Cloud Bastion Host

Best Practices

 Issue
 01

 Date
 2020-12-01





Copyright © Huawei Technologies Co., Ltd. 2022. 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

NUAWEI 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.

Contents

1 Change CBH Instance Specifications	1
1.1 Before You Start	1
1.2 Preparations	4
1.2.1 Checking the System Environment	4
1.2.2 Backing Up the CBH System Data	6
1.3 Changing Specifications of a CBH Instance	11
1.4 Verification After the Change	12
1.4.1 Checking the System Environment	12
1.4.2 (Optional) Restoring CBH System Configurations	14
1.4.3 (Optional) Resetting the Passwords of System Users	16
1.4.4 Verifying the CBH System configurations	19
2 Secondary Authorization for High-Risk Database Operations	22
A Change History	29

Change CBH Instance Specifications

1.1 Before You Start

Application Scenarios

You can change specifications of a CBH instance to meet your business needs.

This document applies to specification changes of a single-node CBH instance on Huawei Cloud.

NOTE

To change specifications of a CBH instance in two-node cluster mode, click **Service Tickets** in the Huawei Cloud management console and submit a service ticket for technical support.

Change Process

This document provides guidance for the system administrator **admin** to change specifications of a CBH instance. The general steps are as follows: Back up the CBH system data before the change; change the instance specifications; restore the CBH system configurations; and verify that the configurations for the original and new CBH systems are consistent.



Figure 1-1 Specification change process

Restrictions on Changing Specifications

Changing specification includes changing the edition and asset specifications of a CBH instance.

- Edition: The edition of a CBH instance can only be changed from the standard to the professional, but cannot be changed from the professional to the standard.
- Asset specifications: include assets, concurrent requests, CPU, memory, and data disks. Asset specifications can only be scaled up.

NOTE

- Changing specifications has no impact on the bandwidth and traffic of the EIP bound to the instance.
- The default capacity of the system disk is 100 GB. Changing specifications does not affect the system disk but expands data disk capacity.
- CBH historical edition provides only functions of the standard edition. To change its specifications, click **Service Tickets** in the upper right corner of the Huawei Cloud management console and submit a service ticket for technical support.

Table 1-1	Edition	change
-----------	---------	--------

Before the Change	After the Change
100 Assets Standard	100 Assets Professional 200 Assets Standard or Professional 500 Assets Standard or Professional 1000 Assets Standard or Professional 5000 Assets Standard or Professional
100 Assets Professional	200 Assets Professional 500 Assets Professional 100 Assets Professional 5000 Assets Professional
200 Assets Standard	200 Assets Professional 500 Assets Standard or Professional 1000 Assets Standard or Professional 5000 Assets Standard or Professional
200 Assets Professional	500 Assets Professional 1000 Assets Professional 5000 Assets Professional
500 Assets Standard	500 Assets Professional 1000 Assets Standard or Professional 5000 Assets Standard or Professional
500 Assets Professional	1000 Assets Professional 5000 Assets Professional
1000 Assets Standard	1000 Assets Professional 5000 Assets Standard or Professional
1000 Assets Professional	5000 Assets Professional
5000 Assets Standard	5000 Assets Professional

Precautions for Changing Specifications

• Software version

To make the functions of the profession edition take effect, the CBH system software version must be V3.2.16.0 or later, or the CBH system cannot be upgraded even the specifications are changed.

If the software version is earlier than V3.2.16.0, **upgrade the system version** first.

• System data backup and restoration

Before you change specifications, back up important system data to prevent system data loss caused by change failures.

After the specifications are changed, reload the backup data to the system to quickly restore the system configurations.

• Specification change time

The entire specification change process includes preparation, background upgrade, and verification after the change. The process takes about 60 minutes. It takes about 30 minutes to change the backend specifications. During this period, close the CBH system, which will interrupt the CBH system service.

To reduce the impact on the system running, change specifications during offpeak hours.

1.2 Preparations

1.2.1 Checking the System Environment

Before the change, query and record the system version information and specifications, including Version, Device System, Max Resources, and Max Concurrent Conns.

- **Step 1** Log in to the CBH system.
- **Step 2** Confirm and record the version number of the CBH system.
 - 1. In the navigation pane on the left, choose **System** > **About** to view the system version information.

