

Blockchain Service

User Guide

Issue 01
Date 2024-06-17



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

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

Trademarks and Permissions



HUAWEI 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.

Contents

1 Enhanced Hyperledger Fabric BCS Management.....	1
1.1 BCS Overview.....	1
1.2 Permissions Management.....	3
1.2.1 Creating a User and Granting BCS Permissions.....	3
1.2.2 Creating a Custom Policy.....	4
1.2.3 Obtaining Resource Permissions.....	7
1.3 Instance Deployment.....	8
1.3.1 Deployment Using a CCE Cluster.....	8
1.4 Instance Management.....	16
1.4.1 Basic Operations.....	16
1.4.2 Changing Access Address.....	21
1.4.3 O&M Center.....	23
1.4.3.1 Viewing Monitoring Data and Logs.....	23
1.4.3.2 Viewing Alarms.....	25
1.4.3.3 Setting Web Disk Space Alarms.....	39
1.4.3.4 Disk Metrics.....	41
1.4.3.5 Viewing O&M Logs.....	42
1.4.3.6 Viewing Chaincode Debug Logs.....	46
1.5 Channel Management.....	47
1.6 Blockchain Management.....	50
1.6.1 Chaincode Management.....	50
1.6.2 Block Browser.....	58
1.7 Downloading SDK Configurations and Certificates.....	59
1.8 Consortium Management.....	61
1.8.1 Forming a Consortium.....	61
1.8.2 Member Management.....	62
1.8.3 Notification Management.....	62
1.9 Add-on Management.....	63
1.9.1 Add-on Overview.....	63
1.10 Contract Repository.....	65
1.11 Backup and Restoration Management.....	67
1.11.1 Creating a Backup.....	67
1.11.2 Restoring a Backup.....	70

1.12 Quotas.....	72
1.13 Key Operations Recorded by CTS.....	73
1.13.1 BCS Operations That Can Be Recorded by CTS.....	74
1.13.2 Querying Audit Logs.....	74

1 Enhanced Hyperledger Fabric BCS Management

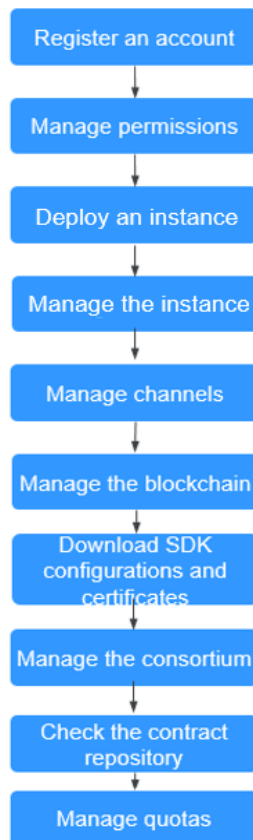
1.1 BCS Overview

Blockchain Service (BCS) allows you to deploy instances, and manage blockchains, channels, members, and notifications. The following figure outlines the BCS usage process.

 **NOTE**

BCS does not involve sensitive user information. Which, why, when, and how data is processed by BCS must comply with local laws and regulations. If sensitive data needs to be transmitted or stored, encrypt data before transmission or storage.

Figure 1-1 Procedure for using BCS



1. Register an account.
Register an account.
2. **Manage permissions.**
Create a user and grant BCS permissions.
3. **Deploy an instance.**
Enhanced Hyperledger Fabric instances can be deployed in CCE clusters.
4. **Manage the instance.**
You can view the running statuses of your enhanced Hyperledger Fabric instances and perform operations on them.
5. **Manage channels.**
Peers communicate through channels. You can create channels and add organizations and peers to them.
6. **Manage the blockchain.**
You can manage chaincodes on the web, including installing, instantiating, and updating chaincodes.
7. **Download SDK configurations and certificates.**
Before developing an application, download the configuration file which contains the user certificate and SDK.
8. **Manage the consortium.**
After creating a consortium blockchain, you can invite tenants to join it.

9. **Check the contract repository.**

The contract repository provides smart contract templates that can implement certain functions. You can directly use the code provided by the templates or use the templates as a foundation for developing your own smart contracts.

10. **Manage quotas.**

You can view and increase your quotas.

1.2 Permissions Management

1.2.1 Creating a User and Granting BCS Permissions

This section describes how to use **IAM** to implement fine-grained permissions control for your BCS resources. With IAM, you can:

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing BCS resources.
- Grant only the permissions required for users to perform a specific task.
- Entrust a Huawei Cloud account or a cloud service to perform professional and efficient O&M on your BCS resources.

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

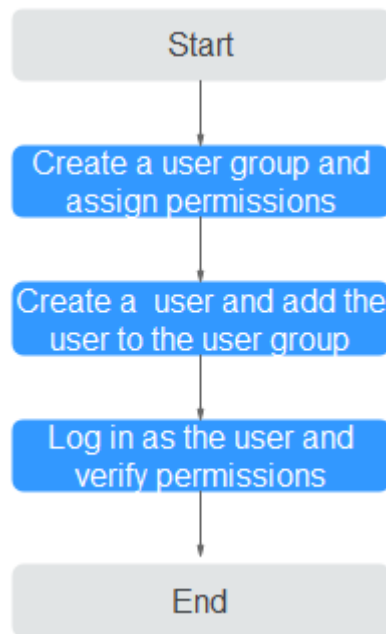
This section describes the procedure for granting permissions (see **Figure 1-2**).

Prerequisites

Learn about the permissions (see **Permissions Management**) supported by BCS and choose policies or roles according to your requirements. For the permissions of other services, see **System-defined Permissions**.

Process Flow

Figure 1-2 Process of granting BCS permissions



1. **Create a user group and assign permissions to it.**

Create a user group on the IAM console, and assign the BCS Administrator policy to the group.

NOTE

- If you select BCS Administrator, you also need to select the following dependent permissions: Tenant Guest, Server Administrator, ELB Administrator, SFS Administrator, SWR Admin, APM FullAccess, AOM FullAccess, CCE Administrator, VPC Administrator, EVS Administrator, and CCE Cluster Admin.
- Contact the account administrator to obtain the operation permissions on other services.

2. **Create a user and add the user to the user group.**

Create a user on the IAM console and add the user to the group created in 1.

3. **Log in** and verify permissions.

Log in to the BCS console as the created user, and verify that the user has the BCS operating permissions.

1.2.2 Creating a Custom Policy

Custom policies can be created to supplement the system-defined policies of BCS.

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

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

For details, see [Creating a Custom Policy](#). The following section contains examples of common BCS custom policies.

Step 1 On the management console homepage, click **Identity and Access Management**.

Step 2 In the navigation pane, choose **Permissions > Policies/Roles** and click **Create Custom Policy**.

Step 3 On the **Create Custom Policy** page, set the policy name, view, content, and description, then click **OK**.

- **Policy Name:** Enter a custom policy name, for example, "partial BCS permissions".
- **Policy View:** Select **JSON**.
- **Policy Content:** Enter the policy content based on the template.

For example, copy the following content to query instances and channels and create channels.

