Cloud Server Backup Service

User Guide

Issue 02

Date 2025-11-24

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Contents

1 What Is CSBS?

This service is available only for users and projects where this service has already been used. If you are new to Huawei Cloud, go to the console of the next-generation service, Cloud Backup and Recovery (CBR), which integrates Cloud Server Backup Service (CSBS).

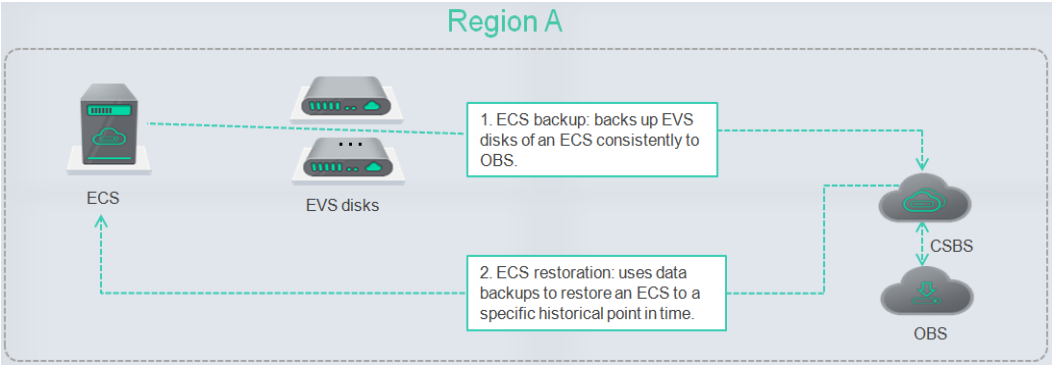
Cloud Server Backup Service (CSBS) enables you to back up Elastic Cloud Servers (ECSs). It works based on the consistency snapshot technology for disks. With CSBS, you can seamlessly use backup data to restore ECS data.

CSBS enhances data integrity and service continuity. For example, if an ECS is faulty or a misoperation causes data loss, you can use data backups to restore data quickly.

By default, CSBS executes a full backup for an ECS that has not been backed up, and performs incremental backups subsequently. Both full backup and incremental backup can restore an ECS to the state at the backup point in time.

CSBS works with ECS and OBS to back up ECS data to object storage, enhancing backup data security. **Figure 1-1** shows the CSBS product architecture.

Figure 1-1 CSBS product architecture



Main Functions

CSBS provides the following functions:

- ECS-based backup

- Policy-driven data backup
- Data backup management
- Image creation using backups

2 Application Scenarios

CSBS offers backup protection for ECSs. It supports crash-consistent backup, which enhances data security. CSBS can be used in the following scenarios:

- Hacker attacks and virus infection

  CSBS can restore an ECS to the latest backup point in time when the ECS has not been affected by hacker attacks and viruses.
- Accidental deletion

  CSBS can restore an ECS to the backup point in time prior to accidental deletion.
- Application update errors

  CSBS can restore an ECS to the backup point in time prior to application update.
- System breakdown

  CSBS can restore an ECS to the backup point in time prior to system breakdown.

3 Related Services

Table 3-1 Related services

Interactive Function	Related Service	Reference
CSBS can back up data of the EVS disks on an ECS, and use the backups to restore lost or corrupted data. Generated backups can be used to create images for fast restoring the service running environment.	Elastic Cloud Server (ECS)	**Creating a CSBS Backup**
CSBS combines ECS and OBS to back up ECS data to object storage, enhancing backup data security.	Object Storage Service (OBS)	**CSBS**
Cloud Trace Service (CTS) records operations of CSBS resources, facilitating query, audit, and backtracking.	Cloud Trace Service (CTS)	**Events**

Table 3-2 CSBS and VBS

Item	CSBS	VBS
Backup and restoration objects	All EVS disks (including system and data disks) on a single ECS	One or more specified EVS disks (system or data disks)

Item	CSBS	VBS
Recommended scenarios	An entire ECS needs to be protected. Use images created using backups to fast restore the service running environment.	Only data disks need to be backed up, because the system disk does not contain personal data.
Advantages	Consistency backup is supported. You can back up all EVS disks simultaneously, eliminating data inconsistency caused by backup time difference.	Backup cost is reduced while maintaining data security.

4 Basic Concepts

Backup Policies

A backup policy is a set of rules for backing up data, including the policy name, policy status, execution time of backup jobs, backup period, and retention rules. The retention rules specify the retention duration and number of retained backups. After an ECS is associated with a backup policy, it can be automatically backed up according to the backup policy.

Backup

A backup is a copy of the original data that is backed up. A backup is used to restore the original data. It can be generated in a one-off or periodic method.

CSBS supports one-off backup and periodic backup. A one-off backup job is manually created by users and takes effect for only one time. Periodic backup jobs are automatically driven by a user-defined backup policy.

- The name of a one-off backup is **manualbk**_*xxxx*. It can be user- or system-defined.
- The name of a periodic backup is assigned automatically by the system. The name of a periodic backup is **autobk**_*xxxx*.

Instant Restore

Instant Restore restores ECS data and creating images for backups, which is much faster than normal restoration.