Dashboard / S	System / About	
About		
l i	Product Name :	HUAWEI Operation & Maintenance Audit
	Product ID :	15(
	Service Code :	View
AI	PI Access Key :	To be updated Update View Clear
	HA Key :	Updated at 2019-12-27 14:58:01 Update View
	Version :	V1.0
C	evice System :	V3.3.2.0
	Issue Time :	2019-12-27
		Copyright©2019 Huawei Technologies Co., Ltd. All Rights Reserved.

Figure 1-2 Viewing CBH system version number

2. Record information about Version and Device System.

NOTE

The device system version must be V3.2.16.0 or later, or the change does not take effect. **Upgrade the system software** first if needed.

- **Step 3** Confirm and record the authorization configuration.
 - 1. Choose **System > System Maintain > License** to view the authorization information.

Dashboard / System / S	ystem Maintain
System Maintenanc	e
System Status Sy	stem Mgmt Backup&Restore License Network Diagnosis System Diagnosis
Customer Inf	io :
Authorization Typ	e : Official Version
Statu	s: Activated Update License Backup License
Producti	D: 150
Authorized Module	s: BASE,MODULE_AUTOOPS,MODULE_DB_AUDIT,MODULE_OCR
Max Resource	is : 50
Max Concurrent Conn	is : 50
Expired Tim	e: 2020-08-13 12:47:35

Figure 1-3 Viewing license

2. Record the number of authorized resources in **Max Resources** and the number of concurrent connections of authorized resources in **Max Concurrent Conns**.

----End

1.2.2 Backing Up the CBH System Data

To prevent system data loss caused by possible change failures, back up important system data, including system configurations, resource accounts, and audit logs, before the change.

Backing Up System Configuration Data

You can back up CBH system configuration data and load it to the new CBH system, eliminating the need to repeat manual configurations.

The system configuration data contains all configuration data of the department, user, resource, policy, ticket, operation, audit, and system modules.

Step 1 Log in to the CBH system.

Step 2 Choose **System > System Maintain > Backup&Restore**.

Step 3 Click **New** to back up the system configuration data.

Figure 1-4 Creating a configuration backup

system Mainter	nance					
system Status	System Mgmt	Backup&Restore	License	Network Diagnosis	System Diagnosis	
Config Backup						Auto + New
Time		Version		Size	Remarks	Operation
				No Data		
Config Restore						
l	Jpload : Uploa	d				
	Please config fi	backup the current config I le is complete	before restoring	the system, make sure that	the uploaded	

Step 4 Click **Download** to export the system configuration file to a local computer.

System Maintenance				
System Status System Mgmt	Backup&Restore	License Network Diagnosis	System Diagnosis	
Config Backup				Auto + New
Time	Version	Size	Remarks	Operation
2020-04-15 09:59:26	∨3.3.2.0	45.5KB	move	Restore Download Delete
				20 /page 🔷 🤇 1 📏 Go to 1
Config Restore				
Upload : Upload	d			
Please I	backup the current config b	efore restoring the system, make sure th	at the uploaded	

Figure 1-5 Downloading a backup file

----End

Backing Up Managed Accounts

The authentication keys of different CBH systems are different. After the specification change, the managed accounts imported using the configuration file may fail to be used for system login. You are advised to back up managed accounts to prevent account information loss in case of specification change failure.

A managed account file contains all data of each account, including the username, password, login methods, sudo account, and names and addresses of associated resources.

Step 1 Log in to the CBH system.

Step 2 Choose **Resource** > **Account** and click **Export**.

Figure 1-6 Exporting the account file

Das	hboard	/ Resource / Accour	nt								
A	ccoun	t								C Import	New
	Account	 keyword 		Advanced							Export
		Account ≑	Status 💌	Resource ≑	Host/APP Addr	Port	Protocol 💌	Login Type 🔍	Department 🔻	Operation	
		[Empty]	N/A	RDS_A	192.	3306	MySQL	Manual Login	Test	Manage Join	Delete
		root	N/A	RDS_A	192.	3306	MySQL	Auto Login	Test	Manage Join	Delete
	_										
		Delete Test a	ind verify						20 /page 🤍 🤝	< <mark>1</mark> > G	o to 1

Step 3 Set the encryption password to encrypt the exported managed account file.

Figure 1-7 Setting encryption password

ок			×
Set encryption password :	Max 64 chars allowed. If it is empty, there is not password for the file		
User Password :			
		Cancel	ОК

Step 4 Click OK and save the file locally.

----End

Backing Up Audit Logs

CBH does not support migration of history audit logs. You need to back up system audit logs before the change.