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "bcs:fabricInstance:getDetail",
        "bcs:fabricChannel:create",
        "bcs:fabricChannel:list"
      ]
    }
  ]
}
```

Table 1-1 Policy content parameters

Parameter		Description	Setting
Version		Policy version	Fixed to 1.1 .
Statement	Effect	Whether the actions are allowed	<ul style="list-style-type: none"> - Allow - Deny
	Action	Operations to be performed on BCS	Each action name is in the format of <i>Service name.Resource type.Operation</i> and cannot be customized. Table 1-2 lists the fine-grained permissions supported by BCS. After you set any action, the permissions for the action will be granted to the IAM user.

Table 1-2 Action description

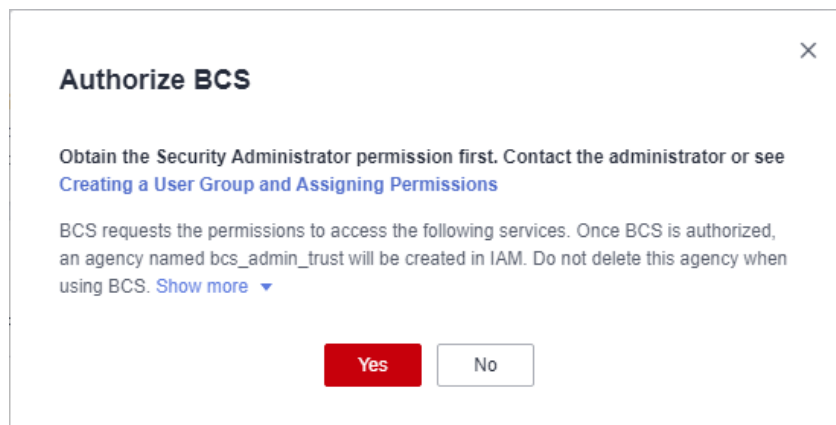
Action	Action Description
bcs:fabricInstance:listQuota	Querying quotas
bcs:fabricInstance:getFlavor	Querying Flavors
bcs:fabricInstance:listRecord	Querying Asynchronous Operation Results
bcs:fabricInstance:createOnDemand	Creating a BCS Service
bcs:fabricInstance:list	Querying the BCS Service List
bcs:fabricInstance:getStatus	Querying Creation Status of a BCS Service
bcs:fabricInstance:getDetail	Querying Service Information
bcs:fabricInstance:getNodes	Querying Peer Information
bcs:fabricInstance:update	Modifying a BCS Service
bcs:fabricInstance:delete	Deleting Service Instances
bcs:fabricInstance:downloadCert	Downloading Certificates
bcs:fabricInstance:downloadSdkCfg	Downloading the SDK Configuration
bcs:fabricInstance:createUserCert	Generating a User Certificate
bcs:fabricInstance:freezeUserCert	Freezing a User Certificate
bcs:fabricInstance:unfreezeUserCert	Unfreezing a User Certificate
bcs:fabricInstance:listInstanceMetric	Querying BCS Monitoring Data
bcs:fabricInstance:listOrgMetric	Listing Entity Monitoring Data of a BCS Service
bcs:fabricInstance:getOrgMetric	Querying the Number of Monitored BCS Organization Instances
bcs:fabricChannel:create	Creating a Channel
bcs:fabricChannel:list	Querying Channel Information
bcs:fabricChannel:addPeer	Adding Peers to a Channel
bcs:fabricChannel:removePeer	Removing a Peer from a Channel
bcs:fabricChannel:removeOrg	Removing Organizations from a Channel
bcs:fabricChannel:delete	Deleting a Channel
bcs:fabricMember:createInvitation	Inviting Tenants to Join a Consortium
bcs:fabricMember:deleteInvitation	Deleting Invitation Information

Action	Action Description
bcs:fabricMember:list	Listing Consortium Members
bcs:fabricMember:quit	Exiting a Consortium
bcs:fabricNotification:list	Querying All Notifications
bcs:fabricNotification:handle	Processing an Invitation

----End

1.2.3 Obtaining Resource Permissions

BCS works closely with multiple cloud services. When you log in to the BCS console for the first time, BCS automatically requests permissions to access those cloud services in the region where you run your applications. Click **Show more** to view details.



- On the **Instance Management** page, click **Buy** next to **Enhanced Hyperledger Fabric Instance**.
- On the **Instance Management** page, click the **Enhanced Hyperledger Fabric** tab.
- In the navigation tree on the left, choose **Channel Management, Member Management, Notification Management, or Plug-in Management**.

After you agree to delegate the permissions, an agency named **bcs_admin_trust** will be created for BCS in IAM. The system account **op_svc_bcs** will be delegated the Administrator or FullAccess permissions to perform operations on other cloud service resources. Permissions take effect only for the current tenant account. For details, see [Account Delegation](#).

To use BCS in multiple regions, you need to request cloud resource permissions in each region. You can go to the IAM console, choose **Agencies**, and click **bcs_admin_trust** to view the delegation records of each region.

 NOTE

- To ensure that BCS works properly, do not delete or modify the `bc_admin_trust` agency when using BCS.
- Obtain the Security Administrator permission on the IAM console before granting BCS permissions. For details, see [Creating a User Group and Assigning Permissions](#).

1.3 Instance Deployment

1.3.1 Deployment Using a CCE Cluster

Enhanced Hyperledger Fabric instances can be deployed in CCE clusters. This section describes how to deploy an enhanced Hyperledger Fabric instance using a CCE cluster.

- Using a CCE cluster: All the instance and blockchain data are stored on Huawei Cloud. Use your own hardware resources or buy new ones on Huawei Cloud.

 NOTE

- The BCS instance will use the CCE cluster exclusively. Ensure that the CCE cluster is available before you deploy the BCS instance.
- When you use BCS for the first time, log in to the CCE console to authorize CCE to access your BCS resources. For details, see [Preparations](#).
- You can prepare a CCE cluster in advance, and select it when you create an enhanced Hyperledger Fabric instance. Alternatively, you can customize a CCE cluster or select **Quick Config** to use the default specifications when you create an enhanced Hyperledger Fabric instance.
- When deploying a BCS instance using a CCE cluster, implement security hardening to ensure that the instance functions properly. For example, you can forbid the root user to remotely log in to the system, disable port 22 in the security group, delete sniffing/development/debugging/compilation tools, set the system session timeout duration (cannot be infinite), and disallow containers to access the management IP of OpenStack (169.254.169.254). Note that access control of 169.254.169.254 will restrict AOM from detecting ICAgent in the cluster, but the data can still be collected and reported. For more security hardening suggestions, see [Node Security Configuration](#).
- If you deploy your instance using a new cluster, BCS automatically disallows containers to access 169.254.169.254 and deletes port 22 from the security group. If you deploy your instance using an existing cluster, implement security hardening by referring to [Node Security Configuration](#).

Prerequisites

Only IAM users with robust permissions can subscribe to BCS instances. For details, see [Permissions Management](#).

You can create a user group, grant permissions to the user group, and then add the user to the user group. In this way, the user has the permissions of the user group.

Deploying a BCS Instance

After the environment is ready, perform the following steps to purchase a BCS instance:

NOTE

If your account is in arrears, the instance web disk will be released and the purchased instances will be unavailable.

Step 1 Go to the page for purchasing [enhanced Hyperledger Fabric instances](#).

Step 2 Configure basic information about the BCS instance by referring to [Table 1-3](#).

Table 1-3 Basic information parameters

Parameter	Description	Example Setting
Billing Mode	BCS instances are billed in pay-per-use mode.	-
Region	Select the region where the blockchain infrastructure is located. You are advised to select the same region as the service application system.	Retain the default value.
Enterprise Project	Select an existing enterprise project, to which the BCS instance will be added. NOTE <ul style="list-style-type: none">If the Enterprise Management service is not enabled, this parameter is unavailable. For details, see Enabling the Enterprise Project Function.When deploying an instance in an existing CCE cluster, choose the same enterprise project as that used by the cluster to ensure instance performance.	default
Instance Name	An instance name can contain 4 to 24 characters, including letters, digits, and hyphens (-). It cannot start with a hyphen (-). NOTE Currently, the name of a created BCS instance cannot be changed. You can only create a new instance with a new name.	Enter bcs-wh .
Edition	BCS provides basic and professional editions. NOTE Editions cannot be changed for a deployed BCS instance.	Select Professional .

Parameter	Description	Example Setting
Blockchain Type	A private blockchain is used only by the tenant that creates it. A consortium blockchain can be used by multiple tenants.	Select Private .
Enhanced Hyperledger Fabric Version	BCS instance version. BCS v4.x.x corresponds to Hyperledger Fabric v2.2.	Select v2.2 .
Consensus Mechanism	The supported mechanisms for blockchain nodes reaching consensus include: Raft (crash fault tolerant) and Fast Byzantine fault tolerance (FBFT). NOTE If Raft (CFT) is selected, a basic or professional edition instance has three orderers by default.	Select FBFT .
Resource Access Initial Password	Password of blockchain administration user admin , ECS user root , or CouchDB database user. It will be used as such a password if you do not set Blockchain Mgmt. Initial Password, Password of Root User, or Initial Password displayed when NoSQL (CouchDB) is selected for Ledger Storage .	-
Confirm Password	Confirm the resource access initial password.	-

Step 3 (Optional) Click **Quick Config** to allow the system to automatically purchase an instance with the specifications listed in [Table 1-4](#).

Table 1-4 Default specifications

Item	Professional Edition	Enterprise Edition
Number of ECSs	1	2
ECS specifications	4 vCPUs 8 GB	4 vCPUs 8 GB
	Note: If the default specifications are sold out, other higher specifications will be purchased by default.	
High availability of the CCE cluster	Yes	Yes
Storage space of SFS Turbo	1000 GB	1000 GB

Item	Professional Edition	Enterprise Edition
EIP	Type: Dynamic BGP; Bandwidth: 5 Mbit/s	

Step 4 Click **Next: Configure Resources**. [Table 1-5](#) describes the resource parameters.

Table 1-5 Resource parameters

Parameter	Description	Example Setting
Environment Resources	Use the default environment or customize your environment resources.	Select Custom .
Cluster	Cluster where the BCS instance will be deployed. You can use an existing cluster or create a new CCE cluster. NOTE <ul style="list-style-type: none"> CCE clusters of v1.19 or earlier are supported. If the BCS instance uses Fabric v1.4, the CCE cluster must be v1.15 or earlier. The memory usage of instantiated containers varies depending on the chaincode language. On each peer, a Go chaincode container takes up 10 MB for running, and a Java chaincode takes up 110 MB. For example, if 100 Java chaincodes need to be instantiated, a 16 vCPUs and 32 GB CCE node is preferred. 	Select Create a new CCE cluster .
AZ	Select the AZ where the ECS is located.	Select AZ1 .
ECS Specifications	Specifications of the ECSs in the CCE cluster.	Select the flavor for 4 vCPUs 8 GB .
ECS Quantity	Enter the required ECS quantity. For details, see Edition Differences .	Enter 2 .
High Availability	If you have high requirements on system reliability, purchase high-availability ECSs.	Yes
VPC	You can create a new virtual private cloud (VPC), select an existing VPC, or let the system automatically create a VPC.	Select Automatically create VPC .
Subnet	A subnet provides dedicated network resources that are logically isolated from other networks for network security.	Select Automatically create subnet .
ECS Login Method	Either a password or key pair can be used to log in to ECSs.	Select Password .

Parameter	Description	Example Setting
Password of Root User	Password of the root user for logging in to ECSs. If you do not enter a password here, the previously specified resource access initial password will be used.	-
Confirm Password	Confirm the ECS login password of the root user.	-
Use EIP of a CCE Node	<ul style="list-style-type: none"> If you select Yes, an EIP bound to the cluster will be used as the blockchain network access address. If the cluster is not bound with any EIP, bind an EIP to the cluster first. If you select No, a private address of the cluster will be used as the blockchain network access address. Ensure that the application can communicate with the internal network of the cluster. 	Select Yes .
Data Backup	Whether to back up the management data and ledger data. This parameter is set to Yes by default. <ul style="list-style-type: none"> Yes: Management data and ledger data of the BCS instance will be backed up in Object Storage Service (OBS) and Cloud Backup and Recovery (CBR). Do not perform any operations on the backup data. No: Data backup is disabled. 	
EIP Billed By	Pay-per-use has been selected for Billing Mode , so EIPs can be charged by bandwidth or traffic.	Select Bandwidth .
EIP Bandwidth	Select a bandwidth as required.	Set it to 5 Mbit/s.

Step 5 Click **Next: Configure Blockchain**. [Table 1-6](#) describes the blockchain parameters.

Table 1-6 Blockchain parameters

Parameter	Description	Example Setting
Blockchain Configuration	Use the default blockchain configurations or customize your own blockchain configurations.	Select Custom .

Parameter	Description	Example Setting
Blockchain Mgmt. Initial Password	Enter the blockchain management initial password. If you do not enter a password here, the previously specified resource access initial password will be used.	-
Confirm Password	Enter the blockchain management initial password again for confirmation.	-
Volume Type	SFS Turbo provides low-latency and high-IOPS file storage.	Select SFS Turbo .
Storage Capacity of Peer Organization (GB)	Stores shared distributed ledger, consensus data, and other intermediate data of the blockchain system.	Set it to 500 GB.
Ledger Storage	File database (GoLevelDB) and NoSQL (CouchDB) are supported. <ul style="list-style-type: none"> File database (GoLevelDB): The Fabric native storage mode is used. Historical transaction data is stored in the blockchain, and status data is stored in the LevelDB. NoSQL (CouchDB): The CouchDB storage mode supported by the Fabric is used to store transaction data and status data. Each CouchDB database is a collection of independent documents. Each document maintains its own data and self-contained schema. 	Select File database (GoLevelDB) .
Peer Organization	Peer organizations to be added to the BCS instance. <ul style="list-style-type: none"> If you use an existing cluster, customize the peer organization name and peer quantity. Automatically create SFS Turbo file system will be displayed in the Network Storage area. If you use a new CCE cluster, customize the peer organization name and peer quantity. 	Add a peer organization named organization with 2 peers.

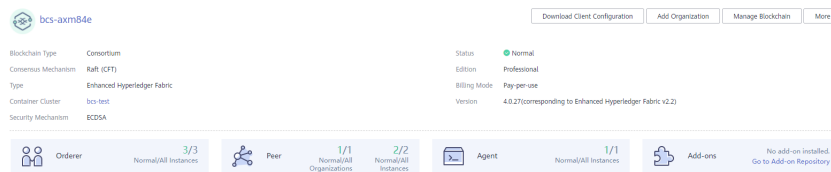
Parameter	Description	Example Setting
Channel Configuration	Channels isolate business in a consortium blockchain. Business participants (some or all of the organizations in a consortium) are channel members. Each channel can be regarded as a sub-chain and corresponds to one distributed ledger.	By default, a channel named channel has been created, and the peer organization you just specified has been added to the channel.
Orderer Quantity	Number of nodes that order transactions into blocks in the blockchain network. When the consensus mechanism is Raft (CFT), the number of orderers is 3.	Enter 3 .
Security Mechanism	Encryption algorithm used to ensure data security. ECDSA and OSCCA-published cryptographic algorithms are supported.	Select ECDSA .
Configure Block Generation	The configuration of block generation includes the block generation interval, maximum number of transactions in a block, and maximum size of a block. A new block is generated at the specified interval or when the transaction quantity or size of a block reaches the threshold. Configure these parameters based on the transaction frequency and service volume. Select Yes or No as required. <ul style="list-style-type: none"> • Yes: Set the block generation interval, transaction quantity per block, and block size as required. • No: You do not need to set parameters. By default, the block generation interval is 2 seconds, the number of transactions per block is 500, and the block size is 2 MB. 	Select No .
Enable Support for RESTful API	If you need to use RESTful APIs to invoke chaincodes, select Yes . NOTE This function is under OBT.	Select No .

Step 6 Click **Next: Confirm**.

Step 7 Confirm the configurations, confirm that you have read and agree to the agreement, and click **Pay Now**.

Wait for several minutes. After a message is displayed indicating successful installation, check the status of the instance. If it is **Normal**, the deployment is completed.

Figure 1-3 Instance status

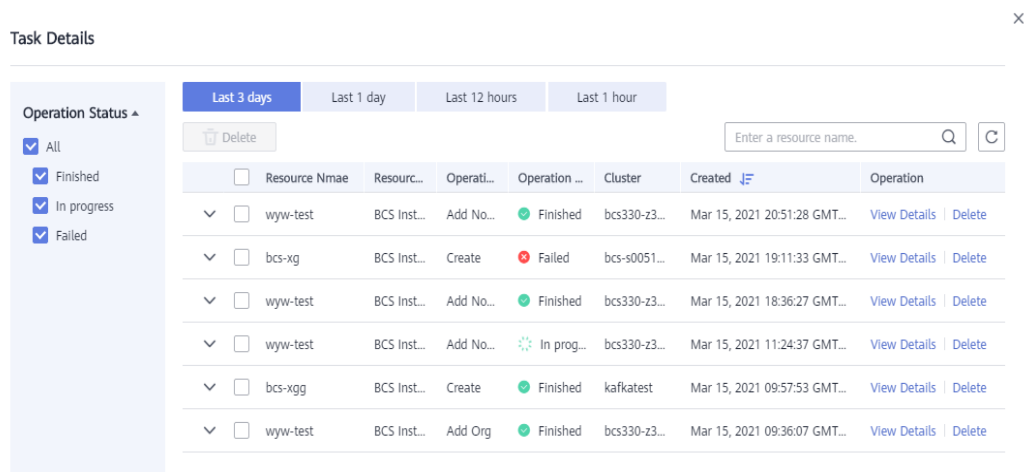


----End

Subsequent Operations (Optional)

View the operation records of creating, deleting, and upgrading instances, adding organizations, expanding peers, creating channels, and adding peers to channels. In the left part of the window, you can filter records by status, including **In progress**, **Upgrading**, **Deleting**, **Finished**, and **Failed**. The figure is for reference only.

Figure 1-4 Operation records



The system stores records of the latest three days.

Step 1 Log in to the BCS console. In the navigation pane, click **Instance Management**.

Step 2 Click **Task Details**.

Search records by the resource name. You can also view details or delete records.

----End

You can configure an anti-affinity label for the cluster node where the BCS instance is deployed. This label can be used to isolate the instance from other applications in the same cluster to ensure normal running of the system.

Step 1 Log in to the CCE console.

Step 2 On the **Clusters** page, click a target cluster.

Step 3 On the **Nodes** tab page, click a node, and click **Manage Labels and Taints**.

Step 4 In the **Batch Operation** area, click **Add Operation**, and select **Add/Update** from the drop-down box. Set **Key** to **nodeScope** and **Value** to **userApplication** for the label to be added.

Manage Labels and Taints

Batch Operation

Update and delete labels and taints of specified nodes in batches.

Add Operation

Node Data

The batch operation will be performed on the following data: [Show](#) ▼

Step 5 Click **OK**.

Step 6 After the label is added, click **Manage Labels and Taints** again. In the **Node Data** area, click **Show** to view the added labels.

----End

1.4 Instance Management

1.4.1 Basic Operations

You can view the running statuses of your enhanced Hyperledger Fabric instances and perform operations on them.

Procedure

Step 1 Log in to the BCS console.

Step 2 In the navigation pane, click **Instance Management**. You can view the overall running status of your instances. For details about the parameters, see [Table 1-7](#).

Figure 1-5 Viewing an enhanced Hyperledger Fabric instance

