Volume Backup Service(VBS)
8.3.0
User Guide

Issue	02
Date	2022-11-15

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.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://e.huawei.com

Contents

1 Quick Start 1
1.1 Introduction 1
1.2 Preparation 3
1.3 Logging In to the Cloud Backup Console 3
1.4 Backing Up EVS Disks 4
1.5 Restoring EVS Disks 12
2 User Guide 13
2.1 Introduction 13
2.1.1 What Is Volume Backup Service? 13
2.1.2 Advantages 15
2.1.3 Application Scenarios 15
2.1.4 Implementation Principles 16
2.1.5 Related Services 21
2.1.6 Key Metrics 22
2.1.7 Accessing and Using VBS 23
2.2 Related Concepts 23
2.2.1 Backup 23
2.2.2 Backup Policy 25
2.2.3 Incremental Backup 25
2.2.4 Full Backup 25
2.2.5 Replication 25
2.2.6 Backups and Replicas 25
2.3 Operation Process 25
2.4 Applying for Backup Space 29
2.5 Creating a Periodic Backup Task 30
2.5.1 Creating a Backup Policy 30
2.5.2 Creating a Backup Task 39
2.6 Manually Changing the Validity Period of a Backup 42
2.7 Executing a Backup Policy Manually 43
2.8 Executing a Replication Policy Manually 45
2.9 Restoring a Disk Using a Backup 46
2.9.1 Creating a Disk Using Backup Data 46
2.9.2 Restoring Backup Data to the Source EVS Disk 47

2.9.3 Restoring Backup Data to Another EVS Disk....48
2.10 Viewing the Overview Information....49
2.11 Managing Backups and Replicas....51
2.11.1 Viewing EVS Disk Backups and Replicas....51
2.11.2 Deleting an EVS Disk Backup or Replica....53
2.12 Managing Backup Policies....53
2.12.1 Editing a Backup Policy....53
2.12.2 Viewing a Backup Policy....54
2.12.3 Associating New EVS Disks with a Backup Policy....54
2.12.4 Disassociating EVS Disks from a Backup Policy....56
2.12.5 Changing a Policy....56
2.12.6 Deleting a Backup Policy....57
2.12.7 Changing the Validity Period of a Backup Policy....57
2.13 Managing Tasks....58
2.13.1 Viewing Tasks....58
2.13.2 Retrying a Task....61
2.13.3 Downloading Tasks....62
2.14 FAQs....62
2.14.1 Accessing the Volume Backup Service Console as a VDC Administrator or a VDC Operator....62
2.14.2 What Is the Difference Between Backup and Replication?....63
2.14.3 Does VBS Support Simultaneous Backup of Multiple EVS Disks on a Server?....63
2.14.4 Must I Stop the Server Before Backing Up EVS Disks on a Server Using VBS?....63
2.14.5 Does VBS Support Cross-region EVS Disk Backup and Restoration?....63
2.14.6 Must I Stop the Server Before Restoring EVS Disk Data with a VBS Backup?....63
2.14.7 Can a VBS Backup of a System Disk Be Used to Restore the System Disk of a Server?....64
2.14.8 Can I Use a VBS Backup to Restore an EVS Disk Whose Capacity Has Been Expanded?....64
2.14.9 Replication Space Cannot Be Released After the Intra-Region Replication Function Is Disabled....64

1 Quick Start

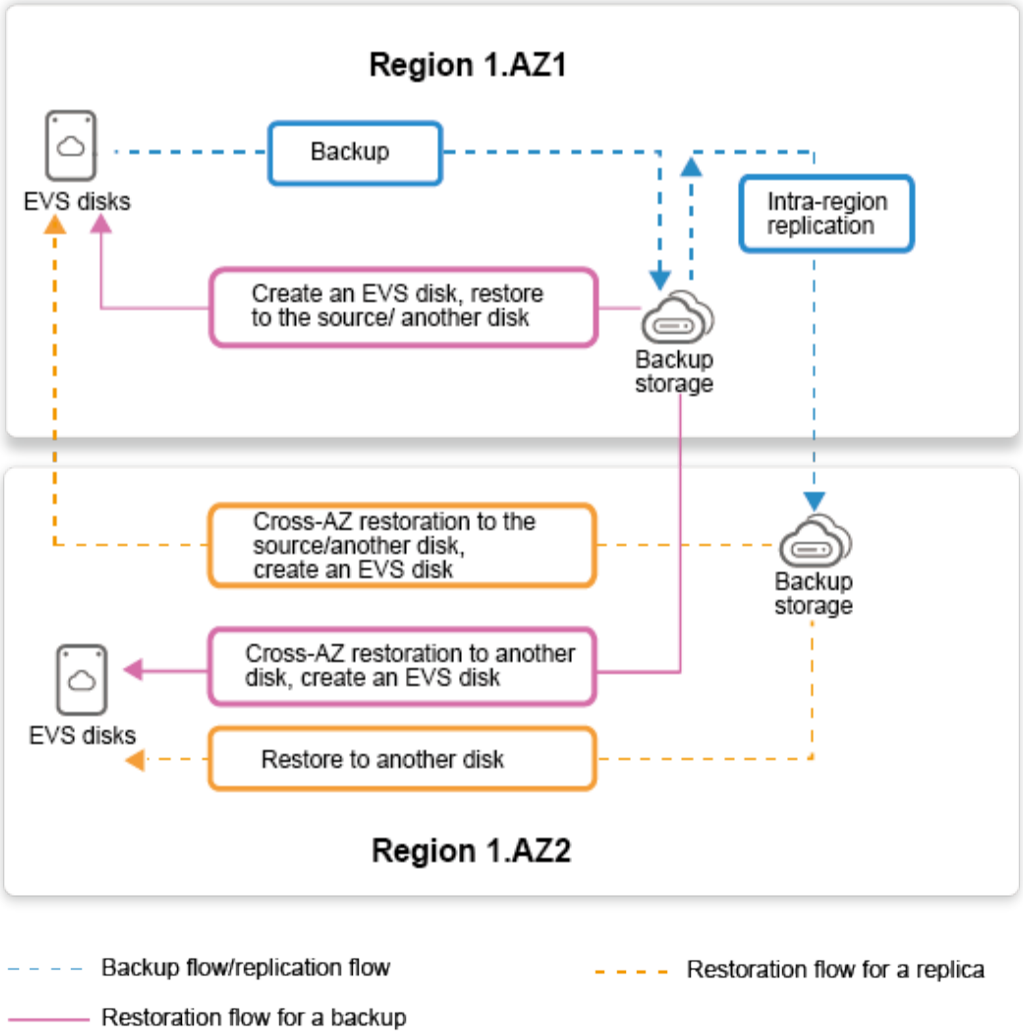
1.1 Introduction
1.2 Preparation
1.3 Logging In to the Cloud Backup Console
1.4 Backing Up EVS Disks
1.5 Restoring EVS Disks

1.1 Introduction

Volume Backup Service (VBS) creates backups of Elastic Volume Service (EVS) disks and allows for restoration from backups, ensuring data security and accuracy.

Figure 1-1 shows the service flow of VBS.

Figure 1-1 Service flow of VBS



The service flow of VBS is divided into two phases: backing up EVS disks and restoring EVS disks.

1. Backing Up EVS Disks
   a. Select EVS disks to be backed up.
   b. Create a backup policy and associate the selected EVS disks to the backup policy. If a backup policy has been configured, you can directly associate the selected EVS disks to the backup policy and do not need to create a backup policy.

NOTE

- Incremental backup policy: Backups start with a full backup. Subsequent backups only back up the data that has changed since the previous backup, which reduces the backup time and saves the backup space. You are advised to use the incremental backup for daily backups.
- Full backup policy: Full backup is performed for each backup. A full backup contains all data of the EVS disk. This backup mode saves more data restoration time. The shortcoming is that a full backup takes a long time and occupies a large space.
- Replication policy: Incremental backup copies and full backup copies are replicated to remote storage devices, improving the security of backup copies. Before configuring the replication policy, confirm that the availability zone (AZ) where the EVS disk resides supports intra-region replication. Otherwise, the policy cannot be configured.

c. The system executes the backup job based on the preset backup policy. Users can also manually execute backup policies to meet unplanned EVS data protection requirements.

2. Restoring EVS Disks
   a. Filter the existing backups and replicas of the EVS disk by disk name.
   b. Select a backup or replica of a specific time point and restore it to the source disk or another disk. You can also use the backup or replica to create a disk.
   c. After an EVS disk is restored, manually attach it to an ECS so that you have access to the data on the EVS disk.

For details about VBS, see *Volume Backup Service (VBS) 8.3.0 User Guide (for Huawei Cloud Stack 8.2.0*.

1.2 Preparation

Before using VBS, make the following preparations:

Obtain the VDC administrator or operator account. If no such account is available, contact the operation administrator to create a VDC and a VDC administrator, and then use the VDC administrator account to create a VDC operator.

For details, see **VDC Tenant Modeling** in ***Huawei Cloud Stack 8.2.0 Resource Provisioning Guide***.

1.3 Logging In to the Cloud Backup Console

Prerequisites

You have obtained a VDC administrator account or a VDC operator account.

Procedure

Step 1 Log in to ManageOne as a VDC administrator or a VDC operator using a browser.

Login address in non-B2B scenarios: https://*Address for accessing ManageOne Operation Portal*, for example, https://console.demo.com.

URL in the B2B scenario: https://*Address for accessing ManageOne Tenant Portal*, for example, https://tenant.demo.com.

URL: **https://***Floating IP address of ManageOne Operation Portal*:**443**

Step 2 Click ☰ in the upper left corner of the page, select a region and resource set and choose **Storage** > **Volume Backup Service**.

----End

1.4 Backing Up EVS Disks

Context

You are advised to set the backup policy as follows:

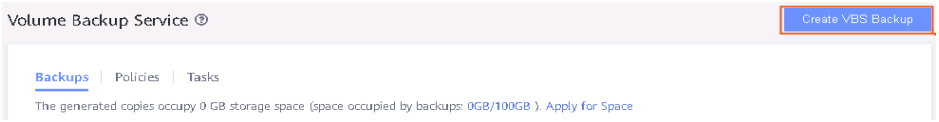
- If you need to back up data at a fixed time every week, for example, after work on Fridays, you are advised to select **By week** when creating a backup policy.
- If you need to back up data at a fixed time every month, for example, on the first day of each month, you are advised to select **By month** when creating a backup policy.
- If you need to back up data at a fixed time every year, for example, November 11, you are advised to select **By year** when creating a backup policy.
- If the backup period exceeds one week, for example, 10 days, you are advised to select **By day** when creating a backup policy.

Prerequisites

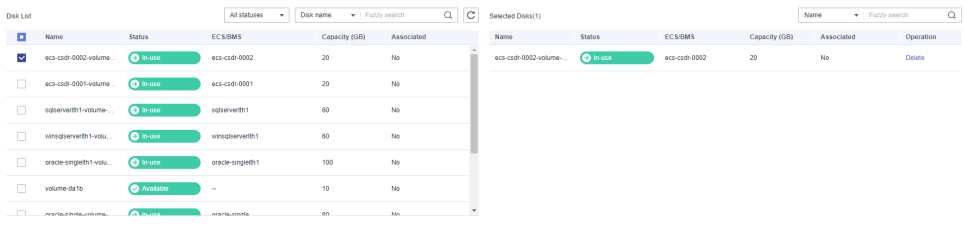
- You have obtained the username and password of a VDC administrator or a VDC operator.
- You have applied for the backup space. For details, see **2.4 Applying for Backup Space**.

Procedure

Step 1 **Access the console of Volume Backup Service**. Then click **Create VBS Backup** at the upper right corner.



Step 2 Specify the AZ where the EVS disks are located and select the EVS disks to be backed up.

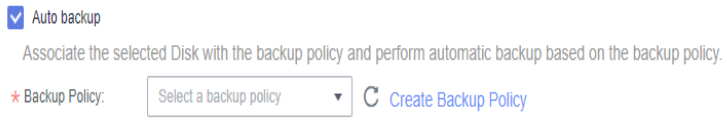


Step 3 Create a backup policy.

NOTE

If a proper backup policy has been created, skip this step and go to **Step 4**.

1. Click **Create Backup Policy**.



2. Set the basic information of the backup policy. **Table 1-1** describes related parameters.

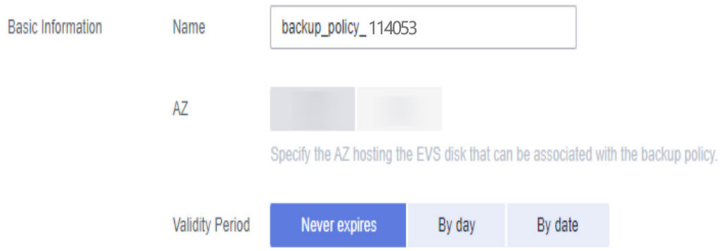


Table 1-1 Parameter description

Parameter	Description	Example Value
Name	Backup policy name It is a string of 1 to 255 characters containing only digits, letters, underscores (_), and hyphens (-).	backup_policy_114053
AZ	Only EVS disks in this AZ can be associated with the backup policy. After a backup policy is created, you cannot modify the AZ to which the backup policy belongs. After you select an AZ, only EVS disks in this AZ can be associated with the policy. If the selected AZ does not support replication, the replication policy cannot be configured.	Beijing
Validity Period	Policy validity period. A policy is effective only when it is within the validity period. You can change the validity period of a policy by referring to **2.12.7 Changing the Validity Period of a Backup Policy**. Possible values are **Never expires**, **By day**, and **By date**. **NOTE** The backup policy will expire at 23:59:59 on the expiration day. For example, if a backup policy is created at 23:30:00 on May 1, and the validity period is one day, it will expire at 23:59:59 on May 1.	Never expires

3. Set the incremental backup policy. **Table 1-2** describes related parameters.

Table 1-2 Parameter description

Parameter	Description	Example Value
Status	Incremental backup policy status – : enabled – : disabled The default **status** is .	
Backup Time	Time point for backing up the EVS disks that have been associated with the policy A maximum of 24 backup time points are allowed. The backup interval of all backup policies (including disabled backup policies) cannot be less than 1 hour. If the data backup time is longer than the interval between two backups, backup cannot be performed at a specified time. For example, if the backup time is set to 9:00, 10:00, and 11:00, the data backup time is 70 minutes each time. If the first backup starts at 9:00 and the backup is complete at 10:10. In this case, the preset backup will not be performed at 10:00 and the next backup will be performed at 11:00.	14:04