Audit logs include history session records, session videos, system login logs, system operation logs, password change logs, and account synchronization logs.

- **Step 1** Log in to the CBH system.
- Step 2 Export history session records.
 - 1. Choose Audit > History Session.
 - 2. Select all history sessions, click **Export**, and save exported text records locally.

Figure 1-8 Exporting history session records

Dashboard / Audit / History Session														
History Session														
Resour	ce 🔻 keyword	(Q Advanced								Export			
	Resource	Protocol 💌	Account	User	Src IP	Start/End Time 🌲	Duration ≑	End State 🔻	Operation					
	127	SSH	sysuser	admin	10.108.17	2019-12-17 11:47:20	00:03:00	Normal	Detail Pla	Download	More			
	127	SSH	sysuser	admin	10.108.17	2019-12-17 11:37:17	00:03:00	Normal	Detail Pla	Download	More			
	Windows	RDP	Administrator	admin	10.108.17	2019-12-17 11:32:25	04:55:42	Interrupted	Detail Pla	Download	More			
	Windows	RDP	Administrator	admin	10.108.17	2019-12-17 10:49:30	00:00:05	Normal	Detail Pla	Download	More			
	Windows	RDP	Administrator	admin	10.108.17	2019-12-17 10:49:20	00:00:03	Normal	Detail Pla	Download	More			
	Delete Video						20 /page	× 1 ··· 1	7 18 19 2	0 21 22)	Go to 21			

Step 3 Download a session video.

NOTE

Session videos cannot be generated or downloaded in batches. Only one video can be generated or downloaded at a time.

- 1. Choose Audit > History Session.
- 2. Choose **More** > **Generate Video** in the **Operation** column of the target session row.

Figure 1-9 Generating a video

Dashboard / Audit / History	Session								
History Session									0
Resource Veryword		Q Advanced							Export
Resource	Protocol 🔻	Account	User	Src IP	Start/End Time 🜲	Duration ≑	End State 🔻	Operation	
127	SSH	sysuser	admin	10.108.17	2019-12-17 11:47:20	00:03:00	Normal	Detail Play Do	ownload More
127	SSH	sysuser	admin	10.108.17	2019-12-17 11:37:17	00:03:00	Normal	Detail Play Do	ownload Generate Vid
Windows	RDP	Administrator	admin	10.108.17	2019-12-17 11:32:25	04:55:42	Interrupted	Detail Play Do	Delete Video
U Windows	RDP	Administrator	admin	10.108.17	2019-12-17 10:49:30	00:00:05	Normal	Detail Play Do	ownload More
Windows	RDP	Administrator	admin	10.108.17	2019-12-17 10:49:20	00:00:03	Normal	Detail Play Do	ownload More 🗸
Delete Video						20 /page	v (1 1	17 18 19 20 <mark>21</mark>	22 > Go to 21

3. After the video is generated, click **Download** and save the video locally.

Figure 1-10 Downloading a video

Dashboard / Audit / History Session													
History Session													
Resour	ce 🔻 keyword		Advanced								Export		
	Resource	Protocol 💌	Account	User	Src IP	Start/End Time 🜲	Duration ≑	End State 💌	Operation				
	127	SSH	sysuser	admin	10.108.17	2019-12-17 11:47:20	00:03:00	Normal	Detail Play	Download	More		
	127	SSH	sysuser	admin	10.108.17	2019-12-17 11:37:17	00:03:00	Normal	Detail Play		More		
	Windows	RDP	Administrator	admin	10.108.17	2019-12-17 11:32:25	04:55:42	Interrupted	Detail Play		More		
	Windows	RDP	Administrator	admin	10.108.17	2019-12-17 10:49:30	00:00:05	Normal	Detail Play		More		
	Windows	RDP	Administrator	admin	10.108.17	2019-12-17 10:49:20	00:00:03	Normal	Detail Play		More 🗸		
	Delete Video						20 /page 🖷	· < 1 ··· 1	7 18 19 20	21 22 >	Go to 21		

Step 4 Export system login logs.

- Choose Audit > System Log > System Logon to switch to the system log page.
- 2. Select all login logs, click **Export**, and save the exported text records locally.