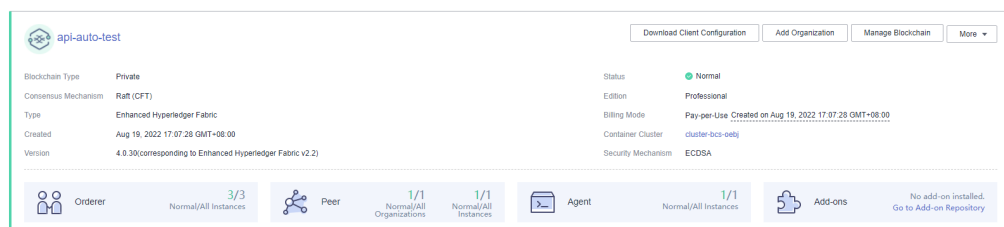


Table 1-7 Parameters

Parameter	Description
Blockchain Type	Type of the blockchain, that is, Consortium or Private .
Consensus Mechanism	Consensus mechanism used by the instance, for example, Raft (CFT) . The following consensus mechanisms are supported: <ul style="list-style-type: none">• FBFT: The fast Byzantine fault tolerance (FBFT) algorithm. It requires 4 to 10 orderers for transaction ordering and tolerates faults at a maximum of $(N - 1)/3$ orderers, where N indicates the total number of orderers. It supports Fabric v2.2.• Raft (CFT): A CFT ordering instance that tolerates faults at a maximum of $(N - 1)/2$ orderers, where N indicates the total number of orderers. It supports Fabric v2.2.
Type	Type of the instance, which is Enhanced Hyperledger Fabric .
Created	Time when the BCS instance was created, for example, Dec 10, 2022 20:30:21 GMT+08:00 .
Container Cluster	The cluster where the BCS instance is deployed.
Security Mechanism	Encryption algorithm used to ensure data security.
Status	Status of the BCS instance, which can be Unknown, Normal, Abnormal, Creating, Upgrading, Adding peers, EIP abnormal, Deleting, Frozen, Hibernated , or Cluster frozen .
Edition	There are basic professional editions.
Billing Mode	Billing mode of the BCS instance, that is, Pay-per-use . <ul style="list-style-type: none">• Pay-per-use: The creation time is displayed. For example: Pay-per-use Created on Aug 10, 2020 20:30:21.
Version	BCS instance version.
Orderer	Numbers of normal and abnormal orderer organizations.
Peer	Numbers of peer organizations and instances.
Agent Peer	Numbers of normal and abnormal agent organizations.
Add-ons	Number of add-ons. For example, 1/2 indicates that the total number of instances is 2 and 1 instance is normal.

Step 3 On the **Instance Management** page, you can perform operations listed in [Table 1-8](#).

Table 1-8 Operations

Category	Operation	Description
Organization management	Adding an organization	<ol style="list-style-type: none"> On an instance card, click Add Organization. Specify the organization name, network storage instance, and peer quantity. Click Next. <p>NOTE</p> <ul style="list-style-type: none"> Do not perform operations on the instance when adding an organization. The Price is an hourly price for a pay-per-use instance after the change. After you add an organization to an existing channel, update the endorsement policy of the channel before instantiating the chaincode. Otherwise, the instantiation may fail due to a certificate verification failure. After organization addition, the price will change. Pay attention to the notes on the upper part of the page and the price at the bottom.
Instance management	Downloading client configurations	Before developing an application, download the SDK configurations and application certificates for accessing the blockchain network. On the Instance Management page, click Download Client Configuration and select configuration files to download, including the SDK configuration file, orderer certificate, and peer certificates. For details, see Downloading SDK Configurations and Certificates .
	Managing the blockchain	This operation is available only after an EIP is bound. On an instance card, click Manage Blockchain to view, install, instantiate, upgrade, and delete chaincodes.

Category	Operation	Description
	Upgrading the version	<p>A BCS instance can be upgraded to the latest version if Upgradable is displayed in the upper left corner of the instance card. The operations are as follows:</p> <ol style="list-style-type: none"> 1. Log in to the BCS console. 2. In the navigation pane, click Instance Management. 3. Choose More > Upgrade on an instance card. 4. View the current instance version or upgrade the BCS instance to the latest version. <p>NOTE</p> <ul style="list-style-type: none"> • Before upgrading your consortium blockchain instance, reach an agreement with other members to eliminate effects on their instances. • Do not initiate version upgrade when the chaincode is being installed or instantiated. • You can upgrade a BCS instance from the version corresponding to Hyperledger Fabric v1.4 to the version corresponding to Hyperledger Fabric v2.2. If one member in a consortium blockchain has upgraded, all consortium members must also upgrade to the same version. Otherwise, transactions will fail. <ul style="list-style-type: none"> – BCS v3.x.x corresponds to Hyperledger Fabric v1.4.0. – BCS v4.x.x corresponds to Hyperledger Fabric v2.2. • You can only upgrade an instance from an earlier version to a later version. Rollback is supported only if the upgrade fails.
	Rolling back upgrade	<p>If the version fails to be updated, you can roll back the upgrade. The operations are as follows:</p> <ol style="list-style-type: none"> 1. Log in to the BCS console. 2. In the navigation pane, click Instance Management. 3. Choose More > Roll Back Version on an instance card. 4. During the rollback, the instance status is Upgrading. After the rollback is completed, the instance status is Normal. <p>NOTE</p> <p>Instances failed the upgrade can be upgraded again after the rollback.</p>

Category	Operation	Description
	Resetting the management password	Choose More > Reset Management Password on an instance card. By default, resetting this password will also reset the passwords for logging in to the Blockchain Management console and Trusted Computing Platform. If you do not want to reset these passwords together, change the passwords on the Blockchain Management console or Trusted Computing Platform separately.
	Changing the blockchain network access address	Choose More > Change Access Address on an instance card, select a new address, and click OK .
	Hibernating	Choose More > Hibernate on an instance card, and click OK . NOTE Only instances in the Normal state can be hibernated.
	Waking	Choose More > Wake , and click OK . NOTE Only instances in the Hibernated state can be woken.
	Deleting	Choose More > Delete . NOTE Data, chaincodes, and applications on the blockchain nodes cannot be restored. Exercise caution. <ul style="list-style-type: none"> • If you delete the CCE cluster, the SFS file system used by the instance will also be deleted, and the blockchain data cannot be restored. • If you delete the SFS file system used by the instance, the blockchain data cannot be restored, but the CCE cluster still exists.

Step 4 Click an instance name to view the instance details.

- Viewing instance basic information
On the **Basic Information** tab page, view the instance details, agent peers, orderers, peers, CPU usage, and physical memory usage.
- Monitoring data
On the **Monitoring** tab page, view monitoring data about the instances.
For details about how to view monitoring information, see [Viewing Monitoring Data and Logs](#).
- Viewing logs
On the **Logs** tab, view the logs of the organization instances and add-on instances.

For details about how to view log information, see [Viewing Monitoring Data and Logs](#).

- Downloading certificates


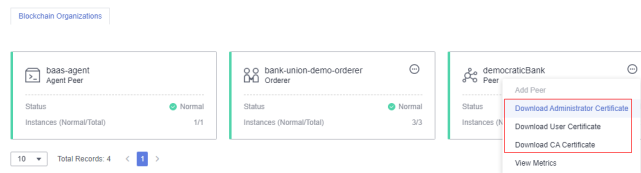
In the **Blockchain Organizations** area on the **Basic Information** tab page, click  to download the certificates.


Figure 1-6 Downloading certificates



NOTE

You can click **Download Client Configuration** on an instance card to download the SDK and certificates. For details, see [Downloading SDK Configurations and Certificates](#).

- Adding peers

In the **Blockchain Organizations** area on the **Basic Information** tab page, click , and click **Add Peer**. Specify the peer quantity, confirm the configurations, and click **Submit**.

NOTE

- Do not perform operations on the instance when adding peers.
- The **Price** is an hourly price for a pay-per-use instance after the change.
- Each organization supports a maximum of 2 peers in a basic or professional edition instance. No more peers can be added after the number of peers has reached the maximum allowed limit.

----End

1.4.2 Changing Access Address

You can update the access address of an instance by IP or domain name.

Changing Address By IP

Step 1 Log in to the BCS console.

Step 2 On the **Instance Management** page, click the **Enhanced Hyperledger Fabric** tab.

Step 3 Choose **More > Change Access Address** on the card of a BCS instance.

Step 4 Set **Updated By** to **IP** and specify whether to **Customize New Address**. If you keep the default setting (**No**), select a new address, and click **OK**.

NOTE

If you set **Customize New Address** to **Yes**, use a valid private network address of the cluster or a valid EIP bound to the cluster. If there is a blockchain network failure, check and modify the IP address.

----End

Changing Address By Domain Name

Prerequisites: You have registered a domain name with the domain name registrar.

- Step 1** Log in to the Domain Name Service (DNS) console.
- Step 2** On the **Public Zones** page, click **Create Public Zone**, enter the **Domain Name** registered with the domain name registrar. For details, see [Creating a Public Zone](#).
- Step 3** In the zone list on the **Public Zones** page, click a domain name to display the **Record Sets** page. Perform the following steps to configure the record set for the domain name. For details, see [How Do I Add Record Sets to Subdomains?](#)

NOTE

- In DNS, a record set is a collection of resource records that belong to the same domain name to define DNS record types and values.
- Add a prefix to the domain name in the **Name** field on the **Add Record Set** page. The prefix and the public domain name correspond to a BCS instance.

Step 4 Click **Add Record Set**.

Step 5 Specify the **Name**. Enter the access address of the BCS instance in the **Value** field.

NOTE

To obtain the address, go to the BCS console, on the **Instance Management** page, choose **More > Change Access Address** on a BCS instance card, then record the **Current Address**.

Add Record Set

Name ?

* Type

* Line ?

* TTL(s) **5 min** 1 h 12 h 1 day ?

* Value ?

Weight ?

Tag It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. [View predefined tags](#) C
To add a tag, enter a tag key and a tag value below.

10 tags available for addition.

Description 0/255

- Step 6** After the domain name resolution is complete, go to the BCS console.
- Step 7** Choose **More > Change Access Address** on the card of a BCS instance.
- Step 8** Set **Updated By** to **Domain name**, enter a domain name, and click **OK**.

Change Access Address ×

Current Address

Updated By **Domain name**

----End

1.4.3 O&M Center

1.4.3.1 Viewing Monitoring Data and Logs

BCS provides O&M monitoring capabilities. Technical support engineers can view the monitoring data and logs on the BCS console.

Viewing Monitoring Data

- Step 1** Log in to the BCS console.
- Step 2** In the navigation pane, click **Instance Management** to view the basic information of a BCS instance, including the blockchain type, consensus mechanism, status, and creation time.

Step 3 On an instance card, click the instance name.

Step 4 Click the **Monitoring** tab to view the service monitoring and instance monitoring data.

- Service monitoring allows you to view the CPU usage, physical memory usage, network traffic, TPS, and disk usage of the service.

NOTE

TPS of invitee instances is not displayed.

- Instance monitoring allows you to view the organization instance information, including the CPU usage, disk read rate, disk write rate, physical memory usage, uplink rate, and downlink rate.

You can click **View Metrics** to view the data of the last 15 minutes. You can also click **More** to view more monitoring data.

Figure 1-7 Viewing more monitoring data



----End

Viewing Logs

Step 1 Log in to the BCS console.

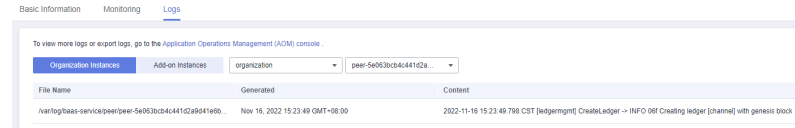
Step 2 In the navigation pane, click **Instance Management** to view the basic information of a BCS instance, including the blockchain type, consensus mechanism, status, and creation time.

Step 3 On an instance card, click the instance name.

Step 4 Click the **Logs** tab. By default, log data in the last 5 minutes is displayed, including the log file name, creation time, and log content.

To view more logs or export logs, go to the AOM console.

Figure 1-8 Viewing logs



----End

1.4.3.2 Viewing Alarms


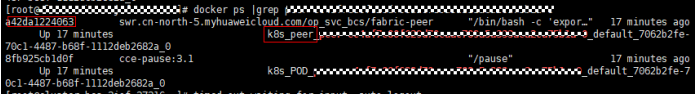
BCS provides O&M monitoring capabilities. Technical support can view alarms generated in BCS and CCE. [Table 1-9](#) lists common alarms.

NOTE


Perform preliminary checks based on the following table. If the alarm persists, contact technical support.

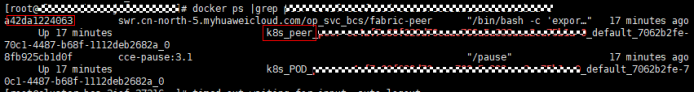
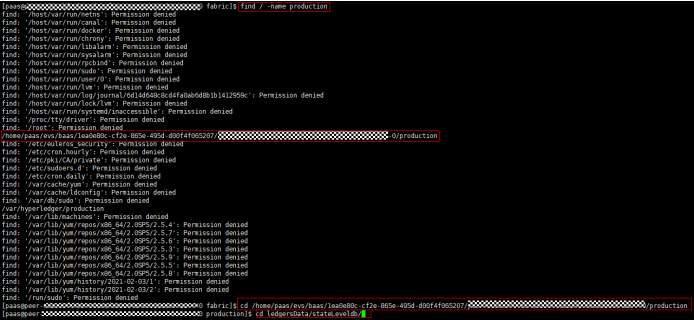
If an alarm is generated in CCE, and BCS instances are running properly, refer to [Cloud Container Engine FAQs](#).

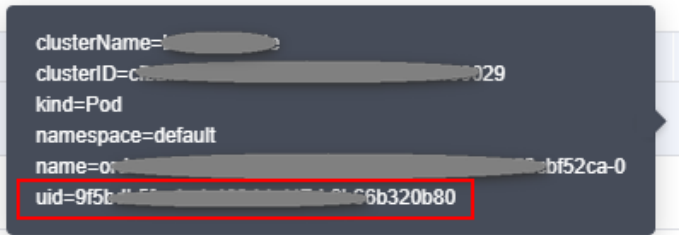
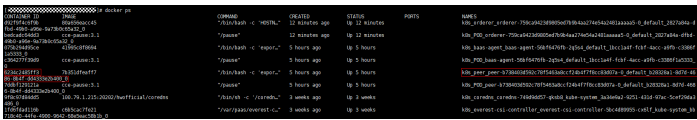
Table 1-9 Common alarms for BCS

Alarm Name	Alarm Source	Solution
PeerConnect Failed	BCS	<p>Peers fail to connect to orderers. Possible causes include:</p> <ul style="list-style-type: none"> • The network may have fluctuated. • The orderer is abnormal. <p>If the network fluctuates, the alarm will be automatically cleared within a few minutes.</p> <p>If the alarm persists and is not cleared after a few minutes, the peer may have been disconnected from the orderer. In this case, perform the following steps:</p> <ol style="list-style-type: none"> 1. Log in to the BCS console, click Instance Management in the navigation pane, and click an instance to go to the instance details page. 2. On the BCS instance details page, click the Monitoring tab and then the Active tab. Record the value of name in the Resource Name column. <p>Figure 1-9 Checking name of the failed peer</p>  <p>Figure 1-9 Checking name of the failed peer</p> <pre> clusterName=... clusterID=cfb2...0029 kind=Pod namespace=default name=ord...52ca-0 uid=9f...320b80 </pre> <ol style="list-style-type: none"> 3. Log in to all nodes (bound with EIPs) in the CCE cluster where the instance is deployed and run the docker ps grep name command (as shown in the following figure). The container whose name starts with k8s_peer (or k8s_orderer for an orderer) is the container for which the alarm is generated. The container ID is at the start of the section. <p>Figure 1-10 Viewing the command output</p>  <p>Figure 1-10 Viewing the command output</p> <pre> [root@4526a122466d]# docker ps grep Up 17 minutes 70c1-4487-b68f-1112deb2682a_0 k8s_peer_ 8fb925cb1d0f cce-pause:3.1 /pause" 17 minutes ago Up 17 minutes 9c1-4487-b68f-1112deb2682a_0 k8s_POD_..._default_7062b2fe-7 </pre> <p>NOTE For details about how to log in to a node in a CCE cluster, see Viewing O&M Logs on a Backend VM.</p> <ol style="list-style-type: none"> 4. Check whether the container is normal. 5. If the container is abnormal, run the docker restart Container ID command to restart the container.

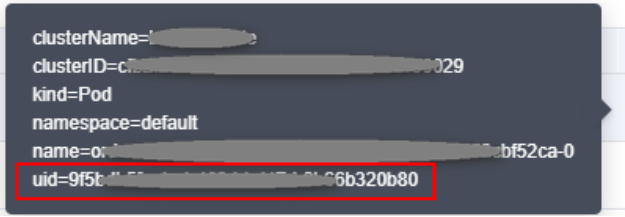
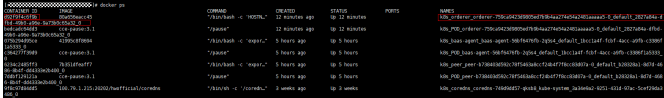
Alarm Name	Alarm Source	Solution
		6. If the fault persists, go to Log > Log Files on the AOM console. Download the log files of the peer and orderer on the cluster for which the alarm is generated, and send the log files to technical support.

Alarm Name	Alarm Source	Solution
PeerWriteDB Failed	BCS	<p>A peer fails to access database files. Possible causes include:</p> <ul style="list-style-type: none"> • The status database file is damaged or lost. • The storage service mounted to the status database is deleted. <p>To rectify this fault, perform the following steps:</p> <ol style="list-style-type: none"> 1. Log in to the BCS console, click Instance Management in the navigation pane, and click an instance to go to the instance details page. 2. Click the value next to Cluster to go to the CCE console, and click the target cluster. On the Storage page, check whether the PVC bound to the peer exists and is normal. <ul style="list-style-type: none"> • If it does not exist or is abnormal, create a PVC and bind it to the BCS instance. • If it exists, perform the following steps. 3. On the BCS instance details page, click the Monitoring tab and then the Active tab. Record the value of name in the Resource Name column. <p>Figure 1-11 Checking name of the peer that failed to access the database</p>  <pre> clusterName=... clusterID=cfb2...00029 kind=Pod namespace=default name=ord...2ca-0 uid=9f...b320b80 </pre> 4. Click the alarm and record clusterID and name. 5. Go to the CCE console, click Storage, and check whether the PVC bound to the peer exists. If it does not exist, create a PVC and bind it to the peer. 6. Log in to all nodes (bound with EIPs) in the CCE cluster where the instance is deployed and run the docker ps grep name command (as shown in the following figure). The container whose name starts with k8s_peer (or k8s_orderer for an orderer) is the container for which the alarm is generated. The container ID is at the start of the section.

Alarm Name	Alarm Source	Solution
		<p>Figure 1-12 Viewing the command output</p>  <p>NOTE For details about how to log in to a node in a CCE cluster, see Viewing O&M Logs on a Backend VM.</p> <ol style="list-style-type: none"> Run the docker exec -it container id /bin/bash command to enter the container. Run the find / -name production command to go to the found path, as shown in the following figure. <p>Figure 1-13 Viewing the path</p>  <p>Check whether the CURRENT, LOG, and MANIFEST-000*** files exist in the ledgersData/stateLeveldb/ directory. If these files do not exist, run the docker restart Container ID command to restart the peer container.</p> <ol style="list-style-type: none"> If the fault persists, go to Log > Log Files on the AOM console. Download the log files of the peer and orderer on the cluster for which the alarm is generated, and send the log files to technical support.

Alarm Name	Alarm Source	Solution
