Cloud Backup and Recovery

Hybrid Cloud Backup Feature Guide

Issue   01

Date   2020-02-25

Contents

1 What Is Hybrid Cloud Backup?

Overview

CBR allows you to synchronize backups of on-premises VMware VMs to the cloud, manage these backups, and restore data to cloud servers using such backups.

Hybrid cloud backup includes:

- VMware backup: You can synchronize the backups of VMware VMs to the cloud.

If a disaster happens to your data center or the fiber network becomes inaccessible, you can use the backups to quickly create servers on the cloud, minimizing service downtime. You can also replicate the backups to other regions as needed to quickly deploy services on the cloud.

Figure 1-1 Hybrid cloud backup architecture
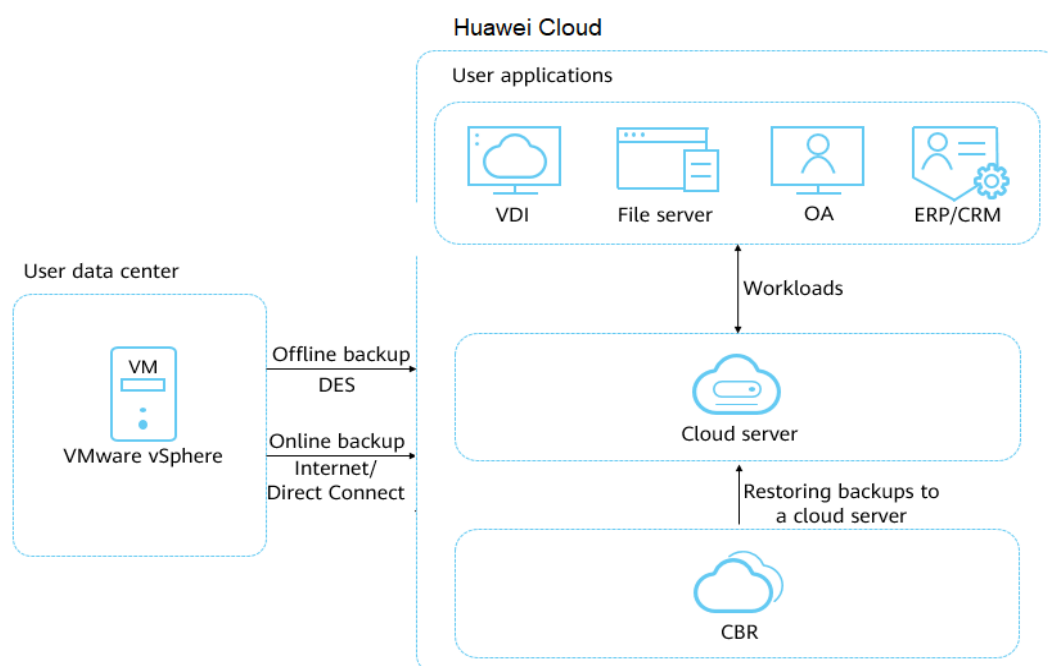
Advantages

- Cost-effectiveness

  CBR provides pay-per-use billing and elastic scaling of resources to keep costs down. By contrast, building a DR center on-premises is costly, time-consuming, and labor intensive.

- Cloud-based DR

  Most conventional backup software cannot restore data to cloud servers. However, you can use CBR to migrate on-premises backups to the cloud for data restoration on-premises or in the cloud.

- Fast data restoration

  To migrate an on-premises data center to the cloud or migrate services across regions in the cloud, usually you need to provision new cloud servers, manually configure software and domain names, and commission the system, which takes a long time. CBR allows you to synchronize on-premises backups to the cloud, and then restore data to cloud servers from the backups within minutes.

2 Application Scenarios

VMware Backup

VMware hybrid cloud backup allows you to back up VMware VMs in your data center. You can use the public cloud as the remote DR site, and synchronize the backups of VMware VMs to the cloud. In case of an accidental deletion, software upgrade failure, or virus attack, you can use the synchronized backups to restore on-premises VMware VMs. If a network fault or natural disaster occurs, you can restore data to cloud servers from backups, mitigating service interruptions.

Figure 2-1 shows the VMware backup architecture.

Figure 2-1 VMware backup architecture
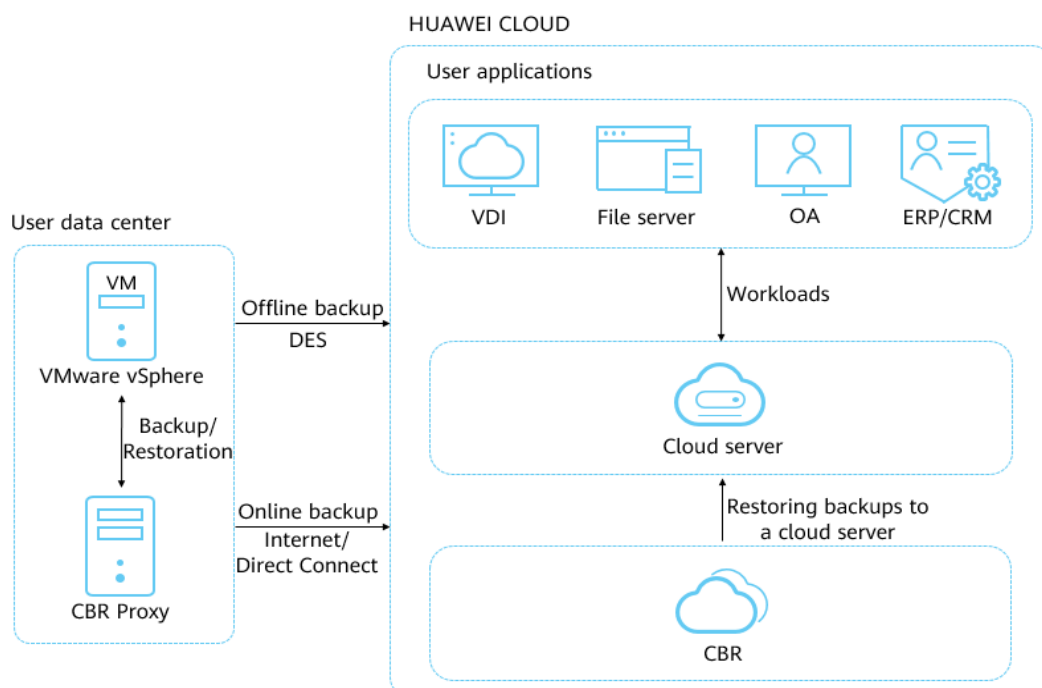
3 Constraints

VMware Backup

- VM backups from the following VMware vSphere versions can be restored to cloud servers: 5.1, 5.5, 6.0, 6.5. If you do not need to restore the backups to cloud servers, there is no restriction on the VMware version.

- To obtain better performance and operation experience, you are advised to use the OSs listed in **Table 3-1**, which have passed the compatibility test.

- The VDDK version of VMware 6.5 VMs must be 6.0.3.

- Backups synchronized to the cloud cannot be used to create cloud servers.

- Backups synchronized to the cloud can only be restored to other cloud servers running the same OS, and can be restored to system disks or data disks.

- Servers whose system disks are configured with LVM cannot be restored on cloud.

- Before the restoration, configure security groups according to the procedure. Otherwise, the restoration may fail.

Table 3-1 OSs that support restoration to the cloud

OS	Supported Version
Windows	Windows 7
	Windows Server 2008 R2
	Windows Server 2012
	Windows Server 2012 R2
	Windows Server 2016
	Windows Server 2019

OS	Supported Version
CentOS	CentOS 6.4
	CentOS 6.5
	CentOS 7.2
	CentOS 7.3
	CentOS 7.4
	CentOS 7.5
	CentOS 7.6
	CentOS 7.7
Red Hat	Red Hat 6.4
	Red Hat 6.5
	Red Hat 7.2

4 VMware Backup

4.1 VMware Backup Process

Figure 4-1 shows the process for backing up VMware VMs.

Figure 4-1 VMware backup process
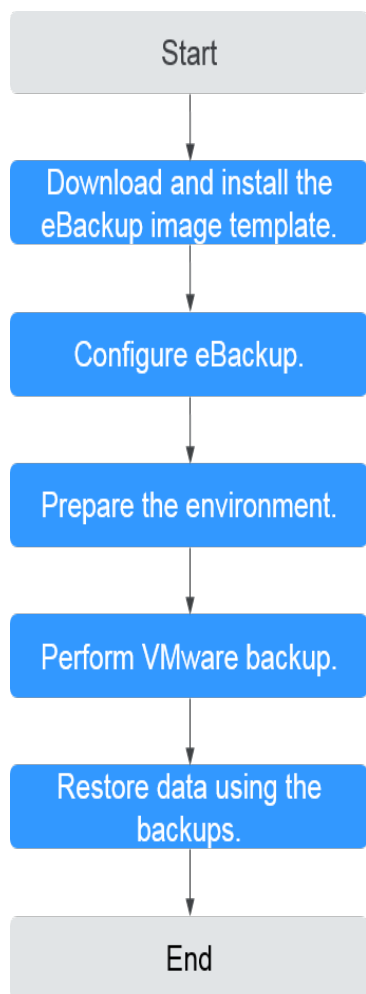
1. Download and install the eBackup image template: Download the eBackup image template before backing up VMware VMs. For details, see **Downloading the eBackup Image Template** and **Installing eBackup**.

2. Configure eBackup: Configure eBackup after the installation. For details, see **Configuring the Backup Server**.

3. Prepare the environment: After eBackup is configured, prepare the environment by referring to **Adding a VMware Protected Environment**. Also, you need to purchase a hybrid cloud backup vault on the console. Then create a storage unit, storage pool, and a vault in eBackup. For details, see **Purchasing a Hybrid Cloud Backup Vault for VMware Backups**.

4. Perform VMware backup: After the preparations are complete, you can back up VMware data. For details, see **Creating a Protected Set**.

5. Restore data using the backups: Use the backup data of the VM disks to restore to the original VM or another VM, or synchronize the backup data to the cloud and then restore to servers on the cloud using the backups. For details, see **Restoring VM Disks to the Original VM**.

4.2 Downloading the eBackup Image Template

Before backing up VMware VMs, you need to download the eBackup image template from the console and install eBackup.

When downloading a software package, obtain the **.asc** signature file and use the digital signature public key and validation tool provided by the Huawei support website to validate the software package integrity.

📖 **NOTE**

    Installing eBackup does not affect VM services and occupies few resources.

Procedure

Step 1 Log in to the CBR console.

1. Log in to the management console.

2. Click ⊙ in the upper left corner and select a region.

3. Choose **Storage** > **Cloud Backup and Recovery** > **Hybrid Cloud Backups** > **VMware Backups**.

Step 2 Click the **Image Download and Installation** tab. Then click **Download** below **eBackup Image Template**.

After the template is downloaded, you can download the *eBackup Installation Guide* and install eBackup by following the instructions provided in the guide.

----End

Follow-up Procedure

If the download dialog box disappears when you download eBackup using Google Chrome, rectify the fault by following the instructions in **The Download Dialog Box Disappears When I Download eBackup on a VMware VM**.

4.3 Enabling Cloud and On-premises Communication

After the eBackup image template is downloaded, you need to configure the network to enable cloud and on-premises communication.

Context

There are two methods for enabling network communication on and off the cloud, which are suitable for different scenarios. Select either of them based on site requirements.

Through a VPC endpoint

If your local data center has been connected to your VPC through a VPN connection or a direct connection, you can use a VPC endpoint to access CBR through the intranet, so as to migrate VMware backups to the cloud. To access the gateway of CBR, configure the private IP address of the VPC endpoint and private domain name of CBR in the **hosts** file of eBackup. Then, the VPC endpoint will automatically resolve the domain name to the corresponding IP address, implementing on-premises and cloud communication. For details about VPC endpoints, see **What Is VPC Endpoint?**

Through the network plane configured with an external IP address

If you have configured an IP address that can connect to external networks when planning the network in your local data center, bind the NIC of the backup storage plane to the IP address when configuring the backup server. Then you can migrate VMware backups to the cloud.

Procedure for Configuring Communication Through a VPC Endpoint

Step 1 Log in to the Huawei Cloudconsole.

1. Log in to the management console.

2. Click ⊙ in the upper left corner and select a region.

3. Choose **Network** > **VPC Endpoint** > **VPC Endpoints**.

Step 2 Click **Create VPC Endpoint** in the upper right corner.

Step 3 Buy and configure a VPC endpoint by referring to **Accessing OBS**.

----End

Procedure for Configuring the Communication on the Network Plane Bound with an External IP Address

Step 1 Complete operations in **Planning the Network** and **Installing eBackup**.

Step 2 Complete **Step 1** to **Step 5** in **Configuring the Backup Server**.

Step 3 In **Step 6**, bind the NIC of the backup storage plane to the IP address that is connected to external networks.

----End

4.4 Planning the Network

Before installing and configuring eBackup, you need to understand the network requirements and suggestions for eBackup to facilitate network planning.

Typical Networking Suggestions

By default, eBackup has five network planes. You need to plan an IP address for each network plane to ensure communication between eBackup and peripheral components. **Network Planes** describes the network planes. This section describes typical networking suggestions for eBackup in VMware backup to the cloud.

- Plan two IP addresses for eBackup: an internal IP address and a public IP address.

  In this scenario, ensure that the internal IP address can communicate with the terminal that accesses the eBackup management plane, vCenter Server/ESXi host, and production storage; ensure that the public IP address can communicate with the backup storage.

  In this case, configure two NICs for eBackup. One is configured with the internal IP address, and the other with the public IP address.

  The production management plane, backup management plane, internal communication plane, and production storage plane of eBackup are integrated and bound to the NIC using the internal IP address. The eBackup backup storage plane is bound to the NIC using the public IP address.

  Table 4-1 lists the example IP addresses of eBackup network planes and peripheral components.

- Plan one IP address for eBackup.

  In this scenario, ensure that the IP address can communicate with the terminal that accesses the eBackup management plane, vCenter Server/ESXi host, production storage, and backup storage.

  In this case, configure one NIC for eBackup and configure an internal IP address for the NIC.

  All eBackup network planes are integrated. The production management plane, backup management plane, internal communication plane, production storage plane, and backup storage plane of eBackup are bound to the same NIC.

  Table 4-1 lists the example IP addresses of eBackup network planes and peripheral components.

Network Planes

Figure 4-2 shows the eBackup network planes.

Figure 4-2 eBackup network planes
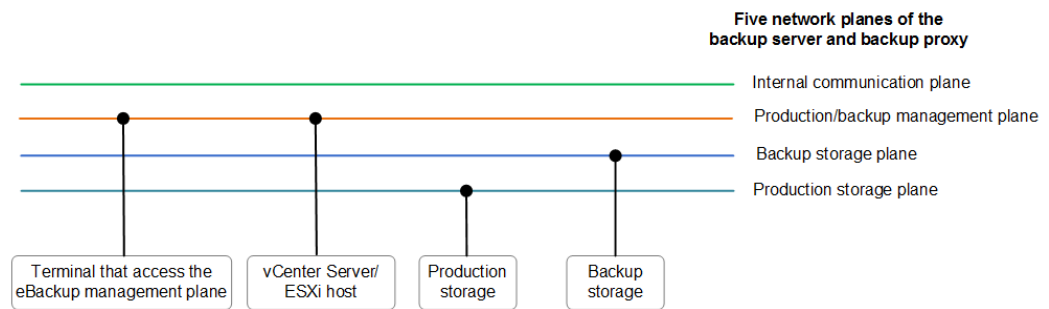
Table 4-1 eBackup network plane description

Item	Description	Example Configuration (Two IP Addresses Planned)	Example Configuration (One IP Addresses Planned)
Terminal that accesses the eBackup management plane	The terminal uses the IP address of the eBackup management plane to access the eBackup system to configure and manage backup and restoration services.	192.168.1.11	192.168.1.11
vCenter Server/ESXi host	Centrally manages vCenter Servers or ESXi hosts of VMware VMs.	192.168.1.15	192.168.1.15
Production storage	Production storage connected to the VMware virtual environment	192.168.1.16	192.168.1.16
Backup storage	Purchased vault that stores backup data	10.10.1.15	192.168.1.18
Management plane	• Production management plane Network plane between the backup server, backup proxy, and vCenter Server/ESXi host • Backup management plane Network plane between the backup server, backup proxy, and terminal that accesses the eBackup management plane	192.168.1.10	192.168.1.10

Item	Description	Example Configuration (Two IP Addresses Planned)	Example Configuration (One IP Addresses Planned)
Internal communication plane	Network plane between the backup server and backup proxy	192.168.1.10	192.168.1.10
Production storage plane	Network plane between the backup server, backup proxy, and production storage	192.168.1.10	192.168.1.10
Backup storage plane	Network plane between the backup server, backup proxy, and backup storage	10.10.1.10	192.168.1.10

4.5 Installing eBackup

This section describes how to use VMware vSphere Client to create a VM using an eBackup image template and configure a network for the VM.

Context

- VM backups from the following VMware vSphere versions can be restored to cloud servers: 5.1, 5.5, 6.0, 6.5. If you do not need to restore the backups to cloud servers, there is no restriction on the VMware version.

- An eBackup management system has only one backup server but supports multiple backup proxies. Plan the number of backup proxies based on the number of VMs to be protected.

- This section uses VMware vSphere Client 6.0 as an example. If the VMware vSphere Client of another version is used, see the related VMware documents.

- The image template does not contain Virtual Disk Development Kit (VDDK) of VMware. You need to visit **https://developer.vmware.com/web/sdk/6.0/vddk/** to download VDDK.

- The VDDK version of VMware 6.5 VMs must be 6.0.3.

- If the eBackup image package installed only supports VMware 6.5 or earlier and you want to upgrade it to a version supporting VMware 6.7 or later, upgrade eBackup first.

- The VM used to install eBackup must have at least 4 vCPUs and 8 GiB of memory, and the system disk and data disks of the VM must each have at least 200 GB of capacity.

Prerequisites

- VMware vSphere Client has been installed.

- The eBackup image template has been downloaded.

- The VDDK package **VMware-vix-disklib-6.0.3-4888596.x86_64.tar.gz** has been obtained.

● A cross-platform file transfer tool, such as WinSCP, is available.

Procedure

Step 1 Decompress the downloaded eBackup image template package to obtain the files.

Step 2 Start the VMware vSphere Client and choose **File** > **Deploy OVF Template**.

Step 3 Select. Click **Next**.

