Cloud Server Backup Service

User Guide

Issue	04
Date	2019-02-23

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

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

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

Contents

1 Permissions Management

1.1 Creating a User and Granting CSBS Permissions

This section describes how to use IAM to implement fine-grained permissions control for your CSBS resources. With IAM, you can:

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing CSBS resources.
- Grant only the permissions required for users to perform a special task.
- Entrust a HUAWEI CLOUD account or cloud service to perform efficient O&M on your CSBS resources.

If your HUAWEI CLOUD account does not require individual IAM users, skip this section.

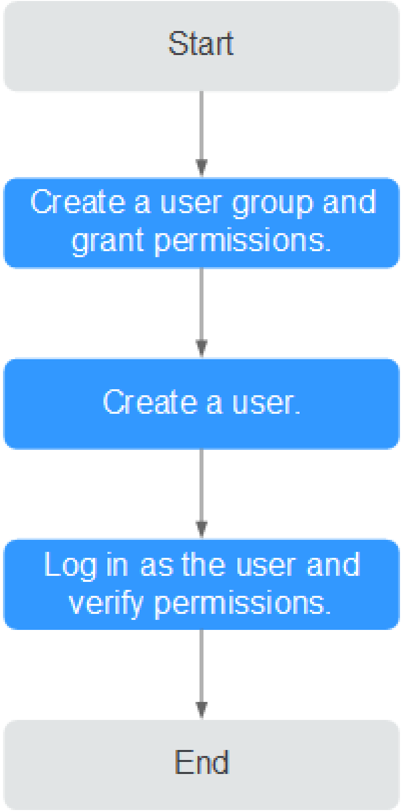
This section describes the procedure for granting permissions (see **Figure 1-1**).

Prerequisites

Learn about the permissions (see **CSBS Permissions**) supported by CSBS and choose policies or roles according to your requirements. For the permissions of other services, see **System Permissions**.

Process Flow

Figure 1-1 Process of granting CSBS permissions


Start
Create a user group and grant permissions.
Create a user.
Log in as the user and verify permissions.
End

1. **Create a user group and assign permissions** to it.

   Create a user group on the IAM console, and attach the **CSBS Administrator** policy to the group.

2. **Create an IAM user**.

   Create a user on the IAM console and add the user to the group created in **1**.

3. **Log in** and verify permissions.

   Log in to the CSBS console by using the user created in **2**, and verify that the user only has read permissions for CSBS.

   – Choose **Service List** > **Cloud Server Backup Service**. Then click **Create CSBS Backup** on the CSBS console. If a CSBS backup is successfully created, the **CSBS Administrator** policy has already taken effect.

   – Choose any other service in the **Service List**. If a message appears indicating that you have insufficient permissions to access the service, the **CSBS Administrator** policy has already taken effect.

2 Backup

2.1 Viewing a Backup

After a backup job is delivered or completed, you can set search criteria to filter backups from the backup list and view backup details.

Prerequisites

A backup job has been created.

View Backup Details

Step 1 Log in to the CSBS management console.

1. Log in to the management console.
2. Under Storage > **Cloud Server Backup Service**.

Step 2 Click the **Backups** tab. Search for backups by filtering conditions.

- You can search for backups by selecting a state from the **All statuses** drop-down list in the upper right corner of the backup list.

  Table 2-1 describes each state.

Table 2-1 State description

State	State Attribute	Description
All statuses	--	All statuses of backups.
Available	A stable state	A stable state of a backup after the backup is created This state allows various operations.

State	State Attribute	Description
Creating	An intermediate state	An intermediate state of a backup from the start of a backup job to the completion of the backup job. In this state, a progress bar is displayed indicating the backup progress. If the progress bar remains unchanged for a long time, an exception has occurred. Contact customer service for support.
Restoring	An intermediate state	An intermediate state when using the backup to restore data. In this state, a progress bar is displayed indicating the restoration progress. If the progress bar remains unchanged for a long time, an exception has occurred. Contact customer service for support.
Deleting	An intermediate state	An intermediate state from the start of deleting the backup to the completion of deleting the backup. In this state, a progress bar is displayed indicating the deletion progress. If the progress bar remains unchanged for a long time, an exception has occurred. Contact customer service for support.
Error	A stable state	A backup enters the **Error** state when an exception occurs when the backup is being used. A backup in this state cannot be used for backup or restoration, and must be deleted manually. If manual deletion fails, contact customer service for support.

- You can search for backups by selecting a time segment displayed in the upper right corner of the backup list.
- You can search for backups by server name, server ID, backup name, or backup ID. Click 🔍 to search for target backups.

  For a backup created via a successful application-consistent backup job, its name in the **Backups** tab page is marked with A.

Step 3 Click ˅ on the left of a backup name to view details about the backup.

----End

View Backup Space Usage

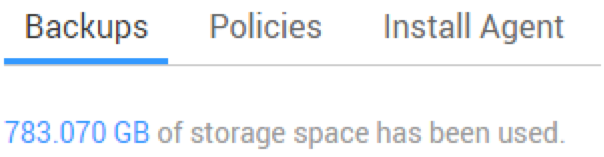
Step 1 Log in to the CSBS management console.

1. Log in to the management console.

2. Under Storage > **Cloud Server Backup Service**.

Step 2 Click the **Backups** tab and then the number indicating the used storage space in the backup overview. **Figure 2-1** provides an example.

Figure 2-1 Backup overview

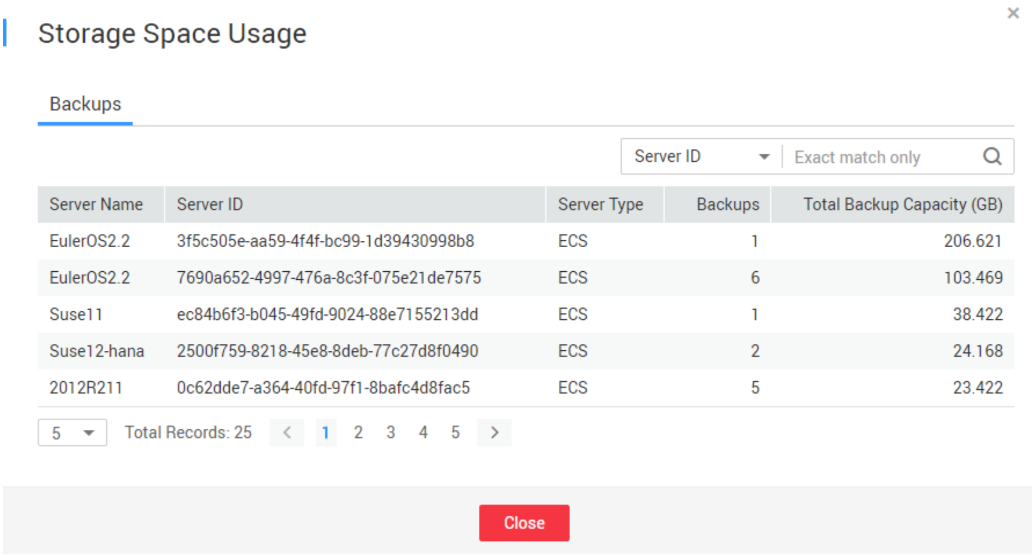


783.070 GB of storage space has been used.

Step 3 In the displayed dialog box, view the storage space usage.

Backups specifies the number of backups created for an ECS and **Total Backup Capacity (GB)** specifies the capacity used by the ECS's backups in total.

Figure 2-2 Storage space usage



Server Name	Server ID	Server Type	Backups	Total Backup Capacity (GB)
EulerOS2.2	3f5c505e-aa59-4f4f-bc99-1d39430998b8	ECS	1	206.621
EulerOS2.2	7690a652-4997-476a-8c3f-075e21de7575	ECS	6	103.469
Suse11	ec84b6f3-b045-49fd-9024-88e7155213dd	ECS	1	38.422
Suse12-hana	2500f759-8218-45e8-8deb-77c27d8f0490	ECS	2	24.168
2012R211	0c62dde7-a364-40fd-97f1-8bafc4d8fac5	ECS	5	23.422

Total Records: 25 < 1 2 3 4 5 >

----End

2.2 Deleting a Backup

You can delete unwanted backups to reduce space usage and costs.

Context

CSBS supports manual deletion of backups and automatic deletion of expired backups. The latter deletion method is implemented using the backup retention rule in the backup policy. For details, see **Creating a Backup Policy**.

Prerequisites

- At least one backup exists in CSBS.

- The backups are in the **Available** or **Error** state.

Procedure

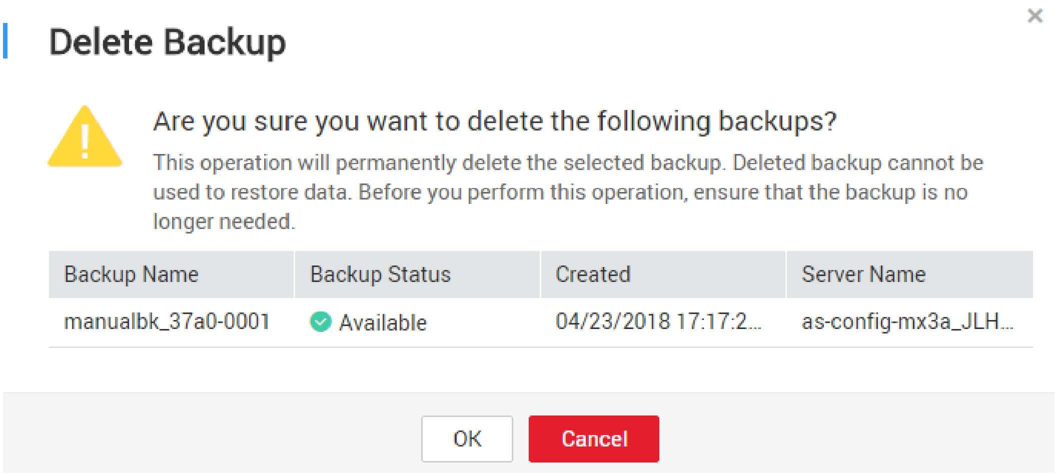
Step 1 Log in to the CSBS management console.

1. Log in to the management console.
2. Under Storage > **Cloud Server Backup Service**.

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

Step 3 In the row of the backup, click **More** > **Delete**. See **Figure 2-3**. Alternatively, select the backups you want to delete and click **Delete** in the upper left corner to delete them in a batch.

Figure 2-3 Deleting a backup



Delete Backup

Are you sure you want to delete the following backups?

This operation will permanently delete the selected backup. Deleted backup cannot be used to restore data. Before you perform this operation, ensure that the backup is no longer needed.

Backup Name	Backup Status	Created	Server Name
manualbk_37a0-0001	✓ Available	04/23/2018 17:17:2...	as-config-mx3a_JLH...

Step 4 Click **Yes**.

----End

2.3 Using Backups to Create Images

CSBS allows you to create images using ECS backups. You can use the images to provision ECSs for fast restoring the service running environment.