PeerNodeDiskAvailableNotEnough	BCS	<p>The peer disk space is insufficient and needs to be expanded. Perform the following steps to expand the disk space:</p> <ol style="list-style-type: none"> 1. Log in to the BCS console, click Instance Management in the navigation pane, and click an instance to go to the instance details page. 2. Click the Monitoring tab and then the Active tab. Record the value of uid in the Resource Name column. <p>Figure 1-14 Checking uid</p>  <ol style="list-style-type: none"> 3. Log in to all nodes (bound with EIPs) in the CCE cluster where the BCS instance is deployed and run the docker ps command on the nodes one by one until you find the Container ID, that is, the first 12 digits of the uid obtained in the previous step. Record the value of the corresponding NAMES. <p>Figure 1-15 Viewing the command output</p>  <p>For example, if the value of NAMES is k8s_peer_peer-b738403d592c78f5463a8ccf24b4f7f8cc83d07a-0_default_b28328a1-8d7d-4686-8b4f-dd4333e2b400_0, the corresponding peer name is peer_peer-b738403d592c78f5463a8ccf24b4f7f8cc83d07a-0.</p> <p>NOTE For details about how to log in to a node in a CCE cluster, see Viewing O&M Logs on a Backend VM.</p> <ol style="list-style-type: none"> 4. On the BCS instance details page, click More on the Basic Information tab page and then click View Details next to Network Storage to obtain PVC Name.

Alarm Name	Alarm Source	Solution
		<ol style="list-style-type: none"><li data-bbox="655 416 1442 533">5. Log in to the CCE console, click Clusters, and select a target cluster. On the cluster details page, click Storage.<li data-bbox="655 533 1442 647">6. On the PersistentVolumeClaims (PVCs) tab page, choose More > Scale-out in the Operation column containing the recorded PVC.


Alarm Name	Alarm Source	Solution
OrdererNode DiskAvailableNotEnough	BCS	<p>The orderer disk space is insufficient and needs to be expanded. Perform the following steps to expand the disk space:</p> <ol style="list-style-type: none"> 1. Log in to the BCS console, click Instance Management in the navigation pane, and click an instance to go to the instance details page. 2. Click the Monitoring tab and then the Active tab. Record the value of uid in the Resource Name column. <p>Figure 1-16 Checking uid of the orderer</p>  <p>Figure 1-17 Checking the value of NAMES</p>  <p>For example, if the value of NAMES is k8s_orderer_orderer-759ca9423d9805ed7b9b4aa274e54a2481aaaaa5-0_default_2827a84a-dfdb-49b0-a96e-9a73b0c65a32_0, the corresponding orderer name is orderer_orderer-759ca9423d9805ed7b9b4aa274e54a2481aaaaa5-0.</p> <p>NOTE For details about how to log in to a node in a CCE cluster, see Viewing O&M Logs on a Backend VM.</p> <ol style="list-style-type: none"> 4. On the BCS instance details page, click More on the Basic Information tab page and then click View Details next to Network Storage to obtain PVC Name.

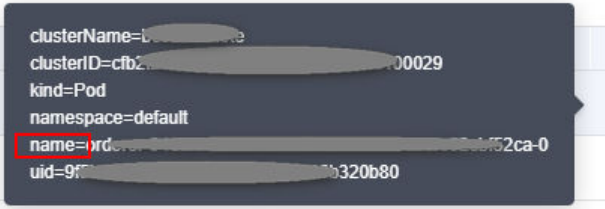
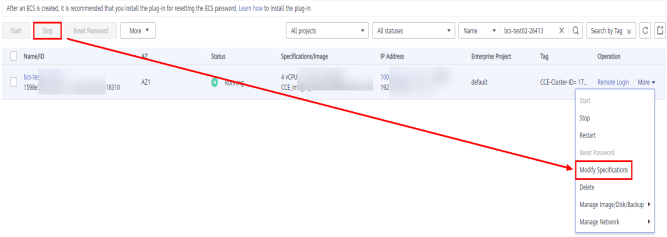
Alarm Name	Alarm Source	Solution
		<ol style="list-style-type: none"> 5. Log in to the CCE console, click Clusters, and select a target cluster. On the cluster details page, click Storage. 6. On the PersistentVolumeClaims (PVCs) tab page, choose More > Scale-out in the Operation column containing the recorded PVC.
FailedPullImage	CCE	<p>The image address is incorrect. For example, the image address configured in the add-on at some sites is incorrect, or the permission configured for the image repository is incorrect.</p> <p>If a large number of images are pulled concurrently, some images may fail to be pulled. If the images can be pulled successfully after retry, the alarm is cleared.</p>
BackOffPullImage	CCE	<p>The image address is incorrect. For example, the image address configured in the add-on at some sites is incorrect, or the permission configured for the image repository is incorrect. If the images can be pulled successfully after retry, the alarm is cleared.</p>
FailedCreate	CCE	<p>Check the pod status of baas-agent, peer, and orderer.</p> <p>Do as follows:</p> <ol style="list-style-type: none"> 1. Check whether the pod scheduling policy is correct. Log in to the CCE console, click Clusters, and select a target cluster to view its details. Choose Workloads > Deployments or StatefulSets in the navigation pane, click the workload name to go to the workload details page, and check CPU requests and memory requests on the Pods tab. 2. Check whether the node resources are sufficient. Log in to the CCE console, click Clusters, and select a target cluster to view its details. Click Nodes in the navigation pane on the left. On the Nodes tab page, check CPU requests and memory requests.

Alarm Name	Alarm Source	Solution
BackOffStart	CCE	<p>Check the pod status of baas-agent, peer, and orderer. Do as follows:</p> <ol style="list-style-type: none">1. Check whether the pod scheduling policy is correct. Log in to the CCE console, click Clusters, and select a target cluster to view its details. Choose Workloads > Deployments or StatefulSets in the navigation pane, click the workload name to go to the workload details page, and check CPU requests and memory requests on the Pods tab.2. Check whether the node resources are sufficient. Log in to the CCE console, click Clusters, and select a target cluster to view its details. Click Nodes in the navigation pane on the left. On the Nodes tab page, check CPU requests and memory requests.
Unhealthy	CCE	<p>Check the pod status of baas-agent, peer, and orderer. Do as follows:</p> <p>Log in to the CCE console, click Clusters, and select a target cluster to view its details. Choose Workloads > Deployments or StatefulSets in the navigation pane, and check the health check details on the Containers tab.</p>

Alarm Name	Alarm Source	Solution
FailedScheduling	CCE	<p>Check the pod status of baas-agent, peer, and orderer. Do as follows:</p> <ol style="list-style-type: none"> 1. Check whether the node resources are sufficient. Log in to the CCE console, click Clusters, and select a target cluster to view its details. Click Nodes in the navigation pane on the left. On the Nodes tab page, check CPU requests and memory requests. 2. Check whether the pod scheduling policy is correct. Log in to the CCE console, click Clusters, and select a target cluster to view its details. Choose Workloads > Deployments or StatefulSets in the navigation pane, click the workload name to go to the workload details page, and click Scheduling Policies. <p>NOTE The coredns add-on is a DNS server that provides domain name resolution services for Kubernetes clusters. coredns chains plug-ins to provide additional features. At least two nodes are required to ensure the proper running of coredns. Therefore, if the number of nodes in the cluster where the BCS instance is located is less than 2, the alarm indicating failed scheduling is frequently generated. This alarm does not affect BCS functions.</p> <p>Do as follows:</p> <ol style="list-style-type: none"> 1. Log in to the BCS console. 2. In the navigation pane, click Instance Management. 3. Click an instance name to go to the instance details page. 4. On the Monitoring tab page, locate the row that contains the alarm, hover the mouse pointer over the resource name, and check the value of name. If the value starts with "coredns-", the alarm does not need to be handled.
Rebooted	CCE	<p>The node has been restarted. If the baas-agent, peer, and orderer services are deployed on the node, check whether the pod status is abnormal. If these instances are not deployed on the node, BCS is not affected.</p> <p>Do as follows:</p> <ol style="list-style-type: none"> 1. Check whether the restart is caused by manual operations (such as shutdown and restart). 2. Check whether the restart is caused by node resource overload. Go to the AOM console, choose Monitoring > Host Monitoring in the navigation pane, and check the CPU usage and memory usage.

Alarm Name	Alarm Source	Solution
NodeNotReady	CCE	<p>If the baas-agent, peer, and orderer services are deployed on the node, restore the node status or migrate services to other nodes.</p> <p>Do as follows:</p> <ol style="list-style-type: none"> 1. Check whether the node resources are sufficient. Log in to the CCE console, click Clusters, and select a target cluster to view its details. Click Nodes in the navigation pane on the left. On the Nodes tab page, check CPU requests and memory requests. 2. Restart the node. 3. Log in to the CCE console, click Clusters, and select a target cluster to view its details. Click Nodes in the navigation pane on the left. On the Nodes tab page, choose More > Reset in the Operation column.

Alarm Name	Alarm Source	Solution
High Memory Usage on the Node	BCS	<p>If the memory usage exceeds 80%, the possible causes are as follows:</p> <ol style="list-style-type: none"> 1. There are too many transaction requests in a short time. 2. The memory capacity of the node where the container is located cannot meet what is required by the instance specifications. <p>Do as follows:</p> <ol style="list-style-type: none"> 1. Log in to the BCS console. In the navigation pane, click Instance Management. 2. Click an instance name to go to the instance details page. 3. On the BCS instance details page, click the Monitoring tab and then the Active tab. Record the value of name in the Resource Name column. <p>Figure 1-18 Checking the value of name of the peer</p>  <p>The screenshot shows a terminal window with the following text: <pre> clusterName=... clusterID=cfb2...00029 kind=Pod namespace=default name=ord...52ca-0 uid=9f...320b80 </pre> The 'name=' line is highlighted with a red box. </p> <ol style="list-style-type: none"> 4. Go to the CCE console and locate the cluster where the abnormal node is. Click Nodes and click the node name to go to the ECS console. 5. Stop the ECS, and then choose More > Modify Specifications. Select a new flavor with desired memory.

Alarm Name	Alarm Source	Solution
Excessive memory usage	BCS	<p>If the memory usage exceeds 90%, the possible causes are as follows:</p> <ol style="list-style-type: none"> 1. There are too many transaction requests in a short time. 2. The memory capacity of the node where the container is located cannot meet what is required by the instance specifications. <p>Do as follows:</p> <ol style="list-style-type: none"> 1. Log in to the BCS console. In the navigation pane, click Instance Management. 2. Click an instance name to go to the instance details page. 3. On the BCS instance details page, click the Monitoring tab and then the Active tab. Record the value of name in the Resource Name column. <p>Figure 1-19 Checking the value of name</p>  <ol style="list-style-type: none"> 4. Go to the CCE console and locate the cluster where the abnormal node is. Click Nodes and click the node name to go to the ECS console. 5. Stop the ECS, and then choose More > Modify Specifications. Select a new flavor with desired memory. <p>Figure 1-20 Modifying specifications</p> 

Viewing Alarms

- Step 1** Log in to the BCS console.
- Step 2** In the navigation pane, click **Instance Management** to view the basic information of a BCS instance, including the blockchain type, consensus mechanism, status, and creation time.
- Step 3** On an instance card, click the instance name.
- Step 4** Click the **Monitoring** tab to view alarms generated in BCS and CCE. In the upper right corner, you can filter alarms generated in the last 30 minutes, 1 hour, or 1 day, or search for a specified alarm.
- Step 5** Click an alarm to view its details. Alarm sources include BCS and CCE. For details about how to handle alarms, see [Table 1-9](#).

----End

1.4.3.3 Setting Web Disk Space Alarms

Introduction

BCS is connected to AOM. AOM is a one-stop platform for technical support to monitor the application and resource operating state in real time. By analyzing metrics, alarms, and logs, you can quickly locate root causes to ensure smooth running of services.

The following describes how to use AOM to monitor the disk status (file storage) of a BCS instance. After receiving an alarming notification indicating that the disk space is insufficient, technical support needs to expand the disk capacity to prevent services from becoming abnormal.

Setting Alarms

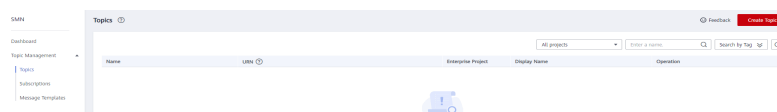
When technical support needs to check the web disk metrics, they can use the AOM service to set alarm rules for the disk metrics. If a metric exceeds the threshold, the system automatically sends an alarming SMS message or email.

- Step 1** Log in to the SMN console, create a topic and add subscription.

If you need to obtain resource change information in real time, create a topic and add subscribers to this topic. In this way, the email addresses or mobile numbers of recipients are noted by the system. When establishing rules, you can select the relevant recipient.

1. Create a topic.

Figure 1-21 Creating a topic



2. Select **APM** for **Services that can publish messages to this topic**. Otherwise, notifications cannot be sent.

Figure 1-22 Configuring a topic policy

Configure Topic Policy

Topic Name test001

Policy **Basic**

Users who can publish messages to this topic

Topic creator

All users

Specified user accounts

Enter one or more account IDs or URNs, each on a separate line.

[Learn how to obtain an account ID.](#)

Services that can publish messages to this topic

CAD OBS DWS VOD MPC LIVE

Moderation APM CloudVR CloudVR_live CIE

OK Cancel

3. Add subscription to the topic.

Figure 1-23 Adding a subscription task

Add Subscription

Topic Name test001

* Protocol SMS

* Endpoint ?

Endpoints	Description
<input type="text"/>	<input type="text"/>

[+ Add Endpoint](#)

[Batch Add Endpoints](#)

OK Cancel

Step 2 Go to the AOM console to create alarm rules.

1. In the navigation pane, choose **Alarm Center > Alarm Rules**. Then, click **Create Alarm Rule**.
2. Set basic information such as the rule name and description.
3. Set **Rule Type** to **Threshold alarm**, set **Monitored Object** and **Alarm Condition**, and click **Create Now**. For details, see [Creating a Threshold Rule](#).

----End

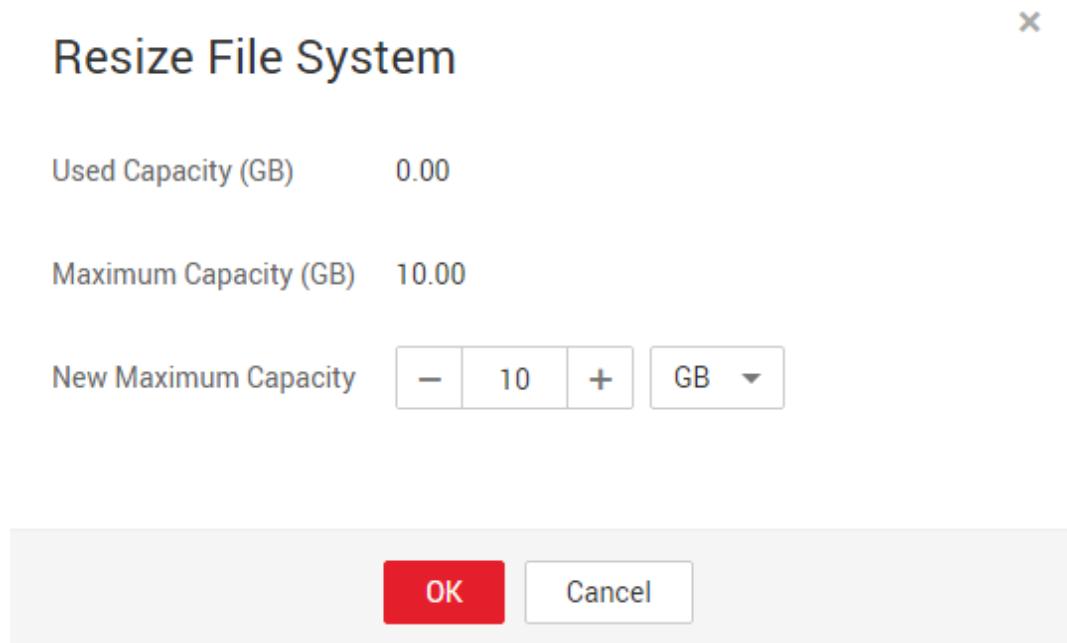
Handling Alarms

After receiving an alarming notification indicating that the disk space is insufficient, technical support needs to expand the disk capacity to prevent services from becoming abnormal.

Step 1 Choose **Service List > Storage > Scalable File Service** on the console.

- Step 2** In the SFS file system list, locate the file system used for the cluster where the BCS instance is deployed.
- Step 3** Click **Resize** in the **Operation** column.
- Step 4** Set **New Maximum Capacity**, and click **OK**.

Figure 1-24 Resizing the file system



----End

1.4.3.4 Disk Metrics

After metric thresholds and alarming criteria related to disk usage are configured, alarming short messages or emails can be sent to technical support. In this way, technical support can detect and handle service exceptions in a timely manner to reduce the loss caused by exceptions. The following table lists the metrics related to disks used for BCS services.

Table 1-10 Node metrics

Metrics	Description	Meaning	Value Range	Unit
diskAvailableCapacity	Available disk space	Disk space that is not used	≥ 0	MB
diskCapacity	Disk capacity	Total disk capacity	≥ 0	MB
diskReadRate	Disk read rate	Data volume read from the disk per second	≥ 0	KB/s

Metrics	Description	Meaning	Value Range	Unit
diskRWStatus	Disk read/write status	Read/write status of the disk on a node	0 (read and write) and 1 (read-only).	None
diskUsedRate	Disk usage	Percentage of the used disk space to the total disk space	≥ 0	Percentage
diskWriteRate	Disk write rate	Data volume written into the disk per second	≥ 0	KB/s

Disk metrics can be calculated on the following basis.

Table 1-11 Metric measurement bases

Basis	Description
clusterId	Cluster ID
clusterName	Cluster name
hostID	Node ID
namespace	Cluster namespace
nodeIP	IP addresses of a node
nodeName	Node name

1.4.3.5 Viewing O&M Logs

Introduction

If an exception occurs when you use a BCS instance, view the O&M logs to analyze and locate the fault for quick rectification. This section describes how to view the O&M logs of each BCS instance node in the CCE cluster on the frontend GUI and backend virtual machines (VMs).

Table 1-12 BCS instance logs

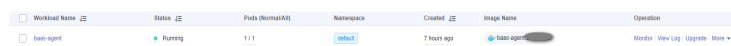
Component	Description	Log Path
baas-agent	Blockchain management run log	/var/paas/sys/log/baas-agent/baas-agent.log /var/paas/sys/log/baas-agent/audit.log
peer	Peer run log	/var/paas/sys/log/baas-service/peer/audit.peer-*****-*.log /var/paas/sys/log/baas-service/peer/peer-*****-*.trace
orderer	Orderer run log	/var/paas/sys/log/baas-service/orderer/audit.orderer-*****-*.log /var/paas/sys/log/baas-service/orderer/orderer-*****-*-start.trace /var/paas/sys/log/baas-service/orderer/orderer-*****-*.trace

Viewing Logs on the Frontend GUI

Step 1 View and record the node name on the **Workloads** page of the CCE console.

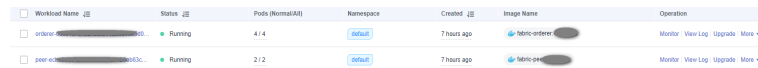
1. Choose **Workloads > Deployments**, click the cluster where the BCS instance is deployed. View and record the name of the baas-agent node, for example, baas-agent.

Figure 1-25 Checking baas-agent node name



2. Choose **Workloads > StatefulSets**, click the cluster where the BCS instance is deployed. View and record the orderer and peer node names, for example, peer-xx.

Figure 1-26 Checking peer and orderer nodes



Step 2 Go to the AOM console to view logs.

1. In the navigation pane on the left of the AOM console, choose **Log > Log Files**, and select the cluster where the BCS instance is located.
2. Select a recorded node name, and click **View** in the **Operation** column to view the node logs.
3. Click **Enable Real-Time Viewing**. Then, you can view O&M logs of the node in real time.

----End

Viewing O&M Logs on a Backend VM

Step 1 On the CCE console, view and record the node name on the **Workloads** page. For details, see [Viewing Logs on the Frontend GUI](#).

Step 2 On the **Instance Management** page of the BCS console, locate the instance and choose **More > Change Access Address** to view the access address.

Figure 1-27 Changing the blockchain network access address

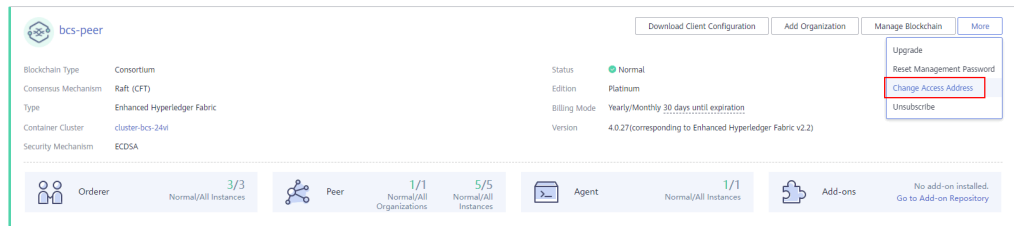
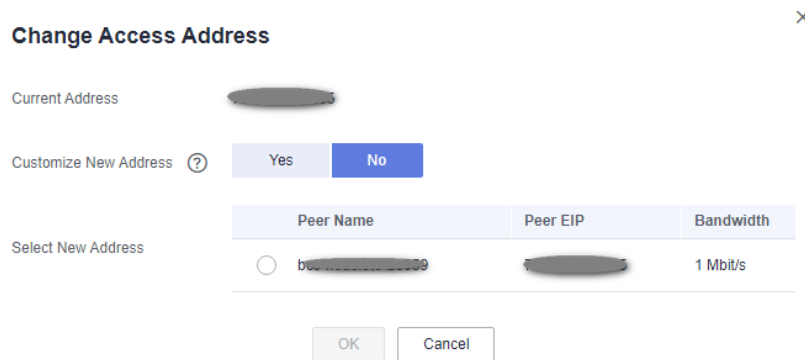


Figure 1-28 Viewing the access address

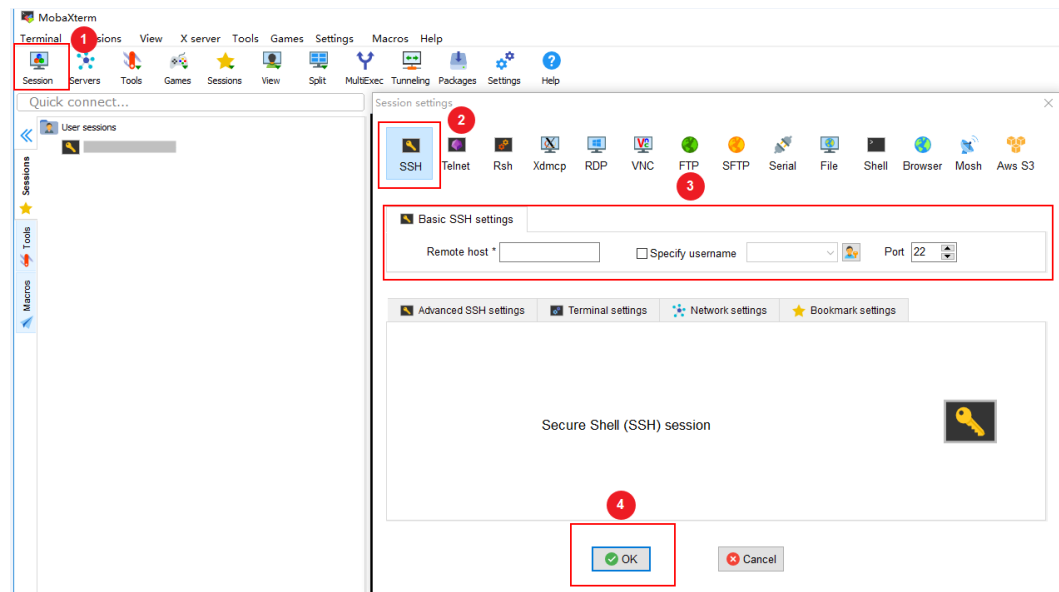


NOTE

The node where the BCS instance is deployed must be bound with an EIP.

Step 3 Log in to the VM corresponding to the access address, and view the O&M logs.

Figure 1-29 Logging to the VM



Enter the VM address (the access address obtained in [Step 2](#)) for **Remote host**, and enter the VM username for **Specify username**.

1. Check baas-agent node logs.
 - a. Run the following command to query the baas-agent node ID:
docker ps|grep baas-agent

Figure 1-30 Checking the baas-agent node ID

