.....</b>	<b>23</b>
8.1 Shared Responsibilities.....	23
8.2 Asset Identification and Management.....	24
8.3 Identity Authentication and Access Control.....	24
8.4 Data Protection Controls.....	25
8.5 Audit and Logging.....	28
8.6 Service Resilience.....	30
8.7 Certificates.....	30
<b>9 Restrictions on Using CBH.....</b>	<b>32</b>
<b>10 Permissions Management of CBH Instances.....</b>	<b>38</b>
<b>11 IAM-based Permissions Management.....</b>	<b>42</b>
<b>12 CBH and Other Services.....</b>	<b>47</b>
<b>13 Personal Data Protection Mechanism.....</b>	<b>49</b>
<b>14 Security Statement.....</b>	<b>52</b>
<b>A Change History.....</b>	<b>54</b>

# 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

# 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 2-1** 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"><li>• <b>Batch importing</b> CBH enables you to synchronize users from a third-party server or import users in batches, eliminating the need to create users repeatedly.</li><li>• <b>User groups</b> CBH allows you to add users of the same type in a group and assign permissions by user group.</li><li>• <b>Batch management</b> CBH enables you to manage user accounts in batches, including deleting, enabling, and disabling user accounts, resetting user passwords, and modifying basic user configurations.</li></ul>

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&amp;M.</p> <ul style="list-style-type: none"> <li>● Resource types           <p>CBH supports management of a wide range of resource types, including host (such as Windows and Linux hosts), Windows application, and database (such as MySQL and Oracle) resources.</p> <ul style="list-style-type: none"> <li>- 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.</li> <li>- 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.</li> </ul> </li> <li>● Resource management           <ul style="list-style-type: none"> <li>- 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&amp;M.</p> </li> <li>- 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> </li> <li>- 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> </li> <li>- 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> </li> <li>- 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> </li> <li>- Batch management</li> </ul> </li> </ul>



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 2-2** 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"> <li>● 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.</li> <li>● 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.</li> <li>● Login restrictions CBH controls system user logins from many dimensions, including login validity period, login duration, multi-factor verification, IP addresses, and MAC addresses.</li> </ul>

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"> <li>● 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&amp;M initiates an O&amp;M session, the watermark indicating their identity will be displayed in the background of the session window.</li> <li>● 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.</li> <li>● 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.</li> <li>● Batch authorization You can grant permissions for multiple resources to multiple users by user group or account group.</li> </ul>

## 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 2-3** 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"><li>• <b>System login logs</b> 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.</li><li>• <b>System operation logs</b> All system operation actions are recorded. System operation logs can be exported with just a few clicks.</li><li>• <b>System reports</b> 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.</li><li>• <b>Alarm notification</b> 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.</li></ul>

Function	Description
Resource O&M audit	<p>A CBH system records user operations throughout the entire O&amp;M process and supports multiple O&amp;M auditing techniques. It audits user operations, identifies O&amp;M risks, and provides the basis for tracing and analyzing security events.</p> <ul style="list-style-type: none"> <li>● Auditing techniques <ul style="list-style-type: none"> <li>- Linux command audits For command operations through character-oriented protocols (such as SSH and Telnet), a CBH system records the entire O&amp;M process, parses operation commands, reproduces operation commands, and quickly locates and replays operations using keywords in input and output results.</li> <li>- 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.</li> <li>- 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.</li> <li>- 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.</li> </ul> </li> <li>● O&amp;M audit methods <ul style="list-style-type: none"> <li>- Real-time monitoring Ongoing O&amp;M sessions can be monitored, viewed, and terminated.</li> <li>- History logs All O&amp;M operations are recorded and history session logs can be exported with just a few clicks.</li> <li>- Session videos Linux commands and Windows operations can be recorded by video.  Video files can be downloaded with just a few clicks.</li> <li>- Operation reports CBH uses various reports to display O&amp;M statistics in one place, including O&amp;M action distribution over time, resource access times, session duration, two-person authorization, command interception, number of commands, and number of transferred files.</li> </ul> </li> </ul>

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"> <li>- 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.</li> </ul>

## O&M Functions

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

**Table 2-4** Efficient O&M functions

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

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

## 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.

# 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.



# 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.

# 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, 2,000, 5,000, and 10,000. The professional edition provides the following asset specifications: 10, 20, 50, 100, 200, 500, 1,000, 2,000, 5,000, and 10,000.

