Cloud Bastion Host

Service Overview

Issue 07

Date 2025-09-29

HUAWEI

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 What Is CBH?

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 *Sarbanes-Oxley Act* and *DJCP (or MLPS)*
  - 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, DJCP, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27001, and other internal control regulations

2 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.

3 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.

4 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 4-1 Account management

Feature	Description
System user accounts	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. • 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	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. • Resource types CBH supports management of a wide range of resource types, including servers (such as Windows and Linux servers), Windows applications, and databases (such as MySQL and Oracle). – 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-server architecture Windows applications, such as Microsoft Edge, Google Chrome, and Oracle tools. • Resource management – Batch importing 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. – Account group management 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. – Password autofill 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. – Automatic password change of managed resource accounts CBH supports password rules so that you can periodically change account passwords to keep managed accounts secure. – Automatic synchronization of managed resource accounts 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. – Batch management CBH allows you to batch manage information and accounts of managed resources, including deleting a resource, adding a

Feature	Description
	resource label, modifying resource information, verifying a managed account, and deleting a managed account.

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 4-2 Permissions management

Function	Description
CBH system access permission	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. • 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	You can assign permissions for resources by user, user group, account, and account group. • 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 4-3 Operation audit description

Function	Description
System operation audit	All operations in a CBH system are recorded, and alarms are reported for misoperations, malicious operations, and unauthorized operations. • 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	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. ● Auditing techniques – 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 – 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
	Operation reports can be exported with just a few clicks and periodically sent by email. – Log backup You can back up history session logs to a remote Syslog server, OBS bucket, or FTP/SFTP server for disaster recovery.

O&M Functions

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

Table 4-4 Efficient O&M functions

Function	Description
O&M using a web browser	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. • 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	CBH enables one-click interconnection with multiple O&M tools, enabling you to perform O&M without changing client usage habits. • 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	CBH enables automated O&M to simplify online complex operations, eliminating repetitive manual effort and improving efficiency. • 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.

5 Edition Differences

CBH provides two editions: **Standard** and **Professional**. This section describes the differences between the editions. You can select an edition based on your service requirements.

CBH Instance Editions

Table 5-1 CBH instance editions

Edition	Function Description	Edition Specifications
Standard edition	Basic functions: identity authentication, permission control, account management, and operation audit	• 10 • 20 • 50 • 100 • 200 • 500 • 1000 • 2000 • 5000 • 10000
Professional edition	Basic functions: identity authentication, permission control, account management, and operation audit Enhanced functions: cloud service O&M, automated O&M, and database O&M audits	• 10 • 20 • 50 • 100 • 200 • 500 • 1000 • 2000 • 5000 • 10000

Specification Configuration

For details about the configuration differences between different specifications, see **Table 5-2**.

Table 5-2 Configuration of different specifications

Asset Quantity	Max. Concurrent Connections	CPUs	Memory	System Disk	Data Disk
10	10	4 vCPUs	8 GB	100 GB	200 GB
20	20	4 vCPUs	8 GB	100 GB	200 GB
50	50	4 vCPUs	8 GB	100 GB	500 GB
100	100	4 vCPUs	8 GB	100 GB	1,000 GB
200	200	4 vCPUs	8 GB	100 GB	1,000 GB
500	500	8 vCPUs	16 GB	100 GB	2,000 GB
1,000	1,000	8 vCPUs	16 GB	100 GB	2,000 GB
2,000	1,500	8 vCPUs	16 GB	100 GB	2,000 GB
5,000	2,000	16 vCPUs	32 GB	100 GB	3,000 GB
10,000	2,000	16 vCPUs	32 GB	100 GB	4,000 GB

NOTICE

The number for each asset quantity scale in **Max. Concurrent Connections** in **Table 5-2** is based on the concurrent connections of character protocol clients (such as the SSH client and MySQL client). The number of concurrent connections for graphical protocols (such as HTML5 web-based O&M and RDP client O&M) largely depends on factors like the resolution, color depth, and image dynamics. According to the lab test results, the number of concurrent connections for graphical protocols is only 1/10 to 1/3 of that for character protocols.