Backups generated before Instant Restore is enabled do not support instant restoration. To use the feature, perform a full backup and select **Enable** next to **Full Backup** when creating the backup. For details, see . After Instant Restore is enabled, manual backups for ECSs that have not been backed up automatically support instant restoration, without requiring the selection of **Enable** next to **Full Backup**.

No matter whether an ECS has been backed up or not, its automatic backups generated after Instant Restore is enabled do not support instant restoration, unless you manually perform a full backup on it.

Application-Consistent Backup

There are three types of backup consistency:

- Inconsistent backup: Files and disks are backed up at different points in time.
- Crash-consistent backup captures data existing on disks upon backup and backs up files and disks at the same point in time, without backing up memory data and quieting application systems. Backup consistency of application systems is not ensured. Though the application consistency is not ensured, disks, such as **chkdsk**, will be checked upon operating system re-startup to restore damaged data and log rollback will be performed on databases to keep data consistent.
- Application-consistent backup backs up files and disks at the same point in time, including memory data, to ensure application system consistency.

Project

Projects are used to group and isolate OpenStack resources (computing, storage, and network resources). A project can be a department or a project team. Multiple projects can be created for one account.

5 Region and AZ

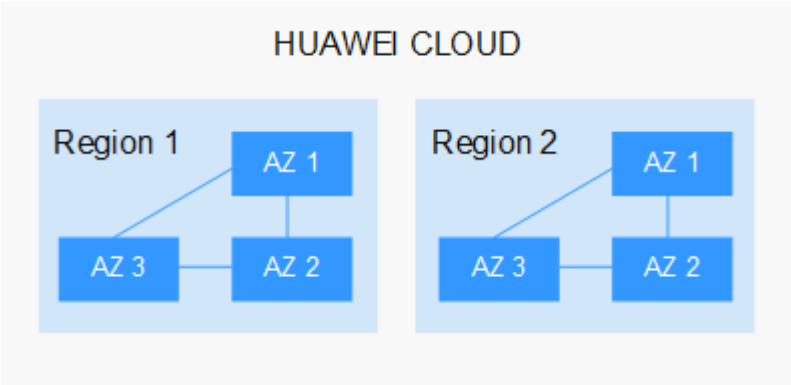
Concept

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.

Figure 5-1 shows the relationship between regions and AZs.

Figure 5-1 Regions and AZs



Huawei Cloud provides services in many regions around the world. You can select a region and an AZ based on requirements. For more information, see **Huawei Cloud Global Products and Services**.

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.

  - 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**.

6 Accessing and Using CSBS

6.1 How to Access CSBS

Web-based service management platforms, including HTTPS-based application programming interfaces (APIs) and the management console, are provided for you to access the CSBS service.

- APIs

  Use this access method if you are required to integrate the ECSs on the cloud service platform into a third-party system for secondary development. For detailed operations, see the *Cloud Server Backup Service API Reference*.

- Management console

  Use this access method if you do not need secondary development. If you already have a cloud service account, log in to the management console and click **Cloud Server Backup Service** on the homepage.

User Permissions

The public cloud system provides two types of user permissions by default: user management and resource management. User management refers to the management of users and user groups. Resource management refers to the control operations that can be performed by users on cloud service resources.

For details, see **System-defined Policies/Roles**.

6.2 Constraints and Limitations

Note the following constraints and limitations about CSBS:

- An ECS can be associated with only one backup policy.
- An ECS with shared EVS disks cannot be backed up using CSBS.
- CSBS supports crash-consistent backup of EVS disks on an ECS but not application-consistent backup of them.
- CSBS does not support consistent backup of multiple ECSs.

- CSBS supports backup and restoration of all EVS disks as a whole instead of part of the EVS disks on an ECS. In addition, CSBS does not support file- or directory-level restoration.

7 Permissions Management

If you want to assign different permissions to employees in your enterprise to access your CSBS resources purchased on Huawei Cloud, 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 CSBS resources but must not delete them or perform any high-risk operations. To achieve this result, you can create IAM users for the software developers and grant them only the permissions required for using CSBS resources.

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

IAM can be used free of charge. You pay only for the resources in your account. For more information about IAM, see **IAM Service Overview**.

CSBS Permissions

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.

CSBS is a project-level service deployed and accessed in specific physical regions. To assign CSBS permissions to a user group, specify the scope as region-specific projects and select projects (such as **ap-southeast-2**) 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 CSBS, the users need to switch to a region where they have been authorized to use this service.

Table 7-1 describes the system-defined role supported by CSBS. The role is dependent on other roles and needs to be used together with them to take effect.

Table 7-1 System-defined role supported by CSBS

Role/Policy Name	Description	Dependency
CSBS Administrator	CSBS administrator rights	This role is dependent on the **Server Administrator** role. • **Tenant Guest**: A global role, which must be assigned in the global project.

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

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

Operation	Server Administrator
Creating a backup	√
Deleting a backup	√
Using a backup to restore an ECS	√
Using backups to create images	√
Install Agent	√

Helpful Links

- IAM Service Overview
- Creating a User and Granting CSBS Permissions

8 Change History

Release Date	What's New
2019-02-23	This issue is the second official release. Modified the following content: Added content related to application-consistent backup.
2018-11-19	This issue is the first official release.

