Blockchain Service

Service Overview

Issue 01

Date 2023-08-14

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

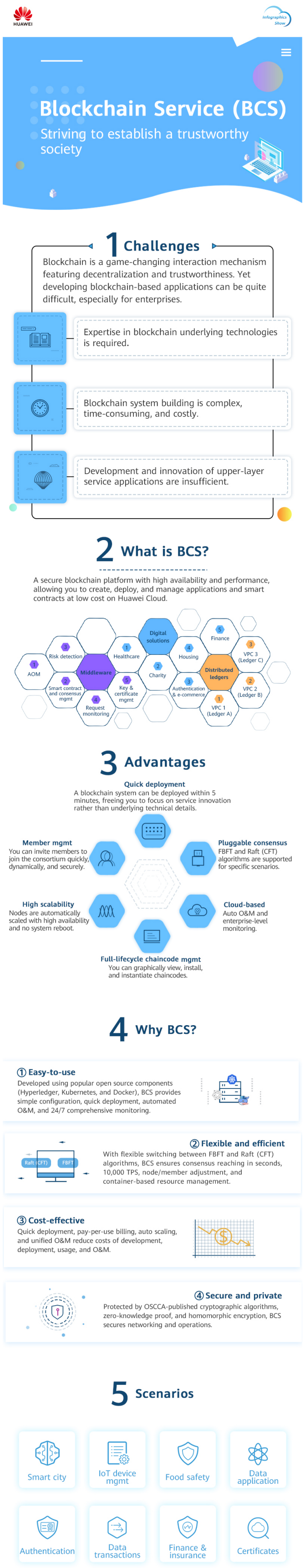
Notice

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 Infographics



Blockchain Service (BCS)

Striving to establish a trustworthy society

1 Challenges

Blockchain is a game-changing interaction mechanism featuring decentralization and trustworthiness. Yet developing blockchain-based applications can be quite difficult, especially for enterprises.

Expertise in blockchain underlying technologies is required.

Blockchain system building is complex, time-consuming, and costly.

Development and innovation of upper-layer service applications are insufficient.

2 What is BCS?

A secure blockchain platform with high availability and performance, allowing you to create, deploy, and manage applications and smart contracts at low cost on Huawei Cloud.

3 Advantages

Quick deployment
A blockchain system can be deployed within 5 minutes, freeing you to focus on service innovation rather than underlying technical details.

Member mgmt
You can invite members to join the consortium quickly, dynamically, and securely.

Pluggable consensus
FBFT and Raft (CFT) algorithms are supported for specific scenarios.

High scalability
Nodes are automatically scaled with high availability and no system reboot.

Cloud-based
Auto O&M and enterprise-level monitoring.

Full-lifecycle chaincode mgmt
You can graphically view, install, and instantiate chaincodes.

4 Why BCS?

① Easy-to-use
Developed using popular open source components (Hyperledger, Kubernetes, and Docker), BCS provides simple configuration, quick deployment, automated O&M, and 24/7 comprehensive monitoring.

② Flexible and efficient
With flexible switching between FBFT and Raft (CFT) algorithms, BCS ensures consensus reaching in seconds, 10,000 TPS, node/member adjustment, and container-based resource management.

③ Cost-effective
Quick deployment, pay-per-use billing, auto scaling, and unified O&M reduce costs of development, deployment, usage, and O&M.

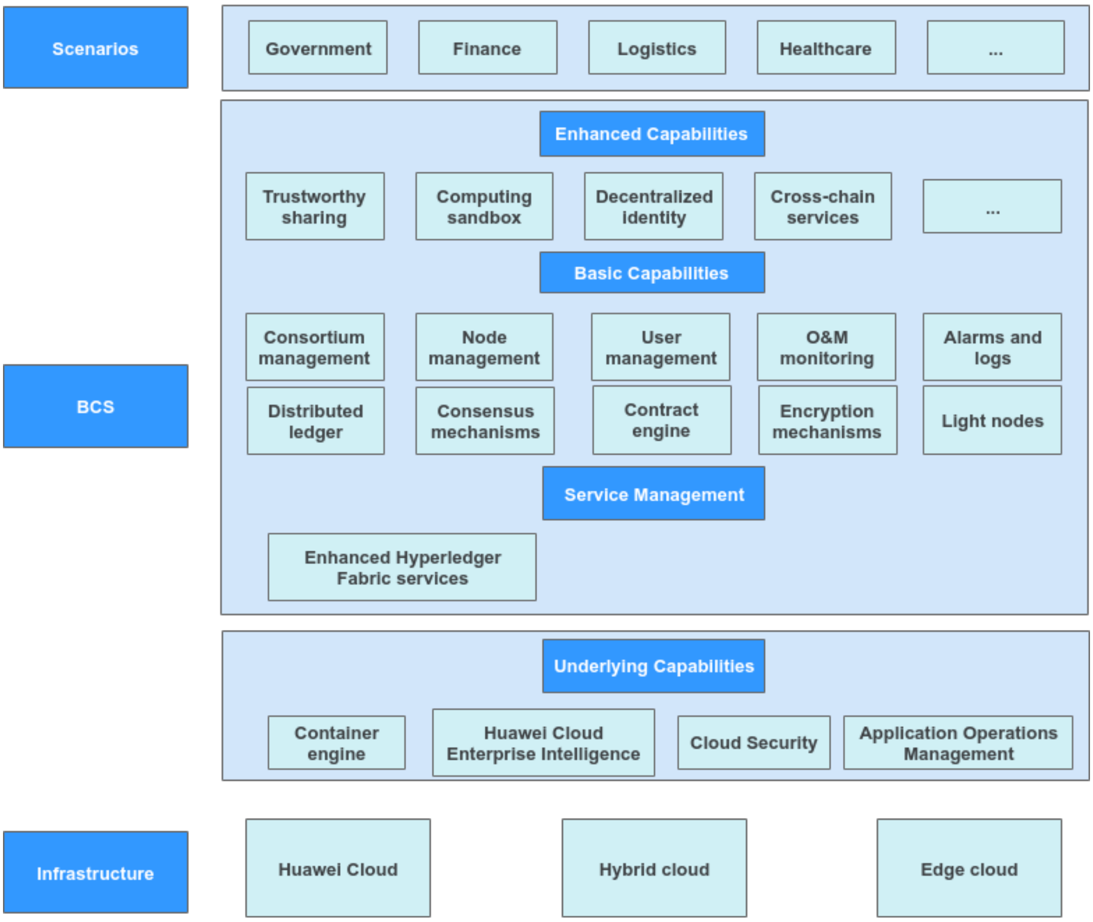
④ Secure and private
Protected by OSCCA-published cryptographic algorithms, zero-knowledge proof, and homomorphic encryption, BCS secures networking and operations.