Step 4 View details of the OVF template and click **Next**.

Step 5 Specify the name and location for the deployed template, and click **Next**.

Step 6 Select the host or cluster on which you want to run the deployed template, and click **Next**.

Step 7 Select the target storage of the VM file and click **Next**.

Step 8 Set the VM disk format to **Thick Provision Lazy Zeroed**, and click **Next**.

Step 9 Select the network mapping of the VM and click **Next**.

Step 10 View the VM deployment settings and click **Finish**.

Step 11 Wait until the VM is deployed.

Step 12 Modify network labels of VMs.

1. In the VM list on the left, click the created VM.
2. Click the **Getting Started** tab.
3. Click **Edit virtual machine settings**.
4. On the page that is displayed, select a network adapter, and select a network label from the **Network label** drop-down list based on the site requirements.

   📖 NOTE

   The VM created using the template has three NICs by default. Select the network label based on **Planning the Network**.

5. After modifying the network labels of all network adapters, click **OK**.

Step 13 In the VM list on the left, click the created VM.

Step 14 Click 🔼 to wait for the VM to start.

Step 15 After the VM is started, click the **Console** tab.

Step 16 Enter **root** and its password to log in to the VM.

The preset password of user **root** is **Cloud12#$**.

Step 17 Configure a static IP address for each NIC of the VM.

For IP address planning, see **Planning the Network**.

1. Run the **cd /etc/sysconfig/network-scripts/** command to go to the **network-scripts** directory.
2. Run the **ip a** command to view the network adapter name on the VM. **eth0** is as an example name. Replace it with the actual name.

3. Run the **vi ifcfg-eth0** command to open the **ifcfg-eth0** configuration file:

4. Press **i** to enter editing mode and modify the file.

   Set the following parameters. If they do not exist, enter them manually.

   - **BOOTPROTO="static"** indicates that the static IP address is used.
   - **IPADDR**, **NETMASK**, and **GATEWAY**: Set them to the planned VM IP address, subnet mask, and gateway, respectively.
   - **ONBOOT=yes** indicates that the network adapter is started upon system startup.

5. Press **Esc**, enter **:wq**, and press **Enter** to save the settings and exit.

6. Configure static IP addresses for other network adapters by referring to **Step 17.3** to **Step 17.5**.

Step 18 Run the **service network restart** command to restart the network.

Step 19 On the maintenance terminal, use WinSCP to upload **VMware-vix-disklib-6.0.3-4888596.x86_64.tar.gz** to any directory, for example, **/opt**.

Step 20 Run the **cd /opt** command to go to the **/opt** directory.

Step 21 Run the **tar -xvf VMware-vix-disklib-6.0.3-4888596.x86_64.tar.gz** command to decompress the VDDK package.

Step 22 Run the **mkdir -p /opt/huawei-data-protection/ebackup/microservice/ebk_vmware/lib/3rd/vddk/lib64** command to create the **/opt/huawei-data-protection/ebackup/microservice/ebk_vmware/lib/3rd/vddk/lib64** directory.

Step 23 Run the **cp -d /opt/vmware-vix-disklib-distrib/lib64/lib* /opt/huawei-data-protection/ebackup/microservice/ebk_vmware/lib/3rd/vddk/lib64/** command to copy the VDDK file to the directory created in **Step 22**.

Step 24 Run the **chmod 550 -R /opt/huawei-data-protection/ebackup/microservice/ebk_vmware/lib/3rd/vddk/** command to change the directory permissions.

Step 25 Run the **chown hcpprocess:hcpmgr -R /opt/huawei-data-protection/ebackup/microservice/ebk_vmware/lib/3rd/vddk/** command to change the directory owner group to **hcpprocess**.

----End

Follow-Up Operations

- If a user uses a private line or VPN to access Huawei Cloud, configure theHuawei Cloud DNS on the backup server and backup proxy.

- If an eBackup server needs to connect to other network segments or IP addresses of the management or storage plane (including production storage plane and backup storage plane), you need to configure the route.

  a. Run the **ifconfig** command to check the information about the network adapter that communicates with the management plane or storage plane.

  ```
  eth2   Link encap:Ethernet  HWaddr 2A:BE:D4:88:99:01
       inet addr:192.168.31.190  Bcast:192.168.31.255  Mask:255.255.255.0
  …
  ```

  b. Run the **vi /etc/sysconfig/static-routes** command to open the configuration file.

c. Add the following route information to the file and enter **:wq** to save the file and exit.

```
any net 192.168.1.0 netmask 255.255.255.0 gw 192.168.31.1 dev eth2
```

📖 **NOTE**

The four columns in the command output indicate the target network, subnet mask of the target network, local gateway, and network adapter name, respectively.

d. Run the **service network restart** command to restart network to make the route take effect.

e. Run the **route** command to check the route information.

```
Kernel IP routing table
Destination    Gateway        Genmask        Flags Metric Ref    Use Iface
192.168.1.0    192.168.31.1   255.255.255.0  UG    0     0        0 eth2
```

4.6 Configure eBackup

4.6.1 Configuring the Backup Server

Initiate a server on which eBackup is installed as backup server and configure related parameters.

Prerequisites

- Network plane parameters of the backup server have been planned.
- A cross-platform remote access tool, such as PuTTY, is available.
- The password of user **root** for logging in to the eBackup server has been obtained.

Procedure

Step 1 Log in to the eBackup server to be configured as user **root**.

The default password of user **root** is **Cloud12#$**.

Use a cross-platform access tool or the console of the VMware vSphere Client to log in.

Step 2 Run the **cd** *PathOfBackupSoftwarePackage* command to go to the directory containing the initial configuration script.

The backup software installation package is stored in **/opt/eBackup_8.0.0-LHC01/action**.

Step 3 Run the **sh ebackup_utilities.sh config** command to start the initial configuration.

The following information is displayed:

```
Please select network type for this machine:
 1.ipv4
 2.ipv6
```

Step 4 Enter **1** and press **Enter**.

```
1
Please select a role for this machine:
```

```
1.Backup Server
2.Backup Proxy
3.Backup Manager
4.Backup Workflow Server
```

Step 5 Enter **1** and press **Enter**.

```
1
===============================================================================
=============
Note:
In the following steps you will be required to configure four network planes for eBackup.
The definition of each network plane is as follows:
Backup management plane: the communication plane for eBackup to provide external services.
Internal communication plane: the communication plane between backup server and backup proxy.
Production management plane: the communication plane between eBackup and the management plane of
the production end.
Storage plane: the communication plane between eBackup and the storage plane of the production end
and communication plane between eBackup and backup storage.
===============================================================================
=============

Set network adapter for 'Backup management' network plane:
[1] bond1 MAC=28:6E:D4:88:C6:F2 IP=192.168.1.10 MASK=255.255.254.0
[2] bond2 MAC=28:6E:D4:88:C6:F3 IP=10.10.1.10 MASK=255.255.254.0
Which network adapter from the above list would you like to bind to the 'Backup management' network
plane?
```

Step 6 Configure network planes for the backup server.

> **NOTICE**
>
> You need to bind NICs to the five network planes of the backup server. Select the
> NIC to be bound based on the network planning in **Planning the Network**.
>
> In this section, the backup server is configured with two NICs, the backup
> management plane, production management plane, internal communication
> plane, and production storage plane are bound to one NIC, and the backup
> storage plane is bound to another NIC.

1. Select the network adapter you want to bind to the backup management
   plane, and press **Enter**.

   > 📖 **NOTE**
   >
   > If you choose **bond1** as the network adapter binding to the backup management
   > plane, input **1**.

   ```
   1
   Set network adapter for 'Internal communication' network plane:
   [1] bond1 MAC=28:6E:D4:88:C6:F2 IP=192.168.1.10 MASK=255.255.254.0
   [2] bond2 MAC=28:6E:D4:88:C6:F3 IP=10.10.1.10 MASK=255.255.254.0
   Which network adapter from the above list would you like to bind to the 'Internal communication'
   network plane?
   ```

2. Select the network adapter you want to bind to the internal communication
   plane, and press **Enter**.

   ```
   1
   Set network adapter for 'Production management' network plane:
   [1] bond1 MAC=28:6E:D4:88:C6:F2 IP=192.168.1.10 MASK=255.255.254.0
   [2] bond2 MAC=28:6E:D4:88:C6:F3 IP=10.10.1.10 MASK=255.255.254.0
   Which network adapter from the above list would you like to bind to the 'Production management'
   network plane?
   ```

3. Select the network adapter you want to bind to the production management
   plane, and press **Enter**.

```
1
Set network adapter for 'Production Storage' network plane:
[1] bond1 MAC=28:6E:D4:88:C6:F2 IP=192.168.1.10 MASK=255.255.254.0
[2] bond2 MAC=28:6E:D4:88:C6:F3 IP=10.10.1.10 MASK=255.255.254.0
Which network adapter from the above list would you like to bind to the 'Production Storage'
network plane?
```

4. Select the network adapter you want to bind to the production storage plane, and press **Enter**.

```
1
Set network adapter for 'Backup Storage' network plane:
[1] bond1 MAC=28:6E:D4:88:C6:F2 IP=192.168.1.10 MASK=255.255.254.0
[2] bond2 MAC=28:6E:D4:88:C6:F3 IP=10.10.1.10 MASK=255.255.254.0
Which network adapter from the above list would you like to bind to the 'Backup Storage' network
plane?
```

5. Select the network adapter you want to bind to the backup storage plane, and press **Enter**.

```
2
Enter a floating IP address that is in the same network segment as the internal communication plane.
```

6. Configure the floating IP address.

Enter the floating IP address of the internal communication plane. Ensure that the floating IP address is in the same network segment as the IP address of the internal communication plane and is not occupied.

If the following command output is displayed, the configuration is successful.

```
192.168.1.12
Configuration succeeded.
grep: this version of PCRE is compiled without UTF support
The ebk_accelerator agent of OceanStor BCManager eBackup was started successfully.
Start:ebk_accelerator service succeeded.
start reload gaussdb
grep: this version of PCRE is compiled without UTF support
The ebk_backup agent of OceanStor BCManager eBackup was started successfully.
Start:ebk_backup service succeeded.
grep: this version of PCRE is compiled without UTF support
The ebk_copy agent of OceanStor BCManager eBackup was started successfully.
Start:ebk_copy service succeeded.
grep: this version of PCRE is compiled without UTF support
The ebk_delete agent of OceanStor BCManager eBackup was started successfully.
Start:ebk_delete service succeeded.
grep: this version of PCRE is compiled without UTF support
The ebk_mgr agent of OceanStor BCManager eBackup was started successfully.
Start:ebk_mgr service succeeded.
grep: this version of PCRE is compiled without UTF support
The ebk_restore agent of OceanStor BCManager eBackup was started successfully.
Start:ebk_restore service succeeded.
grep: this version of PCRE is compiled without UTF support
The ebk_vmware agent of OceanStor BCManager eBackup was started successfully.
Start:ebk_vmware service succeeded.

service hcp start:completed
You can access the eBackup UI using the following link.
 https://192.168.1.10:8088 or 192.168.1.10
Alternatively, you can access the eBackup CLI through SSH session.
```

Step 7 Run the following commands in sequence to perform security hardening:

After security hardening, do not log in as user **root**. Instead, log in as user **hcp**. The default password of user **hcp** is **PXU9@ctuNov17!**.

cd /opt/huawei-data-protection/ebackup/bin/StandardHardening

echo -e "yes\nyes\n"|./StandardSuseHardening.sh

📖 **NOTE**

> After you run this command, the eBackup server restarts. If you need to log in to the eBackup server, try again later.

----End

4.6.2 (Optional) Configuring a Backup Proxy

If backup proxies are planned for an eBackup management system, you need to initialize servers (except the backup server) running eBackup as backup proxies and configure related parameters.

Prerequisites

- Backup proxy parameters have been planned. Multiple backup proxies can be configured in one eBackup system.
- The backup server has been configured.
- A cross-platform remote access tool, such as PuTTY, is available.
- The password of user **root** for logging in to the eBackup server has been obtained.

Procedure

Step 1 Log in to the eBackup server to be configured as user **root**.

The default password of user **root** is **Cloud12#$**.

Use a cross-platform access tool or the console of the VMware vSphere Client to log in.

Step 2 Run the **cd** *PathOfBackupSoftwarePackage* command to go to the directory containing the initial configuration script.

The backup software installation package is stored in **/opt/eBackup_8.0.0-LHC01/action**.

Step 3 Run the **sh ebackup_utilities.sh config** command to start the initial configuration.

The following information is displayed:

```
Please select network type for this machine:
 1.ipv4
 2.ipv6
```

Step 4 Enter **1** and press **Enter**.

```
1
Please select a role for this machine:
 1.Backup Server
 2.Backup Proxy
 3.Backup Manager
 4.Backup Workflow Server
```

Step 5 Enter **2** and press **Enter**.

```
2
=====================================================================================
=============
Note:
```

> In the following steps you will be required to configure four network planes for eBackup.
> The definition of each network plane is as follows:
> Backup management plane: the communication plane for eBackup to provide external services.
> Internal communication plane: the communication plane between backup server and backup proxy.
> Production management plane: the communication plane between eBackup and the management plane of the production end.
> Storage plane: the communication plane between eBackup and the storage plane of the production end and communication plane between eBackup and backup storage.
> ==
>
> Set network adapter for 'Backup management' network plane:
> [1] bond1 MAC=28:6E:D4:88:C6:F2 IP=192.168.1.11 MASK=255.255.254.0
> [2] bond2 MAC=28:6E:D4:88:C6:F3 IP=10.10.1.11 MASK=255.255.254.0
> Which network adapter from the above list would you like to bind to the 'Backup management' network plane?

Step 6 Configure network planes for the backup proxy.

NOTICE

You need to bind NICs to the five network planes of the backup proxy. Select the NIC to be bound based on the network planning in **Planning the Network**.

In this section, the backup proxy is configured with two NICs, the backup management plane, production management plane, internal communication plane, and production storage plane are bound to one NIC, and the backup storage plane is bound to another NIC.

---

1. Select the network adapter you want to bind to the backup management plane, and press **Enter**.

   NOTE

   If you choose **bond1** as the network adapter binding to the backup management plane, input **1**.

   > 1
   > Set network adapter for 'Internal communication' network plane:
   > [1] bond1 MAC=28:6E:D4:88:C6:F2 IP=192.168.1.11 MASK=255.255.254.0
   > [2] bond2 MAC=28:6E:D4:88:C6:F3 IP=10.10.1.11 MASK=255.255.254.0
   > Which network adapter from the above list would you like to bind to the 'Internal communication' network plane?

2. Select the network adapter you want to bind to the internal communication plane, and press **Enter**.

   > 1
   > Set network adapter for 'Production management' network plane:
   > [1] bond1 MAC=28:6E:D4:88:C6:F2 IP=192.168.1.11 MASK=255.255.254.0
   > [2] bond2 MAC=28:6E:D4:88:C6:F3 IP=10.10.1.11 MASK=255.255.254.0
   > Which network adapter from the above list would you like to bind to the 'Production management' network plane?

3. Select the network adapter you want to bind to the production management plane, and press **Enter**.

   > 1
   > Set network adapter for 'Production Storage' network plane:
   > [1] bond1 MAC=28:6E:D4:88:C6:F2 IP=192.168.1.11 MASK=255.255.254.0
   > [2] bond2 MAC=28:6E:D4:88:C6:F3 IP=10.10.1.11 MASK=255.255.254.0
   > Which network adapter from the above list would you like to bind to the 'Production Storage' network plane?

4. Select the network adapter you want to bind to the production storage plane, and press **Enter**.

```
1
Set network adapter for 'Backup Storage' network plane:
[1] bond1 MAC=28:6E:D4:88:C6:F2 IP=192.168.1.11 MASK=255.255.254.0
[2] bond2 MAC=28:6E:D4:88:C6:F3 IP=10.10.1.11 MASK=255.255.254.0
Which network adapter from the above list would you like to bind to the 'Backup Storage' network
plane?
```

5. Select the network adapter you want to bind to the backup storage plane, and press **Enter**.

```
2
Please input the leader IP(The IP of internal communication plane at backup server):
```

6. Enter the internal communication plane IP address of the backup proxy and press **Enter**.

```
192.168.1.10
Please input the floating IP address at backup server:
```

7. Enter the floating IP address of the backup proxy and press **Enter**.

```
192.168.10.12
Please enter the public key of the backup server. To obtain the public key, run the following CLI
command: show server_public_key.
To use the default public key, press Enter.
```

8. Enter the public key of the backup proxy and press **Enter**. If you use the default public key, press **Enter**.

   ◫ NOTE

   > After the initial configuration of the backup proxy is complete, you need to reconfigure the backup proxy once the backup server is replaced. During the reconfiguration, the default public key cannot be used. For how to obtain the new public key of the backup server, see **Related Operations**.

   If the following command output is displayed, the configuration is successful.

   ```
   service hcp start:completed
   You can access the eBackup UI using the following link.
    https://backup server's backup management plane:8088 or backup server's backup management
   plane
   Alternatively, you can access the eBackup CLI through SSH session.
   ```

Step 7 Run the following commands in sequence to perform security hardening:

After security hardening, do not log in as user **root**. Instead, log in as user **hcp**. The default password of user **hcp** is **PXU9@ctuNov17!**.

cd /opt/huawei-data-protection/ebackup/bin/StandardHardening

echo -e "yes\nyes\n"|./StandardSuseHardening.sh

   ◫ NOTE

   > After you run this command, the eBackup server restarts. If you need to log in to the eBackup server, try again later.

----End

Related Operations

After the initial configuration of the backup proxy is complete, you need to reconfigure the backup proxy once the backup server is replaced. During the reconfiguration, the default public key cannot be used. Perform the following steps to obtain the new public key of the backup server:

1. Log in to the backup server as user **hcp**.

   The default password of user **hcp** is **PXU9@ctuNov17!**.

2. Run the **su root** command and enter the password of user **root** to switch to user **root**.

3. Run the **cd /opt/huawei-data-protection/ebackup/cli/** command to go to the **/opt/huawei-data-protection/ebackup/cli/** directory.

4. Run the **sh hcpcli.sh admin** command and enter the password of user **admin**.

   The default password of user **admin** is **PXU9@ctuNov17!**.

5. Run the **setting** command.

6. Run the **show server_public_key** command to obtain the public key.
   ```
   IP          Public Key
   -----------  ---------------------------------------
   172.28.12.5  E]D)b9M?G.mgAhl@cA)bhKc1F(.B[+uLkiEGp-+/
   ```

   The field under **Public Key** is the public key.

