Cloud Backup and Recovery

Troubleshooting

Issue	01
Date	2024-08-31

Contents

1 Failed to Execute a Backup Task

Symptom

A manual or scheduled backup task fails.

Troubleshooting

Possible causes are listed here in order of their probability.

If the fault persists after you have ruled out one cause, move on to the next one.

Figure 1-1 Troubleshooting

Table 1-1 Troubleshooting

Possible Cause	Solution
The vault capacity has been used up.	For detailed handling measures, see **The Vault Capacity Has Been Used Up**.
The vault is frozen because your account is in arrears.	**Top up your account**.
Other operations are being performed on the resource to be backed up.	For detailed handling measures, see **Other Operations Are Being Performed on the Resource to Be Backed Up**.

Possible Cause	Solution
The system is busy.	Back up the data in off-peak hours or **submit a service ticket**.

The Vault Capacity Has Been Used Up

Backup stops once the usage of the vault exceeds the upper limit. Take the following measures when the storage capacity of your vault is not enough:

- Log in to the CBR console, locate the target vault, and delete unwanted backups by following instructions in **Deleting a Backup**.
- If you want to retain the generated backups, expand the vault capacity. For details, see **Expanding Vault Capacity**.
- If a backup policy has been applied to the vault, disable the backup policy or remove the policy from the vault. To disable the policy, see **Disabling a Backup Policy**. To remove the policy, see **Removing a Policy from a Vault**. Then, automatic backup is disabled, and the storage capacity of the vault will not change. You can also **modify the backup policy** or **dissociate resources from the vault**.

Other Operations Are Being Performed on the Resource to Be Backed Up

Automatic backup may fail when other operations, such as backup and restoration, are being performed on the target resource.

1. Log in to the CBR console and check whether the status of the target resource is **Available** or **Running**.

   Figure 1-2 Checking the resource status
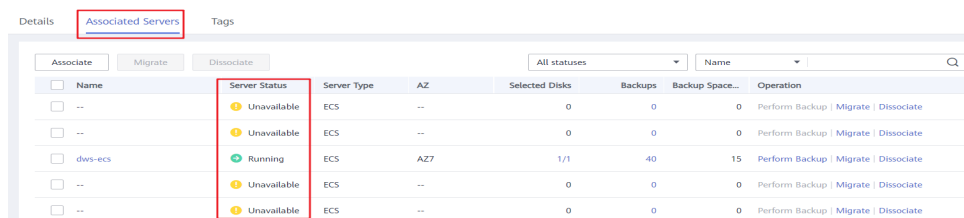
2. If yes, perform the backup again. If no, wait until the status of the target resource becomes **Available** or **Running**.

Submitting a Service Ticket

If the problem persists, **submit a service ticket**.

2 Failed to Delete a Backup

Symptom

The **Delete** button is unavailable, or a backup fails to be deleted.

Troubleshooting

Possible causes are listed here in order of their probability.

If the fault persists after you have ruled out one cause, move on to the next one.
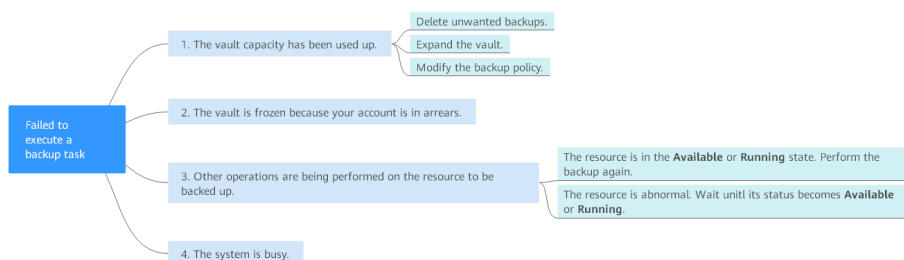
Table 2-1 Troubleshooting

Possible Cause	Solution
The backup is being created or is being used for restoration.	Wait until the backup is created or the restoration completes and then delete it.
The backup is a cloud server backup and has been used to create an image, so the **Delete** button for the backup is grayed out.	Delete the image before deleting the backup. For details, see **Deleting Images**.
A system exception occurs.	Delete the backup again. If the problem persists, **submit a service ticket**.
Insufficient permissions.	Check whether the account has the deletion permission on the IAM console.

Submitting a Service Ticket

If the problem persists, **submit a service ticket**.

3 Failed to Expand the Vault Capacity

Symptom

Failed to expand the capacity of a vault.

Troubleshooting

Possible causes are listed here in order of their probability.

If the fault persists after you have ruled out one cause, move on to the next one.
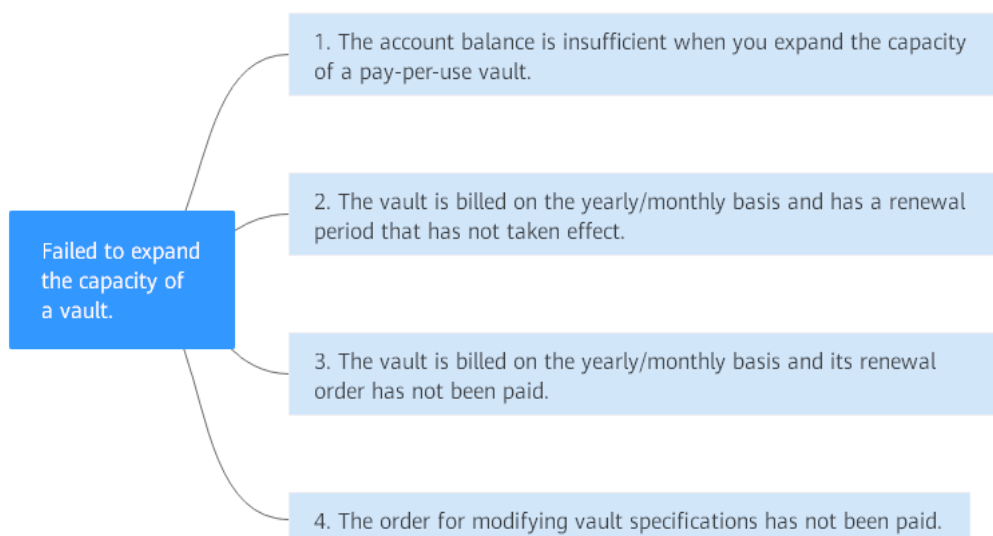
Figure 3-1 Troubleshooting

Table 3-1 Troubleshooting

Possible Cause	Solution
The account balance is insufficient when you expand the capacity of a pay-per-use vault.	Top up your account and try again. For details, see **Topping Up an Account**.
The vault is billed on the yearly/monthly basis and has a renewal period that has not taken effect.	For detailed handling measures, see **The Vault Is Billed on the Yearly/monthly Basis and Has a Renewal Period That Has Not Taken Effect**.
The vault is billed on the yearly/monthly basis and its renewal order has not been paid.	Go to management console, choose **Billing Center** > **Orders** to check whether there are unpaid vault renewal orders. If yes, complete the payment promptly.
The order for modifying vault specifications has not been paid.	Go to management console, choose **Billing Center** > **Orders** to check whether there are unpaid orders for modifying vault specifications. If yes, complete the payment promptly.

