Cloud Backup and Recovery

Service Overview

Issue	06
Date	2023-03-13

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Contents

1 What Is CBR?

Overview

Cloud Backup and Recovery (CBR) enables you to easily back up Elastic Cloud Servers (ECSs), Bare Metal Servers (BMSs), Elastic Volume Service (EVS) disks, SFS Turbo file systems, local files and directories, and on-premises VMware virtual environments. In case of a virus attack, accidental deletion, or software or hardware fault, you can use the backup to restore data to any point when the data was backed up.

CBR protects your services by ensuring the security and consistency of your data.

CBR Architecture

CBR involves backups, vaults, and policies.

Backup

A backup is a copy of a particular chunk of data and is usually stored elsewhere so that it may be used to restore the original data in the event of data loss. There are the following types of backups:

- Cloud disk backup: provides snapshot-based backups for EVS disks.
- Cloud server backup: uses the consistency snapshot technology to protect data for ECSs and BMSs. Backups of non-database servers are common server backups, and those of database servers are application-consistent backups.
- SFS Turbo backup: backs up data of SFS Turbo file systems.
- Hybrid cloud backup: protects data of on-premises OceanStor Dorado storage systems and VMware VMs by storing their backups to the cloud. You can manage the backups on CBR Console.
- File backup: backs up data of a single or multiple files, instead of the entire cloud servers or on-premises hosts.

Vault

CBR stores backups in vaults. Before creating a backup, you need to create at least one vault and associate the resources you want to back up with the vaults. Then the resources can be backed up to the associated vaults.

Vaults can be either backup vaults or replication vaults. Backup vaults store resource backups, and replication vaults store backup replicas.

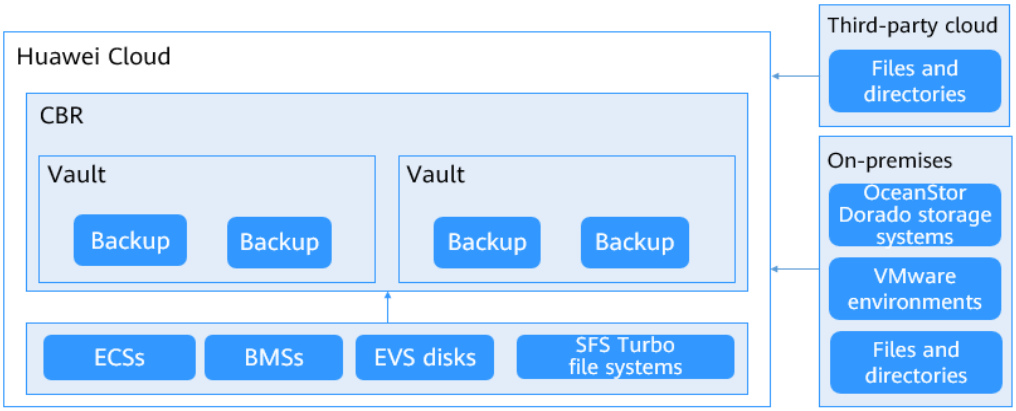
Different types of resources must be backed up to different types of vaults. For example, cloud servers must be backed up to server backup vaults, not disk backup vaults or any other types of vaults.

Policy

There are backup policies and replication policies.

- A backup policy defines when you want to take a backup and for how long you would retain each backup.
- A replication policy defines when you want to replicate from backup vaults and for how long you would retain each replica. Backup replicas are stored in replication vaults.

Figure 1-1 CBR architecture



Differences Among the Backup Types

Table 1-1 Differences among the backup types

Item	Cloud Server Backup	Cloud Disk Backup	SFS Turbo Backup	Hybrid Cloud Backup	File Backup
What to back up	All disks (system and data disks) on a server	One or more specific disks (system or data disks)	SFS Turbo file systems	Backups of on-premises hosts and VMs	A single or multiple files on cloud servers or on-premises hosts

Item	Cloud Server Backup	Cloud Disk Backup	SFS Turbo Backup	Hybrid Cloud Backup	File Backup
When to use	You want to back up entire cloud servers.	You want to back up only data disks.	You want to back up entire SFS Turbo file systems.	You want to manage backups of on-premises servers and restore data on the cloud.	You want to back up and restore a single or multiple files on the cloud.
Advantages	All disks on a server are backed up at a time.	Only data of specific disks is backed up, which costs less than backing up an entire server.	File system data and their backups are stored separately, and the backups can be used to create new file systems.	On-premises data can be backed up to the cloud and used to re-build services in the cloud.	You can back up data by file or directory, which is inexpensive than backing up an entire server or a disk.

Backup Mechanism

CBR in-cloud backup offers block-level backup, and CBR file backup provides file-level backup. The first backup is a full backup and backs up all used data blocks. For example, if a disk size is 100 GB and 40 GB has been used, only the 40 GB of data is backed up. An incremental backup backs up only the data changed since the last backup to save the storage space and backup time.

A backup will not be deleted if it is depended on by other backups, ensuring that other backups can still be used for restoration. Both a full backup and an incremental backup can be used to restore data to a given backup point in time.

When creating a backup of a disk, CBR also creates a snapshot for it. CBR keeps only the latest snapshot. Every time it creates a new snapshot during backup, it deletes the old snapshot.

CBR stores backups in OBS to ensure data security.

Backup Options

CBR supports one-off backup and periodic backup. A one-off backup is manually created and is executed only once. Periodic backup tasks are automatically executed based on a user-defined backup policy.