7. Enter **exit** and press **Enter** to exit the **setting** interface.

8. Enter **exit** and press **Enter** to exit the **admin** interface.

9. Enter **y** and press **Enter** to exit.

4.6.3 (Optional) Configuring HA

You can configure high availability (HA) for backup servers to enhance the reliability of backup servers.

Prerequisites

You have determined the backup servers and backup proxies corresponding to the active and standby HA nodes.

Context

HA refers to that active and standby modules work in hot or cold backup mode to implement specific functions. When the active module is faulty, the standby module automatically takes over the role of the active module to implement system functions, improving system reliability.

To enable eBackup to support the HA function, plan at least two eBackup servers (with one initialized as the backup server, and the others as backup proxies). After eBackup is installed and configured, the HA function is disabled by default. You need to configure HA parameters to configure eBackup as an HA system. After the configuration, the backup server and one backup proxy work in active/standby mode. If the backup server fails, the backup proxy takes over the role of the backup server to ensure normal system operation.

Procedure

Step 1 On the navigation bar, choose 〰 > **Server**.

Step 2 **(Optional)** In the upper right corner, set the search criteria and click 🔍 to search for the desired server.

Step 3 Click the drop-down arrow of **HA Management** and choose **Add HA member** from the shortcut menu.

Step 4 Select a backup proxy whose **Accessibility Status** is **Accessible**, and **Register Status** is **Registered** as the standby node in the HA system as prompted. Then set the backup server as the active node.

Step 5 Configure **Floating IP address** and **Quorum gateway(s)**.

Quorum gateways must be able to communicate with management planes of active and standby nodes. The IP addresses of the quorum gateways must be unique and must not start with 127.

----End

4.6.4 Configuring Management Data Backup Storage

Configure the backup storage for eBackup system management data (database and configuration files), which can be used to restore the eBackup system in the event of a disaster. eBackup supports the NFS, S3, FTP and SFTP storage as the backup storage of management data. This section describes how to configure the backup storage of the S3 type.

Context

- When backing up eBackup management data, calculate the shared storage capacity in advance. If the shared storage capacity is not enough, the latest backup job will fail. The shared storage capacity is related to the backup data retention policy:

  - If **Daily Backup** is selected

    The capacity of shared storage for storing backup management data = [(Number of yearly backups + Number of monthly backups + Number of weekly backups + Number of daily backups +1) x 10 + 15] GB.

    - For example, if the default retention policy is used, the capacity of shared storage for storing backup management data = [(0 + 1 + 1 + 1 + 1) × 10 + 15] GB = 55 GB.

    - If **Number of retained copies generated in yearly backup** is set to **Permanent**, planned capacities depend on the number of years for saving backups. The capacity of shared storage for storing backup management data = [(Number of years for saving backups + Number of monthly backups + Number of weekly backups + Number of daily backups + 1) × 10 + 15] GB.

  - If **Hourly Backup** is selected

    The capacity of shared storage for storing backup management data = [(Number of yearly backups + Number of monthly backups + Number of weekly backups + Number of daily backups + Number of hourly backups + 1) x 10 + 15] GB.

    - For example, if the default retention policy is used, the capacity of shared storage for storing backup management data = [(0 + 1 + 1 + 1 + 1 + 1) × 10 + 15] GB = 65 GB.

    - If **Number of retained copies generated in yearly backup** is set to **Permanent**, planned capacities depend on the number of years for saving backups. The capacity of shared storage for storing backup management data = [(Number of years for saving backups +

Number of monthly backups + Number of weekly backups + Number of daily backups + Number of hourly backups + 1) × 10 + 15] GB.

- Configure separate backup storage space for eBackup management data.
- You are advised to use the purchased hybrid cloud backup vault for S3 backup storage.

Prerequisites

- You have planned the capacity of the S3 shared storage. The capacity of the shared storage must meet the requirements. Or, the backup job will fail. For details, see **Context**.
- You have obtained the domain name or IP address of the S3 storage service plane, and the name, AK, and SK of the bucket that stores backup data.

Procedure

Step 1 Log in to the eBackup management system using the **admin** account.

For details, see **Logging In to eBackup**.

Step 2 In the navigation tree, choose ⚙ > **Configuration** > **Management Data Backup**.

Step 3 Click **Set Backup Storage**.

Step 4 Configure the backup storage of the eBackup management data.

Table 4-2 describes the parameters.

NOTICE

Do not use the same bucket as the backup storage of the management data and user VM data. Or, backup jobs will fail.

Table 4-2 Backup storage (S3) parameters

Parameter	Description	Setting Rule
Type	Type of the backup storage for the management data	S3
Protocol	Network protocol for the communication between the eBackup management system and S3 storage. Options include **HTTP** and **HTTPS**.	- If **HTTPS** is specified, import a valid certificate to verify the S3 storage. Obtain the certificate from the S3 storage administrator in advance. - Security risks arise if the protocol is set to **HTTP**. You are advised to select the HTTPS protocol.

Parameter	Description	Setting Rule
AK	Access Key (AK) confirms the identity of a user accessing the object-based storage system.	-
SK	Secret Key (SK) allows a user to access an object-based storage system. Secret access keys and access key IDs are in one-to-one match.	-
Path	Path to access the S3 storage	IPV4 path format: *IP address or domain name*:/*bucket name* *IP address* and *domain name* indicate the service IP address and the domain name of the object-based storage system, respectively. A bucket name contains 3 to 255 characters and can contain letters, digits, and special characters. Special characters include periods (.), hyphens (-), and underscores (_).
Identifier	Name of a subdirectory saving management data backups, which differentiates the management data backups of different eBackup systems	An identifier contains 1 to 64 characters and can contain only letters, digits, underscores (_), and hyphens (-).

Parameter	Description	Setting Rule
If a subdirectory with the same name already exists, the system uses the existing subdirectory forcibly.	Whether to write data if a subdirectory with the same name already exists ● If selected The backup data will be written to the subdirectory even if a subdirectory with the same name exists.l **NOTE** If multiple eBackup systems use the same backup subdirectory, management data backups may be unavailable. Use a subdirectory for each eBackup system. ● If not selected You cannot create a backup subdirectory if a subdirectory with the same name already exists. In this case, use a different name for the subdirectory.	-

Step 5 Click **OK**.

After the configuration is completed, the backup storage configuration status will be shown to the right of the **Set Backup Storage** button.

● ⟳ : The configuration is in progress.

● No icon: The configuration is successful.

● 🔴 : The configuration failed.

📖 **NOTE**

If the configuration fails, click **Set Backup Storage** and reconfigure.

Step 6 **(Optional)** Configure a backup policy for the management data.

📖 **NOTE**

To ensure the system database security of the backup software, you are advised to back up the database periodically. The system performs full backups for every time.

● Click **Automatic Backup Settings**. In the dialog box that is displayed, configure an automatic backup policy as prompted.

  – If **Daily Backup** is selected, the default system settings are as follows.

Figure 4-3 Setting daily backup

– If **Hourly Backup** is selected, the default system settings are as follows.

Figure 4-4 Setting hourly backup
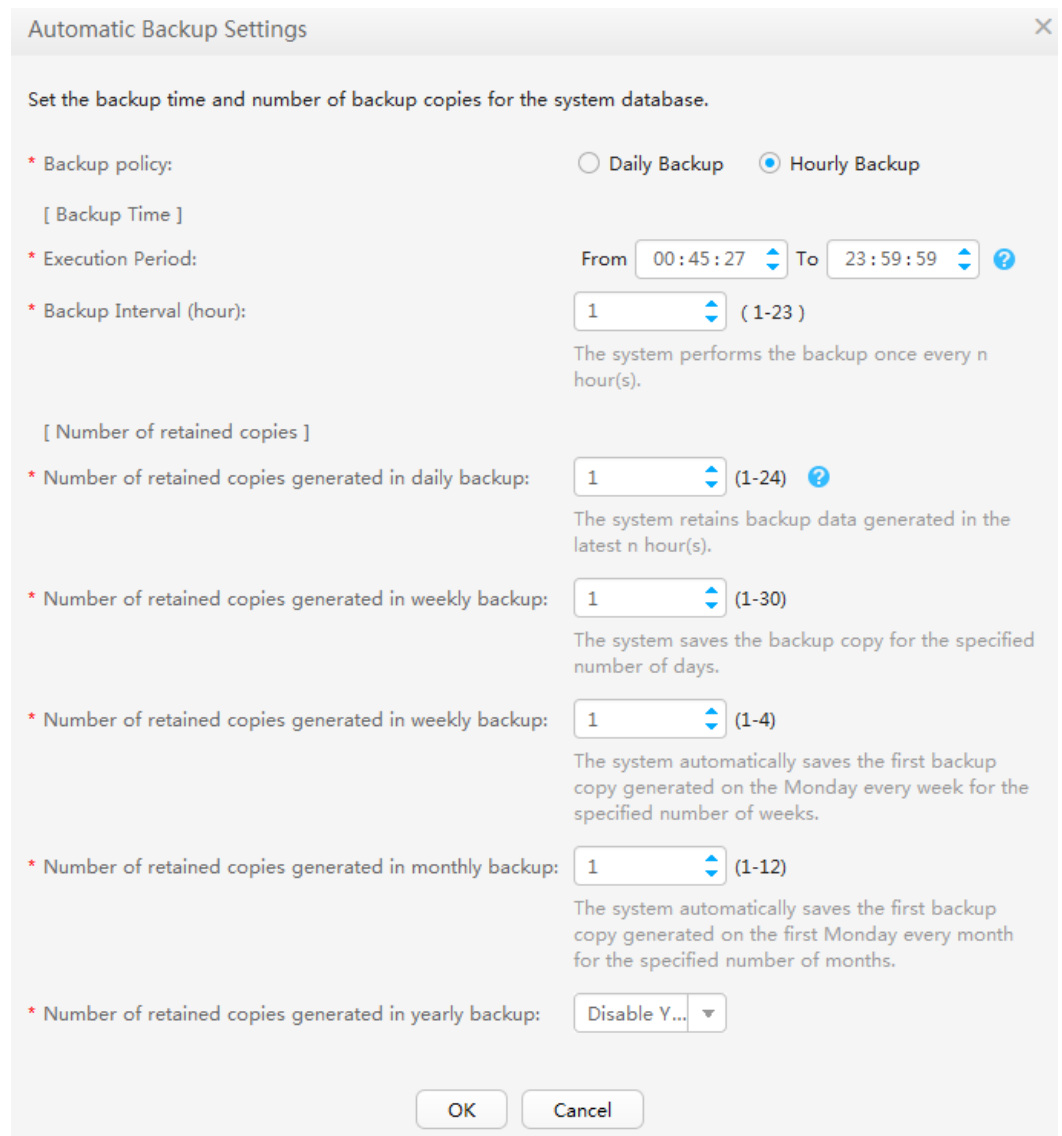
- Hourly backup: Backup generated every n hour(s) in the system.

- Daily backup: first backup generated per day.

- Weekly backup: first backup generated on Monday per week.

- Monthly backup: first backup generated on the first Monday per month.

- Yearly backup: first backup generated on the first Monday per year.

□ NOTE

You are advised to set the backup time to off-peak hours to reduce impact on services, for example, 00:00 to 02:00.

After the automatic backup policy is configured, restart the eBackup process on the backup server to make the policy take effect. For details, see "Restarting the eBackup Process."

If the backup time overlaps (for example, monthly backup and weekly backup are both performed on Monday), the system performs backups based on the backup policy with the highest priority. The priorities of the following backup policies descend: yearly backup > monthly backup > weekly backup > daily backup > hourly backup.

● Click **Immediate Manual Backup**. The backup job is executed immediately.

◻ NOTE

You are advised to manually back up the system database immediately before and after a major operation, such as an upgrade and critical data modification.

----End

Follow-Up Operations

If you need to delete unnecessary backup data, you can find and delete the data according to package names of backup data. The file name is in the format of **[Backup data type][Backup type][Service name][Year][Month][Day][Minute] [Second][Backup period][No.].db**. The following uses **FMTEBACKUP20170811110307X001.db** as an example.

Table 4-3 Parameter description

Parameter	Description	Rule
F	Backup type	The value can be: ● **F**: full backup ● **I**: incremental backup
MT	Backup option	The value can be: ● **MT**: manual backup ● **AT**: automatic backup
EBACKUP	Service name	Fixed at **EBACKUP**
2017081111 0307	Time when the backup was executed	In the format of *YYYYMMDDHHMMSS*
X	Backup Period	The value can be: ● **D**: daily backup ● **W**: weekly backup ● **M**: monthly backup ● **Y**: yearly backup ● **X**: manual backup (Manual backups will not be automatically deleted.) **NOTE** If the backup time overlaps (for example, monthly backup and weekly backup are both performed on Monday), the system performs backups based on the backup policy with the highest priority. The priorities of the following backup policies descend: yearly backup > monthly backup > weekly backup > daily backup > hourly backup.
001	Backup data number	-

4.7 Adding a VMware Protected Environment

The eBackup management system can protect VMs in the VMware environment. After adding a VMware protected environment, eBackup management system can back up and restore VMs in the protected environment.

Context

- When a VMware protected environment is added to the eBackup management system, if the name of a VM contains special characters such as %/\-.", the VM name displayed in eBackup management system will be inconsistent with the actual one, for example, a name containing % will be displayed as %25. For details, see the *vSphere Web Services SDK Programming Guide*. It is recommended that the name of a VMware VM not contain special characters.

- The system disk of the VMware VM to be backed up must be in slot 0. Or, the backup of the system disk will be displayed as a data disk after the VM is backed up to the cloud. Therefore, ensure that the system disk is in slot 0 before the backup. The following uses VMware vSphere 6.0 as an example. The GUI varies with the version.

    a. Log in to the VMware vSphere web client and locate the VM to be backed up.

    b. Choose **Summary** > **Edit Settings**.

    c. Click the system disk. If the value of **Virtual Device Node** is **SCSI (0:0)**, the system disk is in slot 0. Otherwise, change the value of **Virtual Device Node** to **SCSI (0:0)**.

Figure 4-5 Confirming the system disk slot
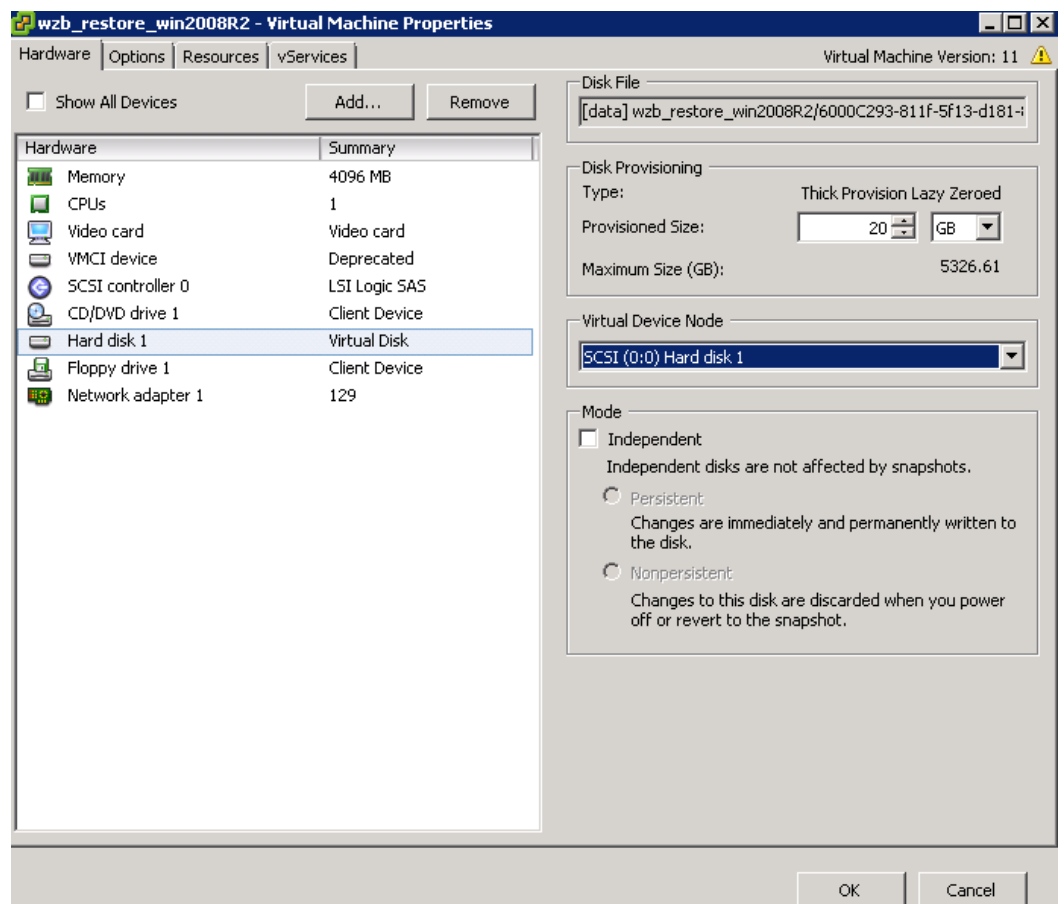
Prerequisites

- Network connectivity is normal between eBackup servers and the VMware management plane.

- **Accessibility Status** of the eBackup servers is **Accessible**, and **Register Status** is **Registered**. For more information, see **Managing an eBackup Server**.

Procedure

Step 1 Log in to the eBackup management system using the **admin** account.

For details, see **Logging In to eBackup**.

Step 2 On the navigation bar, choose ⬡ > **VMware**.

Step 3 Click ➕ in the **Protected Environment** area.

Step 4 Set basic information about a VMware protected environment. **Table 4-4** describes the parameters.

Figure 4-6 Add Protected Environment

Table 4-4 Parameter description

Parameter	Description	Setting Rule
Name	Name of a user-defined protected environment	The name contains 1 to 128 characters and can contain letters, digits, plus signs (+), underscores (_), hyphens (-), periods (.), and at signs (@).
vCenter/ESXi IP	● If vCenter Server manages VMs in a unified manner, enter the IP address of vCenter Server. ● If VMs are managed by an independent ESXi host, enter the management IP address of the ESXi host. NOTE The ESXi host is not managed by any vCenter Server.	Obtain it from the VMware administrator.

