3 Managing Snapshots

3.1 Overview.....................................................................................................................................................................111
3.2 Manually Creating a Snapshot....................................................................................................................................112
3.3 Setting the Automated Snapshot Policy..................................................................................................................114
3.4 Viewing Snapshot Information...................................................................................................................................115
3.5 Copying Automated Snapshots...................................................................................................................................116
3.6 Restoring a Snapshot..................................................................................................................................................117
3.7 Deleting Manual Snapshots........................................................................................................................................119

4 Managing Parameter Templates

4.1 Overview.....................................................................................................................................................................120
4.2 Creating a Parameter Template...................................................................................................................................121
4.3 Managing Parameter Values........................................................................................................................................122
4.4 Setting the Parameter Value Policy............................................................................................................................123
4.5 Viewing a Parameter Value...........................................................................................................................................124
4.6 Copying a Parameter Value..........................................................................................................................................125
4.7 Restoring a Parameter Value.......................................................................................................................................126
4.8 Deleting a Parameter Value..........................................................................................................................................127

5 Permissions Management

5.1 Basic Concepts...........................................................................................................................................................126
5.2 Creating a User and Granting Permissions................................................................................................................131
5.3 Creating a Custom Policy...........................................................................................................................................136
5.4 Syntax of Fine-Grained Policies................................................................................................................................144
5.5 RBAC Syntax of RBAC Policies................................................................................................................................149

6 Managing MRS Data Sources

6.1 Importing Data from MRS to DWS............................................................................................................................153
6.2 Creating an MRS Data Source Connection................................................................................................................154
6.3 Updating the MRS Data Source Configuration..........................................................................................................156

7 Monitoring a Cluster

7.1 Overview.....................................................................................................................................................................158
7.2 Monitoring MRS Components...................................................................................................................................159
7.3 Monitoring Cluster Health...........................................................................................................................................160
7.4 Monitoring Cluster Performance.................................................................................................................................161
7.5 Monitoring Cluster Resource Utilization.....................................................................................................................162

8 Notifying Events

8.1 Overview.....................................................................................................................................................................168
8.2 Configuring Event Notifications.................................................................................................................................169
8.3 Managing Event Notifications................................................................................................................................170
8.4 Viewing Event Notifications....................................................................................................................................171
8.5 Deleting Event Notifications....................................................................................................................................172

Copyright © Huawei Technologies Co., Ltd.
## Contents

8.2 Subscribing to Event Notification ................................................................. 171
8.3 Viewing Events ............................................................................................ 174

### 9 Audit Logs .................................................................................................. 175
9.1 Viewing Audit Logs of Key Operations on the Management Console ............ 175
9.2 Configuring the Database Audit Log ............................................................. 178
9.3 Dumping the Database Audit Log ................................................................. 181

### 10 Error Code Reference .............................................................................. 185

### A Change History ......................................................................................... 187
1 Managing Clusters

1.1 Accessing the DWS Management Console

Scenario

This section describes how to log in to the DWS management console and use DWS.

Procedure

Step 1  Log in to the public cloud management console.

Step 2  From the menu on top of the management console, choose Service List.

Step 3  In the EI Enterprise Intelligence list, click Data Warehouse Service to enter the DWS management console.

----End

1.2 Creating a Cluster

To use DWS in the public cloud environment, you need to create a data warehouse cluster first. The pay-per-use billing mode is used by default when you create a data warehouse cluster. This billing mode allows you to turn your cloud resources on or off at any time. You are billed based on the actual service duration (hourly), so that you can customize a data warehouse cluster that meets your computing and storage needs. Alternatively, you can buy a yearly/monthly package and create a cluster. In this billing mode, you need to prepay nodes on a yearly or monthly basis. This mode offers you significant discounts compared with the pay-per-use mode. For details, see Buying Yearly/Monthly Packages.

This section describes how to create a data warehouse cluster on the DWS management console.

Preparations Before Creating a Cluster

- The flavor of nodes in the cluster has been evaluated.

Choose as many nodes as possible to ensure high-performance storage and computing capabilities for service applications based on service requirements. A node in a data warehouse...
warehouse cluster contains two DataNodes. The DataNode instance stores service data (support for row-based, column-based, and hybrid storage), executes the data query tasks, and returns the execution results.

- A network access topology has been designed.
- Plan an appropriate AZ and configure the network to isolate the data warehouse cluster from other public cloud services based on the service application requirements.
- Ensure that the number of available nodes meets the following conditions. Otherwise, the cluster cannot be created.
  - The number of available nodes must be greater than or equal to three, because at least three nodes are required for creating a cluster. You can view the number of available nodes on the Cluster Management page.
  - The number of nodes in the cluster to be created must be less than or equal to the number of available nodes.

Creating a Cluster

**Step 1** Log in to the management console at https://console.huaweicloud.com/dws/?locale=en-us.

**Step 2** On the Cluster Management page, click Create DWS Cluster.

**Step 3** Select the Region.

**Step 4** Configuring node-related parameters

### Table 1-1 Region parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region</td>
<td>Select the actual region where the cluster nodes run. For more information about the endpoint, visit <a href="https://console.huaweicloud.com/dws/?locale=en-us">Regions and Endpoints</a>.</td>
<td>CN North-Beijing1</td>
</tr>
<tr>
<td>AZ</td>
<td>Select an AZ associated with the cluster region. For more information, see <a href="https://console.huaweicloud.com/dws/?locale=en-us">Regions and AZs</a>.</td>
<td>AZ1</td>
</tr>
</tbody>
</table>

- **NOTE**

The number of nodes in a new cluster cannot exceed the quota that can be used by a user or 32. If the node quota is insufficient, click **Increase quota** to submit a service ticket and apply for a higher node quota.

If you have yearly/monthly nodes that meet service requirements, you are advised to use these nodes first to save costs. If no yearly/monthly nodes are available, click **Buy Yearly/Monthly Package**.
Figure 1-1 Configuring node-related parameters

Table 1-2 Node configuration parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster Type</td>
<td>Available cluster types are:</td>
<td>Enterprise-grade</td>
</tr>
<tr>
<td></td>
<td>- <strong>Enterprise-grade</strong>: provides capabilities of querying large amounts of data in batches.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Ultra-high concurrency</strong>: provides capabilities of interactive, highly concurrent queries on small amounts of data with low latency.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong></td>
<td>This parameter can only be viewed by OBT users.</td>
</tr>
</tbody>
</table>

*NOTE* This parameter can only be viewed by OBT users.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node Flavor</td>
<td>Available node flavors include:</td>
<td>dws.dc.4xlarge</td>
</tr>
<tr>
<td></td>
<td>- <strong>Computing-intensive</strong>: Computing-intensive nodes are configured with SSDs with higher I/O performance, and are suitable for scenarios with high concurrency and low latency, for example, interactive queries.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Disk-intensive</strong>: Disk-intensive nodes are equipped with HDDs with larger capacity but lower I/O. These nodes apply to service scenarios where the data storage volume is large but the query concurrency and delay requirements are not too high, for example, batch processing tasks.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Select the vCPU and memory resources of each node in the cluster. Item <strong>Concurrent Queues</strong> in the node flavor indicates the maximum number of concurrent jobs supported by the system.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For more information about the node flavors supported by DWS, see <a href="#">DWS Pricing Details</a>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>AZ1</strong> of region CN South-Guangzhou supports node flavors <strong>dws.d2.xlarge</strong> and <strong>dws.d2.12xlarge</strong> only.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>AZ2</strong> of region CN East-Shanghai2 supports node flavors <strong>dws.d2.xlarge</strong>, <strong>dws.d2.12xlarge</strong>, <strong>dws.m3.xlarge</strong> only.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Flavors <strong>gs.m3.xlarge</strong>, <strong>gs.m3.4xlarge</strong>, <strong>gs.m3.8xlarge</strong>, and <strong>gs.m3.15xlarge</strong> can be selected only by OBT users.</td>
<td></td>
</tr>
<tr>
<td>Nodes</td>
<td>Specify the number of nodes in the cluster. The number of nodes ranges from 3 to 32.</td>
<td>3</td>
</tr>
<tr>
<td>Total Capacity (TB)</td>
<td>Display the cluster's total capacity. The storage capacity of each flavor is the actual database space used for storing data. The displayed storage capacity has deducted the disk space consumed by backups and RAIDs.</td>
<td>-</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Example Value</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Yearly/Monthly Nodes</td>
<td>Display the number of yearly/monthly nodes of the selected flavor in the current region.</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>• If you have not purchased yearly/monthly nodes, click <strong>Buy Yearly/Monthly Package</strong> to purchase them. For details, see <strong>Buying Yearly/Monthly Packages</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If you have purchased a yearly/monthly package, the nodes within the package range will not be charged during the validity period and the extra nodes will be charged based on pay-per-use pricing. For example, if <strong>Nodes</strong> is set to 3 and your <strong>Yearly/Monthly Nodes</strong> is 2, two nodes are not charged within the validity period of yearly/monthly nodes and one node is charged based on pay-per-use pricing.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 5** Configure cluster-related parameters.

**Figure 1-2 Cluster parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster Name</td>
<td>Set the name of the data warehouse cluster. Enter 4 to 64 characters. Only case-insensitive letters, digits, hyphens (-), and underscores (_) are allowed. The value must start with a letter.</td>
<td>dws-demo</td>
</tr>
<tr>
<td>Cluster Version</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Default Database</td>
<td>postgres</td>
<td></td>
</tr>
<tr>
<td>Administrator Account</td>
<td>dbadmin</td>
<td></td>
</tr>
<tr>
<td>Administrator Password</td>
<td>..............................................................................................................................................................................................................</td>
<td></td>
</tr>
<tr>
<td>Confirm Password</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database Port</td>
<td>8000</td>
<td></td>
</tr>
</tbody>
</table>

**Table 1-3 Parameter description**
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster Version</td>
<td>Display the version of the database instance installed in the cluster.</td>
<td>1.3.0</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The version number is the default one and, as of publication, cannot be changed.</td>
<td></td>
</tr>
<tr>
<td>Default Database</td>
<td>The default database name of the cluster is <strong>postgres</strong>.</td>
<td>postgres</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This name cannot be changed.</td>
<td></td>
</tr>
<tr>
<td>Administrator Account</td>
<td>Set the administrator name of the database.</td>
<td>dbadmin</td>
</tr>
<tr>
<td></td>
<td>The administrator username must:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Consist of lowercase letters, digits, or underscores.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Start with a lowercase letter or an underscore.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Contain 1 to 63 characters.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Cannot be a keyword of the DWS database.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For details about the keywords of the DWS database, see <strong>Keyword</strong> in the <strong>Data Warehouse Service Database Developer Guide</strong>.</td>
<td></td>
</tr>
<tr>
<td>Administrator Password</td>
<td>Set the password of the database administrator account.</td>
<td>Dws2018demo!</td>
</tr>
<tr>
<td></td>
<td>The password complexity requirements are as follows:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Consists of 8 to 32 characters.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Cannot be the same as the username or the username written in reverse order.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Must contain at least 3 of the following character types: uppercase letters, lowercase letters, digits, and special characters -!@#%*(&amp;-+=/{]}::;&lt;&gt;?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Passes the weak password check.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Change the password regularly and keep it secure.</td>
<td></td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Enter the database administrator password again.</td>
<td>Dws2018demo!</td>
</tr>
<tr>
<td>Database Port</td>
<td>Set the port used when the client or application connects to the database in the cluster.</td>
<td>8000</td>
</tr>
<tr>
<td></td>
<td>The port ranges from 8000 to 10000.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 6** Configure network parameters.
Figure 1-3 Network parameters

Table 1-4 Network parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPC</td>
<td>Specify a virtual private network for nodes in a cluster to isolate networks of different services. If you create a data warehouse cluster for the first time and have not configured the VPC, click View VPC. On the VPC management console that is displayed, create a new VPC that satisfies your needs. For details about how to create a VPC, see Creating a VPC in the Virtual Private Cloud User Guide. After selecting a VPC from the drop-down list, click View VPC to enter the VPC management console and view the detailed information about the VPC. You can click to refresh the options in the VPC drop-down list.</td>
<td>vpc-dws</td>
</tr>
<tr>
<td>Subnet</td>
<td>Specify a subnet for the VPC. A subnet provides dedicated network resources that are isolated from other networks, improving network security.</td>
<td>subnet-dws</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Example Value</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Security Group</td>
<td>Specify a security group for the VPC. A security group restricts access rules to enhance security when DWS and other services access each other.</td>
<td>Automatic creation</td>
</tr>
</tbody>
</table>

- Automatically create a security group. If **Automatic creation** is selected, the system automatically creates a default security group. This option is selected by default.

The rule of the default security group is as follows: The outbound allows all access requests, while the inbound is only open to the database port that you set to connect to the data warehouse cluster.

The format of the default security group's name is `dws-<cluster name>-<database port of the data warehouse cluster>`, for example, `dws-dws-demo-8000`.

**NOTE**
If the quotas of the security group and the security group rule are insufficient, an error message will be displayed after you submit the cluster creation application. Select an existing group and retry.

- Manually create and configure a security group.
You can also log in to the VPC management console to manually create a security group. Then, go back to the page for creating data warehouse clusters, click the button next to the **Security Group** drop-down list to refresh the page, and select the new security group.

To enable the DWS client to connect to the cluster, you need to add an inbound rule to the new security group to grant the access permission to the database port of the data warehouse cluster. An example of the inbound rule is as follows:

- **Protocol**: TCP
- **Port**: 8000. Use the database port set when creating the data warehouse cluster. This port is used for receiving client connections to DWS.
- **Source**: Select **IP address** and use the host IP address of the client host, for example, `192.168.0.10/32`. 
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
</table>
| Public Network Access   | Specify whether users can use a client to connect to a cluster's database over the Internet. The following methods are supported:  
  - **Do not use**: The EIP is not required.  
  - **Buy now**: Users specify the bandwidth of the EIP and the system automatically assigns an EIP that exclusively uses bandwidth to each cluster so that users can use the EIP to access the cluster over the Internet.  
  - **Specify**: A specified EIP is bound to the cluster. If no available EIPs are displayed in the drop-down list, click Create EIP to go to the Elastic IP page and create an EIP that satisfies your needs. You can set the bandwidth as needed.  
  
**NOTE**  
If you use the EIP binding function for the first time, the system prompts you to create the DWS/AccessVPC agency to authorize DWS to access VPC. After the authorization is successful, DWS can switch to a healthy VM when the VM bound with the EIP becomes faulty. | Buy now |
| Bandwidth               | When **EIP** is set to **Buy now**, you need to specify the bandwidth of the EIP, which ranges from 1 Mbit/s to 100 Mbit/s.                                                                                             | 50 Mbit/s     |

**Step 7** Configure the enterprise project to which the cluster belongs. You can configure this parameter only when the Enterprise Project Management service is enabled. The default value is **default**.

An enterprise project facilitates project-level management and grouping of cloud resources and users.

You can select the default enterprise project **default** or other existing enterprise projects. To create an enterprise project, log in to the Enterprise Management console. For details, see the Enterprise Management User Guide.

**Step 8** Select either of the following options for **Advanced Settings**:

- **Default**: Indicates that the following advanced settings use the default configurations.
  - **Automated Snapshot**: By default, the policy for automatically generating cluster snapshots is enabled.
  - **CNs**: Two CNs are deployed by default.
  - **Parameter Template**: The default database parameter template is associated with the cluster.
  - **Tag**: By default, no tag is added to the cluster.
  - **Encrypt DataStore**: This parameter is disabled by default, indicating that the database is not encrypted.
Custom: If you select this option, set the following advanced settings:

- **Automated Snapshot**
  
  indicates that the policy is enabled. It is enabled by default. After the automated snapshot policy is enabled, the system automatically creates snapshots based on the preset time and period. When it is enabled, configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Retention Days    | Set the retention days of the snapshots that are automatically created. The value ranges from 1 to 10 days.  
  **NOTE** You cannot delete the snapshots that are automatically created. The system automatically deletes these snapshots when their retention duration expires. |
| Execution Period  | Set the cycle for creating automated snapshots. You can specify several days in a week for creating snapshots, and set the execution frequency. You can have the system to create a snapshot every day or every several hours each day. |

- **CNs**
  
  The coordinator node (CN) receives access requests from the client and returns the execution results back. Then, the CN divides each task into several smaller ones and assigns them to the DNs for execution.