Function Details and Edition Differences

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 5-3**.

Table 5-3 Function details and edition differences

Function Module	Function	Description	Standard Edition	Professional Edition
Profile	Basic Info	You can view details about the current login user and change the name, phone number, email address, and password.	√	√
	Mobile OTP	You can get guidance for binding a mobile phone token and generating a dynamic password.	√	√
	SSH Pubkey	You can view information about all public keys, and add and manage SSH public keys.	√	√
	My Permission	You can view the permissions the logged-in user has.	√	√
	My Log	You can check logs of instance logins, operations, and resource logins by the logged-in user.	√	√
Basic system information	Dashboard	The dashboard displays the running status of the bastion host, including sessions, tickets, login status, operation status, host types, application types, and system status.	√	√
	Download Center	You can download some remote login tools and local player tools.	√	√
	Messages	After alarm rules are configured, an alarm is generated when an alarm rule is triggered.	√	√
	System	This area displays system details, such as the system ID, credential, version in use, and release date. You can also update credentials and HA keys and obtain service codes in this module.	√	√

Function Module	Function	Description	Standard Edition	Professional Edition
Authentication management	MFA	You can log in to the bastion host using an account (username and password), mobile phone token, SMS message, USB key, or OTP token. ● Account (username and password): The username and password are generated when you apply for the bastion host. This method is valid only for the first login. ● Mobile phone token: You need to configure the mobile number on the bastion host first. Then, after the mobile device or applet is registered, the dynamic password generated is required for logins. ● SMS: You need to configure a mobile number for the account on the bastion host. Then, a random verification code is required for logins. ● USB key: You need to get a USB key and associate it with the account first. Then, the USB key and passwords it generates are required for logins. ● OTP token: You need to get an OTP token device and associate it with the account first. Then, the OTP token and passwords it generates are required for logins.	√	√
	Remote authentication	You can configure remote authentication to use CBH centrally manage all accounts. CBH also allows you to authenticate user identities through AD, RADIUS, LDAP, Azure AD, and SAML remote authentication.	Supported	√
System accounts	User management	You can create, import, export, and delete accounts, configure user groups, and manage account login restrictions.	√	√
	User group management	Users can be managed by group. You can assign permissions to all users in a group at a time. You can create, delete, and edit a user group.	√	√

Function Module	Function	Description	Standard Edition	Professional Edition
	Role management	You can associate users with roles and assign operation and access permissions to the roles, including department administrators, policy administrators, audit administrators, and operation engineers. Only the **admin** account can add roles and modify the permissions of the roles.	√	√
	Resource account management	A resource account is used to log in to a resource managed by a bastion host instance. Multiple resource accounts can be created for a resource. The username and password of a resource account in CBH must be the same as those of the original account that the resource belongs to. Otherwise, the logins to the resource may fail, and no operations can be done for the resource through the bastion host.	√	√
	Resource account group management	You can manage resource accounts by group. You can authorize and verify resource accounts in batches by authorizing account groups. You can create, delete, and maintain account groups and manage account group information.	√	√
Resource	Host resource management	You can add host resources to a bastion host by creating, automatically discovering, importing, or cloning host resources. You can view details about all host resources and manage them through the bastion host centrally.	√	√
	Application resource management	You can import and create application resources through an application server. Then, you can view details about all application resources and manage them through the bastion host centrally. Note that you need to create the application server first.	√	√

Function Module	Function	Description	Standard Edition	Professional Edition
	Cloud resource management	You can import and create application resources through a Kubernetes server. Then, you can view details about all container resources and manage them through the bastion host centrally. Note that you need to create the Kubernetes server first.	×	√
	Resource OS type management	You can add tags to OS types and then group and manage resources by those tags. With OS type tags, you can change server passwords, store password change parameters, and run password rules for resources of a certain OS type at the same time.	√	√
System policies	ACL rules	This type of rule controls who can access which resources. ACL rules are associated with users or user groups. An ACL rule can restrict file transfer, file management, and login time. ACL rules can also be associated with resource accounts.	√	√
	Command rules	• This type of rule controls who can execute what commands for which resources. Command rules are associated with users or user groups. If a user attempts to execute a command that is restricted by a rule, the rule is triggered and takes preconfigured actions immediately. Command rules can also be associated with resource accounts. • You can create custom command sets.	√	√
	Database control rules	• This type of rule controls who can execute what database rules or rule sets. Database control rules are associated with users or user groups. If a user attempts to execute a database rule or rule set that is restricted by a database control rule, the control rule is triggered and takes preconfigured actions immediately. Database control rules can also be associated with resource accounts. • You can create custom rule sets.	×	√