For more details, see [What Are Editions Available in CBH?](#)

## Differences on Specifications

CBH provides the following asset specifications: 10, 20, 50, 100, 200, 500, 1,000, 2,000, 5,000, and 10,000. For details about specifications, see [Table 1 Configuration of different specifications](#).

**Table 5-1** 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
2,000	1,500	8 cores	16 GB	100 GB	2,000 GB
5,000	2,000	16 cores	32 GB	100 GB	3,000 GB
10,000	2,000	16 cores	32 GB	100 GB	4,000 GB

**NOTICE**

The number of concurrent connections in [Table 5-1](#) 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 5-2** 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, and Azure AD 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

Function	Description	Standard edition	Professional edition
	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. <b>NOTE</b> This function applies to cloud databases as well as self-built databases.	Not supported	Supported
Account management	User lifecycle management <ul style="list-style-type: none"> <li>CBH allows you to create a single user account, import user accounts in batches, manage user accounts in batches, and manage user groups.</li> </ul>	Supported	Supported
	Resource account lifecycle management <ul style="list-style-type: none"> <li>CBH allows you to add resources and their accounts one by one or in batches, and classify added accounts into different groups for management.</li> </ul>	Supported	Supported
	Host resource management <ul style="list-style-type: none"> <li>CBH allows you to manage Linux or Windows hosts with the SSH, RDP, VNC, Telnet, FTP, SFTP, or Rlogin protocol configured.</li> </ul>	Supported	Supported
	Application resource management <ul style="list-style-type: none"> <li>CBH allows you to use Windows application servers to manage browser or client application resources, such as Google Chrome, Microsoft Edge, Mozilla Firefox, Oracle Tool and MySQL.</li> </ul>	Supported	Supported
	Database resource management <ul style="list-style-type: none"> <li>CBH allows you to manage DB2, MySQL, SQL Server, and Oracle databases.</li> </ul>	Not supported	Supported
	Automatic password change for managed accounts <ul style="list-style-type: none"> <li>CBH allows you to configure password change policies to let the system periodically change passwords of managed accounts.</li> </ul>	Supported	Supported

Function	Description	Standard edition	Professional edition
	Automatic synchronization of managed resource accounts <ul style="list-style-type: none"> <li>CBH allows you to configure account synchronization policies to let the system detect zombie accounts or unmanaged accounts in a timely manner.</li> </ul>	Not supported	Supported
Operation audit	System login and operation logging <ul style="list-style-type: none"> <li>CBH allows you to export system logs, generate system reports, and configure alarm notifications.</li> </ul>	Supported	Supported
	Resource O&M audit <ul style="list-style-type: none"> <li>CBH allows you to audit the entire O&amp;M process through multiple audit methods, such as monitoring on-going sessions, generating videos for history sessions, exporting text reports, and remote log backup.</li> </ul>	Supported	Supported
	Database operation audit <ul style="list-style-type: none"> <li>CBH allows you to audit the entire database O&amp;M process based on operation commands.</li> </ul>	Not supported	Supported
Efficient O&M	One-stop web browser O&M <ul style="list-style-type: none"> <li>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.</li> </ul>	Supported	Supported
	Third-party client O&M <ul style="list-style-type: none"> <li>CBH can interconnect with multiple O&amp;M tools with just a few clicks, including SSH, FTP, and SFTP client.</li> </ul>	Supported	Supported
	Database O&M <ul style="list-style-type: none"> <li>CBH allows you to log in to the target databases using the single sign-on (SSO) tool with just a few clicks.</li> </ul>	Not supported	Supported
	Automatic O&M <ul style="list-style-type: none"> <li>CBH allows you to manage scripts online and let the system periodically execute preset O&amp;M tasks.</li> </ul>	Not supported	Supported

Function	Description	Standard edition	Professional edition
Ticket application	Access and command authorization ticket application <ul style="list-style-type: none"> <li>• 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.</li> </ul>	Supported	Supported
	Database authorization ticket application <ul style="list-style-type: none"> <li>• 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.</li> </ul>	Not supported	Supported

# 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.



# 7 Pricing Details

## Billing Items

Billed based on the edition and required duration of the CBH instance.

**Table 7-1** Billing items

Billing Item	Billing Description
CBH instances	Billed based on the edition and required duration of the CBH instance.
Required duration	Billed on a yearly or monthly basis.
Elastic IP Address (EIP)	An EIP must be bound to the CBH instance if you want to log in to the CBH instance through a public network. EIPs are separately billed by bandwidth or traffic. For details, see <a href="#">EIP Pricing Details</a> . <b>NOTE</b> To ensure that the CBH system can work normally, ensure that the EIP bound to the mapped CBH instance is available.