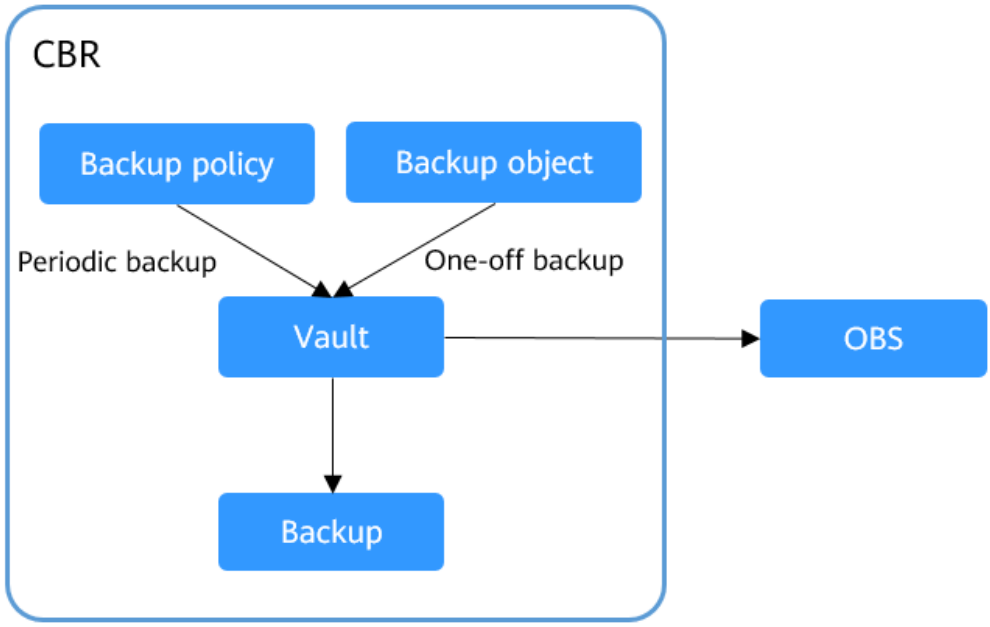
Table 1-2 compares the two backup options.

Table 1-2 One-off backup and periodic backup

Item	One-Off Backup	Periodic Backup
Backup policy	Not required	Required
Number of backup tasks	One manual backup task	Periodic tasks triggered by a preset backup policy
Backup name	User-defined backup name, which is **manualbk**_*xxxx* by default	System-assigned backup name, which is **autobk**_*xxxx* by default
Backup mode	The first backup is a full backup and the consecutive backups are incremental.	The first backup is a full backup and the consecutive backups are incremental.
Application scenario	Executed before patching or upgrading the OS or upgrading an application. A one-off backup can be used for restoration if the patching or upgrading fails.	Executed for routine maintenance. The latest backup can be used for restoration if an unexpected failure or data loss occurs.

You can also use the two backup options together if needed. For example, you can associate resources with a vault and apply a backup policy to the vault to execute periodic backup for all the resources in the vault. Additionally, you can perform a one-off backup for the most important resources to enhance data security. **Figure 1-2** shows the use of the two backup options.

Figure 1-2 Use of the two backup options



Access to CBR

You can access the CBR service through the console or by calling HTTPS-based APIs.

- Console

  Use the console if you prefer a web-based UI. Log in to the console and choose **Cloud Backup and Recovery**.

- APIs

  Use APIs if you need to integrate CBR into a third-party system for secondary development. For details, see the **Cloud Backup and Recovery API Reference**.

2 Advantages

Reliable

CBR offers crash-consistent backup for multiple disks on a server and application-consistent backup for database servers. The backups protect against human errors, virus attacks, and natural disasters, and ensure your data security and reliability.

Efficient

Incremental forever backups shorten the time required for backup by 95%. With Instant Restore, CBR offers an RPO of as low as 1 hour and an RTO of only several minutes.

NOTE

Recovery Point Objective (RPO) specifies the maximum acceptable period in which data might be lost.

Recovery Time Objective (RTO) specifies the maximum acceptable amount of time for restoring the entire system after a disaster occurs.

Easy to Use

CBR is easier to use than conventional backup systems. You can complete backup in just three steps, and no professional backup skills are required.

Secure

If the disks are encrypted, their backups are also encrypted to ensure data security. You can also replicate backups across regions to implement remote disaster recovery.

3 Application Scenarios

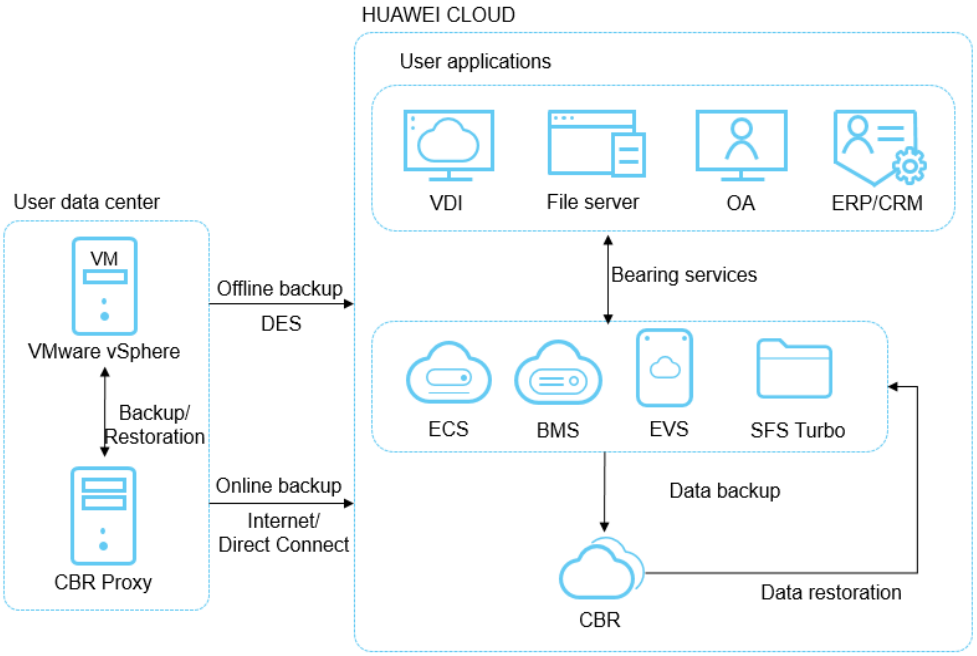
CBR is ideal for data backup and restoration. The backups can maximize your data security and consistency.