5 Scenarios

2 What Is BCS?

Blockchain Service (BCS) is a blockchain platform for enterprises and developers. BCS helps you quickly deploy, manage, and maintain blockchain networks, lowering the threshold for using blockchains. In this way, you can focus on the development and innovation of your own business to quickly implement business using blockchains.

Figure 2-1 BCS architecture



- **Infrastructure**

The infrastructure layer offers underlying resources required for creating a blockchain network, including resources on nodes used to compute and store data in the network.

- **BCS**

  BCS provides enhanced Hyperledger Fabric blockchain instances, which consist of user management, node management, and O&M monitoring modules. It helps you quickly create, manage, and efficiently maintain an enterprise-grade blockchain system for upper-layer applications.

  - Enhanced Hyperledger Fabric instances are seamlessly integrated with Hyperledger Fabric, and are enhanced with the full-stack, trustworthy capabilities, including elastic computing, container, security, and AI services. They can meet enterprise- and finance-grade reliability, performance, and privacy requirements.

- **Scenarios**

  BCS can be used in multiple scenarios of various industries. Industry-specific applications connect to the blockchain platform to ensure data reliability and security.

- **Security management**

  Privacy isolation, consensus algorithms, and OSCCA-published cryptographic algorithms based on light nodes provide secure computing, trustworthy data sharing, and distributed identity capabilities.

Benefits of Blockchain

Higher efficiency: Builds a trusted multi-party collaboration platform to reduce disputes and improve transaction efficiency.

Reduced costs: Reduces extra costs and the participation of third parties.

Lower risks: Precludes the possibility of tampering to reduce risks of frauds and network errors.

Stronger trust: Builds up trust between transaction participants using shared ledgers, processes, and records.

Transparent audit: Audit institutions can audit the immutable ledgers at any time.

More Information

- Data in a blockchain system is generated and stored in blocks, which are chained in a time sequence. Hence the term "blockchain".
- All nodes in a blockchain system participate in data verification, storage, and maintenance. Consensus must be reached to create a block. Any new block is broadcast to all nodes, ensuring synchronization on the entire network. After this, it cannot be modified or deleted.

3 Functions

BCS provides the following functions to help you quickly deploy blockchains featuring security, high efficiency, and cost-effectiveness.

Instance Deployment

You can purchase resources when deploying a blockchain system, without a need to prepare resources required by the system in advance.

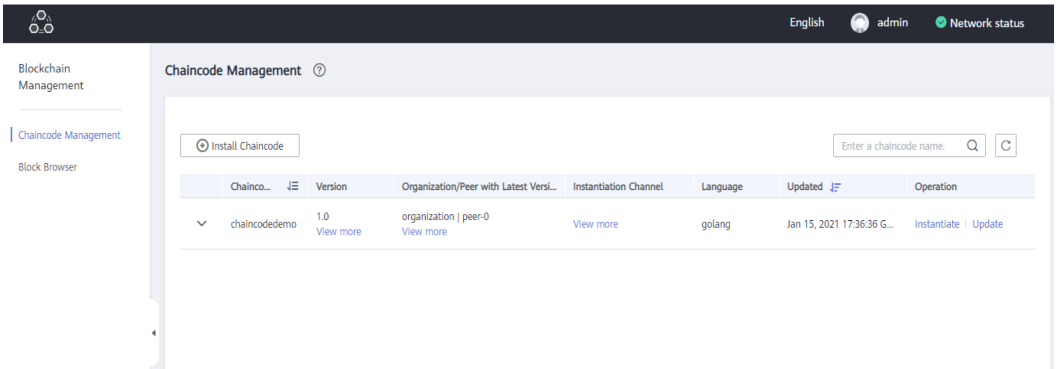
- The blockchain network configuration and deployment are completed in minutes, instead of days.
- Underlying technological details are masked. You do not need to care about the underlying technology implementation and platform construction.
- You can create consortium or private blockchains.

Instance Management

You can view the running statuses of your BCS instances and perform operations on them, for example, adding organizations, upgrading, and obtaining client configurations.

Chaincode Management

You can manage chaincodes on the graphical user interface (GUI) throughout the entire chaincode lifecycle, including coding, debugging, installation, instantiation, and upgrade.

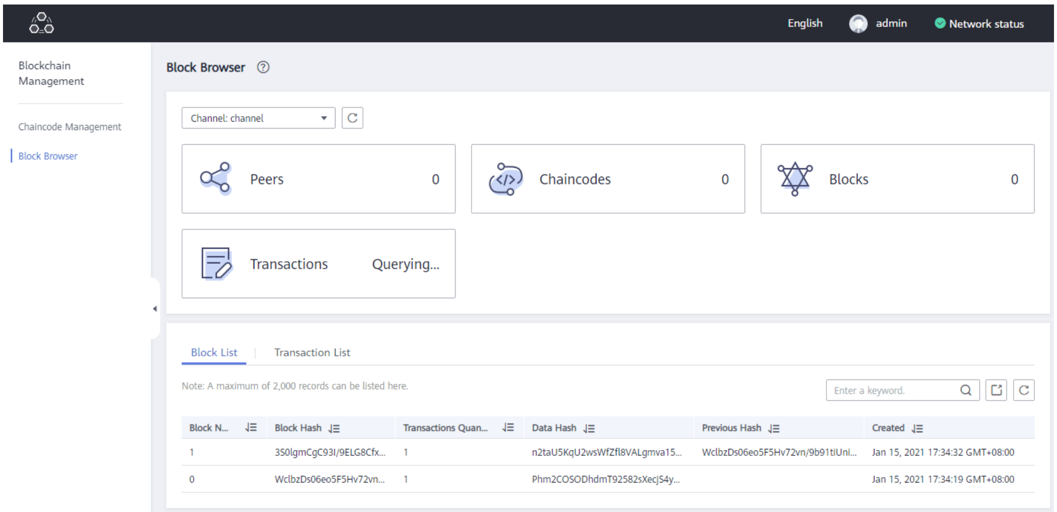


Chaincode Management

	Chainco...	Version	Organization/Peer with Latest Versi...	Instantiation Channel	Language	Updated	Operation
	chaincodedemo	1.0 View more	organization | peer-0 View more	View more	golang	Jan 15, 2021 17:36:36 G...	Instantiate | Update

Block Browser

In the block browser, you can query the block and transaction quantities and details, peer statuses, and performance data for blockchain maintenance.