### NOTE

To manage application resources through application publishing servers, purchase resources such as Windows servers, images, enterprise authorization codes, and client licenses at additional costs.

## Billing Modes

CBH is billed on a yearly/monthly basis only.

You can get a 17% discount for a one-year subscription, a 30% discount for a two-year subscription, and 50% discount for a three-year subscription. If you want to use CBH for a long time, buy it by the year to save more money.

For details, see [CBH Pricing Details](#).

## Changing Billing Options

- Changing instance specifications  
If your business increases, CBH allows you to change CBH specifications within the billing cycle. You can upgrade your instance from a basic edition to an enhanced edition or to another basic edition of higher specifications. However, the edition of an instance cannot be changed to a lower one.
- Unsubscribing  
If you want to stop using a CBH instance, go to the Billing Center to [unsubscribe](#) from it.

## Renewal

When a yearly/monthly-billed CBH instance is about to expire, you can choose **More > Renew** in the **Operation** column on the CBH instance list page to renew the instance to extend the validity period. After the instance is renewed, the mapped CBH system is automatically renewed.

For more information about renewal, including exporting the renewal list and changing subscriptions, see [Renewal Management](#).

## Expiration and Overdue Payment

If a yearly/monthly-billed resource fails to be renewed in a given time, there is a retention period. The retention period varies depending on subscription methods. For details about how to process resources in the retention period, see [Retention Period](#).

When your account is in arrears, you can view the arrears details. You need to pay the arrears within the specified period. To prevent resources from being stopped or released, top up your account in a timely manner. For details, see [Making Repayments](#).

# 8 Security

---

## 8.1 Shared Responsibilities

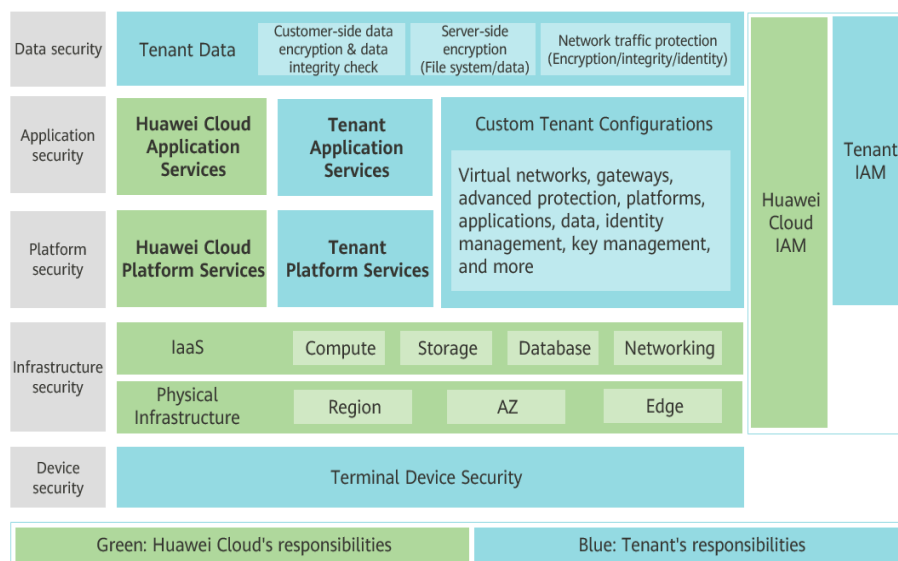
Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system for different regions and industries based on Huawei's unique software and hardware advantages, laws, regulations, industry standards, and security ecosystem.

**Figure 8-1** illustrates the responsibilities shared by Huawei Cloud and users.

- **Huawei Cloud:** Ensure the security of cloud services and provide secure clouds. Huawei Cloud's security responsibilities include ensuring the security of our IaaS, PaaS, and SaaS services, as well as the physical environments of the Huawei Cloud data centers where our IaaS, PaaS, and SaaS services operate. Huawei Cloud is responsible for not only the security functions and performance of our infrastructure, cloud services, and technologies, but also for the overall cloud O&M security and, in the broader sense, the security and compliance of our infrastructure and services.
- **Tenant:** Use the cloud securely. Tenants of Huawei Cloud are responsible for the secure and effective management of the tenant-customized configurations of cloud services including IaaS, PaaS, and SaaS. This includes but is not limited to virtual networks, the OS of virtual machine hosts and guests, virtual firewalls, API Gateway, advanced security services, all types of cloud services, tenant data, identity accounts, and key management.