Data Backup and Restoration

You can use CBR to quickly restore data to the latest backup point if any of the following incidents occur:

- Hacker or virus attacks
- Accidental deletion
- Application update errors
- System breakdown

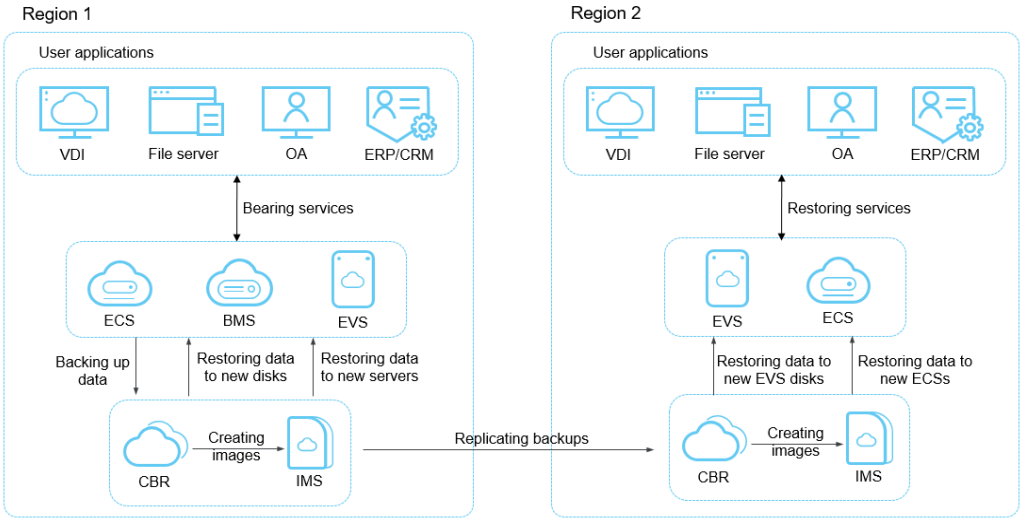
Figure 3-1 Data backup and restoration



Rapid Migration & Deployment

You can use cloud server backups to create images and then use such images to quickly provision new cloud servers with the same configuration as existing ones. See **Figure 3-2**.

Figure 3-2 Rapid service migration and deployment



4 Functions

Table 4-1 lists the functions of CBR.

Before using CBR functions, it is recommended that you learn about **basic CBR concepts**.

Table 4-1 CBR functions

Category	Function	Description
Cloud disk backup	**Manual disk backup**	Cloud disk backup provides snapshot-based backup for EVS disks on servers. You can back up specific disks to protect data on them.
	Policy-based backup	You can create, modify, or delete a backup policy. A backup policy defines the schedule and retention for automatic backups.
	Backup management	You can set search criteria to quickly find the backups you want to manage. Then you can view their details, share, restore, or delete them if needed.
	Disk restoration using backups	When a disk is faulty, or their data is lost, you can use a backup to quickly restore the data.
	Disk creation using backups	You can use a disk backup to create a disk that contains the same data as the backup.
	Backup sharing	You can share a disk backup with other accounts to allow them to use the backup to create disks.

Category	Function	Description
Cloud server backup	**Manual server backup**	Cloud server backup uses the consistency snapshot technology to protect data of ECSs and BMSs. You can use CBR to back up an entire server to protect their data, especially when high data consistency is required, such as in RAID clusters.
	Backup of specific disks on a server	You can create a single backup for multiple disks on a server to save the vault space.
	Policy-based backup	You can create, modify, or delete a backup policy. A backup policy defines the schedule and retention for automatic backups.
	Backup management	You can set search criteria to quickly find the backups you want to manage. Then you can view their details, share, restore, replicate, or delete them if needed.
	Server restoration using backups	When a server is faulty, or their data is lost, you can use a backup to quickly restore the data.
	Backup sharing	You can share a server backup with other accounts to allow them to use the backup to create servers.
	Image creation using server backups	You can create images from ECS backups and then use the images to quickly provision ECSs to restore service.
	Database server backup	Cloud server backup supports application-consistent backup in addition to crash-consistent backup. You can use cloud server backup to back up ECSs running MySQL or SAP HANA databases, because application-consistent backup ensures that the backed-up data is transactionally consistent.

Category	Function	Description
	Cross-region replication	You can replicate backups from one region to another and then use the replicas in the destination region to create images and provision servers.
SFS Turbo backup	Manual SFS Turbo file system backup	You can back up SFS Turbo file systems and use the backups create new SFS Turbo file system.
	Policy-based backup	You can create, modify, or delete a backup policy. A backup policy defines the schedule and retention for automatic backups.
	Backup management	You can set search criteria to quickly find the backups you want to manage. Then you can view their details, share, restore, replicate, or delete them if needed.
	File system creation using backups	You can use an SFS Turbo file system backup to create a file system that contains the same data as the backup.
	Cross-region replication	You can replicate backups from one region to another and then use the replicas in the destination regions to create file systems.
Hybrid cloud backup	Synchronization of on-premises server backups to the cloud	If an on-premises VMware VM has been backed up offline and the backups has been uploaded to an OBS bucket, you can synchronize the backups from the OBS bucket to a hybrid cloud backup vault for disaster recovery.
	Server restoration using backups	You can use the backups in the hybrid cloud backup vault to restore data to cloud servers for disaster recovery, service migration, development, and testing.
File backup	File backup	You can back up files and directories on your cloud servers and on-premises hosts, instead of backing up the entire servers or disks.

Category	Function	Description
	Data restoration using backups	If data of a file is lost due to accidental deletion or virus attack, you can use the backups to restore the data.