Figure 1-11	Exporting	system	login logs	,
-------------	-----------	--------	------------	---

Dashboard	/ Audit / System Log							
System	Log							0
System L	.ogon System Operat	ion						
User	keyword	Q Advanced						Export
	Time 🌲	User	Source IP	Content	Logon Type 🔍	Result 💌	Remarks	
	2020-04-15 09:26:45	admin_A		Logged in	Web	Success	-	
	2020-04-15 09:26:35	admin_A		Logged in	Web	Failed	Logon failure, password error	
	2020-04-02 10:19:56	admin_A		Logged out	Web	Success	-	
	2020-04-02 10:19:23	admin_A		Logged in	Web	Success		
	2020-04-02 10:19:13	admin_A		Logged in	Web	Failed	Logon failure, password error	
	2020-03-23 14:57:50	admin_A		Logged out	Web	Success		
	2020-03-23 10:00:58	admin_A		Logged in	Web	Success		
	2020-03-20 15:55:17	admin_A		Logged out	Web	Success		
							20 /page 📼 < 1 >	Go to 1

Step 5 Export system operation logs.

- Choose Audit > System Log > System Operation to switch to the system log page.
- 2. Select all operation logs, click **Export**, and save the exported text records locally.

stem	Log							
stem I	_ogon System Opera	tion						
lser	keyword		Advanced					
	Time 💠	User	Source IP	Module 💌	Content	Result 💌	Remarks	
	2020-04-15 09:59:26	admin_A		System	New backup [2020-04-15 09:59:25]	Success	-	
	2020-03-19 15:03:27	admin_A		Policy	DB access [DB-ACL] created	Success	-	
	2020-03-19 14:55:00	admin_A		Policy	ACL rule [test-susan] created	Success		
	2020-03-19 14:53:32	admin_A		Resource	Host [RDS_A] created	Success		
	2020-03-19 14:53:32	admin_A		Resource	The account [root] of the host [RDS_A] created	Success	-	
	2020-03-19 14:50:06	admin_A		Policy	DB access rule [DB-test] created	Success	-	
	2020-03-19 14:40:59	admin_A		User	The password of User [admin_A] modified	Success	-	

Figure 1-12 Exporting system operation logs

----End

1.3 Changing Specifications of a CBH Instance

Prerequisites

- You have obtained credentials for logging in to the management console.
- An EIP has been bound to the CBH instance.
- You have backed up system data by referring to Backing Up the CBH System Data.
- You have disabled the CBH system and terminated all other operations in the CBH system.

Procedure

- **Step 1** Log in to the management console.
- **Step 2** In the **Operation** column of the target instance, choose **More** > **Change Edition**.

Figure 1-13 Instances

					Instance name 🔹 🔻	Enter a keyword. Q C
Instance Name	AZ	Status	Private IP Address	EIP	Billing Mode	Operation
∨ CBH-4a67	cn-east-3b	C Running	172.16.0.57	-	Yearly/Monthly 30 days until expiration	Login Start More 🕶

Step 3 Select an edition you want.

Select an Edition and click Next to go to the Details page.

Step 4 Confirm and pay the order.

After confirming the order details, click **Submit**. On the payment page, finish the payment.

Step 5 The specifications are automatically changed in the background.

It takes about 30 minutes for the change to take effect.

During the change, the instance status changes from **Upgrading** to **Restarting**. After the CBH system is restarted, the instance status changes to **Running**.

Step 6 The specifications are changed in the background.

If the instance status changes to **Running** and the instance details are updated, the backend change is completed.

You can then log in to the CBH system and start to verify the change.

----End

1.4 Verification After the Change

1.4.1 Checking the System Environment

After the change, verify that the settings of **Version**, **Device System**, **Max Resources**, and **Max Concurrent Conns** are the same as that of the new CBH edition.

- **Step 1** Log in to the CBH system.
- **Step 2** Verify the system version.
 - 1. In the navigation pane on the left, choose **System** > **About** to view the system version information.
 - 2. Check the information of Version and Device System.

HUAWEI Operation & Maintenance Audit
15(
View
To be updated Update View Clear
Updated at 2019-12-27 14:58:01 Update View
V1.0
V3.3.2.0
2019-12-27
Copyright©2019 Huawei Technologies Co., Ltd. All Rights Reserved.

Figure 1-14 Viewing CBH system version number

- **Step 3** Check whether the original and new CBH systems have the consistent authorization information.
 - 1. Choose **System > System Maintain > License** to view the authorization information.