  The value ranges from 2 to the number of cluster nodes minus 1. The maximum value is 5 and the default value is 2. In a large-scale cluster, you are advised to deploy multiple CNs.

- **Parameter Template**
  
  A parameter template is a set of parameters for data warehouses. You need to select a parameter template from the drop-down list and associate it with the cluster during cluster creation. You can select the default parameter template or a customized parameter template.

  For details about parameter templates, see *Managing Parameter Templates*.

- **Tag**
  
  A tag is a key-value pair used to identify a cluster. For details about the keys and values, see *Table 1-6*.

  For more information about tags, see *Tagging Overview*. 
### Table 1-6 Tag parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tag key</td>
<td>You can:</td>
<td>key01</td>
</tr>
</tbody>
</table>
|           | ▪ Select a predefined tag key or an existing resource tag key from the drop-down list of the text box.  
|           |   **NOTE** |               |
|           |   To add a predefined tag, you need to create one on TMS and select it from the drop-down list of Tag key. You can click **View predefined tags** to enter the **Predefined Tags** page of TMS. Then, click **Create Tag** to create a predefined tag.  
|           |   For more information, see **Creating Predefined Tags** in the **Tag Management Service User Guide**.  
|           | ▪ Enter a tag key in the text box. A tag key can contain a maximum of 36 Unicode characters, which cannot be null. The first and last characters cannot be spaces. Cannot contain the following characters: =*<>\,|/  
|           |   **NOTE** |               |
|           |   The key name must be unique in the same cluster. |               |
| Tag value | You can:    | value01        |
|           | ▪ Select a predefined tag value or resource tag value from the drop-down list of the text box.  
|           | ▪ Enter a tag value in the text box. A tag key can contain a maximum of 43 Unicode characters, which can be null. The first and last characters cannot be spaces. Cannot contain the following characters: =*<>\,|/ |               |

#### Encrypt DataStore

- indicates that database encryption is disabled. This function is disabled by default.

- indicates that database encryption is enabled. After this function is enabled, Data Encryption Workshop (DEW) encrypts the cluster and the cluster's snapshot data.

When you enable database encryption for each project in each region for the first time, the system displays a **Create Delegation** dialog box. Click **Yes** to authorize DWS to access KMS and create a KMS basic edition key (this key cannot be used for DWS database encryption). If you click **No**, the encryption function is not enabled. Select the created KMS key from the **KMS Key Name** drop-down list. If no professional edition key is available, you can log in to the DEW console to create one. For details, see the **Data Encryption Workshop User Guide**.
**NOTICE**

- The database encryption function cannot be disabled once it is enabled.
- After the database encryption function is enabled, do not delete or disable the KMS key used to encrypt the DWS cluster. Otherwise, the cluster will become abnormal.

---

**Step 9** Click Next. The Details page is displayed.

**NOTE**

If the number of applied nodes, vCPU (cores), or memory (GB) exceed the user's remaining quota, a warning dialog box is displayed indicating insufficient quota and displaying the detailed remaining quota and the current quota application information. In this case, you can click Increase quota in the warning dialog box to submit a service ticket and apply for higher node quota.

For details about quota, see What Is User Quota?.

**Step 10** Click Submit.

After the submission is successful, the creation starts. Click Back to Cluster List. The cluster management page is displayed. The initial status of the cluster is Creating. Cluster creation takes some time. Wait for a while. After the cluster becomes Available, it is ready for use.

----End

1.3 Buying Yearly/Monthly Packages

DWS also supports yearly/monthly packages. You can make a one-off payment according to the purchased service duration. The service duration ranges from one month to three years. It is economical and recommended for long-term users.

After you purchase a yearly/monthly package, the system will not automatically create a cluster for you. You need to manually create clusters on the DWS management console. For detailed procedures, see Creating a Cluster. If you have created a cluster and then buy a yearly/monthly package that has the same region and node flavor as the cluster, the system automatically associates the package with the cluster. After the yearly/monthly package expires, you will be billed in pay-per-use mode if you continue to use the service. The cluster will not be released. For details and precautions about the yearly/monthly package, see the Billing Modes in the Data Warehouse Service Price Details.

This section describes how to buy DWS in yearly/monthly package mode.

**Buying Yearly/Monthly Packages**

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

**Step 2** Click Buy Yearly/Monthly Package

**Step 3** On the Buy Yearly/Monthly DWS Package page, specify the Region.
### Table 1-7 Region parameter description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region</td>
<td>Select the AZ where nodes in the cluster run. Yearly/Monthly packages in different regions are isolated. Select the region based on your requirements. For more information about the endpoint, visit <a href="#">Regions and Endpoints</a>.</td>
<td>CN North-Beijing1</td>
</tr>
</tbody>
</table>

### Step 4
Set the following cluster parameters. The **Reference Price** of the cluster is displayed at the bottom of the page. You can click [Pricing details](#) to view the charging details.

### Figure 1-4 Selecting a node flavor

![Node flavor selection](image)

### Table 1-8 Flavor parameter description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
</table>
| Cluster Type | DWS cluster types include:  
- **Enterprise-grade**: provides capabilities of querying large amounts of data in batches.  
- **Ultra-high concurrency**: provides capabilities of interactive, highly concurrent queries on small amounts of data with low latency.  

**NOTE**
This parameter can only be viewed by OBT users. | Enterprise-grade |
<p>| Node Flavor | Select CPU and memory resources for each node in the cluster. For more information about the node flavors supported by DWS, see <a href="#">DWS Pricing Details</a>. | dws.dc.4xlarge |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nodes</td>
<td>Select the number of nodes in the cluster.</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>If you purchase a data warehouse cluster for the first time, you are advised to purchase at least three nodes (minimal scale of a cluster). If you are not a first-time user, select the number of nodes as required.</td>
<td></td>
</tr>
<tr>
<td>Validity Period</td>
<td>Drag the <strong>Validity Period</strong> bar to determine the purchase duration.</td>
<td>-</td>
</tr>
</tbody>
</table>

**NOTE**

- Yearly/Monthly nodes are bound to a specific region and flavor. You can get discounts only when the yearly/monthly package you purchase and the nodes you run have the same region and flavor.

**Step 5**  Click **Buy Now**. The **Confirm** page is displayed.

**Step 6**  Confirm the order information and click **Pay Now**.

**Step 7**  Choose either of the following payment modes:

- Choose **Balance** and click **Pay**.
- Choose **Online Payment** and click **Pay**.
- Choose **Request Online Contract and Pay**, fill in the contract content, and click **Create Formal Contract**.

After you purchase a yearly/monthly package, the system will not automatically create a cluster for you. If you have not created a cluster, go to the **DWS management console** to create one. For details, see **Creating a Cluster**.

--- End

### 1.4 Querying Cluster Status Information

On the **Cluster Management** page of the DWS management console, you can view the general information about a cluster in the cluster list, such as the cluster status, task information, recent events, and node flavor.

**Querying General Information of a Cluster**

Log in to the DWS management console. In the navigation tree on the left, click **Cluster Management**. The cluster list displays all clusters. If there are a large number of clusters, you can turn pages to view the clusters in any status.

Enter the cluster name in the search box, and click to search for a cluster. Alternatively, in the **All projects** drop-down list above the cluster list, select the target project. Click to refresh the cluster list. You can also click **Search by Tag** to search for clusters based on filtering criteria. For details, see **Searching for Clusters Based on Tags**.
Clusters are listed in chronological order by default, with the most recent clusters displayed at the top. **Table 1-9** lists the cluster list parameters.

**Figure 1-5 Cluster list**

![Cluster list](#)

**Table 1-9 Cluster list parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster Name</td>
<td>Cluster name specified when a cluster is created.</td>
</tr>
<tr>
<td>Cluster Status</td>
<td>Cluster running status. For details, see <a href="#">Cluster Status</a>.</td>
</tr>
<tr>
<td>Task Information</td>
<td>Cluster task status. For details, see <a href="#">Cluster Task Information</a>.</td>
</tr>
<tr>
<td>Node Flavor</td>
<td>Node flavors of clusters. For details about the node flavors, see <a href="#">DWS Pricing Details</a>.</td>
</tr>
<tr>
<td>Recent Events</td>
<td>Number of recent events in a cluster. You can click the number to view event details.</td>
</tr>
<tr>
<td>Enterprise Project</td>
<td>Enterprise project to which a cluster belongs.</td>
</tr>
</tbody>
</table>

**Operation**

- **View Metric**: For details, see [Monitoring a Cluster](#).
- **Restart**: Click **Restart** to restart a cluster. For details, see [Restarting a Cluster](#).
- **More**
  - **Resize Cluster**: For details, see [Resizing a Cluster](#).
  - **Create Snapshot**: For details, see [Manually Creating a Snapshot](#).
  - **Reset Password**: For details, see [Resetting Passwords](#).
  - **Delete**: Click **Delete** to delete a cluster. For details, see [Deleting a Cluster](#).

**Cluster Status**

**Table 1-10 Cluster status description**

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available</td>
<td>Indicates that the cluster runs properly.</td>
</tr>
<tr>
<td>Status</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Read-only         | A cluster goes into this status when the disk usage of the cluster or a single node in the cluster is greater than 90%. The cluster can still work in this status but supports only query operations. Write operations are not supported. You can contact technical support engineers to cancel the read-only status. After the read-only status is canceled for the cluster, you are advised to perform the following operations:  
  - Use the SQL client tool to connect to the database as the administrator and run the following command to periodically clear and reclaim the storage space:  
    ```sql
    VACUUM FULL;
    ```  
  - After you delete data stored in DWS data warehouses, dirty data may be generated possibly because the disk space is not released. This results in disk space waste. It is recommended that the storage space be cleared periodically.  
  - You are advised to check the disk capacity and analyze whether the existing cluster specifications meet service requirements. If not, expand the cluster capacity. For details, see Resizing a Cluster. |
| Low performance   | A cluster goes into this status when some nodes in the cluster cannot work properly, which has no adverse impact on DWS. The cluster can still work in this status. You can restart the cluster to restore the nodes. For details, see Restarting a Cluster.                                                                                       |
| Redistributing    | A cluster goes into this status when it detects that the service data volume on the original nodes is significantly larger than that on the new node after a new node is added to the cluster. In this case, the system automatically redistributes data on all nodes. The cluster can still work in this status.                                      |
| Redistributing, failed | A cluster goes into this status when data redistribution fails, but no data loss occurs. The cluster can still work in this status. You are advised to contact technical support.                                                                                     |
| Degraded          | A cluster goes into this status when some nodes in the cluster are faulty, but the whole cluster runs properly. You are advised to contact technical support.                                                                                                                                                               |
| Unavailable       | A cluster goes into this status when it cannot provide the database service. You are advised to contact technical support.                                                                                                                                                                                                 |
| Creating          | Indicates that a cluster is being created.                                                                                                                                                                                                                                                                                                    |
| Creation, failed  | Indicates that a cluster fails to be created.                                                                                                                                                                                                                                                                                                |
| Creating, restoring | Indicates that a cluster is being created and it is restored from a snapshot. In this status, the cluster is being restored. A snapshot will be restored to a new cluster. During the process, the new cluster goes into this status.                                                                                     |
| Frozen            | Indicates that a cluster has been frozen.                                                                                                                                                                                                                                                                                                   |
Cluster Task Information

Table 1-11 Task information description

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating snapshot</td>
<td>Indicates that a snapshot is being created in the cluster.</td>
</tr>
<tr>
<td>Snapshot creation failed</td>
<td>Indicates that a snapshot fails to be created.</td>
</tr>
<tr>
<td>Configuring</td>
<td>Indicates that the system is storing modifications of cluster parameters.</td>
</tr>
<tr>
<td>Restarting</td>
<td>Indicates that a cluster is being restarted.</td>
</tr>
<tr>
<td>Restart failed</td>
<td>Indicates that a cluster fails to be restarted.</td>
</tr>
<tr>
<td>Resizing</td>
<td>Indicates that a cluster is being resized.</td>
</tr>
<tr>
<td>Resize failed</td>
<td>Indicates that a cluster fails to be resized.</td>
</tr>
</tbody>
</table>

1.5 Viewing Basic Cluster Information

Log in to the DWS management console. In the navigation tree on the left, click **Cluster Management**. In the cluster list, locate the required cluster and click its name. The **Basic Information** page is displayed.

Figure 1-6 Basic cluster information

On a cluster's **Basic Information** page, you can view the following information:

- **Cluster Information**: Table 1-12 lists the related parameters.
- **Database Attribute**: Table 1-13 lists the related parameters.
- **Node Configuration**: Table 1-14 lists the related parameters.
- **Network**: Table 1-15 lists the related parameters.
- **Data Encryption Information**: Table 1-16 lists the related parameters.

### Table 1-12 Cluster information

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster Name</td>
<td>Cluster name specified when the cluster is created.</td>
</tr>
<tr>
<td>Cluster Status</td>
<td>Cluster running status. For details, see Cluster Status.</td>
</tr>
<tr>
<td>Parameter Configuration Status</td>
<td>Parameter configuration status of a cluster.</td>
</tr>
<tr>
<td>Task Information</td>
<td>Cluster task status. For details, see Cluster Task Information.</td>
</tr>
<tr>
<td>Cluster ID</td>
<td>ID of the cluster.</td>
</tr>
<tr>
<td>Nodes</td>
<td>Number of nodes in the cluster.</td>
</tr>
<tr>
<td>Cluster Version</td>
<td>Cluster version information.</td>
</tr>
<tr>
<td>Used Storage Capacity</td>
<td>Used storage capacity of the cluster.</td>
</tr>
<tr>
<td>Created</td>
<td>Time when the cluster was created.</td>
</tr>
<tr>
<td>Last Snapshot Created</td>
<td>Time when the last snapshot was created.</td>
</tr>
<tr>
<td>Maintenance Window</td>
<td>Maintenance window of the cluster.</td>
</tr>
<tr>
<td></td>
<td>You can click Configure on the right of Maintenance Window to configure the</td>
</tr>
<tr>
<td></td>
<td>maintenance window. For more information, see Configuring the Maintenance</td>
</tr>
<tr>
<td></td>
<td>Window.</td>
</tr>
<tr>
<td>Enterprise Project</td>
<td>Enterprise project to which a cluster belongs. You can click the enterprise</td>
</tr>
<tr>
<td></td>
<td>project name to view and edit it on the console of the Enterprise Project</td>
</tr>
<tr>
<td></td>
<td>service.</td>
</tr>
</tbody>
</table>