5 Security

5.1 Shared Responsibilities

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

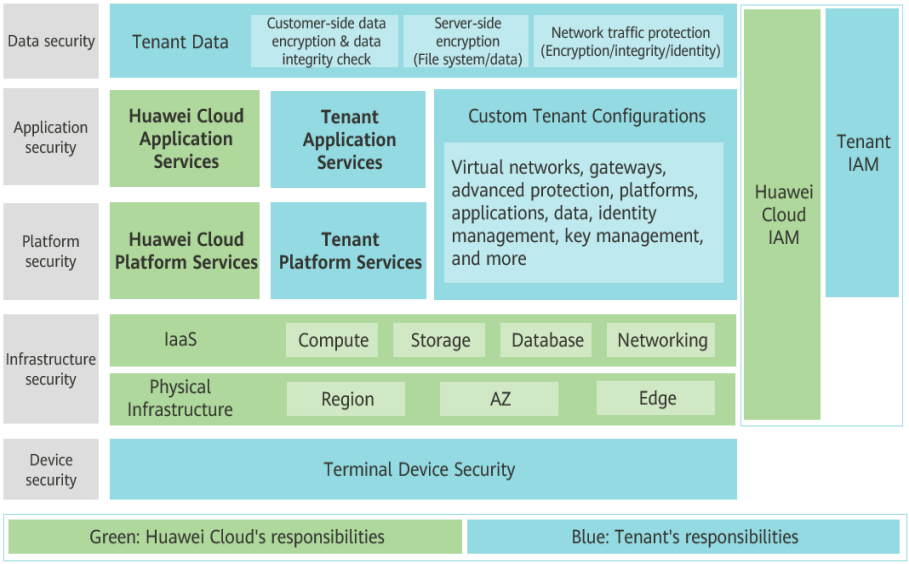
Figure 5-1 illustrates the responsibilities shared by Huawei Cloud and users.

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

guests, virtual firewalls, API Gateway, advanced security services, all types of cloud services, tenant data, identity accounts, and key management.

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

Figure 5-1 Huawei Cloud shared security responsibility model



5.2 Identity Authentication and Access Control

You can access CBR through the CBR console, APIs, and SDKs. No matter which method you choose, you actually use REST APIs to access CBR.

CBR APIs support only authenticated requests. You must obtain the authentication information from Huawei Cloud IAM before you can access CBR. For details about IAM authentication, see **Authentication**.

5.3 Data Protection

CBR takes many measures to keep data secure and reliable.

Table 5-1 CBR data protection

Measure	Description
Transmission encryption (HTTPS)	To ensure the transmission security, backup data is stored to OBS buckets via HTTPS.

Measure	Description
Backup data encryption	If a disk you want to back up is encrypted, the backups generated for this disk will also be encrypted. When such a backup is used to restore data, the encrypted data will first be decrypted and then restored to the target disk.
Cross-region replication	Cross-region replication allows you to automatically and asynchronously replicate backups from one region to a replication vault in a different region based on a replication policy. The cross-region disaster recovery capabilities it offers can cater to your needs for remote backup.

5.4 Auditing and Logging

Auditing

Cloud Trace Service (CTS) records operations on the cloud resources in your account. You can use the logs generated by CTS to perform security analysis, track resource changes, audit compliance, and locate faults.

After you enable CTS and configure a tracker, CTS can record management and data traces of CBR for auditing.

For details about how to enable and configure CTS, see **CTS Getting Started**.

For the CBR management and data traces supported by CTS, see **Auditing**.

Logging

CBR shows tasks of critical operations on the web page. You can log in the CBR console, choose **Tasks** from the navigation page on the left, and view the task list in the right pane. Alternatively, you can **query the task list** via the API.

5.5 Resilience

CBR uses a multi-level reliability architecture and provides technical solutions, including cross-region replication, to guarantee data durability and reliability.

5.6 Risk Monitoring

Cloud Eye is a multi-dimensional monitoring platform that allows you to view the resource usages and service running status, and respond to exceptions in a timely manner for the smooth running of services.

CBR uses Cloud Eye to perform monitoring over resources and operations, helping you monitor your vaults and backups and receive alarms and notifications in real time. You can obtain your vault usage in real time and be notified for events, such as backup creation or deletion failures.

For details about supported CBR metrics and how to create alarm rules, see **Monitoring**.

5.7 Fault Recovery

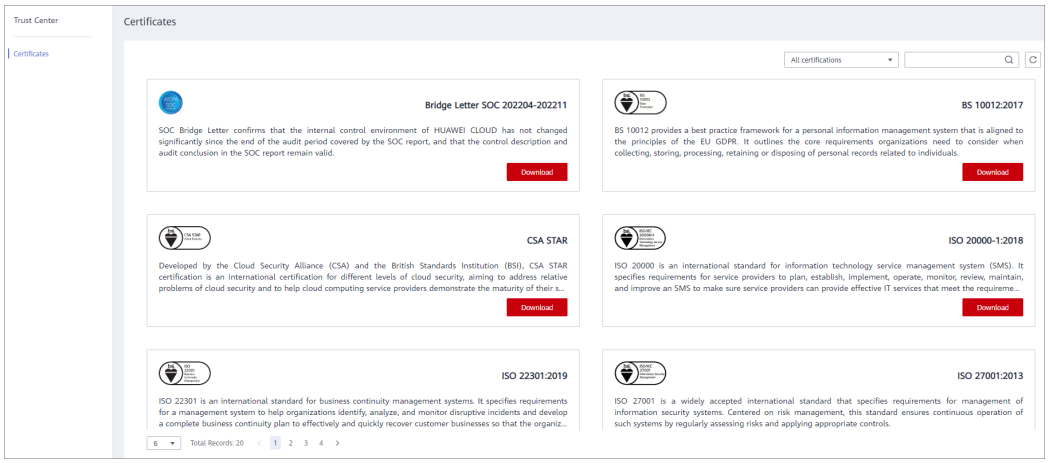
CBR allows you to back up and restore certain cloud resources, including ECSs, EVS disks, SFS Turbo file systems, and Workspace desktops. If any of these types of resources fail, you can use backups to restore to the source or new resources, thus quickly restoring data and services. For more information, see **Function Overview**.