**Huawei Cloud Security White Paper** elaborates on the ideas and measures for building Huawei Cloud security, including cloud security strategies, the shared responsibility model, compliance and privacy, security organizations and personnel, infrastructure security, tenant service and security, engineering security, O&M security, and ecosystem security.

**Figure 8-1** Huawei Cloud shared security responsibility model



## 8.2 Asset Identification and Management

CBH has been interconnected with RMS. In the upper right corner of Huawei Cloud Console, choose **Resources > My Resources** to view your resources, such as Elastic Cloud Server (ECS), Virtual Private Cloud (VPC), Object Storage Service (OBS), and Cloud Bastion Host (CBH). You can use RMS to view resource details, such as the ECS status and specifications.

CBH allows you to add Linux host, Windows host, and database resources using protocols such as SSH, RDP, VNC, TELNET, FTP, SFTP, DB2, MySQL, SQL Server, Oracle, SCP and Rlogin. You can add resources one by one or in batches. In addition, CBH can manage application servers for applications such as Google Chrome, Microsoft Edge, Mozilla Firefox, SecBrowser, Oracle Tool, MySQL, SQL Server Tool, dbisql, VNC Client, VSphere Client, and Radmin.

## 8.3 Identity Authentication and Access Control

### Identity Authentication

You can access a CBH instance through a web console or an SSH client. With a web console, you can use all CBH functions, such as resource configuration and command execution. With an SSH client, you can only maintain resources managed in the CBH system.

When you create a CBH instance, you are required to set a username and password. They are used for logging in to the CBH instance through a web console and SSH client. If web console is used, SMS messages, mobile OTPs, USB keys, and OTP devices can be used for login authentication.

### Access control

You can use security groups, web application firewalls (WAFs), access control lists (ACLs), and Virtual Private Clouds (VPCs) to control access to CBH instances.

**Table 8-1** Access controls supported by CBH

Access Control Method		Description
Permissions control	VPC	A Virtual Private Cloud (VPC) is a private and isolated virtual network created on Huawei Cloud. VPC along with EIP, Cloud Connect, and Dedicated Connect establishes a reliable, secure communication channel for your cloud resources to communicate with each other, the internet, and on-premises networks.
	Security Group	A security group is a collection of access control rules for cloud resources, such as cloud servers, containers, and databases, that have the same security protection requirements and that are mutually trusted within a VPC. You can define different access control rules for a security group, and these rules are then applied to all the instances added to this security group.
	Web Application Firewall (WAF)	WAF acts as a shield for web applications and websites. Powered by machine learning, WAF intelligently examines website traffic and defends against malicious requests and unknown threats.

## 8.4 Data Protection Controls

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, cannot be obtained by unauthorized or unauthenticated entities or people and to prevent data leakage, CBH encrypts your personnel data in transit and in storage to control access to the data and records logs for operations performed on the data.

### Personal Data to Be Collected

The following lists the personal data generated or collected by CBH.

Service	Type	Collection Method	Modifiable	Mandatory
CBH instances	Login name	Login name configured by the system administrator during user creation	No	Yes Login names are used to identify users.
	Password	<ul style="list-style-type: none"> <li>• Password configured by the system administrator during user creation or password resetting</li> <li>• Password reset during or after the first login</li> </ul>	Yes	Yes This password is used by the user to log in to a CBH system.
	Email address	<ul style="list-style-type: none"> <li>• Email address configured by the administrator during user creation</li> <li>• Email address entered by a user after the user logs in to the CBH system</li> </ul>	Yes	Yes This email address is used to receive notifications sent by the CBH system.

Service	Type	Collection Method	Modifiable	Mandatory
	Phone number	<ul style="list-style-type: none"> <li>Mobile phone number configured by the administrator during user creation</li> <li>Mobile phone number entered by a user after the user logs in to the CBH system</li> </ul>	Yes	Yes <ul style="list-style-type: none"> <li>This mobile phone number is used to receive SMS notifications from the CBH system.</li> <li>This mobile phone number is also used to receive verification codes sent by the CBH system during password resetting.</li> </ul>

- **Transmission Mode**

CBH supports HTTP and HTTPS. HTTPS is recommended to enhance the security of data transmission.