```
[root@log-1t-44243 ~]# docker ps |grep baas-agent
0b2911c07a7b    db11e1933c3d    "/bin/bash -c 'exp..." 2 days ago    Up 2 day
s
1efddfa0d7bd    cfe-pause:11.23.1    k8s_POD_baas-agent-9885db668-mxvm4_default_933fee36-b356-11e9-b003-fa163ec54113_0    "/pause"    2 days ago    Up 2 day
s
k8s_POD_baas-agent-9885db668-mxvm4_default_933fee36-b356-11e9-b003-fa163ec54113_0
```

- b. Run the following command to query the baas-agent node logs:
docker logs ID -f

Figure 1-31 Checking the baas-agent node logs

```
[root@log-1t-44243 ~]# docker ps |grep baas-agent
0b2911c07a7b    db11e1933c3d    "/bin/bash -c 'exp..." 2 days ago    Up 2 day
s
1efddfa0d7bd    cfe-pause:11.23.1    k8s_POD_baas-agent-9885db668-mxvm4_default_933fee36-b356-11e9-b003-fa163ec54113_0    "/pause"    2 days ago    Up 2 day
s
k8s_POD_baas-agent-9885db668-mxvm4_default_933fee36-b356-11e9-b003-fa163ec54113_0
[root@log-1t-44243 ~]# docker logs -f 0b2911c07a7b
The make env.sh user is root, bcsid is 18636745-821a-cf15-5abd-152ee3b7115b
chown: changing ownership of '/opt/gopath/src/github.com/hyperledger/fabric/orderer/crypto/ordererOrganizations/orderer-89c01f73e87fd64b084f2716aa050925c20860cb-admin/admin/.data': Read-only file system
chown: changing ownership of '/opt/gopath/src/github.com/hyperledger/fabric/orderer/crypto/ordererOrganizations/orderer-89c01f73e87fd64b084f2716aa050925c20860cb-admin/admin/tls': Read-only file system
chown: changing ownership of '/opt/gopath/src/github.com/hyperledger/fabric/orderer/crypto/ordererOrganizations/orderer-89c01f73e87fd64b084f2716aa050925c20860cb-admin/admin/msp': Read-only file system
chown: changing ownership of '/opt/gopath/src/github.com/hyperledger/fabric/orderer/crypto/ordererOrganizations/orderer-89c01f73e87fd64b084f2716aa050925c20860cb-admin/admin/...' 2019-07-31 05:46:43.468296142711s/server-key': Read-only file system
```

2. Check the logs of a peer node.
 - a. Run the following command to query the peer node ID:
docker ps|grep peer

Figure 1-32 Checking the peer ID