Figure	1-15	Viewing	license
--------	------	---------	---------

Dashboard / System / System	faintain	
System Maintenance		
System Status System	Igmt Backup&Restore License Network Diagnosis System Diagnosis	
Customer Info :		
Authorization Type :	Official Version	
Status :	Activated Update License Backup License	
ProductID :	150	
Authorized Modules :	BASE,MODULE_AUTOOPS,MODULE_DB_AUDIT,MODULE_OCR	
Max Resources :	50	
Max Concurrent Conns :	50	
Expired Time :	2020-08-13 12:47:35	

- 2. Check whether the authorization information is consistent with that of the new CBH edition.
 - If they are consistent, the specification change is successful.
 - If no, contact technical support.

----End

1.4.2 (Optional) Restoring CBH System Configurations

After the change is completed, the number of system assets, number of concurrent requests, CPU, and data disks are upgraded accordingly, which does not affect system data.

If system data is lost due to a change failure, you can import the backup files, such as system configuration files and resource account files, and restore the system configurations.

Importing the Backup File of the CBH System Configurations

You can reuse the system configuration data of the original CBH system in the new CBH system by uploading the system configuration back file to the new system.

The system configuration data contains all configuration data of the department, user, resource, policy, ticket, operation, audit, and system modules.

Step 1 Log in to the CBH system.

Step 2 Choose **System > System Maintain > Backup&Restore**.

Step 3 In the **Config Restore** area, click **Upload**, select the configuration file exported from the original CBH system, and upload it.

Figure 1-16 Uploading the backup configuration file

Dashboard / System / System Maintain	
System Maintenance	
System Status System Mgmt Backup&Restore License Network Diagnosis System Diagnosis	
Config Backup	Auto + New ×
Config Restore	*
Upload: Upload	
Please backup the current config before restoring the system, make sure that the uploaded config file is complete	

Step 4 Click OK.

It takes about 5 minutes for the imported configuration data to take effect. It may take a longer time if there is a large amount of system configuration data.

----End

Importing the Backup File of Managed Accounts

The authentication keys of different CBH systems are different. After the change, the managed accounts imported using the configuration file may fail to be used for system login. To ensure the availability of the managed accounts, you are advised to import the backup file of the managed accounts.

A managed account backup file contains all data of each account, including the username, password, login methods, sudo account, and names and addresses of associated resources.

- **Step 1** Log in to the CBH system.
- **Step 2** Choose **Resource** > **Account** in the navigation pane.
- **Step 3** Click **Import** to go to the **Import Account** page.

Figure 1-17 Account

Dashboa	rd /	Resource / Acco	ount								
Acco	unt									C Import	New
Acco	ount	keyword	(Advanced							Export
		Account ≑	Status 💌	Resource ≑	Host/APP Addr	Port	Protocol 💌	Login Type 🔻	Department 💌	Operation	
						No Data					

Step 4 On the **Import Account** page, click **Upload**, select the account file exported from the original CBH system, and upload it.

Figure 1-18 Import Account

Import Account	×
Download template :	Download
Upload :	Upload Only extension xls/xlsx/csv supported
Options :	✓ Override existing accounts ✓ Verify Account
	Cancel

- Step 5 After the upload is complete, choose More > Override existing accounts or Verify Account.
- Step 6 Click OK.

----End

1.4.3 (Optional) Resetting the Passwords of System Users

After the specifications of a CBH instance are changed, you are advised to reset the system user passwords to enhance the password security and availability.

You can let the system generate a new password for users in batches or manually reset different passwords for system users.

- **Step 1** Log in to the CBH system.
- **Step 2** Choose **User** > **User** in the navigation pane.
 - To reset passwords in batches, go to Step 3.
 - To manually reset a password, go to **Step 4**.
- **Step 3** Reset the same login password of multiple system users.
 - 1. Select the users whose password needs to be reset.

Figure 1-19 Resetting a user's password

shboard	/ User / User											
User										O Im	iport	New
Auto Re	ecognition 🔻	keyword			Advanced							Export
	LoginName	÷		UserName 4	÷	Status 💌	Role 💌	Departmen	t 💌	Operation		
	z123			ZZ		Enabled	admin-A	Test		Manage	Join	Delete
	User_A			san		Enabled	User	Test		Manage	Join	Delete
	admin_A			Sam		 Enabled 	admin-A	Test		Manage	Join	
			Edit D Edit R Edit m Edit vi Edit ti Edit IF	ept ole ultifactor alidity period me limit								
			Edit M	IAC limit								
~	Delete	Enable	Disable	More 🔺					20 /page	The second secon	> G	o to 1

2. Choose **More** > **Reset Password** to go to the password resetting dialog box.

Figure 1-20 Batch resetting passwords

Reset Password			×
* Password :]	
* Confirm Password :	Random Passwd - Conv Passwd		
	8-32 length of chars, including letters, digit and special chars , space not allowed		
		Cancel	ок

3. Reset the password and click **OK**.

NOTE

After you batch reset the passwords for multiple system users, these users need to use the reset password to log in to the CBH system. For security purposes, CBH asks each system user to change the password upon the first login.