- **Storage Mode**

CBH uses advanced 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 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, plaintext passwords are invisible to anyone.

- **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, or dynamic token. This protects sensitive user information from breaches.

## 8.5 Audit and Logging

### Audit

A 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.

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 8-2** CBH audit functions

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"> <li>• System logon logs</li> </ul> <p>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.</p> <ul style="list-style-type: none"> <li>• System operation logs</li> </ul> <p>All system operation actions are recorded. System operation logs can be exported with just a few clicks.</p> <ul style="list-style-type: none"> <li>• System reports</li> </ul> <p>CBH displays all operation details of users in one place, including user statuses, user and resource creation, login methods, abnormal logins, and session controls.</p> <p>System reports can be exported with just a few clicks and periodically reported by email.</p> <ul style="list-style-type: none"> <li>• Alarm notifications</li> </ul> <p>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.</p>



Function	Description
Resource O&M audit	<p>A CBH system records user operations throughout the entire O&amp;M process and supports multiple O&amp;M auditing techniques. It audits user operations, identifies O&amp;M risks, and provides the basis for tracing and analyzing security events.</p> <ul style="list-style-type: none"> <li>● Audit techniques</li> </ul> <p>Linux command audits</p> <p>For command operations through character-oriented protocols (such as SSH and Telnet), a CBH system records the entire O&amp;M process, parses operation commands, reproduces operation commands, and quickly locates and replays operations using keywords in input and output results.</p> <ul style="list-style-type: none"> <li>● Windows operation audit</li> </ul> <p>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.</p> <ul style="list-style-type: none"> <li>● Database command audit</li> </ul> <p>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.</p> <ul style="list-style-type: none"> <li>● File transfer audits</li> </ul> <p>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.</p> <ul style="list-style-type: none"> <li>● O&amp;M audit methods</li> </ul> <p>Real-time monitoring</p> <p>Ongoing O&amp;M sessions can be monitored, viewed, and terminated.</p> <ul style="list-style-type: none"> <li>● History logs</li> </ul> <p>All O&amp;M operations are recorded and history session logs can be exported with just a few clicks.</p> <ul style="list-style-type: none"> <li>● Session videos</li> </ul> <p>Linux commands and Windows operations can be recorded by video recordings.</p> <p>Video recordings can be downloaded with just a few clicks.</p> <ul style="list-style-type: none"> <li>● Operation reports</li> </ul> <p>CBH uses various reports to display O&amp;M statistics in one place, including O&amp;M action distribution over time, resource access times, session duration, two-person authorization, command interception, number of commands, and number of transferred files.</p>

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"> <li>• Log Backup</li> </ul> <p>CBH allows you to back up history session logs to a remote Syslog server, FTP/SFTP server, and OBS bucket for disaster recovery.</p>

## Logging

CBH supports managing password change logs and command execution logs and viewing system logs and audit logs.

CBH had interconnected with Log Tank Service (LTS) for log collection, analysis, and storage. You can use LTS to efficiently perform device O&M management, service trend analysis, and security monitoring and audit.

For details about LTS and how to enable LTS, see "Configuring LTS for CBH".

## Log Records

A 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.

## 8.6 Service Resilience

CBH uses multi-active stateless cross-AZ deployment and inter-AZ data disaster recovery (DR) to enable service processes to be quickly started and recovered if a fault occurs, ensuring service continuity and reliability.

CBH defends against DoS attacks by taking advantages of Huawei Cloud DDoS attack mitigation capabilities

## 8.7 Certificates

### Compliance Certificates

Huawei Cloud services and platforms have obtained various security and compliance certifications from authoritative organizations, such as International Organization for Standardization (ISO). You can [download](#) them from the console.

Figure 8-2 Downloading compliance certificates

**Download Compliance Certificates**

Please enter a keyword to search

**BS 10012:2017**

BS 10012 provides a best practice framework for a personal information management system that is aligned to the principles of the EU GDPR. It outlines the core requirements organizations need to consider when collecting, storing, processing, retaining or disposing of personal records related to individuals.

Download

**ENS**

Mandatory law for companies in the public sector and their technology suppliers

Download

**Singapore Multi Tier Cloud Security (MTCS) Level 3**

The MTCS standard was developed under the Singapore Information Technology Standards Committee (ITSC). This standard requires cloud service providers to adopt well-rounded risk management and security practices in cloud computing. The HUAWEI CLOUD Singapore region has obtained the level 3 (highest) certification of MTCS.