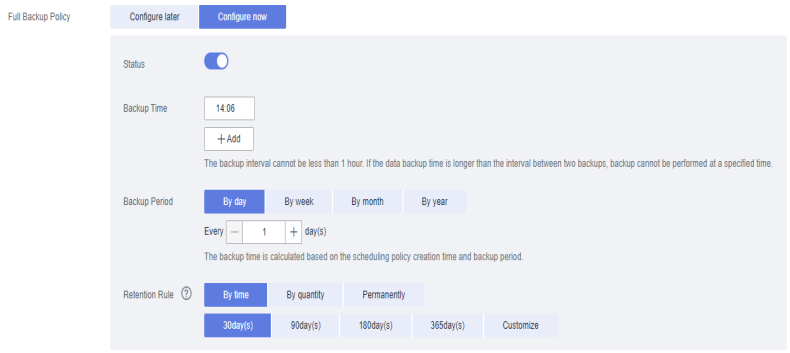
Parameter	Description	Example Value
Backup Period	Period for backing up the EVS disks that have been associated with the policy Example: – **By day**: The backup period can be set to 1 to 180 days. The backup time is calculated based on the scheduling policy creation time and the backup period. – **By week**: Specifies on which days of each week the backup job will be executed. – **By month**: Specifies on which days of each month the backup job will be executed. – **By year**: Specifies on which months and dates of each year the backup task will be executed. **NOTE** If a selected date does not exist in the current month, no backup will be generated at that day.	**By day**: Every day

Parameter	Description	Example Value
Retention Rule	Retention rule for the backups automatically generated according to the incremental backup policy. Backups that do not comply with the rule will be automatically deleted. **NOTE** – If copies are retained by time, the expiration time is displayed in the copy details. Copies that exceed the retention period are deleted based on the expiration time. – If backups are retained by quantity, the system checks the number of backups after each automatic backup is complete and automatically deletes the backups that are beyond the set quantity. – The more frequent the backup of an EVS disk, the more backups will be saved, the better the data will be protected, and the larger the storage space will be occupied. Determine the backup frequency based on the data importance and service volume. Perform relatively frequent backup operations for important data. – **By time**: The automatically generated backups are saved according to the set backup period. If backups violate the set period, they are automatically deleted. **By time** can be set to **30 days**, **90 days**, **180 days**, **365 days**, or **Custom**. **Customize** can be set to any value ranging from 1 to 99,999. – **By quantity**: The automatically generated backups are saved according to the set retention quantity. If backups violate the set quantity, they are automatically deleted. **By quantity** can be set to **30**, **90**, **180**, **365**, and **Customize**. **Customize** can be set to any value ranging from 1 to 99,999. For example, if **By quantity** is set to	By time: 30 days

Parameter	Description	Example Value
	30, each EVS disk associated with the policy can have up to 30 backups. – **Permanently**: All automatically generated backups are permanently saved. If you select **Permanently**, backups and replicas can only be manually deleted. Reserve sufficient space.	

4. Set the full backup policy.

   The parameter description of the full backup policy is similar to that of the incremental backup policy. You are advised to set **Option** to **Configure later**. You can modify the backup policy as required and enable the full backup policy. For details, see **2.12.1 Editing a Backup Policy**.



5. Set the replication policy.

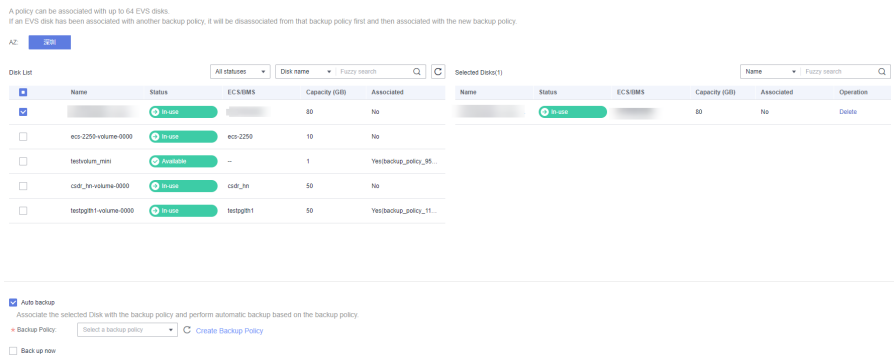
   For details about the parameters for the replication policy, see **Table 2-9**. You are advised to set **Option** to **Configure later**. You can modify the backup policy as required and enable the replication policy. For details, see **2.12.1 Editing a Backup Policy**.

   NOTE

   If the selected AZ does not support replication, the replication policy cannot be configured.

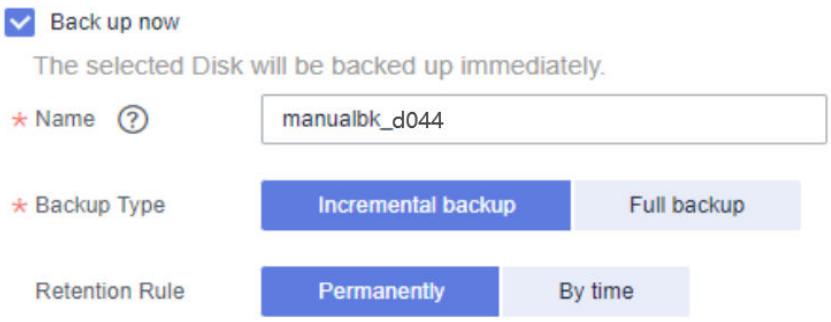
6. Click **OK**. The backup policy configuration is complete.
7. The system automatically refreshes and selects the newly created backup policy by default. Go to **Step 3.5**.

Step 4 Select the backup policy and associate the selected EVS disk to the backup policy.



Step 5 Configure **Back up now**.

After a VBS instance is created, the system immediately backs up the EVS disks in the instance.



1. Select **Back up now**.
2. Set the backup parameters. **Table 1-3** describes the parameters.

Table 1-3 Parameter description

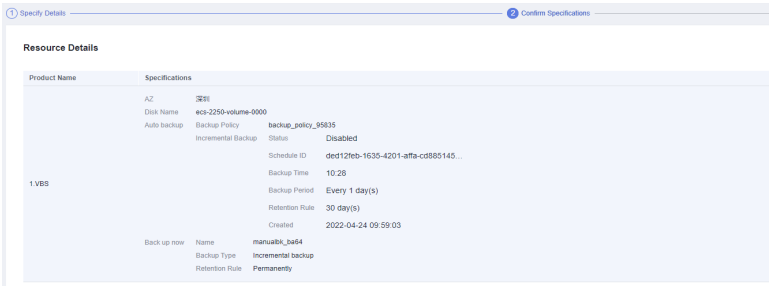
Parameter	Description	Example Value
Name	Name of the backup to be created. It is a string of 1 to 64 characters containing only digits, letters, underscores (_), and hyphens (-). **NOTE** You can use the default name, which defaults to **manualbk**_*xxxx*. When multiple ECSs are to be backed up, the system automatically adds suffixes to their names. For example, if the name is **manualbk_app** and two EVS disks are backed up, the names of the backup copies generated by the system are: **manualbk_app-0001** and **manualbk_app-0002**.	manualbk_d044
Backup Type	Incremental backup or full backup.	Incremental Backup

Parameter	Description	Example Value
Retention Rule	Retention rule for backups generated by **Back up now**. Backups that exceed the limit set in the retention rule will be automatically deleted. By default, backups are retained permanently. You can also set a retention period for backups generated by **Back up now**. Backups that exceed the set retention period will be automatically deleted. **By time** can be set to **30 days**, **90 days**, **180 days**, **365 days**, and **Customize**. **Customize** can be set to any value ranging from 1 to 99,999. **NOTE** If copies are retained by time, the expiration time is displayed in the copy details. Copies that exceed the retention period are deleted based on the expiration time.	Permanently

You can select both the backup modes at the same time. When both the backup modes are selected, backup will be performed immediately and periodic backups will be performed according to the backup policy subsequently.

Step 6 Click **Create Now**.

On the **Confirm Specifications** page that is displayed, confirm the detailed information and click **Submit**.



Step 7 Back to the **Backups** page as prompted.

Step 8 The system immediately backs up the EVS disk associated with the backup policy.

When the **Status** of the backup becomes **Available**, the backup is successful. The system periodically backs up the EVS disk based on the backup policy.

----End

1.5 Restoring EVS Disks

Prerequisites

- You have obtained a VDC administrator account or a VDC operator account.
- At least one backup is generated and its **Status** is **Available**.

Precautions

- Before restoring an EVS disk on an ECS, stop the ECS and detach the disk from the ECS. For details, see **Operation Help Center > Elastic Volume Service > User Guide (for ECS)** > **Releasing an EVS Disk > Detaching an EVS Disk**. After the restoration, attach the disk and start the ECS by referring to **Operation Help Center > Elastic Volume Service > User Guide (for ECS) > Attaching an EVS Disk**.
- Before restoring an EVS disk on a BMS, stop the BMS and detach the disk from the BMS. For details, see **Operation Help Center > Elastic Volume Service > User Guide (for BMS)** > **Releasing an EVS Disk > Detaching a Data Disk**. After the restoration, attach the disk and start the BMS by referring to **Operation Help Center > Elastic Volume Service > User Guide (for BMS) > Attaching an EVS Disk**.

Procedure

Step 1 Log in to the Cloud Backup Console. On the **Backups** tab page, filter out the EVS disk backups by **Disk name**.

Step 2 Choose **Restore** > **Source Disk** corresponding to the point-in-time backup.

NOTE

VBS allows you to restore data to **Source Disk**, **Another Disk**, or **Create Disk**. Restoring data to **Source Disk** is used as an example in this section. Select **Another Disk** or **Create Disk** as required. For details, see **2.9.3 Restoring Backup Data to Another EVS Disk** or **2.9.1 Creating a Disk Using Backup Data**.

Step 3 Click **OK** as promoted.

Step 4 Click the **Tasks** tab to view the restoration task status. If **Status** is **Succeeded**, the restoration is successful.

----End

2 User Guide

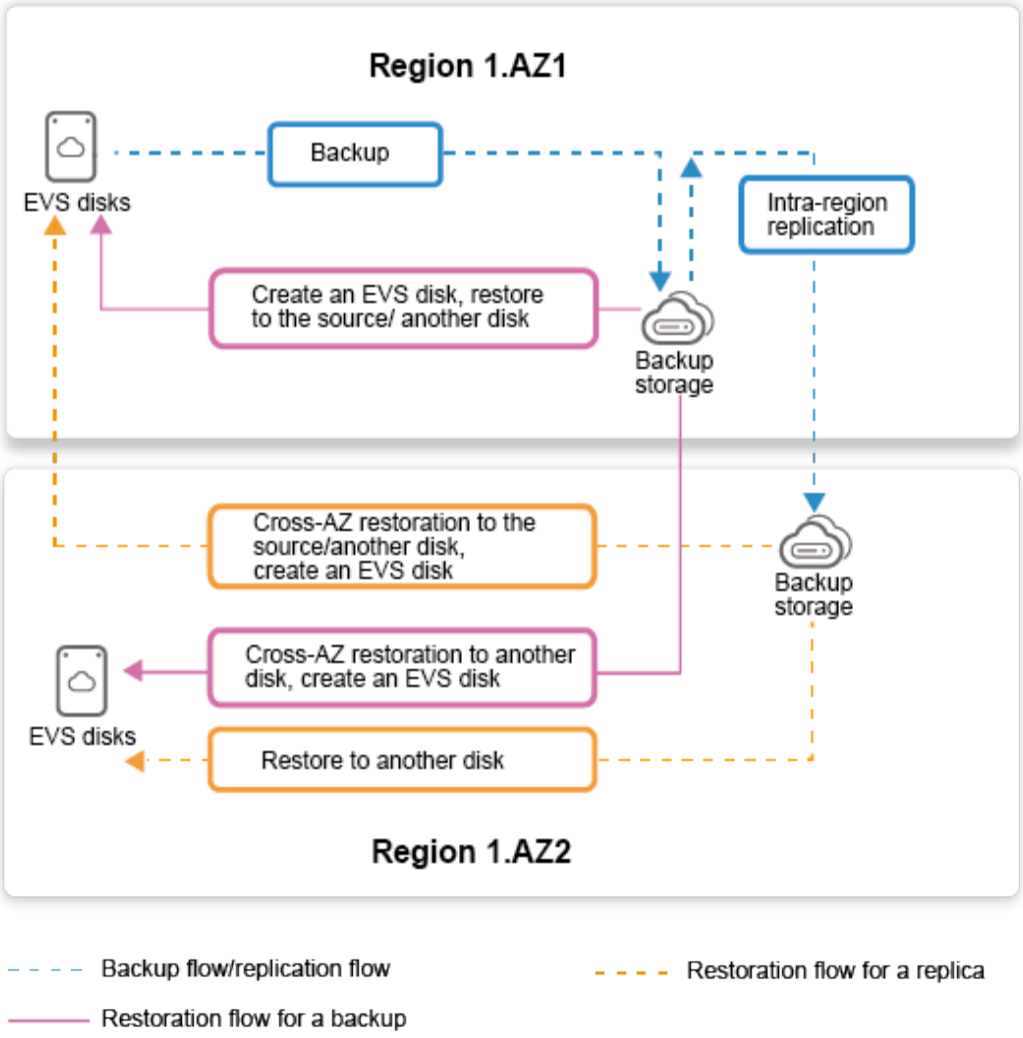
2.1 Introduction
2.2 Related Concepts
2.3 Operation Process
2.4 Applying for Backup Space
2.5 Creating a Periodic Backup Task
2.6 Manually Changing the Validity Period of a Backup
2.7 Executing a Backup Policy Manually
2.8 Executing a Replication Policy Manually
2.9 Restoring a Disk Using a Backup
2.10 Viewing the Overview Information
2.11 Managing Backups and Replicas
2.12 Managing Backup Policies
2.13 Managing Tasks
2.14 FAQs

2.1 Introduction

2.1.1 What Is Volume Backup Service?

Definition

Volume Backup Service (VBS) creates backups of Elastic Volume Service (EVS) disks and allows for restoration from backups, ensuring data security and accuracy.



Functions

VBS has the following functions:

- EVS disk backup
- Policy-driven data backup
- Backup data management
- Backup replication and saving
- EVS disk data restoration using backups or replicas
- EVS disk creation using backups or replicas
- Task management

Restrictions and Limitations

- The service only protects EVS disks created on ManageOne Operation Portal (ManageOne Tenant Portal in B2B scenarios).
- An EVS disk can be added to a VBS policy only.
- EVS disks cannot be restored in a batch.

- Concurrent backup on the same EVS disk is not supported.
- EVS disk-level restoration is supported and file- and directory-level restoration are not supported.
- Consistency backup of multiple EVS disks is not supported.
- It is not recommended to back up an EVS disk whose capacity exceeds 64 TB.
- Backups and intra-region replicas can be restored in any AZ in the region.
- If you want to restore an attached EVS disk, detach it before starting the restoration.
- EVS disk snapshots generated during backup will occupy space of the production storage. (The space occupied by the EVS disk snapshots is equal to the service change amount of the original EVS disk during the snapshot retention period.)
- If an EVS disk of a Windows ECS installed using the cloud-init image is restored to the system disk of a new ECS and the new ECS uses a key pair for authentication, you need to reset the password for logging in to the new ECS on the ECS console.
- Backup for the VMware EVS disks is not supported.