### Table 1-13 Database attribute parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Database</td>
<td>Database that is automatically created during cluster creation. When you</td>
</tr>
<tr>
<td></td>
<td>connect to the cluster for the first time, you need to connect to the</td>
</tr>
<tr>
<td></td>
<td>default database.</td>
</tr>
<tr>
<td>Initial Administrator</td>
<td>Administrator user specified during cluster creation. When you connect to</td>
</tr>
<tr>
<td></td>
<td>the cluster for the first time, you need to use the initial administrator</td>
</tr>
<tr>
<td></td>
<td>and password to connect to the default database.</td>
</tr>
<tr>
<td>Port</td>
<td>Port for accessing the cluster database over the public network or private</td>
</tr>
<tr>
<td></td>
<td>network. Database port specified during cluster creation. It is used to</td>
</tr>
<tr>
<td></td>
<td>listen to client connections.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>JDBC URL (Private Network)</td>
<td>In the private network environment, you can use the JDBC URL (private network) to connect to the cluster when developing applications.</td>
</tr>
<tr>
<td>JDBC URL (Public Network)</td>
<td>In the public network environment, you can use the JDBC URL (public network) to connect to the cluster when developing applications.</td>
</tr>
<tr>
<td>Private Network Domain Name</td>
<td>Name of the domain for accessing the database in the cluster through the private network. The private network domain address is automatically generated when you create a cluster. The default naming rule is <code>cluster name.dws.myhuaweicloud.com</code>.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong></td>
</tr>
<tr>
<td></td>
<td>If the cluster name does not comply with the domain name standards, the prefix of the default access domain name will be adjusted accordingly.</td>
</tr>
<tr>
<td></td>
<td>Click <strong>Modify</strong> to change the private network access domain name. The access domain name contains 4 to 63 characters, which consist of letters, digits, and hyphens (-), and must start with a letter. For more information, see <strong>Managing Access Domain Names</strong>.</td>
</tr>
<tr>
<td>Private Network IP Address</td>
<td>IP address for accessing the database in the cluster through the private network. The private network address is automatically generated when you create a cluster.</td>
</tr>
<tr>
<td>Public Network Domain Name</td>
<td>Name of the domain for accessing the database in the cluster through the public network.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong></td>
</tr>
<tr>
<td></td>
<td>• If you have not bound an EIP to the cluster, Public Network IP Address, Public Network Port, and Public Network Domain Name are left blank.</td>
</tr>
<tr>
<td></td>
<td>• If you bind an EIP during cluster creation, the public network domain name is automatically generated. The default naming rule is <code>cluster name.dws.huaweiclouds.com</code>.</td>
</tr>
<tr>
<td></td>
<td>• Bind an EIP to the cluster before binding the public network domain name to the cluster. Click <strong>Create</strong> to bind the public network domain name to the cluster.</td>
</tr>
<tr>
<td></td>
<td>• You can click <strong>Modify</strong> to modify the public network domain name bound to the cluster. The domain name contains 4 to 63 characters, which consist of letters, digits, and hyphens (-), and must start with a letter.</td>
</tr>
<tr>
<td></td>
<td>• You can click <strong>Release</strong> to release the public network domain name bound to the cluster.</td>
</tr>
<tr>
<td></td>
<td>For more information, see <strong>Managing Access Domain Names</strong>.</td>
</tr>
<tr>
<td>Public Network IP Address</td>
<td>IP address for accessing the database in the cluster through the public network.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong></td>
</tr>
<tr>
<td></td>
<td>• If no EIP is assigned during cluster creation and Public Network IP Address is empty, click <strong>Bind EIP</strong> to bind an EIP to the cluster.</td>
</tr>
<tr>
<td></td>
<td>• If an EIP is bound during cluster creation, click <strong>Unbind EIP</strong> to unbind the EIP.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>ODBC URL</td>
<td>In DWS, you can use an ODBC driver to connect to the database. The drivers can connect to the database through the ECS in the public cloud or over the Internet.</td>
</tr>
</tbody>
</table>

### Table 1-14 Node configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node Flavor</td>
<td>Node flavor of the cluster.</td>
</tr>
<tr>
<td>Node Specifications</td>
<td>Specifications of the node flavor.</td>
</tr>
</tbody>
</table>

### Table 1-15 Network

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region</td>
<td>Current working zone of the cluster.</td>
</tr>
<tr>
<td>AZ</td>
<td>AZ selected during cluster creation.</td>
</tr>
<tr>
<td>VPC</td>
<td>VPC selected during cluster creation. A VPC is a secure, isolated, and logical network environment.</td>
</tr>
<tr>
<td>Subnet</td>
<td>Subnet selected during cluster creation. A subnet provides dedicated network resources that are isolated from other networks, improving network security.</td>
</tr>
<tr>
<td>Security Group</td>
<td>Security group selected during cluster creation.</td>
</tr>
</tbody>
</table>

### Table 1-16 Data encryption information

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>KMS Key Name</td>
<td>Indicates the database encryption key of the cluster when Encrypt DataStore is enabled.</td>
</tr>
<tr>
<td>Last Key Rotation Time</td>
<td>Indicates the time when the last encryption key is rotated when Encrypt DataStore is enabled.</td>
</tr>
</tbody>
</table>

### 1.6 Managing Clusters That Fail to Be Created

If a cluster fails to be created, you can go to the Cluster Management page of the DWS management console to view the cluster status and the cause of failure.
Checking the Cause of a Creation Failure

Step 1  Log in to the DWS management console and click Cluster Management in the left navigation pane to enter the Cluster Management page.

Step 2  In the cluster list, locate the cluster whose Cluster Status is Creation failed.

Step 3  Click 🟢 in the Cluster Status column to view the cause of the creation failure.

You can refer to Error Code Description to rectify the fault based on the error code displayed with the cause of failure. If the fault persists, contact technical support engineers.

----End

Deleting a Cluster That Fails to Be Created

You can delete a cluster that fails to be created if you do not need it. Before deleting a failed cluster, you are advised to check the cause of creation failure.

Step 1  Log in to the DWS management console and click Cluster Management in the left navigation pane to enter the Cluster Management page.

Step 2  In the cluster list, locate the row containing the failed cluster to be deleted, and choose More > Delete.

Step 3  (Optional) If the cluster is bound with an EIP during creation, you can click Release the EIP bound with the cluster to release the EIP.

Step 4  In the dialog box that is displayed, click Yes to delete the cluster.

If the cluster to be deleted uses an automatically created security group that is not used by other clusters, the security group is automatically deleted when the cluster is deleted.

----End

1.7 Managing Access Domain Names

Overview

A domain name is a string of characters separated by dots to identify the location of a computer or a computer group on the Internet, for example, www.example.com. You can enter a domain name in the address box of the web browser to access a website or web application.

On DWS, you can access clusters using the private network domain name or the public network domain name.

Private network domain name: Name of the domain for accessing the database in the cluster through the private network. The private network domain name is automatically generated when you create a cluster. The default naming rule is cluster name.dws.myhuaweicloud.com. If the cluster name does not comply with the domain name standards, the prefix of the default access domain name will be adjusted accordingly.

Public network domain name: Name of the domain for accessing the database in the cluster through the public network. If a cluster is not bound to an EIP, it cannot be accessed using the Public Network Domain Name. If you bind an EIP during cluster creation, the public
network domain name is automatically generated. The default naming rule is \textit{cluster name.dws.huaweiclouds.com}.

After a cluster is created, you can set private and public domain names for accessing the cluster as required. The operations are as follows:

- Modifying a Private Network Domain Name
- Creating a Public Network Domain Name
- Modifying a Public Network Domain Name
- Releasing a Public Network Domain Name

\section*{Modifying a Private Network Domain Name}

The private network domain name is automatically generated during cluster creation. After the cluster is created, you can modify the default domain name based on site requirements.

To modify the private network domain name, perform the following steps:

\textbf{Step 1} Log in to the management console at \url{https://console.huaweicloud.com/dws/?locale=en-us}.

\textbf{Step 2} In the navigation tree on the left, click \textbf{Cluster Management}.

\textbf{Step 3} In the cluster list, find the target cluster and click the cluster name. The \textbf{Basic Information} page is displayed.

\textbf{Step 4} In the \textbf{Database Attribute} area, click \textbf{Modify} next to the automatically generated \textbf{Private Network Domain Name}.

\textbf{Figure 1-7} Viewing the private network domain name

\textbf{Step 5} In the \textbf{Modify Private Network Domain Name} dialog box, enter the target domain name and click \textbf{OK}.

\textbf{Figure 1-8} Modifying the private network domain name

\begin{center}
\textit{Modify Private Network Domain Name}
\end{center}

The private network domain name contains 4 to 63 characters, which consist of letters, digits, and hyphens (-). It must start with a letter.
After the domain name is modified, click copy button next to the private network domain name to copy it.

----End

Creating a Public Network Domain Name

A cluster is not bound to an EIP by default during cluster creation. That is, cluster access using the public network is disabled. After a cluster is created, if you want to access it through the public network, bind an EIP to the cluster and create a public network domain name.

To create a public network domain name, perform the following steps:

Step 1 Log in to the management console at https://console.huaweicloud.com/dws/?locale=en-us.

Step 2 In the navigation tree on the left, click Cluster Management.

Step 3 In the cluster list, find the target cluster and click the cluster name. The Basic Information page is displayed.

Step 4 In the Database Attribute area, Public Network Domain Name and Public Network IP Address are empty. Click Bind EIP to bind the cluster with an EIP.

Step 5 Select an EIP from the drop-down list in the Bind EIP dialog box.

If no available EIPs are displayed, click View EIP to go to the Elastic IP page and create an EIP that satisfies your needs. After the new EIP is created, click the refresh icon next to the drop-down list. The newly created EIP will be displayed in the EIP drop-down list.

After the EIP is bound successfully, the specific public network IP address is displayed in the Database Attribute area.

Figure 1-9 Binding an EIP

![Bind EIP](image)

Step 6 In the Database Attribute area, click Create next to Public Network Domain Name to create a public network domain name for the cluster.

Step 7 In the Apply for Public Network Domain Name dialog box, enter the target domain name and click OK.
Figure 1-10 Applying for a public network domain name

**Apply for Public Network Domain Name**

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>dws-demo .dws.huaweicloud.com</th>
</tr>
</thead>
</table>

Enter 4 to 63 characters. Only letters, digits, and hyphens (-) are allowed. The value must start with a letter.

| OK | Cancel |

The public network domain name contains 4 to 63 characters, which consist of letters, digits, and hyphens (-). It must start with a letter.

The specific public network domain name is displayed in the **Database Attribute** area after being created. Click copy button to copy the public network domain name.

----End

Modifying a Public Network Domain Name

If you bind an EIP during cluster creation, the public network domain name is automatically generated. After a cluster is created, you can modify the public network domain name as required.

To modify the public network domain name, perform the following steps:

**Step 1** Log in to the management console at [https://console.huaweicloud.com/dws/?locale=en-us](https://console.huaweicloud.com/dws/?locale=en-us).

**Step 2** In the navigation tree on the left, click **Cluster Management**.

**Step 3** In the cluster list, find the target cluster and click the cluster name. The **Basic Information** page is displayed.

**Step 4** Click **Modify** next to the **Public Network Domain Name** in the **Database Attribute** area.

**Step 5** In the **Modify Public Network Domain Name** dialog box, enter the target domain name and click **OK**.

Figure 1-11 Modifying the public network domain name

**Modify Public Network Domain Name**

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>dws-demo .dws.huaweicloud.com</th>
</tr>
</thead>
</table>

Enter 4 to 63 characters. Only letters, digits, and hyphens (-) are allowed. The value must start with a letter.

| OK | Cancel |

----End
Releasing a Public Network Domain Name

After a cluster is created, you can release unnecessary public network domain names. To do so, perform the following steps:

Step 1  Log in to the management console at https://console.huaweicloud.com/dws/?locale=en-us.

Step 2  In the navigation tree on the left, click Cluster Management.

Step 3  In the cluster list, find the target cluster and click the cluster name. The Basic Information page is displayed.

Step 4  Click Release next to the Public Network Domain Name in the Database Attribute area.

Step 5  In the Release Domain Name dialog box, click Yes.

    ----End

1.8 Modifying Parameters

After a cluster is created, you can modify its database parameters as required. For details about the database parameters that can be modified, see Parameter Description.

You can modify parameters only when the cluster status is Available or Low performance and the task information is not in the Creating snapshot, Scaling out, Configuring, or Restarting state.

Modifying Parameters

Step 1  Log in to the management console at https://console.huaweicloud.com/dws/?locale=en-us.

Step 2  In the navigation tree on the left, click Cluster Management.

Step 3  In the cluster list, find the target cluster and click the cluster name. The Basic Information page is displayed.

Step 4  Click the Parameter Modifications tab and modify the parameter values. Then click Save.

Step 5  In the Modification Preview dialog box, confirm the modifications and click Save.

    ----End

1.9 Configuring Cluster Security Settings

1.9.1 Separating Rights of Roles

Scenario

By default, the administrator user created during data warehouse cluster creation is a database system administrator, who can create other users and view the audit logs of the database. The rights separation mode is disabled.

To protect cluster data, DWS supports separation of rights of roles so that different roles have different rights.
For details about the default permission model and the permission model with rights separation enabled, see *Separation of Duties* in the *Data Warehouse Service Database Developer Guide*.

**Impact on the System**

After you have modified the security parameters and the modifications take effect, the cluster may be restarted, which makes the cluster unavailable temporarily.

**Prerequisites**

To modify the cluster's security configuration, ensure that the following conditions are met:

- The Cluster Status is Available or Low performance.
- The Task Information cannot be Creating snapshot, Scaling out, Configuring, or Restarting.

**Procedure**

**Step 1** Log in to the management console at [https://console.huaweicloud.com/dws/?locale=en-us](https://console.huaweicloud.com/dws/?locale=en-us).

**Step 2** In the navigation tree on the left, click Cluster Management.

**Step 3** In the cluster list, click the name of a cluster. On the page that is displayed, click Security Settings.

By default, Configuration Status is Synchronized, which indicates that the latest database result is displayed.

**Step 4** On the Security Settings page, set rights separation.

- Indicates that Rights Separation is enabled. After Rights Separation is enabled, set the usernames and passwords of the Security Administrator and Audit Administrator. The system automatically creates the two users. You can use the two users to connect to the databases and perform database-related operations.

- Indicates that Rights Separation is disabled. By default, Rights Separation is disabled.
Figure 1-12 Security configuration

Table 1-17 Security parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Administrator</td>
<td>The administrator username must:</td>
<td>security_admin</td>
</tr>
<tr>
<td></td>
<td>• Consist of lowercase letters, digits, or underscores.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Start with a lowercase letter or an underscore.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Contain 1 to 63 characters.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Cannot be a keyword of the DWS database. For details about the keywords</td>
<td></td>
</tr>
<tr>
<td></td>
<td>of the DWS database, see <strong>Keyword</strong> in the <em>Data Warehouse Service</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Database Developer Guide</em>.</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>The password complexity requirements are as follows:</td>
<td>Dws_2018!</td>
</tr>
<tr>
<td></td>
<td>• Consists of 8 to 32 characters.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Cannot be the same as the username or the username written in reverse</td>
<td></td>
</tr>
<tr>
<td></td>
<td>order.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Must contain at least 3 of the following character types:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>uppercase letters, lowercase letters, digits, and special characters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>~!@#$%^&amp;*()-_=+</td>
<td>{[]};:&lt;,&gt;/?</td>
</tr>
<tr>
<td></td>
<td>• Passes the weak password check.</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Example Value</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Enter the password of the security administrator again.</td>
<td>-</td>
</tr>
<tr>
<td>Audit Administrator</td>
<td>The administrator username must:&lt;br&gt;• Consist of lowercase letters, digits, or underscores.&lt;br&gt;• Start with a lowercase letter or an underscore.&lt;br&gt;• Contain 1 to 63 characters.&lt;br&gt;• Cannot be a keyword of the DWS database. For details about the keywords of the DWS database, see <strong>Keyword</strong> in the <em>Data Warehouse Service Database Developer Guide</em>.</td>
<td>audit_admin</td>
</tr>
</tbody>
</table>
| Password | The password complexity requirements are as follows:<br>• Consists of 8 to 32 characters.<br>• Cannot be the same as the username or the username written in reverse order.<br>• Must contain at least 3 of the following character types: uppercase letters, lowercase letters, digits, and special characters ~!@#%^&*()-_=+|\[
{|};,:<.>/?\[
| Confirm Password | Enter the password of the audit administrator again.                        | -             |

**Step 5** Click **Apply**.

**Step 6** In the displayed **Save Configuration** dialog box, select or deselect **Restart the cluster** and click **Yes**.

- If you select **Restart the cluster**, the system saves the settings on the **Security Settings** page and restarts the cluster immediately. After the cluster is restarted, the security settings take effect immediately.

- If you do not select **Restart the cluster**, the system only saves the settings on the **Security Settings** page. Later, you need to manually restart the cluster for the security settings to take effect.

After the security settings are complete, **Configuration Status** can be one of the following on the **Security Settings** page:

- **Applying**: The system is saving the settings.
- **Synchronized**: The settings have been saved and taken effect.
- **Take effect after restart**: The settings have been saved but have not taken effect. Restart the cluster for the settings to take effect.