The Vault Is Billed on the Yearly/monthly Basis and Has a Renewal Period That Has Not Taken Effect

If your yearly/monthly vault has a renewal period that has not taken effect, its capacity expansion will fail. Expand the vault after the renewal period takes effect or after the renewal is unsubscribed. For details about how to unsubscribe an order, see **Unsubscribing from a Renewal Period**.

For example, the validity period of the current subscription is from August 1 to August 31. If you renew your subscription on August 15, the renewal will take effect from September 1 to September 30. If you expand the capacity of the vault on August 20, the expansion will fail.

Submitting a Service Ticket

If the problem persists, **submit a service ticket**.

4 Failed to Attach Disks

Symptom

Failed to attach disks despite following the procedure: Create EVS disks using the same disk backup (XFS file system backup) and attach them to the same server (to which multiple EVS disks with XFS file system backup have been attached). Running the **mount** command to attach disks fails.

Possible Cause

The superblock of an EVS disk (with XFS file systems) stores a universally unique identifier (UUID) about the file system. If a server has multiple disks (with XFS file systems), multiple UUIDs will exist on the server. Multiple disks may have the same UUID, which can cause the file system mounting to fail.

Troubleshooting Methods

When attaching an EVS disk, use parameters without UUID control or reallocate a new UUID to ensure that each UUID is unique.

Solution

Step 1 Log in to the server to which EVS disks failed to be attached.

Step 2 Resolve the problem in either of the following ways:

- Use a parameter without UUID when attaching an EVS disk: Run **mount -o nouuid /dev/***Device name***/***Mount path*, for example:

  mount -o nouuid /dev/sda6 /mnt/aa

- Reallocate a new UUID: Run **xfs_admin -U generate /dev/***Device name*.

  📖 **NOTE**

  Because setting a parameter without UUID requires you to execute the command every time, you are advised to reallocate a new UUID.

----End

5 Data Disks Are Not Displayed After a Windows Server Is Restored

Symptom

When a Windows server is restored, the data disks are not displayed.

Possible Cause

Due to the limitations of Windows operating systems, data disks are in offline mode after a server is restored.

Solution

Step 1 On the Windows desktop, right-click the **My Computer** icon.

Step 2 Choose **Manage** from the shortcut menu. The **Computer Management** page is displayed.

Step 3 In the navigation tree, choose **Storage** > **Disk Management**.

Data disks are in the offline state, as shown in **Figure 5-1**.

Figure 5-1 Data disks in the offline state
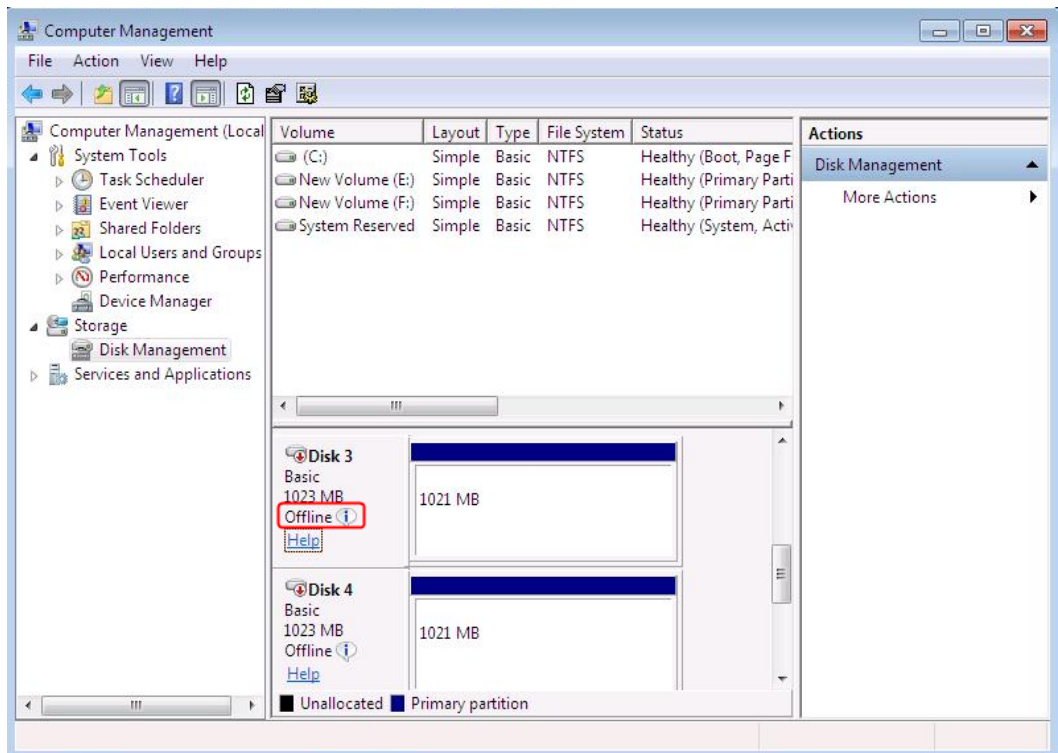
Step 4 Right-click a data disk in the offline state and choose **Online**, as shown in **Figure 5-2**.