Block Browser

Channel: channel

Peers 0

Chaincodes 0

Blocks 0

Transactions Querying...

Block List | Transaction List

Note: A maximum of 2,000 records can be listed here.

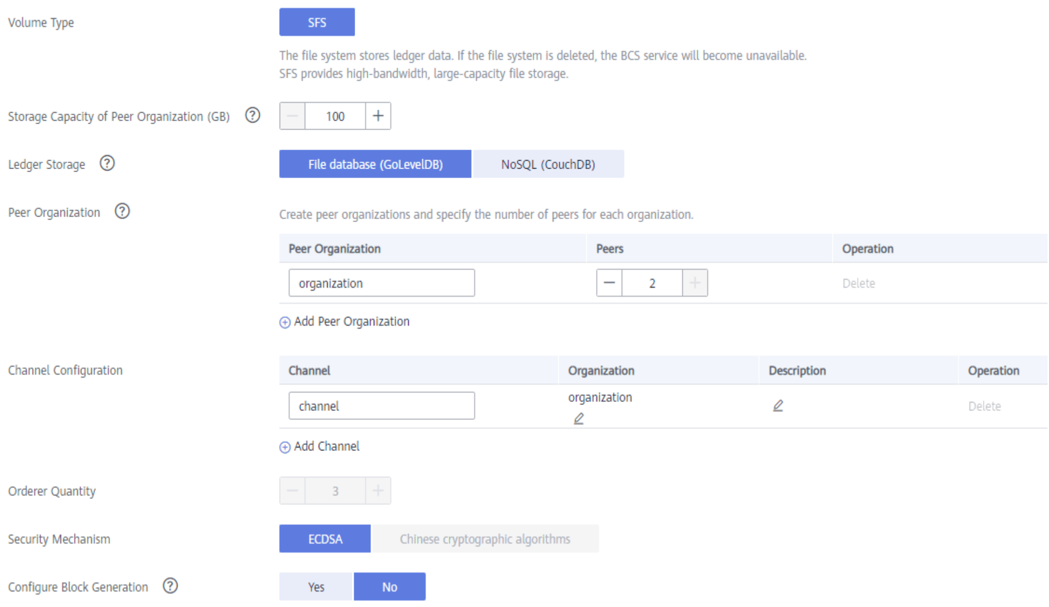
Enter a keyword.

Block N...	Block Hash	Transactions Quan...	Data Hash	Previous Hash	Created
1	3S0lgmCgC93I/9ELG8Cfx...	1	n2taU5KqU2wsWfZfl8VALgmva15...	WclbzDs06eo5F5Hv72vn/9b91tiUni...	Jan 15, 2021 17:34:32 GMT+08:00
0	WclbzDs06eo5F5Hv72vn...	1	Phm2COSODhdmT92582sXecjS4y...		Jan 15, 2021 17:34:19 GMT+08:00

Ledger Storage

File database (GoLevelDB) and NoSQL (CouchDB) are available for ledger storage.

- File database: Historical transaction data is stored in the blockchain, and status data is stored in LevelDB.
- NoSQL: Transaction and status data are stored in CouchDB.



Volume Type: SFS

The file system stores ledger data. If the file system is deleted, the BCS service will become unavailable.
SFS provides high-bandwidth, large-capacity file storage.

Storage Capacity of Peer Organization (GB): 100

Ledger Storage: File database (GoLevelDB) | NoSQL (CouchDB)

Peer Organization: Create peer organizations and specify the number of peers for each organization.

Peer Organization	Peers	Operation
organization	2	Delete

Add Peer Organization

Channel Configuration

Channel	Organization	Description	Operation
channel	organization		Delete

Add Channel

Orderer Quantity: 3

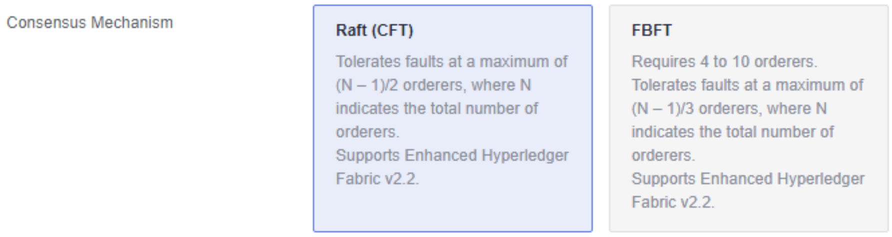
Security Mechanism: ECDSA | Chinese cryptographic algorithms

Configure Block Generation: Yes | No

Consensus Algorithms

BCS supports two consensus algorithms for different scenarios.

- **Raft (CFT)**: A crash fault tolerance (CFT) algorithm that tolerates faults at a maximum of (N – 1)/2 orderers, where N indicates the total number of orderers. It also supports Fabric v2.2.
- **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 also supports Fabric v2.2.



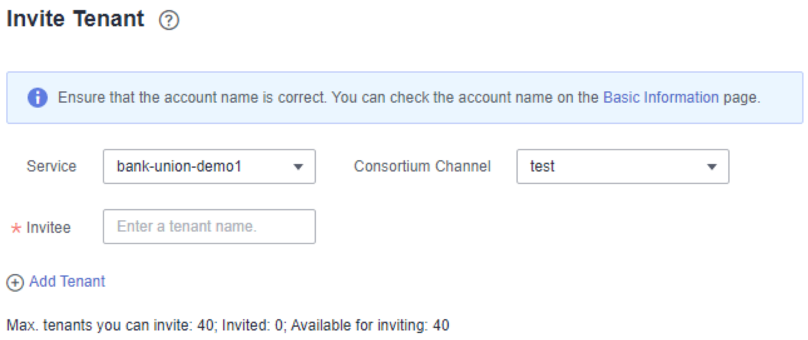
Consensus Mechanism

Raft (CFT)
Tolerates faults at a maximum of (N – 1)/2 orderers, where N indicates the total number of orderers.
Supports Enhanced Hyperledger Fabric v2.2.

FBFT
Requires 4 to 10 orderers.
Tolerates faults at a maximum of (N – 1)/3 orderers, where N indicates the total number of orderers.
Supports Enhanced Hyperledger Fabric v2.2.

Consortium Member and Organization Management

- A consortium initiator can dynamically invite other tenants to conveniently and quickly set up a consortium blockchain. Peers of each consortium member run in a separate virtual private cloud (VPC) for independent management, ensuring security and controllability.
- You can dynamically add peer organizations to a BCS instance.



Invite Tenant ?