Prerequisites

- The following operations have been performed before you use an ECS's backup to create an image:
  - You have optimized the Linux ECS (referring to **(Optional) Optimizing a Linux Private Image**) and installed Cloud-Init (referring to **Installing Cloud-Init**).
  - You have optimized the Windows ECS (referring to **(Optional) Optimizing a Windows Private Image**) and installed Cloudbase-Init (referring to **Installing Cloudbase-Init**).
- The backup you want to use to create an image meets either of the following two conditions:

- The backup is in the **Available** state.
- The backup is in the **Creating** state which is marked with **Image can be created**.

NOTE

Once a backup creation starts, the backup enters the **Creating** state. After a while, a message stating "Image can be created" is displayed under **Creating**. In this case, the backup can be used for creating an image, even though it is still being created and cannot be used for restoration.

- The backup you want to use to create an image contains the system disk data.

Description

- Images created from a backup are the same, so CSBS allows you to use a backup to create only one full-ECS image that contains the whole data of the ECS's system disk and data disks, in order to save the image quota. After an image is created, you can use the image to provision multiple ECSs in a batch.
- A backup with an image created cannot be deleted manually or automatically. If you want to delete such a backup, delete its image first. If a backup is automatically generated based on a backup policy and the backup has been used to create an image, the backup will not be counted as a retained backup and will not be deleted automatically.

Procedure

Step 1 Log in to the CSBS management console.

1. Log in to the management console.
2. Under Storage > **Cloud Server Backup Service**.

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

Step 3 In the row of the backup, click **Create Image**.

Step 4 Create an image by referring to **Creating a Full-ECS Image Using a CSBS Backup**.

Step 5 If you want to use an image to provision ECSs, see **Creating ECSs Using an Image**.

----End

2.4 Enabling Application-Consistent Backup

2.4.1 Changing a Security Group

Context

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. Users can also create custom security groups by themselves.

When creating a security group, you need to add the inbound and outbound access rules and enable the ports required for application-consistent backup to prevent application-consistent backup failures.

Description

Before using the application-consistent backup function, you need to change the security group. To ensure network security, CSBS 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.

Procedure

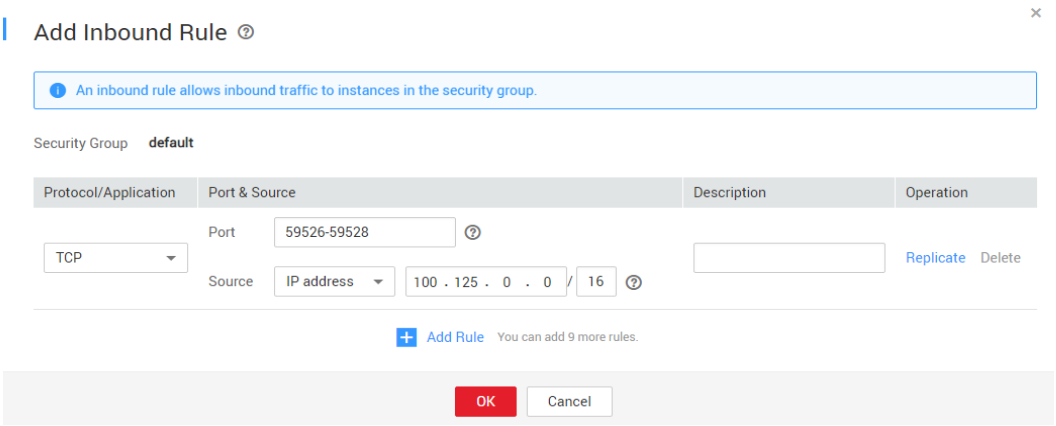
Step 1 Access the cloud server console.

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

Step 3 Click the **Security Group** tab and select the target security group. Click **Modify Security Group Rule** for an elastic cloud server on the right of the ECS page. Click **Change Security Group** for a bare metal server. In the dialog box displayed, click **Manage Security Group**.

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 2-4**. 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 2-4 Adding an inbound rule



Add Inbound Rule ⓘ ×

An inbound rule allows inbound traffic to instances in the security group.

Security Group **default**

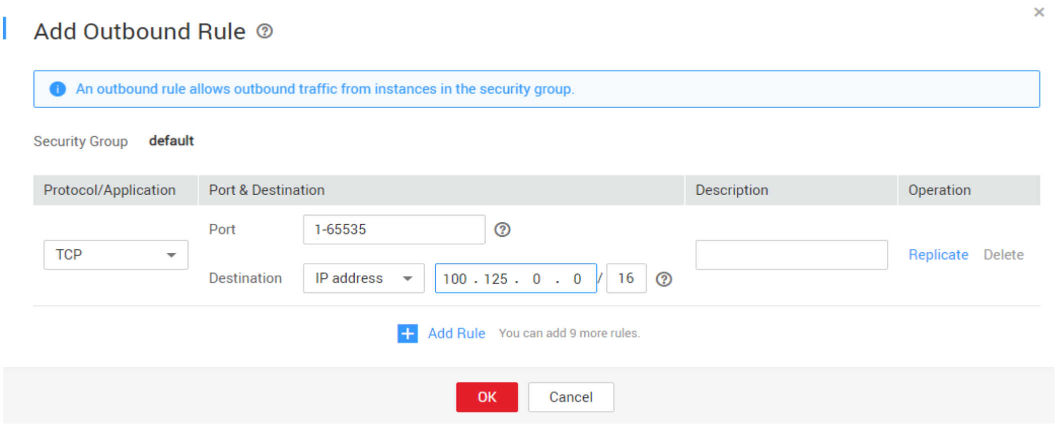
Protocol/Application	Port & Source	Description	Operation
TCP	Port 59526-59528 Source IP address 100 . 125 . 0 . 0 / 16		Replicate Delete

Add Rule You can add 9 more rules.

OK Cancel

Step 5 Click the **Outbound Rules** tab, and then click **Add Rule**. The **Add Outbound Rule** dialog box is displayed, as shown in **Figure 2-4**. Select **TCP** for **Protocol/ Application**, enter **1-65535** 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 outbound rule.

Figure 2-5 Adding an outbound rule



Add Outbound Rule ⓘ ×

An outbound rule allows outbound traffic from instances in the security group.

Security Group **default**

Protocol/Application	Port & Destination	Description	Operation
TCP	Port 1-65535 Destination IP address 100 . 125 . 0 . 0 / 16		Replicate Delete

Add Rule You can add 9 more rules.

OK Cancel

----End

2.4.2 Installing the Agent

Context

There are three types of backup consistency:

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

- Application-consistent backup backs up files and disks at the same point in time, including memory data, to ensure application system consistency.

Description

- Before enabling application-consistent backup, change the security group and install the Agent on your ECSs. This section guides you to download and install the Agent.
- During the Agent installation, the system requires the **rdadmin** user's permissions to run the installation program. For O&M security purposes, change the user **rdadmin**'s password of the Agent OS regularly and disable this user's remote login permission.
- **Table 2-2** lists OSs that support installation of the Agent.

Table 2-2 OSs that support installation of the Agent

Database	OS	Supported Version
SQLServer 2008/2012	Windows	Windows Server 2008, 2008 r2, 2012 , 2012 r2 for x86_64
SQLServer 2014/2016/ EE	Windows	Windows Server 2012, 2012 r2, 2016 Datacenter for x86_64
MySQL 5.5/5.6/5.7	Red Hat	Red Hat Enterprise Linux 6, 7 for x86_64
	SUSE	SUSE Linux Enterprise Server 11, 12 for x86_64
	CentOS	CentOS 6, 7 for x86_64
	Euler	EulerOS 2.2 and 2.3 for x86_64
HANA 1.0/2.0	SUSE	SUSE Linux Enterprise Server 12 for x86_64

NOTICE

To install the Agent, the system will open the firewall of a port from 59526 to 59528 of the ECS. When port 59526 is occupied, the firewall of port 59527 is enabled, and so on.

Prerequisites

- You have obtained a username and its password for logging in to the management console.
- The security group has been configured.
- The **Agent Status** of the ECS is **Not installed**.
- If you use Internet Explorer, you need to add the websites you will use to trusted sites.

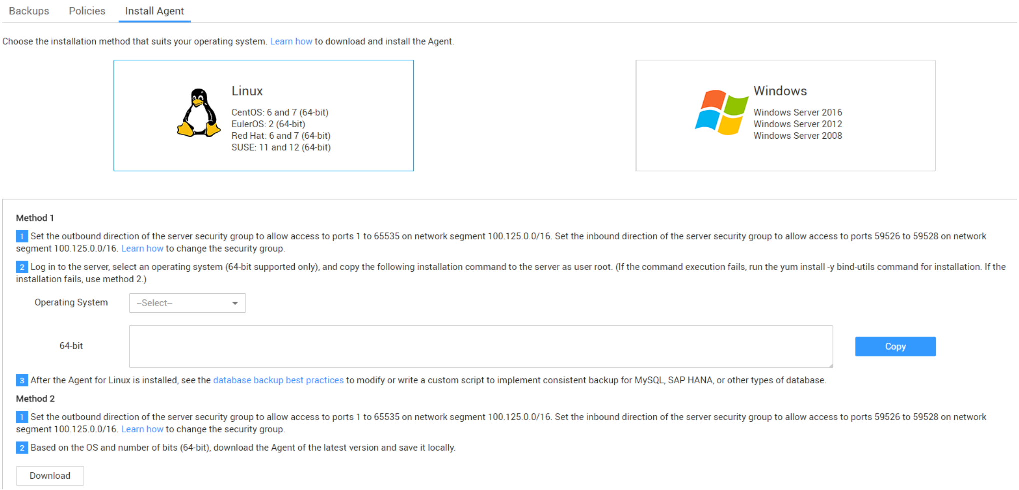
Installing the Agent for Linux (Method 1)

Step 1 Log in to the CSBS management console.

1. Log in to the management console.
2. Under Storage > **Cloud Server Backup Service**.

Step 2 Click the **Install Agent** tab to go to the **Install Agent** tab page.

Figure 2-6 Installation screen



Choose the installation method that suits your operating system. Learn how to download and install the Agent.

Linux
CentOS: 6 and 7 (64-bit)
EulerOS: 2 (64-bit)
Red Hat: 6 and 7 (64-bit)
SUSE: 11 and 12 (64-bit)

Windows
Windows Server 2016
Windows Server 2012
Windows Server 2008

Method 1

1 Set the outbound direction of the server security group to allow access to ports 1 to 65535 on network segment 100.125.0.0/16. Set the inbound direction of the server security group to allow access to ports 59526 to 59528 on network segment 100.125.0.0/16. Learn how to change the security group.

2 Log in to the server, select an operating system (64-bit supported only), and copy the following installation command to the server as user root. (If the command execution fails, run the yum install -y bind-utils command for installation. If the installation fails, use method 2.)

Operating System --Select--

64-bit

3 After the Agent for Linux is installed, see the database backup best practices to modify or write a custom script to implement consistent backup for MySQL, SAP HANA, or other types of database.

Method 2

1 Set the outbound direction of the server security group to allow access to ports 1 to 65535 on network segment 100.125.0.0/16. Set the inbound direction of the server security group to allow access to ports 59526 to 59528 on network segment 100.125.0.0/16. Learn how to change the security group.

2 Based on the OS and number of bits (64-bit), download the Agent of the latest version and save it locally.

Step 3 In method 1, select the corresponding Agent version as required, and copy the installation command in step 2.

Step 4 On the ECS page, select the target server and click **Remote Login** in the **Operation** column to log in to the ECS.