Step 4 Manually reset different passwords for system users.

1. Export the user list template.

Select the users you want to export and click **Export** in the upper right corner. If no users are selected, information about all users is exported by default.

Figure 1-21 Exporting information about all users

D	bhoard	Ulter / Heer										
	User									O Im	port	New
	Auto Rec	cognition 👻 keyword			Advanced							Export
		LoginName 🗇		UserName	¢	Status 🤝	Role 👻	Department 📼		Operation		
	~	z123		zz		 Enabled 	admin-A	Test		Manage	Join	Delete
	2	User_A		san		 Enabled 	User	Test		Manage	Join	Delete
		admin_A		Sam		 Enabled 	admin-A	Test		Manage	Join	
		Delete Enable	Disable	More 💌					20 /page	- 1	G	o to 1

2. Configure user passwords.

Save the exported user information file locally, change the plaintext password in the **Cleartext Password** row corresponding to the user **Login Name** as needed, and save the file.

Figure 1-22 Changing a password

Login name	e AuthType	Cleartext Password	AD domain	Username	Mobile	Email	Role	Dept	Remarks	User Group	Ç
User_A	Local	29fHLTx!3c\$<		san	134****922	te****@hi	User	Test		G2	
z123	Local	/^c~8Mn6N01p		ZZ	124****9224	te***@hi	admin-A	Test			

- 3. Import the user list.
 - a. On the **User** page, click **Import**.

Figure 1-23 Importing the user information file

shboard	/ User / User						
Jser						O Import	Ne
Auto Re	cognition 👻 keyword	Q Advanced					Exp
	LoginName 💠	UserName 💠	Status 🤝	Role 💌	Department 🔝	Operation	
	z123	22	 Enabled 	admin-A	Test	Manage Join I	Delet
	User_A	san	 Enabled 	User	Test	Manage Join I	Delete
	admin_A	Sam	 Enabled 	admin-A	Test	Manage Join	
	Delete Enable Disable	More 🔝			20 /page	 ✓ 1 > Go 	to 🔄

b. Click **Upload** and select the modified user information file.

Figure 1-24 Import User

Import User			×
Download template :	Download		
Upload :	Upload Only extension of xls/xlsx/csv supported		
Options :	✓ Override existing user		
		Cancel	ОК

- c. Select **Override existing user** for **Options**.
- d. Click **OK**.

----End

1.4.4 Verifying the CBH System configurations

After the instance specifications are changed, log in the CBH system as system administrator **admin** to verify system configuration consistence for each module in the navigation pane of the CBH system.

You need to verify system configurations in the department, user, resource, policy, ticket, audit, operation, and system modules. For more details, see **Table 1-2**

Level 1 Module	Level 2/3 Module	Verification Item
Departme nt	None	Department level, department name, number of users, and number of hosts.
User	User	Number of users and basic information about each user, such as the login name, user name, status, role, and department.
	User Group	Number of user groups, user group names, and group members.
	Role	Role configuration.
Resource	Host	Number of managed hosts and basic information about each managed host, including the host name, host address, port number, protocol type, OS type, and number of accounts.

Table 1-2 System configuration verification

Level 1 Module	Level 2/3 Module	Verification Item
	Applicati on Publish	 Number of applications, names, addresses, associated hosts, and department of each application. Number of application servers, names, addresses, types, and department of each application server.
	Account	 Number of accounts and basic information about each account, including the account name, related resources, host or application address, port number, and department. Whether accounts can be used. You can select accounts in batches and click Verify to check whether the selected accounts can be used to log in to the system.
	Account Group	Number of account groups, account group names, members in an account group, and number of members in an account group.
Operation	Host label	Number of labels of managed hosts, such as the number of labels, names, and labeled hosts.
	Applicati on Label	Verify the configuration information about the number of tags, names, and tagged application resources released by the application.
Policy	ACL Rules	Number of ACL rules and basic information about each ACL rule, such as rule name, status, associated users, and associated accounts.
	Cmd Rules	 Number of policies, policy names, actions, and associated command sets. Number of command sets, names, commands, and parameters.
	Chpwd Rules	Number of policies and basic information about each policy, such as policy names, status, execution modes, and password change mode.
Audit	System Report	Auto Send configuration
	Ops Report	Auto Send configuration
Ticket	ACL Ticket	Basic information about the authorization ticket, including ticket number, status, and application time
System	Security	System login security configuration, including user locking, policy password, web login, and SSH client login.