Function Module	Function	Description	Standard Edition	Professional Edition
	Password rules	This type of rule is associated with resource accounts of hosts, so that a user can change passwords of resource accounts associated with a policy at the same time.	√	√
	Account synchronization rules	This type of rule helps synchronize host resource account details. Synchronization rules are associated with resource accounts. You can execute a synchronization rule to synchronize details of all resource accounts the rule is associated with at the same time.	×	√
Resource operation	Host resource operation	You can log in to host resources through browsers and clients and perform operations such as operation session sharing, file transfer, file management, and preset commands.	√	√
	Application resource operation	You can log in to application resources using a browser and perform operations such as operation session sharing, file transfer, and file management.	√	√
	Cloud service resource operation	You can log in to container resources using a browser and perform operations, including operation session sharing.	×	√
	Operation script management	You can import and edit scripts to be executed on the bastion host to complete complex or repetitive tasks, improving efficiency.	×	√
	Fast operation	You can directly run preset commands and scripts and transfer files on the bastion host for quick resource operation. Logs of all operations are provided.	×	√
	Operation task management	You can customize manual, scheduled, or scheduled operation tasks for commands, scripts, and file transfer. All task operation logs are provided.	×	√
System audit	Live session audit	All on-going sessions are logged. You can view the resource, type, account, and source IP address of any session.	√	√

Function Module	Function	Description	Standard Edition	Professional Edition
	Historical session audit	All closed historical sessions are logged. You can view the resource, type, account, and source IP address of any session.	√	√
	System log audit	All logins to and operations on the bastion host are logged in detail. You can check who logged in to the system over which IP address at which time, as well as what specific functions and operations are performed after each login.	√	√
	Operation report audit	An operation report collects statistics on the operation time, the number of resource access times, how long the session lasts, source IP address access status, session collaboration, two-person authorization, command interception, number of character commands, and number of transferred files by time, user, and resource.	√	√
	System report audit	A system report collects statistics on system operation control, resource operation, source IP addresses, login mode, abnormal logins, sessions, and status.	√	√
Ticket	ACL tickets	If you do not have the permission to access a resource, you can submit a ticket to apply for the permissions. Such permissions include file transfer, file management, keyboard audit. This type of permission is valid to a specific resource account in a fixed time range.	√	√
	Command control ticket management	If you do not have the permission to run commands to operate a certain resource, you can submit a ticket to apply for the permission for the resource. This type of permission is valid to a specific resource account in a fixed time range.	√	√
	Database ticket management	If you do not have the permission to perform operations on a database resource, you can submit a ticket to apply for the permission. This type of permission is valid to a specific resource account in a fixed time range.	×	√

Function Module	Function	Description	Standard Edition	Professional Edition
	Ticket approval management	This page displays details about all tickets. You can review tickets on this page.	√	√
	Ticket configuration	You can customize the scope, submission method, effective time, and approval process of a ticket.	√	√
System configuration	Security	You can configure the maximum incorrect password attempts, zombie users, password change period, login timeout, certificate, proxy security layer, mobile phone token, USB key, inspection, expiration notification, and session restriction.	√	√
	Network	You can view the network interface list, DNS, and default gateway details of the bastion host, and configure static routes.	√	√
	HA	If the bastion host is deployed in primary/standby mode, you can enable or disable HA.	√	√
	Port	You can check operation, web console, and SSH console ports in use. You can also change the port if needed, which is not recommended.	√	√
	Outgoing	You can configure the way to send alarms. Currently, email, SMS, and LTS are supported. After the LTS agent is installed, LTS can send bastion host logs to the server.	√	√
	Alarm	You can configure the alarm mode and level for different message types, including the login status, user operations, resource operation events, and operation activities.	√	√
	Theme	The default logo of the bastion host can be customized.	√	√