Ensure that the account name is correct. You can check the account name on the Basic Information page.

Service: bank-union-demo1 ▾   Consortium Channel: test ▾

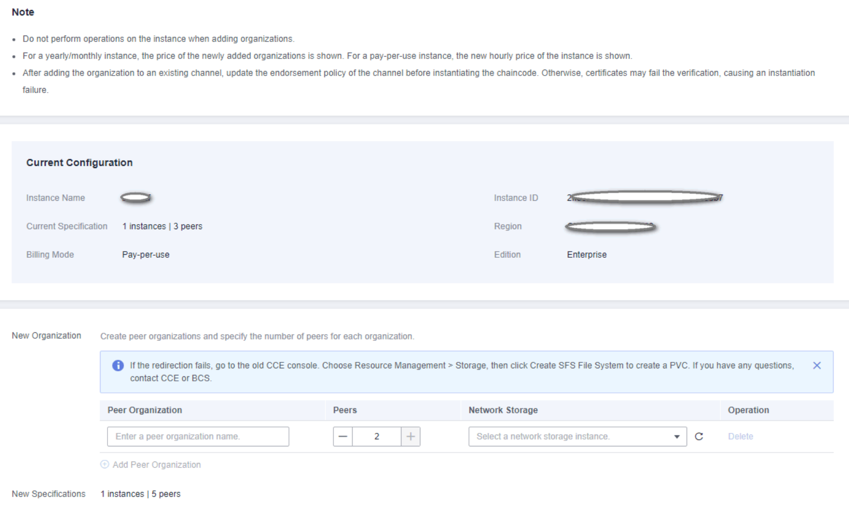
* Invitee: Enter a tenant name.

⊕ Add Tenant

Max. tenants you can invite: 40; Invited: 0; Available for inviting: 40

Auto Scaling of Nodes

You can scale nodes as required, without rebooting systems.



Note

- Do not perform operations on the instance when adding organizations.
- For a yearly/monthly instance, the price of the newly added organizations is shown. For a pay-per-use instance, the new hourly price of the instance is shown.
- After adding the organization to an existing channel, update the endorsement policy of the channel before instantiating the chaincode. Otherwise, certificates may fail the verification, causing an instantiation failure.

Current Configuration

Instance Name	[redacted]	Instance ID	[redacted]
Current Specification	1 instances | 3 peers	Region	[redacted]
Billing Mode	Pay-per-use	Edition	Enterprise

New Organization: Create peer organizations and specify the number of peers for each organization.

If the redirection fails, go to the old CCE console. Choose Resource Management > Storage, then click Create SFS File System to create a PVC. If you have any questions, contact CCE or BCS.

Peer Organization	Peers	Network Storage	Operation
Enter a peer organization name.	2	Select a network storage instance.	Delete

New Specifications: 1 instances | 5 peers

Contract Scan

Automatic analysis tools are provided to ensure the smart contract safety from the source. Based on the vulnerabilities and issues commonly found in consortium blockchain smart contracts, the check reports and solutions are generated to help users and developers audit code security, detect risks, and resolve problems.

Privacy Protection

- In each channel, members are assigned different access permissions to certain data, ensuring the data privacy of members within a channel.
- Different channels are also isolated from each other, protecting block data of all members in a channel from other channels.

Application Access

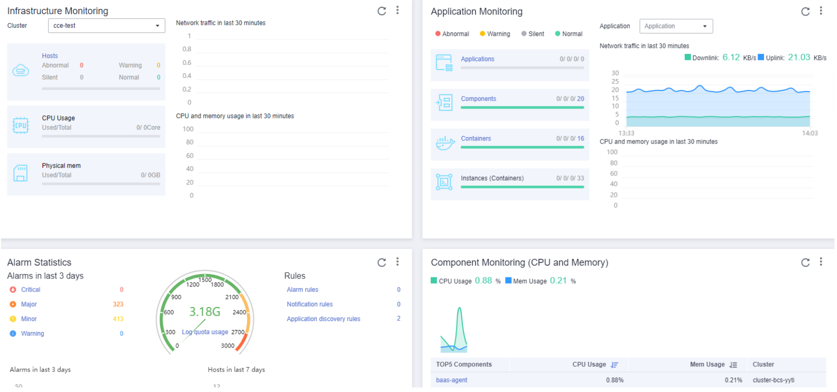
Applications can access blockchain networks using software development kits (SDKs) and RESTful APIs.

- SDK configuration files can be downloaded. After simple configuration, an application can be connected to a blockchain network.
- Applications can invoke chaincodes through RESTful APIs. The policy of multi-organization endorsement is supported.

Monitoring and O&M

BCS connects to the monitoring platform to monitor data and resources in real time and generate alarms and notifications when necessary.

- Automated O&M: BCS actively upgrades the underlying blockchain platform and updates patches to seamlessly integrate with the Huawei Cloud O&M system.
- Enterprise-grade monitoring: Multi-dimensional monitoring is performed on clusters 24/7, and user-defined alarms can be reported through multiple channels.



Infrastructure Monitoring

Cluster: cce-test

Hosts
Abnormal 0 Warning 0
Silent 0 Normal 0

CPU Usage
Used/Total 0/ 0Core

Physical mem
Used/Total 0/ 0GB

Application Monitoring

Application: Application

Applications 0/ 0/ 0/ 0
Components 0/ 0/ 0/ 20
Containers 0/ 0/ 0/ 16
Instances (Containers) 0/ 0/ 0/ 33

Downlink: 6.12 KB/s Uplink: 21.03 KB/s

Alarm Statistics

Alarms in last 3 days

Critical	0
Major	323
Minor	413
Warning	0

3.18G Log quota usage

Rules

Alarm rules	0
Notification rules	0
Application discovery rules	2

Component Monitoring (CPU and Memory)

CPU Usage 0.88 % Mem Usage 0.21 %

TOP5 Components	CPU Usage	Mem Usage	Cluster
baas-agent	0.88%	0.21%	cluster-bcs-yyti

4 Advantages

Open and Easy to Use

Building an enterprise-grade distributed blockchain network is not easy. It requires not only in-depth knowledge of blockchain but also complex design and configuration, which is error-prone and costly.

- BCS can help enterprises deploy blockchain networks within only 5 minutes, reducing the development and deployment costs by as much as 80%.
- BCS hosts functions of full-lifecycle management and GUI-based smart contract coding, commissioning, and deployment. Customers using BCS can focus on the innovation and development of their own service applications.