Level 1 Module	Level 2/3 Module	Verification Item
	Outgoing	Email and SMS gateway configuration.
	Authentic ate	AD domain, RADIUS, and LDAP authentication configurations.
	Ticket	Basic settings and approval process of tickets.
	Alarm	Alarm channel and alarm level (severity)
	Storage Mgmt	Auto deletion.
	Log Backup	Remote backup to the Syslog server and remote backup to the FTP/SFTP server.
	Backup& Restore	Automatic configuration backups.

2 Secondary Authorization for High-Risk Database Operations

With CBH editions, you can delete, modify, and view your database instances by running commands. To secure sensitive database information and prevent key information from being lost or disclosed, CBH gives you the ability to configure an approval process for high-risk database operations and monitor key information.

Use administrator *admin_A* as an example to describe how to authorize O&M user *User_A* to perform secondary authorization for high-risk operations on MySQL database instance *RDS_A*.

Application Scenarios

With Cloud Bastion Host (CBH), you can dynamically identify and intercept highrisk commands (including deleting databases, modifying key information, and viewing sensitive information) to interrupt database O&M sessions by setting database control policies and preset command execution policies. In addition, the system automatically generates a database authorization ticket and sends it to the administrator for secondary authorization. O&M users can resume interrupted O&M sessions only after the administrator approves the ticket and authorizes the high-risk operations.

Constraints

Currently, secondary authorization of high-risk operations only applies to the commands executed on the MySQL or Oracle database instances.

Prerequisites

- The security group to which the CBH instance belongs has enabled the database access port, and the network connection between the database and the CBH system is normal.
- Database *RDS_A* has been managed as a host resource.
- O&M user *User_A* has obtained the access control permission for *RDS_A*.

Configuring the Secondary Authorization Policy

To approve high-risk operations on database instances, you need to preset command rules on the **DB Rules** page in the **Policy** module and enable **Dynamic approval** in the **Action** field.

- Step 1 Log in to the CBH system as *admin_A*.
- Step 2 Choose Policy > DB Rules to go to the DB Rules page.
- **Step 3** Configure the database rule set and select the preset high-risk operation commands.
 - 1. Click the **RegSet** tab.

Figure 2-1 RegSet

shboard / Policy / DB Rules					
DB Rules				C	Nev
DB Rules RegSet					
RegSet name v keyword Q					
RegSet name	Protocol	•	Operation		
DB-test	MySQL		Manag e	Add regulatio n	Delet e
Delete	20	/page	• <	1) Go	to 1

2. Click **New** to create a rule set for MySQL databases. Use the *DB-test* rule set as an example.

Figure 2-2 New RegSet

New RegSet			×
* RegSet name :	DB-test		
	1-64 length of chars, including letters, digit or"-"		
Protocol :	MySQL		
		Cancel	ОК

3. Click Add Regulation in the Operation column of the *DB-test* row to add a library, table, or command rule. The following describes how to add the **DELETE** command for deleting table content.

NOTE

- The **Cmd** field is mandatory. You must select at least one command. You can select multiple commands at a time.
- Set the **Lib** or **Table** field to restrict operation commands on the database library or tables.
- If the **Lib** or **Table** field is left blank, all operation commands in the database are restricted.