Function Module	Function	Description	Standard Edition	Professional Edition
Bastion host system maintenance	Data storage maintenance	You can view the usage of the system and data disks, modify the web disk space, customize the log storage period, and delete logs automatically or manually.	√	√
	Log backup	You can back up logs to a local PC, OBS server, syslog server, or FTP/SFTP server.	√	√
	System maintenance	You can view the status of the system, customize the system address and time, back up and restore the operating system, view the authorization information, and diagnose the network and system.	√	√

6 Security

6.1 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.

Unlike traditional on-premises data centers, cloud computing separates operators from users. This approach not only enhances flexibility and control for users but also greatly reduces their operational workload. For this reason, cloud security cannot be fully ensured by one party. Cloud security requires joint efforts of Huawei Cloud and you, as shown in **Figure 6-1**.

- **Huawei Cloud**: Huawei Cloud is responsible for infrastructure security, including security and compliance, regardless of cloud service categories. The infrastructure consists of physical data centers, which house compute, storage, and network resources, virtualization platforms, and cloud services Huawei Cloud provides for you. In PaaS and SaaS scenarios, Huawei Cloud is responsible for security settings, vulnerability remediation, security controls, and detecting any intrusions into the network where your services or Huawei Cloud components are deployed.
- **Customer**: As our customer, your ownership of and control over your data assets will not be transferred under any cloud service category. Without your explicit authorization, Huawei Cloud will not use or monetize your data, but you are responsible for protecting your data and managing identities and access. This includes ensuring the legal compliance of your data on the cloud, using secure credentials (such as strong passwords and multi-factor authentication), and properly managing those credentials, as well as monitoring and managing content security, looking out for abnormal account behavior, and responding to it, when discovered, in a timely manner.

Figure 6-1 Huawei Cloud shared security responsibility model

Cloud security responsibilities are determined by control, visibility, and availability. When you migrate services to the cloud, assets, such as devices, hardware, software, media, VMs, OSs, and data, are controlled by both you and Huawei Cloud. This means that your responsibilities depend on the cloud services you select. As shown in **Figure 6-1**, customers can select different cloud service types (such as IaaS, PaaS, and SaaS services) based on their service requirements. As control over components varies across different cloud service categories, the responsibilities are shared differently.

- In on-premises scenarios, customers have full control over assets such as hardware, software, and data, so tenants are responsible for the security of all components.
- In IaaS scenarios, customers have control over all components except the underlying infrastructure. So, customers are responsible for securing these components. This includes ensuring the legal compliance of the applications, maintaining development and design security, and managing vulnerability remediation, configuration security, and security controls for related components such as middleware, databases, and operating systems.
- In PaaS scenarios, customers are responsible for the applications they deploy, as well as the security settings and policies of the middleware, database, and network access under their control.
- In SaaS scenarios, customers have control over their content, accounts, and permissions. They need to protect their content, and properly configure and protect their accounts and permissions in compliance with laws and regulations.

6.2 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.

6.3 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 6-1 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.

6.4 Data Protection Controls

CBH takes many measures to keep data stored in CBH secure and reliable.

Table 6-2 CBH data protection controls and features

Data Protection Measure	Description
Protection for data at rest	CBH encrypts sensitive data in your website traffic to keep the data from leakage.
Protection for data in transit	Data is encrypted when it is transmitted between microservices to prevent leakage or tampering during transmission. CBH keeps your configuration data secure as the configuration data is transmitted over HTTPS.
Data isolation	CBH isolates its tenant zone from its management plane. Operation permissions for CBH are isolated by user. Your policies and logs are isolated from those of others.
Data destruction	To prevent information leakage caused by residual data, Huawei Cloud sets different retention periods based on the customer level. If the customer does not renew the subscription or recharge the account after the retention period expires, the data stored in the cloud service will be deleted and the cloud service resources will be released.