2.1.2 Advantages

VBS supports both full backup and incremental backup. If data is fully backed up by default in the first backup, incremental backups are performed subsequently. For both full and incremental backups, you can restore the data in EVS disks to the state when the backup was created.

VBS also supports replication of backups. If a backup is damaged, you can use its replica to restore data.

VBS is easy to use. You can perform backup and restoration for the EVS disks on the ECS/BMS (referred to as server in this document) with one click.

VBS has the following advantages:

- Ease-of-Use

  Backup can be configured in three steps and does not require elaborate planning. Compared with traditional backup services, VBS saves your efforts in planning and expanding servers and storage devices.
- Flexibility

  With different backup policies, backup can be automatically done to cover various backup scenarios. Permanent incremental backup, incremental restoration, and short backup window.
- Cost-Effectiveness

  Permanent incremental backup is used. The initial full backup backs up all data on the server. Subsequent backups are incremental, occupying a small amount of space.

2.1.3 Application Scenarios

Table 2-1 describes the VBS application scenarios.

Table 2-1 VBS application scenarios

Application Scenarios	Function
Hacker attacks and virus infection	VBS can restore EVS disks to the latest backup point in time when the server has not been affected by hacker attacks and viruses.
Mis-deletion	VBS can restore data to the backup point in time prior to the mis-deletion.
Application update errors	VBS can immediately restore the system to the latest backup time point before the application update to restore normal system operation.
Server breakdown	VBS can immediately restore the disk data before the system breaks down or restore the data to another disk.
Local AZ fault	The data can be restored in other AZs using replicas to restore the services quickly.

2.1.4 Implementation Principles

Logical Architecture

Figure 2-1 shows the logical architecture of VBS.

Figure 2-1 Logical architecture of VBS

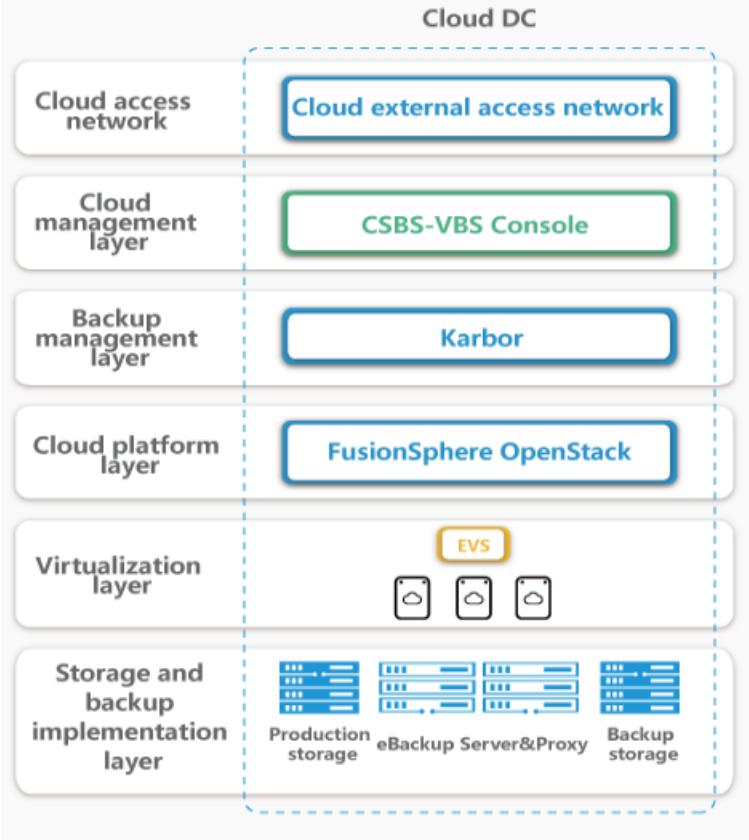


Table 2-2 describes the key components of VBS.

Table 2-2 Key components of VBS

Component	Function	Typical Deployment Principle
CSBS-VBS Console	Users can apply for VBS and back up and restore EVS disks on the Cloud Backup Console.	Deployed at the region layer. Backup service console is deployed on the static server of ManageOne. You do not need to apply for independent resources.
Karbor	Saves and schedules backup policies, and provides APIs for connecting to the cloud management platform.	Deployed in the region on three VMs. **NOTE** In the CSHA scenario, two nodes are deployed.
eBackup Driver	Used to communicate with the Cinder Driver of the FusionSphere OpenStack and eBackup Server&Proxy.	Deployed on the compute node and control node to which the backend storage (which can be backed up by eBackup) is connected.

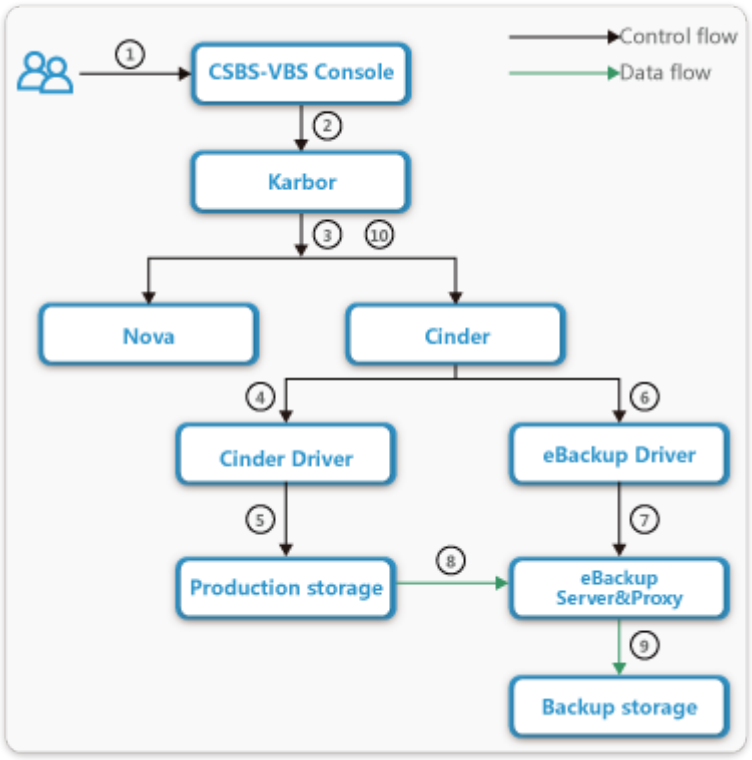
Component	Function	Typical Deployment Principle
eBackup Server&Proxy	Interacts with the production storage and backup storage and perform backup and restoration tasks.	Deployed in an AZ. At least two physical machines need to be deployed. Configure HA for the two nodes. If the production storage is Huawei distributed block storage, one set of eBackup Server&Proxy is deployed for each set of Huawei distributed block storage. For details about how to deploy eBackup Server&Proxy, see **Huawei Cloud Stack 8.2.0 Integration Design Suite**. VBS and CSBS deployed on one site can share the eBackup Server&Proxy.
Production storage	Storage devices used to store production data. For details, see **OceanStor BCManager 8.3.0 eBackup Version Mapping**.	The production storage and Server&Proxy must be deployed in the same data center. The network latency between the production storage and Server&Proxy is fewer than 2 ms.
Backup storage	Storage devices used to back up production data. For details, see **OceanStor BCManager 8.3.0 eBackup Version Mapping**.	The backup storage and production storage can be deployed in the same data center or in different data centers. The network quality requirements for level-1 backup storage and Server&Proxy are as follows: • NAS: Network latency ≤ 2 ms • Object storage: Network latency ≤ 20 ms The network quality requirements for level-2 backup storage and Server&Proxy are as follows: • NAS: Network latency ≤ 2 ms • Object storage: Network latency ≤ 20 ms

Service Flow

Backup

Figure 2-2 shows the backup service flow.

Figure 2-2 Backup service flow

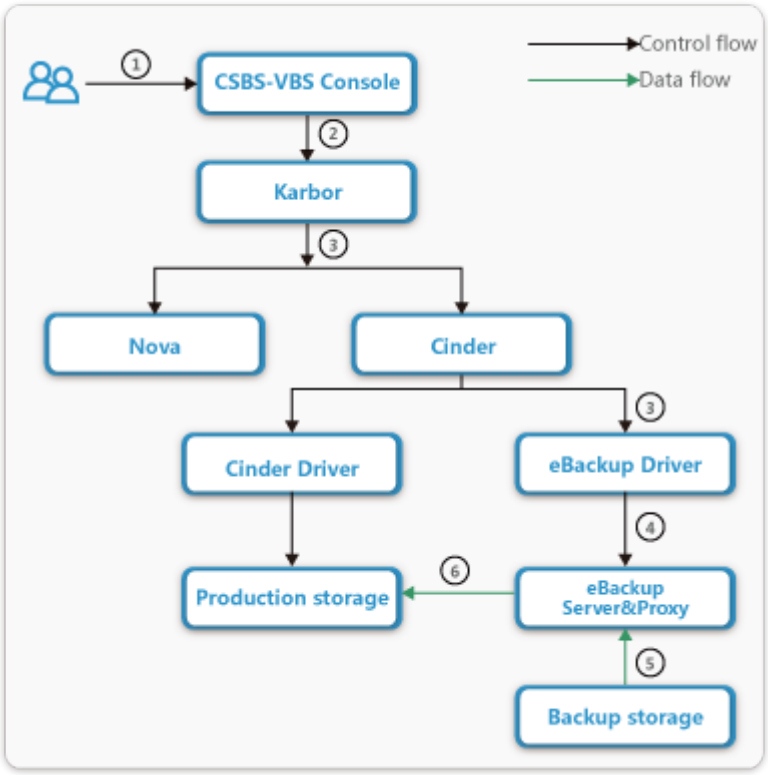


1. A user accesses CSBS-VBS Console.
2. CSBS-VBS Console delivers the backup task to Karbor.
3. Karbor delivers a snapshot creation command and a backup command to Cinder.
4. Cinder delivers a snapshot creation command to Cinder Driver.
5. Cinder Driver schedules the backup task automatically and creates a backup snapshot on the production storage.
6. Cinder delivers the backup command to eBackup Driver.
7. eBackup Driver delivers the backup command to the specified eBackup Server&Proxy.
8. The volume snapshot in the production storage is mounted to eBackup Server&Proxy to obtain full backup or incremental backup data.
9. eBackup Server&Proxy writes the backup data to the backup storage.
10. When the backup is successful, if the last backup exists, Karbor invokes the Cinder API to delete the snapshot of the last backup generated during the backup.

Restoration

Figure 2-3 shows the restored service flow.

Figure 2-3 Backup service flow

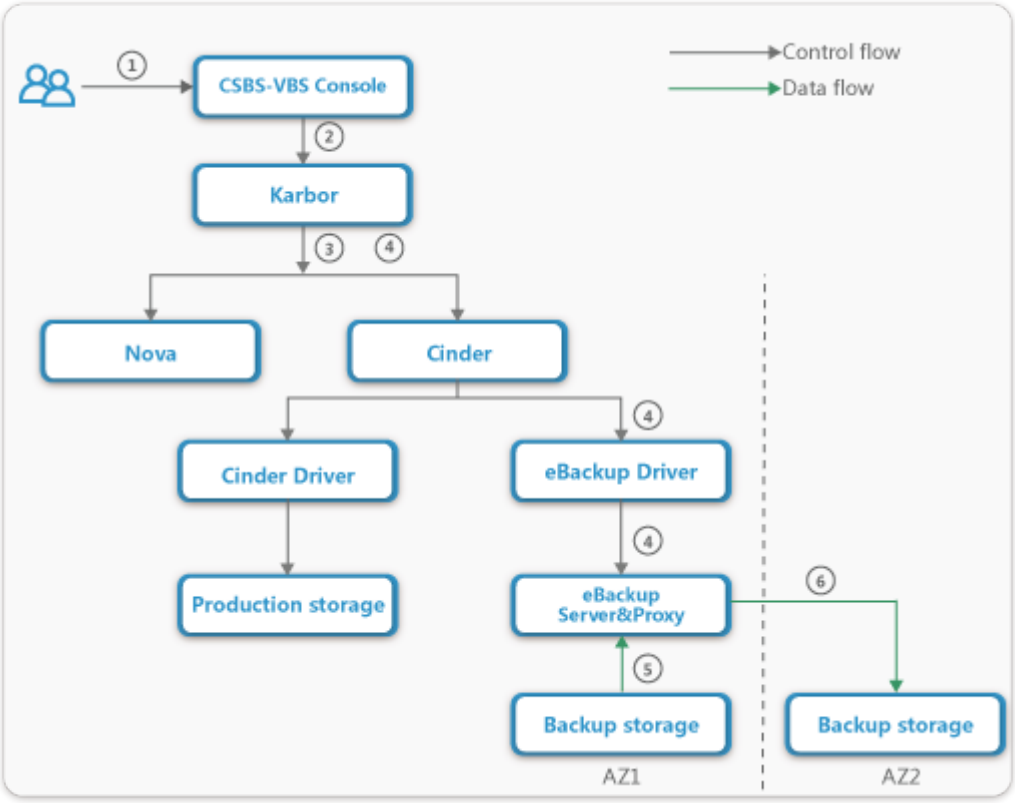


1. A user selects the backup to be restored and selects the target volume (the source volume, another volume, or a new volume).
2. CSBS-VBS Console delivers a restoration task to Karbor based on the tenant's restoration request.
3. Karbor invokes the Cinder restoration API and eBackup Driver to deliver the restoration task.
4. eBackup Driver invokes eBackup Server&Proxy to restore data volumes.
5. eBackup Server&Proxy reads backup data from the backup storage.
6. eBackup Server&Proxy writes the backup data to the physical storage where the target volumes reside.

Intra-Region Replication

Figure 2-4 shows the intra-region replication service flow.

Figure 2-4 Intra-region replication service flow



1. A user creates a replication policy on CSBS-VBS Console.
2. CSBS-VBS Console delivers the replication task to Karbor based on the backup scheduling policy.
3. Karbor invokes the Cinder import API to import replication records of the corresponding backup records. In this way, new backup records are generated.
4. Karbor initiates replication task scheduling and invokes Cinder and eBackup Driver to deliver the task of replicating backups to eBackup Server&Proxy.
5. eBackup Server&Proxy reads backup data from the local backup storage.
6. eBackup Server&Proxy writes the local backup data to the remote backup storage.

2.1.5 Related Services

Figure 2-5 and **Table 2-3** show the relationship between VBS and other cloud services.