Parameter	Description	Setting Rule
Username	Name of the user to log in to the VMware vSphere web Client	
Password	Password of the user to log in to VMware vSphere web Client	
Protocol	Network protocol used for communication between the eBackup management system and the management plane of vCenter Server or the ESXi host. **HTTPS** is supported.	-
Port	Network port used for communication between the eBackup management system and the management plane of vCenter Server or the ESXi host	The default port is 443.
Certificate	Certificate used to authenticate the protected environment ● Auto Match If you have imported certificates for the protected environment by choosing ⚙ > **Certificate**, the system automatically discovers a matching certificate from the imported ones. ● Manually Upload Obtain the certificate using either of the following methods: – Obtain certificates from the VMware administrator. – Use a web browser to log in to the VMware vCenter environment and download the certificate package to a local directory. After the package is downloaded, change the file name extension to **.zip** and open the package. Find the file of ***.0** format and change its file name extension to ***.crt**.	You are advised to import a valid CA root certificate. Or, the backup management system cannot authenticate the protected environment, resulting in security risks. To ensure compatibility of protected environments, the eBackup management system has no restrictions on protocol versions supported by certificates. Obtain certificates from the VMware administrator.

Step 5 Click **OK**.

📖 NOTE

- When a VMware protected environment is added, the system automatically obtains the VM information. The structure of the navigation tree is the same as that of the protected environment.

- After the VMware protected environment is successfully added, view the environment name in the navigation tree on the left. You can see that the system automatically adds the IP address of the vCenter Server or ESXi host to the end of the name.

- When you add a VMware protected environment for the first time, the system automatically scans for the environment information. You can view the scanning progress by choosing > **Job**.

  When the scanning succeeds, the icon next to the tier 1 node is , with the scanning date and time displayed in the labels of the scanning job icon. If the scanning fails or is in progress, the icon next to the tier 1 node is , with the latest scanning date and time displayed in the labels of the scanning job icon.

- By default, the system scans for the environment information every hour. If the information is changed, you can click or next to each tier 1 node to manually trigger the scanning.

- After a successful scan, go to the **Protected Environment** area and click to refresh the information in the navigation tree on the left.

----End

Follow-Up Operations

The VM that you want to protect can be backed up only after it is added to a protected set. Select the VM to be protected and add it to a protected set by clicking **Add to Existing Protected Set** or **Add to New Protected Set**.

4.8 Preparing for Backup Storage

4.8.1 Purchasing a Hybrid Cloud Backup Vault for VMware Backups

This section describes how to create a hybrid cloud backup vault to store VMware backups.

Constraints

- A VMware VM can be associated with only one vault.

- Multiple VMware VMs can use the same vault.

Procedure

Step 1 Log in to the CBR console.

1. **Log in to the management console**.

2. Click ⊙ in the upper left corner and select a region.

3. Click ≡ and choose **Storage** > **Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

Step 2 In the upper right corner of the page, click **Buy Hybrid Cloud Backup Vault**.

Step 3 Select a billing mode.

- Yearly/monthly is a prepaid billing mode. You are billed based on the subscription duration you specify. This mode provides lower prices and is ideal when the resource use duration is predictable.

- Pay-per-use is a postpaid billing mode. You are billed based on your resource usage. With this mode, you can increase or delete resources at any time. Fees are deducted from your account balance.

Step 4 Specify the vault capacity.

Step 5 (Optional) Add tags to the vault.

A tag is represented in the form of a key-value pair. Tags are used to identify, classify, and search for vaults. Vault tags are used to filter and manage vaults only. A vault can have a maximum of 10 tags.

Table 4-5 describes the parameters of a tag.

Table 4-5 Tag parameter description

Parameter	Description	Example Value
Key	Each tag has a unique key. You can customize the key or select the key of an existing tag created in TMS. A tag key: ● Can contain 1 to 36 Unicode characters. ● Cannot be left blank, cannot start or end with spaces, or contain non-printable ASCII (0-31) characters or the following special characters: =*<>\,|/	Key_0001
Value	A tag value can be repetitive or left blank. A tag value: ● Can contain 0 to 43 Unicode characters. ● Can be an empty string, but cannot start or end with spaces, or contain non-printable ASCII (0-31) characters or the following special characters: =*<>\,|/	Value_0001

Step 6 Specify a name for the vault.

A name must contain 1 to 64 characters including digits, letters, underscores (_), or hyphens (-), for example, **vault-98c8**.

☐ NOTE

You can use the default name, which is in the format of **vault_**_xxxx_.

Step 7 Click **Next**. Confirm the order details and click **Submit**.

Step 8 Complete the payment as prompted.

Step 9 Go back to the VMware backup page. You can see the created vault in the vault list.

You can replicate the new vault or expand the vault capacity. For details, see **Vault Management**.

----End

4.8.2 Creating a Storage Unit

A storage unit is a basic unit allocated for backing up user data in the backend storage. The storage space can be used only after the backend storage is mapped and storage units are created. This section describes how to add a hybrid cloud backup vault to eBackup and create storage units.

Prerequisites

- The backup storage plane of the eBackup server can access the domain name (**obs.**_regionid_.**myhuaweicloud.com**) of the backup vault.
- A hybrid cloud backup vault has been purchased.

Procedure

Step 1 On the navigation bar, choose > **Storage Unit**.

Step 2 Click **Create**.

Figure 4-7 Create Storage Unit

Create Storage Unit

* Name:	Storage_20190624185830
Description:	
* AK:	Enter the AK of your HUAWEI CLOUD account.
* SK:	Enter the SK of your HUAWEI CLOUD account.
* Region:	Enter the ID of the region, for example, cn-north-1.
* Project:	Enter the project ID of the region.
* Vault:	Enter the ID of the purchased vault.
Offline Transmission:	OFF

OK   Cancel

Step 3 Set basic information about the storage unit as prompted.

> **NOTICE**
>
> Backup storage of the system management data and user data cannot share one hybrid cloud backup vault. Or, the backup jobs may fail.
>
> If you enable **Offline Transmission**, connect the Teleport device or disk to the VMware environment and ensure that the eBackup server can access the Teleport device or disk.

Step 4 Click **OK**.

> 📖 **NOTE**
>
> - After a storage unit is created, the system automatically mounts storage space.
> - After the storage unit with **Offline Transmission** enabled is created, the system creates an S3 storage unit and a NAS storage unit. When creating a storage pool, add both storage units.
> - The **Accessibility Status** of the storage unit is **Scanning** after you create a storage unit. The storage unit takes some time to connect to backup proxies. Wait for a moment, the system will automatically refresh the status of the storage unit. For details, see **Viewing a storage unit** in **Managing a Storage Unit**.

----End

4.8.3 Creating a Storage Pool

A storage pool provides an abstract layer to implement physical isolation. The failure of a storage pool does not affect backup services in other storage pools.

Prerequisites

A storage unit has been created according to **Creating a Storage Unit**.

Procedure
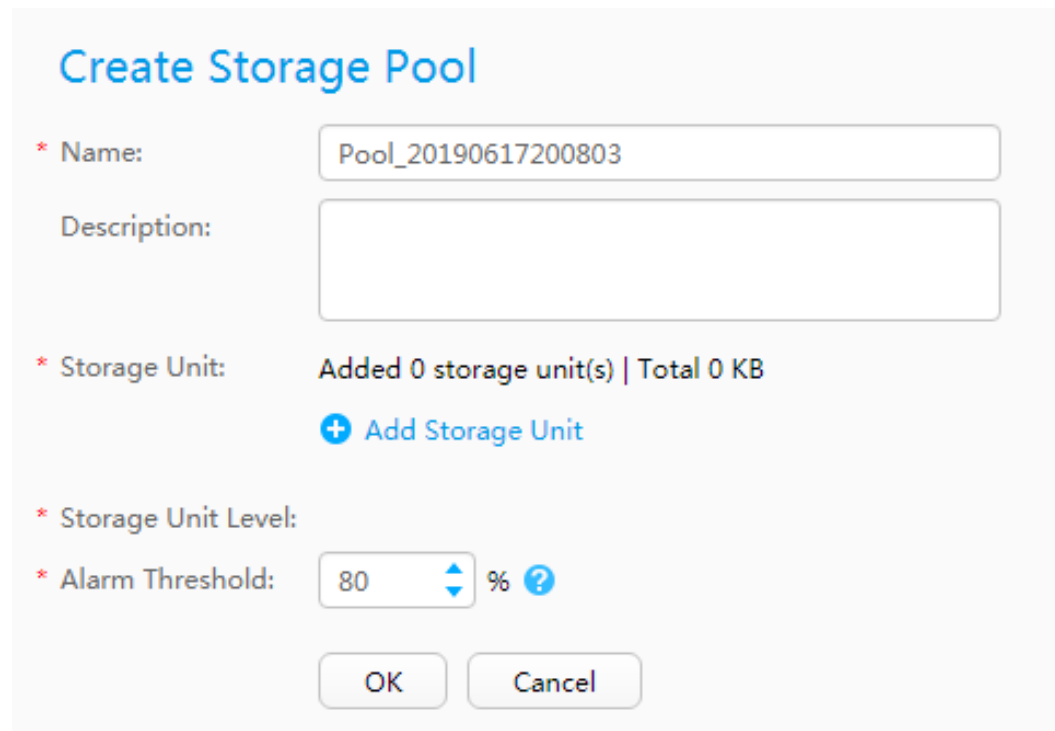
Step 1 On the navigation bar, choose ⊞ > **Storage Pool**.

Step 2 Click **Create**.

Figure 4-8 Create Storage Pool

Step 3 Set basic information of a storage pool. **Table 4-6** describes the parameters.

Table 4-6 Parameter description

Parameter	Description	Setting Rule
Name	Name of a user-defined storage pool	The name contains 1 to 128 characters and can contain letters, digits, plus signs (+), underscores (_), hyphens (-), periods (.), and at signs (@).

Parameter	Description	Setting Rule
Description	Description of a storage pool	The description contains a maximum of 1,024 characters.
Storage Unit	Click ⊕. In the **Add Storage Unit** dialog box, select an existing storage unit or create a storage unit if no storage units are available. If you want to create a storage unit and enable **Offline Transmission**, add both the created S3 and NAS storage units.	A storage unit cannot be added to multiple storage pools.
Alarm Threshold	If the storage pool usage exceeds the threshold, an alarm is reported, prompting you to expand capacity or delete unneeded backup data. If you do not do so, subsequent backup jobs may fail.	An appropriate alarm threshold helps you monitor the capacity usage of a storage pool. The default threshold is 80%. You are advised to set this parameter to a value ranging from 70% to 90%.

Step 4 Click **OK**.

----End

4.8.4 Creating a Repository

A repository is a space allocated in a storage pool. It provides storage space to store backup data and provides data source to restore data. Before backup, create a repository.

Prerequisites

A storage pool has been created according to **Creating a Storage Pool**.

Procedure

Step 1 On the navigation bar, choose ⬡ > **Repository**.

Step 2 Click **Create**.

Step 3 Set basic information of a repository. **Table 4-7** describes the parameters.

Figure 4-9 Create Repository

Table 4-7 Parameter description

Parameter	Description	Setting Rule
Name	Name of a user-defined repository	The name contains 1 to 128 characters and can contain letters, digits, plus signs (+), underscores (_), hyphens (-), periods (.), and at signs (@).
Description	Description of a repository	The description contains a maximum of 1,024 characters.
Storage Pool	Select an existing storage pool and create a repository based on the storage pool.	• If a storage pool has been planned for a repository, select the planned storage pool. • If no storage pool is planned for a repository and the existing resources need to be used, select a proper storage pool that can provide sufficient storage space for the backup data.
Full Quota	Enable or disable full quota.	• **ON**: The repository capacity is the maximum available capacity. • **OFF**: The repository capacity is specified by a user.

Parameter	Description	Setting Rule
Capacity	Capacity of a repository This parameter is available only when **Full Quota** is **OFF**.	The repository capacity must be greater than the total capacity of the unallocated space in the selected storage pool.
Alarm Threshold	If the repository usage exceeds the threshold, an alarm is reported, prompting you to expand capacity or delete unneeded backup data. If you do not do so, subsequent backup jobs may fail.	An appropriate alarm threshold helps you monitor the capacity usage of a repository. The default threshold is 80%. You are advised to set this parameter to a value ranging from 70% to 90%.

Step 4 Click **OK**.

----End

4.9 Perform VMware Backup

4.9.1 Creating a Protected Set

A protected set consists of backup objects to be protected. You can apply the same backup policy to all backup objects in a protected set to reduce backup time and increase backup efficiency.

Prerequisites

The protected environment has been added to the eBackup management system, and scanning for the protected environment is successful.

Context

If the name of a VMware VM backup object contains special characters such as %/\-.", the VM name displayed in the eBackup management system will be inconsistent with the actual one, for example, a name containing % will be displayed as %25. For details, see the *vSphere Web Services SDK Programming Guide*. It is recommended that the name of a VMware VM not contain special characters.

Procedure

Step 1 On the navigation bar, choose > **Protected Set**.

Step 2 Click **Create**.

Step 3 Set basic information of a protected set. **Table 4-8** describes the parameters.

Figure 4-10 Create Protected Set
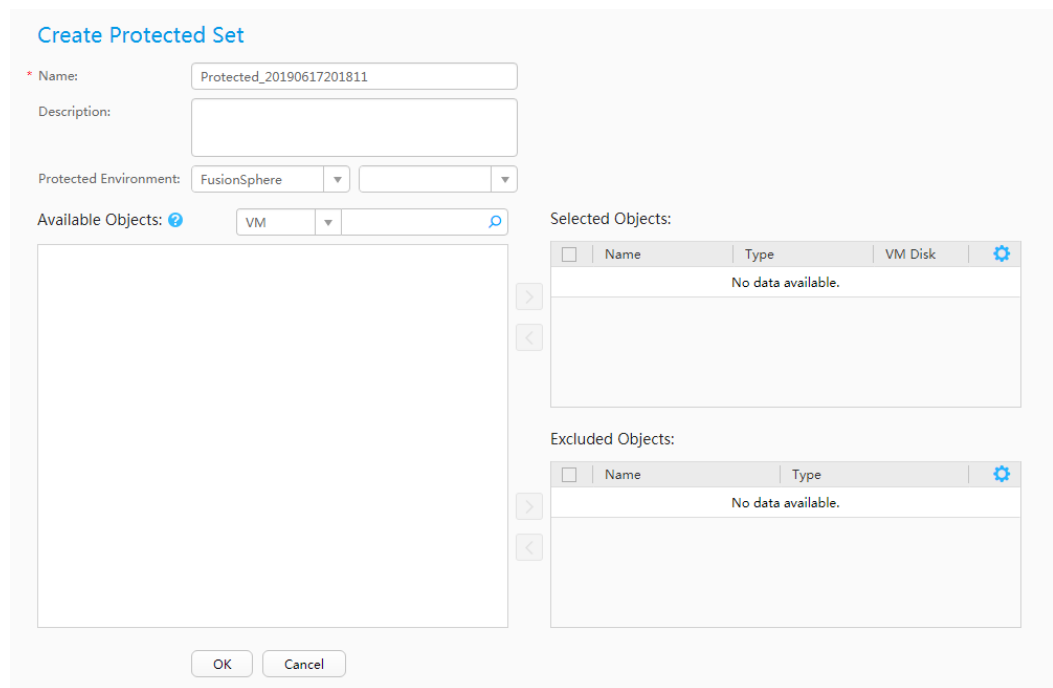
Table 4-8 Parameter description

Parameter	Description	Setting Rule
Name	Name of a user-defined protected set	The name contains 1 to 128 characters and can contain letters, digits, plus signs (+), underscores (_), hyphens (-), periods (.), and at signs (@).
Description	Description of a protected set	The description contains a maximum of 1,024 characters.
Protected Environment	Select the protected environment type and then select the protected environment added to the eBackup management system.	Select a VMware protected environment.

Parameter	Description	Setting Rule
Available Objects	To select backup objects, click ![icon] and add them to the **Selected Objects** list. To exclude backup objects, click ![icon] and add them to the **Excluded Objects** list.	You can use either of the following methods to select backup objects: In the navigation tree, select the required backup objects; or, set filtering criteria and select the required backup objects that meet the filtering criteria. **NOTE** ● The backup management system does not support the backup of the protected object whose name exceeds 512 characters. ● You can select multiple backup objects at a time by hold down **Ctrl** or **Shift**.
Selected Objects	Objects to be backed up By default, the system considers all disks on VMs as backup objects. To exclude some disks, click ![icon] and remove the disks in the **VM Disks** dialog box. **NOTE** ● The eBackup management system uses **IDE (Bus Number: Slot Number)** to identify a disk. ● If you select disks of multiple VMs as backup objects, all disks that can be created on the VMs are selected by default. The system automatically ignores the disks that do not exist.	The total number of selected objects and excluded objects is 200.
Excluded Objects	Objects not to be backed up	The total number of selected objects and excluded objects is 200.

Step 4 Click **OK**.

----End

4.9.2 Creating a VMware Backup Policy

A backup policy defines rules for executing backup jobs and generating backups. A backup plan can initiate a backup job only after a backup policy is set for the backup plan. You can create different backup policies to meet diverse backup requirements.

Procedure

Step 1 On the navigation bar, choose ⬆️ > **Backup Policy**.

Step 2 Click **Create**.

Step 3 Set basic information of a backup policy.

Table 4-9 Parameter description

Parameter	Description	Setting Rule
Backup Policy Name	Name of a user-defined backup policy	The name contains 1 to 128 characters and can contain letters, digits, plus signs (+), underscores (_), hyphens (-), periods (.), and at signs (@).
Description	Description of a backup policy	The description contains a maximum of 1,024 characters.

Paramet er	Description	Setting Rule
Schedule	Plan for executing backup jobs based on a specific backup policy. The value can be **Periodic** or **One time**. When **Schedule** is set to **Periodic**, you need to set scheduling plans for incremental backup. You can determine whether to enable periodic full backup based on site requirements. Related parameters are described as follows: **NOTE** If incremental backup and full backup are set to be executed at the same point in time, the system will execute full backup first. ● **Weeks in a Month**: Execute backup jobs weekly or in a specific week of each month. ● **Days in a Week**: Execute backup jobs on certain days of a week, which is used together with **Weeks in a Month**. For example, execute backup jobs on Wednesday and Sunday in the first week of each month. ● **Excluded Days in a Month**: Execute backup jobs not in those specific days. ● **Execution Time**: A specific point in time. The system automatically executes backup jobs at the point in time. You can set one or more points in time. The system performs backup jobs in time sequence. ● **Execution Period**: A specific execution period. The system executes a backup job many times at a certain interval within a specific	A higher backup frequency provides more reliable data protection, but requires a longer time and larger space. Choose a schedule based on data importance and service volume. Define a high backup frequency for critical data.