Figure 5-2 Setting a data disk to be online
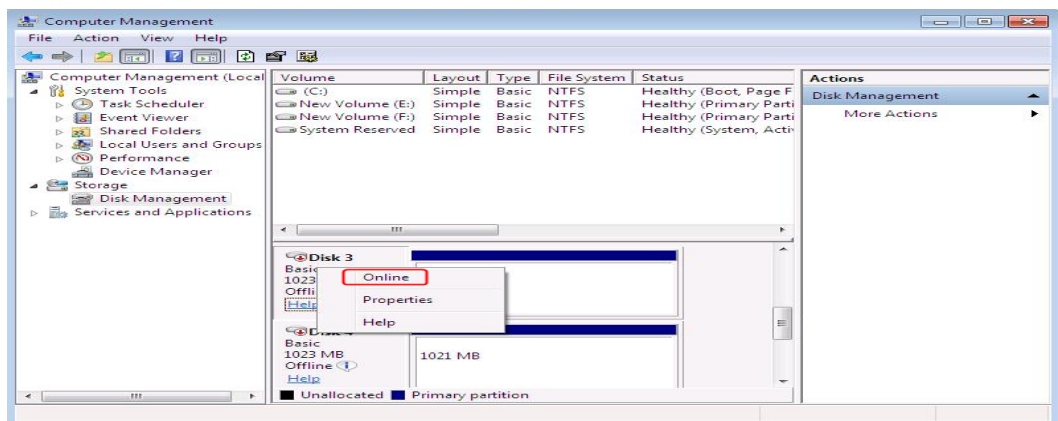
After the data disk status changes to **Online**, the data disk will be displayed in the disk list, as shown in **Figure 5-3**.

In addition, the data disk will be properly displayed on the server.

Figure 5-3 Viewing online data disks
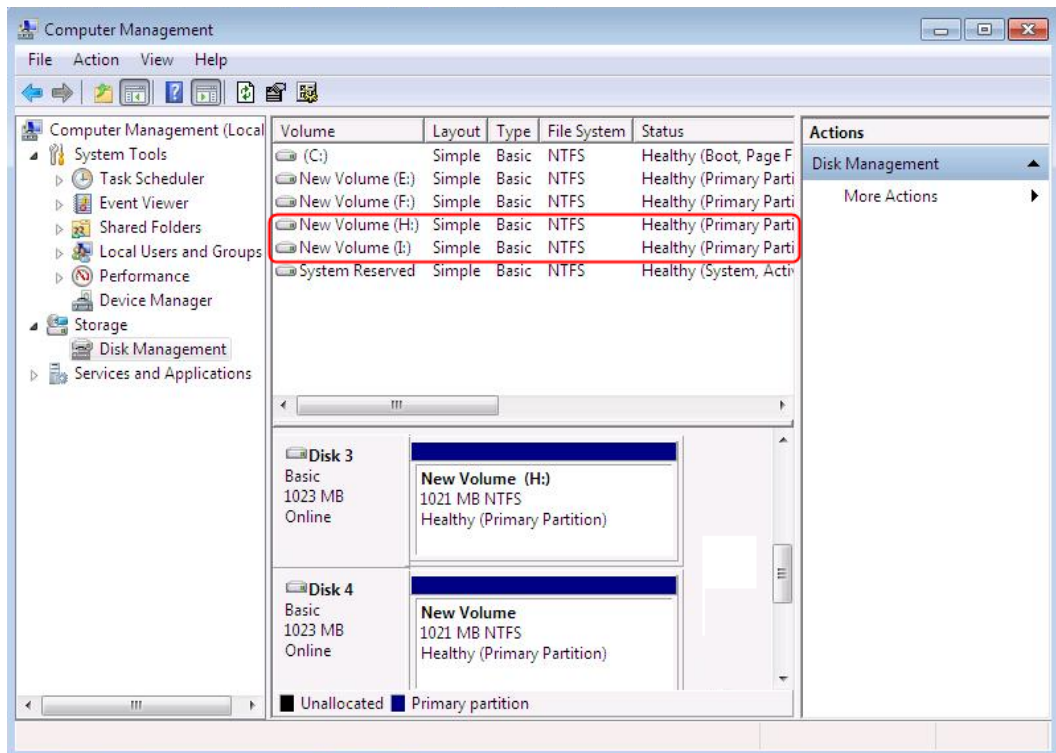
----End

6 Failed to Cancel Backup Sharing

Symptom

When you cancel the backup sharing, the system prompts a message indicating that the canceling failed.

Troubleshooting

Possible causes are listed here in order of their probability.

If the fault persists after you have ruled out one cause, move on to the next one.

Figure 6-1 Troubleshooting

Table 6-1 Troubleshooting

Possible Cause	Solution
The shared backup was used to create images.	Delete the images and then delete the shared backup. For details, see **Deleting Images**.
The status of the shared backup failed to be updated.	Try again or **submit a service ticket**.

7 Failed to Download or Install the Agent Required by Application-Consistent

Symptom

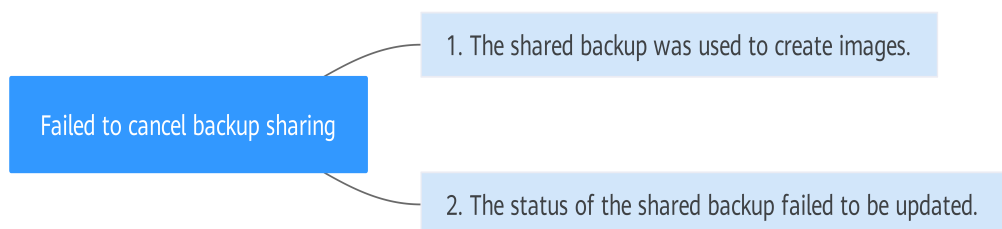The system displays a message indicating that the script cannot be downloaded or the Agent fails to be installed in Linux mode 2.

Possible Causes

- Cause 1: The DNS cannot resolve the OBS domain name.
- Cause 2: The OpenSSL version of the target server is too early.

Solution for Cause 1

Cause 1: The DNS cannot resolve the domain name.

You need to manually change the DNS server address to a private DNS server address of Huawei Cloud by referring to **What Are the Private DNS Server Addresses Provided by the DNS Service?** If the problem persists, try later or use the Linux mode 1 to install it.

Procedure (Linux)

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

Step 2 Run the **vi /etc/resolv.conf** command to edit the **/etc/resolv.conf** file. Add the DNS server IP address above the existing name server information, as shown in **Figure 7-1**.

Figure 7-1 Configuring DNS

The format is as follows:
```
nameserver 100.125.1.250
nameserver 100.125.17.29
```

Step 3 Press **Esc**, input **:wq**, and press **Enter** to save the changes and exit the vi editor.

Step 4 Run the following command to check whether the IP address is added. If yes, the operation is complete.

cat /etc/resolv.conf

----End

Procedure (Windows)

Step 1 Go to the ECS console and log in to the ECS running Windows Server 2012.

Step 2 Click **This PC** in the lower left corner.