Figure 2-5 Relationship between VBS and other cloud services

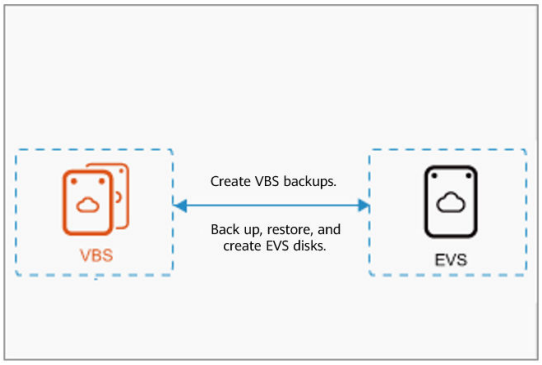


Table 2-3 Relationship between VBS and other cloud services

Service	Description
EVS	VBS relies on EVS and backs up EVS disks. Users can use a backup or replica to restore data on the original EVS disk or to another existing EVS disk, or use the backup or replica to create an EVS disk.

2.1.6 Key Metrics

Table 2-4 shows the key metrics of VBS.

Table 2-4 Key metrics of VBS

Item	Requirement
Maximum capacity of an EVS disk	64 TB
Maximum number of backup policies for one user	32
Maximum number of EVS disks that can be associated with one policy	64
Backup retention period of one policy	99,999 days
Number of retained backup of one single policy	99,999
Whether to support permanent retention of backups	Yes
Recovery Point Objective (RPO)	1 hour

Item	Requirement
Recovery Time Objective (RTO)	The RTO depends on the amount of data to be restored. Restoration time = Data amount/ Restoration performance. The restoration performance depends on the backup storage type (NFS or S3) and network type (GE, 10GE, or 25GE).

2.1.7 Accessing and Using VBS

Two methods are available:

- Using the GUI

  Log in to ManageOne Operation Portal (or ManageOne Tenant Portal in B2B scenarios). Click  in the upper left corner, select a region and resource set, and select the cloud service.

- API

  Use this mode if you need to integrate the cloud service into a third-party system for secondary development. For details, see the Volume Backup Service (VBS) 8.3.0 API Reference (for Huawei Cloud Stack 8.2.0) in the **Volume Backup Service (VBS) 8.3.0 Usage Guide (for Huawei Cloud Stack 8.2.0)**.

2.2 Related Concepts

2.2.1 Backup

A process of copying all or partial data from disks of the application host or dedicated storage devices to another storage medium for purposes of restoration in case the data is lost or becomes inaccessible due to mis-operations or system failures.

Figure 2-6 shows the backup principle.

Backup is implemented based on the storage snapshot technology and snapshot comparison technology. For each backup, eBackup creates a snapshot for the EVS disk to be backed up. For the first backup, eBackup performs a full backup using snapshot data. For the Nth backup, eBackup performs only incremental backups (namely, backs up only data changes between the current data and the last snapshot data).

After a backup is complete, eBackup deletes earlier EVS disk snapshots, retaining only the latest snapshot for comparing the differences with the snapshot to be generated in the next backup.

Figure 2-6 Backup principle

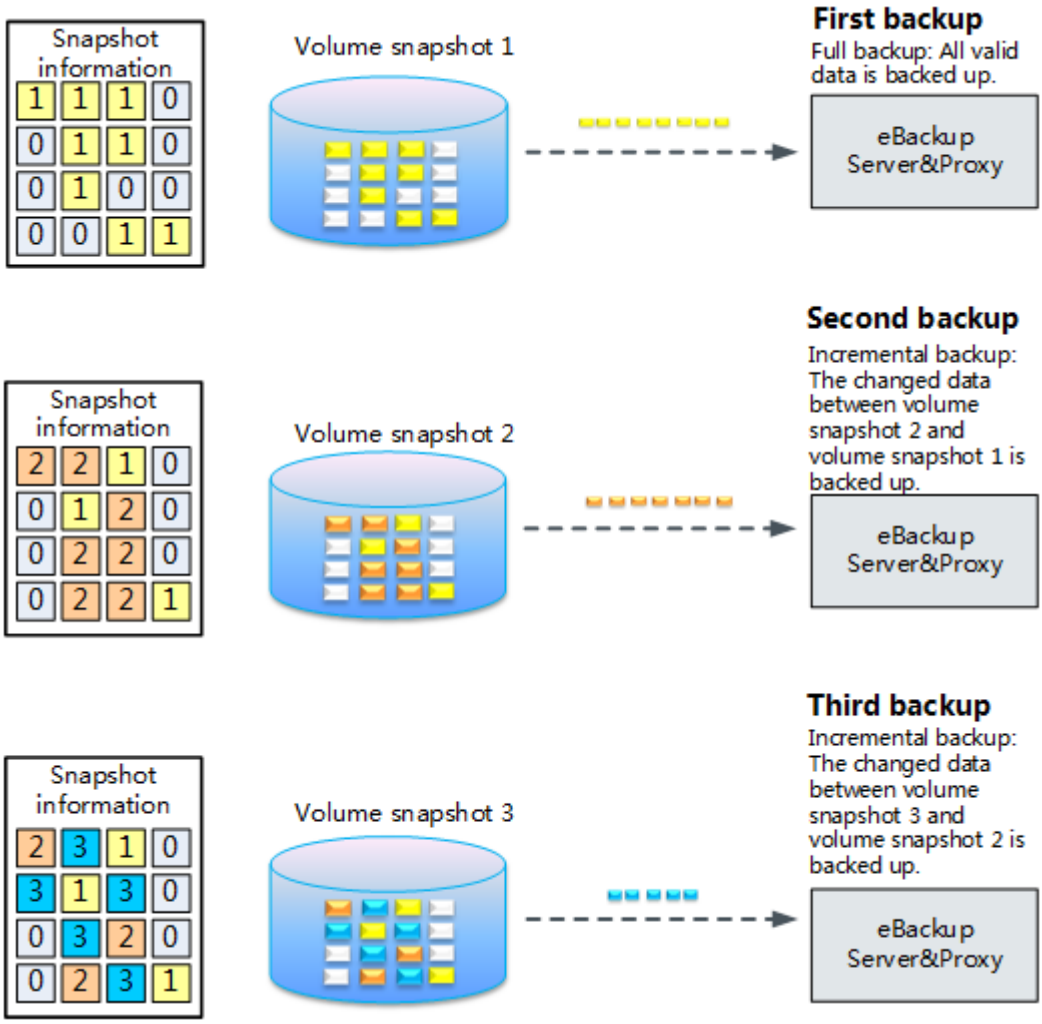
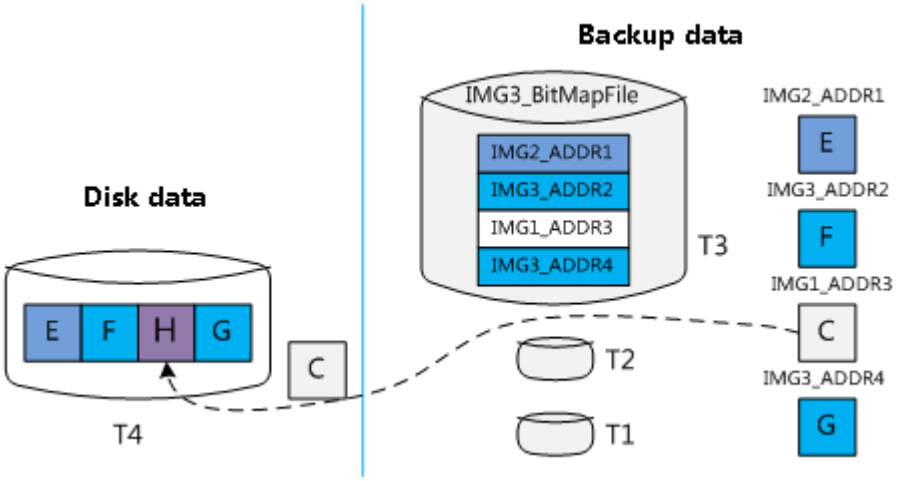


Figure 2-7 shows the restoration principle.

Restoration is implemented based on the snapshot comparison technology. eBackup obtains the data difference between the backup data and the target disk data. Only the differential data is restored to the target disk. Before the restoration, there is no need to obtain intact disk data.

Figure 2-7 Restoration principle



2.2.2 Backup Policy

A policy used to automatically back up data by specifying the backup time, backup period, retention rules, and other items. After a backup target is associated with a backup policy, the system will automatically back up data and delete expired backups according to the policy.

You can set policies for incremental backup, full backup, and replication.

2.2.3 Incremental Backup

A backup mode in which data objects modified since the last full backup or incremental backup are copied.

2.2.4 Full Backup

A backup mode in which all of the backup object is copied.

2.2.5 Replication

Replication is a process of storing a backup on a remote storage device in the local region to improve backup data reliability.

You can configure a replication policy in the backup policy to achieve periodic replication of backups, and VBS allows you to manually replicate policies.

2.2.6 Backups and Replicas

Backups are generated by full backup or incremental backup jobs. Replicas are generated by replication jobs.

2.3 Operation Process

Figure 2-8 and **Table 2-5** describe the process of creating a VBS task.

Figure 2-8 Process of creating a VBS task

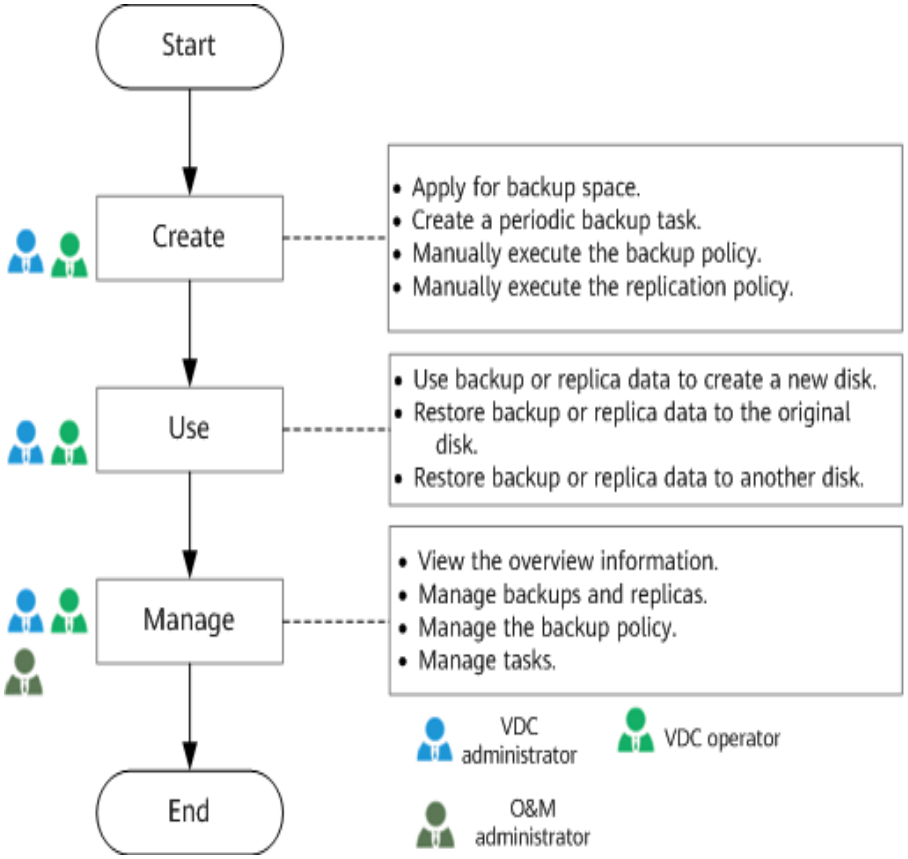


Table 2-5 Process description

Operation	Description and Reference	Operator and UI Portal
2.4 Applying for Backup Space	When you use VBS for the first time or the backup space of your resource set is insufficient, you can apply for space to store backups and replicas. For details, see 2.4 Applying for Backup Space.	ManageOne Operation Portal (ManageOne Tenant Portal in B2B scenarios): • VDC operator • VDC administrator
2.5 Creating a Periodic Backup Task	You can create a backup policy to drive the system to automatically execute backup and replication tasks according to the execution period defined in the policy. This enables fast data restoration upon data loss or damage of EVS disks, ensuring proper service running. For details, see 2.5.1 Creating a Backup Policy.	ManageOne Operation Portal (ManageOne Tenant Portal in B2B scenarios): • VDC operator • VDC administrator

Operation	Description and Reference	Operator and UI Portal
	You can create a backup policy and associate the EVS disk with it. In this way, the EVS disk is protected. For details, see **2.5.2 Creating a Backup Task**.	ManageOne Operation Portal (ManageOne Tenant Portal in B2B scenarios): • VDC operator • VDC administrator
2.7 Executing a Backup Policy Manually	The system backs up the EVS disk according to the backup policy at the preset time and generates a backup. You can also manually perform full backup or incremental backup. For details, see **2.7 Executing a Backup Policy Manually**.	ManageOne Operation Portal (ManageOne Tenant Portal in B2B scenarios): • VDC operator • VDC administrator
2.8 Executing a Replication Policy Manually	The system replicates the existing backup according to the backup policy at the preset time and generates a replica. You can also manually trigger the replication. Before using this function, you need to configure intra-region replication. For details to perform replication, see **2.8 Executing a Replication Policy Manually**.	ManageOne Operation Portal (ManageOne Tenant Portal in B2B scenarios): • VDC operator • VDC administrator
2.9 Restoring a Disk Using a Backup	If you want to use data in the EVS disk for testing or quick service replication, you can use the backup to create a disk. For details, see **2.9.1 Creating a Disk Using Backup Data**.	ManageOne Operation Portal (ManageOne Tenant Portal in B2B scenarios): • VDC operator • VDC administrator
	If the source disk is faulty, you can use the backups to restore data to ensure service continuity. For details, see **2.9.2 Restoring Backup Data to the Source EVS Disk**.	ManageOne Operation Portal (ManageOne Tenant Portal in B2B scenarios): • VDC operator • VDC administrator

Operation	Description and Reference	Operator and UI Portal
	If you have another EVS disk, you can restore the backup data to this disk. For details, see **2.9.3 Restoring Backup Data to Another EVS Disk**.	ManageOne Operation Portal (ManageOne Tenant Portal in B2B scenarios): • VDC operator • VDC administrator
2.10 Viewing the Overview Information	On the **Overview** page, you can view **Resource**, **Storage space**, and **Task Overview** information. For details, see **2.10 Viewing the Overview Information**.	ManageOne Operation Portal (ManageOne Tenant Portal in B2B scenarios): • VDC administrator • VDC operator
2.11 Managing Backups and Replicas	You can manually manage existing backups and replicas, such as viewing and deleting them. You can also apply for more space required for backup. For details, see **2.11 Managing Backups and Replicas**.	ManageOne Operation Portal (ManageOne Tenant Portal in B2B scenarios): • VDC operator • VDC administrator
2.12 Managing Backup Policies	You can effectively manage backup policies by performing a series of operations on them. For details, see **2.12 Managing Backup Policies**.	ManageOne Operation Portal (ManageOne Tenant Portal in B2B scenarios): • VDC operator • VDC administrator
2.13 Managing Tasks	Task management helps users better understand the detailed information about backup tasks, replication tasks, restoration tasks, deletion tasks, and export tasks in the latest 30 days. Tasks can be exported. For details, see **2.13 Managing Tasks**.	ManageOne Operation Portal (ManageOne Tenant Portal in B2B scenarios): • VDC operator • VDC administrator

2.4 Applying for Backup Space

When you use VBS for the first time or the backup space of your resource set is insufficient, you can apply for space to store backups and replicas. The backup space is used to store backups and replicas generated by the backup service. You can also apply for freeing up your spare backup space so that they can be used by other users.