Paramet er	Description	Setting Rule
	period of time. You can set one or more execution periods. **NOTE** ● A new backup job is started only after an ongoing backup job is completed. ● If a VM is added to a protected set within an execution period and an ongoing backup job is not complete, the system will back up the newly added VM after the execution period ends. ● When the execution period ends, an ongoing backup job can continue but a **Pending** backup job will not be processed.	
One time	Backup jobs of the backup policy are executed once only. The policy execution time must be set. If this parameter is set, the system automatically executes full backup instead of incremental backup. This parameter is available only when **Schedule** is set to **One time**.	The policy execution time must be later than the current system time.

Parameter	Description	Setting Rule
Retention	Defines the period of time or number of backups that backups generated for a protected object can be retained. Three types are available: ● Permanent Backups are retained permanently. ● By Backup Quantity Total number of backups can be retained It refers to the total number of backups that generated for a protected object can be retained. Once the number of generated backups exceeds the value, the system automatically deletes the oldest backups that are not within the retention scope of **Number of retained backups in a year/month/week/day**. Number of retained backups in a year, month, week, or day One backup is retained in every year, month, week, or day since the current time to the time you set. If the current year is 2014 and you want to retain one backup every year in the previous 3 years, the system will retain the latest backups generated in years 2011, 2012, and 2013. ● By Time Retained for a period Backups generated based on a backup policy will be retained for xx years, months, weeks, or days. Once the retention period ends, the system	● The total number of retained backups ranges from 1 to 100, and the default value is 90. ● The number of retained backups in a year ranges from 0 to 999, and the default value is 10. ● The number of retained backups in a month ranges from 0 to 999, and the default value is 10. ● The number of retained backups in a week ranges from 0 to 9999, and the default value is 10. ● The number of retained backups in a day ranges from 0 to 99999, and the default value is 10. **NOTE** The total number of retained backups and the backups retained by time cannot be left blank at the same time. ● The retention period for years ranges from 1 to 25, and the default value is 1. ● The retention period for months ranges from 1 to 300, and the default value is 1. ● The retention period for weeks ranges from 1 to 1300, and the default value is 1. ● The retention period for days ranges from 1 to 9125, and the default value is 1. If backups are retained permanently, they can be used to restore data at any time. But, space occupied by backups cannot be reused. If the space provided by repository is used up, new backups will not be generated. Consider the following when deciding the number of backups to be retained and the retention period:

Parameter	Description	Setting Rule
	automatically deletes expired backups. Retained until a specific day Backups generated based on a backup policy will be retained for a specific point in time. Once the retention period ends, the system automatically deletes expired backups.	• Data importance and disaster recovery requirements. If data of the latest month must be retained, you are advised to set the retention period to at least one month. • Available space of the repository. If the available space of the repository is sufficient, you are advised to retain more copies of important backups or retain backups for a long period of time.
Create Verification Data	After this option is enabled, the system will create verification data for backup data and verify the integrity and consistency of the backup data. If this option is disabled, the system only verifies the consistency of the backup metadata. The verification data is used to ensure the integrity and consistency of the backup data when full verification is executed for backups. **NOTE** Backup data refers to the real data of users. Backup metadata is the additional information about the location of data blocks, number of disks and others.	This function affects backup performance. If you have demanding requirements on the integrity and consistency of the backup data and no special requirements on backup performance, you are advised to enable this option.
Data Layout	Format of backup data saved on the backup storage. The value can be: Compress: Compressing backup data helps save storage space.	-

Parameter	Description	Setting Rule
Retry	Maximum number of retries. If this parameter is set to **ON**, you need to set **Retry Times** and **Retry Window**. The **Retry Window** is the maximum time range for retrying failed backup jobs.	The retry times ranges from 1 to 10. The retry window ranges from 1 to 168. For example, a backup job is performed at 9:00. At 9:10, the backup job fails. In the retry plan, the number of retries is set to 3 and the retry window is set to one hour. By default, the system performs a failed backup job five minutes after the backup job execution failure. Therefore, the backup job is performed again between 9:15 and 10:10. ● If the backup job still fails after three retries within the specified period or the three retries cannot be completed within the specified period, the system will not perform the backup job again. ● If the backup job succeeds within the specified period, the system will not perform the backup job again.

Step 4 Click **OK**.

----End

4.9.3 Creating a Backup Plan

A backup plan consists of a repository, protected set, and backup policy. After a backup plan is created, you can perform backup jobs based on the plan.

Prerequisites

At least a repository, a protected set, and a backup policy are available.

Context

After configuring associated jobs for a backup plan, you can use the backup plan wizard to select created objects and start backup jobs. This section instructs you to create a backup plan by using an existing repository, protected set, and backup policy. In addition, the eBackup management system provides the quick entry for creating a backup plan which aims at providing a key job configuration wizard to help the user that initially uses eBackup to quickly create a backup plan.

Procedure
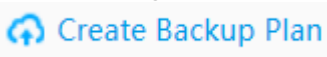
Step 1 On the navigation bar, choose > **Backup Plan**. Or, choose >

 in the eBackup management system.

Step 2 Click **Create**.

Step 3 On the **General Info** page, set basic information of a backup plan.

Figure 4-11 Setting general information

1. Enter a backup plan name in **Name**.

   📖 NOTE

   > The name contains 1 to 128 characters and can contain letters, digits, plus signs (+), underscores (_), hyphens (-), periods (.), and at signs (@).

2. Enter the description of the backup plan in **Description**.

3. Determine whether to enable **Offline Transmission**.

   – If you enable **Offline Transmission**, you need to enable the repository corresponding to the storage unit for which **Offline Transmission** is enabled. When Teleport devices or disks are disconnected from the VMware environment and are ready to be sent to the Huawei Cloud data center, or they have been sent to the data center and the data has been uploaded, you need to modify the status of **Offline Transmission** in the backup plan. For details, see **Follow-Up Operations**.

   – If you do not enable **Offline Transmission**, you can enable it in the backup plan later. For details, see **Follow-Up Operations**.

4. Click **Next**.

   The **Protected Set** page is displayed.

Step 4 Select a protected set using either of the following methods:

- Select a protected set from the list.

- Search for a desired protected set in the upper right part of the list and select it.

  📖 NOTE

  - If no protected sets are available in the list, click the **Create Protected Set** tab in the upper right part of the page to create one.

  - If there is no VM or VM disk in the protected set, the system will not execute the backup job.

Step 5 Click **Next**.

The **Backup Policy** page is displayed.

Step 6 Select a backup policy using either of the following methods:

- Select a backup policy from the list.
- Search for a desired backup policy in the upper right part of the list and select it.

📖 **NOTE**

If no backup policies are available in the list, click the **Create Backup Policy** tab in the upper right part of the page to create one.

Step 7 **(Optional)** Select **Activate**. After the policy is activated, the system automatically executes backup jobs based on the backup policy.

📖 **NOTE**

- **Activate** is selected by default. You can deselect this option, and execute a backup job manually or execute a backup job automatically based on a backup policy when required.
- When the backup policy selected was set to **One time**, if the time you create a backup plan is later than the policy execution time, the system will execute the backup job immediately after the backup plan is created (**Activate** is selected).

Step 8 Click **Next**.

The **Repository** page is displayed.

Step 9 Select a repository using either of the following methods:

- Select a repository from the list.
- Search for a desired repository in the upper right part of the list and select it.

📖 **NOTE**

- If you enable **Offline Transmission** in **Step 3**, you need to enable the repository corresponding to the storage unit for which **Offline Transmission** is enabled.
- If no repositories are available in the list, click the **Create Repository** tab in the upper right part of the page to create one.
- If a backup job requires more storage capacity than the available capacity of its repository while the storage pool of the repository has sufficient capacity, the backup job will be executed. If the capacity of the repository is used up, no backup job will be executed.

Step 10 Click **Completed**.

NOTICE

You are advised not to run multiple backup plans that contain the same VM at the same time. Or, the backup jobs may fail.

----End

Follow-Up Operations

Step 1 On the navigation bar, choose ⊙ > **Backup Plan**.

Step 2 Move the mouse pointer to the backup plan you want to modify and click ✏ in the button area on the right, or click the backup plan you want to modify and click ✏ in the preview area on the right.

Step 3 Enable **Offline Transmission** based on your site requirement.

- **Disabled**: Select this option when Teleport devices have been sent to the Huawei data center and data has been uploaded.

- **Enabled**: Select this option when you need to use **Offline Transmission**.

- **Suspended**: Select this option when the Teleport devices or disks have been disconnected from the VMware environment.

📖 **NOTE**

- If **Offline Transmission** in a backup plan is set to **Disabled** and the corresponding job or recovery job is in the running, stopping, or waiting for scheduling state, you cannot set it to **Enabled**. Set it to **Enabled** after the job is complete.

- If **Offline Transmission** in a backup plan is set to **Disabled**, you cannot set it to **Suspended**.

- If **Offline Transmission** in a backup plan is set to **Enabled** and the corresponding job or recovery job is in the running, stopping, or waiting for scheduling state, you cannot set it to **Suspended**. Set it to **Suspended** after the job is complete.

- If **Offline Transmission** in a backup plan is set to **Enabled**, you cannot set it to **Disabled**.

- If **Offline Transmission** in a backup plan is set to **Suspended**, you cannot set it to **Enabled**.

Step 4 Click **OK**.

----End

4.9.4 (Optional) Manually Executing a Backup Job

For a created backup plan, a backup job can be executed automatically based on a backup policy, or you can manually execute a backup job.

Prerequisites

The available storage capacity of the repository is sufficient for the backup plan to execute backup jobs.

Context

Backup jobs can be executed in either of the following ways:

- Automatic:

  A backup job is automatically executed based on a backup policy.

- Manual:

  A backup job is manually enabled by a user and is executed based on a backup policy.

When a backup job is manually executed, the eBackup management system supports full backup and incremental backup. You can select a backup type based on your needs and available storage resources. **Table 4-10** describes backup types.

Table 4-10 Backup types

Backup Type	Description	Configuration Suggestion
Full backup	A full backup backs up all the data of a selected backup object, regardless of when the data was modified or backed up the last time. By default, the system initially executes a full backup based on a backup policy. You can manually trigger full backups as needed. Full backup provides the most complete backup protection; however, full backup takes a long time and occupies a large space.	If you have a high demand on data security but not on the restoration period and storage space, you can select full backup. If the system has not executed any backup job before, you can only select full backup. If the system has performed backup jobs before, you can select full backup or incremental backup.
Increment al backup	An incremental backup backs up all data that has been changed since the last full backup or incremental backup. The amount of data backed up each time is small, and the backup time is short. By default, the system initially executes a full backup based on a backup policy. During the backup, if the system detects that the previous backup is unavailable, the system implements full backup.	You can adopt full backup + incremental backup if you have high requirements for backup time and have sufficient storage resources.

Procedure

Step 1 On the navigation bar, choose ⊙ > **Backup Plan**.

Step 2 Manually execute backup using either of the following methods:

Figure 4-12 Manually executing backup
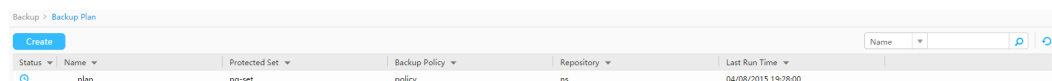
- Move the mouse pointer to a backup plan where you want to execute backup and click ▶ in the function pane.

- Click the backup plan and click ▶ in the preview area on the right.

📖 **NOTE**

> If there is an ongoing backup job of the same protected object in the backup plan, the system adds a backup job and set it to the **Pending** state.

- If backup jobs have been executed based on the backup plan before, the system automatically performs an incremental backup after you click ▶.

- If no backup jobs have not been executed based on the backup plan, the system automatically performs a full backup after you click ▶.

- At any time after a backup plan is created, you can click ▶ Full Backup, and the system will perform full backup based on the backup job manually triggered.

The **Info** dialog box is displayed.

Step 3 Click **Yes**.

----End

4.10 Restore

If protected objects data at the production end is damaged or lost, and needs to be restored, the eBackup management system can restore the backup data to the production end using the backups generated at specific points in time.

Restore Constraints

Pay attention to the following constraints before restoring VMware VMs:

- When data on a VMware VM is restored in LAN-free (SAN transport) mode, if the VM is installed with lazy zeroed disks, its data will be restored in LAN-base (NBD or NBDSSL) mode.

- Backup data of a VM in a later VMware vSphere version cannot be restored to a VM in an earlier VMware vSphere version.

- During data restoration, the eBackup management system automatically shuts down the VM to be restored and the VM cannot be started. Or, the restoration fails or the restored data is incorrect.

- During VM disk restoration, if multiple disks on the source VM have undergone volume management (such as logical volume management on Linux OS or dynamic volume management on Windows OS) and only some disks are restored, data on these disks cannot be accessed.

- A dynamic disk group must be restored to the target VM at a time. Backup images of a dynamic disk group cannot be mounted to a VM for many times. The backup images to be restored of a dynamic disk group cannot be mounted to the source VM.

- In the following scenarios, the disk space to which no backup data is written will not be zeroed and reclaimed:

> – Incremental restoration. Backup data is written to the original disk.
>
> – Full restoration. Backup data is written to the original disk.

4.10.1 Restoring to Cloud Servers Using VMware Backups

VMware backup data can be used to restore to other servers on the cloud, implementing cloud-based disaster recovery and rapid service deployment.

Context

- Backups synchronized to the cloud cannot be used to create cloud servers.

- Synchronized backups can only be used to restore to other cloud servers and can be restored to system disks or data disks.

- Before the restoration, configure security groups according to the procedure. Otherwise, the restoration may fail.

- When LVM is used to manage the system disks of VMware VMs, VMware backups cannot be restored to cloud servers.

Changing a Security Group

A security group is a collection of access control rules for ECSs that have the same security protection requirements and are mutually trusted in a VPC. After a security group is created, you can create different access rules for the security group to protect the ECSs that are added to this security group. The default security group rule allows all outgoing data packets. ECSs in a security group can access each other without the need to add rules. The system creates a security group for each cloud account by default. You can also create custom security groups by yourself.

Before using the VMware backup restoration function, you need to change the security group. To ensure network security, CBR has not set the inbound direction of a security group, so you need to manually configure it.

In the outbound direction of the security group, ports 1 to 65535 on the 100.125.0.0/16 network segment must be configured. In the inbound direction, ports 59526 to 59528 on the 100.125.0.0/16 network segment must be configured. The default outbound rule is 0.0.0.0/0, that is, all data packets are permitted. If the default rule in the outbound direction is not modified, you do not need to configure the outbound direction.

Step 1 Access the cloud server console.

Step 2 In the navigation pane on the left, choose **Elastic Cloud Server**. On the page displayed, select the target server. Go to the target server details page.

Step 3 Click the **Security Groups** tab and select the target security group. On the right of the ECS page, click **Modify Security Group Rule** for an ECS.

Step 4 On the **Security Groups** page, click the **Inbound Rules** tab, and then click **Add Rule**. The **Add Inbound Rule** dialog box is displayed, as shown in **Figure 4-13**. Select **TCP** for **Protocol/Application**, enter **59526-59528** in **Port & Source**, select **IP address** for **Source** and enter **100.125.0.0/16**. After supplementing the description, click **OK** to complete the setting of the inbound rule.

Figure 4-13 Adding an inbound rule
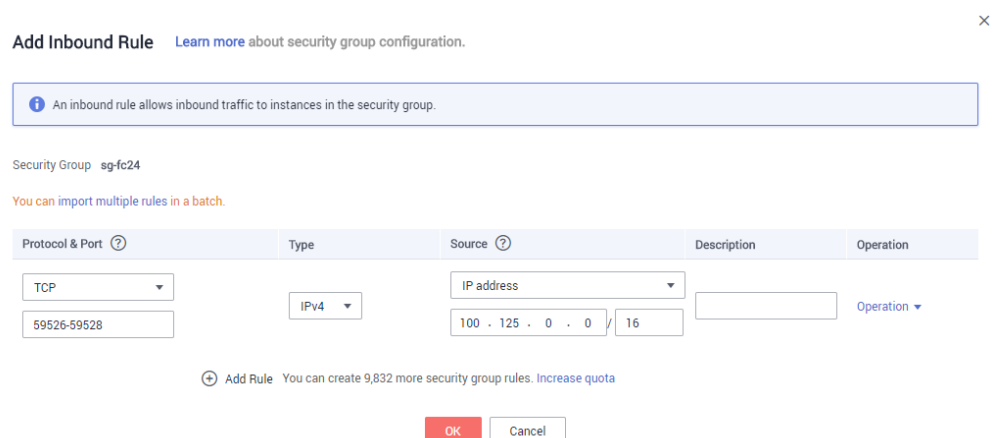
Step 5 Click the **Outbound Rules** tab, and then click **Add Rule**. The **Add Outbound Rule** dialog box is displayed, as shown in **Figure 4-14**. Select **TCP** for **Protocol/ Application**, enter **1-65535** in **Port & Source**, select **IP address** for **Destination** and enter **100.125.0.0/16**. After supplementing the description, click **OK** to complete the setting of the outbound rule.

Figure 4-14 Adding an outbound rule
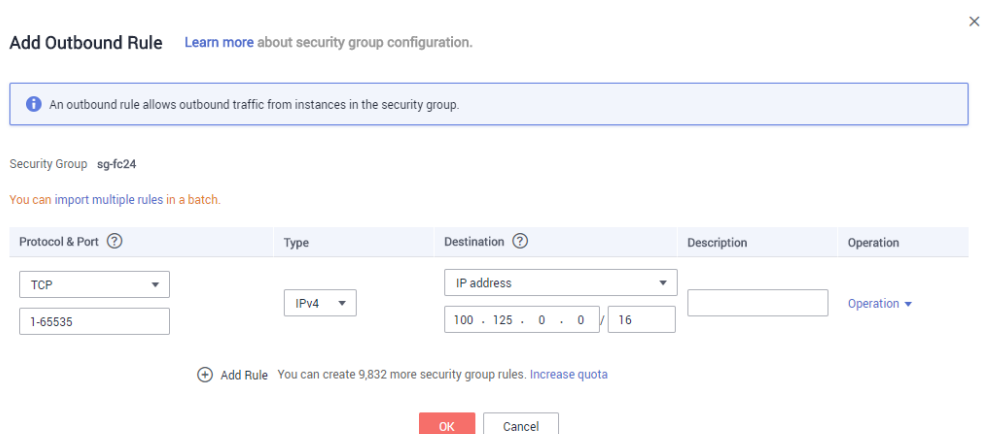
----End

Restoring Data Using a VMware Backup

Step 1 Log in to the CBR console.