6.5 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 6-3 CBH audit functions

Function	Description
System operation audit	All operations in a CBH system are recorded, and alarms are reported for misoperations, malicious operations, and unauthorized operations. • 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 notifications 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	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. ● Audit techniques 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 audit 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 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 recordings. Video recordings 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
	Operation reports can be exported with just a few clicks and periodically sent by email. • 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.

Logging

CBH supports managing password 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.

6.6 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.

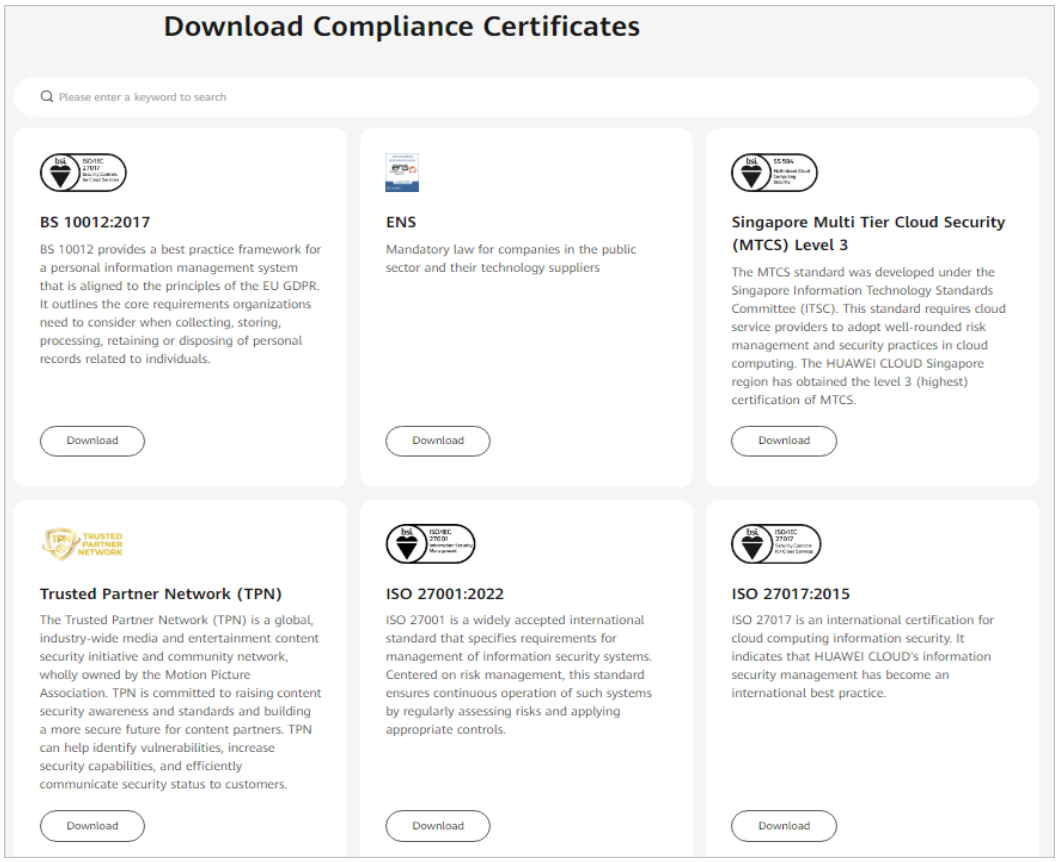
CBH defends against DoS attacks by taking advantages of Huawei Cloud DDoS attack mitigation capabilities

6.7 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.