Step 3 On the page that is displayed, right-click **Network** and choose **Properties** from the drop-down list. The **Network and Sharing Center** page is displayed, as shown in **Figure 7-2**. Click **Local Area Connection**.

Figure 7-2 Page for network and sharing center
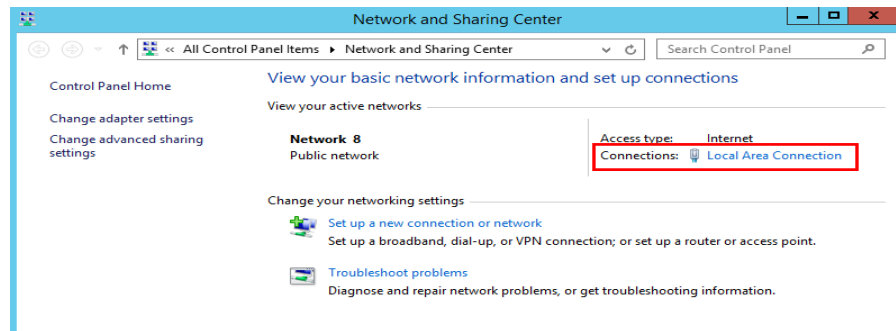
Step 4 In the **Activity** area, select **Properties**. See **Figure 7-3**.

Figure 7-3 Local area connection
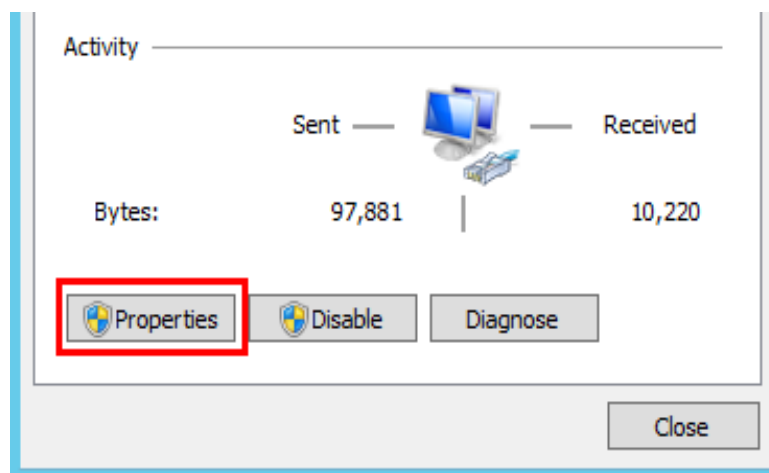
Step 5 In the **Local Area Connection Properties** dialog box that is displayed, select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**. See **Figure 7-4**.

Figure 7-4 Local area connection properties

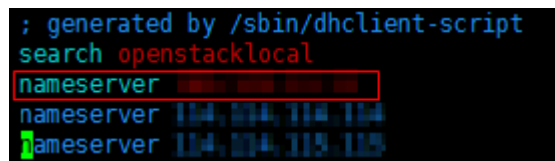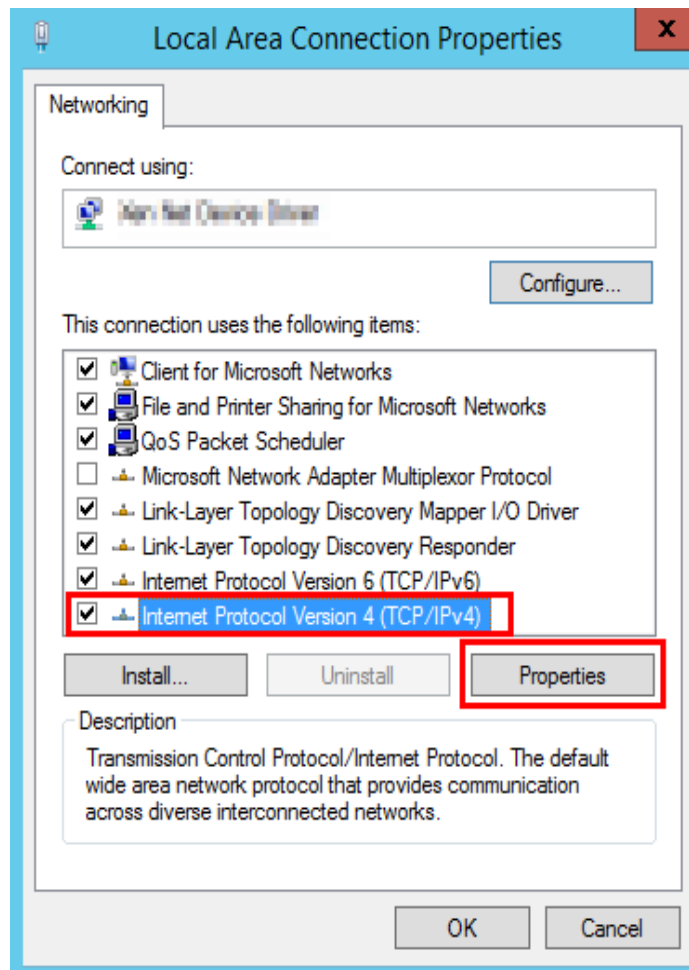**Step 6** In the dialog box that is displayed, select **Use the following DNS server addresses:** and configure DNS, as shown in **Figure 7-5**. You need to manually change the DNS server address to a private DNS server address of Huawei Cloud by referring to **What Are the Private DNS Server Addresses Provided by the DNS Service?** Then click **OK**.

Figure 7-5 Configuring DNS
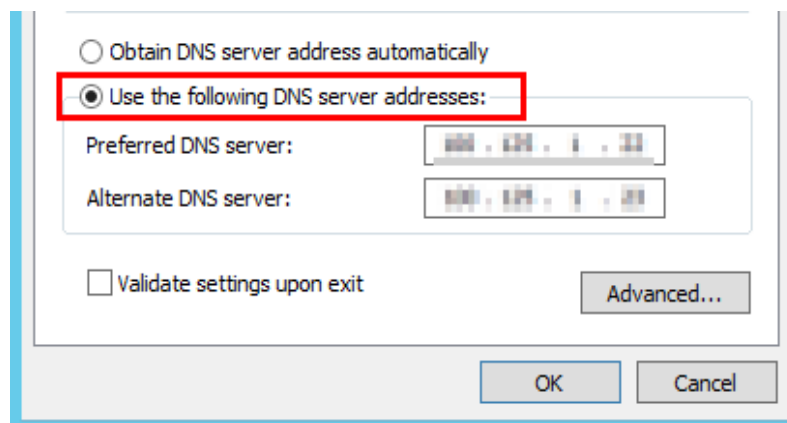
----End

Solution for Cause 2

Cause 2: The OpenSSL version of the target server is too early.