Step 5 Paste the installation command in step 2 to the server and run the command as the **root** user. If the execution fails, run the **yum install -y bind-utils** command to install the dig module.

Step 6 Finish the installation as instructed. If the installation fails, use method 2.

Step 7 After the Agent for Linux is installed, see the best practices of application-consistent backup to modify or write a custom script to implement consistent backup for MySQL, SAP HANA, or other database types.

----End

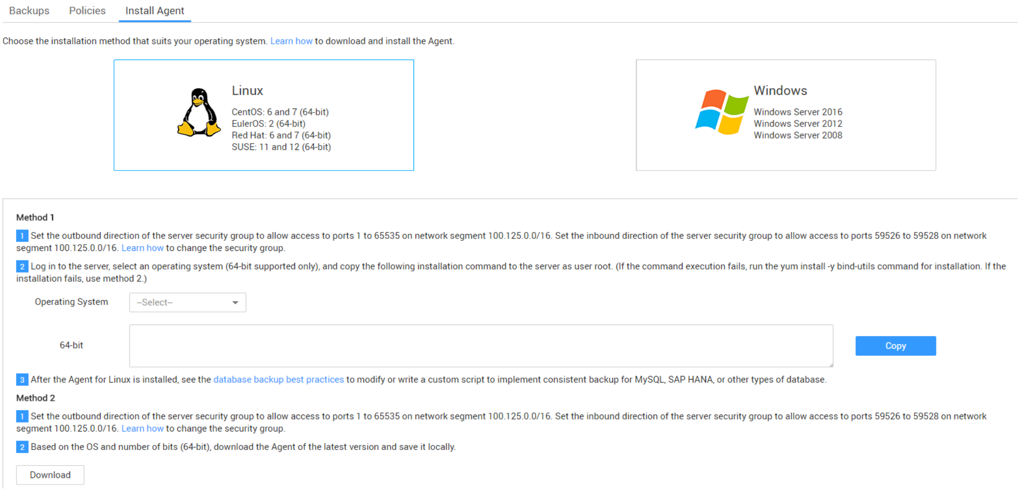
Installing the Agent for Linux (Method 2)

Step 1 Log in to the CSBS management console.

1. Log in to the management console.
2. Under Storage > **Cloud Server Backup Service**.

Step 2 Click the **Install Agent** tab to go to the **Install Agent** tab page.

Figure 2-7 Installation screen



Choose the installation method that suits your operating system. Learn how to download and install the Agent.

Linux

CentOS: 6 and 7 (64-bit)
EulerOS: 2 (64-bit)
Red Hat: 6 and 7 (64-bit)
SUSE: 11 and 12 (64-bit)

Windows

Windows Server 2016
Windows Server 2012
Windows Server 2008

Method 1

1 Set the outbound direction of the server security group to allow access to ports 1 to 65535 on network segment 100.125.0.0/16. Set the inbound direction of the server security group to allow access to ports 59526 to 59528 on network segment 100.125.0.0/16. Learn how to change the security group.

2 Log in to the server, select an operating system (64-bit supported only), and copy the following installation command to the server as user root. (If the command execution fails, run the yum install -y bind-utils command for installation. If the installation fails, use method 2.)

Operating System: --Select--

64-bit

3 After the Agent for Linux is installed, see the database backup best practices to modify or write a custom script to implement consistent backup for MySQL, SAP HANA, or other types of database.

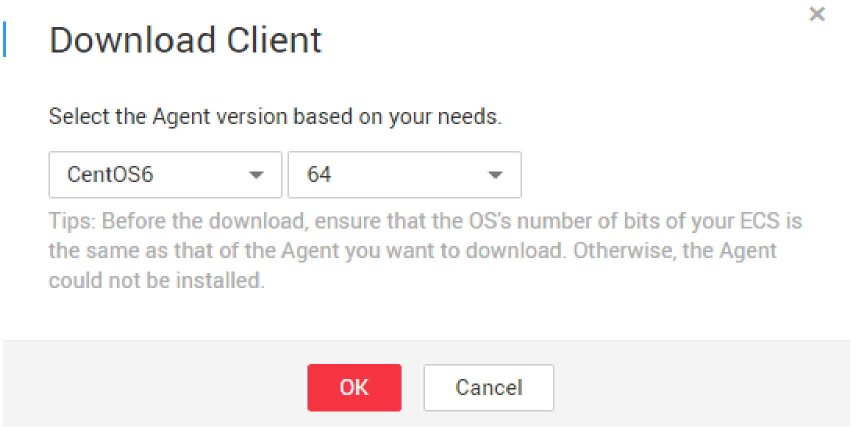
Method 2

1 Set the outbound direction of the server security group to allow access to ports 1 to 65535 on network segment 100.125.0.0/16. Set the inbound direction of the server security group to allow access to ports 59526 to 59528 on network segment 100.125.0.0/16. Learn how to change the security group.

2 Based on the OS and number of bits (64-bit), download the Agent of the latest version and save it locally.

Step 3 In method 2, click **Download**. In the dialog box, select the version to be downloaded based on the operating system type of the target ECS, and click **OK**. See **Figure 2-8**.

Figure 2-8 Downloading the Agent



Download Client

Select the Agent version based on your needs.

CentOS6 ▾ 64 ▾

Tips: Before the download, ensure that the OS's number of bits of your ECS is the same as that of the Agent you want to download. Otherwise, the Agent could not be installed.

Step 4 Use a file transfer tool, such as Xftp, SecureFX, or WinSCP, to upload the Agent installation package to your ECS.

Step 5 After the upload, go to the ECS page. Select the target server and click **Remote Login** in the **Operation** column to log in to the ECS.

Step 6 Run the **tar -zxvf** command to decompress the Agent installation package to any directory and run the following command to go to the **bin** directory:

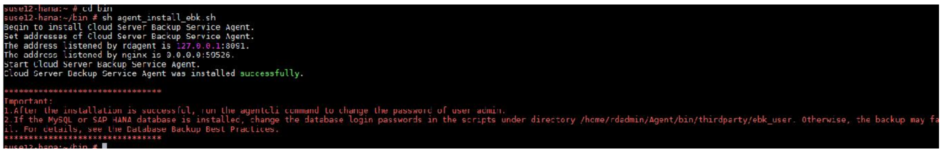
cd *storage directory of the installation package*

Step 7 Run the following command to run the installation script:

sh agent_install_ebk.sh

Step 8 The system displays a message indicating that the client is installed successfully. See **Figure 2-9**.

Figure 2-9 Successful client installation



```
suse12-hana:~ # cd bin
suse12-hana:~/bin # sh agent_install_ebk.sh
Begin to install Cloud Server Backup Service Agent.
Set addresses of Cloud Server Backup Service Agent.
The address listened by rdagent is 127.0.0.1:8091.
The address listened by nginx is 0.0.0.0:59526.
Start Cloud Server Backup Service Agent.
Cloud Server Backup Service Agent was installed successfully.

********************************
Important:
1.After the installation is successful, run the agentcli command to change the password of user admin.
2.If the MySQL or SAP HANA database is installed, change the database login passwords in the scripts under directory /home/rdadmin/Agent/bin/thirdparty/ebk_user. Otherwise, the backup may fa
il. For details, see the Database Backup Best Practices.
********************************
suse12-hana:~/bin #
```

Step 9 If the MySQL or SAP HANA database has been installed on the ECS, run the following command to encrypt the password for logging in to the MySQL or SAP HANA database:

/home/rdadmin/Agent/bin/agentcli encpwd

Step 10 Use the encrypted password in **step 9** to replace the database login password in the script in **/home/rdadmin/Agent/bin/thirdparty/ebk_user/**.

Step 11 After the Agent for Linux is installed, see the *Database Backup Best Practice* to modify or write a custom script to implement consistent backup for MySQL, SAP HANA, or other types of database.

----End

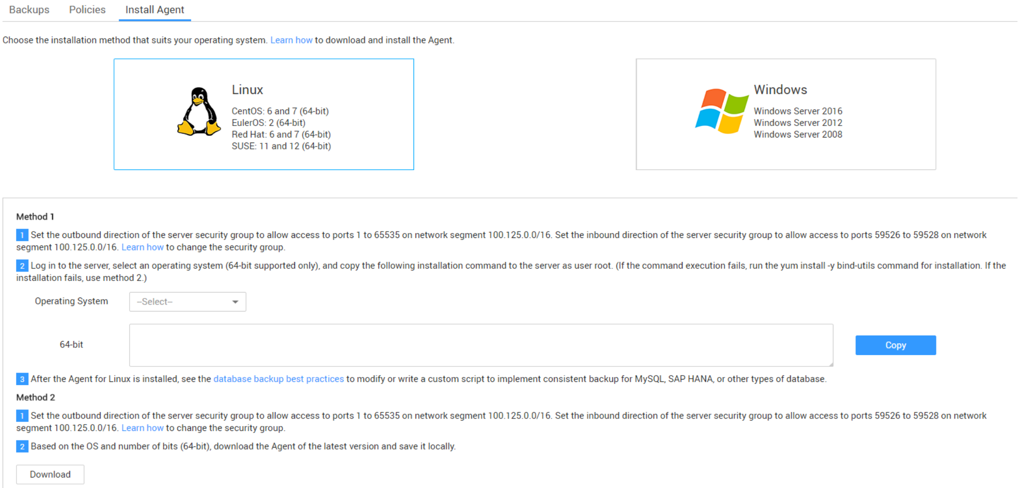
Installing the Agent for Windows (Method 1)

Step 1 Log in to the CSBS management console.

1. Log in to the management console.
2. Under Storage > **Cloud Server Backup Service**.

Step 2 Click the **Install Agent** tab to go to the **Install Agent** tab page.

Figure 2-10 Installation screen



Choose the installation method that suits your operating system. Learn how to download and install the Agent.

Linux
CentOS: 6 and 7 (64-bit)
EulerOS: 2 (64-bit)
Red Hat: 6 and 7 (64-bit)
SUSE: 11 and 12 (64-bit)

Windows
Windows Server 2016
Windows Server 2012
Windows Server 2008

Method 1

1 Set the outbound direction of the server security group to allow access to ports 1 to 65535 on network segment 100.125.0.0/16. Set the inbound direction of the server security group to allow access to ports 59526 to 59528 on network segment 100.125.0.0/16. Learn how to change the security group.

2 Log in to the server, select an operating system (64-bit supported only), and copy the following installation command to the server as user root. (If the command execution fails, run the yum install -y bind-utils command for installation. If the installation fails, use method 2.)

Operating System: --Select--

64-bit:

3 After the Agent for Linux is installed, see the database backup best practices to modify or write a custom script to implement consistent backup for MySQL, SAP HANA, or other types of database.

Method 2

1 Set the outbound direction of the server security group to allow access to ports 1 to 65535 on network segment 100.125.0.0/16. Set the inbound direction of the server security group to allow access to ports 59526 to 59528 on network segment 100.125.0.0/16. Learn how to change the security group.

2 Based on the OS and number of bits (64-bit), download the Agent of the latest version and save it locally.

Step 3 In method 2, click **Download**. Save the downloaded installation package to a local directory.

Step 4 Use a file transfer tool, such as Xftp, SecureFX, or WinSCP, to upload the Agent installation package to your ECS.