----End
1.10 Encrypting Databases

1.10.1 Database Encryption Overview

Encrypting DWS Databases

In DWS, you can enable database encryption for a cluster to protect static data. After you enable encryption, data of the cluster and its snapshots is encrypted. Encryption is an optional and immutable setting that can be configured during cluster creation. To encrypt an unencrypted cluster (or in reverse), you need to export all data from the unencrypted cluster and import it to a new cluster that has enabled database encryption.

If encryption is required, enable it during cluster creation. Although encryption is an optional setting of DWS, you are advised to enable this setting for clusters to protect data.

Using KMS to Encrypt DWS Databases

When you choose KMS to manage DWS keys, a three-layer key management structure is adopted, including the cluster master key (CMK), cluster encryption key (CEK), and database encryption key (DEK).

- The CMK is used to encrypt the CEK and is stored in KMS.
- The CEK is used to encrypt the DEK. The CEK plaintext is stored in the data warehouse cluster's memory, and the ciphertext is stored in DWS.
- The DEK is used to encrypt database data. The DEK plaintext is stored in the data warehouse cluster's memory, and the ciphertext is stored in DWS.

The procedure of using the keys is as follows:

1. You choose a CMK.
2. DWS randomly generates the CEK and DEK plaintext.
3. KMS uses the CMK you choose to encrypt the CEK plaintext and imports the encrypted CEK ciphertext to DWS.
4. DWS uses the CEK plaintext to encrypt the DEK plaintext and saves the encrypted DEK ciphertext.
5. DWS transfers the DEK plaintext to the cluster and loads it to the cluster's memory.

When the cluster is restarted, it automatically requests the DEK plaintext from DWS through an API. DWS loads the CEK and DEK ciphertext to the cluster's memory, invokes KMS to decrypt the CEK using the CMK, loads the CEK to the memory, decrypts the DEK using the CEK plaintext, loads the DEK to the memory, and returns it to the cluster.

Rotating Encryption Keys

Encryption key rotation is used to update the ciphertext stored on DWS. On DWS, you can rotate the encrypted CEK of an encrypted cluster.

The procedure of rotating the keys is as follows:
1. The DWS cluster starts key rotation.
2. DWS decrypts the CEK ciphertext stored on DWS based on the CMK to obtain the CEK plaintext.
3. Use the obtained CEK plaintext to decrypt the DEK ciphertext in DWS to obtain the DEK plaintext.
4. DWS randomly generates new CEK plaintext.
5. DWS uses the new CEK plaintext to encrypt the DEK and saves the encrypted DEK ciphertext.
6. Use the CMK to encrypt the new CEK plaintext and import the encrypted CEK ciphertext to DWS.

You can plan the key rotation interval based on the service requirements and data type. To improve data security, you are advised to periodically rotate the keys to prevent the keys from being cracked. Once you find that your keys may have been disclosed, rotate the keys in time.

**NOTE**
- When DWS rotates the cluster's CEK, snapshots of the cluster do not need CEK rotation, because the CEK is not stored in snapshots. The CEK plaintext is stored in the DWS cluster memory, and the ciphertext is stored in DWS.
- The DEK is not updated during key rotation, so data encryption and decryption are not affected.

**Constraints**
- The database encryption function cannot be disabled once it is enabled.
- After the database encryption function is enabled, do not delete or disable the KMS key used to encrypt the DWS cluster. Otherwise, the cluster will become abnormal.

### 1.10.2 Rotating Encryption Keys

If you have enabled the Encrypt DataStore function in Advanced Settings during cluster creation, you can rotate the encryption keys for the cluster after the cluster is created successfully. Each key rotation will update the CEK once. During the key rotation, the cluster is still in Available status.

**Rotating Encryption Keys for Data Warehouse Clusters**

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

**Step 2** In the navigation tree on the left, click **Cluster Management**.

**Step 3** In the cluster list, find the target cluster and click the cluster name. The Basic Information page is displayed.

**Step 4** In the Data Encryption Information area, click **Key Rotation**.

![Rotating encryption keys](image)
Step 5  In the dialog box that is displayed, click Yes.

----End

1.11 Managing Tags

1.11.1 Tagging Overview

A tag is a key-value pair customized by users and used to identify cloud resources. It helps users to classify and search for cloud resources.

Tags are composed of key-value pairs.

- A key in a tag can have multiple values.
- A cloud resource must have a unique key.

On DWS, after creating a cluster, you can add identifiers to items such as the project name, service type, and background information using tags. If you use tags in other cloud services, you are advised to create the same tag key-value pairs for cloud resources used by the same business to keep consistency.

DWS supports the following two types of tags:

- Resource tags
  Non-global tags created on DWS
- Predefined tags
  Predefined tags created on Tag Management Service (TMS). Predefined tags are global tags.
  For details about predefined tags, see the Tag Management Service User Guide.

On DWS, tags can be added to the following resources:

- Cluster
  Tags can be added to a cluster when the cluster is being created or after it is successfully created. You can search for the cluster in the cluster list using tags.
  Each cluster can have a maximum of 10 tags added to it.
  After you add tags to a cluster and then create a snapshot for the cluster, the tags cannot be restored if you use the snapshot to restore the cluster. Instead, you need to add tags again.
  When a cluster is deleted, non-predefined tags associated with the cluster are also deleted. Predefined tags need to be deleted on TMS.

1.11.2 Tag Management

This section describes how to search for clusters based on tags and how to add, modify, and delete tags for clusters.

Searching for Clusters Based on Tags

If tags have been added to a cluster, you can search for the cluster by setting tag filtering conditions to quickly find it.
Step 1  Log in to the management console at https://console.huaweicloud.com/dws/?locale=en-us.

Step 2  Click Cluster Management.

Step 3  Click Search by Tag on the upper right of the cluster list to expand the tab page.

**Figure 1-14 Search by tag**

Step 4  In the Search by Tag area, click the Tag Key text box to select a tag key from the drop-down list and then click the Tag Value text box to select the corresponding tag value.

You can only enter a tag key or value that exists in the drop-down list. If no tag key or value is available, create a tag for the cluster. For details, see Adding a Tag to a Cluster.

Step 5  Click † to add the selected tag to the area under the text boxes.

- Select another tag in the text boxes and click † to generate a tag combination for cluster search. You can add a maximum of 10 tags to search for data warehouse clusters. If you specify more than one tag, clusters containing all the specified tags will be displayed.
- To delete an existing tag, click next to the tag.
- You can click Reset to clear all added tags.

**Figure 1-15 Adding the tag key and value**

Step 6  Click Search. The target cluster will be displayed in the cluster list.

----End

Adding a Tag to a Cluster

Step 1  On the Cluster Management page, click the name of the cluster to which a tag is to be added, and click the Tags tab.
Step 2 Click **Add Tag**. The **Add Tag** dialog box is displayed.

Step 3 Configure the tag parameters in the **Add Tag** dialog box.

**Figure 1-16** Tags page

![Tags page](image)

**Figure 1-17** Adding a tag to a cluster

**Add Tag**

It is recommended that you use TMS’s predefined tag function to add the same tag to different cloud resources. [View predefined tags](#)

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>key01</td>
<td>value01</td>
</tr>
</tbody>
</table>

Delete

Tag key

Tag value

You can add 9 more tags.

**Table 1-18** Tag parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tag key</td>
<td>You can:</td>
<td>key01</td>
</tr>
<tr>
<td></td>
<td>● Select a predefined tag key or an existing resource tag key from the drop-down list of the text box.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong> To add a predefined tag, you need to create one on TMS and select it from the drop-down list of <strong>Tag key</strong>. You can click <a href="#">View predefined tags</a> to enter the <strong>Predefined Tags</strong> page of TMS. Then, click <strong>Create Tag</strong> to create a predefined tag. For more information, see <a href="#">Creating Predefined Tags</a> in the Tag Management Service User Guide.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Enter a tag key in the text box. A tag key can contain a maximum of 36 Unicode characters, which cannot be null. The first and last characters cannot be spaces. Cannot contain the following characters: =*&lt;&gt;,</td>
<td>/</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong> The key name must be unique in the same cluster.</td>
<td></td>
</tr>
</tbody>
</table>
### Modifying a Tag

**Step 1** On the [Cluster Management](#) page, click the name of the cluster to which a tag is to be modified, and click the **Tags** tab.

**Step 2** Locate the row that contains the tag to be modified, click **Edit** in the **Operation** column. The [Edit Tag](#) dialog box is displayed.

![Figure 1-18 Editing a tag](#)

**Step 3** Enter the new key value in the **Value** text box.

**Step 4** Click **OK**.

---End

### Deleting a Tag

**Step 1** On the [Cluster Management](#) page, click the name of the cluster to which a tag is to be deleted, and click the **Tags** tab.
Step 2  Locate the row that contains the tag to be deleted, click **Delete** in the **Operation** column. The **Delete Tag** dialog box is displayed.

**Figure 1-19** Deleting a tag

![Delete Tag Dialog Box](image)

Step 3  Click **Yes** to delete the tag.

---End

1.12 Managing Enterprise Projects

The enterprise project is a cloud resource management mode. Enterprise Management provides users with comprehensive management on cloud-based finance. Different from common management consoles that feature independent control and configuration of cloud products, the Enterprise Management console is oriented to resource management, helping enterprises manage cloud-based finance in a hierarchical manner, such as management of companies, departments, and projects.

Users who have enabled the Enterprise Project Management service can use it to manage cloud service resources.

**Binding an Enterprise Project**

You can select an enterprise project during cluster creation to associate it with the cluster. For details, see [Creating a Cluster](#). The **Enterprise Project** drop-down list displays the projects you created. In addition, the system has a built-in enterprise project (**default**). If you do not select an enterprise project for the cluster, the default project is used.

Note that the Enterprise Project Management service is still in the OBT. Only users with the OBT permission can set enterprise projects. Common users cannot view the enterprise project information.

During cluster creation, if the cluster is successfully bound to an enterprise project, the cluster will be successfully created. If the binding fails, the system sends an alarm and the cluster fails to be created.
Snapshots of a cluster retain the association between the cluster and its enterprise project. When the cluster is restored, the association is also restored.

When you delete a cluster, the association between the cluster and its enterprise project is automatically deleted.

**Viewing Enterprise Projects**

After a cluster is created, you can view the associated enterprise project in the cluster list and Basic Information page. You can query only the cluster resources of the project on which you have the access permission.

In the cluster list on the Cluster Management page, view the enterprise project to which the cluster belongs.

**Figure 1-20** Viewing the enterprise project

In the cluster list, find the target cluster and click the cluster name. The Basic Information page is displayed, on which you can view the enterprise project associated with the cluster. Click the enterprise project name to view and edit it on the Enterprise Management console.

**Figure 1-21** Viewing the enterprise project

When querying the resource list of a specified project on the Enterprise Management console, you can also query the DWS resources.

**Searching for Clusters by Enterprise Project**

Log in to the DWS management console, choose Cluster Management, click All projects above the cluster list, and select the required project name from the drop-down list to view all clusters associated with the project.

**Figure 1-22** Searching for clusters by enterprise project
Migrating a Cluster to or Out of an Enterprise Project

A data warehouse cluster can be associated with only one enterprise project. After a cluster is created, you can migrate it from its current enterprise project to another one on the Enterprise Management console, or migrate the cluster from another enterprise project to a specified enterprise project. After the migration, the cluster is associated with the new enterprise project. The association between the cluster and the original enterprise project is automatically released.

For details about how to add resources to an enterprise project, see Adding Resources to an Enterprise Project in the Enterprise Management User Guide.

For details about how to remove resources from an enterprise project, see Removing Resources from an Enterprise Project in the Enterprise Management User Guide.

Enterprise Project-Level Authorization

If permissions preset in the system cannot meet requirements, you can customize policies and grant the policies to user groups for refined access control. As an independent managed object, the enterprise project can be bound to a user group, and the customized policy can be granted to the user group. This implements refined authorization at the enterprise project level.

Step 1 Log in to the IAM console and create a custom policy.

For details, see Creating a Custom Policy.

Step 2 Click Enterprise in the upper right corner of the management console to enter the Enterprise Management console.

Step 3 Choose Personnel Management > User Group Management in the left navigation tree. Then, create a user group and add users to it, add the user group to a project, and grant the newly created custom policy to the group so that users in the group can obtain the permissions defined by the policy.

For details, see Managing User Groups in the Enterprise Management User Guide.

----End

1.13 Resetting Passwords

DWS allows you to reset the password of the administrator. If the administrator forgets the password or the account is locked because the number of consecutive incorrect password attempts reaches the upper limit, the administrator can reset the password on the Cluster Management page. After the password is reset, the account can be automatically unlocked. You can set the maximum number of incorrect password attempts (10 by default) by configuring the failed_login_attempts parameter on the Parameter Modifications tab of the cluster. For details, see Modifying Parameters.

Resetting a Password

Step 1 Log in to the management console at https://console.huaweicloud.com/dws/?locale=en-us.

Step 2 Click Cluster Management.
Step 3  In the Operation column of the target cluster, choose More > Reset Password.

**Figure 1-23** Password resetting

![Reset Password form]

Step 4  On the displayed Reset Password page, set a new password, confirm the password, and then click OK.

The password complexity requirements are as follows:

- Consists of 8 to 32 characters.
- Cannot be the same as the username or the username written in reverse order.
- Must contain at least 3 of the following character types: uppercase letters, lowercase letters, digits, and special characters ~!@#$%^&*()-_=+|{}';:,<.>/?.
- Passes the weak password check.
- Be different from the old password and cannot be the reverse of the old password.
- Cannot use a history password.

**NOTE**

If the default administrator account of the cluster is deleted or renamed, password resetting fails.

----End

### 1.14 Resizing a Cluster

As your data warehouse capacity and performance requirements change, you can adjust the sizes of existing clusters on the management console to make full use of computing and storage resources provided by DWS.

- A cluster of versions earlier than 1.5.0 can be scaled out only by adding nodes, and the flavor of added nodes must be the same as that of original nodes in the cluster. For details, see Scaling Out a Cluster.
For a cluster of version 1.5.0 or later, you can adjust its size by changing the number of nodes or node flavor. For details, see Resizing a Cluster.

**NOTE**

The newly added nodes are charged in pay-per-use mode by default. You can purchase yearly/monthly nodes matching the newly added nodes in terms of node quantity and node flavor so that the new nodes are charged at preferential prices.

**Impact on the System**

- Before resizing a cluster, exit the client connections that have created temporary tables because temporary tables created during cluster resizing will become invalid and operations performed on these temporary tables will fail. Temporary tables created after cluster resizing are not affected.

- After the cluster resizing operation is performed, the cluster automatically takes a snapshot. After the snapshot is created, the cluster is resized.

- When a cluster is being resized, functions such as cluster restart, resizing, snapshot creation, administrator password resetting, and cluster deletion are disabled.

- During cluster resizing, the cluster automatically restarts. Therefore, the cluster stays **Unavailable** for a period of time. After the cluster is restarted, it becomes **Available**. During the last stage of cluster resizing, the system dynamically distributes user data in the cluster to all nodes. During the distribution, the cluster is in the **Read-only** status and data cannot be written to it.

  Do not perform queries that take more than 20 minutes during the redistribution (The default time for applying for the write lock during redistribution is 20 minutes). Otherwise, data redistribution may fail due to timeout when waiting for locking.

- If a new snapshot is created for the cluster that has been resized, the new snapshot contains data on the newly added nodes.

- If the cluster resizing fails, the database automatically performs the rollback operation in the background so that the number of nodes in the cluster can be restored to that before the resizing.
  - If the rollback is successful and the cluster can be normally used, you can perform **Resize Cluster** again. If the resizing still fails, contact the technical support.
  - If the database fails to be rolled back due to some exceptions, the cluster may become **Unavailable**. In this case, you cannot **Resize Cluster** or restart the cluster. Contact the technical support.

**Prerequisites**

- The cluster to be resized is in the **Available**, **Read-only**, or **Low performance** state.

- If the cluster version is earlier than 1.5.0, ensure that the following conditions are met:
  - The number of existing nodes in the cluster for which you want to resize must be less than or equal to 29.

    If the number is greater than 29, you can click **Service Tickets > Create Service Ticket** in the upper right corner of the management console to increase the node quota. A cluster can house a maximum of 256 nodes.