5.8 Certificates

Compliance Certificates

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

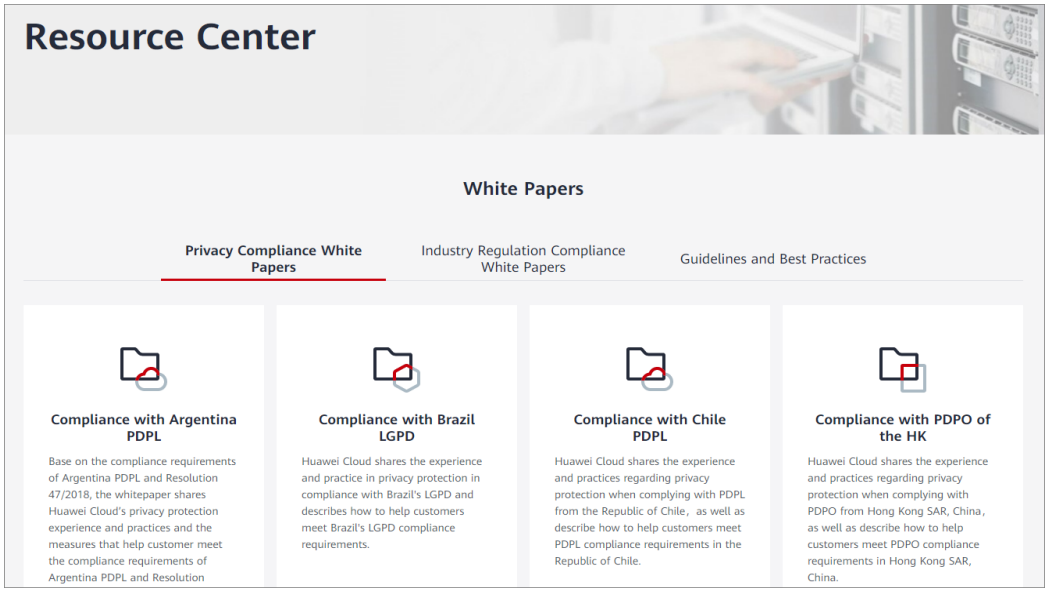
Figure 5-2 Downloading compliance certificates



Resource Center

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

Figure 5-3 Resource center



6 Billing

Billing Items

You are billed for the storage space and optionally the data traffic required for backup replication. Pricing of the storage space varies with vault types. See details in the following table.

Category	Billing Item	Description	Billing Mode
Storage space	Disk backup vault	If cloud disks need to be backed up, buy disk backup vaults to store the backups.	Pay-per-use Yearly/ Monthly
	Server backup vault	If cloud servers (without applications) need to be backed up, buy server backup vaults to store the backups.	Pay-per-use Yearly/ Monthly
	SFS Turbo backup vault	If SFS Turbo file systems need to be backed up, buy SFS Turbo backup vaults to store the backups.	Pay-per-use Yearly/ Monthly
	Database server backup vault	If cloud servers (with applications) need to be backed up, buy database server backup vaults to store the backups. You need to enable **Application-Consistent Backup** on the **Buy Server Backup Vault** page before using database server backup vaults. For more information, see **Application-Consistent Backup Overview**.	Pay-per-use Yearly/ Monthly
	Hybrid cloud backup vault	If backups of on-premises VMware VMs and OceanStor Dorado arrays need to be stored, buy hybrid cloud backup vaults.	Pay-per-use Yearly/ Monthly

Category	Billing Item	Description	Billing Mode
	Replication vault	If you need to replicate backups to another region, buy replication vaults in the destination region.	Pay-per-use Yearly/ Monthly
Data traffic	Outbound traffic over the Internet	If hybrid cloud backups on the cloud are used to restore data to on-premises IDCs, outbound traffic is charged.	Free for a limited time
	Cross-region replication traffic	If backups or vaults are replicated to another region, traffic for cross-region replication is charged for the source region.	Pay-per-use Yearly/ Monthly

NOTE

For more information, see **CBR pricing details**.

Billing Examples

Example 1

Purchase a pay-per-use vault for cloud servers without databases deployed:

If a user purchases a 400-GB server backup vault for their 100-GB cloud server in the CN-Hong Kong region, the user is billed for the 400-GB server backup vault in CBR.

Example 2

Purchase a pay-per-use vault for cloud servers with databases deployed:

If a user purchases an 800-GB database server backup vault for their 100-GB database server in the CN-Hong Kong region, and the user is billed for the 800-GB database server backup vault in CBR.

Example 3

Replicate a backup to another region:

If a user purchases a 100-GB server backup vault in the CN-Hong Kong region and a 200-GB replication vault in the AP-Bangkok region and replicates 40 GB of data from the vault in CN-Hong Kong to the vault in AP-Bangkok, the user is billed for the 100-GB backup vault, the 200-GB replication vault, and the traffic for replicating 40 GB of data.

Billing Modes

Two billing modes are available: pay-per-use and yearly/monthly. Select a billing mode that best suits your business needs.

- **Pay-per-use**

  You pay for the duration you use the resources. Prices are calculated by the hour, and no minimum fee is required.

- **Yearly/Monthly**

  Yearly/monthly is a prepaid billing mode. You are billed based on the subscription duration you specify. This mode is ideal when the resource use duration is predictable. A longer subscription often means a lower cost.

CBR also provides replication traffic packages for cross-region replication. If you do not have such a package, you will be billed per use.

For more information, see **CBR pricing details**.