```
[root@master1-5801 ~]# docker ps |grep peer
c8c7983887fa    ka1a0cf1411    "/bin/bash -c 'expor..." 3 weeks ago    Up 3 weeks    k8s_peer_58aea736051a6156347ae3bc12112980298_1_default_850a1c5e-a84a-4161-8bc2-c307394
892f2f0    ka1a0cf1411    "/bin/bash -c 'expor..." 3 weeks ago    Up 3 weeks    k8s_peer_95469f08446623869447b7022af5334ab5ee_1_default_b3a1201f-9068-4c43-a46a-7145cd2
c8e1c9b73a    ka1a0cf1411    "/bin/bash -c 'expor..." 3 weeks ago    Up 3 weeks    k8s_peer_95469f08446623869447b7022af5334ab5ee_1_default_b3a1201f-9068-4c43-a46a-7145cd2
8095f8    cce-pause:3.1    "/pause"    3 weeks ago    Up 3 weeks    k8s_POD_peer_58aea736051a6156347ae3bc12112980298_1_default_850a1c5e-a84a-4161-8bc2-c307394
```

- b. Run the following command to query the peer node logs:
docker logs -f ID

Figure 1-33 Checking the peer logs

```
[root@master01-54891 ~]# docker logs -f 58c7683b87a
chown: changing ownership of '/etc/hyperledger/temp_fabriccoreconfigmap/core.yaml': Read-only file system
chown: changing ownership of '/etc/hyperledger/temp_fabriccoreconfigmap/.2021_02_02_09_34_59_413905497/core.yaml': Read-only file system
chown: changing ownership of '/etc/hyperledger/temp_fabriccoreconfigmap/.2021_02_02_09_34_59_413905497': Read-only file system
chown: changing ownership of '/etc/hyperledger/temp_fabriccoreconfigmap/.data': Read-only file system
chown: changing ownership of '/etc/hyperledger/impmapping/impmapping.json': Read-only file system
chown: changing ownership of '/etc/hyperledger/impmapping/.data': Read-only file system
chown: changing ownership of '/etc/hyperledger/impmapping/.2021_02_02_09_34_59_565881316/impmapping.json': Read-only file system
chown: changing ownership of '/etc/hyperledger/impmapping/.2021_02_02_09_34_59_565881316': Read-only file system
chown: changing ownership of '/etc/hyperledger/impmapping': Read-only file system
chown: changing ownership of '/etc/hyperledger/temp_fabriccoreconfigmap/core.yaml': Read-only file system
chown: changing ownership of '/etc/hyperledger/temp_fabriccoreconfigmap/.2021_02_02_09_34_59_413905497/core.yaml': Read-only file system
chown: changing ownership of '/etc/hyperledger/temp_fabriccoreconfigmap/.2021_02_02_09_34_59_413905497': Read-only file system
chown: changing ownership of '/etc/hyperledger/temp_fabriccoreconfigmap/.data': Read-only file system
chown: changing ownership of '/etc/hyperledger/impmapping/.data': Read-only file system
chown: changing ownership of '/etc/hyperledger/impmapping/impmapping.json': Read-only file system
chown: changing ownership of '/etc/hyperledger/impmapping/.2021_02_02_09_34_59_565881316/impmapping.json': Read-only file system
chown: changing ownership of '/etc/hyperledger/impmapping/.2021_02_02_09_34_59_565881316': Read-only file system
chown: changing ownership of '/etc/hyperledger/impmapping': Read-only file system
++ hostname
+ H05NWE-peer-50aea7369551a6c15634c7ae3bc12212980298-1
+ sed -i '/fileSystemPath: V:/var/hyperledger/production/c/ fileSystemPath: /home/paas/evs/baas/1a518637-0a63-6e67-253b-5846420c45fc/peer-50aea7369551a6c15634c7ae3bc12212980298-1/production' core.yaml
+ sed -i '/id: /dev/c/ id: peer-50aea7369551a6c15634c7ae3bc12212980298-1' core.yaml
+ sed -i '/localMspId: EF4417A/ localMspId: 50aea7369551a6c15634c7ae3bc12212980298SP' core.yaml
++ 'l' -z 32623 'l'
++ sed -i '/address: 0.0.0.0:7051/c/ address: peer-50aea7369551a6c15634c7ae3bc12212980298-1.peer-50aea7369551a6c15634c7ae3bc12212980298.default.svc.cluster.local:32624' core.yaml
++ /bin/ip route get 1.2.3.4
++ head -1
++ tr -s ' '
++ cut -d ' ' -f7
+ localIP=0.0.0.207
```

3. Check the logs of an orderer node.

- a. Run the following command to query the orderer ID:
docker ps|grep orderer

Figure 1-34 Checking the orderer ID

```
[root@mf-test-60988 ~]# docker ps|grep orderer
77daf8baf444      89f4ba19145e      /bin/bash -c 'H05...'   2 days ago        Up 2 days
orderer_orderer-6f8ddd01fb38c8dff68ecdcd9bb5d97e27df1ecf-0 default_B167d0d7-b750-11e9-bdf7-fal63e730475_0
```

- b. Run the following command to query the orderer logs:
docker logs -f ID

Figure 1-35 Checking the orderer logs