Procedure

Step 1 Use a browser to log in to ManageOne as a VDC administrator or VDC operator.

URL in non-B2B scenarios: **https://***Domain name of ManageOne Operation Portal*, for example, **https://console.demo.com**

URL in B2B scenarios: **https://***Domain name of ManageOne Tenant Portal*, for example, **https://tenant.demo.com**

You can log in using a password or USB key.

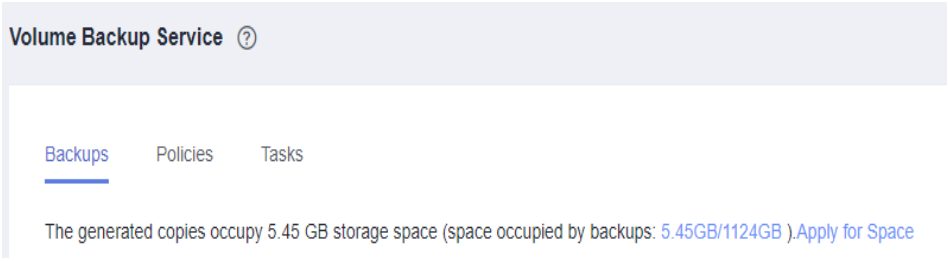
- Login using a password: Enter the username and password.

  The password is that of the VDC administrator or VDC operator.
- Login using a USB key: Insert a USB key with preset user certificates, select the required device and certificate, and enter a PIN.

Step 2 Click  in the upper left corner of the page, select a region and choose **Storage** > **Volume Backup Service**.

Step 3 Click **Apply for Space**, as shown in **Figure 2-9**.

Figure 2-9 Applying for space



Step 4 Apply for the backup space and replication space, as shown in **Figure 2-10**.

NOTE

- The space you apply for will be assigned to your project and shared with other users in your project. For example, if 10 users are in the same project and one of them applies for 1 TB space, the 1 TB space will be shared by the 10 users.
- To reduce space, the space left must be greater or equal to the used space.
- To add space, the backup or replication space applied for cannot be larger than the remaining VDC quota.
- If the intra-region replication function is not configured, the page for applying space only displays application information of the backup space.

Figure 2-10 Creating an application

Step 5 Click **Apply Now**.

If you do not want to apply for space immediately, click **Add to Cart**. The order cannot be added to the cart because **Current Space** is greater than 0.

Step 6 In the displayed **Information** dialog box, click **View Orders**.

On the **My Requests** page, you can check and export order information.

If **Order Status** is **Successful**, the space is applied for.

----End

2.5 Creating a Periodic Backup Task

2.5.1 Creating a Backup Policy

You can create a backup policy to drive the system to automatically execute backup and replication tasks according to the execution period defined in the policy. This enables fast data restoration upon data loss or damage of EVS disks, ensuring proper service running.

Context

You are advised to set the backup policy as follows:

- If you need to back up data at a fixed time every week, for example, after work on Fridays, you are advised to select **By week** when creating a backup policy.
- If you need to back up data at a fixed time every month, for example, on the first day of each month, you are advised to select **By month** when creating a backup policy.
- If you need to back up data at a fixed time every year, for example, November 11, you are advised to select **By year** when creating a backup policy.
- If the backup period exceeds one week, for example, 10 days, you are advised to select **By day** when creating a backup policy.

Prerequisites

- You have applied for the backup space. For details, see **2.4 Applying for Backup Space**.
- Configure intra-region replication before configuring the replication policy.

Procedure

Step 1 Use a browser to log in to ManageOne as a VDC administrator or VDC operator.

URL in non-B2B scenarios: **https://***Domain name of ManageOne Operation Portal*, for example, **https://console.demo.com**

URL in B2B scenarios: **https://***Domain name of ManageOne Tenant Portal*, for example, **https://tenant.demo.com**

You can log in using a password or USB key.

- Login using a password: Enter the username and password.

  The password is that of the VDC administrator or VDC operator.
- Login using a USB key: Insert a USB key with preset user certificates, select the required device and certificate, and enter a PIN.

Step 2 Click ☰ in the upper left corner of the page, select a region and choose **Storage** > **Volume Backup Service**.

Step 3 On the **Volume Backup Service** page, click the **Policies** tab.

Step 4 Click **Create**.

Step 5 Set policy parameters, as shown in **Figure 2-11**. **Table 2-6** describes related parameters.

Figure 2-11 Configuring a backup policy

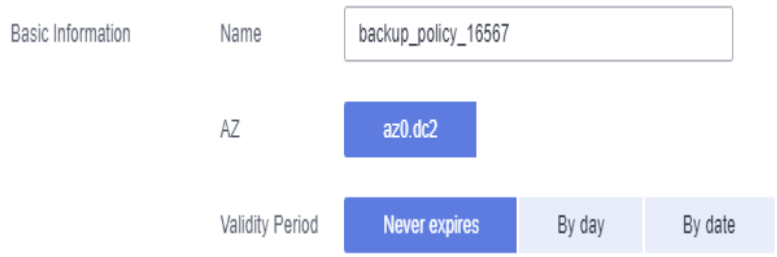


Table 2-6 Parameter description

Parameter	Description	Example Value
Name	Backup policy name, which is a character string of 1 to 255 characters containing letters, digits, underscores (_), and hyphens (-).	backup_policy_155051

Parameter	Description	Example Value
AZ	Target AZ. Only disks in this AZ can be associated with the backup policy. After you select the AZ, only EVS disks in this AZ can be associated with the policy. If the selected AZ does not support replication, replication policies cannot be configured.	Heilongjiang
Validity Period	Policy validity period. A policy is effective only when it is within the validity period. You can change the validity period of a policy as required. Possible values are **Never expires**, **By day**, and **By date**. **NOTE** The backup policy will expire at 23:59:59 on the expiration day. For example, if the backup policy is created at 23:30:00 on May 1, and the validity period is one day, it will expire at 23:59:59 on May 1.	Never expires

Step 6 Configure an incremental backup policy, as shown in **Figure 2-12**. **Table 2-7** describes related parameters.

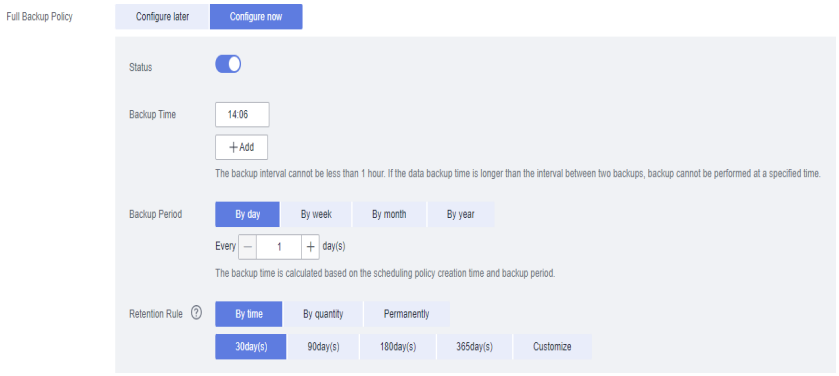
Figure 2-12 Configuring an incremental backup policy

Table 2-7 Parameter description

Parameter	Description	Example Value
Status	Policy status • : enabled • : disabled The default **status** is .	
Backup Time	Time point for backing up the EVS disk that has been associated with the policy A backup policy supports a maximum of 24 backup time points. The backup interval of all backup policies (including disabled backup policies) cannot be less than 1 hour. If the data backup time is longer than the interval between two backups, backup cannot be performed at a specified time. For example, if the backup time is set to 9:00, 10:00, and 11:00, the data backup time is 70 minutes each time. If the first backup starts at 9:00 and the backup is complete at 10:10. In this case, the preset backup will not be performed at 10:00 and the next backup will be performed at 11:00.	14:04
Backup Period	Backup execution interval • **By day**: The backup period can be set to 1 to 180 days. The backup time is calculated based on the scheduling policy creation time and the backup period. • **By week**: Specifies on which days of each week the backup task will be executed. • **By month**: Specifies on which days of each month the backup task will be executed. • **By year**: Specifies on which months and dates of each year the backup task will be executed. **NOTE** If a selected date does not exist in the current month, no backup will be generated at that day.	**By day**: Every day
Add	Click **Add** to add an incremental backup scheduling plan. A backup policy can contain a maximum of four incremental backup scheduling plans.	-

Step 7 Configure a full backup policy, as shown in **Figure 2-13**. **Table 2-8** describes related parameters.

Figure 2-13 Configuring a full backup policy



- If you do not want to configure a full backup policy, go to **Step 8**.

  You can configure a full backup policy later. For details, see **2.12.1 Editing a Backup Policy**.
- To configure a full backup policy, click **Configure Now**. Click **Add** and set parameters. **Table 2-8** describes the parameters.

Table 2-8 Parameter description

Name	Description	Example Value
Status	Policy status • : enabled • : disabled The default **status** is .	
Backup Time	Time point for backing up the EVS disk that has been associated with the policy A backup policy supports a maximum of 24 backup time points. The backup interval of all backup policies (including disabled backup policies) cannot be less than 1 hour. If the data backup time is longer than the interval between two backups, backup cannot be performed at a specified time. For example, if the backup time is set to 9:00, 10:00, and 11:00, the data backup time is 70 minutes each time. If the first backup starts at 9:00 and the backup is complete at 10:10. In this case, the preset backup will not be performed at 10:00 and the next backup will be performed at 11:00.	14:05

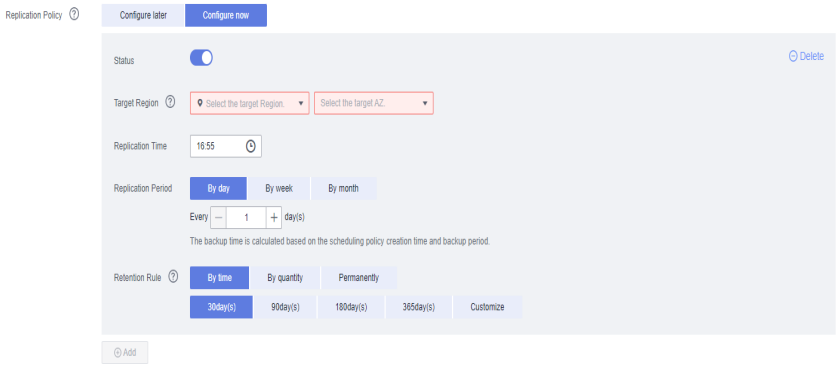
Name	Description	Example Value
Backup Period	Backup execution interval • **By day**: The backup period can be set to 1 to 180 days. The backup time is calculated based on the scheduling policy creation time and the backup period. • **By week**: Specifies on which days of each week the backup task will be executed. • **By month**: Specifies on which days of each month the backup task will be executed. • **By year**: Specifies on which months and dates of each year the backup task will be executed. **NOTE** If a selected date does not exist in the current month, no backup will be generated at that day.	**By day**: Every day

Name	Description	Example Value
Retention Rule	Retention rule for the backups automatically generated according to the full backup policy. Backups that do not comply with the rule will be automatically deleted. **NOTE** • If backups are retained by time, the system automatically starts to delete backups that have been retained for a period longer than the retention period from 00:00 every day. • If backups are retained by quantity, the system checks the number of backups after each automatic backup is complete and automatically deletes the backups that are beyond the set quantity. • More frequent backup of EVS disks creates more backups and delivers a higher level of data protection but occupies more storage space. Determine the backup frequency based on the data importance and service volume. Perform relatively frequent backup operations for important data. • **By time**: The automatically generated backups are saved according to the set retention period. If backups violate the set period, they are automatically deleted. **By time** can be set to **30 days**, **90 days**, **180 days**, **365 days**, and **Customize**. **Customize** can be set to any value ranging from 1 to 99,999. • **By quantity**: The automatically generated backups are saved according to the set retention quantity. If backups violate the set quantity, they are automatically deleted. **By quantity** can be set to **30**, **90**, **180**, **365**, or **Customize**. **Customize** can be set to an integer ranging from 1 to 99,999. For example, if **By quantity** is set to 30, each EVS disk associated with the policy can have up to 30 backups. • **Permanently**: All automatically generated backups are permanently saved. Reserve adequate storage capacity as copies can be deleted manually only after configuration is successful.	By time: 30 days
Add	Click **Add** to add a full backup scheduling plan. A backup policy can contain a maximum of four full backup scheduling plans.	-

Step 8 Configure the replication policy, as shown in **Figure 2-14**.

This parameter is displayed only when the replication policy is configured.

Figure 2-14 Configuring a replication policy



- If you do not need to configure the replication policy, go to **Step 9**

  You can configure the policy later through **2.12.1 Editing a Backup Policy**.
- If you need to configure the replication policy, click **Configure now**.

  Click **Add** to create a replication policy and set parameters. **Table 2-9** describes the parameters.

  NOTE

  The replication policy can be configured only after the replication function is enabled.

  Replication is to replicate incremental or full backups that have been generated to the target end. Therefore, if the target backup storage is not configured, the replication task will fail.