Step 1 Use a remote management tool (such as PuTTY or Xshell) to connect to your ECS through the elastic IP address.

Step 2 Select the Agent version based on your needs, copy the command of installation mode 2 to the server, and change **https** to **http** in wget. Run the command as the root user.

----End

8 Failed to Install the Agent on Windows

Scenario 1: User rdadmin Already Exists

Symptom

The Agent of application-consistent backup failed to be installed on a Windows server. Message "Agent working user rdadmin exist" is displayed.

Possible Causes

- User **rdadmin** has been created on the Windows server before the Agent is installed.
- If the Agent installation has been performed on the Windows server, user **rdadmin** will be created even if the installation fails.

Solution

Step 1 Log in to the Windows server, click the Windows icon in the lower left corner of the desktop, and choose **Control Panel** > **User Accounts**.

Step 2 Check whether user **rdadmin** exists. If the user exists, confirm that it is not created by other applications and then delete it.

Step 3 After the user is deleted, install the Agent again.

----End

Scenario 2: Installation Failed Due to Registry Modification

Symptom

You have changed the default encoding format by modifying the registry.

Example: Create autorun in **\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft \Command Processor** and set its value to **chcp 65001**.

Solution

Change the value to **chcp 65001 > nul**.

Step 1 Press **Win**+**R** to open the **Run** dialog box and then enter **regedit**.

Step 2 Go to the **\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor** directory.

Step 3 Right-click and choose **New** > **String Value** (REG_SZ) from the shortcut menu. Name the string **autorun**.

Step 4 Double-click and change the value to **chcp 65001 > nul**.

----End

9 Failed to Implement Application-Consistent Backup

Symptom

The user has installed the required Agent on the cloud servers running MySQL databases or SAP HANA applications, but the application-consistent backup fails.

Possible Cause

The unfreezing and freezing scripts are not modified according to the steps provided in **Using a Custom Script to Implement Application-Consistent Backup** in the *Cloud Backup and Recovery Best Practices*.

Solution

Before performing application-consistent backup, modify the unfreezing and freezing scripts by referring to **Using a Custom Script to Implement Application-Consistent Backup**.

10 A Server Created Using an Image Enters Maintenance Mode After Login

Symptom

A server is created using the image of a cloud server backup. However, upon login to the server, the server enters maintenance mode and cannot be used.

Possible Cause

After the server creation, the configuration parameters contained in the **/etc/fstab** file in the system disk of the new server are that of the backup source server, causing the UUID information to be inconsistent with the new data disks. As a result, the ECS encounters an error when uploading **/etc/fstab** during the bootup and enters maintenance mode.

Solution

The following uses CentOS as an example.

Step 1 After creating an ECS using an image, log in to the ECS console, click **Remote Login** in the row of the ECS.

Step 2 On the maintenance mode page that is displayed, access the system as prompted.

Figure 10-1 Maintenance mode of the system


```
CentOS Linux 7 (Core)
Kernel 3.10.0-1062.12.1.el7.x86_64 on an x86_64

Hint: Num Lock on

cli-demo login: root
Password:
Last login: Tue Feb  7 16:48:33 on tty1

        Welcome to Huawei Cloud Service

[root@cli-demo ~]#
```

Step 3 Run the **cat /etc/fstab** command to check the disk attachment information.

Figure 10-2 Data disk UUIDs


```
WARNING! The remote SSH server rejected X11 forwarding request.
Last login: Tue Feb  7 16:35:37 2023

          Welcome to         Cloud Service

[root@cli-demo ~]#
[root@cli-demo ~]# cat /etc/fstab

#
# /etc/fstab
# Created by anaconda on Mon Apr 27 13:51:12 2020
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=207b19eb-8170-4983-acb5-9098af381e72 /                       ext4    defaults        1 1
UUID=08e5c568-86ca-40ce-8145-66b3ea53076a /tmp/test               ext4    defaults        1 0
[root@cli-demo ~]#
```

Step 4 Run the **vi /etc/fstab** command to open the file, press **i** to enter the editing mode, and delete the attachment information of all data disks. Then, press **Esc** to exit the editing mode and run **:wq!** to save the change and exit.

Figure 10-3 /etc/fstab after being updated


```
[root@cli-demo ~]# vi /etc/fstab
[root@cli-demo ~]# cat /etc/fstab

#
# /etc/fstab
# Created by anaconda on Mon Apr 27 13:51:12 2020
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=207b19eb-8170-4983-acb5-9098af381e72 /                       ext4    defaults        1 1

[root@cli-demo ~]#
```

Step 5 Run the **reboot** command to restart the system.

Figure 10-4 Normal bootup page


```
CentOS Linux 7 (Core)
Kernel 3.10.0-1062.12.1.el7.x86_64 on an x86_64

cli-demo login:
```

Step 6 After entering the system, attach the data disks manually.

Figure 10-5 Attaching the data disks manually

```
[root@cli-demo ~]#
[root@cli-demo ~]# cat /etc/fstab

#
# /etc/fstab
# Created by anaconda on Mon Apr 27 13:51:12 2020
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=207b19eb-8170-4983-acb5-9098af381e72 /                    ext4    defaults        1 1

[root@cli-demo ~]#
[root@cli-demo ~]# mount /dev/vdb /tmp/test
[root@cli-demo ~]#
[root@cli-demo ~]#
```

Step 7 Run the **blkid** command to obtain the UUID information of the data disks.

Figure 10-6 Obtaining UUIDs of data disks

```
[root@cli-demo ~]# blkid
/dev/vda1: UUID="207b19eb-8170-4983-acb5-9098af381e72" TYPE="ext4"
/dev/vdb: UUID="08e5c568-86ca-40ce-8145-66b3ea53076a" TYPE="ext4"
[root@cli-demo ~]#
```

Step 8 Run the **vi /etc/fstab** command to open the file, press **i** to enter the editing mode, and add the attachment information of all data disks. Then, press **Esc** to exit the editing mode and run **:wq!** to save the change and exit.