Changing Billing Mode

- Yearly/monthly is a prepaid billing mode. You are billed based on the subscription duration you specify. This mode is ideal when the resource use duration is predictable. A longer subscription often means a lower cost.
- Pay-per-use is a postpaid billing mode. You are billed based on your resource usage and you can increase or delete resources any time.

If the resource use is stable, you can change a pay-per-use vault to a yearly/monthly vault to save more money. For details, see **Changing the Billing Mode from Pay-per-Use to Yearly/Monthly**.

Expiration

For details, see **Service Suspension and Resource Release**.

Renewal

Choose **More** > **Renew** in the **Operation** column of the yearly/monthly vault to renew your subscription. For more information about renewal, including auto-renewal, exporting the renewal history, and changing subscriptions, see **Renewal Management**.

Overdue Payment

Possible causes of overdue payment:

- The account balance is not enough after you buy a pay-per-use vault.
- Traffic fees generated during backup replication are greater than your account balance.

Service status and operation restrictions when an account is in arrears:

In the retention period, your vaults and backup data are retained. You can view existing backups but cannot create new backups or add tags. If you do not pay off the outstanding fees before the retention period expires, your data will be automatically released and cannot be restored. For how to repay arrears, see **Top-Up and Repayment**.

For details about the retention period, see **Service Suspension and Resource Release**.

7 Permissions Management

If you need to assign different permissions to employees in your enterprise to control their access to your CBR resources on Huawei Cloud, 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 for your employees, and assign permissions to them to control their access to specific resource types. For example, you can create IAM users for software developers and grant them only the permissions required for using CBR resources to allow them to use CBR resources but prevent them from performing any other operations.

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

IAM is free of charge. For more information about IAM, see **IAM Service Overview**.

CBR Permissions

By default, new IAM users do not have permissions assigned. You need to add an IAM 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.

CBR is a project-level service deployed and accessed in specific physical regions. To assign CBR permissions to a user group, specify the scope as region-specific projects and select projects for the permissions to take effect. If **All projects** is selected, the permissions will take effect for the user group in all region-specific projects. When accessing CBR, the users need to switch to a region where they have been authorized to use this service.

You can grant users permissions by using roles and policies.

- Roles: A type of coarse-grained authorization mechanism that defines permissions related to users responsibilities. Only a limited number of service-level roles for authorization are available. When using roles to grant permissions, you need to also 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. Most policies define permissions based on APIs. For the API actions supported by CBR, see **Permissions Policies and Supported Actions**.

Table 7-1 lists all the system-defined roles and policies supported by CBR.

Table 7-1 System-defined policies supported by CBR

Policy Name	Description	Type
CBR FullAccess	Administrator permissions for CBR. Users granted these permissions can operate and use all vaults, backups, and policies.	System-defined policy
CBR BackupsAndVaults-FullAccess	Common user permissions for CBR. Users granted these permissions can create, view, and delete vaults and backups, but cannot create, update, or delete policies.	System-defined policy
CBR ReadOnlyAccess	Read-only permissions for CBR. Users granted these permissions can only view CBR data.	System-defined policy

Table 7-2 lists the common operations supported by each system-defined policy or role of CBR. Select the policies or roles as required.

Table 7-2 Common operations supported by each system-defined policy or role of CBR

Operation	CBR FullAccess	CBR BackupsAndVaultsFullAccess	CBR ReadOnlyAccess
Querying vaults	√	√	√
Creating vaults	√	√	
Listing vaults	√	√	√
Updating vaults	√	√	
Deleting vaults	√	√	
Associating resources	√	√	
Dissociating resources	√	√	
Creating policies	√		

Operation	CBR FullAccess	CBR BackupsAndVaultsFullAccess	CBR ReadOnlyAccess
Updating policies	√		
Applying policies to a vault	√	√	
Removing policies from a vault	√	√	
Deleting policies	√		
Synchronizing backups	√	√	
Replicating vaults	√	√	
Performing backups	√	√	
Updating subscriptions	√	√	
Querying the Agent status	√	√	
Deleting backups	√	√	
Restoring data using backups	√	√	
Replicating backups	√	√	
Associating vaults	√	√	
Batch adding or deleting vault tags	√	√	
Adding vault tags	√	√	
Editing tags	√	√	

Helpful Links

- **IAM Service Overview**
- **Creating a User Group and User and Granting CBR Permissions**
- **Permissions Policies and Supported Actions**

8 Constraints

General

- A vault can be associated with only one backup policy.
- A vault can be associated with only one replication policy.
- A vault can be associated with a maximum of 256 resources.
- A maximum of 32 backup policies and 32 replication policies can be created.
- Only backups in the **Available** or **Locked** vaults can be used to restore data.
- Backups in a **Deleting** vault cannot be deleted.
- Backups cannot be downloaded to a local PC or uploaded to OBS.
- A vault and its associated servers or disks must be in the same region.
- Concurrent data restoration is not supported.

Cloud Disk Backup

- Only disks in the **Available** or **In-use** state can be backed up.
- Frozen disks in the retention period cannot be backed up.
- A new disk must be at least as large as the backup's source disk.
- Cloud disk backups cannot be replicated to other regions.

Cloud Server Backup

- A maximum of 10 shared disks can be backed up with a cloud server.
- Only backups in the **Available** or **Locked** vaults can be used to create images and be replicated to different regions.
- Frozen servers in the retention period cannot be backed up.
- Cloud servers support crash-consistent backup, whereas database servers support application-consistent backup in addition to crash-consistent backup.
- You can back up specific disks on a server, but such a backup must be restored as a whole. File- or directory-level restoration is not supported.
- Images cannot be created from backups if the amount of resources associated with a server backup vault exceeds the quota.
- You are advised not to back up a server whose disk size exceeds 4 TB.