Table 2-9 Parameter description

Name	Description	Example Value
Status	Policy status: – : enabled – : disabled The default **status** is .	
Target Region	Region to which the backup is replicated Only regions that support replication will be displayed. Select the region and resource set first, and then select the target region.	North China
Replication Time	Replication execution time point. Only one replication time point can be configured.	10:14

Name	Description	Example Value
Replication Period	Replication execution time period: – **By day**: The replication period can be set to 1 to 180 days. The replication time is calculated based on the scheduling policy creation time and replication period. – **By week**: Specifies on which days of each week the replication task will be executed. – **By month**: Specifies on which days of each month the replication task will be executed. **NOTE** If a selected date does not exist in the current month, no backup will be generated at that day.	**By week**: Wednesday
Retention Rule	Retention rule for the replicas automatically generated according to the replication policy. Replicas that do not comply with the rule will be automatically deleted. **NOTE** – Manually generated replicas can only be deleted manually. – If replicas are retained by time, the system automatically starts to delete replicas that have been retained for a period longer than the retention period from 00:00 every day. – If replicas are retained by quantity, the system checks the number of replicas after each automatic replication is complete and automatically deletes the replicas that are beyond the set quantity. – **By time**: The automatically generated backups are saved according to the set retention period. If backups violate the set duration, they are automatically deleted. **By time** can be set to **30 days**, **90 days**, **180 days**, **365 days**, and **Customize**. **Customize** can be set to any value ranging from 1 to 99,999. – **By quantity**: The automatically generated replicas are saved according to the set retention quantity. If replicas violate the set quantity, they are automatically deleted. **By quantity** can be set to **30**, **90**, **180**, **365**, or **Customize**. **Customize** can be set to an integer ranging from 1 to 99,999. For example, if **By quantity** is set to 30, each EVS disk associated with the policy can have up to 30 backups. – **Permanently**: All automatically generated backups and replicas are permanently saved. Reserve adequate storage capacity as copies can be deleted manually only after configuration is successful.	By time: 180 days

Step 9 Click **OK**.

----End

2.5.2 Creating a Backup Task

This section describes how to quickly create a VBS backup task.

Prerequisites

- You have obtained the username and password of a VDC administrator or a VDC operator.
- You have applied for the backup space. For details, see **2.4 Applying for Backup Space**.

Precautions

An EVS disk can be backed up only when its status is **Available** or **In-use**. If you have performed operations such as expanding the capacity, or attaching, detaching, and deleting an EVS disk, refresh the page first to ensure the completion of the operation and then determine whether to back up the disk.

For an EVS disk that has been attached to a server and serves as a system disk, you can back up its data only when the server is in the **Running**, **Stopped**, or **Dormant** status. Otherwise, the backup request may time out, and the backup may fail.

Procedure

Step 1 Use a browser to log in to ManageOne as a VDC administrator or VDC operator.

URL in non-B2B scenarios: **https://***Domain name of ManageOne Operation Portal*, for example, **https://console.demo.com**

URL in B2B scenarios: **https://***Domain name of ManageOne Tenant Portal*, for example, **https://tenant.demo.com**

You can log in using a password or USB key.

- Login using a password: Enter the username and password.

  The password is that of the VDC administrator or VDC operator.
- Login using a USB key: Insert a USB key with preset user certificates, select the required device and certificate, and enter a PIN.

Step 2 Click  in the upper left corner of the page, select a region and choose **Storage** > **Volume Backup Service**.

Step 3 Click **Create VBS Backup** in the upper right corner.

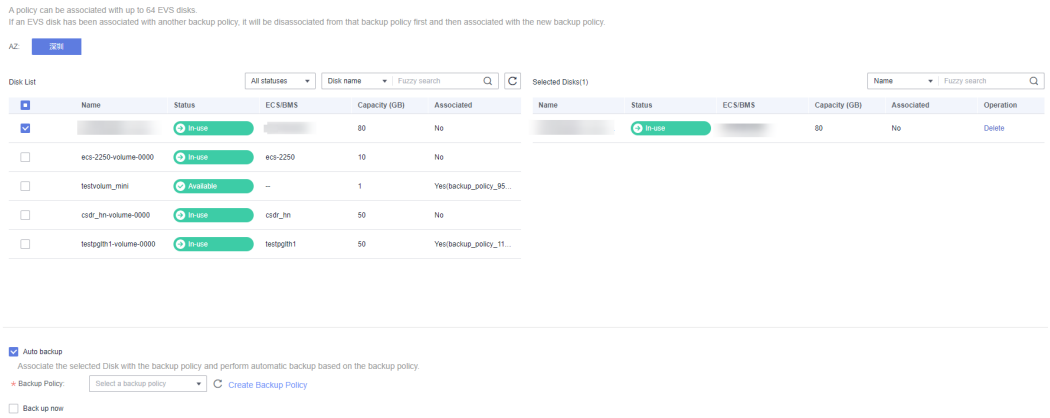
Step 4 Select an AZ to which the disk belongs.

Step 5 From the **Disk List** on the left, click to select the EVS disks you want to back up. Then, they appear in the **Selected Disks** list on the right, as shown in **Figure 2-15**. You can click **Delete** in the **Operation** column to delete EVS disks that do not need to be backed up.

NOTE

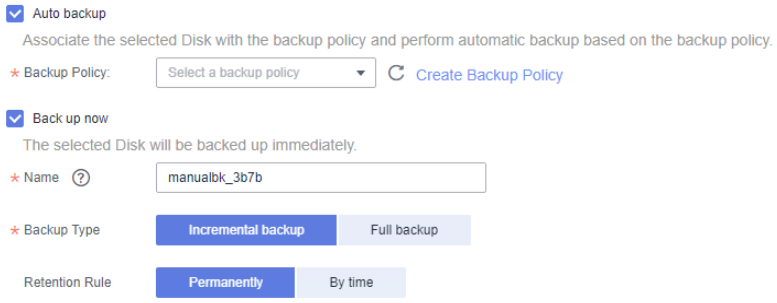
- A maximum of 64 EVS disks can be associated with a backup policy.
- You can filter the disks by specifying the disk status, as well as by searching for **Disk name**, **Disk ID**, **Server name**, **Server ID**, and so on.
- EVS disks in different AZs cannot be associated with the same backup policy.
- If the selected EVS disk has been associated with another backup policy, it will be disassociated from that backup policy first and then associated with the new backup policy.

Figure 2-15 Selecting disks



Step 6 Configure the backup mode, as shown in **Figure 2-16**.

Figure 2-16 Configuring a backup mode



Two backup modes are available:

- **Auto backup**

  After a VBS backup is created, the system periodically backs up the disks on the server based on the backup policy. **Auto backup** is selected by default.

  In the **Backup Policy** drop-down list, select a backup policy. Alternatively, click **Create Backup Policy** to create a backup policy. For details, see **2.5.1 Creating a Backup Policy**.

  NOTE

  After a backup policy is created, the system automatically refreshes the backup policy list and selects the backup policy by default. To change the policy, select another policy from the drop-down list.

- **Back up now**

  After a VBS is created, the system immediately backs up the EVS disks.

  a. Select the check box on the left of **Back up now**.

  b. Set the backup parameters. **Table 2-10** describes the parameters.

  Table 2-10 Parameter description

Parameter	Description	Example Value
Name	Name of the backup to be created. It is a string of 1 to 64 characters containing only Chinese characters, letters, digits, underscores (_), and hyphens (-). **NOTE** You can use the default name **manualbk**_*xxxx*. When multiple EVS disks are to be backed up, the system automatically adds suffixes to their names. For example, if the VBS name is **manualbk_app** and two EVS disks are backed up, the names of the backup copies generated by the system are: **manualbk_app-0001** and **manualbk_app-0002**.	manualbk_49d2
Backup Type	Incremental backup or full backup.	Incremental Backup

Parameter	Description	Example Value
Retention Rule	Retention rule for backups generated by **Back up now**. Backups that exceed the limit set in the retention rule will be automatically deleted. By default, backups are retained permanently. You can also set a retention period for backups generated by **Back up now**. Backups that exceed the set retention period will be automatically deleted. **By time** can be set to **30 days**, **90 days**, **180 days**, **365 days**, and **Customize**. **Customize** can be set to any value ranging from 1 to 99,999. **NOTE** If copies are retained by time, the expiration time is displayed in the copy details. Copies that exceed the retention period are deleted based on the expiration time.	Permanently

You can select both the backup modes at the same time. When both the backup modes are selected, backup will be performed immediately and periodic backups will be performed according to the backup policy subsequently.

Step 7 Click **Create Now**.

Step 8 Confirm the VBS backup information and click **Submit**.

Click **Back to Backup List** as prompted to view the backups.

----End

2.6 Manually Changing the Validity Period of a Backup

After creating a VBS backup, you can manually change the validity period of the VBS backup.

Prerequisites

- You have obtained the username and password of a VDC administrator or a VDC operator.
- You have applied for the backup space. For details, see **2.4 Applying for Backup Space**.
- The EVS disks have been associated with a backup policy.

Procedure

Step 1 Use a browser to log in to ManageOne as a VDC administrator or VDC operator.

URL in non-B2B scenarios: **https://***Domain name of ManageOne Operation Portal*, for example, **https://console.demo.com**

URL in B2B scenarios: **https://***Domain name of ManageOne Tenant Portal*, for example, **https://tenant.demo.com**

You can log in using a password or USB key.

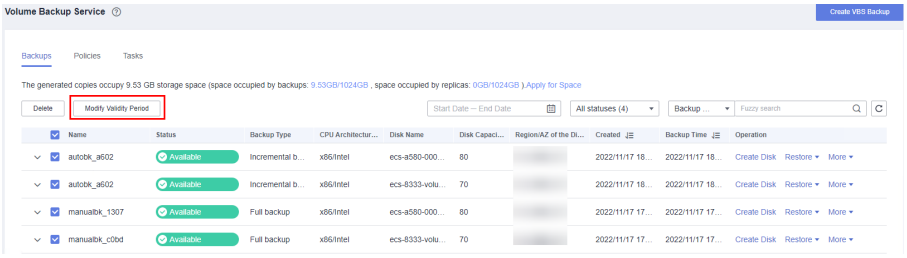
- Login using a password: Enter the username and password.

  The password is that of the VDC administrator or VDC operator.
- Login using a USB key: Insert a USB key with preset user certificates, select the required device and certificate, and enter a PIN.

Step 2 Click ☰ in the upper left corner of the page, select a region and choose **Storage** > **Volume Backup Service**.

Step 3 On the **Volume Backup Service** page, click the **Backups** tab page.

Step 4 In the backup list, locate the target backup and click **Modify Validity Period** to change the expiration time of the backup.



----End

2.7 Executing a Backup Policy Manually

After a VBS is created, the system automatically schedules and backs up the disks based on the preset backup policy. You can also perform manual backup on EVS disks based on your own requirements periodically.

Prerequisites

- You have obtained the username and password of a VDC administrator or a VDC operator.
- You have applied for the backup space. For details, see **2.4 Applying for Backup Space**.
- The EVS disks have been associated with a backup policy.

Precautions

When performing this operation, you need to associate EVS disks with the policy. If no EVS disk is associated, the system displays a message indicating that no EVS

disk can be backed up in the backup policy. For details about how to attach an EVS disk, see **2.12.3 Associating New EVS Disks with a Backup Policy**.

Procedure

Step 1 Use a browser to log in to ManageOne as a VDC administrator or VDC operator.

URL in non-B2B scenarios: **https://***Domain name of ManageOne Operation Portal*, for example, **https://console.demo.com**

URL in B2B scenarios: **https://***Domain name of ManageOne Tenant Portal*, for example, **https://tenant.demo.com**

You can log in using a password or USB key.

- Login using a password: Enter the username and password.

  The password is that of the VDC administrator or VDC operator.
- Login using a USB key: Insert a USB key with preset user certificates, select the required device and certificate, and enter a PIN.

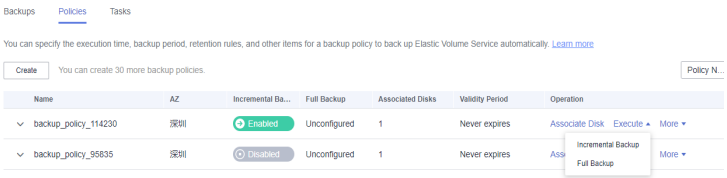
Step 2 Click ☰ in the upper left corner of the page, select a region and choose **Storage** > **Volume Backup Service**.

Step 3 On the **Volume Backup Service** page, click the **Policies** tab.

Step 4 Manually perform incremental backup or full backup. See **Figure 2-17**.

- To perform incremental backup, choose **Execute** > **Incremental Backup** in the row where the backup policy is located.
- To perform full backup, choose **Execute** > **Full Backup** in the row where the backup policy is located.

Figure 2-17 Performing backup

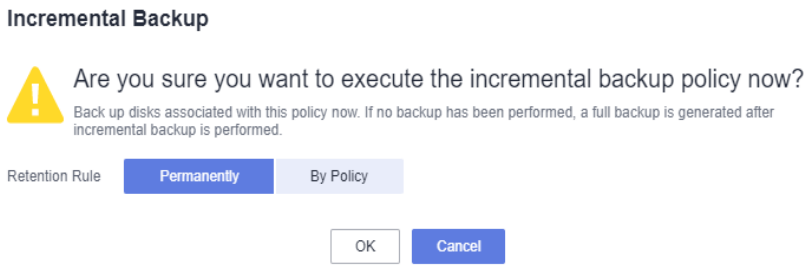


Step 5 Set the retention rule.

The default value is **Permanently**. You can also set it to **By Policy**.

If you select **By Policy**, you can select a scheduling plan in the backup policy. The system retains manually created backups based on the retention rule in the scheduling plan. **Figure 2-18** uses manual incremental backup as an example.

Figure 2-18 Retention rule for backups generated by manual incremental backup



NOTE

If full backup is not configured in the backup policy, backups generated by manual full backup can only be retained permanently.

Step 6 Click **OK** to complete the manual incremental backup or full backup.

The system automatically switches to the **Task list** area. When **Status** becomes **Succeeded**, the manual backup is executed successfully.

----End

2.8 Executing a Replication Policy Manually

After a VBS is created, the system automatically schedules and replicates the backups based on the preset backup policy. You can also perform manual replication on EVS disks based on your own requirements periodically.

Prerequisites

- You have obtained the username and password of a VDC administrator or a VDC operator.
- You have applied for the replication space. For details, see **2.4 Applying for Backup Space**.
- The EVS disks have been associated with a backup policy.
- The intra-region replication function has been configured.

Precautions

- Replication is done for backups. Therefore, before performing replication, ensure that a backup has been generated under the backup policy.
- A backup can be replicated only once. If the replica corresponding to a backup is deleted, the backup cannot be replicated again.

Procedure

Step 1 Use a browser to log in to ManageOne as a VDC administrator or VDC operator.

URL in non-B2B scenarios: **https://***Domain name of ManageOne Operation Portal*, for example, **https://console.demo.com**

URL in B2B scenarios: **https://***Domain name of ManageOne Tenant Portal*, for example, **https://tenant.demo.com**

You can log in using a password or USB key.

- Login using a password: Enter the username and password.

  The password is that of the VDC administrator or VDC operator.
- Login using a USB key: Insert a USB key with preset user certificates, select the required device and certificate, and enter a PIN.

Step 2 Click  in the upper left corner of the page, select a region and choose **Storage** > **Volume Backup Service**.