1. **Log in to the management console**.

2. Click 📍 in the upper left corner and select a region.

3. Click ☰ and choose **Storage** > **Cloud Backup and Recovery**. Select a backup type from the left navigation pane.

Step 2 Click the **Backups** tab. Locate the desired backup. For details, see **Viewing a Backup**.

Step 3 In the row of the backup, click **Restore**. See **Figure 4-15**. If no ECS is available, purchase ECSs by referring to **Purchasing an ECS**.

Figure 4-15 Restoring VMware backup data to another server
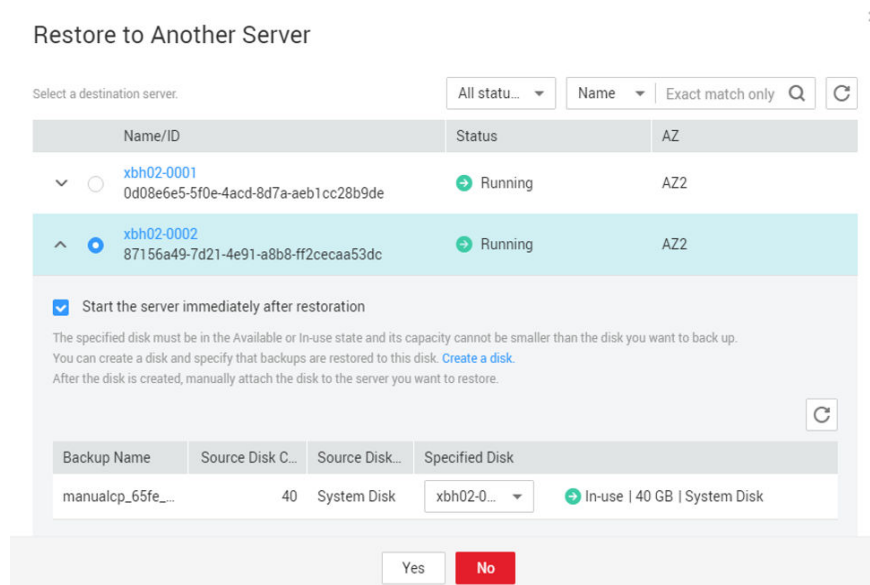
Step 4 (Optional) If you do not want the server to automatically start after the restoration, deselect **Start the server immediately after restoration**.

If you deselect **Start the server immediately after restoration**, manually start the server after the restoration is complete.

NOTICE

Servers are shut down during restoration. It is therefore recommended that you perform restoration operations during off-peak hours.

Step 5 In the **Specified Disk** drop-down list, select the target disk to which the backup will be restored.

NOTE

- If the server has only one data disk, the backup is restored to the disk by default.
- If the server has only one system disk, you need to create a disk for restoration.
- You can also restore the backup to another disk on the backup server by selecting the disk from the drop-down list. However, the specified destination disk must be at least as large as the backup source disk. You can view the size of the specified destination disk in the **Specified Disk** column and the size of the source disk in the **Source Disk Capacity** column. If the capacity of a disk is insufficient, expand disk capacity by referring to **Disk Capacity Expansion**.

Step 6 Click **Yes** and confirm the restoration is successful.

In the backup list, view the restoration status. When the backup enters the **Available** state or the status of the corresponding restoration task in **Tasks** is **Successful**, the restoration is successful.

To view failed restoration tasks, refer to **Managing Tasks**.

----End

Follow-up Procedure

If the VMware VM you backed up has multiple data disks and the data disks belong to the logical volume manager (LVM) group, an error might occur during the restoration. If an error occurs, do the instructions in **Failed to Restore a VMware Backup to a Cloud Server**.

4.10.2 Restoring VM Disks to the Original VM

You can restore disks on a single VM to the original VM.

Prerequisites

A full backup has been performed for the VM disks to be restored, and the backup status is **Valid**.

Procedure

Step 1 On the navigation bar, choose > **VMware**.

Step 2 In the **Backed Up Environment** area, click the protected environment where the VM disks you want to restore reside.

Step 3 Select the VM housing the disks to be restored using either of the following methods:

- Click the VM in the list.
- Search for the VM on the upper right of the list. Then click the VM.

Step 4 Select the backup required for the restore.

- In the preview area on the right, move the mouse pointer to the backup required for the VM restore and click .
- In the preview area on the right, move the mouse pointer to the backup required for the VM disk restore and click .

  📖 **NOTE**

  Before the restore, you can either perform a fast verification by selecting **Quick Verification** or perform a full verification by selecting **Full Verification**. If the verification status is **Valid**, the backup can be used to restore data.

Step 5 Click **Restore VM Disk to Original VM**.

Step 6 Select the VM disks you want to restore.

  📖 **NOTE**

  If you select all the disks of the VM, it will restore the original VM.

Step 7 **(Optional)** Select **Start VM after restore**.

Step 8 Click **OK**.

----End

4.10.3 Restoring VM Disks to a Specified VM

You can restore disks on a single VM to a specified VM. Before the restoration, ensure that the target VM has the same disk controllers as the backup VM. Or, the restoration will fail.

Prerequisites

A full backup has been performed for the VM disks to be restored, and the backup status is **Valid**.

Procedure

Step 1 On the navigation bar, choose > **VMware**.

Step 2 In the **Backed Up Environment** area, click the protected environment where the VM disks you want to restore reside.

Step 3 Select the VM housing the disks to be restored using either of the following methods:

- Click the VM in the list.

- Search for the VM on the upper right of the list. Then click the VM.

Step 4 Select the backup required for the restore.

- In the preview area on the right, move the mouse pointer to the backup required for the VM restore and click .

- In the preview area on the right, move the mouse pointer to the backup required for the VM disk restore and click .

  📖 **NOTE**

  Before the restore, you can either perform a fast verification by selecting **Quick Verification** or perform a full verification by selecting **Full Verification**. If the verification status is **Valid**, the backup can be used to restore data.

Step 5 Click **Restore VM Disk to Specific VM**.

Step 6 Select the VM to which you want to restore the disk backups.

  📖 **NOTE**

  You can also restore the disk backups to other disks on the original VM.

Step 7 Select the disk backups to be restored.

  📖 **NOTE**

  You can click to select datastores for other disks on the VM to restore VM disks.

Step 8 Select the datastores to which you want to restore the disk backups.

 NOTE

Datastores provide storage space for the disks to be restored. The drop-down list displays all datastores that can be accessed from selected VM. You can select a datastore to which the disks are restored.

Step 9 **(Optional)** Select **Start VM after restore**.

Step 10 Click **OK**.

----End

4.11 Managing a VMware Protected Environment

A protected environment is the source of backup data and is often referred to as the production side. After the protected environment is added to the eBackup backup management system, you can perform operations such as viewing, modifying, and deleting the protected environment that has been added.

Icon Description

After a VMware protected environment is added to eBackup backup management system, the system automatically obtains the VM information. **Table 4-11** lists the related icons. For definitions about objects in a VMware protected environment and their relationship, see the document delivered along VMware.

Table 4-11 Icons in a VMware protected environment

Object	Icon	Description
vCenter Server	/	Running on a Windows server, vCenter Servers provide convenient single-point control for DCs, manage VMware ESXi hosts in a centralized manner, and provide basic DC services. denotes that the certificate is not added, and denotes that the certificate is added.
DC		DCs are the main containers for objects such as hosts and VMs. You can add hosts, folders, and clusters to DCs.
Folder		Folders allow you to group objects of the same type for convenient management. Folders can contain subfolders or objects of the same type such as DCs, clusters, datastores, networks, VMs, templates, and hosts. For example, you can add a subfolder containing hosts to a folder already containing hosts, but cannot add a subfolder containing VMs to the folder already containing hosts.
Cluster		Clusters are collections of ESXi hosts and associated VMs. When hosts are added to clusters, host resources become a part of cluster resources. Resources of all hosts are managed in clusters.

Object	Icon	Description
Host		Hosts are physical servers running virtualization software (such as ESXi). VMs can run on hosts, which provide CPU and memory resources and capabilities such as graphics processing unit (GPU), USB devices, network connection, and storage access for VMs. Multiple VMs can run on a single host.
vApp		A vApp is a group of VMs and is managed as a single object. It simplifies the management of complex multi-layer programs running on mutually dependent VMs. Basic operations on vApp are the same as those on a VM or resource pool.
Resource pool		Resource pools are used to divide CPU and memory resources in hosts or clusters. VMs execute and use resources in resource pools. You can create multiple resource pools that are displayed as direct nodes for an independent host or cluster in the navigation tree.
VM		VMs are virtualized computers. Like physical computers, VMs run on operating systems, on which application software is running. VMs run on hosts and obtain the necessary CPU and memory resources as well as capabilities such as video adapter, USB devices, network connection, and storage access. Multiple VMs can run on a single host.
Disk		Disks are storage units divided from datastores associated with hosts. Disks provide storage space for VMs on the associated host. Like physical disks, disks can be used to store data such as operating systems and applications. Virtual disks can be bound to a VM and are used to store configuration files and other disk files for the VM.

Related Operations

Operation	Navigation Path	Description	Key Parameter
Viewing a VMware protected environment	● Viewing basic information: On the navigation bar, choose ⬡ > **VMware**. Click tier 1, tier 2, and tier 3 nodes in the navigation tree. ● Viewing details: On the navigation bar, choose ⬡ > **VMware**. Click tier 1, tier 2, and tier 3 nodes in the navigation tree and view VM information.	**Background** This operation displays information about a VMware protected environment. After the VMware protected environment is added to the eBackup backup management system, the system automatically obtains VM information. **Precautions** ● Before performing this operation, ensure that the VMware protected environment has been created and added to the eBackup system. ● If information of the protected environment is changed, you need to manually synchronize changes to the eBackup backup management system.	● Protection Status Protection status of a VM in the last week. ● UUID UUID is the universally unique identifier of the VM in the protected environment. ● Last Backup Time The latest backup start time of the VM. If the VM has never been backed up, the value is **--**. ● Host The name of the host that the VM is bound to. If the VM has not been bounded, the value is **--**.

Operation	Navigation Path	Description	Key Parameter
Modifying a VMware protected environment	On the navigation bar, choose > **VMware**. In the **Protected Environment** area, select the desired tier 1 node in the navigation tree on the left and click .	**Background** If the information of a VMware protected environment, such as the IP address of a vCenter Server or ESXi host and authentication information, is changed, you need to synchronize the changes in the eBackup backup management system so that the system can promptly obtain the VM information and correctly back up VMs on the vCenter Server or ESXi host. **Precautions** ● Before performing this operation, ensure that the VMware protected environment has been added to the eBackup system. ● If the IP address of the vCenter Server in the protected environment is changed, ensure that the changed IP address is consistent with that at the production end. If the system detects an inconsistency, the change fails. ● You cannot change the IP address of an	None

Operation	Navigation Path	Description	Key Parameter
		ESXi host. If the IP address of the ESXi host needs to be changed, you need to delete the existing protected environment and configure a new one with the new IP address.	

Operation	Navigation Path	Description	Key Parameter

Deleting a VMware protected environment	1. On the navigation bar, choose ⊘ > **VMware**.
	
	2. In the **Protected Environment** area, select the desired tier 1 node (the protected environment that you want to delete) in the navigation tree on the left. Then click each VM on the right. In the preview area, check whether any associated protected set exists.
	
	  ● If any associated protected set is displayed in the **Protected Sets** area, find it on the protected set page. Ensure that the protected set is unneeded and delete it. Then delete the protected environment.
	
	  ● If no associated protected set is displayed in the **Protected Sets** areas of all VMs, delete the protected environment directly.
		Background
		This operation deletes an unneeded protected environment.
		
		Precautions
		Before performing this operation, ensure that to-be-deleted VMs managed by vCenter Server or ESXi hosts are not associated with any protected sets.
			None

Operation	Navigation Path	Description	Key Parameter
	3. In the **Protected Environment** area, select the desired tier 1 node in the navigation tree on the left and click ⊖.		

4.12 Managing Backup Storage

4.12.1 Managing a Storage Unit

A storage unit is a basic unit allocated from the space mapped from a backend storage device and is used for storing backup data. You can view, modify, and delete an existing storage unit.

Operation	Navigation Path	Description	Key Parameters
Viewing a storage unit	• Viewing basic information: On the navigation bar, choose > **Storage Unit**. • Viewing details: On the navigation bar, choose > **Storage Unit**. On the displayed page, click the storage unit you want to view.	**Background** You want to view basic information about a storage unit. **Precautions** Before performing this operation, ensure that the storage unit has been created.	• Accessibility Status There are three states: – All accessible All backup proxies in the eBackup management system can access the storage unit. – Partially accessible Some of the backup proxies in the eBackup management system can access the storage unit. – Inaccessible None of the backup proxies in the eBackup management system can access the storage unit. – Scanning The storage unit is connecting with backup proxies. • Type Storage unit type, which can be: – NFS If the backend storage is NAS storage and is shared to the backup server and backup proxies using NFS, the storage unit type is NFS. – S3 If the backend storage is S3 storage and is shared to the backup server and backup proxies using S3, the storage unit type is S3. • Capacity

Operation	Navigation Path	Description	Key Parameters
			Total capacity of a storage unit – For the NAS backend storage, the total capacity of a storage unit is that of the shared directory. – For the S3 backend storage, the total capacity of a storage unit is that of the bucket. ● Path Path to access the backend storage – For the NAS backend storage, the path is the NFS shared path. – For the S3 backend storage, the path is the bucket access path.

Operation	Navigation Path	Description	Key Parameters
Modifying a storage unit	On the navigation bar, choose 🗄️ > **Storage Unit**. Move the mouse pointer to the storage unit you want to modify and click ✏️ in the button area on the right, or click the storage unit you want to modify and click ✏️ in the preview area on the right.	**Background** You want to update information about a storage unit. After modification, the system automatically synchronizes the modification to the associated storage pool. **Precautions** ● Before performing this operation, ensure that the storage unit has been created. ● Before changing the path of a storage unit, ensure that no jobs are executing on the storage unit. ● The storage unit level cannot be modified when the storage unit has an associated storage pool.	None

Operation	Navigation Path	Description	Key Parameters
Deleting a storage unit	On the navigation bar, choose (icon) > **Storage Unit**. Move the mouse pointer to the storage unit you want to delete and click (icon) in the button area on the right, or click the storage unit you want to delete and click (icon) in the preview area on the right.	**Background** You want to delete a storage unit. **Precautions** Before performing this operation, ensure that the storage unit is not associated with any storage pool. If any associated storage pool is displayed in the **Storage Pool** area, find it on the storage pool page. Ensure that the storage pool is no longer needed and delete it. Then delete the storage unit.	None

4.12.2 Managing a Storage Pool

A storage pool must contain one storage unit only. A storage pool provides an abstraction layer and realizes physical isolation. You can view, modify, and delete a created storage pool.

Operation	Navigation Path	Description	Key Parameter
Viewing a storage pool	• Viewing basic information: On the navigation bar, choose ⊟ > **Storage Pool**. • Viewing details: On the navigation bar, choose ⊟ > **Storage Pool**. On the page that is displayed, click the desired storage pool.	**Background** This operation displays basic information about a storage pool. **Precautions** Before performing this operation, ensure that the storage pool has been created.	Alarm Threshold When the usage of the storage pool exceeds the threshold, an alarm is generated, prompting you to expand the capacity or delete unneeded backup data to release storage space. If you do not expand the capacity or delete unneeded backup data, subsequent backup jobs may fail.
Modifying a storage pool	On the navigation bar, choose ⊟ > **Storage Pool**. Move the mouse pointer to the storage pool that you want to modify and click ✎ in the button area on the right, or click the storage pool that you want to modify and click ✎ in the preview area on the right.	**Background** This operation modifies information about a storage pool. After modification, the system automatically synchronizes the modification to the associated storage unit and repository. **Precautions** Before performing this operation, ensure that the storage pool has been created.	None

Operation	Navigation Path	Description	Key Parameter
Deleting a storage pool	On the navigation bar, choose ⊜ > **Storage Pool**. Move the mouse pointer to the storage pool that you want to delete and click ⊖ in the button area on the right, or click the storage pool that you want to delete and click ⊖ in the preview area on the right.	**Background** This operation deletes an unneeded storage pool. **Precautions** Before performing this operation, ensure that the storage pool to be deleted is not associated with any repository. If any associated repository is displayed in the **Repository** area, find it on the repository page. Ensure that the repository is unneeded and delete it. Then delete the storage pool.	None

4.12.3 Managing a Repository

A repository provides storage space for backups and source data for restore jobs. Backups generated during a backup job are saved in a repository. You can view, modify, and delete an existing repository.

Operation	Navigation Path	Description	Key Parameters
Viewing a repository	• Viewing basic information: On the navigation bar, choose (icon) > **Repository**. • Viewing details: On the navigation bar, choose (icon) > **Repository**. On the displayed page, click the desired repository.	**Background** You want to view basic information about a repository. **Precautions** Before performing this operation, ensure that the repository has been created.	Alarm Threshold If the repository usage exceeds the threshold, an alarm is reported, prompting you to expand capacity or delete unneeded backup data. If you do not do so, subsequent backup jobs may fail.