- Backups can be replicated only to regions that have replication capabilities.
  - A backup can be replicated only when it meets all of the following conditions:
    i. It is an ECS backup.
    ii. It contains system disk data.
    iii. It is in the **Available** state.
  - Only backups can be replicated. Backup replicas cannot be replicated again but can be used to create images.
  - A backup can be replicated to multiple regions but can have only one replica in each destination region. The replication rule varies with the replication method:
    - Manual replication: A backup can be replicated to the destination region as long as it has no replica in that region. A backup can be replicated again if its replica in the destination region has been deleted.
    - Policy-driven replication: Once a backup has been successfully replicated to the destination region, it cannot be replicated to that region again, even if its replica has been deleted.
  - Only regions with replication capabilities can be selected as destination regions.

SFS Turbo Backup

- Only file systems in the **Available** state can be backed up.
- An SFS Turbo file system backup cannot be used to restore data to the original file system.
- Backups can be replicated only to regions that have replication capabilities.
  - A backup can be replicated only when it meets all of the following conditions:
    i. It is generated for an SFS Turbo file system.
    ii. It is in the **Available** state.
  - Only backups can be replicated. Backup replicas cannot be replicated again but can be used to create SFS Turbo file systems.
  - A backup can be replicated to multiple regions but can have only one replica in each destination region. The replication rule varies with the replication method:
    - Manual replication: A backup can be replicated to the destination region as long as it has no replica in that region. A backup can be replicated again if its replica in the destination region has been deleted.
    - Policy-driven replication: Once a backup has been successfully replicated to the destination region, it cannot be replicated to that region again, even if its replica has been deleted.
  - Only regions with replication capabilities can be selected as destination regions.

Hybrid Cloud Backup

- Backups synchronized to the cloud cannot be used to create cloud servers.
- Storage backups can only be restored to data disks on cloud servers.

File Backup

- Before backing up a file, ensure that the file is not being used or changed by an application, and the backup client has the read permissions on this file. Otherwise, the backed-up data will be incomplete.
- Before backing up a file, ensure that the file is not being used or changed by a process, and the backup client has the read permissions on this file. Otherwise, the backed-up data will be incomplete.
- You are advised not to restore file backups when applications are running. Stop the applications and then restore files.
- One backup client can have a maximum of 8 files and directories added.
- Each resource can only have one Agent installed.
- The number of resources where the Agent can be installed is not limited.
- It is recommended that one directory contains no more than 500,000 files.
- One path can contain a maximum of 200 characters.
- The maximum bandwidth allowed for file backup data transmission is 16 Gbit/s. If the maximum bandwidth is reached, flow control will be triggered.
- File backup cannot back up the files stored in SFS file systems that are mounted to cloud servers.
- Backup may fail on directories with frequent file writes in Windows.

9 CBR and Other Services

CBR-related Services

Table 9-1 CBR-related services

Function	Related Service	Reference
CBR backs up data of an ECS and uses the backup to restore data for the ECS. You can also create images from ECS backups and use the images to quickly provision ECSs to restore services.	ECS	**Creating a Cloud Server Backup** **Creating a Cloud Disk Backup**
CBR backs up data of a BMS and uses the backup to restore data for the BMS. The backup and management processes for BMSs and ECSs are the same.	BMS	**1 What Is CBR?** **Creating a Cloud Server Backup**
CBR backs up data of SFS Turbo file systems and uses the backup to create new file systems to restore lost or corrupted data.	SFS	**Creating an SFS Turbo Backup**
CBR stores backups securely in OBS.	OBS	**1 What Is CBR?**
CBR backs up data of EVS disks and uses the backup to create new disks.	EVS	**Creating a Cloud Disk Backup**
Cloud Trace Service (CTS) records operations on CBR resources, facilitating future queries, audits, and backtracking.	CTS	**Auditing**

Function	Related Service	Reference
Data Express Service (DES) allows you to easily migrate massive amount of data to the cloud. After a VMware VM is backed up on-premises, you can use DES Teleports or disks to transmit the backup data to an OBS bucket. Then you can synchronize the backup data from the OBS bucket to a CBR vault.	DES	**Creating a Storage Unit**
IAM is a self-service system for enterprise administrators to manage cloud resources. It provides user identity management and access control functions. When multiple users within an enterprise need to use CBR, the enterprise administrator can use IAM to create IAM users and control these users' access to CBR resources.	IAM	**7 Permissions Management**
Tag Management Service (TMS) enables you to add preset tags to CBR vaults to facilitate vault management.	TMS	**Managing Vault Tags**

10 Basic Concepts

10.1 CBR Concepts

Vault

CBR stores backups in vaults. Vaults can be either backup vaults or replication vaults.

- Backup vaults store backups of a variety of resources, including servers and disks, and are classified into the following types:
  - **Server backup vaults**: store backups of non-database servers or database servers. You can associate servers with a server backup vault and apply a backup or replication policy to schedule automatic backups or replications.
  - **Disk backup vaults**: store only disk backups. You can associate disks with a disk backup vault and apply a backup policy to schedule automatic backups.
  - **SFS Turbo backup vaults**: store only backups of SFS Turbo file systems. You can associate file systems with an SFS Turbo backup vault and apply a backup policy to schedule automatic backups.
  - **Hybrid cloud backup vaults**: store backups synchronized from the on-premises OceanStor Dorado storage systems and VMware VMs. You can replicate backups to a replication vault in a different region and restore data to other servers. Hybrid cloud backup vaults can also store backups of files and directories on your cloud servers and on-premises hosts.
- Replication vaults store replicas of backups for non-database servers and database servers. Such replicas cannot be replicated again.

Backup

A backup is a copy of a particular chunk of data and is usually stored elsewhere so that it may be used to restore the original data in the event of data loss. It can be generated either manually by a one-off backup task or automatically by a periodic backup task.

A one-off backup task is manually created and is executed only once. Periodic backup tasks are automatically executed based on a user-defined backup policy.

- A one-off backup is named **manualbk**_*xxxx* and can be user- or system-defined.
- A periodic backup is named **autobk**_*xxxx* by CBR.