Figure 2-3 Add regulation

Add regulation		>	
Lib :			
	Support wildcards, * represents any char, ? an arbitrary char, [] represents matching char in brackets, scope or reverse (using ! or ^), enter a lib name per line		
Table :			
	Support wildcards, * represents any char, ? an arbitrary char, [] represents matching char in brackets, scope or reverse (using ! or ^), enter a table name per line		
* Cmd :	DELETE X		
	ALTER		
	TRUNCATE		
	EXECUTE	Cancel OK	
	INSERT		
	UPDATE		
	SELECT		
	GRANT		



1. Click the **DB Rules** tab.

Figure 2-4 DB Rules

Dashboard	/ Policy / DB Rules							
DB Ru	les							0 New
DB Rul	es RegSet							
Rule N	lame 🔻 keyword	Q	Advanced					
	Rule Name	Status 🔻	Action 🔻	RegSet	User	Account	Operation	
	DB-ACL	Enabled	req-approval	1 DB-test	≛ User_A ∴ -	L root@RDS_A ∴ -	Manage insert	Relate Delete
List in de	escending order by priority	, drag to change the	priority					

2. Click **New** to create a **Dynamic approval** rule for the database. Use database rule *DB-ACL* as an example.



Figure 2-5 Configuring dynamic approval

3. Relate the rule to rule set *DB-test*.



Figure 2-6 Relating a new database rule to a rule set (RegSet)

4. Relate user *User_A* to resource *RDS_A*.

Figure 2-7 Relating users to resources

Relate User Groups		Relate Accounts Relate Account Groups	
Selectable users	Selected users	Selectable accounts	Selected accounts
Keyword Q	Keyword Q	Keyword Q	Keyword Q
□ ^{Z123} ZZ	S User_A san	[Empty] RDS A/1 0.117	7 root RDS A/ .0.117
□ admin_A Sam			
	<		
	>		
Total 2 items	Selected 1/1 items	Total 1 items	Selected 1/1 items

----End

Verifying the Secondary Authorization Policy

An O&M user performs a high-risk operation and applies for operation permissions after the operation is intercepted. The administrator authorizes the

high-risk operation after review to strengthen the management and control of core database assets.

- Step 1 Log in to *RDS_A* as O&M user *User_A*.
 - 1. Log in to the CBH system.
 - 2. Choose **Operation** > **Host Ops**.
 - 3. Click **Log In** to log in to database resource *RDS_A* using an SSO tool.

Figure 2-8 Database login

Dashboard / Operation / Host Ops					
Host Operation				C Web OPS S	Settings Export
Auto Recognition 🔻 keyword	Q				
Host Name 🌲	Host Addr 🗢	Protocol 🔻 Label 🔻		Account 💌	Operation
RDS_A	.0.117:3306	MySQL	2	root 💌	Login
Batch Login Add	Label Delete Label			20 /page 🔍 🤇	1 👌 Go to 1

- **Step 2** Use the Navicat client as an example. O&M user *User_A* deletes table content from *RDS_A*. The **DELETE** command is automatically intercepted, and a message is displayed indicating that *User_A* does not have the permission to delete the table content.
- **Step 3** O&M user *User_A* submits a database authorization ticket to administrator *admin_A* for approval of the deletion operation.
 - 1. Log in to the CBH system as O&M user User_A.
 - Choose Ticket > DB Tickets and view the tickets generated due to the interception of the deletion.
 - 3. Click **Submit** to submit the application for granting the required permissions on *RDS_A*.

Figure 2-9 DB Tickets

Dashboard /	Ticket / DB Tickets							
DB Tick	tets							0
Ticket N	lumber 🔻 keyword	Q Advanced						
	Ticket Number	Status 🔻	Time ≑	Regulation	Account	Remarks	Operation	
0	202004151156025985402	approving	2020-04-15 11:56:26	Lib=mysql : Table=columns_priv :	± rool@misql		Manage Revoke Submit	
0	202004151155596190079	approving	2020-04-15 11:56:24	Lib=mysql ; Cmd=select	± root@mysql		Manage Revoke Submit	

- **Step 4** The *admin_A* approves or rejects the O&M operations performed by *User_A* based on situation.
 - 1. Log in to the CBH system as administrator *admin_A*.

- 2. Choose **Ticket** > **Approve** and review the ticket submitted by **User_A**.
- 3. Click **Approve** or **Reject** to approve or reject the ticket.

NOTE

Only after the administrator approves the ticket, the O&M user can resume the intercepted high-risk operations.

Figure 2-10 Ticket approval

Ticket N	lo 🔻 keyword 🔍 Advar	nced					
	Ticket No	Status 🔻	Time 👙	Type 🔻	Content	Creator	Operation
0	202004151156(25985402	approving	2020-04-15 11	DB Ticket	Lib=mysql ; Table=columns_priv ; Cmd=select	User_A	Manage Approve Reject F
Π	202004151155596190079	approving	2020-04-15 11	DB Ticket	Lib=mysql ; Cmd=select	User_A	Manage Approve Reject F

----End



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