    - The number of nodes to be added must be less than or equal to the available nodes. Otherwise, the system will prompt a message indicating that resizing is not allowed. You can view the number of available nodes on the **Cluster Management** page.
Scaling Out a Cluster

**NOTE**
- A cluster becomes read-only during scale-out. Exercise caution when performing this operation.
- To ensure data security, you are advised to create a snapshot before the scale-out. For details about how to create a snapshot, see Manually Creating a Snapshot.

A cluster of versions earlier than 1.5.0 can be scaled out only by adding nodes. The procedure is described as follows:

**Step 1** Log in to the management console at [https://console.huaweicloud.com/dws/?locale=en-us](https://console.huaweicloud.com/dws/?locale=en-us).

**Step 2** Click Cluster Management.

All clusters are displayed by default.

**Step 3** In the Operation column of the cluster for which you want to scale out, choose More > Scale Out.

The scale-out page is displayed.

**Figure 1-24 Cluster scale-out**

**Step 4** In the Scaled-Out to spin box, specify the number of nodes in the cluster.
- After the scale-out, the cluster's node quantity must be at least three nodes more than the original quantity. The maximum number of nodes that can be added depends on the available quota. In addition, the number of nodes after the scale-out cannot exceed 32. If the node quota is insufficient, click Increase quota to submit a service ticket and apply for higher node quota.
- If you have yearly/monthly nodes that meet service requirements, you are advised to use these nodes first to save costs. If no yearly/monthly nodes are available, click Buy Yearly/Monthly Package.
- Flavor of the new nodes must be the same as that of existing nodes in the cluster.
- The VPC, subnet, and security group of the cluster with new nodes added are the same as those of the original cluster.

**Step 5** Click Scale Out Now.

**Step 6** Click Submit.
- After the scale-out application is submitted, Task Status of the cluster changes to Scaling out. The scale-out will take several minutes. During the scale-out, the cluster
automatically restarts. Therefore, **Cluster Status** stays **Unavailable** for a period of time. After the cluster is restarted, the status becomes **Available**. During the last stage of the scale-out, the system dynamically distributes user data in the cluster. During the distribution, the cluster is in the **Read-only** status.

- Nodes can be successfully added to the cluster only when **Cluster Status** is **Available** and **Scaling out** is not displayed in **Task Information** any more. Then the cluster begins providing services.
- If **Task Information** of the cluster is **Scale-out failed**, the cluster scale-out fails.

----End

**Resizing a Cluster**

**NOTE**

- In the data redistribution phase of cluster resizing, a cluster becomes read-only and the connection is interrupted for a short period of time. Therefore, exercise caution when performing this operation.
- To ensure data security, you are advised to create a snapshot before the scale-out. For details about how to create a snapshot, see **Manually Creating a Snapshot**.

If the version of a cluster is 1.5.0 or later, you can resize it by adjusting the number of nodes or node flavor. That is, you can increase or decrease the number of nodes in the cluster or select a new node flavor for the cluster. The detailed procedure is as follows:

**Step 1** Log in to the management console at [https://console.huaweicloud.com/dws/?locale=en-us](https://console.huaweicloud.com/dws/?locale=en-us).

**Step 2** Click **Cluster Management**.

**Step 3** In the cluster list, locate the row that contains the cluster to be resized, and choose **More > Resize Cluster**.

The page for resizing the cluster is displayed.

**Figure 1-25 Resizing a cluster**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Log in to the management console at <a href="https://console.huaweicloud.com/dws/?locale=en-us">https://console.huaweicloud.com/dws/?locale=en-us</a>.</td>
</tr>
<tr>
<td>2</td>
<td>Click <strong>Cluster Management</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>In the cluster list, locate the row that contains the cluster to be resized, and choose <strong>More &gt; Resize Cluster</strong>.</td>
</tr>
</tbody>
</table>

The page for resizing the cluster is displayed.
Step 4 Select a proper node flavor based on service requirements. By default, the original flavor of the cluster is selected.

Step 5 In the Set to spin box, specify the target number of nodes in the cluster.
- The maximum number of nodes that can be added depends on the available quota.
- If the node quota is insufficient, click Increase quota to submit a service ticket and apply for higher node quota.
  If you have yearly/monthly nodes that meet service requirements, you are advised to use these nodes first to save costs. If no yearly/monthly nodes are available, click Buy Yearly/Monthly Package.
- The VPC, subnet, and security group of the cluster with new nodes added are the same as those of the original cluster.

Step 6 Click Scale Out Now.

Step 7 Confirm the information and click Submit.
- After the application for resizing the cluster is submitted, DWS creates an automated snapshot for the cluster. In this case, Task Information displays Creating snapshot.
- After the snapshot is created, the system starts resizing the cluster. In this case, Task Information of the cluster changes to Resizing. The process will take several minutes. During cluster resizing, the cluster automatically restarts. Therefore, Cluster Status stays Unavailable for a period of time. After the cluster is restarted, the status becomes Available. During the last stage of the resizing, the system dynamically distributes user data in the cluster. During the distribution, the cluster is in the Read-only status.
- When a cluster is being resized, you can click its name in the cluster list to enter the cluster details page and view the cluster resizing information, including the number of original nodes, number of target nodes, resizing status, start time, original node flavor, and target node flavor.
- A cluster is successfully resized only when Cluster Status becomes Available and Resizing is not displayed in Task Information any more. Then the cluster begins providing services.
- If Task Information of the cluster is Resize failed, the cluster resizing fails.

---End

1.15 Restarting a Cluster

If a cluster is in low performance or cannot work properly, you may need to restart it for restoration. After modifying a cluster's configurations, such as security settings and parameters in the parameter template, manually restart the cluster to make the configurations take effect.

Impact on the System
- A cluster cannot provide services during the restart. Therefore, before the restart, ensure that no task is running and all data is saved.
  If the cluster is processing service data, such as importing data, querying data, creating snapshots, or restoring snapshots, cluster restarting will cause file damage or restart failure. You are advised to stop all cluster tasks before restarting the cluster.
  View the Session Count and Active SQL Count metrics to check whether the cluster has active events. For details, see Monitoring a Cluster.
The time required for restarting a cluster depends on the cluster scale and services. Generally, it takes about 3 minutes to restart a cluster. The duration does not exceed 20 minutes.

- If the restart fails, the cluster may be unavailable. Contact technical support engineers or try again later.

### Procedure

- **Step 1** Log in to the management console at [https://console.huaweicloud.com/dws/?locale=en-us](https://console.huaweicloud.com/dws/?locale=en-us).
- **Step 2** Click **Cluster Management**.
- **Step 3** In the **Operation** column of the cluster to be restarted, click **Restart**.
- **Step 4** In the dialog box that is displayed, click **Yes**.

Task Information changes to **Restarting**. When **Cluster Status** changes to **Available** again, the cluster is successfully restarted.

---

### 1.16 Upgrading a Cluster

After you create a data warehouse cluster, the system automatically configures a random maintenance window for the cluster. Alternatively, you can customize a maintenance window as required. For details about how to view and configure the maintenance window, see *Configuring the Maintenance Window*.

The validity period of the maintenance window (maximum maintenance duration) is 4 hours. During this period, you can upgrade the cluster, install operating system patches, and harden the system. If no maintenance tasks are performed within the planned maintenance window, the cluster continues to run properly until the next maintenance window. DWS will notify you about any maintenance operation by sending SMS messages. Exercise caution when you operate clusters during the maintenance period.

If a node needs to be replaced due to a hardware fault, the repairCluster event will be triggered. You can obtain the latest progress from section *Subscribing to Event Notification* to ensure that services are running properly. Background O&M personnel are responsible for performing node replacement operations during the maintenance window.

If the upgrade affects the current query request and service running, contact technical support engineers for emergency handling.

A cluster is charged by hour or yearly/monthly package as long as it is in **Available** status. Since the cluster is charged by hour or yearly/monthly package, you would not see any difference in the bill if a node failure or system upgrade only causes a brief interruption (for example, 15 minutes) for the cluster. If such events cause major system interruption (very rare case), you will not be charged for those downtime hours.

### Upgrading a Cluster

You do not need to care about DWS cluster patching or upgrading because DWS will handle version upgrade automatically. After DWS is upgraded, the service automatically upgrades the clusters to the latest version within the maintenance window. During the upgrade, the cluster is automatically restarted and cannot provide services for a short period of time.
Therefore, you are advised to set a suitable time range when the number of connected users and the number of active tasks are small.

**NOTE**

After the cluster is upgraded, it cannot be rolled back.

The following figure describes the cluster version.

**Figure 1-26 Version description**

- **Service patch upgrade**: The last digit of cluster version X.X.X is changed. For example, the cluster is upgraded from 1.1.0 to 1.1.1.
  - Duration: The whole process will take less than 10 minutes.
  - Impact on services: During this period, services will be interrupted for 1 to 3 minutes.

- **Service upgrade**: The first two digits of cluster version X.X.X are changed. For example, the cluster is upgraded from 1.1.0 to 1.2.0.
  - Duration: The whole process will take less than 30 minutes.
  - Impact on services: During this period, the database cannot be accessed.

**Configuring the Maintenance Window**

**Step 1** Log in to the management console at [https://console.huaweicloud.com/dws/?locale=en-us](https://console.huaweicloud.com/dws/?locale=en-us).

**Step 2** Click Cluster Management.

**Step 3** In the cluster list, click the name of the target cluster. The Basic Information page is displayed.

In the Cluster Information area, you can view the Maintenance Window.

**Step 4** On the right of Maintenance Window, click Configure.

**Step 5** In the dialog box that is displayed, configure the maintenance window.
### 1.17 Deleting a Cluster

**Scenario**

You can delete redundant or unwanted clusters from your DWS as follows:

**Impact on the System**

Deleted clusters cannot be recovered. Additionally, you cannot access user data and automated snapshots in a deleted cluster because the data and snapshots are automatically deleted. If you delete a cluster, its manual snapshots will not be deleted.

**Procedure**

**Step 1** Log in to the management console at [https://console.huaweicloud.com/dws/?locale=en-us](https://console.huaweicloud.com/dws/?locale=en-us).

**Step 2** Click ![location](image) in the upper left corner of the management console to select a region.

**Step 3** On the Cluster Management page, locate the cluster to be deleted.

**Step 4** Locate the row that contains the target cluster, choose More > Delete.

**Step 5** In the displayed dialog box, confirm the deletion. You can determine whether to perform the following operations:
- Create a snapshot for the cluster.

  If the cluster status is normal, you can click Create Snapshot. In the dialog box that is displayed, enter the snapshot name and click OK to create a snapshot for the cluster to be deleted. After the snapshot is created, go back to the Cluster Management page and delete the cluster.
Release the EIP bound to the cluster.

If the cluster is bound with an EIP, you can click **Release the EIP bound to the cluster** to release the EIP of the cluster to be deleted. If you do not release the EIP, it will be billed based on the Elastic IP pricing rule of VPC.

**Figure 1-28** Deleting a cluster

---End

**Step 6** Click **Yes**.

If the cluster to be deleted uses an automatically created security group that is not used by other clusters, the security group is automatically deleted after the cluster is deleted.

---End
2 Connecting to a Cluster

2.1 Methods of Connecting to a Cluster

If you have created a data warehouse cluster, you can use the SQL client tool or a third-party driver such as JDBC and ODBC to connect to the cluster and access the database in the cluster.

The procedure for connecting to a cluster is as follows:

1. **Obtaining the Cluster Connection Address**
2. If SSL encryption is used, perform the following steps:
   a. *(Optional) Configuring SSL Connection*
   b. *(Optional) Downloading SSL Certificate*
3. Connect to the cluster and access the database in the cluster. You can choose any one of the following methods to connect to a cluster:
   - Use the SQL client tool to connect to the cluster.
     - **Using the gsql Client to Connect to a Cluster**
     - **Using pgAdmin to Connect to a Cluster**
     - **Using the Data Studio GUI Client to Connect to a Cluster**
     - **Using Extended Application pgAdmin4 to Connect to the Cluster**
   - Use JDBC, ODBC, and psycopg2 third-party drivers to connect to the cluster.
     - **Using a JDBC Driver to Connect to the Database**
     - **Using an ODBC Driver to Connect to the Database**
     - **Using the Third-Party Function Library psycopg2 of Python to Connect to a Cluster**
     - **Configuring the JDBC Connection to Connect to a Cluster Using IAM Authentication**
2.2 Obtaining the Cluster Connection Address

Scenario

You can access data warehouse clusters using different methods and the connection address of each connection method varies. This section describes how to view and obtain the private network address in the public cloud, public network address on the Internet, and JDBC connection strings.

To obtain the cluster connection address, use either of the following methods:

- Obtaining the Cluster Connection Address on the Connection Management Page
- Obtaining the Cluster Access Addresses on the Basic Information Page

Obtaining the Cluster Connection Address on the Connection Management Page

Step 1 Log in to the DWS management console.

Step 2 In the navigation tree on the left, click Connection Management.

Step 3 In the Data Warehouse Connection Information area, select an available cluster.

You can only select clusters in the Available state.

Figure 2-1 Data warehouse connection information

Step 4 View and obtain the cluster connection information.

- Private Network Address
- Public Network Address
- JDBC URL (Private Network)
- JDBC URL (Public Network)
- ODBC URL
If no EIP is automatically assigned during cluster creation, **Public Network Address** is empty. If you want to use a public network address (consisting of an EIP and the database port) to access the cluster from the Internet, click **Bind EIP** to bind one.

- If an EIP is bound during cluster creation but you do not want to use the public network address to access the cluster, click **Unbind EIP** to unbind the EIP. After the EIP is unbound, **Public Network Address** is empty.

---

**Obtaining the Cluster Access Addresses on the Basic Information Page**

**Step 1** Log in to the management console at [https://console.huaweicloud.com/dws/?locale=en-us](https://console.huaweicloud.com/dws/?locale=en-us).

**Step 2** In the navigation tree on the left, click **Cluster Management**.

**Step 3** In the cluster list, click the name of the cluster that you want to view. The **Basic Information** page is displayed.

**Step 4** In the **Database Attribute** area, view and obtain the cluster's access address information, including the private network address and public network address.

**Figure 2-2 Access addresses**

**Table 2-1 Database attribute parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Database</td>
<td>Database that is automatically created during cluster creation. When you connect to the cluster for the first time, you need to connect to the default database.</td>
</tr>
<tr>
<td>Initial Administrator</td>
<td>Administrator user specified during cluster creation. When you connect to the cluster for the first time, you need to use the initial administrator and password to connect to the default database.</td>
</tr>
<tr>
<td>Port</td>
<td>Port for accessing the cluster database over the public network or private network. Database port specified during cluster creation. It is used to listen to client connections.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>JDBC URL (Private Network)</td>
<td>In the private network environment, you can use the JDBC URL (private network) to connect to the cluster when developing applications.</td>
</tr>
<tr>
<td>JDBC URL (Public Network)</td>
<td>In the public network environment, you can use the JDBC URL (public network) to connect to the cluster when developing applications.</td>
</tr>
<tr>
<td>Private Network Domain Name</td>
<td>Name of the domain for accessing the database in the cluster through the private network. The private network domain address is automatically generated when you create a cluster. The default naming rule is <code>cluster name.dws.myhuaweicloud.com</code>. NOTE: If the cluster name does not comply with the domain name standards, the prefix of the default access domain name will be adjusted accordingly. Click <strong>Modify</strong> to change the private network access domain name. The access domain name contains 4 to 63 characters, which consist of letters, digits, and hyphens (-), and must start with a letter. For more information, see <em>Managing Access Domain Names</em>.</td>
</tr>
<tr>
<td>Private Network IP Address</td>
<td>IP address for accessing the database in the cluster through the private network. The private network address is automatically generated when you create a cluster.</td>
</tr>
<tr>
<td>Public Network Domain Name</td>
<td>Name of the domain for accessing the database in the cluster through the public network. NOTE: If you have not bound an EIP to the cluster, <strong>Public Network IP Address</strong>, <strong>Public Network Port</strong>, and <strong>Public Network Domain Name</strong> are left blank. If you bind an EIP during cluster creation, the public network domain name is automatically generated. The default naming rule is <code>cluster name.dws.huaweiclouds.com</code>. Bind an EIP to the cluster before binding the public network domain name to the cluster. Click <strong>Create</strong> to bind the public network domain name to the cluster. You can click <strong>Modify</strong> to modify the public network domain name bound to the cluster. The domain name contains 4 to 63 characters, which consist of letters, digits, and hyphens (-), and must start with a letter. You can click <strong>Release</strong> to release the public network domain name bound to the cluster. For more information, see <em>Managing Access Domain Names</em>.</td>
</tr>
<tr>
<td>Public Network IP Address</td>
<td>IP address for accessing the database in the cluster through the public network. NOTE: If no EIP is assigned during cluster creation and <strong>Public Network IP Address</strong> is empty, click <strong>Bind EIP</strong> to bind an EIP to the cluster. If an EIP is bound during cluster creation, click <strong>Unbind EIP</strong> to unbind the EIP.</td>
</tr>
</tbody>
</table>
### 2.3 (Optional) Configuring SSL Connection

DWS supports connections in SSL authentication mode so that data transmitted between the DWS client and the database can be encrypted. The SSL connection mode delivers higher security than the common mode. By default, the SSL function is enabled in a cluster to allow SSL or non-SSL connections from the client. For security purposes, you are advised to enable SSL connection. If you want to use SSL connection forcibly, enable **Require SSL Connection** for the cluster.