Step 3 On the **Volume Backup Service** page, click the **Policies** tab.

Step 4 Choose **Execute** > **Replication** in the row where the backup policy is located.

NOTE

- If the AZ to which the backup policy belongs does not support replication, replication cannot be performed.
- If you perform the replication task before the backup policy generates a backup, no replica will be generated.
- A replica generated by manual replication cannot be automatically deleted. If you need to manually delete it, see **2.11.2 Deleting an EVS Disk Backup or Replica**.

Step 5 Click **OK**.

Then, you are redirected to **Backup Tasks**. When **Status** becomes **Succeeded**, the manual replication is executed successfully.

Click the **Tasks** tab page, and see **Managing Tasks** to manage backup tasks.

----End

2.9 Restoring a Disk Using a Backup

2.9.1 Creating a Disk Using Backup Data

You can create a disk by using a VBS backup or replica. Data originally existing in the disk is the same as the backup or replica.

Prerequisites

- The **Status** of backup or replica is **Available**.
- Configure EVS-related features. Set **is_supported_vbs** to **true**. For details, see *User Guide* > **How to Enable the EVS Disk Backup Service for an ECS** in the ***Elastic Cloud Server (ECS) Usage Guide (for Huawei Cloud Stack 8.2.0)*** or *User Guide* > **How to Enable the EVS Disk Backup Service for a BMS** in the **Bare Metal Server (BMS) Usage Guide (for Huawei Cloud Stack 8.2.0)**.

Procedure

Step 1 **Access the volume backup service console as a VDC administrator or a VDC operator**.

Step 2 On the **Backups** tab page, click **Create Disk** in the row of the desired backup.

Step 3 Set disk parameters.

NOTE

Note the following when setting the parameters:

- The capacity of the newly created EVS disk cannot be smaller than that of the original EVS disk of the backup data.
- Batch creation is not supported when you use a backup to create an EVS disk. **Quantity** can only be **1**.

Step 4 Click **Next**.

Step 5 Confirm the VBS backup information and click **Apply Now**.

Step 6 Go to the EVS page and check whether the disk is created successfully.

A restoration task is automatically generated. When **Status** of the restoration task changes to **Succeeded**, the restoration task is successful.

NOTE

When a new EVS disk created using a VBS backup is attached to a server, the architecture of the server must be the same as that of the server to which the backup is attached.

----End

2.9.2 Restoring Backup Data to the Source EVS Disk

You can restore an EVS disk using its backup or replica to the status at the backup point in time.

Prerequisites

- The **Status** of backup or replica is **Available**.
- The **Status** of the disk is **Available**.

Precautions

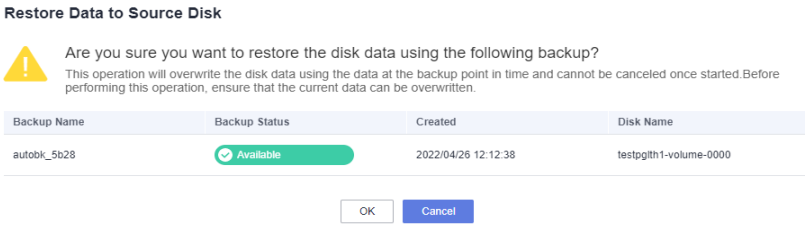
- Before restoring data on a disk of an ECS, stop the ECS and detach the EVS disk from the ECS. For details, see *User Guide* > **EVS Disk** > **Releasing an EVS Disk** > **Detaching an EVS Disk** in the ***Elastic Cloud Server (ECS) Usage Guide (for Huawei Cloud Stack 8.2.0)***. After the restoration, attach the EVS disk and start the ECS by referring to *User Guide* > **Attaching an EVS Disk** in the ***Elastic Cloud Server (ECS) Usage Guide (for Huawei Cloud Stack 8.2.0)***.
- Before restoring data on a disk of a BMS, stop the BMS and detach the EVS disk from the BMS. For details, see *User Guide* > **Data Disks** > **Detaching an EVS Disk** in the ***Bare Metal Server (BMS) Usage Guide (for Huawei Cloud Stack 8.2.0)***. After the restoration, attach the EVS disk and start the BMS by referring to *User Guide* > **Data Disks** > **Attaching an EVS Disk** in the ***Bare Metal Server (BMS) Usage Guide (for Huawei Cloud Stack 8.2.0)***.

Procedure

Step 1 **Access the volume backup service console as a VDC administrator or a VDC operator**.

Step 2 On the **Backups** tab page, click **Restore** in the row of the desired backup and choose **Source Disk** from the drop-down list. See **Figure 2-19**.

Figure 2-19 Restoring data to the source EVS disk



Step 3 Click **OK** as prompted.

Step 4 Click the **Task** tab. If **Status** of the restoration task is **Succeeded**, the backup has been successfully restored to the original disk.

----End

2.9.3 Restoring Backup Data to Another EVS Disk

You can restore data of an EVS disk using its backup or replica to the status at the backup point in time and to a specified disk.

Prerequisites

- The **Status** of backup or replica is **Available**.
- The **Status** of other EVS disks to be restored are **Available**.

Precautions

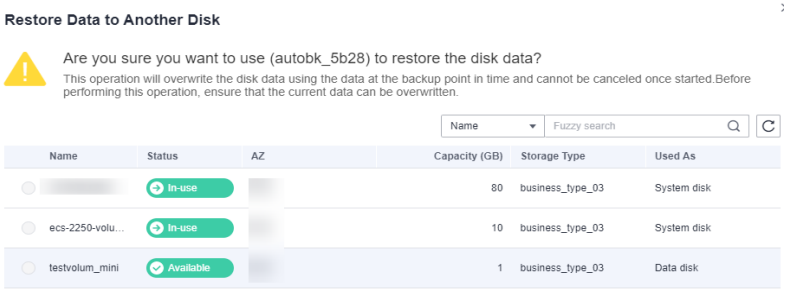
- Before restoring data on a disk of an ECS, stop the ECS and detach the EVS disk from the ECS. For details, see *User Guide* > **EVS Disk** > **Releasing an EVS Disk** > **Detaching an EVS Disk** in the ***Elastic Cloud Server (ECS) Usage Guide (for Huawei Cloud Stack 8.2.0)***. After the restoration, attach the EVS disk and start the ECS by referring to *User Guide* > **Attaching an EVS Disk** in the ***Elastic Cloud Server (ECS) Usage Guide (for Huawei Cloud Stack 8.2.0)***.
- Before restoring data on a disk of a BMS, stop the BMS and detach the EVS disk from the BMS. For details, see *User Guide* > **Data Disks** > **Detaching an EVS Disk** in the ***Bare Metal Server (BMS) Usage Guide (for Huawei Cloud Stack 8.2.0)***. After the restoration, attach the EVS disk and start the BMS by referring to *User Guide* > **Data Disks** > **Attaching an EVS Disk** in the ***Bare Metal Server (BMS) Usage Guide (for Huawei Cloud Stack 8.2.0)***.

Procedure

Step 1 **Access the volume backup service console as a VDC administrator or a VDC operator**.

Step 2 On the **Backups** tab page, click **Restore** in the row of the desired backup and choose **Another Disk** from the drop-down list. See **Figure 2-20**.

Figure 2-20 Restoring data to another EVS disk



Step 3 In the dialog box that is displayed, specify a disk and click **OK**.

NOTE

- The selected disk cannot be smaller than the source disk in size.
- When an EVS disk restored using a VBS backup is attached to a server, the architecture of the server must be the same as that of the server to which the backup is attached.

Step 4 Click **OK** as prompted.

Step 5 Click the **Task** tab. If **Status** of the restoration task is **Succeeded**, the backup has been successfully restored to another disk.

Click the **Tasks** tab page, and see **Managing Tasks** to manage restoration tasks.

Step 6 Access the EVS console and check the status of the target EVS disk.

When **Status** of the target EVS disk is **Available**, the restoration succeeds.

----End

2.10 Viewing the Overview Information

On the **Overview** page, you can view **Resource**, **Storage Space**, and **Task Overview** information.

Prerequisites

You have obtained the username and password of a VDC administrator or a VDC operator.

Procedure

Step 1 Use a browser to log in to ManageOne as a VDC administrator or VDC operator.

URL in non-B2B scenarios: **https://***Domain name of ManageOne Operation Portal*, for example, **https://console.demo.com**

URL in B2B scenarios: **https://***Domain name of ManageOne Tenant Portal*, for example, **https://tenant.demo.com**

You can log in using a password or USB key.

- Login using a password: Enter the username and password.

  The password is that of the VDC administrator or VDC operator.

- Login using a USB key: Insert a USB key with preset user certificates, select the required device and certificate, and enter a PIN.

Step 2 Click ☰ in the upper left corner of the page, choose **Storage** > **Volume Backup Service**.

Step 3 In the navigation tree on the left, choose **Overview**. The **Overview** page is displayed.

Step 4 On the **Overview** page, view the overall data of backup services, as shown in **Figure 2-21**. **Table 2-11** describes each section.

Figure 2-21 Overview

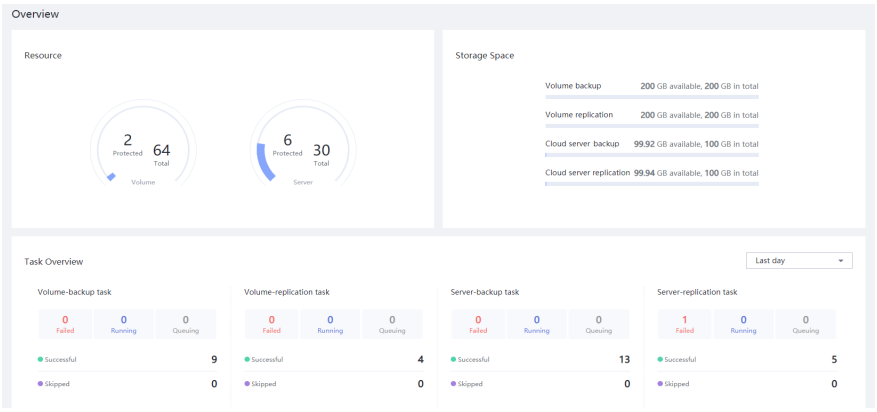


Table 2-11 Overview description

Section	Description
Resource	In this section, you can view the total number of different resources and the number of protected resources, including: • Volume • Server
Storage Space	In this section, you can view the total capacity and used capacity of different resources for backup and replication, including: • Volume backup • Volume replication • Cloud server backup • Cloud server replication

Section	Description
Task Overview	• In this section, you can view the numbers of backup and replication tasks in each of the following execution status: **Failed**, **Running**, **Queuing**, **Successful**, and **Skipped** . • You can select **Last day**, **Last week**, and **Last month** from the drop-down list in the upper right corner to display the task execution status. – Last day: the latest 24 hours since the current time – Last week: the latest 7 x 24 hours since the current time – Last month: the latest 30 x 24 hours since the current time For example, if you select **Last day** and the current time is 15:00 on February 24, 2021, the system displays the tasks from 15:00 on February 23, 2021 to 15:00 on February 24, 2021.

----End

2.11 Managing Backups and Replicas

2.11.1 Viewing EVS Disk Backups and Replicas

You can view existing backups and replicas to understand protection status of EVS disks.

Prerequisites

At least one backup or replica is available.

Precautions

- The **Retention Rule** only applies to backups and replicas automatically generated based on the policy. Backups and replicas that exceed the limit set in the retention rule will be automatically deleted.
- Backups retained based on policies can be automatically deleted.

Procedure

Step 1 **Access the volume backup service console as a VDC administrator or a VDC operator**.

Step 2 On the **Backups** tab page, you can set search criteria at the upper right corner to filter backups and replicas.

Step 3 Click ⌄ on the left of a backup to view its details. **Table 2-12** describes related parameters.

NOTE

This parameter is displayed only when the replication policy is configured.

Table 2-12 Parameter description

Type	Parameter	Description
Backup	Name	Automatically generated backup or replica name, which complies with the following rules: ● Automatic execution: – For backups: **autobk_xxxx** – For replicas: **autocp_xxxx** ● Manual execution: – For backups: **manualbk_xxxx** – For replicas: **manualcp_xxxx** **xxxx** is automatically generated by the system.
	Backup ID	Backup ID, which is automatically generated.
	Status	Backup status, which can be **Queuing**, **Available**, **Creating**, **Restoring**, **Deleting**, or **Error**
	AZ	AZ to which the EVS disk belongs
	Created	Creation time of the backup
	Source Backup ID	Replica's corresponding backup ID. You can use this ID to locate the source backup of the replica. This parameter is displayed only when is on the right of backup name.
	Schedule ID	Policy schedule ID used for generating the backup. Only replicas retained based on policies have scheduling IDs. The scheduling ID of replicas not retained based on policies is --.
	Replication Status	Replication status, which can be **To be replicated**, **Not replicated**, **Replicating**, **Replication failed**, or **Replication succeeded** This parameter is not displayed only when is on the right of backup name.
	Expired At	A backup created by days has an expiration time.
Disks	Name	Name of the source disk You can click the disk name to go to the disk details page.
	Disk ID	ID of the source disk

Type	Parameter	Description
	Capacity (GB)	Disk size
	Used As	Disk attribute, which can be **System Disk** or **Data Disk**

----End

2.11.2 Deleting an EVS Disk Backup or Replica

This operation allows you to delete earlier backups and replicas or manually created backups and replicas.

Prerequisites

At least one backup or replica is available.

Precautions

A backup or replica can be deleted only when it is in the **Available** or **Error** status.

Procedure

Step 1 **Access to volume backup service console as a VDC administrator or a VDC operator**.

Step 2 On the **Backups** tab page, click **Delete** in the row of the desired backup.

You can set search criteria to filter backups.

Step 3 In the dialog box that is displayed, confirm the information and click **OK**.

Step 4 If you need to delete multiple backups or replicas, select on the left of the target backups or replicas and click **Delete** above the list. In the displayed dialog box, confirm the deletion information and click **OK**.

----End

2.12 Managing Backup Policies

2.12.1 Editing a Backup Policy

You can modify the status, backup time, backup period, retention rule, and validity period of a full backup, incremental backup, or replication policy.

Prerequisites

A backup policy has been created.

Precautions

If the backup policy has a backup or replication task being executed when you modify it, the task continues running until it finishes.

Procedure

Step 1 **Access the volume backup service console as a VDC administrator or a VDC operator**.

Step 2 On the **Volume Backup Service** page, click the **Policies** tab.

You can search for a policy by policy name or schedule ID.

Step 3 Click **More** in the row containing the desired policy and choose **Edit Policy** from the drop-down list.

Step 4 Modify parameters according to **Table 2-6**, **Table 2-7**, **Table 2-8** and **Table 2-9**.

Step 5 Click **OK**.