Download

**Trusted Partner Network (TPN)**

The Trusted Partner Network (TPN) is a global, industry-wide media and entertainment content security initiative and community network, wholly owned by the Motion Picture Association. TPN is committed to raising content security awareness and standards and building a more secure future for content partners. TPN can help identify vulnerabilities, increase security capabilities, and efficiently communicate security status to customers.

Download

**ISO 27001:2022**

ISO 27001 is a widely accepted international standard that specifies requirements for management of information security systems. Centered on risk management, this standard ensures continuous operation of such systems by regularly assessing risks and applying appropriate controls.

Download

**ISO 27017:2015**

ISO 27017 is an international certification for cloud computing information security. It indicates that HUAWEI CLOUD's information security management has become an international best practice.

Download

## Resource Center

Huawei Cloud also provides the following resources to help users meet compliance requirements. For details, see [Resource Center](#).

Figure 8-3 Resource center

**Resource Center**

**White Papers**

Privacy Compliance White Papers | Industry Regulation Compliance White Papers | Guidelines and Best Practices

**Compliance with Argentina PDPL**

Base on the compliance requirements of Argentina PDPL and Resolution 47/2018, the whitepaper shares Huawei Cloud's privacy protection experience and practices and the measures that help customer meet the compliance requirements of Argentina PDPL and Resolution

**Compliance with Brazil LGPD**

Huawei Cloud shares the experience and practice in privacy protection in compliance with Brazil's LGPD and describes how to help customers meet Brazil's LGPD compliance requirements.

**Compliance with Chile PDPL**

Huawei Cloud shares the experience and practices regarding privacy protection when complying with PDPL from the Republic of Chile, as well as describe how to help customers meet PDPL compliance requirements in the Republic of Chile.

**Compliance with PDPO of the HK**

Huawei Cloud shares the experience and practices regarding privacy protection when complying with PDPO from Hong Kong SAR, China, as well as describe how to help customers meet PDPO compliance requirements in Hong Kong SAR, China.

# 9 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 [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 9-1](#).
- A CBH system can be logged in only through IP address and port number.

**Table 9-1** 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
Accessing GaussDB databases through CBH	Outbound	TCP	18000
License servers	Outbound	TCP	9443

Scenario Description	Direction	Protocol/ Application	Port
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

## Supported Resources

You can use CBH to manage servers you purchased on other clouds and on-premises servers as long as they can communicate with CBH through protocols supported by CBH and these servers.

- 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
  - Relational Database Service (RDS) DB instances
  - Databases on Elastic Cloud Servers (ECSs)
- Supported database versions

**Table 9-2** 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 9-3](#) lists the supported operating system versions.

**Table 9-3** 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 9-4** 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 <b>NOTE</b> 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 9-5** Clients that can be invoked during operation

Operation Method	Resource Protocol Type/Application Type	Supported Client
Database operation (in the <b>Host Operation</b> module)	MySQL	Navicat 11, 12, 15, and 16 MySQL Administrator 1.2.17 MySQL CMD DBeaver 22 and 23

Operation Method	Resource Protocol Type/Application Type	Supported Client
	SQL Server	Navicat 11, 12, 15, and 16 SSMS 17
	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](#).

# 10 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. For details about the actions supported by CBH, see [Permissions and Supported Actions](#).

**Table 10-1** lists all the system-defined roles and policies supported by CBH instances.

**Table 10-1** 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 10-2** lists the common operations for each system-defined policy or role of CBH instances. Select the policies or roles as required.

**Table 10-2** 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

Operation	CBH FullAccess	CBH ReadOnlyAccess
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
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

## Related Topics

- [IAM Service Overview](#)
- [Creating a User Group and Granting CBH Instance Permissions to the Group.](#)
- [Creating Custom Policies for CBH Instances](#)
- [CBH Instance Permissions and Supported Actions](#)