Flexible and Efficient

- BCS supports multiple efficient consensus algorithms and deeply optimizes existing algorithms to achieve balance between security and efficiency.
- Consensus within seconds can realize 100,000 transactions per second (TPS), meeting service performance requirements.
- Blockchain ledgers are stored in the efficient Huawei Cloud elastic storage files, satisfying the demand of fast storing massive amount of user data.
- Nodes of multiple roles and members can dynamically join or quit consortium blockchains.

Cost-Effective

- Instance hibernation and waking at any time and the pay-per-use billing mode
- The Application Operations Management (AOM) service is used for comprehensive O&M on the BCS instances, providing system status, performance, and transaction monitoring, maintenance, and alarming to reduce O&M costs.
- The node scaling function greatly improves the cost-effectiveness.

Secure and Private

Comprehensive approach to blockchain security:

- The Huawei Cloud security system ensures stable and secure running of blockchains.
- The Hyperledger-assured security system prevents data tampering and protects privacy by means of certificate management and the blockchain structure of data.
- Innovative algorithms such as homomorphic encryption and zero-knowledge proofs provide further privacy protection.
- OSCCA-published cryptographic algorithms are used for encryption and decryption.

Trustworthy and Collaborative

BCS provides the Trusted Computing Platform to facilitate trusted cooperation between multiple parties. This platform has the following core features:

- Decentralized identity (DID) management, which is in compliance with the W3C DID and W3C verifiable credential (VC) standards. This feature lowers the threshold of trust and improves cooperation efficiency.
- Blockchain-based, trusted data sharing, which ensures trusted data flow between multiple parities, breaks data silos, and realizes data value.
- Confidential computing, which is based on blockchain, Trusted Execution Environment (TEE), and federated learning technologies. The raw data can be computed without being revealed, ensuring data privacy.

5 Key Concepts

Blockchain

In a narrow sense, a blockchain is a list of data records (called blocks) linked in chronological order using cryptography and a distributed ledger to prevent data tampering and forging. In a broad sense, the blockchain technology is a new distributed infrastructure and computing paradigm that uses the blockchain data structure to verify and store data, distributed node consensus algorithms to generate and update data, cryptography to ensure security of data transmission and access, and smart contracts formed by automated scripts to implement programming and operate data.

Distributed Ledger

A distributed ledger is a database shared, replicated, and synchronized among network members. It records transactions between network participants, such as exchange of assets and data. Use of a distributed ledger eliminates the time and expenditure of ledger reconciliation. Any reference to ledgers in BCS documents means distributed ledgers.

- Decentralized and trustless: Data copies are stored on nodes. No central node or a third-party organization is responsible for data control.
- Collectively maintaining data consistency: Each participant uses a public key as its identity. Nodes independently check the data validity and collectively determine the data to be written to the ledger, by consensus.
- Reliable data, difficult to be tampered with: Data is stored in blocks. Each node stores all blocks. Data access permissions can be customized. Block chaining prevents data tampering.

Smart Contract

A smart contract, also called a chaincode, is a code logic that runs on a blockchain and is automatically executed under a specific condition. It is an important method for a user to implement service logic when using a blockchain. Thanks to the blockchain features, the execution results of smart contracts are reliable and cannot be forged or tampered with.

- Cheating is prevented. Smart contracts are automatically triggered when conditions are met. Execution results are verified independently.

- Results cannot be modified because the data is stored in the blockchain.
- Contract content is reliable because it is stored in the blockchain.
- Privacy is protected. Only specified participants can obtain contract content and data.

Peer

Peers are network nodes that maintain ledgers. One or more peers form a peer organization.

Orderer

Orderers are nodes that order transactions into a block.

Channel

A channel isolates the ledger data of a transaction from that of other transactions in a consortium blockchain to ensure confidentiality. Each channel can be considered a sub-blockchain and corresponds to a specific ledger. The ledger in a channel is invisible to other channels.

Distributed Consensus

A majority of independent participants in a system need to achieve consensus on a transaction or operation, for example, verification of double-spending transactions, verification of service logic validity, and the decision on whether to write verified data to the existing ledger.

Hash Algorithm

A hash value of a digital content segment can be used to verify data integrity. Any minor modification to digital content leads to a significant change in the hash value. A qualified hash algorithm can be used to easily obtain a hash value from digital content, but it is almost impossible to calculate the original digital content by using a hash value.

Organization

A channel contains multiple members (organizations). If identity certificates of two entities on the blockchain network can be traced back to a same Root certificate authority (CA), the two entities belong to a same organization.

6 Edition Differences

Enhanced Hyperledger Fabric

BCS provides basic and professional editions with different specifications. For details, see **Table 6-1**. **Table 6-2** lists the cluster specifications.

For the pricing details of each edition, see **Product Price Details**.

NOTE

Only one BCS instance can be deployed in a container cluster.

Table 6-1 Comparison between editions

Item		Basic Edition	Professional Edition
Applicable scenario		Small scale commercial use	Medium-scale commercial use
Consortium blockchain		Supported	Supported
Peak transaction performance		≤ 500 TPS	≤ 2000 TPS
Consensus algorithms	Raft(CFT)	Supported	Supported
	FBFT	Not supported	Supported
Node management	Maximum number of organizations	2	5
	Maximum number of peers in an organization	2	2
	Maximum number of orderers	3	4
	Maximum number of channels	2	4

Item		Basic Edition	Professional Edition
	Automatic recovery from node faults	Supported	Supported
	Node auto scaling	Supported	Supported
	Maximum number of light nodes	Not supported	10
Security functions	ECDSA	Supported	Supported
	OSCCA-published cryptographic algorithms	Not supported	Supported
	Additive homomorphic encryption	Not supported	Supported
	Zero knowledge proof	Not supported	Supported
High availability	Invoking smart contracts through RESTful APIs	Supported	Supported
	Common deployment	Supported	Supported
	High-availability deployment	Not supported	Not supported
O&M and monitoring	O&M logging	Supported	Supported
	Node status monitoring	Supported	Supported
	Status alarms	Supported	Supported
Service support	Named service manager	Not supported	Not supported
	Remote technical support from the R&D team	Not supported	Not supported
	Onsite technical support	Not supported	Not supported

Table 6-2 Specifications

Edition	Cloud Container Engine (CCE) Cluster	Elastic Cloud Server (ECS)	Elastic IP (EIP) Address	VPCs and Subnets	Container Networking
Basic Edition	cce.s1.small (small-scale, single-master CCE cluster, supporting a maximum of 50 nodes) Single-AZ deployment	Specification: 4 vCPUs and 8 GB memory Quantity: Number of peers in the organization/ 2 + Number of orderers (1)	Private blockchain: no EIPs Consortium blockchain: one EIP for each cluster node EIP bandwidth: 1 Mbit/s	VPC: 1; subnet: 1	VPC network
Professional Edition	cce.s2.small (small-scale, high-availability CCE cluster, supporting a maximum of 50 nodes) Multi-AZ deployment	Specification: 8 vCPUs and 16 GB memory Quantity: Number of peers in the organization/ 2 + Number of orderers	Private blockchain: no EIPs Consortium blockchain: one EIP for each cluster node EIP bandwidth: 5 Mbit/s	VPC: 1; subnet: 1	VPC network

7 Application Scenarios

7.1 Transactions Between Subsidiaries

BCS provides end-to-end (E2E) audit support for inter-subsidiary transactions by building a collaboration consortium with subsidiaries of a multinational company and audit organizations involved, developing trust and eliminating reconciliation and discrepancies between the transaction parties.