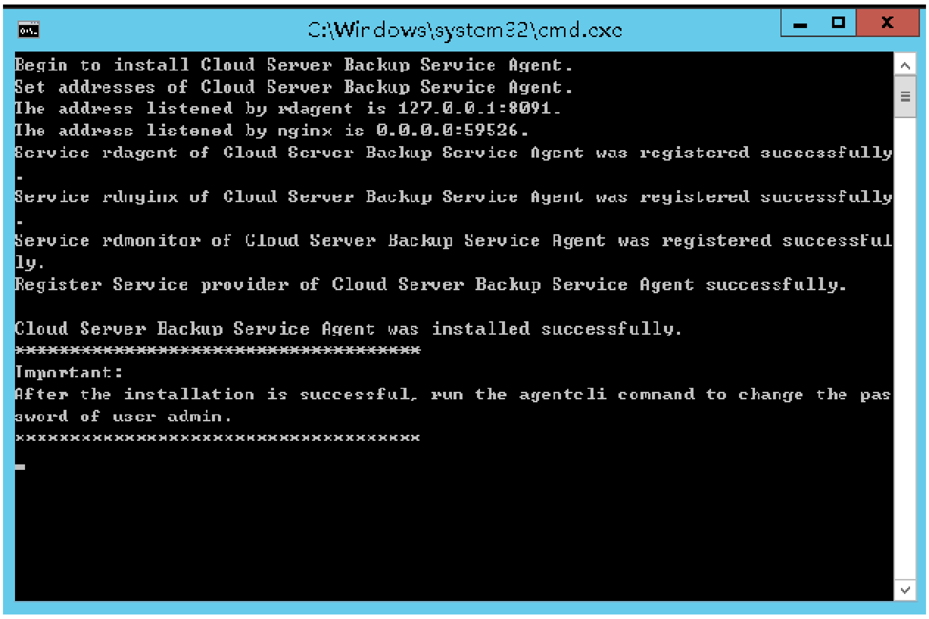
Step 5 Log in to the ECS console and then log in to the ECS as the administrator.

Step 6 Decompress the installation package to any directory and go to the *Installation path***\bin** directory.

Step 7 Double-click the **agent_install_ebk.bat** script to start the installation.

Step 8 The system displays a message indicating that the client is installed successfully. See **Figure 2-11**.

Figure 2-11 Successful client installation



```
Begin to install Cloud Server Backup Service Agent.
Set addresses of Cloud Server Backup Service Agent.
The address listened by rdagent is 127.0.0.1:8091.
The address listened by nginx is 0.0.0.0:59526.
Service rdagent of Cloud Server Backup Service Agent was registered successfully
.
Service rdnginx of Cloud Server Backup Service Agent was registered successfully
.
Service rdmonitor of Cloud Server Backup Service Agent was registered successful
ly.
Register Service provider of Cloud Server Backup Service Agent successfully.

Cloud Server Backup Service Agent was installed successfully.
*************************************
Important:
After the installation is successful, run the agentcli command to change the pas
sword of user admin.
*************************************
_
```

----End

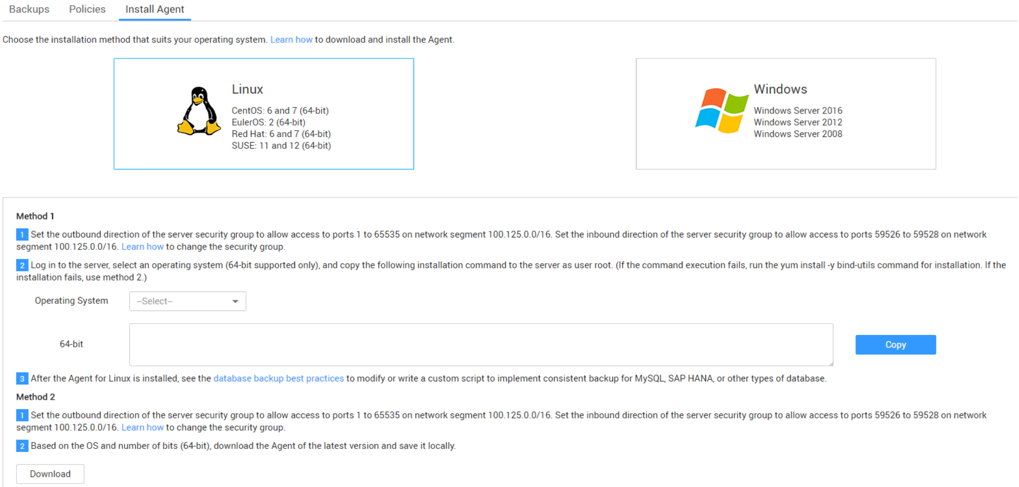
Installing the Agent for Windows (Method 2)

Step 1 Log in to the CSBS management console.

1. Log in to the management console.
2. Under Storage > **Cloud Server Backup Service**.

Step 2 Click the **Install Agent** tab to go to the **Install Agent** tab page.

Figure 2-12 Installation screen



Choose the installation method that suits your operating system. Learn how to download and install the Agent.

Linux
CentOS: 6 and 7 (64-bit)
EulerOS: 2 (64-bit)
Red Hat: 6 and 7 (64-bit)
SUSE: 11 and 12 (64-bit)

Windows
Windows Server 2016
Windows Server 2012
Windows Server 2008

Method 1

1 Set the outbound direction of the server security group to allow access to ports 1 to 65535 on network segment 100.125.0.0/16. Set the inbound direction of the server security group to allow access to ports 59526 to 59528 on network segment 100.125.0.0/16. Learn how to change the security group.

2 Log in to the server, select an operating system (64-bit supported only), and copy the following installation command to the server as user root. (If the command execution fails, run the yum install -y bind-utils command for installation. If the installation fails, use method 2.)

Operating System: --Select--

64-bit

3 After the Agent for Linux is installed, see the database backup best practices to modify or write a custom script to implement consistent backup for MySQL, SAP HANA, or other types of database.

Method 2

1 Set the outbound direction of the server security group to allow access to ports 1 to 65535 on network segment 100.125.0.0/16. Set the inbound direction of the server security group to allow access to ports 59526 to 59528 on network segment 100.125.0.0/16. Learn how to change the security group.

2 Based on the OS and number of bits (64-bit), download the Agent of the latest version and save it locally.

Step 3 On the ECS page, select the target server and click **Remote Login** in the **Operation** column to log in to the ECS as the administrator.

Step 4 Copy the installation commands in step 2 of method 2 to the server and run the command in the CMD window.

Step 5 Copy any IP address in the response name, paste it in the address box of the browser, and replace **0.0.0.0** in the following address with the address. Replace **cn-north-1** with the actual region. The following command uses North China as an example. Then, press **Enter** in the browser to download the installation package.

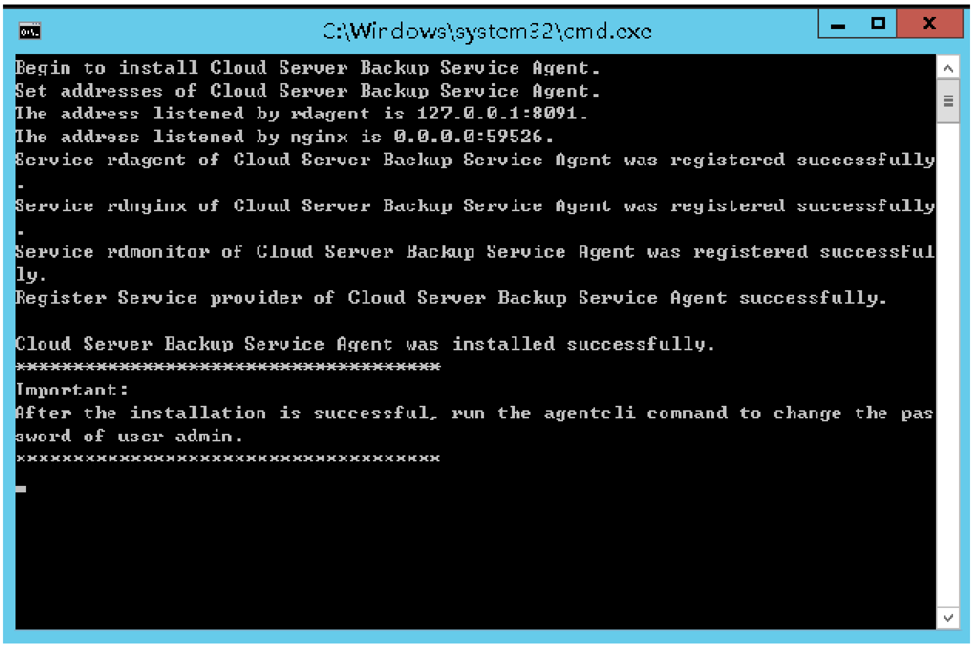
http://*0.0.0.0*/csbs-agent-*cn-north-1*/Cloud Server Backup Agent-WIN64.zip

Step 6 Decompress the file to obtain the installation file. Decompress the installation package to any directory and go to the *Installation path***\bin** directory.

Step 7 Double-click the **agent_install_ebk.bat** script to start the installation.

Step 8 The system displays a message indicating that the client is installed successfully. See **Figure 2-13**.

Figure 2-13 Successful client installation



```
Begin to install Cloud Server Backup Service Agent.
Set addresses of Cloud Server Backup Service Agent.
The address listened by rdagent is 127.0.0.1:8091.
The address listened by nginx is 0.0.0.0:59526.
Service rdagent of Cloud Server Backup Service Agent was registered successfully
.
Service rdnginx of Cloud Server Backup Service Agent was registered successfully
.
Service rdmonitor of Cloud Server Backup Service Agent was registered successful
ly.
Register Service provider of Cloud Server Backup Service Agent successfully.

Cloud Server Backup Service Agent was installed successfully.
*************************************
Important:
After the installation is successful, run the agentcli comnand to change the pas
sword of user admin.
*************************************
```

----End

2.4.3 Creating an Application-Consistent Backup

CSBS supports crash-consistent backup and application-consistent backup. Application-consistent backup ensures the consistency of applications between the file/disk data and the backup data. This backup mode suits scenarios such as backing up ECSs with MySQL or SAP HANA databases.

On CSBS Console, application-consistent backups can be created using any of the following methods:

- Manual backup: When creating a cloud server backup, you can manually perform application-consistent backup at a time.

- Automatic backup: Enable application-consistent backup in the backup policy to periodically create application-consistent backups.
- Executing a backup policy: Select a backup policy where application-consistent backup is enabled and manually perform the backup operation.

This section describes how to create an application-consistent backup using the first method. For details about how to use the second and third methods, see **Creating a Backup Policy** and **Executing a Backup Policy at Once** respectively.

NOTE

The following constraints and restrictions apply to the three methods.

Constraints and Limitations

- Application-consistent backup for clusters, for example, MySQL clusters, is not supported. Application-consistent backup is supported only for a single server.
- You are advised to perform application-consistent backup in off-peak hours.
- Application-consistent backup for bare metal servers is supported.

Procedure

Step 1 Log in to the CSBS management console.

1. Log in to the management console.
2. Under Storage > **Cloud Server Backup Service**.

Step 2 In the upper right corner of the page, click **Create CSBS Backup**.