```
[root@mf-test-60988 ~]# docker logs 77daf8baf444
chown: changing ownership of '/etc/hyperledger/configtx/.data': Read-only file system
chown: changing ownership of '/etc/hyperledger/configtx/genesis.block': Read-only file system
chown: changing ownership of '/etc/hyperledger/configtx/.2019_08_05_07_13_20_605881597/genesis.block': Read-only file system
chown: changing ownership of '/etc/hyperledger/configtx/.2019_08_05_07_13_20_605881597': Read-only file system
chown: changing ownership of '/etc/hyperledger/configtx': Read-only file system
chown: changing ownership of '/etc/hyperledger/temp_ordererconfigmap/.data': Read-only file system
chown: changing ownership of '/etc/hyperledger/temp_ordererconfigmap/orderer.yaml': Read-only file system
chown: changing ownership of '/etc/hyperledger/temp_ordererconfigmap/.2019_08_05_07_13_20_296162454/orderer.yaml': Read-only file system
chown: changing ownership of '/etc/hyperledger/temp_ordererconfigmap/.2019_08_05_07_13_20_296162454': Read-only file system
chown: changing ownership of '/etc/hyperledger/configtx/.data': Read-only file system
chown: changing ownership of '/etc/hyperledger/configtx/genesis.block': Read-only file system
chown: changing ownership of '/etc/hyperledger/configtx/.2019_08_05_07_13_20_605881597/genesis.block': Read-only file system
chown: changing ownership of '/etc/hyperledger/configtx/.2019_08_05_07_13_20_605881597': Read-only file system
chown: changing ownership of '/etc/hyperledger/temp_ordererconfigmap/.data': Read-only file system
chown: changing ownership of '/etc/hyperledger/temp_ordererconfigmap/orderer.yaml': Read-only file system
chown: changing ownership of '/etc/hyperledger/temp_ordererconfigmap/.2019_08_05_07_13_20_296162454/orderer.yaml': Read-only file system
chown: changing ownership of '/etc/hyperledger/temp_ordererconfigmap/.2019_08_05_07_13_20_296162454': Read-only file system
chown: changing ownership of '/etc/hyperledger/temp_ordererconfigmap': Read-only file system
```

----End

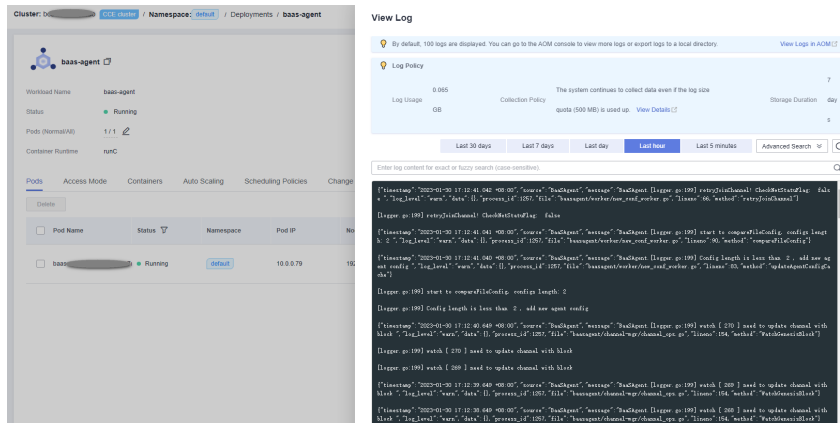
1.4.3.6 Viewing Chaincode Debug Logs

You can view chaincode debug logs to analyze and locate problems. This section describes how to view chaincode debug logs on the CCE console.

Procedure

- Step 1** Log in to the CCE console.
- Step 2** Go to the **Clusters** page, select the cluster where the BCS instance is deployed, and choose **Workloads > Deployments**.
- Step 3** Click the workload whose name starts with **baas-agent**.
- Step 4** Click **Logs** in the upper right corner to view the logs of the chaincode container. To view more logs or export logs, go to the AOM console.

Figure 1-36 Viewing the chaincode pod logs



----End

1.5 Channel Management

Peers communicate through channels. You can create channels and add organizations and peers to them.

Creating a Channel

Step 1 Log in to the BCS console.

Step 2 Click **Channel Management** in the navigation pane on the left. Click **Create Channel** in the upper right corner of the page.

NOTE

- The maximum number of channels for each instance is 2 for the professional edition and 4 for the enterprise edition.
- In a consortium, channels cannot be created for invitees' instances.

Step 3 Select an instance, enter a channel name and description, and click **OK**.

----End

Managing Channel Organizations and Peers

 NOTE

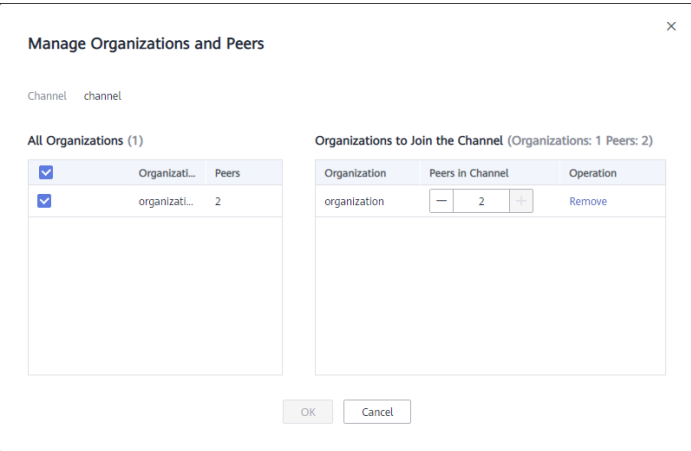
This operation is not supported for invitees.

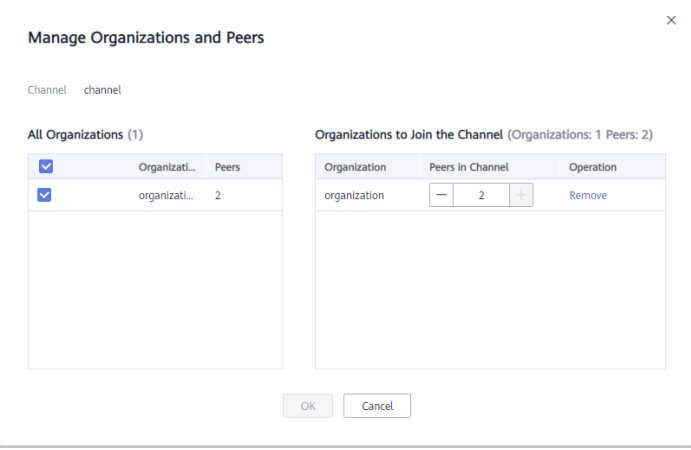
- Step 1** After the channel is created, click **Manage Organization and Peer** in the **Operation** column of the channel list.
 - Step 2** Select organizations and specify the number of peers you want to add to the channel.
 - Step 3** Click **OK**.
- End

Other Operations

Table 1-13 Other operations

Operation	Description
Searching for a channel	Enter a channel name in the search box at the upper right corner of the Channel Management page to search for the channel.
Querying channels	A channel list is displayed on the Channel Management page. You can view the channel name, instance name, and the channel nodes.
Viewing a peer	Click View Peer in the Operation column of the channel list to view peer information by organization, including the Membership Service Provider (MSP) ID, peer details (name, IP address, port, and domain), and whether the peer has been added to the channel.

Operation	Description
<p>Removing peers in an organization from a channel</p>	<p>Click Manage Organization and Peer in the Operation column of the channel list. Decrease the value for Peers in Channel under Organizations to Join the Channel, then click OK to remove peers from the channel.</p> <p>Figure 1-37 Managing organizations and peers</p>  <p>NOTE Keep at least 1 peer in the channel. To remove an organization from the channel, you can manually set the number of peers in the channel to 0.</p>

Operation	Description
<p>Removing organizations from a channel</p>	<p>Click Manage Organization and Peer in the Operation column of the channel list. Under Organizations to Join the Channel, click Remove in the row that contains the target organization, then click OK to remove the organization from the channel.</p> <p>Figure 1-38 Removing organizations from a channel</p>  <p>NOTE If an organization is listed in the endorsement policy of a chaincode, update the endorsement policy after the organization is removed from the channel. Otherwise, transactions will fail. For details, see Chaincode Management.</p>
<p>Deleting a channel</p>	<p>Click Delete in the Operation column, then click OK.</p> <p>NOTE Clear all organization nodes in a channel before you delete it.</p>

1.6 Blockchain Management

1.6.1 Chaincode Management

You can install, instantiate, and update chaincodes on the web. You can also check the Golang chaincode security during installation and update.

 **NOTE**

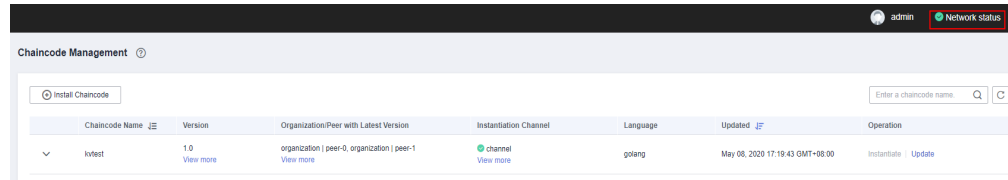
A maximum of 500 chaincodes can be installed. The total specification of the CCE clusters must be at least 500 vCPUs and 1000 GB memory.

Note

1. Before installing a chaincode, compress the chaincode file into a .zip package.

2. If the **Network Status** displayed in the upper right corner of the **Blockchain Management** page is abnormal, do not perform any operations. Wait for a few minutes until the network is recovered.

Figure 1-39 Normal network status



Installing a Chaincode

- Step 1** Log in to the **Blockchain Management** console.
- Step 2** On the **Chaincode Management** page, click **Install Chaincode**.
- Step 3** Specify the chaincode name, version, and other parameters by referring to [Table 1-14](#).

Figure 1-40 Installing a chaincode

Install Chaincode

* Chaincode Name

* Chaincode Version

Ledger Storage

Select All Peers

Organization & Peer

Language

Chaincode File

Chaincode Description

0/500

Code Security Check

Table 1-14 Chaincode parameters

Parameter	Description
Chaincode Name	Chaincode name, which can contain 6 to 25 including lowercase letters and digits, and must start with a letter.
Chaincode Version	Chaincode version.
Ledger Storage	Default option: File database (goleveldb) .
Select All Peers	Check the box to select all peers.
Organization & Peer	Manually select organizations and peers.
Language	Golang, Node.js, and Java are supported.
Chaincode File	Add a chaincode file.
Chaincode Description	Enter a description.
Code Security Check	This option is displayed only when the chaincode language is Golang. Enable this option to check code security.

Step 4 Click **Install**.

Step 5 Click  next to a chaincode name to view the details.

Step 6 Click **Download** in the **Operation** column to view the check result. (The following example is for reference only.)

 **NOTE**

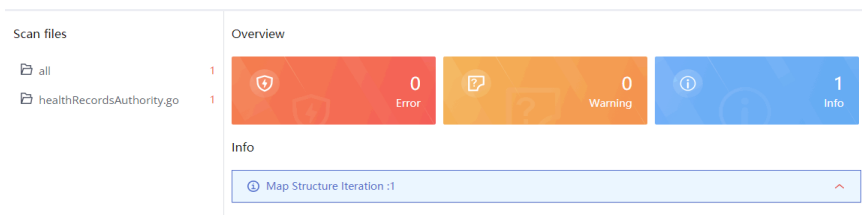
If **Code Security Check** is not enabled, no check report will be generated, and the **Download** button will not be displayed.

Figure 1-41 Downloading the check report

Chaincode Version	SHA-256 Hash	Description	Installed	Operation
1.0	3455d016a31349749ff575c7b00c131782e130832a0a1afe61f...		Nov 15, 2021 10:26:23 GMT+08:00	Download Delete

- Decompress the package and open the HTML file to view the check result details. There are three types of issues: error, warning, and info. Error-level issues must be resolved. Otherwise, the chaincode functions will be affected. Warning-level issues can be handled by reconstructing the code. Info-level issues can be handled selectively as required.

Figure 1-42 Scanned files



2. For example, there is an info-level issue in the proceeding figure. You can click the issue to view its details, including a brief description, wrong example, scanning details, modification advice, and revision example.

 **NOTE**

Modify the code based on the chaincode check result and update the chaincode or install it again.

----End

Instantiating a Chaincode

After a chaincode is installed, it must be instantiated on the channel so that the peers can interact with each other using the distributed ledger and the chaincode container. Before instantiating a chaincode, add the peers to the channel. Otherwise, the chaincode cannot be instantiated.

 **NOTE**

- The memory usage of instantiated containers varies depending on the chaincode language. On each peer, a Go chaincode container takes up 10 MB for running, and a Java chaincode takes up 110 MB. For example, if 100 Java chaincodes need to be instantiated, a 16 vCPUs and 32 GB CCE node is preferred.
- Before instantiating a chaincode, compress the chaincode file into a .zip package.

Step 1 Click **Instantiate** in the **Operation** column of the chaincode list.

Step 2 Specify the channel for instantiation, chaincode version, endorsement policy, endorsing organizations, and chaincode parameters.

 **NOTE**

Endorsement is a process in which organizations perform a chaincode transaction and return a proposal response to a client application. An endorsement policy specifies how many members of different organizations on a channel are required to execute and validate a transaction based on the specified smart contract to make the transaction valid. Therefore, an endorsement policy defines the organization peers that must "endorse" (that is, approve of) the execution of a proposal.

- **Endorsement from any of the following organizations:** A transaction is valid as long as any one of the organizations endorses it.
- **Endorsement from all of the following organizations:** A transaction is valid only when all organizations endorse it.

Figure 1-43 Instantiating a chaincode

Instantiate Chaincode [X]

Chaincode Name: kvtest001

Channel: channel

Chaincode Version: 2.0

* Initialization Function: Enter a function, for example, init().
Chaincode function that will be invoked

Chaincode Parameters: For example, a,200,b,250
Enter the parameters of the initialization function init(). Separate multiple parameters with commas.

Endorsement Policy: Endorsement from any of the following organizations
 Endorsements from all of the following organizations

Endorsing Organizations: byl-ief-002, byl-ief-003

Privacy Protection Configuration: No Yes

Please input JSON data.
For example:


```
{
  "name": "collectionPrivateDetails",
  "policy": "OR('Org1MSP.member', 'Org2MSP.member')",
  "requiredPeerCount": 0,
  "maxPeerCount": 3,
  "blockToLive": 0,
  "memberOnlyRead": true
}
```

 0/5,000

[Instantiate] [Cancel]

Step 3 Enter the private data (JSON format) to be protected in the text box below **Privacy Protection**.

If you want to restrict data in a shared channel to certain specified members, use the privacy protection function. Skip this step if privacy protection is not required for your chaincode.

Configure privacy protection by referring to the example and the following parameter description:

- **name:** Name of the collection of private data, for example, collectionPrivateDetails.

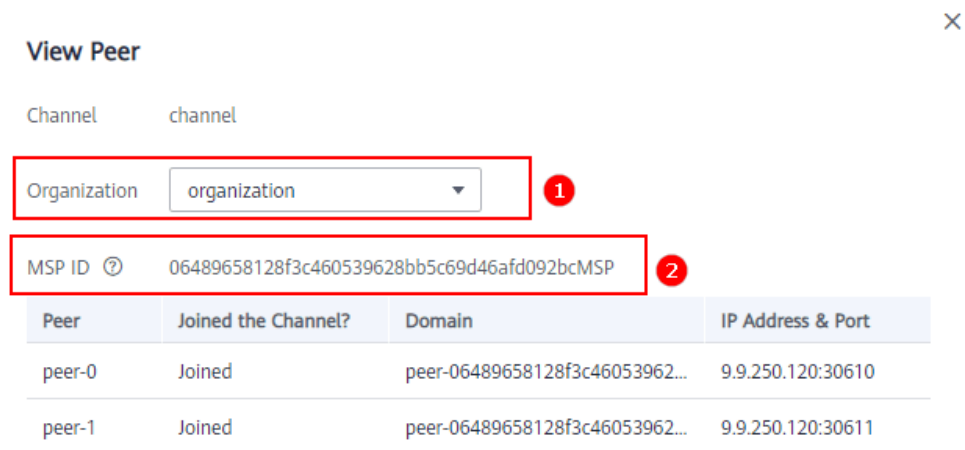
In a chaincode, if you want to write data to the collection of private data, ensure that the collection name is the same as that defined here.