Industry Status Quo and Pain Points

- **Lack of trust between subsidiaries**

  Transaction parties do not fully trust in each other for ownership and fund transfer during contract execution and transactions.

- **Delayed financial settlement**

  Reconciliation of internal transactions requires a large amount of manpower and long time. The discrepancy in reconciliation may lead to delayed settlement and report issuance.

- **Low efficiency and high cost**

  Internal reconciliation is time-consuming and requires a large number of financial personnel's efforts. However, the reconciliation result may still be incorrect, and it is hard to perform supervision.

- **No simple method of data sharing**

  The financial data of subsidiaries is distributed in different types of enterprise resource planning (ERP) systems, which are not integrated or connected.

- **Regulators lacking trust in company**

  A multinational company must keep data for many years (usually 10 or more years) and provide evidence to external auditors or authorities, demonstrating that data sources are trustworthy and the data has not been tampered with.

- **Restatements**

  Inter-subsidiary transfer pricing and complex transactions may cause tax base erosion and profit shifting (BEPS) and may result in financial statement restatements.

Solution Architecture

The BCS-based inter-subsidiary transaction solution has the following features:

- **Unified ledger**

  Tamper-proof, consistent business transaction records are traceable, eliminating the necessity of reconciliation and meeting audit requirements.

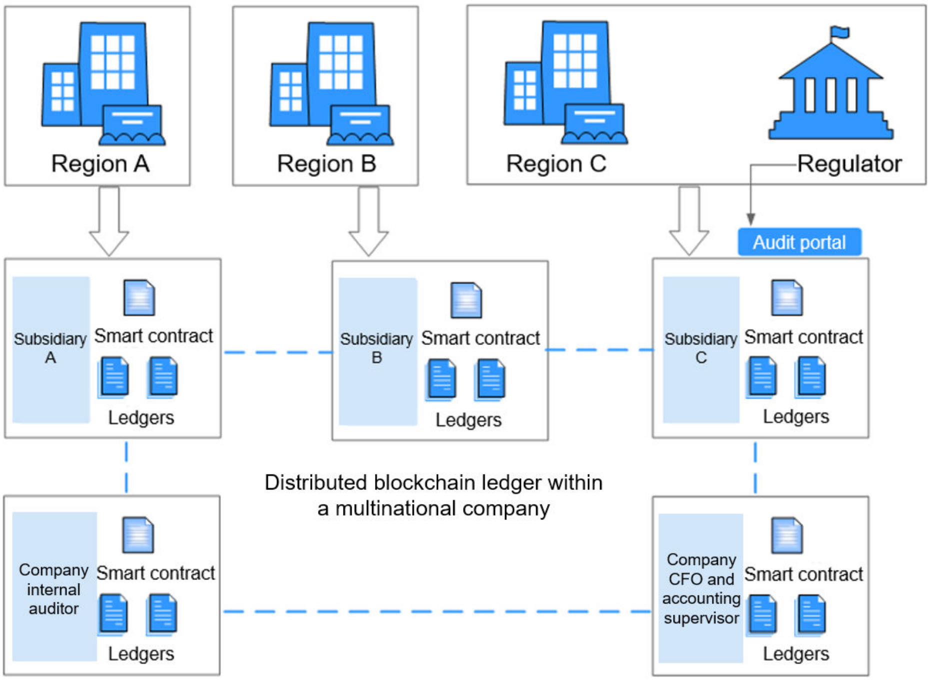
- **Digital assets**

  Tokens are used to record the transaction assets and rights to realize the life-cycle management of digital assets.

- **Smart contract fulfillment**

  Automated fulfillment ensures the fairness of transactions based on the contract terms and conditions.

Figure 7-1 Solution architecture



Solution Highlights

- Ensuring consistency of inter-subsidiary transaction records and the balance of accounting without the need for reconciliation
- Using tokens to follow goods' statuses, timing, locations, and ownership changes and strictly adhering to the contract clauses to carry out transactions, improving the trust between transaction parties
- Simplifying and normalizing the inter-subsidiary supply chain processes
- Supporting transactions that involve different systems
- Providing E2E traceable and immutable information for internal and external audits

7.2 Supply Chain Logistics

Manufacturers, warehousing institutes, logistics providers, and customers can use BCS to comprise collaboration consortia and use IoT technologies to record all the logistics information of goods, including production, warehousing, line haul transportation, reselling, and local logistics. The consortia break down information silos, improve circulation of information, and build trust between parties.

Industry Status Quo and Pain Points

- **Disadvantage of using paper documents**

  Many phases of logistics still involve manual operations and paper documents. This causes long duration of the process, high costs, slow reconciliation, and risks of document losses or damage. The cost on maintaining and transferring documents accounts for 1/5 of the total logistics cost.

- **Low efficiency**

  Participants in a supply chain have their own information systems, independent from each other. There is no unified standard or system. It is difficult for them to collaborate effectively.

- **Long duration**

  Electronic information can be easily tampered with. Therefore, paper documents are used as the only type of proof for settlement, but extend the accounting period and the carriers' average collection period of receivables.