Step 3 In the server list, select the servers you want to back up. After servers are selected, they are added to the list of selected servers.

Step 4 In the **Configure Backup** area, configure a backup scheme for the selected ECSs and then select **Back Up Now**. For details about the parameters, see **Creating a CSBS Backup**.

Step 5 Determine whether to select **Enable** next to **Application-Consistent Backup**. If selected, the system will perform application-consistent backups. If you select **Continue to back up data after the application-consistent backup fails.** at the same time, the system will perform crash-consistent backup if the application-consistent backup job fails. Otherwise, the whole backup operation fails.

NOTE

Before using application-consistent backup, change the security group and install the Agent. For details, see **Changing a Security Group**.

Step 6 Click **Next**.

Step 7 Check the details, confirm the settings, and click **Submit**.

Step 8 Return to the CSBS page as prompted. If the execution fails, rectify the fault based on the error details on the creation result page.

On the **Backup** tab page, if the value of **Backup Status** is **Available** and the value of **A** next to the backup name is blue, the application-consistent backup job is successfully executed. If **A** next to the backup name is gray, the application-consistent backup job fails to be executed.

----End

2.4.4 Uninstalling the Agent

Scenarios

This section describes how to uninstall the Agent if application-consistent backup is no longer needed.

Prerequisites

The username and password for logging in to an ECS have been obtained.

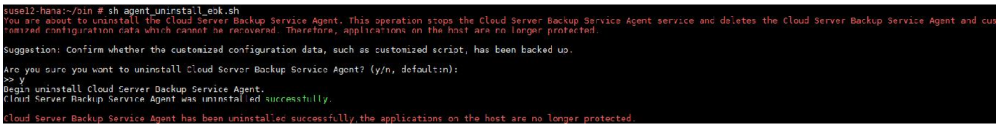
Uninstall the Agent for Linux

Step 1 Log in to the ECS and run the **su -root** command to switch to user **root**.

Step 2 In the **home/rdadmin/Agent/bin** directory, run the following command to uninstall the Agent. **Figure 2-14** displays an example. If the word **successfully** in green is displayed, the Agent is uninstalled successfully.

sh agent_uninstall_ebk.sh

Figure 2-14 Agent installed successfully



```
suse12-hana:~/bin # sh agent_uninstall_ebk.sh
You are about to uninstall the Cloud Server Backup Service Agent. This operation stops the Cloud Server Backup Service Agent service and deletes the Cloud Server Backup Service Agent and cus
tomized configuration data which cannot be recovered. Therefore, applications on the host are no longer protected.

Suggestion: Confirm whether the customized configuration data, such as customized script, has been backed up.

Are you sure you want to uninstall Cloud Server Backup Service Agent? (y/n, default:n):
>> y
Begin uninstall Cloud Server Backup Service Agent.
Cloud Server Backup Service Agent was uninstalled successfully.

Cloud Server Backup Service Agent has been uninstalled successfully,the applications on the host are no longer protected.
```

----End

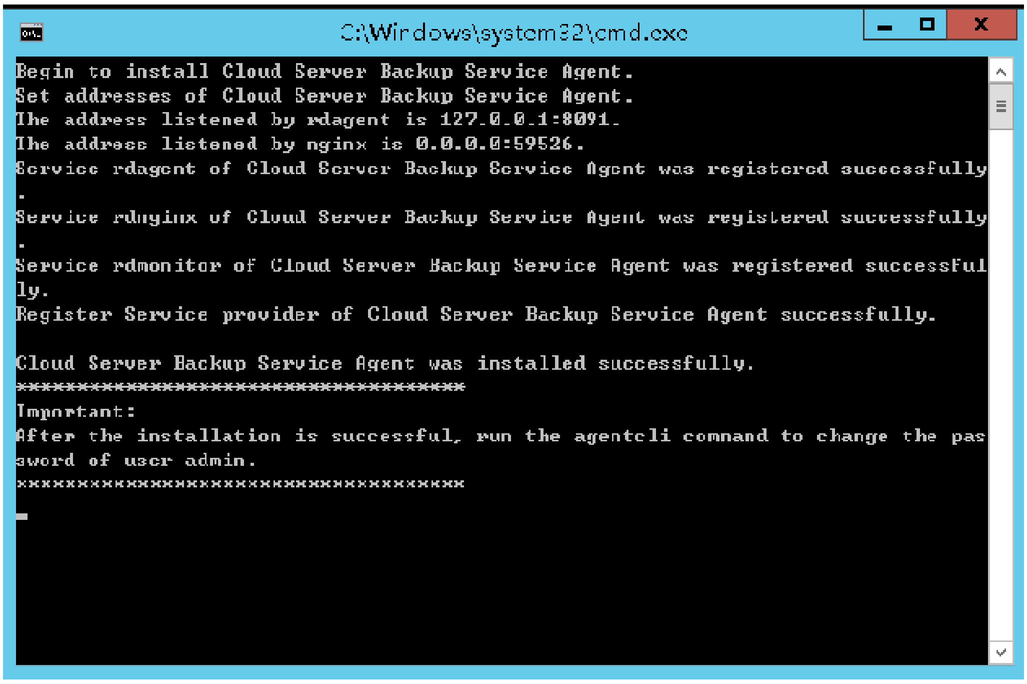
Uninstall the Agent for Windows

Step 1 Log in to the ECS.

Step 2 In the *Installation path***/bin** directory, double-click **agent_uninstall_ebk.bat**. The window for uninstalling the Agent is displayed.

After the uninstallation is complete and successful, the window will be automatically closed. See **Figure 2-15**.

Figure 2-15 Agent uninstalled successfully



```
Begin to install Cloud Server Backup Service Agent.
Set addresses of Cloud Server Backup Service Agent.
The address listened by rdagent is 127.0.0.1:8091.
The address listened by nginx is 0.0.0.0:59526.
Service rdagent of Cloud Server Backup Service Agent was registered successfully
.
Service rdnginx of Cloud Server Backup Service Agent was registered successfully
.
Service rdmonitor of Cloud Server Backup Service Agent was registered successful
ly.
Register Service provider of Cloud Server Backup Service Agent successfully.

Cloud Server Backup Service Agent was installed successfully.
*************************************
Important:
After the installation is successful, run the agentcli comnand to change the pas
sword of user admin.
*************************************
```

----End

Agent Security Maintenance

For details about how to perform security maintenance on Agent, such as changing the password and replacing the certificate, see **Client-Side security Maintenance**.

3 Backup Policies

3.1 Creating a Backup Policy

A backup policy can drive the system to automatically execute CSBS backup jobs at the specified interval. Periodic backups can be used to restore data quickly against data corruption or loss.

Context

- Automatic backup jobs require enabling the backup policy. The system automatically backs up ECSs associated with the backup policy and deletes expired backups.
- Each user can create a maximum of 32 backup policies.
- A maximum of 64 ECSs can be associated with a backup policy.

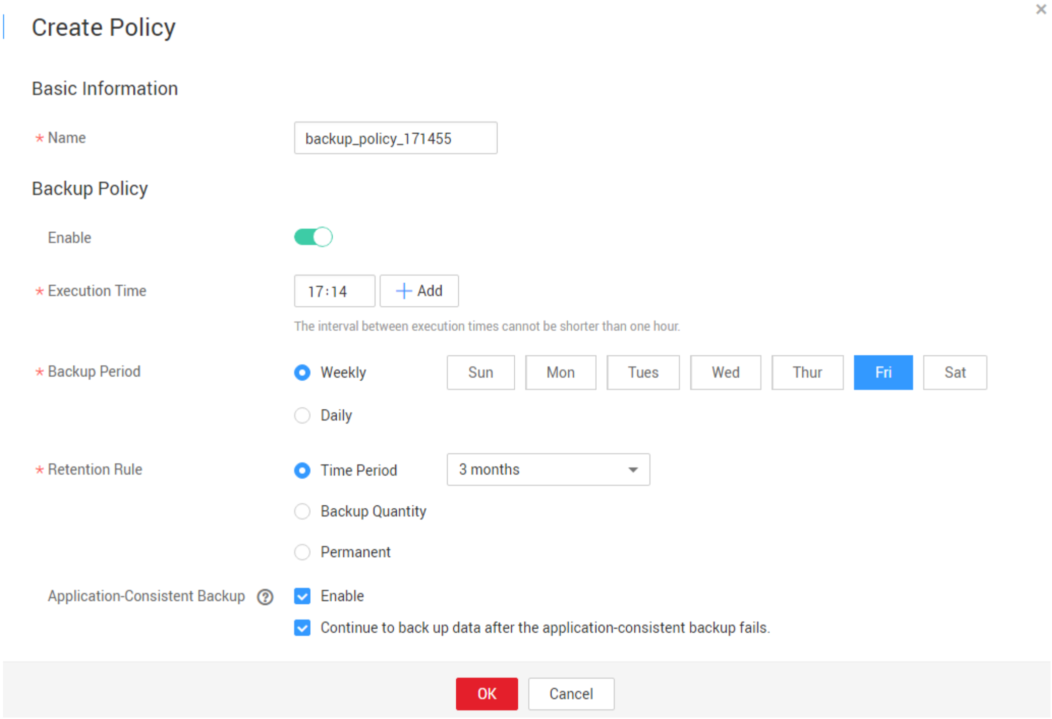
Procedure

Step 1 Log in to the CSBS management console.

1. Log in to the management console.
2. Under Storage > **Cloud Server Backup Service**.

Step 2 On the **Policies** tab page, click **Create Backup Policy**. See**Figure 3-1**.

Figure 3-1 Creating a backup policy



Create Policy

Basic Information

* Name: backup_policy_171455

Backup Policy

Enable

* Execution Time: 17:14 + Add

The interval between execution times cannot be shorter than one hour.

* Backup Period: ● Weekly (Sun, Mon, Tues, Wed, Thur, **Fri**, Sat) ○ Daily

* Retention Rule: ● Time Period (3 months) ○ Backup Quantity ○ Permanent

Application-Consistent Backup: ☑ Enable ☑ Continue to back up data after the application-consistent backup fails.

Step 3 Set the backup policy parameters according to **Table 3-1**.

Table 3-1 Parameter description

Parameter	Description	Remarks
Name	Backup policy name. It is a string of 1 to 255 characters that can contain only digits, letters, underscores (_), and hyphens (-).	backup_policy
Status	Whether to enable the backup policy. - Enabled: - Disabled:	Only after the backup policy is enabled, the system automatically backs up ECSs associated with the backup policy and deletes expired backups.

Parameter	Description	Remarks
Application-Consistent Backup	If selected, the system will perform application-consistent backups. If you select **Continue to back up data after the application-consistent backup fails.** at the same time, the system will perform crash-consistent backup if the application-consistent backup job fails. Otherwise, the whole backup operation fails. **NOTE** Before using application-consistent backup, change the security group and install the Agent. For details, see **Enabling Application-Consistent Backup**.	-
Execution Time	Execution time of the backup policy in a day A maximum of 24 backup times can be set in a day. The backup interval must be one hour or more. If backup jobs are executed in two consecutive days, the interval between the execution times of the last backup of the former day and the first backup of the latter day must be one hour or more.	00:00, 02:00 It is recommended that backup jobs be executed during off-peak hours or when there are no services running.
Backup Period	Dates for executing the backup job. ● Weekly Specifies on which days of each week the backup job will be executed. You can select multiple days. ● Daily Specifies the interval (every 1 to 30 days) for executing the backup job.	Every day If you select **Daily**, the first backup time is supposed to be in the day when the backup policy is created. If the creation time of the backup policy is later than the latest execution time, the initial backup will be performed in the next backup cycle. It is recommended that backup jobs be executed during off-peak hours or when there are no services running.