On the **Security Settings** page of the cluster, you can enable or disable **Require SSL Connection**.

![NOTE](image)

- After you have changed the security setting parameters and the changes take effect, the cluster may be restarted, which makes the cluster unavailable temporarily.
- To modify the cluster’s security configuration, ensure that the following conditions are met:
  - The **Cluster Status** is **Available** or **Low performance**.
  - The **Task Information** cannot be **Creating snapshot**, **Scaling out**, **Configuring**, or **Restarting**.

The following parts are included in this section:

- **Configuring SSL Connection**
- **Combinations of SSL Connection Parameters on the Client and Server**

#### Configuring SSL Connection

1. **Step 1** Log in to the management console at [https://console.huaweicloud.com/dws/?locale=en-us](https://console.huaweicloud.com/dws/?locale=en-us).
2. **Step 2** In the navigation tree on the left, click **Cluster Management**.
3. **Step 3** In the cluster list, click the name of a cluster. On the page that is displayed, click **Security Settings**.

   By default, **Configuration Status** is **Synchronized**, which indicates that the latest database result is displayed.

4. **Step 4** In the **SSL Connection** area, click **Require SSL Connection** switch to enable the function (recommended).

   ![switch](image)

   - **on**: indicates that the server forcibly requires SSL connection.
   - **off**: indicates that the server does not forcibly require SSL connection. This function is disabled by default.
Figure 2-3 SSL connection

* Require SSL Connection

Apply

**NOTE**
- If the gsql client or ODBC driver provided by DWS is used, DWS supports the TLSv1.2 SSL protocol.
- If the JDBC driver provided by DWS is used, DWS supports SSL protocols, such as SSLv3, TLSv1, TLSv1.1, and TLSv1.2. The SSL protocol used between the client and the database depends on the Java Development Kit (JDK) version used by the client. Generally, JDK supports multiple SSL protocols.

**Step 5** Click **Apply**.

The system automatically saves the SSL connection settings. On the Security Settings page, Configuration Status is Applying. After Configuration Status changes to Synchronized, the settings have been saved and taken effect.

---End

**Combinations of SSL Connection Parameters on the Client and Server**

Whether the client uses the SSL encryption connection mode and whether to verify the server certificate depend on client parameter `sslmode` and server (cluster) parameters `ssl` and `require_ssl`. The parameters are described as follows:

- **ssl (Server)**
  - The `ssl` parameter indicates whether to enable the SSL function. `on` indicates that the function is enabled, and `off` indicates that the function is disabled.
    - The default value is `on` for clusters whose version is later than 1.3.1 (including 1.3.1), and you cannot set this parameter on the DWS management console.
    - For clusters whose version is earlier than 1.3.1, the default value is `on`. You can set this parameter in the SSL Connection area on the cluster's Security Settings page of the DWS management console.

- **require_ssl (Server)**
  - The `require_ssl` parameter specifies whether the server forcibly requires SSL connection. This parameter is valid only when `ssl` is set to `on`. `on`: The server forcibly requires SSL connection. `off`: The server does not require SSL connection.
    - The default value is `off` for clusters whose version is later than 1.3.1 (including 1.3.1). You can set the `require_ssl` parameter in the Require SSL Connection area of the cluster's Security Settings page on the DWS management console.
    - For clusters whose version is earlier than 1.3.1, the default value is `off`, and you cannot set this parameter on the DWS management console.
- **sslmode (Client)**
  
  You can set this parameter in the SQL client tool.
  - In the gsql command line client, this parameter is the \texttt{PGSSLMODE} parameter.
  - On the Data Studio client, this parameter is the \texttt{SSL Mode} parameter.

The combinations of client parameter \texttt{sslmode} and server parameters \texttt{ssl} and \texttt{require_ssl} are as follows:

**Table 2-2** Combinations of SSL connection parameters on the client and server

<table>
<thead>
<tr>
<th>ssl (Server)</th>
<th>sslmode (Client)</th>
<th>require_ssl (Server)</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>disable</td>
<td>on</td>
<td>The server requires SSL, but the client disables SSL for the connection. As a result, the connection cannot be set up.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>off</td>
<td>The connection is not encrypted.</td>
</tr>
<tr>
<td></td>
<td>allow</td>
<td>on</td>
<td>The connection is encrypted.</td>
</tr>
<tr>
<td></td>
<td>allow</td>
<td>off</td>
<td>The connection is not encrypted.</td>
</tr>
<tr>
<td></td>
<td>prefer</td>
<td>on</td>
<td>The connection is encrypted.</td>
</tr>
<tr>
<td></td>
<td>prefer</td>
<td>off</td>
<td>The connection is encrypted.</td>
</tr>
<tr>
<td></td>
<td>require</td>
<td>on</td>
<td>The connection is encrypted.</td>
</tr>
<tr>
<td></td>
<td>require</td>
<td>off</td>
<td>The connection is encrypted.</td>
</tr>
<tr>
<td></td>
<td>verify-ca</td>
<td>on</td>
<td>The connection is encrypted and the server certificate is verified.</td>
</tr>
<tr>
<td></td>
<td>verify-ca</td>
<td>off</td>
<td>The connection is encrypted and the server certificate is verified.</td>
</tr>
<tr>
<td>off</td>
<td>disable</td>
<td>on</td>
<td>The connection is not encrypted.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>off</td>
<td>The connection is not encrypted.</td>
</tr>
<tr>
<td></td>
<td>allow</td>
<td>on</td>
<td>The connection is not encrypted.</td>
</tr>
<tr>
<td></td>
<td>allow</td>
<td>off</td>
<td>The connection is not encrypted.</td>
</tr>
<tr>
<td></td>
<td>prefer</td>
<td>on</td>
<td>The connection is not encrypted.</td>
</tr>
<tr>
<td></td>
<td>prefer</td>
<td>off</td>
<td>The connection is not encrypted.</td>
</tr>
<tr>
<td></td>
<td>require</td>
<td>on</td>
<td>The client requires SSL, but SSL is disabled on the server. Therefore, the connection cannot be set up.</td>
</tr>
<tr>
<td></td>
<td>require</td>
<td>off</td>
<td>The client requires SSL, but SSL is disabled on the server. Therefore, the connection cannot be set up.</td>
</tr>
<tr>
<td></td>
<td>verify-ca</td>
<td>on</td>
<td>The client requires SSL, but SSL is disabled on the server. Therefore, the connection cannot be set up.</td>
</tr>
</tbody>
</table>
### 2.4 (Optional) Downloading SSL Certificate

DWS supports the standard SSL (TLS 1.2). As a highly secure protocol, SSL authenticates bidirectional identification between the server and client using digital signatures and digital certificates to ensure secure data transmission. To support SSL connection, DWS has obtained the formal certificates and keys for the server and client from the CA certification center. It is assumed that the key and certificate for the server are `server.key` and `server.crt` respectively; the key and certificate for the client are `client.key` and `client.crt` respectively, and the name of the CA root certificate is `cacert.pem`.

By default, the SSL function is enabled for a data warehouse cluster (the server) to allow SSL and non-SSL connections from the client. In addition, the certificate, private key, and root certificate of the server have been configured by default.

If the client or JDBC/ODBC driver needs to use SSL connection, you must configure related SSL connection parameters in the client or application code. The DWS management console provides the SSL certificate required by the client. The SSL certificate contains the default certificate, private key, root certificate, and private key password encryption file required by the client. Download the SSL certificate to the host where the client resides and specify the path of the certificate on the client.

![NOTE](https://www.huawei.com)

Using the default certificate may pose security risks. To improve system security, you are advised to periodically change the certificate to prevent password cracking. If you need to replace the certificate, contact the customer service.

This section describes how to download an SSL certificate.

**Downloading the SSL Certificate File**

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

**Step 2** In the navigation tree on the left, click Connection Management.

**Step 3** In the Driver area, click here to download the SSL certificate file.
2.5 Using the gsql CLI Client to Connect to a Cluster

2.5.1 Downloading Clients

DWS provides client tool packages that match the cluster versions. You can download the desired client tool package on the DWS management console.

The client tool package contains the following:

- **Database connection tool gsql and the script for testing sample data**
  
gsql is a command line client running on the Linux operating system. It is used to connect to the database in a data warehouse cluster.
  
The script for testing sample data is used when you start an example.

- **GDS tool package**
  
Gauss Data Service (GDS) is a data service tool. You can use the GDS tool to import a data file in a common file system to the DWS database. The GDS tool package must be installed on the server where the data source file is located. The server where the data source file is located is called a data server or GDS server.

**Downloading the Client**

**Step 1**  Log in to the management console at https://console.huaweicloud.com/dws/?locale=en-us.

**Step 2**  In the navigation tree on the left, click Connection Management.

**Step 3**  Select the DWS client of the corresponding version from the drop-down list of gsql CLI Client.

Choose **RedHat x64** or **SUSE x64** according to the operating system of the client to be installed.

- The **RedHat x64** client can be used on the following operating systems:
  - RHEL 6.4/6.5/6.6/6.7/7.1/7.2
  - CentOS 6.4/6.5/6.6/6.7
  - EulerOS 2.0 SP2

- The **SUSE x64** client can be used on the following operating systems:
  - SLES11 SP1/SP2/SP3/SP4
Step 4  Click **Download** to download the gsql tool matching the current cluster version. Click **Historical Version** to download the gsql tool corresponding to the cluster version.

If clusters of different versions are available, you will download the gsql tool matching the earliest cluster version after clicking **Download**. If there is no cluster, you will download the gsql tool of the earliest version after clicking **Download**. DWS clusters are compatible with earlier versions of gsql tools.

**NOTE**

In the cluster list on the **Cluster Management** page, click the name of the specified cluster and click the **Basic Information** tab to view the cluster version.

Table 2-3 lists the files and folders in the downloaded tool package.

**Table 2-3 Files and folders in the downloaded tool package**

<table>
<thead>
<tr>
<th>File or Folder</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bin</td>
<td>This folder contains the executable files of gsql in Linux.</td>
</tr>
<tr>
<td>gds</td>
<td>This folder contains the files of the GDS data service tool. The GDS tool is used for parallel data loading and can import the data files stored in a common file system to a DWS database.</td>
</tr>
<tr>
<td>lib</td>
<td>This folder contains the <strong>lib</strong> library required for executing the gsql client.</td>
</tr>
</tbody>
</table>
| sample        | This folder contains the following directories and files:  
|               | • **setup.sh**: Script file for configuring the AK/SK before using the gsql to import sample data  
|               | • **tpcds_load_data_from_obs.sql**: Script file for importing the TPC-DS sample data using the gsql client  
|               | • **query_sql** directory: Script file for querying the TPC-DS sample data |
| gsql_env.sh   | Script file for configuring environment variables before running the gsql client. |

---End

### 2.5.2 Preparing an ECS as the gsql Client Host

The gsql command line client provided by DWS runs on the Linux operating system. Before using it to remotely connect to a data warehouse cluster, you need to prepare a Linux host for installing and running the gsql client. If you use a public network address to access the cluster,
you can install the gsql client on your own Linux host. Ensure that the Linux host has a public network address. For your convenience, you are advised to create a Linux ECS. This section describes how to prepare an ECS. If you already have a qualified ECS, skip this section.

Preparing an ECS

For details about how to purchase an ECS, see Quickly Purchasing an ECS in the Elastic Cloud Server Getting Started.

The purchased ECS must meet the following requirements:

- The ECS and data warehouse cluster must belong to the same region and AZ.
- If you use the gsql client provided by DWS to connect to the data warehouse cluster, the ECS image must meet the following requirements:

  There is no special requirement for the image's specifications. The image's operating system must be one of the following Linux operating systems supported by the gsql client:

  - The **RedHat x64** client can be used on the following operating systems:
    - RHEL 6.4/6.5/6.6/6.7/7.1/7.2
    - CentOS 6.4/6.5/6.6/6.7
    - EulerOS 2.0 SP2
  - The **SUSE x64** client can be used on the following operating systems:
    - SLES11 SP1/SP2/SP3/SP4

- If the client accesses the cluster using the private network address, ensure that the created ECS is in the same VPC as the data warehouse cluster.

  For details about VPC operations, see VPC and Subnet in the Virtual Private Cloud User Guide.

- If the client accesses the cluster using the public network address, ensure that both created ECS and the data warehouse cluster have an EIP.

  When purchasing an ECS, set EIP to Buy now or Specify.

- The security group rules of the ECS must enable communication between the ECS and the port that the data warehouse cluster uses to provide services.

  For details about security group operations, see Security > Security Group in the Virtual Private Cloud User Guide.

Ensure that the security group of the ECS contains rules meeting the following requirements. If the rules do not exist, add them to the security group:

- Transfer Direction: Outbound
- Protocol: The value must contain TCP, for example, TCP and All.
- Port: The value must contain the database port that provides services in the data warehouse cluster. For example, set this parameter to 1-65535 or a specific DWS database port.
- Destination: The IP address set here must contain the IP address of the cluster to be connected. For example, set this parameter to 0.0.0.0/0 or the specific connection address of the data warehouse cluster.
The security group rules of the data warehouse cluster must ensure that DWS can receive network access requests from clients. Ensure that the cluster's security group contains rules meeting the following requirements. If the rules do not exist, add them to the security group:

- **Transfer Direction**: Inbound
- **Protocol**: The value must contain TCP, for example, TCP and All.
- **Port**: Set this parameter to the database port that provides services in the data warehouse cluster, for example, **8000**.
- **Source**: The IP address set here must contain the IP address of the DWS client host, for example, **192.168.0.10/32**.

### 2.5.3 Using the gsql Client to Connect to a Cluster

This section describes how to connect to a database through an SQL client after you create a data warehouse cluster and before you use the cluster's database. DWS provides the gsql client that matches the cluster version for you to access the cluster using the cluster's public or private network address.

#### Using the gsql CLI Client to Connect to a Cluster

**Step 1** Prepare a Linux ECS to install and run the gsql client.

For details, see [Preparing an ECS as the gsql Client Host](#).

**Step 2** Download the gsql client by referring to [Downloading Clients](#), and use an SSH file transfer tool (such as WinSCP) to upload the client to a target Linux host.
The user who uploads the client must have the full control permission on the target directory on the host to which the client is uploaded.

Alternatively, you can remotely log in to the Linux host where the gsql is to be installed in SSH mode and run the following command in the Linux command window to download the gsql client:

`wget https://obs.myhwclouds.com/dws/download/dws_client_redhat_x64.tar.gz --no-check-certificate`

**Step 3** Use the SSH tool to remotely log in to the host where the client is installed.

For details about how to log in to an ECS, see [Login Using an SSH Password](#) in the [Elastic Cloud Server User Guide](#).