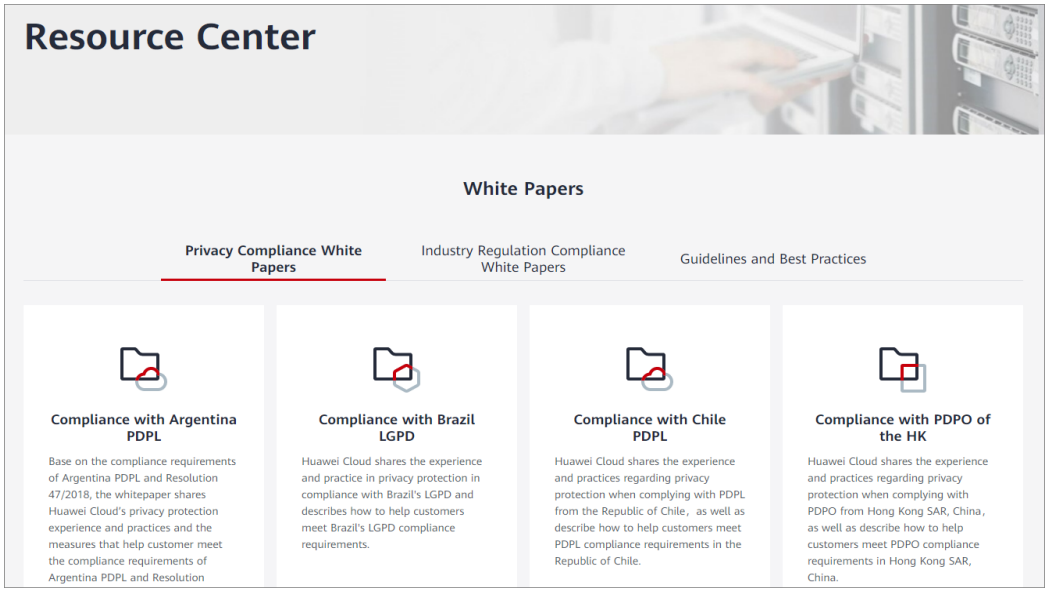
Figure 6-2 Downloading compliance certificates



Resource Center

Huawei Cloud also provides the following resources to help users meet compliance requirements. For details, see **Resource Center**.

Figure 6-3 Resource center



7 Permissions Management of CBH Instances

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

With IAM, you can create IAM users under your Huawei Cloud account for your employees, and assign permissions to the users to control their access to specific Huawei Cloud 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 Huawei Cloud account does not need individual IAM users for permissions management, then you may skip over this section.

Huawei Cloud IAM is a free service. You only pay for the resources in your account. For more details 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 which the permissions apply to. Make sure the permissions apply only to selected projects. 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. Some roles depend other roles to take effect. When you assign such roles to users, remember to assign the roles

they depend on. 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 7-1 lists some system-defined roles and policies supported by CBH instances.

Table 7-1 System permissions for CBH instances

Role/Policy Name	Description	Type
CBH FullAccess	All permissions (except the payment permission) on CBH instances	System-defined policy
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

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 7-2 lists the common operations for each system-defined policy or role of CBH instances. Select the policies or roles as required.

Table 7-2 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
Binding or unbinding an EIP	√	x

Operation	CBH FullAccess	CBH ReadOnlyAccess
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

Role/Policy Dependencies of the CBH Console

Table 7-3 Role/Policy dependencies of the CBH console

Console Function	Dependency	Role/Policy Required
Creating a bastion host	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.

Console Function	Dependency	Role/Policy Required
Creating a cloud asset agency	Data Encryption Workshop (DEW) Elastic Cloud Server (ECS) Relational Database Service (RDS) Identity and Access Management (IAM)	After the CBH FullAccess permission is configured for an IAM user, you need to add related permissions for the user based on **Manually Adding Permissions for CBH FullAccess**.