Parameter	Description	Remarks
Retention Rule	Rule that specifies how backups will be retained. ● Time Period You can choose to retain backups for one month, three months, six months, or one year, or for any desired number (2 to 99999) of days. ● Backup Quantity Specifies the maximum allowed number of backups for a single ECS. The value ranges from 2 to 99999. ● Permanent **NOTE** – When the number of retained backups exceeds the preset value, the system automatically deletes the earliest backups. When the retention periods of retained backups exceed the preset value, the system automatically deletes all expired backups. By default, the system automatically clears data every other day. The deleted backup does not affect other backups for restoration. – This parameter applies only to backups automatically scheduled by a backup policy. Those backups generated by a manually executed backup policy are not affected by this parameter and are not automatically deleted. You can manually delete them from the backup list. – After a backup is used to create an image, the backup will not be counted as a retained backup and will not be deleted automatically. – A maximum of 10 backups are retained for failed periodic backup jobs. They are retained for one month and can be manually deleted.	6 months

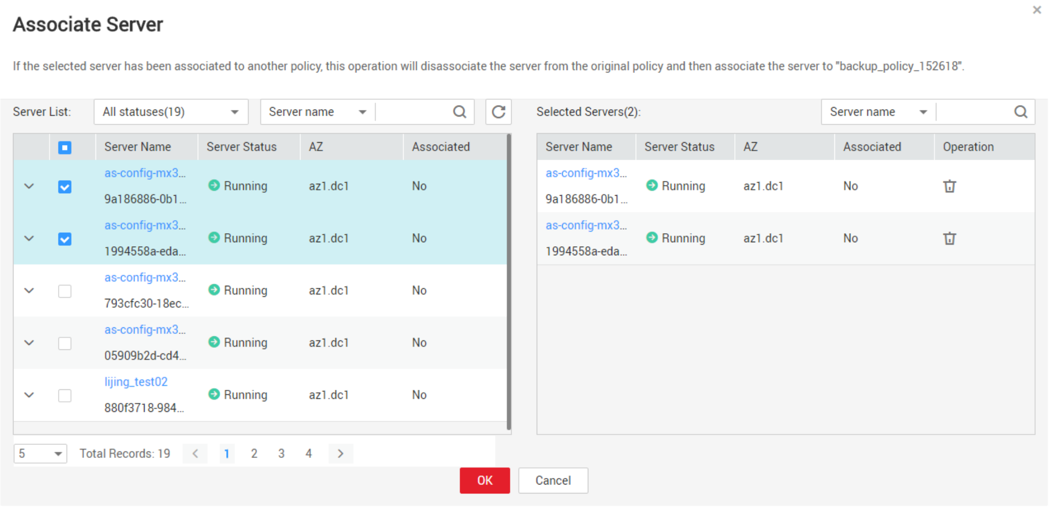
NOTE

More frequent backup intervals create more backups or retain backups for a longer time, protecting data with a higher level but occupying more storage space. Set an appropriate backup period as required.

Step 4 Click **OK**.

Step 5 In the row of the backup policy, click **Associate Server**. See **Figure 3-2**.

Figure 3-2 Associating servers



Associate Server

If the selected server has been associated to another policy, this operation will disassociate the server from the original policy and then associate the server to "backup_policy_152618".

Server List: All statuses(19) Server name

	■	Server Name	Server Status	AZ	Associated
⌄	☑	as-config-mx3... 9a186886-0b1...	Running	az1.dc1	No
⌄	☑	as-config-mx3... 1994558a-eda...	Running	az1.dc1	No
⌄	□	as-config-mx3... 793cfc30-18ec...	Running	az1.dc1	No
⌄	□	as-config-mx3... 05909b2d-cd4...	Running	az1.dc1	No
⌄	□	lijing_test02 880f3718-984...	Running	az1.dc1	No

5 Total Records: 19 < 1 2 3 4 >

Selected Servers(2): Server name

Server Name	Server Status	AZ	Associated	Operation
as-config-mx3... 9a186886-0b1...	Running	az1.dc1	No	🗑
as-config-mx3... 1994558a-eda...	Running	az1.dc1	No	🗑

Step 6 In the available server list, select the ECSs you want to associate. After ECSs are selected, they are added to the list of selected servers.

NOTE

- A maximum of 64 ECSs can be associated with a backup policy.
- If a selected ECS has been associated with another backup policy, it will be disassociated from the original backup policy automatically and then associated with the new backup policy.
- If EVS disks on an ECS have been associated with a VBS backup policy, disassociate them from the VBS backup policy. Otherwise, two backups are generated for each of the EVS disks.
- An ECS with shared EVS disks cannot be associated with a backup policy.
- You can only select ECSs that are in the **Running** or **Stopped** state.

Step 7 Click **OK**.

----End

3.2 Editing a Backup Policy

This section describes how to edit a backup policy.

NOTE

Changing the backup period does not actually change the time of the day when the backup is scheduled to run. For example, you set to run a backup job every seven days. Three days later, you modified the policy to run a backup job every five days. Then the associated server will be backed up two days after your modification.

To actually change when the backup is scheduled to run, dissociate the original policy and associate the server with a new backup policy.

Prerequisites

You have created at least one backup policy.

Procedure

Step 1 Log in to the CSBS management console.

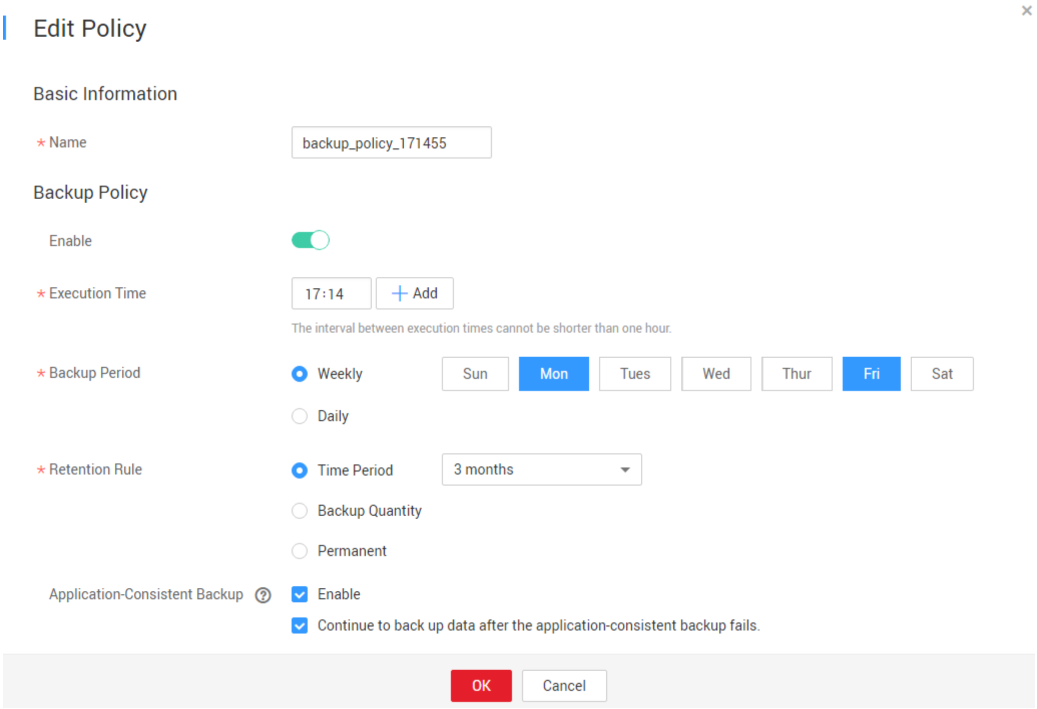
1. Log in to the management console.
2. Under Storage > **Cloud Server Backup Service**.

Step 2 Click the **Policies** tab.

Step 3 In the row of the backup policy you want to modify, click **Edit**.

Step 4 Edit the backup policy. See **Figure 3-3**.

Figure 3-3 Editing a backup policy



Edit Policy

Basic Information

* Name: backup_policy_171455

Backup Policy

Enable: ●

* Execution Time: 17:14 + Add

The interval between execution times cannot be shorter than one hour.

* Backup Period: ● Weekly Sun [✓ Mon] Tues Wed Thur [✓ Fri] Sat

○ Daily

* Retention Rule: ● Time Period 3 months

○ Backup Quantity

○ Permanent

Application-Consistent Backup: ☑ Enable

☑ Continue to back up data after the application-consistent backup fails.

Related parameters are described in **Table 3-1**.

Step 5 Click **OK**.

----End

3.3 Deleting a Backup Policy

You can delete backup policies if required.

Prerequisites

You have created at least one backup policy.

Procedure

Step 1 Log in to the CSBS management console.

1. Log in to the management console.
2. Under Storage > **Cloud Server Backup Service**.

Step 2 Click the **Policies** tab.

Step 3 In the row of the backup policy you want to modify, choose **More** > **Delete**.

NOTE

Deleting a backup policy will not delete backups generated based on the policy. You can manually delete unwanted backups.

Step 4 Click **OK**.

----End

3.4 Executing a Backup Policy at Once

You can manually execute a backup policy to back up an associated ECS immediately.

Context

- If an ECS is being backed up, you cannot manually execute a backup policy on it.
- If a manual backup job is still in progress, scheduled automatic backup operations will be postponed to the next backup cycle. An interval of at least 3 hours is recommended between a manual backup operation and a scheduled automatic backup operation.

Prerequisites

At least one backup policy has been created and has been associated with at least one ECS.

Procedure

Step 1 Log in to the CSBS management console.

1. Log in to the management console.
2. Under Storage > **Cloud Server Backup Service**.

Step 2 Click the **Policies** tab.

Step 3 In the upper right corner of the backup policy you want to execute, choose **More** > **Backup Now**.

Step 4 Click **OK**.

----End

3.5 Enabling and Disabling a Backup Policy

This section introduces how to enable and disable a backup policy.

Procedure

Step 1 Log in to the CSBS management console.

1. Log in to the management console.
2. Under Storage > **Cloud Server Backup Service**.

Step 2 Click the **Policies** tab.

Step 3 In the row of the backup policy you want to enable or disable, click **More** and choose **Enable Backup Policy**, or **Disable Backup Policy**

NOTE

- After a backup policy is enabled, periodic backup jobs will be executed according to the backup policy.
- After a backup policy is disabled, the ongoing backup job is not affected but no more scheduled automatic backup jobs will be executed.

Step 4 Click **OK**.

----End

3.6 Disassociating ECSs from a Backup Policy

When an ECS associated with a backup policy no longer needs to be backed up, you can disassociate it from the backup policy.

Prerequisites

- You have created at least one backup policy.
- The backup policy is associated with at least one ECS.

Procedure

Step 1 Log in to the CSBS management console.