----End

2.12.2 Viewing a Backup Policy

You can view whether full backup, incremental backup, or replication is enabled, as well as the number of associated EVS disks, and the validity period of a backup policy.

Prerequisites

A backup policy has been created.

Procedure

Step 1 **Access to volume backup service console as a VDC administrator or a VDC operator**.

Step 2 On the **Volume Backup Service** page, click the **Policies** tab.

You can search for a policy by policy name or schedule ID.

Step 3 On the **Policies** tab page, view information about the policy, including **Name**, **AZ**, **Associated Disks**, and **Validity Period**, as well as whether **Incremental Backup** or **Full Backup** is configured and enabled.

Click ⌄ on the left of a backup policy to view details about the policy, such as **Replication**, **Incremental backup**, or **Full backup**, and view the servers associated with the policy and the task list of the policy.

----End

2.12.3 Associating New EVS Disks with a Backup Policy

You can associate new EVS disks to an existing backup policy. Backup and replication for these disks will be performed based on this policy.

Prerequisites

- A backup policy has been created.
- You have applied for the backup space. For details, see **2.4 Applying for Backup Space**.

Precautions

- A maximum of 64 EVS disks can be associated with a backup policy.
- Only the disks whose **Status** is **Available** or **In-use** can be associated.
- If the selected EVS disk has been associated with another backup policy, it will be disassociated from that backup policy first and then associated with the new backup policy. When an EVS disk is detached, all its snapshots are automatically deleted. If the EVS disk is associated with a new backup policy, you need to perform a full backup.

Procedure

Step 1 **Access the volume backup service console as a VDC administrator or a VDC operator**.

Step 2 On the **Volume Backup Service** page, click the **Policies** tab.

Step 3 In the row of the desired backup policy, click **Associated Disk**.

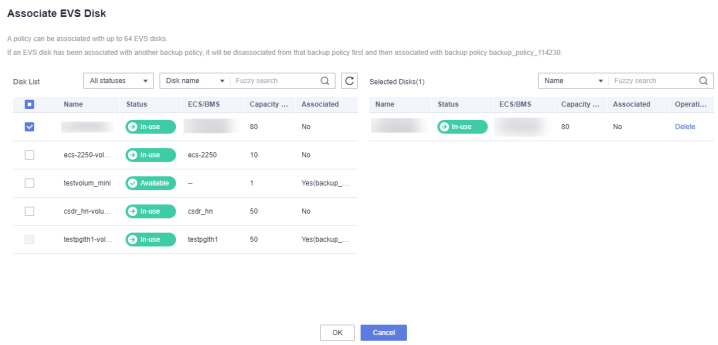
You can click ⌄ on the left of the backup policy, and click **Associate** in the **Associated Disks** area.

Step 4 From the **Disk List** on the left, click ☐ to select the EVS disks you want to back up. Then, they appear in the **Selected Disks** list on the right, as shown in **Figure 2-22**. You can click **Delete** in the **Operation** column to delete EVS disks that do not need to be backed up.

NOTE

- You can filter the disks by specifying the disk status, as well as by searching for **Disk name**, **Disk ID**, **Server name**, **Server ID**, and so on.
- EVS disks in different AZs cannot be associated with the same backup policy.
- If the selected EVS disks have been associated with another backup policy, they will be disassociated from that backup policy first and then associated with the new backup policy.

Figure 2-22 Associating a disk



Step 5 Click **OK**.

The result page is displayed, showing the result of association.

Step 6 Click **Close**.

----End

2.12.4 Disassociating EVS Disks from a Backup Policy

You can disassociate an EVS disk from an existing backup policy. After disassociation, this EVS disk will not be automatically backed up.

Prerequisites

- A backup policy has been created.
- The EVS disks have been associated with a backup policy.

Procedure

Step 1 **Access the volume backup service console as a VDC administrator or a VDC operator**.

Step 2 On the **Volume Backup Service** page, click the **Policies** tab.

Step 3 Click ⌄ on the left of the desired backup policy. The list of associated EVS disks is displayed in the **Associated Disk** area.

Step 4 In the list of associated EVS disks, locate the EVS disk to be disassociated from the backup policy and click **Disassociate** in the **Operation** column.

If you want to disassociate multiple EVS disks, select them and click **Disassociate** above the list.

Step 5 Confirm the information and click **OK**.

----End

2.12.5 Changing a Policy

You can decide whether to automatically backup/replication by enabling or disabling the option for a policy.

Prerequisites

- A policy has been created.
- A policy has been configured.

Precautions

- If a policy has a backup or replication task being executed when you change it, the task continues running until it finishes.
- A policy may contain multiple scheduling plans. You can change one or more scheduling plans.

Procedure

Step 1 **Access to volume backup service console as a VDC administrator or a VDC operator**

Step 2 On the **Volume Backup Service** page, click the **Policies** tab.

Step 3 Locate the row where the backup policy to be modified resides, and choose **More**.

NOTE

- If a full backup policy, incremental backup policy, or a replication policy is **Enabled** or **Disabled**, choose **More** > **Adjust Full Backup Policy Status**, **More** > **Adjust Incremental Backup Policy Status**, or **More** > **Adjust Replication Policy Status**.
- If the incremental backup policy is **Unconfigured**, you cannot perform the change operation.

Step 4 Click **OK**.

----End

2.12.6 Deleting a Backup Policy

If you do not need a backup policy, you can delete it.

Prerequisites

A backup policy has been created.

Precautions

If an automatic scheduling task is being executed when you delete a backup policy, wait until the task is complete and then delete the backup policy.

Procedure

Step 1 **Access to volume backup service console as a VDC administrator or a VDC operator**.

Step 2 On the **Volume Backup Service** page, click the **Policies** tab.

Step 3 Locate the row where the backup policy to be deleted resides, and choose **More** > **Delete Policy**.

NOTE

After a backup policy is deleted, the backup or replica will not be automatically deleted. You need to delete it manually. For details, see **2.11.2 Deleting an EVS Disk Backup or Replica**.

Step 4 Click **OK**.

----End

2.12.7 Changing the Validity Period of a Backup Policy

If the backup policy is about to expire or has expired but you want to continue to use it, you can modify the validity period of the backup policy to make it longer. In

addition, you can shorten the validity period by changing the validity period of the backup policy.

Prerequisites

A backup policy has been created.

Procedure

Step 1 **Access to volume backup service console as a VDC administrator or a VDC operator**.

Step 2 On the **Volume Backup Service** page, click the **Policies** tab.

Step 3 In the row where the backup policy you want to modify resides, choose **More** > **Modify Validity Period**.

NOTE

You can also change the validity period in **2.12.1 Editing a Backup Policy**.

Step 4 Change the validity period of a backup policy.

Possible values are **Never expires**, **By day**, and **By date**.

Step 5 Click **OK**.

----End

2.13 Managing Tasks

2.13.1 Viewing Tasks

Task management helps users better understand the detailed information about backup tasks, replication tasks, restoration tasks, deletion tasks, and export tasks within 30 days.

Prerequisites

At least one task exists.

Precautions

Only tasks of the last 30 days are contained in the Tasks list.

Procedure

Step 1 **Access the volume backup service console as a VDC administrator or a VDC operator**.

Step 2 On the **Volume Backup Service** page, click the **Tasks** tab page.

Step 3 Set the filter criteria to search for the target tasks.

Step 4 Click  and select desired items, including **Task ID**, **Task Type**, **Status**, **Disk Name**, **Policy Name**, **Start Time to End Time**, and **Execution Time (Minute)**.

Step 5 Click ⌄ on the left of a backup to view details. **Table 2-13** describes task parameters.

NOTE

The replication tasks and other replication-related parameters are displayed only when the replication policy is configured.

Table 2-13 Detailed task parameter

Task Type	Name	Description
Backup tasks	Backup ID	The backup ID is automatically generated by the system.
	Backup Name	The backup name is automatically generated by the system and complies with the following rules: • Automatic execution: – For backups: **autobk**_*xxxx* – For replicas: **autocp**_*xxxx* • Manual execution: – For backups: **manualbk**_*xxxx* – For replicas: **manualcp**_*xxxx* *xxxx* is automatically generated by the system. **NOTE** Name of the backup generated by immediate backup can be automatically generated by the system or customized.
	Policy Name	The policy name associated with the backup If a backup is not associated with any policy, the policy name is displayed as "--".
	Schedule ID	Policy scheduling ID Only the backup generated by the automatic schedule policy has a schedule ID. The schedule ID of the backup generated by manual backup is --.
Replication tasks	Source Backup ID	Source backup ID to be replicated
	Source Backup Name	Source backup name to be replicated
	Source Region	Region where the source backup locates

Task Type	Name	Description
	Target Replica ID	Target replica ID generated by replication
	Target Replica Name	Target replica name generated by replication
	Target Region	Region where the target replica locates
	Failure Cause	Cause of the failed task
Restoration tasks	Backup Name	The backup name is automatically generated by the system and complies with the following rules: ● Automatic execution: – For backups: **autobk**_*xxxx* – For replicas: **autocp**_*xxxx* ● Manual execution: – For backups: **manualbk**_*xxxx* – For replicas: **manualcp**_*xxxx* *xxxx* is automatically generated by the system. **NOTE** Name of the backup generated by immediate backup can be automatically generated by the system or customized.
	Backup ID	The backup ID is automatically generated by the system.
	Target EVS Disk Name	Name of the target disk for restoration
	Target EVS Disk ID	ID of the target disk for restoration
Deletion tasks	Backup ID	The backup ID is automatically generated by the system.

Task Type	Name	Description
	Backup Name	The backup name is automatically generated by the system and complies with the following rules: • Automatic execution: – For backups: **autobk**_*xxxx* – For replicas: **autocp**_*xxxx* • Manual execution: – For backups: **manualbk**_*xxxx* – For replicas: **manualcp**_*xxxx* *xxxx* is automatically generated by the system. **NOTE** Name of the backup generated by immediate backup can be automatically generated by the system or customized.
Exporting A Task	-	-

----End

2.13.2 Retrying a Task

You can only retry a task that fails to be retried automatically and is not retried manually.

Prerequisites

The system fails to retry automatically and there is no task that has been manually retried.

Precautions

The task management list only displays the tasks in the latest 30 days.

Procedure

Step 1 **Access the volume backup service console as a VDC administrator or a VDC operator**.

Step 2 On the **Volume Backup Service** page, click the **Tasks** tab page.

Step 3 Set filter criteria to quickly find the backup task that needs to be retried.

Step 4 Click **Retry** in the row where the backup task is located.

Step 5 Click **OK**.

----End

2.13.3 Downloading Tasks

You can set filter conditions to download tasks that meet the conditions to the local PC.

Prerequisites

You have exported the tasks to be downloaded.

Procedure

Step 1 **Access the volume backup service console as a VDC administrator or a VDC operator**.

Step 2 On the **Volume Backup Service** page, click the **Tasks** tab. On the displayed page, click **Export** to export all tasks.

You can also set filter conditions to download the tasks that meet the conditions, and click **Export**.

Step 3 Click **Download** to download the tasks to your local PC.

----End

2.14 FAQs

2.14.1 Accessing the Volume Backup Service Console as a VDC Administrator or a VDC Operator

Procedure

Step 1 Use a browser to log in to ManageOne as a VDC administrator or VDC operator.

URL in non-B2B scenarios: **https://***Domain name of ManageOne Operation Portal*, for example, **https://console.demo.com**

URL in B2B scenarios: **https://***Domain name of ManageOne Tenant Portal*, for example, **https://tenant.demo.com**

You can log in using a password or USB key.

- Login using a password: Enter the username and password.

  The password is that of the VDC administrator or VDC operator.
- Login using a USB key: Insert a USB key with preset user certificates, select the required device and certificate, and enter a PIN.

Step 2 Click  in the upper left corner of the page, select a region and choose **Storage** > **Volume Backup Service**.

----End

2.14.2 What Is the Difference Between Backup and Replication?

A backup operation stores data of an EVS disk to the local backup storage.

A replication operation copies backups (generated in backup operations, used to restore EVS disk data), and stores the backup copies to the remote backup storage. When the local backups are corrupted, the remote backup copies can be used instead to restore EVS disk data.

2.14.3 Does VBS Support Simultaneous Backup of Multiple EVS Disks on a Server?

Yes. You can create a backup policy and associate the backup policy with multiple EVS disks. Then the backup policy can be executed to back up the multiple EVS disks at the same time. Note that the EVS disks must have the same AZ with the associated backup policy.

2.14.4 Must I Stop the Server Before Backing Up EVS Disks on a Server Using VBS?

VBS can back up EVS disks that are in use. When a server is running properly, data is written to EVS disks of the server, and some newly generated data is stored in the server memory as cached data. During EVS disk backup, the data in the memory will not be automatically written to EVS disks, resulting in data inconsistency between EVS disks and their backups.

To ensure data integrity, back up EVS disks during off-peak hours when no data write operations are being performed on the EVS disks. Alternatively, suspend all data write operations and stop the application systems before initiating a backup job. For an extreme requirement for data integrity, stop the server (for cached data to be written to EVS disks) and start an offline backup task.

2.14.5 Does VBS Support Cross-region EVS Disk Backup and Restoration?

EVS disk backup and restoration operations can only be performed within a region but not across regions.

2.14.6 Must I Stop the Server Before Restoring EVS Disk Data with a VBS Backup?

Yes, you must stop the server to which the EVS disk is attached and detach the EVS disk from the server before restoring the EVS disk data using a VBS backup. After the EVS disk data is restored, attach the EVS disk to the server and start the server.

2.14.7 Can a VBS Backup of a System Disk Be Used to Restore the System Disk of a Server?

You can restore the ECS system disk using a VBS backup. Before restoring the system disk, you must detach it from the ECS.

2.14.8 Can I Use a VBS Backup to Restore an EVS Disk Whose Capacity Has Been Expanded?

Yes. If you back up an EVS disk using VBS and later expand the capacity of the EVS disk, you can still use the VBS backup to restore the EVS disk. However, the capacity of the restored EVS disk reverts to the original value due to file system restrictions. To avoid this, create a VBS backup for the EVS disk after expanding its capacity.

2.14.9 Replication Space Cannot Be Released After the Intra-Region Replication Function Is Disabled

Symptom

The VDC operator viewed the used replication space on the **Quota Management** page. However, the space occupied by the replicas was not displayed on the VBS or CSBS page. Clicked **Apply for Space** but the replication space cannot be released.

Possible Cause

The intra-region replication function is enabled in the AZ. After the VDC operator applied for replication quotas, the VDC administrator disabled the intra-region replication function in the AZ.

Procedure

Step 1 Contact the VDC administrator to enable the intra-region replication function of the AZ..

Step 2 On the VBS or CSBS page, click **Apply for Space** to reduce the replication space to 0.

----End