- **Difficult financing**

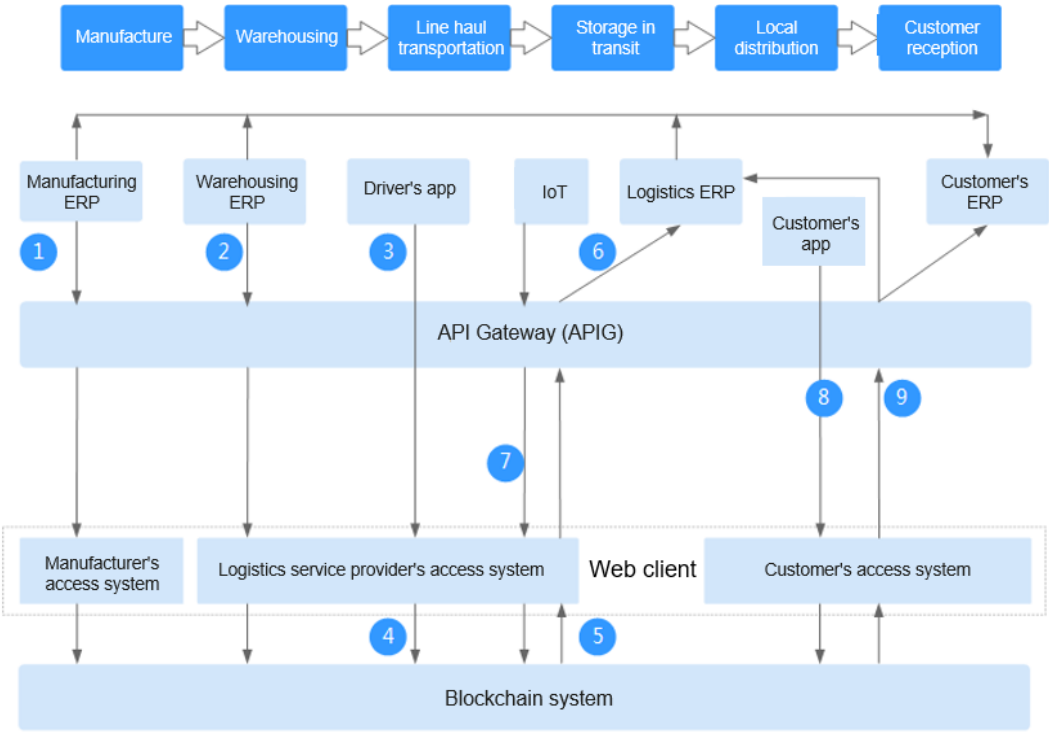
  Most carriers are small- and medium-sized enterprises, lacking credit records, scores, or credibility. Financing is difficult and requires high costs.

Solution Architecture

The supply chain logistics solution provided by BCS can be combined with the IT information systems of logistic participants to achieve the following:

- Jointly maintain unified ledgers, which store immutable and traceable goods transfer records to meet audit requirements.
- Provide common APIs for participants' IT systems to access BCS and input data, which cannot be tampered with. In this way, participants establish their credibility and trust in each other.
- Automatically store the geo-fence information reported by the driver's app to show in real time when, where, and by whom goods are processed.
- Fulfill smart contracts to automatically perform signing, settlement, and calculation to obtain the performance data, which is considered fair due to the automation.

Figure 7-2 Solution architecture



Procedure:

1. Goods delivery information is sent to the blockchain through the access system.
2. Goods reception and delivery information is sent to the blockchain through the access system.
3. The driver collects goods by scanning.
4. Logistics information is sent to the blockchain through the access system.
5. The blockchain system confirms that the received information has been stored.
6. The information is sent to the IT system through APIG.
7. The GPS data of trucks is sent to the blockchain through the access system.
8. The customer reception information is sent to the blockchain through the access system.
9. The blockchain system confirms that the received information has been stored and sent to the ERPs of the logistics service provider and manufacturer.

Solution Highlights

- **Reduced errors**

  Distributed, shared ledgers greatly improve the traceability and transparency of the supply chain and effectively reduce or eliminate changes of frauds and errors.

- **Increased efficiency**

  Electronic proofs of delivery (PODs) are used instead of paper documents to reduce the delay caused by paper works. Smart contracts enable automatic settlement to improve efficiency.

- **Lower costs**

  Quick settlement, automatic order reception, and goods follow-up significantly lower the logistics costs of all the involved parties.

- **Transparent audit**

  Immutability of distributed ledgers and non-repudiation of signatures allow for quick discovery of problems in supply chain logistics.

- **Trust**

In addition to transparent rules and automated settlement, the blockchain technology can help you follow goods all the way through production and transport to final reception. These mechanisms greatly improve the trust between all the involved parties.

7.3 Healthcare

BCS helps healthcare institutions, third-party organizations, and supervision departments to form a collaboration consortium. Healthcare information silos are broken down using electronic medical records that cannot be tampered with to protect privacy. This builds trust between doctors and patients and provides comprehensive health and medical care information for telemedicine and referral.

Industry Status Quo and Pain Points

- **Insecure data**

  Most healthcare data is stored in the data center. If a natural disaster or hacking occurs, patients' electronic medical records stored in the data center may be lost.

- **Information silos**

  There is no appropriate mechanism for mutual trust and data sharing between healthcare institutions, which leads to information silos and makes it difficult to obtain complete and comprehensive data. Data may be modified casually when shared and therefore, is considered unreliable.

- **Repeated medical treatment**

  Data is not shared between healthcare institutions. Performing repetitive health checks and creating new medical records are required when patients go to the different institutions, wasting time, money, and medical resources.

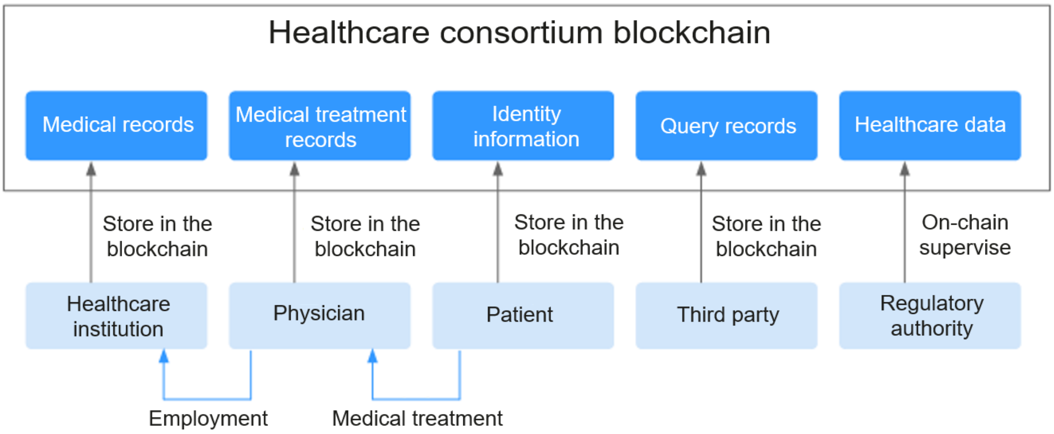
- **No access to personal medical data**

  Patients' medical data is stored in the hospital systems, however, patients cannot access to or manage it.