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"
         ]
      }
   ]
}
```


Manually Adding Permissions for CBH FullAccess

When using a bastion host, you need to manually add permissions to create cloud asset agencies and bind or unbind EIPs.

Table 7-4 Permissions that need to be manually added for CBH FullAccess Permissions

Permission	Description
csms:secretVersion:get	Grants the permissions to obtain secrets from CSMS.
csms:secret:list	Grants the permission to obtain the CSMS secret list.
kms:dek:create	Grants the permission to create keys in KMS.
kms:cmk:list	Grants the permission to obtain the KMS key list.
ecs:cloudServers:list	Grants the permission to obtain the ECS list.
rds:instance:list	Grants the permission to obtain the RDS instance list.
vpc:vpcs:get	Grants the permission to query VPC details.
vpc:publicIps:get	Grants the permission to query the EIP of a VPC.
vpc:ports:update	Grants the permission to bind or unbind an EIP.
iam:agencies:listAgencies	Grants the permission to obtain the IAM agency list.
iam:permissions:listRolesForAgencyOnProject	Grants the permission to obtain the IAM agency role list.
iam:agencies:createAgency	Grants the permission to create an IAM agency.
iam:permissions:revokeRoleFromAgencyOnProject	Grants the permission to associate the IAM agency with a role.
iam:roles:createRole	Grants the permission to create an IAM agency role.
iam:agencies:deleteAgency	Grants the permission to delete an IAM agency.

Manually Adding Permissions for CBH ReadOnlyAccess

When using a bastion host instance, you need to manually add the permission to view the instance details.

Table 7-5 Permissions that need to be manually added for CBH ReadOnlyAccess

Permission	Description
vpc:vpcs:get	Grants permission to query VPC details.

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**

8 Limitations and Constraints

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 connect VPCs in different regions, using CBH to manage resources across regions is still not recommended because cross-region networks are 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.

  Default ports for a security group: 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.

- A CBH system can be logged in only through IP address and port number.

Table 8-1 Inbound and outbound rule configuration reference

Scenario Description	Direction	Protocol/ Application	Port
Accessing a bastion host through a web browser (HTTP and HTTPS) **NOTE** • If HTTPS is used, configure port 443 only. • HTTP automatically redirects requests to HTTPS. If HTTP is used, configure both ports 80 and 443. Otherwise, the automatic redirection will not take effect.	Inbound	TCP	Ports 80 and 443
Accessing a bastion host through Microsoft Terminal Services Client (MSTSC)	Inbound	TCP	53389
Accessing a bastion host through an SSH client	Inbound	TCP	2222
Accessing a bastion host through an FTP client	Inbound	TCP	2121 and 20000 to 21000
Accessing a bastion host through an SFTP client	Inbound	TCP	2222
Remotely accessing Linux cloud servers managed by a bastion host over SSH clients	Outbound	TCP	22
Remotely accessing Windows cloud servers managed by a bastion host over the RDP protocol	Outbound	TCP	3389
Accessing Oracle databases through a bastion host	Inbound	TCP	1521
	Outbound	TCP	1521
Accessing MySQL databases through a bastion host	Inbound	TCP	33306
	Outbound	TCP	3306
Accessing SQL Server databases through a bastion host	Inbound	TCP	1433
	Outbound	TCP	1433
Accessing DB databases through a bastion host	Inbound	TCP	50000

Scenario Description	Direction	Protocol/ Application	Port
	Outbound	TCP	50000
Accessing GaussDB databases through a bastion host	Inbound	TCP	18000
	Outbound	TCP	8000 and 18000
License servers	Outbound	TCP	9443
Huawei Cloud services	Outbound	TCP	443
Accessing a bastion host system through an SSH client in the same security group	Outbound	TCP	2222
SMS service	Outbound	TCP	10743 and 443
Domain name resolution service	Outbound	UDP	53
Accessing PGSQL databases through a bastion host	Inbound	TCP	15432
	Outbound	TCP	5432
Accessing DM databases through a bastion host	Inbound	TCP	15236