**Step 4** (Optional) To connect to the cluster in SSL mode, configure SSL authentication parameters on the host where the client is installed. For details, see [Establishing Secure TCP/IP Connections in SSL Mode](#).

**NOTE**

The SSL connection mode is more secure than the non-SSL mode. You are advised to use the SSL mode on the client.

**Step 5** Run the following commands to decompress the client:

```
cd <Path for saving the client>
tar -xvf dws_client_redhat_x64.tar.gz
```

In the preceding commands:

- `<Path for saving the client>`: Replace it with the actual path.
- `dws_client_redhat_x64.tar.gz`: This is the client tool package of RedHat x64. Replace it with the actual one.

**Step 6** Run the following command to configure the DWS client:

```
source gsql_env.sh
```

If the following information is displayed, the DWS client is successfully configured:

```
All things done.
```

You can connect to a data warehouse cluster through the DWS client.

**Step 7** Run the following command. Replace the values of each parameter with actual values. This command will use the gsql client to connect to the database in the data warehouse cluster:

```
gsql -d <Database name> -h <Cluster address> -U <Database user> -p <Database port> -r
```

The parameters are described as follows:

- **Database name**: Enter the name of the database to be connected. If you use the client to connect to the cluster for the first time, enter the default database `postgres`.
- **Cluster address**: For details about how to obtain this address, see [Obtaining the Cluster Connection Address](#). If a public network address is used for connection, set this parameter to `Public Network Address` or `Public Network Domain Name`. If a private network address is used for connection, set this parameter to `Private Network Address` or `Private Network Domain Name`.
● **Database user**: Enter the username of the cluster's database. If you use the client to connect to the cluster for the first time, set this parameter to the default administrator configured during cluster creation, for example, `dbadmin`.

● **Database port**: Enter the database port set during cluster creation.

For example, run the following command to connect to the `postgres` default database in the data warehouse cluster:

```
gsql -d postgres -h 10.168.0.74 -U dbadmin -p 8000 -r
```

If the following information is displayed after you enter the password as prompted, the connection is successful:

```
postgres>
----End
```

---End

### gsqi Command Reference

For more information about the gsqi commands, see the [Data Warehouse Service Tool Guide](#).

### (Optional) Importing TPC-DS Sample Data Using gsqi

DWS users can import data from external sources to data warehouse clusters. This section describes how to import sample data from OBS to a data warehouse cluster and perform querying and analysis operations on the sample data. The sample data is generated based on the standard TPC-DS benchmark test.

TPC-DS is the benchmark for testing the performance of decision support. With TPC-DS test data and cases, you can simulate complex scenarios, such as big data set statistics, report generation, online query, and data mining, to better understand functions and performance of database applications.

**Step 1** Use the SSH connection tool to remotely log in to the host where the gsqi client is installed.

**Step 2** In the Linux command window, run the following commands to switch to a specific directory and set the AK and SK for importing sample data and the OBS access address:

```
cd ./sample
/bin/bash setup.sh -ak <Access_Key_Id> -sk <Secret_Access_Key> -obs_location obs.myhwclouds.com
```

If the following information is displayed, the settings are successful:

```
setup successfully!
```

**NOTE**

`<Access_Key_Id>` and `<Secret_Access_Key>` indicate the access key ID and secret access key. For details about how to obtain the AK and SK, see [Creating Access Keys (AK and SK)](#). Then, replace the parameters in the statement with the obtained values.

**Step 3** In the Linux command window, run the following command to import the sample data to the data warehouse cluster:

```
Command format:
```

---End
Sample command:

```
gsql -d postgres -h 10.168.0.74 -U dbadmin -p 8000 -f tpcds_load_data_from_obs.sql -r
```

In the preceding command, sample data script `tpcds_load_data_from_obs.sql` is stored in the `sample` directory (for example, `dws_client_redhat_x64/sample`) of the DWS client.

After you enter the administrator password and successfully connect to the database in the cluster, the system will automatically create a foreign table to associate the sample data outside the cluster. Then, the system creates a target table for saving the sample data and imports the data to the target table using the foreign table.

When information similar to the following is displayed, the data is successfully imported.

```
Time:1845600.524 ms
```

**Step 4** In the Linux command window, run the following commands to switch to a specific directory and query the sample data:

```
cd sample/query_sql/
/bin/bash tpcds100x.sh
```

**Step 5** Enter the cluster's public network IP address, access port, database name, user who accesses the database, and password of the user as prompted.

- The default database name is `postgres`.
- Use the administrator username and password configured during cluster creation as the username and password for accessing the database.

After the query is complete, a directory for storing the query result, such as `query_output_20170914_072341`, will be generated in the current query directory, for example, `sample/query_sql/`.

----End

### 2.5.4 Establishing Secure TCP/IP Connections in SSL Mode

If the client or JDBC/ODBC driver needs to use SSL connection, you must configure related SSL connection parameters in the client or application code. The DWS management console provides the SSL certificate required by the client. The SSL certificate contains the default certificate, private key, root certificate, and private key password encryption file required by the client. Download the SSL certificate to the host where the client resides and specify the path of the certificate on the client.

**NOTE**

Using the default certificate may pose security risks. To improve system security, you are advised to periodically change the certificate to prevent password cracking. If you need to replace the certificate, contact the customer service.

For more information about SSL certificates, see [Optional) Downloading SSL Certificate]. The following parts are included in this section:

- **Configuring Digital Certificate Parameters Related to SSL Authentication on the gsql Client**
SSL Authentication Modes and Client Parameters

Configuring Digital Certificate Parameters Related to SSL Authentication on the gsql Client

After a data warehouse cluster is deployed, the SSL authentication mode is enabled by default. The server certificate, private key, and root certificate have been configured by default. You need to configure the client parameters.

**Step 1** Log in to the DWS management console and click **Connection Management** to download the SSL certificate.

For more information about SSL certificates, see (Optional) Downloading SSL Certificate.

**Figure 2-8 Downloading the SSL Certificate File**

**Step 2** Use a file transfer tool (such as WinSCP) to upload the SSL certificate to the host where the client is installed.

For example, save the downloaded certificate `dws_ssl_cert.tar.gz` to the `/home/dbadmin/dws_ssl/` directory.

**Step 3** Use an SSH remote connection tool (such as PuTTY) to log in to the host where the gsql client is installed and run the following commands to go to the directory where the SSL certificate is stored and decompress the SSL certificate:

```
cd /home/dbadmin/dws_ssl/
tar -xvf dws_ssl_cert.tar.gz
```

**Step 4** Run the export command and configure digital certificate parameters related to SSL authentication on the host where the gsql client is installed.

There are two SSL authentication modes: bidirectional authentication and unidirectional authentication. Different authentication modes require different client environment variables. For details, see SSL Authentication Modes and Client Parameters.

The following parameters must be configured for bidirectional authentication:

```
export PGSSLCERT="/home/dbadmin/dws_ssl/sslcert/client.crt"
export PGSSLKEY="/home/dbadmin/dws_ssl/sslcert/client.key"
export PGSSLMODE="verify-ca"
export PGSSLROOTCERT="/home/dbadmin/dws_ssl/sslcert/cacert.pem"
```

The following parameters must be configured for unidirectional authentication:

```
export PGSSLMODE="verify-ca"
export PGSSLROOTCERT="/home/dbadmin/dws_ssl/sslcert/cacert.pem"
```
NOTICE

- You are advised to use bidirectional authentication for security purposes.
- The environment variables configured for a client must contain the absolute file paths.

### Step 5
Change the client private key permissions.

The permissions on the client's root certificate, private key, certificate, and encrypted private key file must be 600. If the permissions do not meet the requirement, the client cannot connect to the cluster in SSL mode.

```bash
chmod 600 client.key
chmod 600 client.crt
chmod 600 client.key.cipher
chmod 600 client.key.rand
chmod 600 cacert.pem
```

---End

### SSL Authentication Modes and Client Parameters

SSL authentication has two authentication modes: bidirectional certification and unidirectional authentication. Table Table 2-4 shows the differences between these two modes. You are advised to use bidirectional authentication for security purposes.

<table>
<thead>
<tr>
<th>Authentication Mode</th>
<th>Description</th>
<th>Environment Variables Configured on a Client</th>
<th>Maintenance</th>
</tr>
</thead>
</table>
| Bidirectional certification (recommended) | The client verifies the server's certificate and the server verifies the client's certificate. Connection can be set up after the verifications are successful. | Set the following environment variables:  
  - PGSSLCERT  
  - PGSSLKEY  
  - PGSSLROOTCERT  
  - PGSSLMODE | This authentication mode is applicable to scenarios that require high data security. When using this mode, you are advised to set the PGSSLMODE client variable to `verify-ca` for network data security purposes. |
<table>
<thead>
<tr>
<th>Authentication Mode</th>
<th>Description</th>
<th>Environment Variables Configured on a Client</th>
<th>Maintenance</th>
</tr>
</thead>
</table>
| Unidirectional authentication | The client verifies the server's certificate, whereas the server does not verify the client's certificate. The server loads the certificate information and sends it to the client. The client verifies the server's certificate according to the root certificate. | Set the following environment variables:  
• PGSSLROOTCERT  
• PGSSLMODE | To prevent TCP-based link spoofing, you are advised to use the SSL certificate authentication. In addition to configuring the client root certificate, you are advised to set the PGSSLMODE variable to verify-ca on the client. |

Configure environment variables related to SSL authentication on the client. For details, see Table 2-5.

**NOTE**

An example path of environment variables is `/home/dbadmin/dws_ssl/` (for example). Replace it with the actual path.

### Table 2-5 Client parameters

<table>
<thead>
<tr>
<th>Environment Variable</th>
<th>Description</th>
<th>Value Range</th>
</tr>
</thead>
</table>
| PGSSLCERT            | Specifies the certificate files for a client, including the public key. Certificates prove the legal identity of the client and the public key is sent to the remote end for data encryption. | The absolute path of the files must be specified, for example: `export PGSSLCERT='/home/dbadmin/dws_ssl/sslcert/client.crt'`  
Default value: null |
| PGSSLKEY             | Specifies the private key file for the client to encrypt digital signatures and data encrypted using the public key. | The absolute path of the files must be specified, for example: `export PGSSLKEY='/home/dbadmin/dws_ssl/sslcert/client.key'`  
Default value: null |
<table>
<thead>
<tr>
<th>Environment Variable</th>
<th>Description</th>
<th>Value Range</th>
</tr>
</thead>
</table>
| PGSSLMODE            | Specifies whether to negotiate with the server about SSL connection and specifies the priority of the SSL connection. | Values and meanings:  
  ● disable: only tries to establish a non-SSL connection.  
  ● allow: tries to establish a non-SSL connection first, and then an SSL connection if the first attempt fails.  
  ● prefer: tries to establish an SSL connection first, and then a non-SSL connection if the first attempt fails.  
  ● require: only tries to establish an SSL connection. If there is a CA file, perform the verification according to the scenario in which the parameter is set to verify-ca.  
  ● verify-ca: tries to establish an SSL connection and check whether the server certificate is issued by a trusted CA.  
  ● verify-full: DWS does not support this mode.  
  Default value: prefer |
| PGSSLROOTCERT        | Specifies the root certificate file for issuing client certificates. The root certificate is used to verify the server certificate. | The absolute path of the files must be specified, for example:  
  ```bash  
  export PGSSLROOTCERT="/home/dbadmin/dws_ssl/sslcert/certca.pem"  
  ```  
  Default value: null |
| PGSSLCRL             | Specifies the certificate revocation list file, which is used to check whether a server certificate is in the list. If yes, the certificate invalid. | The absolute path of the files must be specified, for example:  
  ```bash  
  export PGSSLCRL="/home/dbadmin/dws_ssl/sslcert/sslcert-file.crl"  
  ```  
  Default value: null |

### 2.6 Using pgAdmin to Connect to a Cluster

pgAdmin is a common open source PostgreSQL client tool. For more open source client tools supported by DWS, see [Open Source Clients Supported by DWS](#).

This section describes how to use the pgAdmin client (in Windows operating system) to connect to a cluster.

**Open Source Clients Supported by DWS**

This section describes how to connect to a database through a database client after you have created a data warehouse cluster and before you use the cluster's database.
DWS supports the open-source PostgreSQL client.

The following lists compatible open-source clients:

- PostgreSQL psql 9.2.4 or later
  For more information, see https://www.postgresql.org/.
- pgAdmin
  For more information, see https://www.pgadmin.org/.
- dbbeaver
  For more information, see https://dbeaver.jkiss.org/download/.

Preparations Before Connecting to a Cluster

- An EIP has been bound to the data warehouse cluster.
- You have obtained the administrator username and password for logging in to the database in the data warehouse cluster.
- You have obtained the public network address, including the IP address and port number in the data warehouse cluster. For details, see Obtaining the Cluster Connection Address.
- You have configured the security group to which the data warehouse cluster belongs and added a rule that allows users’ IP addresses to access ports using the TCP.
  For details, see Adding a Security Group Rule in the Virtual Private Cloud User Guide.

Using pgAdmin to Connect to a Cluster

On DWS, you can connect to the database in a cluster using pgAdmin over the Internet. In the following operations, the pgAdmin client is used as an example in the Windows operating system.

Step 1 Visit https://www.pgadmin.org/download/ to download a proper pgAdmin client.

You are advised to download the latest version of the client. The following uses the pgAdmin 4 English version as an example.

Step 2 Install the pgAdmin client.

Step 3 Open the installed pgAdmin client.

Step 4 In the navigation tree on the left, choose Servers > Create > Server.

Figure 2-9 Create Server
Step 5  On the **General** tab page of the window for creating a server connection, enter a value in **Name**.

**Figure 2-10** Create Server - General

![Create Server - General](image)

Step 6  On the **Connection** tab page, enter the following cluster information.

- **Host name/address**: Enter the cluster's access address. Obtain the cluster's **Public Network Address** and **Public Network Domain Name** or **Private Network Address** and **Private Network Domain Name**. For details, see **Obtaining the Cluster Connection Address**. In this example, enter the **Public Network Address**.
- **Port**: Enter the cluster's port number.
- **Maintenance database**: Enter the name of the database to be connected. If you use the client to connect to the cluster for the first time, enter the default database **postgres**.
- **Username**: Enter the username of the cluster's database. If you use the client to connect to the cluster for the first time, set this parameter to the default administrator configured during cluster creation, for example, **dbadmin**.
- **Password**: Enter the password of the corresponding database user.
Step 7  (Optional) On the SSL tab page, enter the cluster information. The SSL connection mode delivers higher security than the common mode. You are advised to use the SSL mode on the client.

Download the SSL certificate. For details, see (Optional) Downloading SSL Certificate. Then, decompress the certificate file to the specified path.

- **SSL mode**: Select an SSL mode from the drop-down list. Possible values are Allow, Prefer, Require, Disable, and Verify-CA (DWS does not support the Verify-Full mode). If SSL mode is set to Verify-CA, the root certificate is required.

- **Client certificate**: Click and select the sslcert\client.crt file in the decompressed directory.

- **Client certificate key**: Click and select the sslcert\client.key file in the decompressed directory.

- **Root Certificate**: Based on the selected SSL Mode, click and select the sslcert\acert.pem file in the decompressed directory.
(Optional) **Certificate revocation list**: List of revoked digital certificates. It is a list consisting of timestamps of all authentications that are abolished by the authentication center.

**SSL compression**: Whether to enable the certificate compression transmission. Select **True** to enable the compression transmission, and select **False** to disable the compressed transmission. In this example, select **False** (default value).

**Figure 2-12 Create Server - SSL**

![SSL Configuration](image)

**Step 8**  After the connection configuration is complete, click **Save**.

The system attempts to connect to the cluster's database. After the connection is successful, the newly created DWS database is displayed in the navigation tree on the left.

**Step 9**  Expand the navigation tree on the left to the database node, right-click **postgres** and choose **Query Tool** from the shortcut menu.
Step 10  On the Query Tool page, enter the following query command, and then click or press F5 to check whether the connection is successful.

```
select * from information_schema.tables
```

If the connection is successful, the Data Output tab page displays a series of records.
2.7 Using the Data Studio GUI Client to Connect to a Cluster

Data Studio is a SQL client tool running on the Windows operating system. It provides various GUIs for you to manage databases and database objects, as well as edit, run, and debug SQL scripts, and view execution plans. Download the Data Studio software package from the DWS management console. The package can be used without installation after being decompressed.