Figure 10-7 Adding attachment information of data disks

```
[root@cli-demo ~]# blkid
/dev/vda1: UUID="207b19eb-8170-4983-acb5-9098af381e72" TYPE="ext4"
/dev/vdb: UUID="08e5c568-86ca-40ce-8145-66b3ea53076a" TYPE="ext4"
[root@cli-demo ~]#
[root@cli-demo ~]#
[root@cli-demo ~]# vi /etc/fstab
[root@cli-demo ~]# vi /etc/fstab
[root@cli-demo ~]# cat /etc/fstab

#
# /etc/fstab
# Created by anaconda on Mon Apr 27 13:51:12 2020
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=207b19eb-8170-4983-acb5-9098af381e72 /                    ext4    defaults        1 1
UUID=08e5c568-86ca-40ce-8145-66b3ea53076a /tmp/test            ext4    defaults        1 0
[root@cli-demo ~]#
```

After the information is added, the system will automatically attach the data disks on restart.

----End

11 Failed to Migrate VMware Backups to the Cloud

Symptom

A migration of VMware backups to the cloud fails.

Troubleshooting

Possible causes are listed here in order of their probability.

If the fault persists after you have ruled out one cause, move on to the next one.
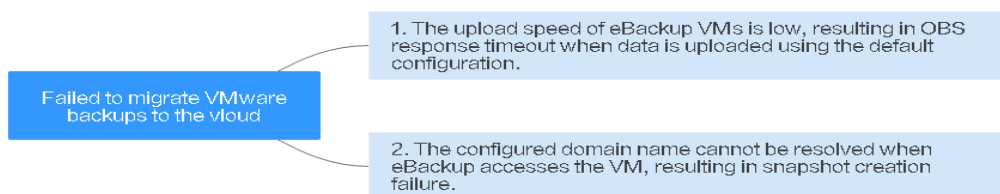
Figure 11-1 Troubleshooting

Table 11-1 Troubleshooting

Possible Cause	Solution
The upload speed of eBackup VMs is low (< 50 MB/s), resulting in OBS response timeout when data is uploaded using the default configuration. "Write data to backup storage failed" is displayed.	For detailed handling measures, see **Upload Speed of eBackup VMs Is Too Low**.

Possible Cause	Solution
The configured domain name cannot be resolved when eBackup accesses the VM, resulting in snapshot creation failure.	In the host file of eBackup, configure a domain name of the vCenter VM that can be resolved.

Upload Speed of eBackup VMs Is Too Low

Step 1 Log in to an eBackup VM as the **hcp** user and switch to the **root** user.

Step 2 Run the following command to edit the **hcpconf.ini** file:

```
vim /opt/huawei-data-protection/ebackup/microservice/ebk_vmware/conf/hcpconf.ini
```

Step 3 Change the values of **ProductStorageMemoryPoolBlockNum** and **CommonTaskUsingMaxThread4Backup** to **2**.

Step 4 Run the **:wq!** command to save and exit the file.

Step 5 Run the **cd /opt/huawei-data-protection/ebackup/microservice/ebk_vmware/ script** command to switch to the directory.

Step 6 Run the **sh ebackup_stop.sh** command. **Figure 11-2** shows the command output.

Figure 11-2 Executing the **sh ebackup_stop.sh** command

Step 7 Run the **sh ebackup_start.sh** command. **Figure 11-3** shows the command output.

Figure 11-3 Executing the **sh ebackup_start.sh** command

Step 8 Upload the VMware backups again and check whether the fault has been rectified. If the fault persists, contact technical support.

----End

Submitting a Service Ticket

If the problem persists, **submit a service ticket**.

12 Failed to Restore a VMware Backup to a Cloud Server

Symptom

When you restore a VMware backup to a cloud server, the restoration task fails.

Possible Cause

The VMware VM has multiple data disks and the data disks belong to the logical volume manager (LVM) group. As a result, an error occurs during the restoration.

Solution

Step 1 Log in to **Network Console** and choose **Access Control** > **Security Groups**.

Step 2 Click **Create Security Group** in the upper right corner to create a security group that does not allow access from any port. See **Figure 12-1**.

Figure 12-1 Creating a security group

Step 3 Switch to **Cloud Server Console** and add the server you want to restore to the security group you created in **Step 2**.

Click the server name. On the **Security Groups** tab page, click **Change Security Group**. See **Figure 12-2**.

Figure 12-2 Changing a security group

Step 4 Log in to the CBR console and choose **Hybrid Cloud Backups** > **VMware Backups**.

Locate the VMware backup you want to use for restoration, click **Restore Data** in the **Operation** column, and select the destination server in **Step 3**. See **Figure 12-3**.

Figure 12-3 Restoring data to another server
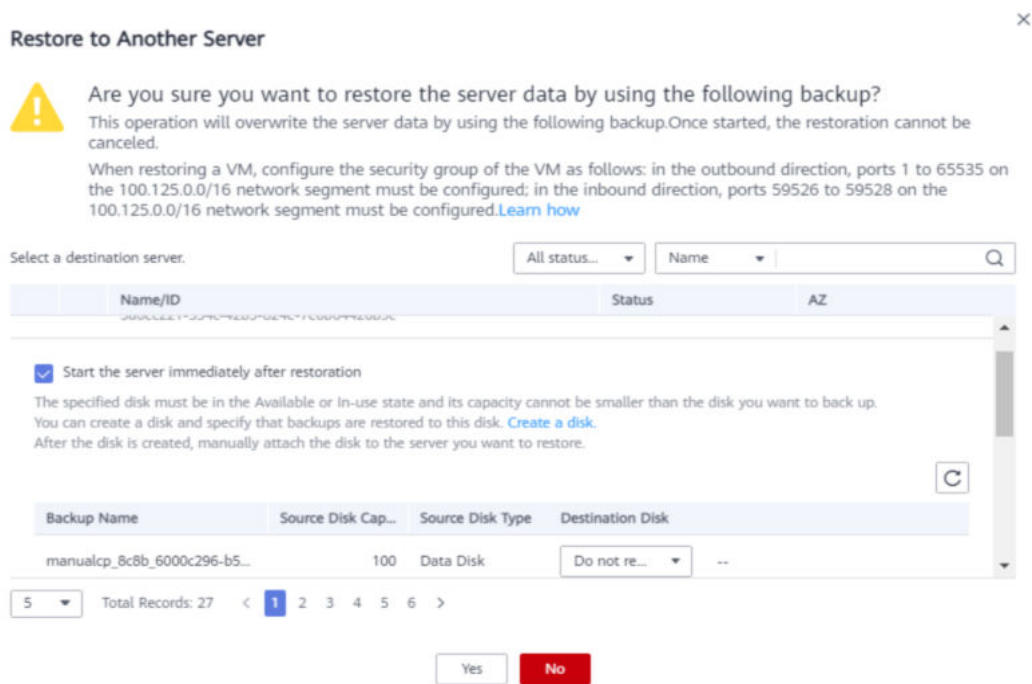
Step 5 On the **Tasks** page, view the restoration progress. When the restoration progress reaches 91%, go to **Cloud Server Console** and attach the new data disk to the server mentioned previously. See **Figure 12-4**.