Operation	Navigation Path	Description	Key Parameters
Modifying a repository	On the navigation bar, choose 🛢️ > **Repository**. Move the mouse pointer to the repository you want to modify and click 🖊 in the button area on the right, or click the repository you want to modify and click 🖊 in the preview area on the right.	**Background** You want to update information about a repository. After modification, the system automatically synchronizes the modification to the associated backup plan. **Precautions** ● Before performing this operation, ensure that the repository has been created. ● After modification, the repository capacity cannot be less than the used capacity or greater than the total available capacity of the storage pool to which the repository belongs.	None

Operation	Navigation Path	Description	Key Parameters
Deleting a repository	On the navigation bar, choose ⬤ > **Repository**. Move the mouse pointer to the repository you want to delete and click ⊖ in the button area on the right, or click the repository you want to delete and click ⊖ in the preview area on the right.	**Background** You want to delete a repository. **Precautions** Before performing this operation, ensure that the repository is not associated with any backup plan. If any associated backup plan is displayed in the **Backup Plan** area, find it on the backup plan page. Ensure that the backup plan is no longer needed and delete it. Then delete the repository. If any associated backup plan is displayed in the **Replication Plan** area, find it on the replication plan page. Ensure that the replication plan is no longer needed and delete it. Then delete the repository.	None

Operation	Navigation Path	Description	Key Parameters
Clearing space	On the navigation bar, choose ⬡ > **Repository**. Move the mouse pointer to the repository whose space you want to clear and click 🧹 in the button area on the right, or click the repository and click 🧹 in the preview area on the right.	**Background** You no longer require some backups and want to remove them from the repository for more space. **Precautions** Before performing this operation, ensure that the repository has been created.	None

4.13 Managing Backups

4.13.1 Managing a Protected Set

A protected set defines backup objects, which can be one or more protected objects. You can assign or exclude disks for all or specified VMs. You can view, modify, clone, and delete an existing protected set.

Operation	Navigation Path	Description	Key Parameters
Viewing a protected set	• Viewing basic information: On the navigation bar, choose (icon) > **Protected Set**. • Viewing details: On the navigation bar, choose (icon) > **Protected Set**. On the displayed page, click the desired protected set.	**Background** You want to view information about the protected environments and protected objects in a protected set. **Precautions** Before performing this operation, ensure that the protected set has been created.	• Protected Environment Type Type of the protected environment in a protected set • Protected Object Number Number of protected objects in a protected set Click the parameter value displayed as a hyperlink. In the displayed dialog box, you can view details about the protected objects in the protected set. Click (icon) next to a protected object to rapidly locate the protected object in the protected environment navigation tree. • Time of Last Validation Time when the validity of the path of a protected object in the protected set is verified for the last time.

Operatio n	Navigation Path	Description	Key Parameters
Modifying a protected set	On the navigation bar, choose ⬆ > **Protected Set**. Move the mouse pointer to the protected set you want to modify and click 🖊 in the button area on the right, or click the protected set you want to modify and click 🖊 in the preview area on the right.	**Background** You want to add backup objects to or remove backup objects from a protected set. After modification, the system automatically synchronizes the modification to the associated backup plan. **Precautions** Before performing this operation, ensure that the protected set has been created.	None
Verifying a protected set	On the navigation bar, choose ⬆ > **Protected Set**. Move the mouse pointer to the protected set you want to verify and click 🔄 in the button area on the right, or click the protected set you want to verify and click 🔄 in the preview area on the right.	**Background** You want to verify the paths of protected objects in a protected set. **Precautions** ● Before performing this operation, ensure that the protected set has been created. ● If verification fails, check whether protected objects in the protected set exist or whether the paths of protected objects are changed.	None

Operation	Navigation Path	Description	Key Parameters
Cloning a protected set	On the navigation bar, choose ⬆ > **Protected Set**. Move the mouse pointer to the protected set you want to clone and click ▤ in the button area on the right, or click the protected set you want to clone and click ▤ in the preview area on the right.	**Background** You want to clone a protected set to create a duplicate. Then you can modify the duplicate to quickly obtain a new protected set instead of creating one, saving configuration time. **Precautions** Before performing this operation, ensure that the protected set has been created.	None

Operation	Navigation Path	Description	Key Parameters

Deleting a protected set	1. On the navigation bar, choose ⊙ > **Protected Set**.
	
	2. Click the protected set you want to delete, and check whether it is associated with any backup plan in the preview area on the right.
	
	    ● If any associated backup plan is displayed in the **Backup Plan** area, find it on the backup plan page. Modify the backup plan to remove the association between the protected set and the backup plan. Or, delete the backup plan after confirming that it is no longer needed. Then delete the protected set.
	
	    ● If no associated
		Background
		You want to delete a protected set.
		
		Precautions
		Before performing this operation, ensure that the protected set to be deleted is not associated with any backup plan.
			None

Operatio n	Navigation Path	Description	Key Parameters

	backup plans are displayed in the **Backup Plan** area, delete the protected set directly.
	
	3. Delete the protected set using either of the following methods:
	
	  ● Move the mouse pointer to the protected set you want to delete and click 🚫 in the button area on the right.
	
	  ● Click the protected set you want to delete and click 🚫 in the preview area on the right.		

4.13.2 Managing a Backup Policy

A backup policy defines the scheduling rule of the system to automatically back up protected objects. The backup policy includes the scheduling plan, backup retention rule, and backup verification rule. One backup policy can be used by multiple backup plans. You can view, modify, clone, and delete an existing backup policy.

Operation	Navigation Path	Description	Key Parameters
Viewing a backup policy	● Viewing basic information: On the navigation bar, choose (icon) > **Backup Policy**. ● Viewing details: On the navigation bar, choose (icon) > **Backup Policy**. On the displayed page, click the backup policy you want to view.	**Background** You want to view information about a backup policy, including the scheduling plan, backup data layout, and associated backup plans. **Precautions** Before performing this operation, ensure that the backup policy has been created.	● Data Layout Layout of backups in repositories. The value can be: – Regular Compression is not enabled. Backups are retained in a general layout. – Compress Backup data is compressed, reducing the backend storage capacity required. ● Backup Plan Number of backup plans associated with the backup policy

Operation	Navigation Path	Description	Key Parameters
Modifying a backup policy	On the navigation bar, choose ⬆ > **Backup Policy**. Move the mouse pointer to the backup policy you want to modify and click ✏ in the button area on the right, or click the backup policy you want to modify and click ✏ in the preview area on the right.	**Background** You can modify a backup policy associated with a backup plan to adjust the backup time, scheduling plan, and retry policy of the protected objects in the backup plan. **Precautions** - Before performing this operation, ensure that the backup policy has been created. - After a backup policy is modified, the system will automatically update pending backup jobs associated with the backup policy. Ongoing backup jobs will be executed based on the old policy.	None

Operation	Navigation Path	Description	Key Parameters
Cloning a backup policy	On the navigation bar, choose ⬆ > **Backup Policy**. Move the mouse pointer to the backup policy you want to clone and click 📋 in the button area on the right, or click the backup policy you want to clone and click 📋 in the preview area on the right.	**Background** You want to clone a backup policy to create a duplicate. Then you can modify the duplicate to quickly obtain a new backup policy instead of creating one, saving configuration time. **Precautions** Before performing this operation, ensure that the backup policy has been created.	None

Operation	Navigation Path	Description	Key Parameters
Deleting a backup policy	1. On the navigation bar, choose ⬆ > **Backup Policy**. 2. Click the backup policy you want to delete, and check whether it is associated with any backup plan in the preview area on the right. • If any associated backup plan is displayed in the **Backup Plan** area, find it on the backup plan page. Modify the backup plan to remove the association between the backup policy and the backup plan. Or, delete the backup plan after confirming that it is no longer needed. Then delete the backup policy. • If no associated backup plans are displayed in the **Backup Plan** area, delete the backup policy directly.	**Background** You want to delete a backup policy that you no longer need. **Precautions** • Before performing this operation, ensure that the backup policy to be deleted is not associated with any backup plan. • After a backup policy is deleted, the system will automatically cancel pending backup jobs associated with the backup policy.	None

Operation	Navigation Path	Description	Key Parameters
	3. Delete the backup policy using either of the following methods: ● Move the mouse pointer to the backup policy you want to delete and click ⊖ in the button area on the right. ● Click the backup policy you want to delete and click ⊖ in the preview area on the right.		

4.13.3 Managing a Backup Plan

A backup plan can be associated with only one backup policy, one protected set, and one repository. You can view, modify, clone, and delete an existing backup plan.

Operation	Navigation Path	Description	Key Parameters
Viewing a backup plan	• Viewing basic information: On the navigation bar, choose ⬆ > **Backup Plan**. • Viewing details: On the navigation bar, choose ⬆ > **Backup Plan**. On the displayed page, click the backup plan you want to view.	**Background** You want to view information about a backup plan, including the status, associated protected set, associated repository, and the start time of the latest backup job. **Precautions** Before performing this operation, ensure that the backup plan has been created.	• Status of the backup plan. The value can be: – 🕐 Active Indicates that the backup plan is in the **Active** state. When the backup plan is in this state, the system can perform backup jobs as scheduled. In the preview area, you can click the arrowhead beside **Active** to deactivate the backup plan. – 🕐 Inactive Indicates that the backup plan is in the **Inactive** state. When the backup plan is in this state, the system cannot perform backup jobs as scheduled but you can manually perform backup jobs. In the preview area, you can click the arrowhead beside **Inactive** to activate the backup plan.

Operation	Navigation Path	Description	Key Parameters
Executing a backup plan	On the navigation bar, choose ⬆ > **Backup Plan**. Move the mouse pointer to the backup plan you want to execute and click ▶ in the button area on the right, or click the backup plan you want to execute and click ▶ in the preview area on the right.	**Background** You want to execute a backup plan. **Precautions** • Before performing this operation, ensure that the backup plan has been created. • If the backup plan has ongoing backup jobs, the system adds new backup jobs and sets them to the **Pending** state. • If backup jobs have been executed based on the backup plan before, the system automatically performs an incremental backup after you click ▶. • If no backup jobs have been executed based on the backup plan, the system automatically performs a full backup after you click ▶. • You can click the row of a backup plan at any time after the plan is created to view the plan details. If you click **Full Backup**, the system will perform a full backup as required.	None

Operati on	Navigation Path	Description	Key Parameters
Modifyin g a backup plan	On the navigation bar, choose ⬆ > **Backup Plan**. Move the mouse pointer to the backup plan you want to modify and click 🖊 in the button area on the right, or click the backup plan you want to modify and click 🖊 in the preview area on the right.	**Background** You want to change the protected set or backup policy associated with your backup plan. After the modification, the system will execute backup jobs based on the modified information. **Precautions** Before performing this operation, ensure that the backup plan has been created.	Offline Transmission **Disabled**: Select this option when Teleport devices have been sent to the Huawei data center and data has been uploaded. **Enabled**: Select this option when you need to use **Offline Transmission**. **Suspended**: Select this option when the Teleport devices or disks have been disconnected from the VMware environment.
Cloning a backup plan	On the navigation bar, choose ⬆ > **Backup Plan**. Move the mouse pointer to the backup plan you want to clone and click 📋 in the button area on the right, or click the backup plan you want to clone and click 📋 in the preview area on the right.	**Background** You want to clone a backup plan to create a duplicate. Then you can modify the duplicate to quickly obtain a new backup plan instead of creating one, saving configuration time. **Precautions** Before performing this operation, ensure that the backup plan has been created.	None

Operation	Navigation Path	Description	Key Parameters
Deleting a backup plan	On the navigation bar, choose ⊙ > **Backup Plan**. Move the mouse pointer to the backup plan you want to delete and click 🔴 in the button area on the right, or click the backup plan you want to delete and click 🔴 in the preview area on the right.	**Background** You want to delete a backup plan that you no longer need. **Precautions** ● Before performing this operation, ensure that the backups associated with the backup plan to be deleted will not be used to restore data. ● Ensure that there are no ongoing backup jobs associated with the backup plan.	None

4.13.4 Managing a Backup

A backup contains the backup data generated after a backup plan performs a backup job based on a backup policy. The backup contains all data required to restore backup objects. You can view, modify, clone, and delete an existing backup.

Operation	Navigation Path	Description	Key Parameters
Viewing a backup	You can view a backup using either of the following methods: • Method 1: On the navigation bar, choose ⬇ > **VMware**. In the navigation tree on the left, locate the protected objects for which backup jobs have been performed. Then click the protected objects on the right. • Method 2: On the navigation bar, choose ⬇ > **All Backups**. Click the desired backup and view its details in the preview area on the right. NOTE Both methods provide similar basic functions. The difference is that you can batch delete and verify backups if using method 2.	**Background** You want to view the generation time and verification status of backups of a backup object, and want to restore and delete a backup. **Precautions** Before performing this operation, ensure that the backup has been created.	• Status Verification status of a backup. The value can be: – Valid Indicates that **Quick Verification** or **Full Verification** has been performed to the backup and the result shows that the backup can be used to restore data. – Invalid Indicates that **Quick Verification** or **Full Verification** has been performed to the backup and the result shows that the backup is invalid. In this case, the backup data has been damaged or is unavailable, and the backup cannot be used to restore data. – Not verified Indicates that the backup has not been verified. You need to verify the backup before using it to restore data. • Protected Object (UUID) Unique identifier of the backup-associated protected object in the protected environment

Operation	Navigation Path	Description	Key Parameters
			● Protected Object (GUID) Unique identifier of the backup–associated protected object in eBackup ● Path Path of the backup-associated protected object in the protected environment
Modifying the expiration time of a backup	1. Select a path based on the protected environment type. On the navigation bar, choose ⊙ > **VMware**. 2. In the navigation tree on the left, locate the protected objects for which backup jobs have been performed. Then click the protected objects in the function pane on the right. 3. In the preview area on the right, click the backup whose expiration time you want to modify and click ✎ in the shortcut button area.	**Background** You want to modify the expiration time of a backup. The change does not affect the backup plan and associated backup policy. After the change, the backup is retained based on the new retention rule. **Precautions** Before performing this operation, ensure that the backup whose expiration time you want to modify exists.	● Retained for a period Backups generated based on a backup policy will be retained for xx years, months, weeks, or days. Once the retention period ends, the system automatically deletes expired backups. ● Retained until a specific day Backups generated based on a backup policy will be retained for a specific point in time. Once the retention period ends, the system automatically deletes expired backups.

Operation	Navigation Path	Description	Key Parameters
Using a backup to restore data	1. Select a path based on the protected environment type. On the navigation bar, choose > **VMware**. 2. In the navigation tree on the left, locate the protected objects for which backup jobs have been performed. Then click the protected objects in the function pane on the right. 3. Select a restore type based on data damage and loss in the production end.	**Background** You want to use backups to restore the protected objects, including restoring LUNs, VMs, disks of the VM, and files on disks. **Precautions** ● Before restoring a VM, ensure that full backup has been performed for the VM and the backup is in the **Valid** state. ● Before restoring a disk or files on a disk, ensure that full backup has been performed for the disk and the backup is in the **Valid** state.	Disk restore If data on a disk of a production VM is damaged, lost, or removed, perform this operation to restore the disk.

Operation	Navigation Path	Description	Key Parameters
Deleting a backup	1. Select a path based on the protected environment type. On the navigation bar, choose > **VMware**. 2. In the navigation tree on the left, locate the protected objects for which backup jobs have been performed. Then click the protected objects in the function pane on the right. 3. Select the backup you want to delete and click 🚫 in the preview area on the right.	**Background** You want to delete a backup that you no longer need to clean space. **Precautions** ● Before performing this operation, ensure that the backup will not be used to restore data. ● Ensure that there are no ongoing restoration jobs associated with the backup.	None

4.14 Common Operations

4.14.1 Logging In to eBackup

This section describes how to log in to eBackup.

Procedure

Step 1 Open a web browser on your maintenance terminal.

📖 **NOTE**

- The following browsers are supported:
- Internet Explorer 9 to 11
- Mozilla FireFox 27 to 43
- Google Chrome 28 to 60
- The recommended display resolution is 1280 x 768.
- This section uses Internet Explorer 9 as an example.
- It is strongly recommended that you back up and restore data with eBackup on trusted networks to prevent security threats or loss.

Step 2 In the address bar of the browser, enter **https://**_xxx.xxx.xxx.xxx:port_.

xxx.xxx.xxx.xxx indicates the backup management plane IP address of the backup server, and _port_ indicates a port number, which is **8088** by default. You can also enter the backup management plane IP address of the backup server directly in the address bar, and press **Enter**.

Step 3 Configure the browser.

For how to configure the browser, see **Configuring Internet Explorer**, **Configuring Firefox**, or **Configuring Chrome**.

Step 4 Select a language and enter your username and password.

- eBackup displays contents in your selected language.
- The default username of eBackup is **admin**, and the default password is **PXU9@ctuNov17!**.

Step 5 Click **Login**.

----End

4.14.2 Managing an eBackup Server

This operation allows you to view the status of the backup server and backup proxies of eBackup backup management system to discover and handle anomalies in a timely manner. In addition, you can set HA parameters to configure eBackup as an HA system.

Context

HA refers to that active and standby modules work in hot or cold backup mode to implement specific functions. After the active module is faulty, the standby module automatically takes over the role of the active module to implement system functions, improving system reliability.

To enable eBackup to support the HA function, plan at least two eBackup servers. Initialize one as the backup server, and the other servers as backup proxies. By default, eBackup does not support the HA function. You need to set HA parameters to configure eBackup as an HA system. After the configuration, the backup server and one backup proxy work in active/standby mode. After the backup server fails, the backup proxy takes over the role of the backup server to ensure normal system operation.

Procedure

Step 1 On the navigation bar, choose (icon) > **Server**.

Step 2 **Optional:** In the upper right corner, set the search criteria and click (icon) to search for the desired server.

Step 3 View information about the server. **Table 4-12** describes related parameters.

Table 4-12 Server parameters

Parameter	Description
ID	The only identification of the server in eBackup backup management system.
Accessibility Status	Status of the server. The value can be: ● Accessible The communication between the backup server and backup proxies is normal and backup and restoration services run correctly. ● Inaccessible The backup server communicates with backup proxies through heartbeat to check the status of backup proxies. If the backup server cannot detect a backup proxy in a specific period of time, the status of the proxy is changed to inaccessible.
Register Status	Registry status of the server. The value can be: ● Registered After the backup server and backup proxies are deployed at eBackup backup management system, they are automatically registered with eBackup backup management system. ● Unregistered If you manually unregister a backup proxy, **Register Status** of the server changes to **Unregistered**. If you want to use the backup proxy to perform backup and restoration jobs, register it with eBackup backup management system.
Backup Management Plane IP Address	Backup management plane IP address of the server.
Internal Communication Plane IP Address	Internal communication plane IP address of the server.