1. Log in to the management console.
2. Under Storage > **Cloud Server Backup Service**.

Step 2 Click the **Policies** tab.

Step 3 In the row of the backup policy from which you want to disassociate the ECS, click ⌄ .

Step 4 Under **Associated Servers**, click **Disassociate** in the row of the target ECS, or select the target ECS from the list and then click **Disassociate** in the upper left corner of the list.

NOTE

- When the target ECS is being backed up, you can still disassociate it. However, the backup job will continue and backups will be generated.
- After an ECS is disassociated from the associated backup policy, its existing backups will not be deleted. If you want to delete them, manually delete them.

Step 5 Click **OK**.

----End

3.7 Associating ECSs with a Backup Policy

After creating a backup policy, you can add ECSs to it so that the ECSs are associated with the backup policy.

Prerequisites

- You have created at least one backup policy.
- At least one ECS in the **Running** or **Stopped** state is available.
- A maximum of 64 ECSs can be associated with a backup policy.

Procedure

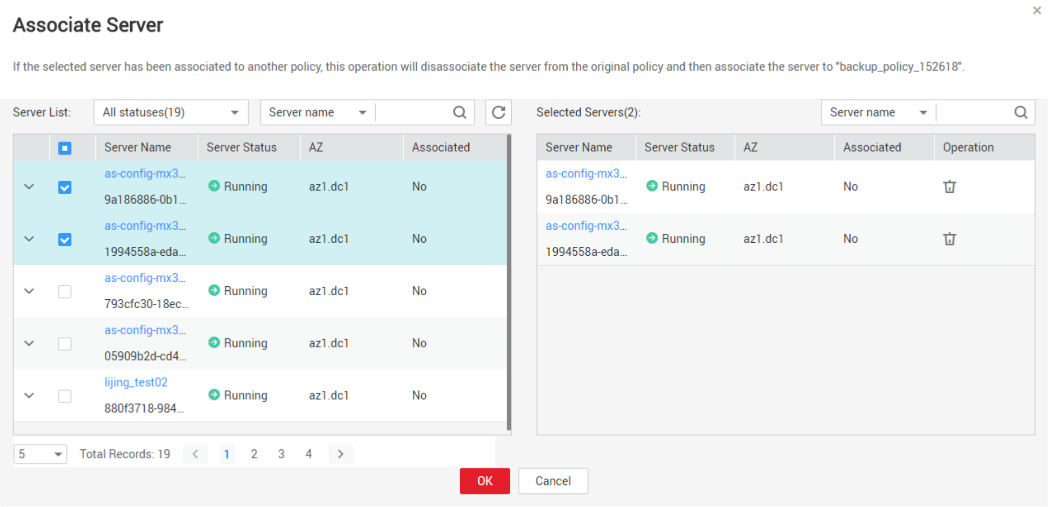
Step 1 Log in to the CSBS management console.

1. Log in to the management console.
2. Under Storage > **Cloud Server Backup Service**.

Step 2 Click the **Policies** tab.

Step 3 In the row of the backup policy with which you want to associate ECSs, click **Associate Server**. See **Figure 3-4**.

Figure 3-4 Associating servers



Associate Server

If the selected server has been associated to another policy, this operation will disassociate the server from the original policy and then associate the server to "backup_policy_152618".

Server List: All statuses(19) | Server name

	■	Server Name	Server Status	AZ	Associated
⌄	☑	as-config-mx3... 9a186886-0b1...	Running	az1.dc1	No
⌄	☑	as-config-mx3... 1994558a-eda...	Running	az1.dc1	No
⌄	□	as-config-mx3... 793cfc30-18ec...	Running	az1.dc1	No
⌄	□	as-config-mx3... 05909b2d-cd4...	Running	az1.dc1	No
⌄	□	lijing_test02 880f3718-984...	Running	az1.dc1	No

5 | Total Records: 19 | < 1 2 3 4 >

Selected Servers(2): Server name

Server Name	Server Status	AZ	Associated	Operation
as-config-mx3... 9a186886-0b1...	Running	az1.dc1	No	🗑
as-config-mx3... 1994558a-eda...	Running	az1.dc1	No	🗑

Step 4 In the server list, select the ECSs you want to associate. After ECSs are selected, they are added to the list of selected servers.

NOTE

- A maximum of 64 ECSs can be associated with a backup policy.
- If a selected ECS has been associated with another backup policy, it will be disassociated from the original backup policy automatically and then associated with the new backup policy.
- If EVS disks on an ECS have been associated with a VBS backup policy, disassociate them from the VBS backup policy. Otherwise, two backups are generated for each of the EVS disks.
- An ECS with shared EVS disks cannot be associated with a backup policy.
- You can only select ECSs that are in the **Running** or **Stopped** state.

Step 5 Click **OK**.

----End

4 Using Backups to Restore ECSs

When EVS disks on an ECS are faulty or ECS data is lost due to misoperations, you can use a backup to restore the ECS.

Context

- CSBS supports backup and restoration of all EVS disks as a whole instead of part of the EVS disks on an ECS.
- Data on data disks cannot be restored to system disks.
- CSBS does not support restoration to ECSs that are in the **Faulty**, **Resizing**, or **Verifying resizing** state.

Prerequisites

- EVS disks on the ECS whose data needs to be restored are running properly.
- The ECS whose data needs to be restored has at least one **Available** backup.

Procedure

Step 1 Log in to the CSBS management console.

1. Log in to the management console.
2. Under Storage > **Cloud Server Backup Service**.

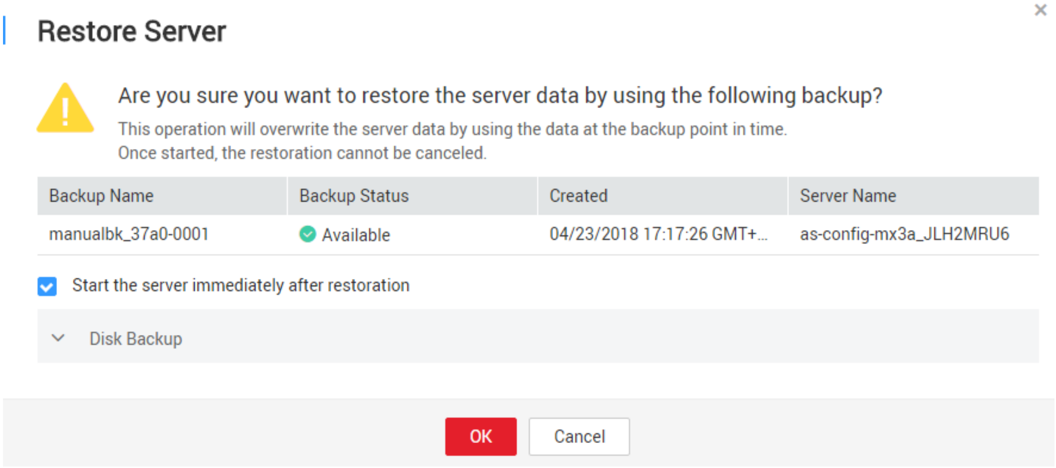
Step 2 Click the **Backups** tab. Locate the backup for the ECS. For details, see **Viewing a Backup**.

Step 3 In the row of the backup, click **Restore**. See **Figure 4-1**.

NOTICE

The historical data at the backup point in time will overwrite the current ECS data. The restoration cannot be undone.

Figure 4-1 Restoring a server



Restore Server

Are you sure you want to restore the server data by using the following backup?

This operation will overwrite the server data by using the data at the backup point in time.
Once started, the restoration cannot be canceled.

Backup Name	Backup Status	Created	Server Name
manualbk_37a0-0001	Available	04/23/2018 17:17:26 GMT+...	as-config-mx3a_JLH2MRU6

☑ Start the server immediately after restoration

Step 4 Optional: Deselect **Start the server immediately after restoration**.

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

NOTICE

VMs are shut down when restoring ECSs. Therefore, perform a restoration job during off-peak hours.

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

NOTE

- If the ECS has only one EVS disk, the backup is restored to the only EVS disk by default.
- If the ECS has multiple EVS disks, the backup will be restored to the original EVS disk. Alternatively, you can specify another EVS disk for the restoration. The specified EVS disk must have an equal capacity to or a larger capacity than the original EVS disk.
- Data on data disks cannot be restored to system disks.

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

In the backup list, view the restoration status. When the backup enters the **Available** state and no new failed restoration job exists in **Task Status**, the restoration is successful.

To query failed restoration jobs, see **Processing Failed Jobs**.

NOTICE

If a Windows ECS is restored, data disks may fail to be displayed due to Windows limitations.

You need to manually set these data disks to be online. For details, see **Data Disks Are Not Displayed After a Windows Server Is Restored**.

----End

5 Processing Failed Jobs

This section introduces how to handle a failed job.

Prerequisites

At least one failed job exists.

Context

- After a backup job fails, a backup whose **Status** is **Error** is generated, and a message is displayed on the **Backup Jobs** tab page of **Job Status**. Click the question mark ⓘ next to the message to view details.
- After a restoration job fails, a message is displayed on the **Restoration Jobs** tab page of **Job Status**. Click ⓘ next to the message to view details.

Procedure

Step 1 Log in to the CSBS management console.

1. Log in to the management console.
2. Under Storage > **Cloud Server Backup Service**.

Step 2 Click the **Backups** tab and then click ● next to **Job Status**.

Step 3 On the **Backup Jobs** tab page, view the cause of the failed job.

Step 4 On the **Restoration Jobs** tab page, view the cause of the failed job.

Step 5 Optional: Click **Delete** in the row of the failed job to delete the job. Alternatively, click **Delete All** in the upper left corner to delete all failed jobs.

----End

6 Events

In CSBS, you can use Cloud Trace Service (CTS) to trace operations in CSBS.

Prerequisites

CTS has been enabled.

Key Operations Recorded by CTS

Table 6-1 CSBS operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Creating a backup policy	backupPolicy	createBackupPolicy
Updating a backup policy	backupPolicy	updateBackupPolicy
Deleting a backup policy	backupPolicy	deleteBackupPolicy
Binding resources	backupPolicy	bindResources
Executing a backup	checkpointItem	createCheckpoint
Restoring a backup	checkpointItem	restoreCheckpointItem
Deleting a backup	checkpointItem	deleteCheckpointItem
Backing up an ECS	cloudServer	backupCloudServer
Deleting a task	operationLog	deleteOperationLog

View Audit Logs

For details about how to view audit logs, see section **Querying Traces** in the *Cloud Trace Service User Guide.*

Disabling or Enabling a Tracker

This section describes how to disable an existing tracker on the CTS console. After the tracker is disabled, the system will stop recording operations, but you can still view existing operation records.

Step 1 Log in to the management console.

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

Step 3 Click **Service List** and choose **Management & Governance** > **Cloud Trace Service**.

Step 4 Click **Tracker** in the left pane.

Step 5 Click **Disable** on the right of the tracker information.

Step 6 Click **OK**.

Step 7 After the tracker is disabled, its status changes from **Disable** to **Enable**. To enable the tracker again, click **Enable** and then click **OK**. The system will start recording operations again.

----End

7 Quotas

What Is Quota?

Quotas can limit the number or amount of resources available to users, such as the maximum number of ECSs or EVS disks that can be created.