For details on how to attach disks, see **Attaching a Non-Shared Disk**. After the disk has been attached, initialize the disk.

Figure 12-4 Viewing the task progress
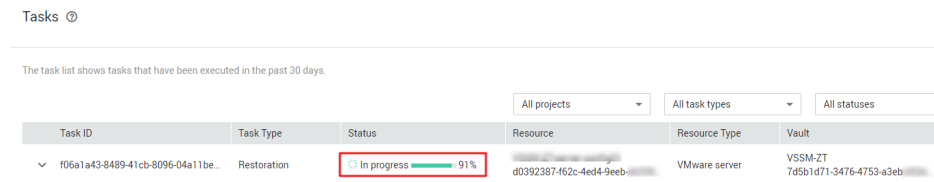

Step 6 Change the security group of the destination server as follows.

In the outbound direction of the security group, configure ports 1 to 65535 on the 100.125.0.0/16 network segment. In the inbound direction, configure ports 59526 to 59528 on the 100.125.0.0/16 network segment.

For details on how to change a security group, see **Changing a Security Group**. See **Figure 12-5**.

Figure 12-5 Allowing access to ports in the security group
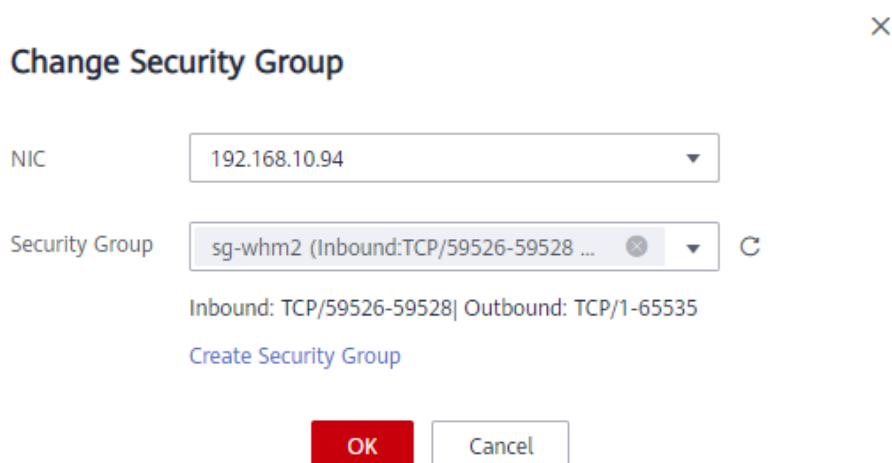
Step 7 Switch back to the **Tasks** page on the CBR console and wait until the restoration is complete.

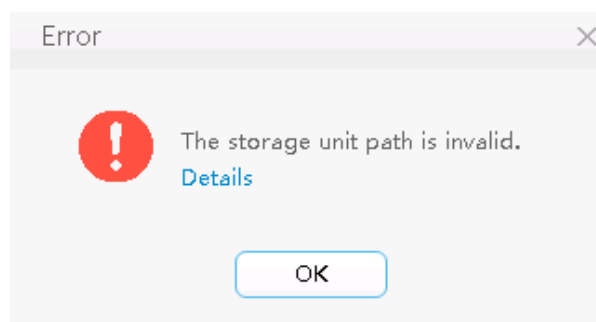After the restoration completes, you can log in to the server to check the restored data.

----End

13 An Error Message Is Displayed Indicating that the Path of a Storage Unit Is Invalid

Symptom

When you create a storage unit on eBackup, the system prompts a message indicating that the path of the storage unit is invalid. See **Figure 13-1**.

Figure 13-1 Error message

Troubleshooting

Possible causes are listed here in order of their probability.

If the fault persists after you have ruled out one cause, move on to the next one.
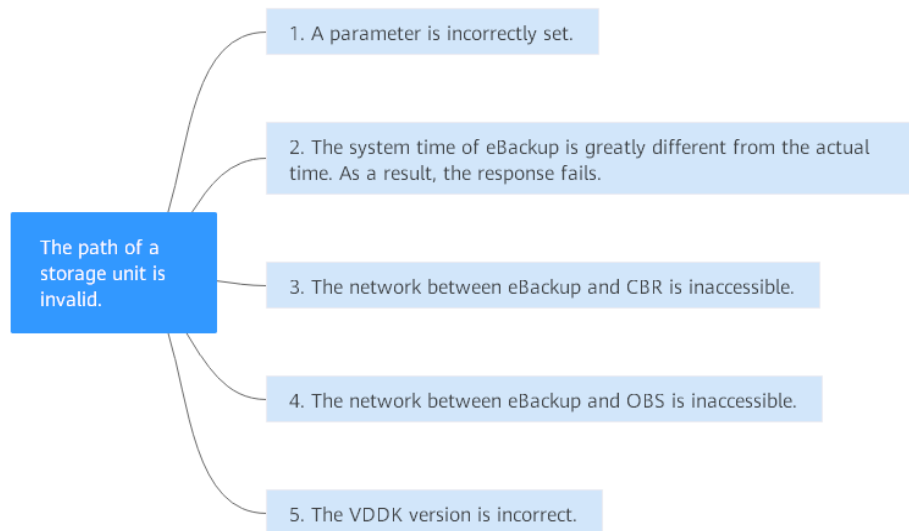
Figure 13-2 Troubleshooting

Table 13-1 Troubleshooting

Possible Cause	Solution
A parameter is incorrectly set.	In the **Create Storage Unit** window on eBackup, check whether the parameters are set correctly. If any parameter values are incorrect, correct them. The AK/SK must be the AK/SK of your account, not of an IAM user.
The system time of eBackup is greatly different from the actual time. As a result, the response fails.	For detailed handling measures, see **The System Time of eBackup Is Greatly Different from the Actual Time**.
The network between eBackup and CBR is inaccessible.	For detailed handling measures, see **The Network Between eBackup and CBR Is Inaccessible**.
The network between eBackup and OBS is inaccessible.	Back up data during off-peak hours or **submit a service ticket**.
The version of the Virtual Disk Development Kit (VDDK) in incorrect.	Use VDDK 6.0.3. You can download the **VMware-vix-disklib-6.0.3-4888596.x86_64.tar.gz** at the VMware official website: https://code.vmware.com/web/sdk/6.0/vddk.