Solution Architecture

A healthcare consortium blockchain is built, comprising healthcare institutions, third parties, physicians, patients, and regulators based on electronic medical records (EMRs). The medical and healthcare data is stored in the blockchain and offered for queries or scientific research, with security and privacy protected by using encryption and smart contract-based authorization mechanisms.

Figure 7-3 Solution architecture



Solution Highlights

- **Information silos broken down**

  The healthcare consortium blockchain connects information systems of healthcare institutions, so that regional inspection as well as ultrasound and radiological examination results can be securely exchanged for online healthcare, two-way referral, and remote consultation.

- **Immutable medical data**

  The EMRs, physicians' diagnosis process and results, medical record query histories, and patient identity information are transparently stored in blockchains to ensure that they cannot be tampered with. This reduces medical disputes and constructs a harmonious healthcare environment.

- **Protected privacy and right to know**

  Encryption and smart contract-based authorization mechanisms offer patients access to their own healthcare data while protecting their privacy. Others can access the data only when authorized.

- **Quick and effective supervision**

  Regulatory authorities can use the data on blockchains to effectively prevent healthcare treatment that violates regulations, reducing medical disputes.

8 Permissions Management

If you need to assign different permissions to employees in your enterprise to access your BCS resources, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you secure access to your Huawei Cloud resources.

With IAM, you can use your Huawei Cloud account to create IAM users, and assign permissions to the users to control their access to specific resources. For example, some software developers in your enterprise need to use BCS resources but should not be allowed to delete the resources or perform any other high-risk operations. In this scenario, you can create IAM users for the software developers and grant them only the permissions required for using BCS resources. For details about permission management and configuration, see **Permissions Management** for enhanced Hyperledger Fabric.

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

IAM is free of charge. You pay only for the resources you use.

You can grant users permissions by using roles and policies.

- Roles: A type of coarse-grained authorization mechanism that defines permissions related to user responsibilities. This mechanism provides only a limited number of service-level roles for authorization. When using roles to grant permissions, you also need to assign other roles on which the permissions depend to take effect. However, roles are not an ideal choice for fine-grained authorization and secure access control.
- Policies: A type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions. This mechanism allows for more flexible policy-based authorization, meeting requirements for secure access control. For example, you can grant ECS users only the permissions for managing a certain type of ECSs.

Enhanced Hyperledger Fabric

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

BCS is a project-level service deployed and accessed in specific physical regions. To assign BCS permissions to a user group, specify the scope as region-specific projects and select projects for the permissions to take effect. If **All projects** is selected, the permissions will take effect for the user group in all region-specific projects. Switch to a region where you have been authorized to access BCS.

Table 8-1 lists the system-defined policy supported by enhanced Hyperledger Fabric.

Table 8-1 System-defined roles and policies supported by enhanced Hyperledger Fabric

Role/Policy Name	Description	Type	Dependency
BCS Administrator	Full operation permissions for enhanced Hyperledger Fabric BCS	System-defined role	Tenant Guest, Server Administrator, ELB Administrator, SFS Administrator, SWR Admin, APM FullAccess, AOM FullAccess, CCE Administrator, VPC Administrator, EVS Administrator, and CCE Cluster Admin
BCS Fabric FullAccess	Full permissions for enhanced Hyperledger Fabric BCS	System-defined policy	None
BCS Fabric ReadOnlyAccess	Read-only permissions for enhanced Hyperledger Fabric BCS	System-defined policy	None

- BCS Fabric FullAccess content:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "bcs:fabric*:*",
                "cce:*:*",
                "ecs:*:*",
                "evs:*:*",
                "vpc:*:*",
                "elb:*:*",
                "aom:*:*",
                "apm:*:*",
                "rds:*:*",
                "dms:*:*",
                "sfs:*:*",
                "sfsturbo:*:*",
                "cloudIDE:*:*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

- BCS Fabric ReadOnlyAccess content:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "bcs:fabric*:get*",
                "bcs:fabric*:list*",
                "cce:*:get*",
                "cce:*:list*",
                "ecs:*:get*",
                "ecs:*:list*",
                "evs:*:get*",
                "evs:*:list*",
                "vpc:*:get*",
                "vpc:*:list*",
                "elb:*:get*",
                "elb:*:list*",
                "aom:*:get*",
                "aom:*:list*",
                "apm:*:get*",
                "apm:*:list*",
                "rds:*:get*",
                "rds:*:list*",
                "dms:*:get*",
                "dms:*:list*",
                "sfs:*:get*",
                "sfsturbo:*:get*",
                "cloudIDE:*:get*",
                "cloudIDE:*:list*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

9 Billing

For details about the pricing of different editions of enhanced Hyperledger Fabric instances, see **Pricing Details**.

10 Restrictions

A maximum of five enhanced Hyperledger Fabric instances can be created.The specifications of each instance vary depending on the edition. For details, see **Edition Differences**.

11 Note on End of Maintenance

Maintenance of the BCS versions earlier than 2.1.33 has been terminated. If you are using a version earlier than 2.1.33, certain operations may be restricted. Upgrade the BCS service to the latest version as soon as possible.

12 Security Notice

12.1 Notice on the Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228)

Vulnerability Description

Apache Log4j2 has a remote code execution vulnerability (CVE-2021-44228). When Apache Log4j2 processes user input during log processing, attackers can construct special requests to trigger remote code execution. The POC has been disclosed and the risk is high. For details, see **Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228)**.

Vulnerability Impact

Apache Log4j2 is used in **Fabric_SDK_Gateway_Java** and **Fabric_SDK_Java** provided by BCS (for encryption using OSCCA-published cryptographic algorithms) and those provided by Hyperledger Fabric. It is also used in the corresponding demos **App_Gateway_Java_Demo**, **App_Java_Src_Demo**, and **App_Java_Jar_Demo**.

The vulnerability in these components has been fixed in the CN North-Beijing4 region. If you use these components, go to the BCS console, switch to the CN North-Beijing4 region, obtain the latest version from **Use Cases**, and perform an upgrade as soon as possible. Before the vulnerability is fixed in your blockchain application, ensure that the input source of your blockchain application is trusted.

Vulnerability Fixing

Upgrade **Fabric_SDK_Gateway_Java**, **Fabric_SDK_Java**, and Apache Log4j2 to the latest versions.

The fixed **Fabric_SDK_Gateway_Java** and **Fabric_SDK_Java** can be obtained from the **Use Cases** module in the CN North-Beijing4 region. For details about how to use these SDKs, see **Using SDKs**.