Backup Policy

A backup policy is a set of rules that define the schedule and retention of backups. After you apply a backup policy to a vault, CBR automatically backs up data and retains backups based on that backup policy.

Replication

Replication is the process of replicating backups from one region to another. You can use the replicas in the destination region to create images and provision servers.

You can manually replicate a single cloud server backup or a hybrid cloud backup. You can also configure replication rules in a policy to periodically replicate backups, including those auto-generated, have not been replicated, or failed to be replicated to the destination region.

For example, if you want to back up a server, select **Backup** for the vault protection type. If you want to replicate backups of this server to a different region, select **Replication** for the vault in this different region.

Instant Restore

Instant Restore restores data and creates images from backups, much faster than a normal restore.

Instant Restore is an enhanced function of CBR and requires no additional configuration. After Instant Restore is provided, you take less time to restore server data or create images.

Enhanced Backup

Enhanced backups are backups generated after Instant Restore is provided. Enhanced backups make it faster to restore server data or create images.

Before providing Instant Restore, CBR generates common backups. After providing Instant Restore, CBR first performs a full backup for each associated resource and then generates enhanced backups. CBR only generates enhanced backups currently.

For the same resource, an enhanced backup and a common backup have the same backup content and size. They only differ in the restoration speed.

Application-Consistent Backup

There are three types of backups in terms of backup consistency:

- Inconsistent backup: An inconsistent backup contains data taken from different points in time. This typically occurs if changes are made to your files or disks during the backup.
- Crash-consistent backup: A crash-consistent backup captures all data on disks at the time of the backup and does not capture data in memory or any pending I/O operations. Although it cannot ensure application consistency, disks are checked by **chkdsk** upon operating system restart to restore damaged data and undo logs are used by databases to keep data consistent.
- Application-consistent backup: An application-consistent backup captures data in memory or any pending I/O operations and allows applications to achieve a quiescent and consistent state.

CBR cloud server backup supports both crash-consistent backup and application-consistent backup (also called database server backup). Install the Agent before enabling application-consistent backup to prevent the database server backup from failing.

Periodic Full Backup

CBR by default performs a full backup for a resource in the initial backup and incremental backups in all subsequent backups.

CBR now allows for periodic full backups in addition to the initial backup. You can configure a policy to perform a full backup after every N incremental backups. This further improves backup data security and meets periodic full backup needs.

Periodic full backups occupy more storage space than incremental backups.

10.2 Project and Enterprise Project

Project

A project is used to group and isolate OpenStack resources, such as the compute, storage, and network resources. A project can be a department or a project team. Multiple projects can be created for one account.

Enterprise Project

An enterprise project manages multiple resource instances by category. Resources and projects in different cloud service regions can be classified into one enterprise project. An enterprise can classify resources based on department or project group and put relevant resources into one enterprise project for management. Resources can be migrated between enterprise projects.

10.3 Region and AZ

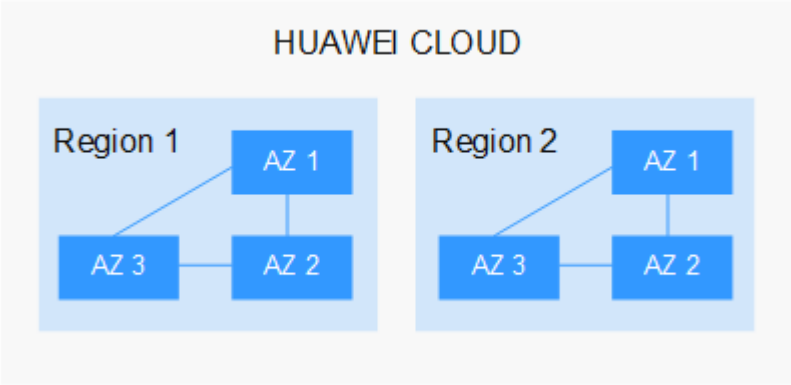
Concept

A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- Regions are divided based on geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified into universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides specific services for specific tenants.
- An AZ contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Within an AZ, computing, network, storage, and other resources are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers, to support cross-AZ high-availability systems.

Figure 10-1 shows the relationship between regions and AZs.

Figure 10-1 Regions and AZs



HUAWEI CLOUD provides services in many regions around the world. Select a region and AZ based on requirements. For more information, see **Huawei Cloud Global Regions**.

Selecting a Region

When selecting a region, consider the following factors:

- Location

  It is recommended that you select the closest region for lower network latency and quick access. Regions within the Chinese mainland provide the same infrastructure, BGP network quality, as well as resource operations and configurations. Therefore, if your target users are on the Chinese mainland, you do not need to consider the network latency differences when selecting a region.

  - If your target users are in Asia Pacific (excluding the Chinese mainland), select the **CN-Hong Kong**, **AP-Bangkok**, or **AP-Singapore** region.
  - If your target users are in Africa, select the **AF-Johannesburg** region.
  - If your target users are in Latin America, select the **LA-Santiago** region.

    NOTE

    The **LA-Santiago** region is located in Chile.

- Resource price

  Resource prices may vary in different regions. For details, see **Product Pricing Details**.

Selecting an AZ

When deploying resources, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs within the same region.
- For lower network latency, deploy resources in the same AZ.

Regions and Endpoints

Before you use an API to call resources, specify its region and endpoint. For more details, see **Regions and Endpoints**.

11 Change History

Released On	Description
2022-07-20	This issue is the sixth official release. Updated the following content: Added the content of file backup.
2021-10-27	This issue is the fifth official release. Updated the following content: Added the content of permissions management.
2020-08-07	This issue is the fourth official release. Updated the following content: Added the description of overdue payment in section "Billing."
2020-04-08	This issue is the third official release. Updated the following content: Added the content of file system backup.
2020-03-31	This issue is the second official release. Updated the following content: Added section "Billing."
2019-07-31	This issue is the first official release.