The System Time of eBackup Is Greatly Different from the Actual Time

On the navigation bar of eBackup, choose ⚙ > **System Time & Zone** to check whether the difference between the system time and the actual time is greater than 1 minute.

If yes, change the system time to the actual time. For details, see **Configuring System Time & Zone**.

The Network Between eBackup and CBR Is Inaccessible

Run the **curl -kv https://**_Domain name_**:443** command to ping the endpoint of the region where your CBR service resides. For details about the regions and endpoints, see **Regions and Endpoints**.

- If the endpoint can be pinged but the problem persists, **submit a service ticket**.

- If the endpoint cannot be pinged, check whether the public network has been configured.

  - If the public network has been configured, check whether the domain name resolution is complete by following the instructions in **How Do I Test Whether Record Sets Have Taken Effect?**

    - If the resolution is complete but the problem persists, **submit a service ticket**.

    - If the domain name has not been resolved, configure the correct user DNS, and run **vi /etc/resolv.conf** to edit the **/etc/resolv.conf** file. Add the DNS server IP address above the existing **nameserver** information. The DNS server IP address is 114.114.114.114.

      Figure 13-3 Modifying the DNS

  - If the public network has not been configured, configure it by following instructions in **Planning the Network**.

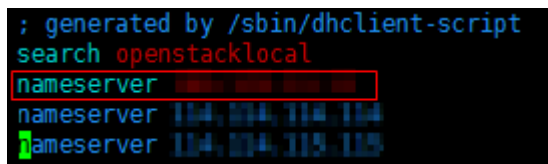## The Network Between eBackup and OBS Is Inaccessible

VMware backups are automatically uploaded to an OBS bucket. If the communication between eBackup and OBS is abnormal, an error will be reported.

Run the **curl -kv https://**_Domain name_**:443** command to ping the endpoint of the region where your OBS service resides. For details about the regions and endpoints, see **Regions and Endpoints**.

- If the endpoint can be pinged but the problem persists, **submit a service ticket**.

- If the endpoint cannot be pinged, check whether the public network has been configured on premises.

– If the public network has been configured, check whether the domain name resolution is complete by following the instructions in **How Do I Test Whether Record Sets Have Taken Effect?**

- If the resolution is complete but the problem persists, **submit a service ticket**.

- If the domain name has not been resolved, configure the correct user DNS, and run **vi /etc/resolv.conf** to edit the **/etc/resolv.conf** file. Add the DNS server IP address above the existing **nameserver** information. The DNS server IP address is 114.114.114.114.

Figure 13-4 Modifying the DNS

– If the public network has not been configured, configure it by following instructions in **Planning the Network**.

Submitting a Service Ticket

If the problem persists, **submit a service ticket**.

Cloud Backup and Recovery
Troubleshooting

14 Failed to Import an eBackup Image Template,
with an Error Displayed Indicating That the File Is
Invalid

14 Failed to Import an eBackup Image Template, with an Error Displayed Indicating That the File Is Invalid

Symptom

When you import an eBackup image template during local eBackup installation, the following information is displayed: **the following manifest file entry (line 1) is invalid: sha256 vmdk**

Possible Cause

The VMware VM does not support the SHA256 hashing algorithm.

Solution

Step 1 Visit **https://developer.vmware.com/home**, download the VMware OVF Tool, and install it.

Step 2 Run the following command to convert the eBackup installation package:

```
ovftool.exe --shaAlgorithm=SHA1 /path/to/the/original/ebackup_xxxx.ovf /path/to/the/new/ova/ebackup-SHA1.ovf
```

☐ **NOTE**

For details, see **https://kb.vmware.com/s/article/2151537**.

Step 3 After the conversion is complete, install eBackup again.

----End

15 The Download Dialog Box Disappears When I Download eBackup on a VMware VM

Symptom

When Google Chrome is used to download the eBackup image template on a VMware VM, the download dialog box blinks and then disappears before the eBackup image template is downloaded.

Possible Cause
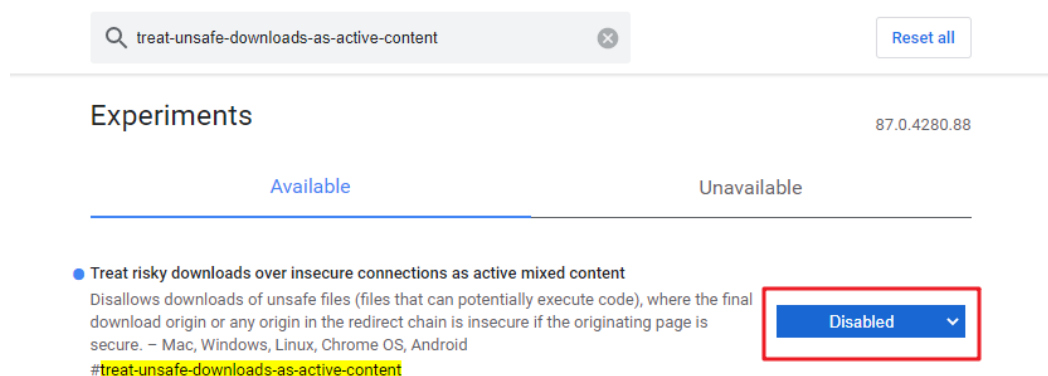
The Chrome settings are incorrect and need to be modified.

Solution

Step 1 Enter **chrome://flags/** in the address box of Google Chrome and press **Enter**.

Step 2 Enter **treat-unsafe-downloads-as-active-content** in the search box.

Step 3 In the search result area, change **Default** to **Disabled**. See **Figure 15-1**.

Figure 15-1 Changing Chrome settings

Step 4 Restart Google Chrome and download the eBackup image template.

----End

16 File Backup Failed Due to Inconsistent Time Between Backup Client and UTC Time

Symptom

During file backup, the time on the backup client was inconsistent with the UTC time, resulting in file backup failure.

Possible Cause

The inconsistent time causes the calibration failure and then file backup failure. The client's NTP information need to be modified.

Solution

Configure the client's NTP information by referring to **How Can I Configure the NTP and DNS Servers for an ECS?**