## 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"
      ]
    }
  ]
}
```

# 11 IAM-based Permissions Management

---

If you need to assign different permissions to employees in your enterprise to access your CBH resources, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control. If your account works good for you and you do not need an IAM account to manage user permissions, then you may skip over this chapter.

IAM is a free service. You only pay for the resources in your account.

With IAM, you can control the access to Huawei Cloud resources through authorization. For example, some developers in your enterprise need to use CBH but you do not want them have permissions to high-risk operations such as deleting CBH instances. To achieve such purpose, you can use IAM to grant them only the permissions to use CBH, but not delete CBH instances. With IAM, you can control their usage of CBH resources.

IAM supports role/policy-based authorization and identity policy-based authorization.

The following table describes the differences between these two authorization models.

**Table 11-1** Differences between role/policy-based and identity policy-based authorization

Name	Core Relationship	Permission	Authorization Method	Application Scenario
Role/Policy-based authorization	User-permissions-authorization scope	<ul style="list-style-type: none"> <li>• System-defined roles</li> <li>• System-defined policies</li> <li>• Custom policies</li> </ul>	Assigning roles or policies to principals	To authorize a user, you need to add it to a user group first and then specify the scope of authorization. It provides a limited number of condition keys and cannot meet the requirements of fine-grained permissions control. This method is suitable for small- and medium-sized enterprises.
Identity Policy-based authorization	User-policy	<ul style="list-style-type: none"> <li>• System-defined policies</li> <li>• Custom identity policies</li> </ul>	<ul style="list-style-type: none"> <li>• Assigning identity policies to principals</li> <li>• Attaching identity policies to principals</li> </ul>	You can authorize a user by attaching an identity policy to it. User-specific authorization and a variety of key conditions allow for more fine-grained permissions control. However, this model can be hard to set up. It requires a certain amount of expertise and is suitable for medium- and large-sized enterprises.

Assume that you want to grant IAM users permission to create ECSs in CN North-Beijing4 and OBS buckets in CN South-Guangzhou. With role/policy-based authorization, the administrator needs to create two custom policies and assign both to the IAM users. With identity policy-based authorization, the administrator only needs to create one custom identity policy and configure the condition key **g:RequestedRegion** for the policy, and then attach the policy to the users or grant the users the access permissions to the specified regions. Identity policy-based authorization is more flexible than role/policy-based authorization.

Policies/identity policies and actions in the two authorization models are not interoperable. You are advised to use the identity policy-based authorization model.

For more information about IAM, see [IAM Service OverviewIAM Service OverviewIAM Service Overview](#).

## Identity Policy-based Permissions Management

CBH supports identity policy-based authorization. New IAM users do not have any permissions assigned by default. You need to first add them to one or more groups and then attach policies or roles to these groups. The users then inherit permissions from the groups and can perform specified operations on cloud services based on the permissions they have been assigned.

CBH is a project-level service deployed and accessed in specific physical regions. When you set **Scope** to **Region-specific projects** and select the specified projects (for example, **ap-southeast-2**) in the specified regions (for example, **AP-Bangkok**), the users only have permissions for ECSs in the selected projects. If you set **Scope** to **All resources**, the users have permissions for ECSs in all region-specific projects. When accessing CBH, the users need to switch to a region where they have been authorized to use the CBH service.

**Table 1** lists all CBH system permissions. System-defined policies in role/policy-based authorization are not interoperable with those in identity policy-based authorization.

**Table 11-2** CBH system permissions

Role/Policy Name	Description	Type	Dependency