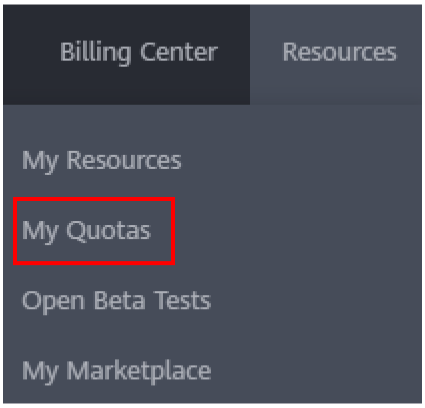
If the existing resource quota cannot meet your service requirements, you can apply for a higher quota.

How Do I View My Quotas?

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. In the upper right corner of the page, choose **Resources** > **My Quotas**.

   The **Service Quota** page is displayed.

   Figure 7-1 My Quotas

4. View the used and total quota of each type of resources on the displayed page.

   If a quota cannot meet service requirements, apply for a higher quota.

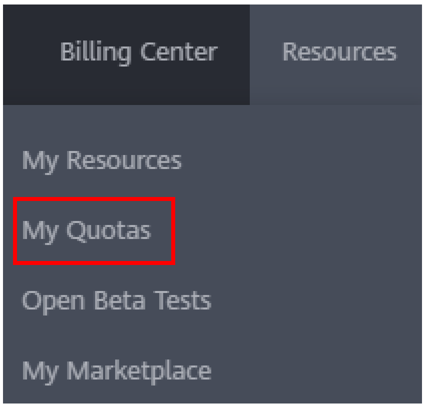
How Do I Apply for a Higher Quota?

1. Log in to the management console.

2. In the upper right corner of the page, choose **Resources** > **My Quotas**.

   The **Service Quota** page is displayed.

   Figure 7-2 My Quotas

3. Click **Increase Quota**.
4. On the **Create Service Ticket** page, configure parameters as required.

   In **Problem Description** area, fill in the content and reason for adjustment.
5. After all necessary parameters are configured, select **I have read and agree to the Tenant Authorization Letter and Privacy Statement** and click **Submit**.

A Client-Side security Maintenance

A.1 Changing the Password of the Account for Reporting Alarms (SNMP v3)

To enhance O&M security, you are advised to change the password of the account for reporting alarms.

Prerequisites

- You have obtained a username and its password for logging in to the management console.
- The username and password for logging in to a server have been obtained.

Context

This section introduces the procedures in Windows and Linux.

NOTICE

If the authentication password and data encryption password for SNMP v3 of the Agent is the same, security risks exist. To ensure system security, you are advised to set the authentication password and data encryption password to be different ones.

The initial authentication password is **BCM@DataProtect6** and the initial data encryption password is **BCM@DataProtect8**.

NOTE

The password must meet the following complexity requirements:

- Contains 8 to 16 characters.
- Contains at least one of the following special characters: `~!@#$%^&*()-_=+\|[{}];:'",<.>/?
- Contains at least two of the following types of characters:
  - Uppercase letters
  - Lowercase letters
  - Digits
- Cannot be the same as the username or the username in reverse order.
- Cannot be the same as the old passwords.
- Cannot contain spaces.

Procedure (Windows)

Step 1 Log in to the server where the Agent is installed.

Step 2 Open the CLI and go to the *installation path***bin** directory.

Step 3 Run the **agentcli.exe chgsnmp** command. Type the login password of the Agent and press **Enter**.

```
Please choose operation:
1: Change authentication password
2: Change private password
3: Change authentication protocol
4: Change private protocol
5: Change security name
6: Change security Level
7: Change security model
8: Change context engine ID
9: Change context name
Other: Quit
Please choose:
```

NOTE

admin is the username configured during the Agent installation.

Step 4 Select the SN of the authorization password or data encryption password that you want to change and press **Enter**.

Step 5 Type the old password and press **Enter**.

Step 6 Type a new password and press **Enter**.

Step 7 Type the new password again and press **Enter**. The password is changed.

----End

Procedure (Linux)

Step 1 Log in to the Linux server using the server password.

Step 2 Run the **TMOUT=0** command to prevent PuTTY from exiting due to session timeout.

NOTE

After the preceding command is executed, the system remains running even when no operation is performed, which results in security risks. For security purposes, run the **exit** command to exit the system after you finish performing operations.

Step 3 Run the **su - rdadmin** command to switch to user **rdadmin**.

Step 4 Run the **/home/rdadmin/Agent/bin/agentcli chgsnmp** command. Type the login password of the Agent and press **Enter**.

NOTE

The installation path of the Agent is **/home/rdadmin/Agent**.

```
Please choose operation:
1: Change authentication password
2: Change private password
3: Change authentication protocol
4: Change private protocol
5: Change security name
6: Change security Level
7: Change security model
8: Change context engine ID
9: Change context name
Other: Quit
Please choose:
```

Step 5 Select the SN of the authorization password or data encryption password that you want to change and press **Enter**.

Step 6 Type the old password and press **Enter**.

Step 7 Type a new password and press **Enter**.

Step 8 Type the new password again and press **Enter**. The password is changed.

----End

A.2 Replacing the Server Certificate

For security purposes, users may want to use a Secure Socket Layer (SSL) certificate issued by a third-party certification authority. The Agent allows you to replace authentication certificates and private key files as long as they provide the authentication certificates and private-public key pairs. The update to the certificate can take effect only after the Agent is restarted, hence you are advised to update the certificate in off-peak hours.

Prerequisites

- You have obtained a username and its password for logging in to the management console.
- The username and password for logging in to a server have been obtained.
- New certificates in the X.509v3 format have been obtained.

Context

- The client is pre-deployed with the Agent AC certificate **bcmagentca**, private key file of the CA certificate **server.key** (The default protection password of this file is **BCM@DataProtect123**), and authentication certificate **server.crt**. All these files are saved in **/home/rdadmin/Agent/bin/nginx/conf** (if you use Linux) or **\bin\nginx\conf** (if you use Windows).

- You need to restart the Agent after replacing a certificate to make the certificate effective.

Procedure (Linux)

Step 1 Log in the Linux server with the Agent installed.

Step 2 Run the **TMOUT=0** command to prevent PuTTY from exiting due to session timeout.

NOTE

After the preceding command is executed, the system remains running even when no operation is performed, which results in security risks. For security purposes, run the **exit** command to exit the system after you finish performing operations.

Step 3 Run the **su - rdadmin** command to switch to user **rdadmin**.

Step 4 Run the **cd /home/rdadmin/Agent/bin** command to go to the script save path.

NOTE

The installation path of the Agent is **/home/rdadmin/Agent**.

Step 5 Run the **sh agent_stop.sh** command to stop the Agent running.

Step 6 Place the new certificates and private key files in the specified directory.

NOTE

Place new certificates in the **/home/rdadmin/Agent/bin/nginx/conf** directory.

Step 7 Run the **/home/rdadmin/Agent/bin/agentcli chgkey** command.

Information similar to the following information is displayed:

```
Enter password of admin:
```

NOTE

admin is the username configured during the Agent installation.

Step 8 Type the login password of the Agent and press **Enter**.

Information similar to the following information is displayed:

```
Change certificate file name:
```

Step 9 Enter a name for the new certificate and press **Enter**.

NOTE

If the private key and the certificate are the same file, names of the private key and the certificate are identical.

Information similar to the following information is displayed:

```
Change certificate key file name:
```

Step 10 Enter a name for the new private key file and press **Enter**.

Information similar to the following information is displayed:

```
Enter new password:
Enter the new password again:
```

Step 11 Enter the protection password of the private key file twice. The certificate is then successfully replaced.

Step 12 Run the **sh agent_start.sh** command to start the Agent.

----End

Procedure (Windows)

Step 1 Log in the Windows server with the Agent installed.

Step 2 Open the CLI and go to the *installation path***\bin** directory.

Step 3 Run the **agent_stop.bat** command to stop the Agent running.

Step 4 Place the new certificates and private key files in the specified directory.

NOTE

Place new certificates in the *installation path***\bin\nginx\conf** directory.

Step 5 Run the **agentcli.exe chgkey** command.

Information similar to the following information is displayed:

```
Enter password of admin:
```

NOTE

admin is the username configured during the Agent installation.

Step 6 Enter a name for the new certificate and press **Enter**.

NOTE

If the private key and the certificate are the same file, names of the private key and the certificate are identical.

Information similar to the following information is displayed:

```
Change certificate key file name:
```

Step 7 Enter a name for the new private key file and press **Enter**.

Information similar to the following information is displayed:

```
Enter new password:
Enter the new password again:
```

Step 8 Enter the protection password of the private key file twice. The certificate is then successfully replaced.

Step 9 Run the **agent_start.bat** command to start the Agent.

----End

A.3 Replacing CA Certificates

Scenarios

A CA certificate is a digital file signed and issued by an authentication authority. It contains the public key, information about the owner of the public key, information about the issuer, validity period, and certain extension information. It is used to set up a secure information transfer channel between the Agent and the server.

If the CA certificate does not comply with the security requirements or has expired, replace it for security purposes.

Prerequisites

- The username and password for logging in to an ECS have been obtained.
- A new CA certificate is ready.

Procedure (Linux)

Step 1 Log in the Linux server with the Agent installed.

Step 2 Run the following command to disable user logout upon system timeout:

TMOUT=0

Step 3 Run the following command to switch to user **rdadmin**:

su - rdadmin

Step 4 Run the following command to go to the path to the Agent start/stop script:

cd /home/rdadmin/Agent/bin

Step 5 Run the following command to stop the Agent:

sh agent_stop.sh

Step 6 Run the following command to go to the path to the CA certificate:

cd /home/rdadmin/Agent/bin/nginx/conf

Step 7 Run the following command to delete the existing CA certificate:

rm bcmagentca.crt

Step 8 Copy the new CA certificate file into the **/home/rdadmin/Agent/bin/nginx/conf** directory and rename the file **bcmagentca.crt**.

Step 9 Run the following commands to change the owner of the CA certificate:

chown rdadmin:rdadmin bcmagentca.crt

Step 10 Run the following command to modify the permissions on the CA certificate:

chmod 400 bcmagentca.crt

Step 11 Run the following command to go to the path to the Agent start/stop script:

cd /home/rdadmin/Agent/bin

Step 12 Run the following command to start the Agent:

sh agent_start.sh

----End

Procedure (Windows)

Step 1 Log in to the ECS with the Agent installed.

Step 2 Go to the *Installation path***\bin** directory.

Step 3 Run the **agent_stop.bat** script to stop the Agent.

Step 4 Go to the *Installation path***\nginx\conf** directory.

Step 5 Delete the **bcmagentca.crt** certificate file.

Step 6 Copy the new CA certificate file into the *Installation path***\nginx\conf** directory and rename the file **bcmagentca.crt**.

Step 7 Go to the *Installation path***\bin** directory.

Step 8 Run the **agent_stop.bat** script to service.

----End

B Change History

Release Date	Description
2019-02-23	This issue is the fourth official release. Updated the following content: Added content related to application-consistent backup.
2019-02-14	This issue is the third official release. Updated the following content: Added the description of quotas.
2018-11-19	This issue is the second official release. Updated the following content: ● Split the document into several parts for release. ● Added the feature for creating images.
2018-04-30	This issue is the first official release.