Parameter	Description
Role	The eBackup server has two roles: ● Backup server As the control center of eBackup backup management system, the backup server is responsible for scheduling and monitoring backup and restoration jobs, managing backup storage, backup proxies, and production systems, and processing and responding to users' operations. The backup server also provides the functions of a backup proxy. ● Backup proxy Backup proxies are responsible for receiving backup and restoration jobs delivered by the backup server and interacting with production systems and backup and restoration systems to perform backup and restoration jobs.
NTP Time Synchronization Status	Status of time consistency between the backup proxies and backup server. The value can be **Synchronized**, **Unsynchronized** or **Unknown**. If the state of a backup proxy is **Unsynchronized**, users can click the backup proxy and click **Synchronize Time** in the right information pane to keep time consistency between the backup proxy and backup server. If the backup proxy is restarted or newly registered, the state may become **Unknown**. In this case, users need to wait for the system to automatically synchronize the time of the backup proxy.
iSCSI initiator name	iSCSI initiator name of a server.
UltraPath software installed or not	Whether UltraPath is installed.
Management plane floating IP address of FusionStorage Manager	Management plane floating IP address of FusionStorage Manager of the FusionStorage cluster to which the server is added.

☐ NOTE

The backup server can serve as a backup proxy. To enable users to conveniently view and manage this function, an independent message related to this function will be displayed on the user interface.

Step 4 Register or unregister backup proxies.

📖 **NOTE**

> You cannot register or deregister the backup server configured with HA or associated with backup proxies.

- Registering a selected backup proxy

  Select a backup proxy whose **Accessibility Status** is **Accessible** and **Register Status** is **Unregistered** and use either of the following methods to register the proxy:

  - Click **Register** in the upper left area of the server list and click **OK** in the **Warning** dialog box that is displayed.

  - Click in the preview area on the right and click **OK** in the **Warning** dialog box that is displayed.

- Registering all backup proxies

  eBackup backup management system supports batch registering of all backup proxies, improving configuration efficiency. Click **Register All** and click **OK** in the **Confirm** dialog box that is displayed. Then the system executes the command to batch register backup proxies whose **Accessibility Status** is **Accessible** and **Register Status** is **Unregistered**.

- Unregistering a selected backup proxy

  Select a backup proxy whose **Register Status** is **Registered**, Click in the preview area on the right and click **OK** in the **Warning** dialog box that is displayed.

NOTICE

Before unregistering a backup proxy whose **Accessibility Status** is **Inaccessible** and **Register Status** is **Registered**, ensure that the server meets one of the following requirements:

- The server is shut down.

- The server is started and all the storage units on the server are unmounted. You can run **mount |grep /opt/huawei-data-protection/ebackup/bricks** to check whether there are mounted storage units. If yes, run **umount /opt/huawei-data-protection/ebackup/bricks** to unmount the storage units.

After unregistering a backup proxy whose **Accessibility Status** is **Accessible** and **Register Status** is **Registered**, ensure that all the storage units on the server are unmounted. You can run **mount |grep /opt/huawei-data-protection/ebackup/bricks** to check whether there are mounted storage units. If yes, run **umount /opt/huawei-data-protection/ebackup/bricks** to unmount the storage units.

After unregistering a backup proxy (including unmounting the storage units), stop the eBackup service and uninstall the eBackup software to ensure that the backup proxy will not automatically connect to the backup server subsequently. If you want to use the backup proxy subsequently reinstall the eBackup software and configure the backup proxy again.

Step 5 **Optional:** Set HA parameters if you want to configure eBackup as an HA system.

📖 **NOTE**

eBackup can be configured as an HA system only when there are at least two eBackup servers in the system, that is, there is at least one independent backup proxy server.

----End

4.14.3 Managing Users

By configuring system administrators, you can effectively ensure the security of system data. Only the default super administrator has the right to manage users. The super administrator can modify user information, delete users, force users to go offline, lock users, and unlock users.

About Users

By configuring different users, you can configure system security policies, implement rights-based service management, and monitor and manage online users in real time.

User Roles and Permissions

The eBackup system provides three user levels: super administrator, administrator, and common user. describes their permissions.

📖 **NOTE**

A maximum of 2000 users can be created in the system.

Table 4-13 User permissions

Role	Description
Super administrator permissions	The system provides a default super administrator admin. This user has all operation rights and can manage all resources. The default super administrator cannot be deleted, locked, deleted, or forcibly logged out. The super administrator can change its own login password. The default super administrator can create administrators and common users to implement rights-based service management.
Administrator	Has all rights except system settings. After logging in to the system as an administrator, you can view only your own user information, operations, and events generated by the system.
Common user	Common users have only the permission to view system resources. After logging in to the system as a common user, you can view only your own user information, operations, and events generated by the system.

- System Security Policy

  System security policies include password policies and login policies. For details about how to configure system security policies, see "Configuring Security Policies" in Related Operations.

- A password policy defines parameters such as the password length, complexity, validity period, and expiration notification time threshold for users logging in to the eBackup backup management system.
- A login policy defines the session timeout period for a user to log in to the eBackup management system, whether the user is automatically locked by the system after the number of consecutive incorrect password attempts reaches a specified value, and how long the user is automatically unlocked.

 NOTE

For details about all accounts of the eBackup system, see Account Information Overview.

Related Operations

Operation	Navigation Path	Description	Key Parameters
Configuring Security Policies	On the navigation bar, choose > Account > Security Policy.	**Background** System security policies include password policies and login policies. Perform this operation when you want to improve system security. **Precautions** ● For security purposes, you are advised to enable Password validity period (days), Minimum password validity period (minutes), and Password lock. ● The value of Password Advance Warning Threshold must be less than or equal to the value of Password Validity Period. If the former value is greater than the latter value, the password warning threshold automatically changes to the current password validity period. ● The minimum password validity period must be shorter than or equal to the password validity period. Otherwise, the system	● Session Timeout (minutes) The session timeout period refers to the period during which a user's session with the eBackup backup management system is disconnected due to timeout. After a user logs in to the eBackup system, if the user does not perform any operation within the session timeout period, the current session is disconnected due to timeout. When you perform operations on the eBackup system again, you need to log in to the system again. ● Errors Maximum number of allowed consecutive incorrect password attempts. When the number of incorrect password attempts reaches the value of this parameter, the system automatically locks the account.

Operation	Navigation Path	Description	Key Parameters
		displays an error message.	**NOTE** This parameter is available only when Password Lock is enabled. After an account is locked, the super administrator can manually unlock the account. Alternatively, the system automatically unlocks the account after the preset automatic unlocking time. ● Automatic Unlock in (Minutes) Duration after which an account is automatically unlocked. You can set this parameter when Password Lock is enabled. – This parameter takes effect only for user accounts automatically locked by the system. If an administrator account or a common user account is manually locked by the super administrator, the locking duration does not take effect. Only the super administrator can manually unlock the account. – The automatic unlocking time takes effect only for administrator accounts and common user

Operation	Navigation Path	Description	Key Parameters
			accounts. The super administrator will be automatically unlocked 15 minutes after being locked.

Operation	Navigation Path	Description	Key Parameters
Viewing user details	On the navigation bar, choose > Account > User.	**Background** Perform this operation when you want to view the basic information, role, and lock status of a user. **Precautions** After logging in to the system, the super administrator can view information about all users. Administrators and common users can view only their own user information after logging in to the system.	• Type Type of a user. The options are as follows: – Local Users A local user is a man-machine interaction account (local authentication) and is used to log in to the eBackup system to manage backup and restore services. – LDAP user An LDAP user is a man-machine interaction account (LDAP authentication). It is used to log in to the eBackup system to manage backup and recovery services. – Interface interconnection user The interface interconnection user is a machine-machine interaction account and is used to interconnect the eBackup management system with other systems. eBackup provides a preset interface interconnection user. The default

Operation	Navigation Path	Description	Key Parameters
			user name is NBIUser, and the default password is Huawei@CLOUD 8!. ● CCR-Node roles User role. For details about role types and their rights, see. **NOTE** Administrators and common users can only search for themselves in the search box in the upper right corner. ● Pin Status Check whether the user is automatically locked by the system or locked by the super administrator. **NOTE** If the IP address is locked, you can click Lock IP to view the IP address of the node that is locked due to incorrect password of the interface interconnection user.

Operation	Navigation Path	Description	Key Parameters
Creating a user	On the navigation bar, choose > Account > User and click Create.	**Background** Perform this operation when you want to create users with the administrator and common user roles to restrict different users' operations on the system and improve system security. **Precautions** The super administrator has the highest rights in the system. Log in to the system as the super administrator.	• Type For details about how to create a user type, see "Viewing User Information" in Related Operations. Users of the Interface interconnection user type have the administrator rights. • Role Role of the new user. For details about role types and their rights, see. Create users based on the operation rights of users with different roles defined in the system to restrict user operations on the system, ensuring service system stability and service data security. • Password Login password of the new user. The default password complexity requirements are as follows: – Contains 8 to 16 characters. – Contains at least one special character chosen from !"#$%&'()*+,-./:;<=>?@[\]^`{_|}~ and spaces. – Contains at least two types of uppercase letters,

Operation	Navigation Path	Description	Key Parameters
			lowercase letters, and digits. – Cannot contain three consecutive same characters. – Cannot be the same as the user name or the user name in reverse order. Besides, passwords in the blacklist are invalid. The blacklist file is stored in the /opt/huawei-data-protection/ebackup/conf directory on the backup server. Passwords in the blacklist are case insensitive. ● Maximum number of user connections Indicates the maximum number of sessions for a single user. If this parameter is not set, there is no restriction.

Operation	Navigation Path	Description	Key Parameters
Modification of user details	On the navigation bar, choose > Account > User. Move the mouse pointer to the user to be modified and click in the button area on the right.	**Background** Perform this operation when you want to modify user information, for example, reset the passwords of administrators and common users and change user roles. **Precautions** ● Only the information about users except the super administrator can be modified. ● After resetting the password when modifying user information, notify the corresponding user to use the new password to log in to the eBackup system. **NOTE** If an interface interconnection user has been used to configure the eBackup driver, you need to reconfigure the eBackup driver once the password of the interface interconnection user is changed.	None

Operation	Navigation Path	Description	Key Parameters
Delete the user.	On the navigation bar, choose > Account > User. Move the mouse pointer to the user to be deleted and click in the button area on the right.	**Background** The super administrator can delete an administrator or common user account that is no longer needed. **Precautions** Only the super administrator can delete a user. The super administrator cannot delete itself.	None
Forcing a subscriber to go offline	On the navigation bar, choose > Account > User. Move the mouse pointer to the user to be forced offline and click in the button area on the right.	**Background** The super administrator can force an administrator or a common user to log out of the system. **Precautions** Only the super administrator can force a user to go offline. The super administrator cannot force itself to go offline.	None

Operation	Navigation Path	Description	Key Parameters
Locking a user	On the navigation bar, choose > Account > User. Move the mouse pointer to the user to be locked and click in the button area on the right.	**Background** Perform this operation when you want to lock a user with the administrator or common user role. **Precautions** ● Only the super administrator can lock a user. The super administrator cannot lock itself. ● A locked user cannot log in to the eBackup system. ● The super administrator can lock a user in either of the following ways: – Automatic lock: You can set Password lockout and Number of incorrect password attempts in the password policy to automatically lock a user whose number of consecutive incorrect password attempts exceeds the upper limit. For details, see "Configuring Security Policies" in	None

Operation	Navigation Path	Description	Key Parameters
		Related Operations. – Manual locking: A user is manually locked. The locked user can log in to the system only after being manually unlocked by the super administrator.	
Unlocking a User	On the navigation bar, choose > Account > User. Move the mouse pointer to the user to be unlocked and click in the button area on the right.	**Background** Perform this operation when you want to unlock a user with the administrator or common user role. **Precautions** Manually unlock a locked user in the system. You can unlock the account in either of the following ways: ● Automatic unlocking: If Password Lock is set in the password policy, the system automatically unlocks the user when the locking duration expires. ● Manual unlocking: The super administrator can manually unlock a user that is automatically or manually locked.	None

4.14.4 Managing Certificates

You can import, view, and delete certificates on eBackup in a unified manner.

Obtaining Certificates

Obtain certificates preferentially from the O&M personnel of the corresponding products. If certificates have not been obtained, obtain them by referring to the following steps. If certificates cannot be obtained, contact Huawei technical support.

VMware CA certificate

Use a web browser to log in to the VMware vCenter environment and download the certificate package to a local directory.

After the package is downloaded, change the file name extension to **.zip** and open the package. Find the file of ***.0** format and change its file name extension to ***.crt**.

During certificate import, set the VMware certificate type to **Protected environment**.

Importing Certificates

1. On the navigation bar, choose ⚙ > **Certificate**.
2. Click **Import**.

    If eBackup and interconnected devices communicate using **HTTPS**, you are advised to import a valid CA certificate. Or, eBackup will fail to authenticate the interconnected devices, resulting in security risks.

3. Select the type of the certificate to be imported.

    -   **Protected environment**: If eBackup and protected environments communicate using **HTTPS**, import a valid certificate to authenticate the protected environments. Obtain the certificate from a protected environment administrator.

        Import the new CA certificates.

    -   **S3 storage**: If S3 storage units are used to store backup management data and communicate with eBackup using **HTTPS**, import a valid certificate to authenticate the storage units. Obtain the certificate from a storage device administrator.

    -   **Email server**: If SSL needs to be enabled for email notification, import a CA certificate of an SMTP server. eBackup uses the certificate to authenticate email servers. Obtain the certificate from the administrator of the SMTP server.

    -   **FTP server**: If a Manager communicates with an FTP server using **FTPS**, import a valid certificate to enable the Manager to authenticate the FTP server. Obtain the certificate from the administrator of the FTP server.

4. Click ⋯ , select the certificate to be imported, and click **Upload**.
5. Click **OK**.

Viewing Certificates

1. On the navigation bar, choose ⚙ > **Certificate**.
2. On the **Certificate** page, view imported certificates. **Table 4-14** describes the details.

Table 4-14 Certificate details

Parameter	Description
Fingerprint	Mark used to identify a certificate
Issued To	Holder of the certificate
Issued By	Certificate authority that issues the certificate
Type	Type of the certificate. The value can be **Protected environment**, **S3 storage**, or **Email**.
Description	Description of the certificate
Creation Time	Time when the certificate is applied for
Certificate Expiration Time	Time when the certificate expires. The expiration time is confirmed after the certificate is issued.

Deleting Certificates

Delete unnecessary or expired certificates.

1. On the navigation bar, choose ⚙ > **Certificate**.
2. Select the certificate to be deleted and click ⛔.
3. Read displayed information and click **OK**.

4.14.5 Configuring System Time & Zone

You can configure, modify, and view the system time zone and NTP server information.

Prerequisites

Only external NTP servers running Linux are supported currently.

Procedure

Step 1 On the navigation bar, choose Click ⚙ > **System Time & Zone**.

Step 2 Configure the system time and zone. **Table 4-15** describes the parameters.

Table 4-15 Parameter description

Parameter	Description
System Time	System time of the eBackup server (including the backup server and all backup proxies)
System Zone	If you modify the system zone of the server to one not supported by eBackup, nothing will be displayed on the system zone page. In such a case, you must reconfigure the system zone to ensure the normal operating of eBackup.
NTP Service Status	If an external NTP service is required, enable the NTP service and configure the NTP server address. **NOTE** Enabled NTP service cannot be disabled.
NTP Server 1	IP address or domain name of an external NTP server
NTP Server 2	Contact it from the NTP service provider.

Step 3 Confirm the configuration and click **OK**.

----End

4.14.6 Configuring Internet Explorer

When using HTTPS to access eBackup in Internet Explorer, you are prompted with a security certificate problem. This section explains how to configure Internet Explorer to prevent the problem. Before using Internet Explorer to access eBackup, ensure that Internet Explorer does not support SSL 3.0.

Context

This section uses Internet Explorer 9.0 as an example.

Procedure

Step 1 If **There is a problem with this website's security certificate** is displayed, click **Continue to this website (not recommended)**.

Step 2 Disable Internet Explorer's support for SSL 3.0.

NOTICE

SSL 3.0 may cause device information leakage. It is recommended that you disable SSL 3.0 on the browser as follows before logging in to eBackup.

1. On the menu bar of Internet Explorer, choose **Tools** > **Internet Options** (If the menu bar is unavailable, press **Alt** to display it.)

2. In the **Internet Options** dialog box, click **Advanced** tab.

3. In the **Security** check box, deselect **Enable SSL 3.0** and **Enable SSL 2.0**. At the same time, select **Enable TLS 1.0**, **Enable TLS 1.1**, **Enable TLS 1.2**.

   eBackup supports TLS 1.0, TLS 1.1 and TLS 1.2. Other protocols (such as SSL 2.0 and SSL 3.0) are not supported.

4. Click **OK**.

----End

4.14.7 Configuring Firefox

When using HTTPS to access eBackup in Firefox, you are prompted with a security certificate problem. This section explains how to configure Firefox to prevent the problem. Before using Firefox to access eBackup, ensure that Firefox does not support SSL 3.0.

Context

This section uses Mozilla FireFox 26 as an example.

Procedure

Step 1 If **This Connection is Untrusted** is displayed, choose **I Understand the Risks** > **Add Exception**.

Step 2 Click **Confirm Security Exception** in the dialog box.

Step 3 Disable Firefox's support for SSL 3.0.

> **NOTICE**
>
> SSL 3.0 may cause device information leakage. It is recommended that you disable SSL 3.0 on the browser as follows before logging in to eBackup.

1. In the address box of Firefox, enter **about:config**.

2. Set the value of **security.tls.version.min** to **1**.

----End

4.14.8 Configuring Chrome

When using HTTPS to access eBackup in Chrome, you are prompted with a security certificate problem. This section explains how to configure Chrome to prevent the problem. Before using Chrome to access eBackup, ensure that Chrome does not support SSL 3.0.

Context

This section uses Google Chrome 37 as an example.

Procedure

Step 1 If **Your connection is not private** is displayed, click **Advanced** and **Proceed to xxx.xxx.xxx.xxx (unsafe)**.

Step 2 Disable Chrome's support for SSL 3.0.

NOTICE

SSL 3.0 may cause device information leakage. It is recommended that you disable SSL 3.0 on the browser as follows before logging in to eBackup.

---

1. Close Chrome.

2. Copy the shortcut icon of Chrome.

3. Right-click the new shortcut icon and choose **Properties**. The **Properties** dialog box is displayed.

4. In **Targets**, enter a space and **--ssl-version-min=tls1**.

----End

5 Change History

Released On	Description
2024-03-30	This issue is the second official release, which incorporates the following change: ● Added support for VMware vSphere 6.7, 7.0, and 8.0.
2020-02-25	This issue is the first official release.