```
stub.PutPrivateData("collectionPrivateDetails", key, value)
```

- **policy:** Peers allowed to access the data in the collection. In the example, only peers of organizations Org1 and Org2 are allowed to obtain the data in the collection.

Click **View Peer** on the **Channel Management** page, and obtain the MSP IDs of the two organizations, as shown in the following figure.

Figure 1-44 Checking the MSP



- **requiredPeerCount:** Number of endorsing peers to which the private data can be disseminated. In the example, value **0** indicates that there is no endorsing peer.
- **maxPeerCount:** Maximum number of orderers, which is **3** in the example. Multiple orderers can be used for data redundancy. If one orderer is unavailable, other orderers can respond to requests for obtaining the private data.
- **blockToLive:** Maximum number of blocks that the private data can live for. If the number of blocks exceeds the threshold, the private data will be cleared. To keep private data indefinitely, set this parameter to **0**.
- **memberOnlyRead:** The default value is **true**. The access policy set in **policy** takes effect only when **memberOnlyRead** is set to **true**.

Example of privacy protection configuration (JSON):

```
[
  {
    "name": "collectionPrivateDetails",
    "policy": "OR('<Org1MSP>.member','<Org2MSP>.member')",
    "requiredPeerCount": 0,
    "maxPeerCount": 3,
    "blockToLive": 0,
    "memberOnlyRead": true
  }
]
```

This configuration indicates that the chaincode uses a private data space called **collectionPrivateDetails**. Only the peers of organizations Org1 and Org2 have access to the data in this space.

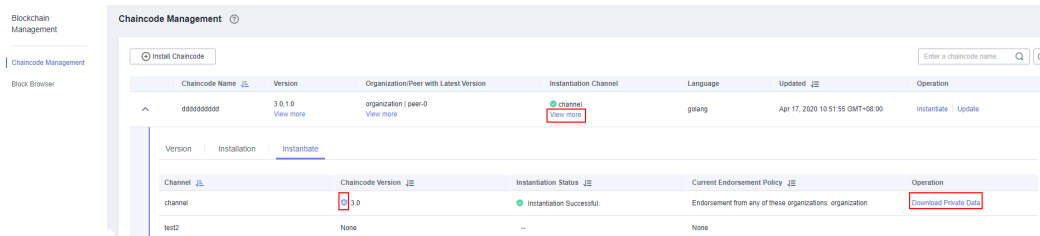
NOTE

The values of **name** and **blockToLive** cannot be modified during subsequent chaincode upgrade. For more information, see [Using Private Data in Fabric](#).

Step 4 Click **Instantiate**.

If privacy protection is configured, you can click **View More** after the chaincode is successfully instantiated to download the private data and check whether the privacy protection settings are correct.

Figure 1-45 Downloading private data




If chaincode instantiation fails, refer to [Chaincode Instantiation Error Codes](#) to determine the cause.

----End

Updating a Chaincode

If your chaincode is updated, install and instantiate it again to meet new business requirements.

- Step 1** Click **Update** in the **Operation** column of the chaincode list.
- Step 2** Specify the chaincode version, select peers, add a chaincode file, and click **Update**.
- Step 3** Instantiate the updated chaincode. For details, see [Instantiating a Chaincode](#).
- Step 4** (Optional) Click  in front of the chaincode name. You can see details about this chaincode, including versions, and installation and instantiation information.

----End

Chaincode Instantiation Error Codes

Chaincode instantiation may fail due to various causes. When confronted with an instantiation failure, you can refer to the following table to determine the cause.

Table 1-15 Error codes

Error Code	Message
6001	Instantiation timed out.
6999	Unknown error.
6701	Client failed to connect to a peer.
6703	Endorsement signature failed verification.
6704	Failed to pull the ccenv image during chaincode compilation.
6705	Chaincode compilation failed.

Error Code	Message
6707	Failed to build a chaincode image.
6708	Failed to create a chaincode container.
6709	Failed to register the chaincode container.
6710	Client failed to connect to an orderer.
6712	Transaction recording in distributed ledgers failed.
6713	Request error determined by the orderer.
6714	The endorsement policy failed the verification.
6715	Instantiation failed because instantiation of another chaincode has already been started.
6716	Error detected in the init() function parameters.
6717	Error detected in the invoke() function parameters.
6720	Failed to create a chaincode certificate.
6721	Chaincode container startup timed out.
6722	Transaction timed out because init() execution abnormally terminates after startup of the chaincode container.
6723	A chaincode with the same schema has already been instantiated on this channel.
6725	The signature set does not satisfy the endorsement policy.
6726	The instantiation policy failed the verification. Select a peer of an organization that exists in the channel before chaincode instantiation to upgrade the chaincode.
6901	Instantiation failed. The chaincode to be instantiated must contain all the tables in the previously instantiated chaincode.
6902	Instantiation failed. The chaincode to be instantiated must contain all the fields in the previously instantiated chaincode.
6903	Instantiation failed. The chaincode to be instantiated must not contain any changes to the field attributes included in the previously instantiated chaincode.
6904	The schema file of the instantiated chaincode does not exist.
6905	Failed to resolve the schema file.
6906	Insufficient disk space.

1.6.2 Block Browser

You can query blockchain information required for maintenance, including the block quantity, transaction quantity, block details, transaction details, performance, and peer statuses.

NOTE

To access blockchain browsers, set the blockchain network access address to a private address of the cluster and ensure that the network between the user and cluster is connected. If you set the access address to an EIP bound to the cluster, unbind the EIP when you are not using the blockchain browser.

Procedure

Step 1 Open the block browser page.

1. Log in to the BCS console.
2. Click **Manage Blockchain** on an instance card.
3. Enter the username and password and click **Log In**.
4. Click **Block Browser** in the navigation pane.

Step 2 Select a channel from the **Channel** drop-down list box. Real-time data is displayed in the lower part of the page.

Step 3 You can view the following data in the block browser.

Table 1-16 Blockchain data

Item	Description
Peers	Number of peers in the selected channel
Chaincodes	Number of installed chaincodes
Blocks	Number of generated blocks
Transactions	Number of transactions that have been performed
Block details	Click the Block List tab to view the block hash and data hash of recent blocks.
Transaction list	<ul style="list-style-type: none">• Click the Transaction List tab to view the information about recent transactions such as the transaction IDs, creators' MSPs, and creation time.• Click View Details in the Operation column of the transaction list to view more details about the transaction.

Item	Description
Performance analysis	<p>The line charts show the trends of performance data, helping you know the performance status.</p> <ul style="list-style-type: none">• Block performance: Click Block to view changes in the block quantity. Move the pointer along the curve to view the number of blocks at different time points.• Transaction performance: Click Transaction to view changes in the transaction quantity. Move the pointer along the curve to view the number of transactions at different time points. <p>NOTE You can select a time granularity (hours or minutes) in the upper right corner of the chart.</p>
Transaction quantity of organizations	<p>The pie chart shows the percentage of each organization's transactions.</p> <p>NOTE Move the pointer on the pie chart to view the transaction quantity and percentage of each organization.</p>
Peer statuses	<p>You can view the running statuses of all peers in the selected channel to detect exceptions of peers in time.</p>

----End

1.7 Downloading SDK Configurations and Certificates

BCS supports chaincode functions such as execution and query. Before developing an application, download the certificates and SDK configuration. The SDKs can use the configuration file to easily access the blockchain network and complete transactions. You do not need to manually configure the SDKs.

Prerequisites

Before downloading the SDK configuration, ensure that the chaincode has been installed and instantiated.

Downloading SDK Configurations and Certificates

The SDK configuration, certificates, and application must be used together. The SDK configuration file contains chaincode and certificate path information. Specify the chaincode name and the storage path of the downloaded certificate on the application executor when downloading the SDK configurations. If the certificate path changes, you must manually change all certificate paths in the SDK configuration file.

BCS supports three types of certificates: administrator certificate, user certificate, and CA certificate. The administrator certificate is required to create, join, and update a channel, and install, instantiate, update, and delete a chaincode. For transactions and query, you are advised to use the user certificate. Download the certificates on the **Instance Management** page.

- An administrator certificate contains the organization's administrator permission certificate and private key and can be used to manage channels and contracts.
- A user certificate contains the organization's user permission certificate and private key and can be used for transactions and queries.
- A CA certificate is the root certificate of an organization. The CA public and private key pair can be used to issue lower-level certificates.

 **NOTE**

- The administrator certificate differs between an orderer and a peer. For management within a channel, use the administrator certificate for peers instead of that for orderers.
- Encrypt the private keys in the downloaded certificates for storage.

Step 1 Log in to the BCS console.

Step 2 In the navigation pane on the left, click **Instance Management**.

Step 3 Click **Download Client Configuration** on an instance card.

Step 4 Select configuration files to download.

- **SDK Configuration File:** Specify the member, chaincode name, certificate path as required.

Table 1-17 SDK file parameters

Parameter	Description
Chaincode Name	Set it as required. The chaincode name must be the same as the name specified during chaincode installation and instantiation.
Certificate Path	Final path for storing the certificate for application compilation. If the certificate path changes, you must manually change all certificate paths in the SDK configuration file.
Channel	Select a channel.
Member	Select peer organizations in the channel.

- An orderer certificate is used for interacting with the blockchain system. Encrypt the private keys in the downloaded certificates for storage.
- A peer certificate is used for performing management operations within a channel. Encrypt the private keys in the downloaded certificates for storage. Select a peer organization and the certificates to be downloaded.

Step 5 Click **Download**. Decompress the SDK and store the retrieved .yaml file. Decompress the downloaded certificate packages and store the files in an application directory for the application to access.

----End

1.8 Consortium Management

1.8.1 Forming a Consortium

After creating a consortium blockchain, you can invite tenants to join it. In addition, you can invite others through different channels to form a consortium blockchain.

NOTE

- Existing BCS instances of Fabric v1.1.0 can be upgraded to v1.4.0. BCS instances of Fabric v1.1.0 can no longer be created.
- BCS instances corresponding to Fabric v1.4.0 can be upgraded to the version corresponding to Fabric v2.2. If one member in a consortium blockchain has upgraded to Fabric v2.2, all consortium members must also upgrade to v2.2. Otherwise, transactions will fail. For details about upgrading the version, see [Step 3](#).
 - BCS v3.x.x corresponds to Hyperledger Fabric v1.4.0.
 - BCS v4.x.x corresponds to Hyperledger Fabric v2.2.
- For existing consortium blockchains of v1.1.0, an invitee can still create a blockchain of v1.1.0 and join the consortium.

Inviting a Tenant

Create a consortium blockchain to invite others to join the consortium.


Step 1 Log in to the BCS console.

Step 2 Click **Member Management** in the navigation pane on the left. Click **Invite Tenant** in the upper right corner of the page.

Step 3 In the **Invite Tenant** window, select your BCS instance and channel, and enter the invitee's name.


Figure 1-46 Inviting a tenant

Invite Tenant 

 Ensure that the account name is correct. You can check the account name on the [Basic Information](#) page.

Service Consortium Channel

* Invitee

 Add Tenant

Step 4 (Optional) Click **Add Tenant** to invite multiple tenants.

NOTE

A maximum of 40 tenants can be invited.

Step 5 Click **OK**. An invitation notification is sent to the invitee.

----End

Accepting/Declining an Invitation

When you are invited to join a consortium blockchain, you will receive a notification. You can either accept or decline it.

Step 1 Log in to the BCS console.

Step 2 Click **Notification Management** in the navigation pane on the left. On the **Notification Management** page, locate the notification and click **View Details** in the **Operation** column.

- To accept the invitation, select the organization that you want to add to the consortium, and then click **Accept**.
- To decline the invitation, click **Decline**.

NOTE

- An invitee can select an existing BCS instance from the drop-down list box or click **Create Instance** to create a new one.

An invitee can accept invitations sent by only one inviting party. To accept invitations from other inviting parties, the invitee must create new BCS instances.

If an invitee receives multiple invitations from multiple channels of an inviting party, the invitee can create a BCS instance using one of the channels, and use the same BCS instance to accept invitations from other channels.

- For details about how to create a BCS instance, see [Instance Deployment](#). To successfully join a consortium blockchain, certain parameters of your instance must have the same settings as the inviting party's BCS instance, such as the blockchain type, consensus mechanism, and security mechanism. Therefore, these parameters are dimmed on the instance configuration page and cannot be modified.

----End

1.8.2 Member Management

You can invite tenants to become blockchain consortium members, who can view invitations and topologies and delete invitations.

- To invite a tenant, click **Invite Tenant** in the upper right corner of the **Member Management** page. For details, see [Inviting a Tenant](#).
- To view an invitation, click **View Invitation** in the **Operation** column on the **Member Management** page.
- To delete an invitation, click **Delete Invitation** in the **Operation** column on the **Member Management** page. After you delete an invitation, it is withdrawn. This operation can be done only if the invitee has not accepted the invitation.
- To view the topology between consortium blockchain members, click **View Topology** in the **Operation** column on the **Member Management** page.

You can invite a tenant to join a channel to establish a consortium blockchain. Tenants cannot be invited to a private blockchain.

1.8.3 Notification Management

When another tenant invites you to join a consortium blockchain, you will receive an invitation notification. Then, you can view the invitation on the **Notification Management** page.

- To accept the invitation, click **View Details** in the **Operation** column of the notification list, select a BCS instance and organization, and click **Accept**.
- To decline the invitation, click **View Details** in the **Operation** column of the notification list, and click **Decline**.
- To delete a notification, click **Delete Notification** in the **Operation** column of the notification list
- To postpone the processing of an invitation, click **View Details** in the **Operation** column of the notification list, and click **Process Later**.

NOTE

- Click **Create Instance** and use the new BCS instance to join the channel.
- Notification statuses include:
 - **Unprocessed**: You have not processed the invitation notification. You can click **View Details** to accept or decline the invitation.
 - **Finished**: You have accepted the invitation to join the consortium blockchain.
 - **Canceled**: The inviting party has deleted the instance before you accept the invitation. You cannot join the consortium blockchain.
 - **Declined**: You have declined the invitation to join the consortium blockchain.
 - **Quit**: You have accepted the invitation and joined the consortium blockchain but later quit the consortium.
 - **Dismissed**: The inviting party has deleted the instance after you joined the consortium blockchain. As a result, the blockchain is dismissed.
 - **Frozen**: The inviting party's account is frozen.
 - **Upgraded**: An instance in the consortium blockchain has been upgraded after you join the blockchain.

1.9 Add-on Management

1.9.1 Add-on Overview

Add-ons allow you to extend the functionality of BCS instances as required. On the **Add-on Management** page, you can install add-ons and upgrade, uninstall, and view details about the installed add-ons. [Table 1-18](#) shows the add-ons.

Table 1-18 Add-ons

Name	Description	Restrictions
baas-restapi	<p>Supports access to the blockchain system by using RESTful APIs. Supports management capabilities such as generation, application, and issuance of distributed identities and verifiable credentials, as well as data release, authorization, sharing, decryption, and digital watermarking (only in CN North-Beijing4).</p> <p>NOTE This function is under OBT.</p>	<p>This add-on can be installed only if the BCS instance meets all of the following conditions:</p> <ul style="list-style-type: none"> Enhanced Hyperledger Fabric architecture Deployed in a CCE cluster v3.0.16 or later (corresponding to Hyperledger Fabric v1.4.0) or v4.0.5 or later (corresponding to Hyperledger Fabric v2.2) Endorsement is from any organization under the BCS instance Uses ECDSA for the security mechanism

Installing the baas-restapi Add-on

- Step 1** Log in to the BCS console.
- Step 2** Click **Add-on Management** in the navigation pane on the left.
- Step 3** On the **Add-on Repository** tab page, click **Install** on the card of the **baas-restapi** add-on.
- Step 4** Set the parameters by referring to [Table 1-19](#).

Table 1-19 Parameters

Parameter	Description	Example Setting
Add-on	Add-on name.	baas-restapi
Version	Add-on version.	3.0.45
Instance	Select a BCS instance.	bcs-6zbgus
Enable DID API	<p>Allows you to manage DIDs, generate, apply, issue verifiable credentials.</p> <p>Determine whether to enable the distributed identity APIs based on the service requirements.</p>	-

Parameter	Description	Example Setting
Enable APIs for Trusted Data Exchange	Allows you to publish, authorize, share, and decode data. Determine whether to enable the trusted data exchange APIs based on the service requirements. NOTE This parameter is displayed only when Enable DID API is enabled.	-
Channel	Select a channel for installing chaincode. NOTE This parameter is displayed only when Enable DID API is enabled.	channel

Step 5 Click **Next**.

 **NOTE**

Do not perform operations on the instance when installing an add-on.

----End

Add-on Instances

Step 1 Log in to the BCS console.

Step 2 Click **Add-on Management** in the navigation pane on the left.

Step 3 View the add-ons on the **Add-on Instances** tab page.

You can perform the following operations on the add-ons as required:

- **baas-restapi:**
 - Click the add-on to view its details.
 - You can click **Scale** next to **Normal/All Instances** to scale the number of instances in the range from 1 to 5.
 - Click **Modify** to enable or disable the APIs for DID and trusted data exchange. After you click **OK**, the instance will be restarted and will be interrupted for a short period of time. Refresh the page later.
 - Click **Uninstall** to uninstall an add-on.

----End

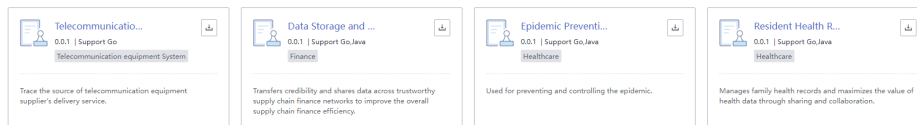
1.10 Contract Repository

A contract template is a smart contract that can implement certain functions. You can directly use the code provided by the templates or use the templates as a foundation for developing your own smart contracts.

In the Contract Management module on the console, you can view contract templates for various industries, download the ones you need, and manage your contract templates.

Downloading a Contract Template

- Step 1** Log in to the BCS console.
- Step 2** Click **Contract Repository** in the navigation pane on the left.
- Step 3** On the **Contract Repository** tab page, view contract templates for different industries, such as finance, healthcare, energy, and aviation.



- Step 4** Click the template name to view details about a contract template, including the version, supported language, category, and interfaces.

Figure 1-47 Viewing contract details

Contract Details
×

Data Storage and Query

Version 0.0.1

Language Go,Java

Category Finance

Description This contract template facilitates sharing of data such as accounts receivable/payable and key contracts across blockchain consortium-based supply chain systems. It allows the credibility of supply chain participants to be transferred based on the endorsement of core enterprises.

Interfaces

	Interface	Parameter	Description
▼	saveRecord	View Details	Saves records
▼	queryRecord	View Details	Queries records
▼	queryRecordByPartial	View Details	Queries records by key...
▼	deleteRecord	View Details	Delete records
▼	setKeyType	View Details	Sets the key type
▼	getKeyType	View Details	Queries the key type

- Step 5** Click to download a contract template.

You can use the downloaded template files to install and instantiate chaincodes. For details, see [Chaincode Management](#).

----End

1.11 Backup and Restoration Management

1.11.1 Creating a Backup

OBS and CBR store BCS backups. Backups of management data are stored in OBS and backups of ledger data are stored in CBR.

You can enable automatic backup when creating an enhanced Hyperledger Fabric instance, or you can enable it by creating a manual backup.

The following introduces two ways of creating backups:

- **Manually backup**
- **Automatically backup**

Creating a Backup Manually

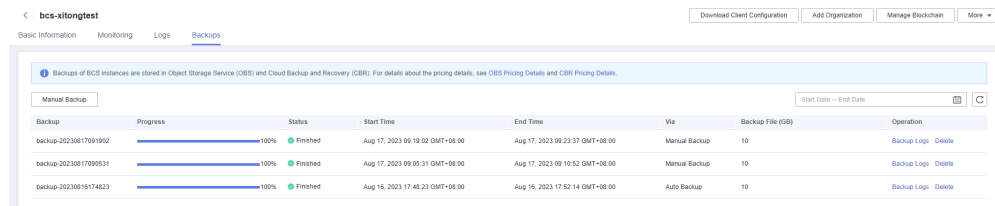
Step 1 Log in to the BCS console.

Step 2 On the **Instance Management** page, click the **Enhanced Hyperledger Fabric** tab.

Step 3 Click an instance to go to the details page.

Step 4 On the **Backups** tab page, click **Manual Backup**.

Step 5 Click **OK**. A backup task is generated. If the task is in the **Finished** state, the data stored on the blockchain is backed up.



The screenshot shows the 'Backups' page in the BCS console for instance 'bcs-xitongtest'. It features a table with columns for Backup ID, Progress, Status, Start Time, End Time, Via, Backup File (GB), and Operation. Three backup tasks are listed, all with a status of 'Finished' and 100% progress. The first two are manual backups, and the last one is an auto backup.

Backup	Progress	Status	Start Time	End Time	Via	Backup File (GB)	Operation
backup-20230817091902	100%	Finished	Aug 17, 2023 09:19:02 GMT+08:00	Aug 17, 2023 09:23:37 GMT+08:00	Manual Backup	10	Backup Logs Delete
backup-20230817090531	100%	Finished	Aug 17, 2023 09:05:31 GMT+08:00	Aug 17, 2023 09:10:52 GMT+08:00	Manual Backup	10	Backup Logs Delete
backup-20230816174823	100%	Finished	Aug 16, 2023 17:48:23 GMT+08:00	Aug 16, 2023 17:52:14 GMT+08:00	Auto Backup	10	Backup Logs Delete

NOTE

- A maximum of 10 manual backups can be created. If there are too many backups, delete unnecessary ones.
- Instances with backups can be billed in the yearly/monthly or pay-per-use mode.
 - If yearly/monthly billing is used, backups will not be deleted immediately but 7 days later after you unsubscribe from the instance. They can also be manually deleted on the OBS and CBR consoles. On the OBS console, go to the **Buckets** page, click an instance (**bcs-backup-nodetele-project ID/BCS instance ID**), and delete the backups. On the CBR console, go to the **SFS Turbo Backups** page, click an instance (**bcs-backup-BCS instance ID**), and delete the backups.
 - If pay-per-use billing is used, you can choose to delete instance backups when deleting an instance. Note that this operation deletes only the ledger data backed up in CBR. You will have to delete backups in OBS manually. You can either delete the CCE cluster or the SFS file system when deleting an instance, that is, select the second or the third checkbox. In this way, you can still restore your instance. But if you select to delete instance backups, the first checkbox, your instance will not be able to be restored.

----End

Enabling Automatic Backup

You can enable automatic backup when creating an enhanced Hyperledger Fabric instance, or you can enable it by [creating a manual backup](#).

Automatic backup applies to the following operations:

- Creating an instance
- Adding a peer to an organization
- Deleting a peer from an organization
- Adding a peer to a channel
- Adding an organization
- Upgrading a BCS instance
- Joining a consortium
- Creating a channel
- Deleting a channel
- Removing an instance from a consortium
- Removing a peer from a channel
- Removing an organization from a channel

NOTE

- Multiple backups will be generated for multiple operations. You will have to wait for the backup process to complete.
- A maximum of 10 automatic backups can be created. The system will delete certain backups to keep only 10 backups.

The backup task will be deleted in the order of priority listed below:

1. A failed task of backing up management plane data or data plane data
2. A backup that contains no management plane data or data plane data
3. A backup whose instance status is abnormal when the backup is complete
4. The earliest backup

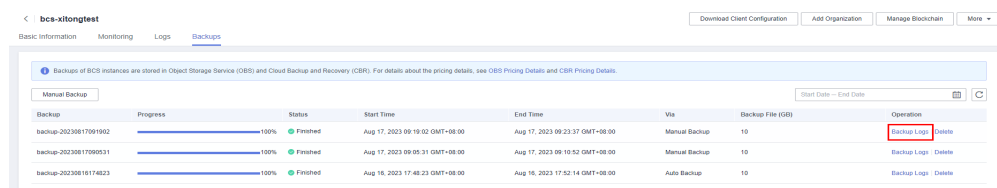
Viewing Backup Logs

Step 1 Log in to the BCS console.

Step 2 On the **Instance Management** page, click the **Enhanced Hyperledger Fabric** tab.

Step 3 Click an instance to go to the details page.

Step 4 On the **Backups** tab page, click **Backup Logs** in the **Operation** column of a backup.



Backup	Progress	Status	Start Time	End Time	Via	Backup File (GB)	Operation
backup-20230817091902	100%	Finished	Aug 17, 2023 09:19:02 GMT+08:00	Aug 17, 2023 09:23:37 GMT+08:00	Manual Backup	10	Backup Logs Delete
backup-20230817090531	100%	Finished	Aug 17, 2023 09:05:31 GMT+08:00	Aug 17, 2023 09:10:52 GMT+08:00	Manual Backup	10	Backup Logs Delete
backup-20230816174823	100%	Finished	Aug 16, 2023 17:48:23 GMT+08:00	Aug 16, 2023 17:52:14 GMT+08:00	Auto Backup	10	Backup Logs Delete

Step 5 View the backup logs.

Backup Logs



Time	Lo...	Description
Aug 17, 2023 09:05:31 GMT+...	Info	start to exec backup task
Aug 17, 2023 09:05:36 GMT+...	Info	start to create efs snapshots
Aug 17, 2023 09:10:51 GMT+...	Info	create efs snapshots succeeded
Aug 17, 2023 09:10:52 GMT+...	Info	create manage backup file success
Aug 17, 2023 09:10:52 GMT+...	Info	when the backup is complete, the insta...

NOTE

create efs snapshots succeeded: Ledger data has been backed up. **create manage backup file success:** Management data has been backed up. **when the backup is complete, the instance status is Normal:** The enhanced Hyperledger Fabric instance is normal when backing up. If all these messages are displayed, the backup is successful.

----End

Deleting a Backup

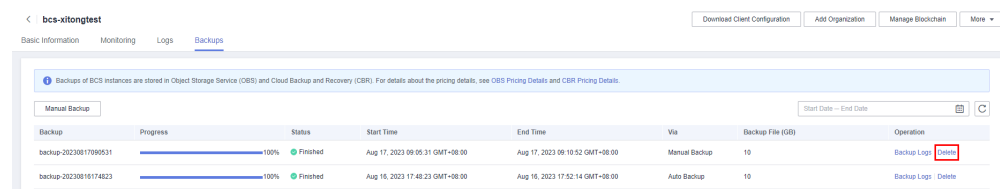
You can delete excess and unnecessary backups as required.

Step 1 Log in to the BCS console.

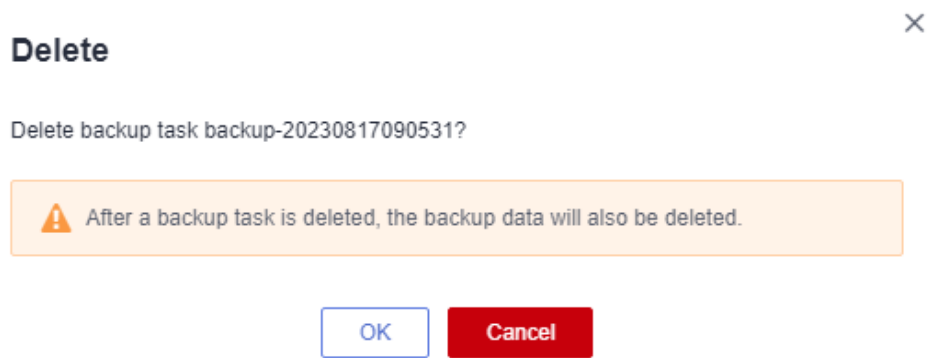
Step 2 On the **Instance Management** page, click the **Enhanced Hyperledger Fabric** tab.

Step 3 Click an instance to go to the details page.

Step 4 On the **Backups** tab page, click **Delete** in the **Operation** column of a backup.



Step 5 Click **OK**.



----End

1.11.2 Restoring a Backup

You can restore backups of enhanced Hyperledger Fabric instances that have been unsubscribed from or deleted.

Prerequisites

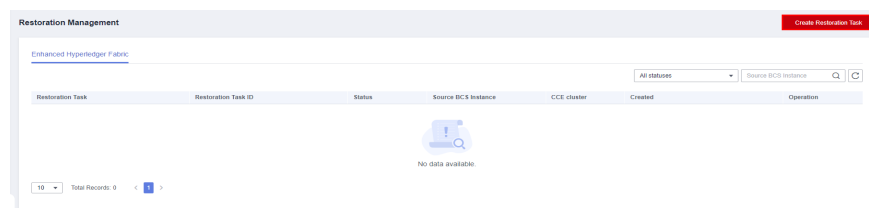
- You have **created a backup for an enhanced Hyperledger Fabric instance**.
- You have unsubscribed from or deleted the enhanced Hyperledger Fabric instance.

Creating a Restoration Task

Step 1 Log in to the BCS console.

Step 2 In the navigation pane, click **Restoration Management**.

Step 3 Click **Create Restoration Task**.



Step 4 Configure task parameters.

Table 1-20 Task parameters

Parameter	Description
Task	Name of a restoration task. Enter 4 to 24 characters. Only letters, digits, and hyphens (-) are allowed. Do not start with a hyphen (-).
Source BCS Instance	The BCS instance to be restored
Backup	The instance backup to be restored
Billing Mode	This is set by default based on the billing mode of the selected BCS instance.
Cluster	<p>The cluster where the BCS instance will be deployed. You can use an existing cluster or create a new one.</p> <p>NOTE</p> <ul style="list-style-type: none"> CCE clusters of v1.19 or earlier are supported. If the BCS instance uses Fabric v1.4, the CCE cluster must be v1.15 or earlier. The memory usage of instantiated containers varies depending on the chaincode language. On each peer, a Go chaincode container takes up 10 MB for running, and a Java chaincode takes up 110 MB. For example, if 100 Java chaincodes need to be instantiated, a 16 vCPUs and 32 GB CCE node is preferred.
Required Duration	This is required if Billing Mode is set to Yearly/Monthly .

Step 5 Click **Create Restoration Task**.

Step 6 On the payment page, confirm the order amount, and make the payment. Then return to the BCS console to view the instance that is being created.

 **NOTE**

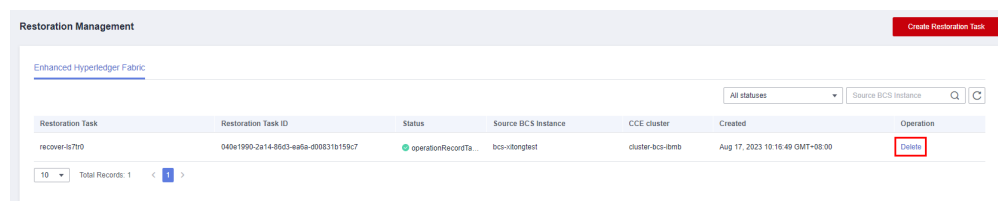
If a restoration task is finished, the BCS instance configuration and block data are restored.

----End

Deleting a Restoration Task

Step 1 Log in to the BCS console.

Step 2 In the navigation pane, click **Restoration Management**, then click **Delete** in the **Operation** column of a restoration task.



Step 3 Click **Yes**.

----End

1.12 Quotas

What Is a Quota?

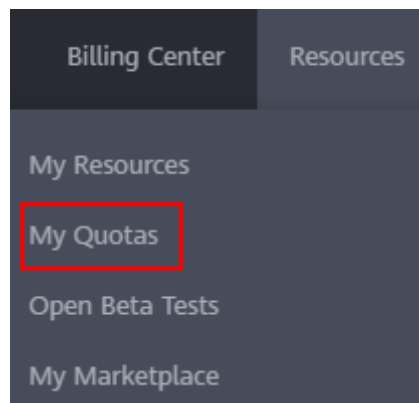
Quotas are enforced for service resources on the platform to prevent unforeseen spikes in resource usage. Quotas can limit the number or amount of resources available to users, such as the maximum number of ECSs or EVS disks that can be created.

If the existing resource quota cannot meet your service requirements, you can apply for a higher quota.

How Do I View My Quotas?

1. Log in to the management console.
2. In the upper right corner of the page, choose **Resources > My Quotas**.

Figure 1-48 My Quotas

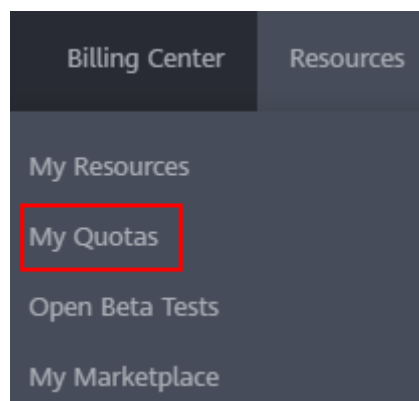


3. View the used and total quota of each type of resources on the displayed page.
If a quota cannot meet service requirements, apply for a higher quota.

How Do I Apply for a Higher Quota?

1. Log in to the management console.
2. In the upper right corner of the page, choose **Resources** > **My Quotas**. The **Service Quota** page is displayed.

Figure 1-49 Going to My Quotas



3. Click **Increase Quota**.
4. On the **Create Service Ticket** page, configure parameters as required.
In the **Problem Description** area, enter the required quota and the reason for the quota adjustment.
5. Read the agreements and confirm that you agree to them, and then click **Submit**.

1.13 Key Operations Recorded by CTS

1.13.1 BCS Operations That Can Be Recorded by CTS

BCS is a highly available and secure blockchain platform with superb performance. It helps enterprises and developers create, deploy, and manage applications and smart contracts conveniently and cost-effectively on Huawei Cloud.

With CTS, you can record operations associated with BCS for future query, audit, and backtracking.

Table 1-21 BCS operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Updating a service	Blockchain	updateBlockchain
Deleting a service	Blockchain	deleteBlockchain
Obtaining the SDK configuration of a BCS service	Blockchain	getBlockchainSdkConfig
Changing the agent password	Blockchain	modifyAgentPassword
Obtaining a service certificate	Blockchain	getBlockchainCert
Binding an EIP	Blockchain	bindEip
Creating a channel	Channel	createChannel
Scaling in/out peers	Blockchain	scalePeers
Adding a peer to a channel	Channel	addPeertoChannel
Buying a service	Blockchain	orderBlockchainService
Inviting a member	MemberList	inviteToMemberList
Deleting member details	MemberInfo	deleteMemberInfo
Deleting a notification	Notification	deleteOneNotification
Updating cloud service status (unsubscription, freezing, and unfreezing)	Blockchain	UpdateServiceStatus

1.13.2 Querying Audit Logs

For details about how to view audit logs, see [Querying Real-Time Traces](#).