	Outbound	TCP	5236
Accessing Redis databases through a bastion host	Inbound	TCP	16379
	Outbound	TCP	6379
Accessing databases through an SSH tunnel	Inbound	TCP	62222

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 8-2 Supported database versions

Database Engine	Engine Version
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 8-3** lists the supported operating system versions.

  Table 8-3 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 supported only by x86 CBH instances. Arm CBH instances do not support application O&M.

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 8-4 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 **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 8-5 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
	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

Operation Method	Resource Protocol Type/Application Type	Supported Client
	dbisql	dbisql
	Google Chrome	Google Chrome
	Edge	Edge
	Mozilla Firefox	Mozilla Firefox
	VNC Client	VNC Viewer
	SecBrowser	SecBrowser
	vSphere Client	vSphere Client
	Radmin	Radmin

Bastion Host Versions and OSs

The OS version varies depending on the bastion host image. The details are as follows:

Table 8-6 Mapping between bastion hosts and OS versions

Bastion Host Version	System Architecture	OS Version
3.3.37.X or earlier	x86	EulerOS 2.2
	Arm	EulerOS 2.8
3.3.38.0 or later to 3.3.50.X or earlier	x86	EulerOS 2.10
	Arm	
3.3.52.0 or later	x86	HCE 2.0
	Arm	

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.

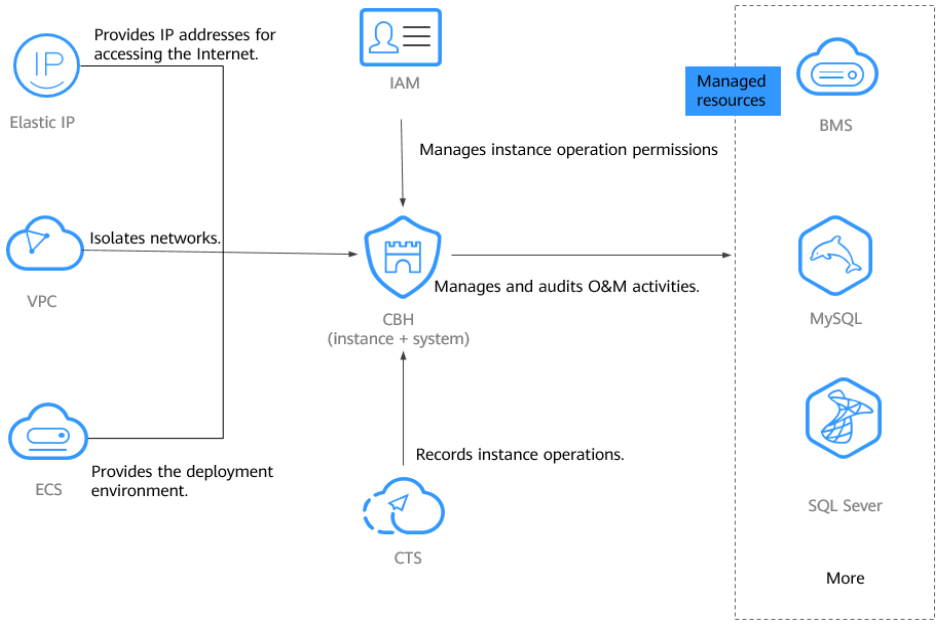
NOTE

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 managed resources and the CBH system over all protocols at the same time. For more details, see **Basic Concepts**.

9 CBH and Other Services

CBH needs to work with other cloud services. **Figure 9-1** shows the dependencies between CBH and other cloud services.

Figure 9-1 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**.

10 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.

For details about how to create a CBH instance, see **Buying 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.

For details about how to log in to resources using SSO, see **Using an SSO Client to Log In to Database Resources for O&M**.

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.

OTP

One-Time Password (OTP) is a unique password that is valid only for a single login session or transaction.

OTPs are required for logging in to a bastion host using SMS messages, mobile phone tokens, or dynamic tokens.

For details about the configuration methods, see **Configuring Multifactor Verification**.

11 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 11-1 lists the personal data generated or collected by CBH.

Table 11-1 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	• 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	• 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	• 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 • 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.

12 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 products, services and features you buy are provided in accordance with 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:

- Third-party browsers

  For browsers and versions supported for logging in to a CBH system, see **Table 12-1**.

  Table 12-1 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

- Nmap

  Reason: Nmap is an industry-leading asset scanning tool. CBH uses this tool to discover hosts in batches, so that you can batch manage hosts.

  Application scenario: CBH uses the Nmap tool to scan and discover assets in a specified network segment, and add the assets to CBH for O&M.

  Risks: Users can discover assets and scan vulnerabilities in a specified network segment through this tool. Only the administrator can use the related functions. The Principle of least privilege is followed during installation and use. The overall risk is low.

Recommended methods for downloading third-party software:

Download the required third-party software in 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.