CBH FullAccess	All permissions (except the payment permission) on CBH instances	System-defined policies	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 policies	None
CBH ServiceLinkedAgencyPolicy	Agency permissions required for CBH to access KMS and CSMS.	System-defined policies	None

**Table 11-3** describes the common operations supported by each system-defined permission of CBH.

**Table 11-3** Common operations supported by system-defined permissions

Operation	CBH FullAccess	CBH ReadOnlyAccess	CBH ServiceLinkedAgencyPolicy
Creating a CBH instance	√	x	x



Operation	CBH FullAccess	CBH ReadOnlyAccess	CBH ServiceLinkedAgencyPolicy
Changing CBH instance specifications (changing specifications)	√	x	x
Querying the CBH instance list	√	√	x
Upgrading the CBH system version	√	x	x
Querying total ECS quota	√	x	x
Binding or unbinding an EIP	√	x	x
Restarting a CBH instance	√	x	x
Starting a CBH instance	√	x	x
Stopping a CBH instance	√	x	x
Querying the AZ of a CBH instance	√	x	x
Checking whether an IPv6 CBH instance can be created	√	x	x
Checking network connection between the CBH instance and the license center	√	x	x
Modifying the network of the CBH instance to ensure that the CBH instance can communicate with the license center	√	x	x
Agency permission required for CBH to access KMS and CSMS resources	√	x	√

## Role/Policy Dependencies of the CBH Console

**Table 11-4** Role/Policy dependencies of the CBH console

Console Function	Dependent Service	Role/Policy Required
Creating a CBH instance	Elastic Cloud Server (ECS) Virtual Private Cloud (VPC)	In addition to CBH FullAccess role, the ECS CommonOperations and VPC FullAccess roles are required for an IAM user to create CBH instances on the console.
Binding or unbinding an EIP	Elastic IP (EIP)	In addition to CBH FullAccess role, the VPC FullAccess role is required for an IAM user to bind an EIP to or unbind an EIP from a CBH instance.
Updating the security group for a CBH instance	Virtual Private Cloud (VPC)	In addition to CBH FullAccess role, the VPC FullAccess role is required for an IAM user to change the security group for a CBH instance.

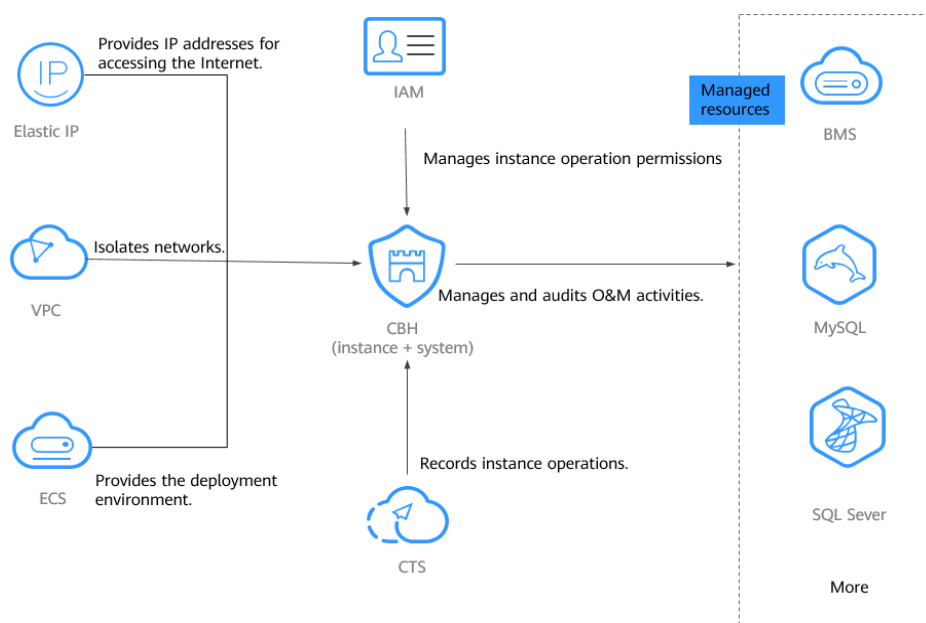
### Reference

- [IAM Service Overview](#)
- Assigning Permissions Using IAM
- Actions Supported by Identity Policy-based Authorization

# 12 CBH and Other Services

CBH needs to work with other cloud services. [Figure 12-1](#) shows the dependencies between CBH and other cloud services.

**Figure 12-1** 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.

## RDS

You can log in to the **Huawei Cloud Relational Database Service (RDS)** databases through CBH to manage databases and login credentials and audit O&M sessions in a more secure way.

## 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**.

# 13 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 personnel 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 13-1** lists the personal data generated or collected by CBH.

**Table 13-1** 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"> <li>• Password configured by the system administrator during user creation or password resetting</li> <li>• 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</li> </ul>	Yes	Yes This password is used by the user to log in to a CBH system.
	Email	<ul style="list-style-type: none"> <li>• Email address configured by the administrator during user creation</li> <li>• Email address entered by a user after the user logs in to the CBH system</li> </ul>	Yes	Yes This email address is used to receive notifications sent by the CBH system.
	Mobile number	<ul style="list-style-type: none"> <li>• Mobile phone number configured by the administrator during user creation</li> <li>• Mobile phone number entered by a user after the user logs in to the CBH system</li> </ul>	Yes	Yes <ul style="list-style-type: none"> <li>• This mobile phone number is used to receive SMS notifications from the CBH system.</li> <li>• This mobile phone number is also used to receive verification codes sent by the CBH system during password resetting.</li> </ul>

## 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.

# 14 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 14-1](#).

**Table 14-1** 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.

# A Change History

---

Released On	Description
2022-12-01	This issue is the first official release.