DataStudio versions include Windows x86 (32-bit Windows system) and Windows x64 (64-bit Windows system).

Preparations Before Connecting to a Cluster

- An EIP has been bound to the data warehouse cluster.
- You have obtained the administrator username and password for logging in to the database in the data warehouse cluster.
- You have obtained the public network address, including the IP address and port number in the data warehouse cluster. For details, see Obtaining the Cluster Connection Address.
- You have configured the security group to which the data warehouse cluster belongs and added a rule that allows users’ IP addresses to access ports using the TCP. For details, see Adding a Security Group Rule in the Virtual Private Cloud User Guide.
Using Data Studio to Connect to the Cluster's Database

**Step 1** DWS provides the Data Studio GUI client running the Windows system. The tool depends on the JDK, so install Java 1.8.0_141 or a later version of JDK on the client host.

In the Windows operating system, you can download the required JDK version from the official website of SDK, and install it by following the installation guide.

**Step 2** Log in to the management console at https://console.huaweicloud.com/dws/?locale=en-us.

**Step 3** Click Connection Management.

**Step 4** On the Download Client and Driver page, download Data Studio GUI Client.

- Select Windows x86 or Windows x64 based on the operating system type and click Download to download the Data Studio tool matching the current cluster version.
  
  If clusters of different versions are available, you will download the Data Studio tool matching the earliest cluster version after clicking Download. If there is no cluster, you will download the Data Studio tool of the earliest version after clicking Download. DWS clusters are compatible with earlier versions of Data Studio tools.

- Click Historical Version to download the corresponding Data Studio version. You are advised to download the Data Studio based on the cluster version.

![Figure 2-15 Downloading clients](image)

If you have clusters of different versions, the system displays a dialog box, prompting you to select the cluster version and download the corresponding client. In the cluster list on the Cluster Management page, click the name of the specified cluster and click the Basic Information tab to view the cluster version.

**Step 5** Decompress the downloaded client software package (32-bit or 64-bit) to the installation directory.

**Step 6** Open the installation directory and double-click Data Studio.exe to start the Data Studio client. See Figure 2-16.

![Figure 2-16 Starting the client](image)
Step 7 Choose **File > New Connection** from the main menu. See Figure 2-17.

![Figure 2-17 Creating a connection](image)

Step 8 In the displayed **New Database Connection** window, enter the connection parameters.

![Figure 2-18 Configuring connection parameters](image)

**Table 2-6 Connection parameters**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Type</td>
<td>Select <strong>HUAWEI CLOUD DWS</strong>.</td>
<td>HUAWEI CLOUD DWS</td>
</tr>
<tr>
<td>Connection Name</td>
<td>Enter the connection name.</td>
<td>dws-demo</td>
</tr>
<tr>
<td>Host</td>
<td>Enter the IP address (IPv4) or domain name of the cluster to be connected.</td>
<td>-</td>
</tr>
<tr>
<td>Host Port</td>
<td>Enter the port address.</td>
<td>8000</td>
</tr>
<tr>
<td>Database Name</td>
<td>Enter the database name.</td>
<td>postgres</td>
</tr>
<tr>
<td>User Name</td>
<td>Enter the name of the user who wants to connect to the database.</td>
<td>-</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for logging in to the database to be connected.</td>
<td>-</td>
</tr>
<tr>
<td>Field Name</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Save Password</td>
<td>Select an option from the drop-down list:</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>- <strong>Current Session Only</strong>: The password is saved only in the current session.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Do Not Save</strong>: The password is not saved.</td>
<td></td>
</tr>
<tr>
<td>Enable SSL</td>
<td>If <strong>Enable SSL</strong> is selected, the client can use SSL to encrypt connections. The SSL connection mode is more secure than common modes, so you are advised to enable SSL connection.</td>
<td>-</td>
</tr>
</tbody>
</table>

When **Enable SSL** is selected, download the SSL certificate and decompress it by referring to **Downloading the SSL Certificate File**. Then, click the **SSL** tab in the window shown in **Figure 2-18** and set the following parameters:

**Table 2-7 Configuring SSL parameters**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client SSL Certificate</td>
<td>Select the <code>sslcert\client.crt</code> file in the decompressed SSL certificate directory.</td>
</tr>
<tr>
<td>Client SSL Key</td>
<td>For Data Studio 18.2.0 SPC1 and later versions, the client SSL key can only be in the PK8 format. Select the <code>sslcert\client.key.pk8</code> file in the decompressed SSL certificate directory. For versions earlier than Data Studio 18.2.0 SPC1, select the <code>sslcert\client.key</code> file in the decompressed SSL certificate directory.</td>
</tr>
<tr>
<td>Root Certificate</td>
<td>When <strong>SSL Mode</strong> is set to <strong>verify-ca</strong>, the root certificate must be configured. Select the <code>sslcert\cacert.pem</code> file in the decompressed SSL certificate directory.</td>
</tr>
<tr>
<td>SSL Password</td>
<td>Set the password for the client SSL key in PK8 format. The default password is <strong>Gauss@MppDB</strong>.</td>
</tr>
<tr>
<td>SSL Mode</td>
<td>Supported SSL modes include:</td>
</tr>
<tr>
<td></td>
<td>- <strong>require</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>verify-ca</strong></td>
</tr>
<tr>
<td></td>
<td>DWS does not support the <strong>verify-full</strong> mode.</td>
</tr>
</tbody>
</table>
Step 9  Click OK to establish the database connection.

If SSL is enabled, click Continue in the displayed Connection Security Alert dialog box.

After the login is successful, the RECENT LOGIN ACTIVITY dialog box is displayed, indicating that the Data Studio is connected to the database. You can run the SQL statement in the SQL Terminal window on the Data Studio page.

For details about how to use other functions of Data Studio, press F1 to view the Data Studio user manual.

---End

2.8 Using Extended Applications to Connect to the Cluster

2.8.1 Managing Extended Applications

After creating a data warehouse cluster, you can add extended applications to the cluster on the Cluster Management page and use the extended applications to connect to the cluster. To connect to a cluster using an extended application, you must specify the cluster's connection address, database name, port, and username and password for logging in to the cluster.

The DWS extended application integrates the open source pgAdmin 4 (web version) client. In pgAdmin, you can type the query content in interactive mode. pgAdmin 4 (web version) can be used by one or more users through web browsers.
Currently, the extended application feature is in the OBT. You can apply for the extended application feature. Move the cursor to **Service Tickets** in the upper right corner of the management console and click **Create Service Ticket** to submit the application for enabling the OBT feature.

For details about the precautions for the OBT features, read the **OBT Trial Use Agreement**.

---

### Adding an Extended Application

**Step 1**  Log in to the management console at [https://console.huaweicloud.com/dws/?locale=en-us](https://console.huaweicloud.com/dws/?locale=en-us).

**Step 2**  In the navigation tree on the left, click **Cluster Management**. All clusters are displayed by default.

**Step 3**  In the cluster list, click the name of the cluster that you want to view. Then click **Application Extension** to display the page.

**Step 4**  Click **Add Application**.

**Step 5**  Set the following parameters on the **Add Application** page. Then, select **I have learned the OBT trial agreement and restrictions on using pgAdmin4**.

- **Application Name**: Select the extended application to be added, for example, pgAdmin4.
- **Application Login Account**: Set the registered login account. Use the email address as the login account.
- **Application Login Password**: Set the registered login password.
- **Confirm Password**: Enter the password again.

**Figure 2-21 Adding an extended application**

![Add Application Form](image.png)
Step 6 Click OK. On the Application Extension page, the system starts to create the extended application.

Wait for approximately 15 minutes. If Running Status of the newly added extended application becomes Available, the extended application is successfully added.

----End

Deleting an Extended Application

Step 1 On the Cluster Management page, click the name of the cluster that you want to view. Then click Application Extension to display the page.

Step 2 In the Operation column of the row where the specified extended application is located, click Delete.

Figure 2-22 Deleting an extended application

Step 3 In the dialog box that is displayed, click OK to delete the extended application.

----End

2.8.2 Using Extended Application pgAdmin4 to Connect to the Cluster

DWS integrates the open source client tool pgAdmin4 (web version) as an extended application. You do not need to download the pgAdmin4 tool and install it. Alternatively, directly use it to connect to the cluster after adding this extended application to the cluster on the DWS management console. This feature is under OBT. You can submit a service ticket to apply for OBT.

To connect to a cluster using the extended application (only the cluster's private network address or private network domain name can be used for the connection), you must specify the cluster's connection address, database name, port, and username and password for logging in to the cluster's database.
Preparations Before Connecting to a Cluster

- You have obtained the username and password for logging in to the database in the data warehouse cluster.
- You have obtained the private network address, including the IP address and port number in the data warehouse cluster, or private network domain name. For details, see Obtaining the Cluster Connection Address.
- The security group rules of the data warehouse cluster must ensure that DWS can receive network access requests from clients. Ensure that the cluster's security group contains rules meeting the following requirements. If the rules do not exist, add them to the security group:
  - **Transfer Direction**: Inbound
  - **Protocol**: The value must contain TCP, for example, TCP and All.
  - **Port**: Set this parameter to the database port that provides services in the data warehouse cluster, for example, 8000.
  - **Source**: The IP address set here must contain the IP address of the DWS client host, for example, 192.168.0.10/32.

**Figure 2-23 Inbound rule**

Adding an Extended Application

**Step 1** Log in to the management console at [https://console.huaweicloud.com/dws/?locale=en-us](https://console.huaweicloud.com/dws/?locale=en-us).

**Step 2** In the navigation tree on the left, click Cluster Management.

All clusters are displayed by default.

**Step 3** In the cluster list, click the name of the cluster that you want to view. Then click Application Extension to display the page.

**Step 4** Click Add Application.

**Step 5** Set the following parameters on the Add Application page. Then, select I have learned the OBT trial agreement and restrictions on using pgAdmin4.
  - **Application Name**: Select the extended application to be added, for example, pgAdmin4.
  - **Application Login Account**: Set the registered login account. Use the email address as the login account.
  - **Application Login Password**: Set the registered login password.
Confirm Password: Enter the password again.

**Figure 2-24** Adding an extended application

### Add Application

- **Application Name**: pgAdmin4
- **Application Login Account**: [Email Address]
  
  Use a valid email address as the login account so that you can receive emails when resetting the password.
- **Application Login Password**: [Password]
- **Confirm Password**: [Password]

I have learned the DBT trail agreement and restrictions on using pgAdmin4.

---

**Step 6** Click OK. On the **Application Extension** page, the system starts to create the extended application.

Wait for approximately 15 minutes. If **Running Status** of the newly added extended application becomes **Available**, the extended application is successfully added.

---

Using Extended Applications to Connect to the Database in a Cluster

**Step 1** On the **Cluster Management** page, click the name of the cluster that you want to view. Then click **Application Extension** to display the page.

**Step 2** Click the **Application Access Address** in the row where the specified extended application is located to open the pgAdmin4 web client login page.

**Step 3** On the login page, enter the **Application Login Account** and **Application Login Password**.
**Figure 2-25** Logging in to the pgAdmin4 web client

Step 4  Click **Login** to log in to the pgAdmin4 web client.

Step 5  In the navigation tree on the left, choose **Servers > Create > Server**.

**Figure 2-26** Create Server

Step 6  On the **General** tab page of the window for creating a server connection, enter a value in **Name**.
Step 7  On the **Connection** tab page, enter the following cluster information.

- **Host name/address**: Enter the cluster's access address. Obtain the cluster's **Private Network Address** and **Private Network Access Domain Name**. For details, see [Obtaining the Cluster Connection Address](#). In this example, enter the **Private Network Address**.

- **Port**: Enter the cluster's port number.

- **Maintenance database**: Enter the name of the database to be connected. If you use the client to connect to the cluster for the first time, enter the default database **postgres**.

- **Username**: Enter the username of the cluster's database. If you use the client to connect to the cluster for the first time, set this parameter to the default administrator configured during cluster creation, for example, **dbadmin**.

- **Password**: Enter the password of the corresponding database user.
Step 8 (Optional) On the SSL tab page, enter the cluster information. The SSL connection mode delivers higher security than the common mode. You are advised to use the SSL mode on the client.

Download the SSL certificate. For details, see (Optional) Downloading SSL Certificate. Then, decompress the certificate file to the specified path.

- **SSL mode**: Select an SSL mode from the drop-down list. Possible values are Allow, Prefer, Require, Disable, and Verify-CA (DWS does not support the Verify-Full mode). If SSL mode is set to Verify-CA, the root certificate is required.

- **Client certificate**: Click and select the `sslcert\client.crt` file in the decompressed directory.

- **Client certificate key**: Click and select the `sslcert\client.key` file in the decompressed directory.

- **Root Certificate**: Based on the selected SSL Mode, click and select the `sslcert\cacert.pem` file in the decompressed directory.

- **(Optional) Certificate revocation list**: List of revoked digital certificates. It is a list consisting of timestamps of all authentications that are abolished by the authentication center.
SSL compression: Whether to enable the certificate compression transmission. Select True to enable the compression transmission, and select False to disable the compressed transmission. In this example, select False (default value).

Figure 2-29 Create Server - SSL

Step 9  After the connection configuration is complete, click Save.

The system attempts to connect to the cluster's database. After the connection is successful, the newly created DWS database is displayed in the navigation tree on the left.

---End

2.8.3 Restrictions on Using pgAdmin4

The following restrictions apply to pgAdmin4:

- Code segments cannot be folded.
- SQL statements cannot be formatted.
- Automatic association is not supported.
The query result cannot be modified.
Objects in the SQL editor window do not have hyperlinks.
Multiple result sets cannot be displayed together.
Graphical execution plans are not supported.
The content cannot be searched.
The Debugger debugging function is not supported.
The database password cannot be saved.
SQL execution plans cannot be queried.
The content of ultra-large result sets cannot be downloaded.

2.9 Using the JDBC and ODBC Drivers to Connect to the Cluster

2.9.1 Development Specifications

If the connection pool mechanism is used during application development, the following specifications must be met. Otherwise, connections in the connection pool have statuses, which will affect the correctness of subsequent operations on the connection pool.

- If the GUC parameter is set in a connection, you must execute `SET SESSION AUTHORIZATION DEFAULT;RESET ALL;` to clear the connection status before returning the connection to the connection pool.
- If a temporary table is used, it must be deleted before the connection is returned to the connection pool.

2.9.2 Downloading the JDBC or ODBC Driver

The JDBC or ODBC driver is used to connect to data warehouse clusters. You can download the JDBC or ODBC driver provided by DWS from the management console or use open source JDBC or ODBC driver.

Open Source JDBC or ODBC Driver

DWS also supports open source JDBC driver: PostgreSQL JDBC 9.3-1103 or later.
DWS also supports open source ODBC driver: PostgreSQL ODBC 09.01.0200 or later.

Downloading the JDBC or ODBC Driver

Step 1 Log in to the DWS management console.
Step 2 In the navigation tree on the left, click Connection Management.
Step 3 In the Driver area, choose a driver that you want to download.
Figure 2-30 Downloading the driver

**JDBC Driver**

Method 1:
Select DWS JDBC Driver and click Download to download the JDBC driver matching the current cluster version. If clusters of different versions are available, you will download the JDBC driver matching the earliest cluster version after clicking Download. If there is no cluster, you will download the JDBC driver of the earliest version after clicking Download. DWS clusters are compatible with earlier versions of JDBC drivers.

Click Historical Version to download the corresponding JDBC driver version. You are advised to download the JDBC driver based on the cluster version.

The JDBC driver can be used on all platforms and depends on JDK 1.6 or later.

If you have clusters of different versions, the system displays a dialog box, prompting you to select the cluster version and download the driver corresponding to the cluster version. In the cluster list on the Cluster Management page, click the name of the specified cluster and click the Basic Information tab to view the cluster version.

Method 2:
Download the SDK software package by configuring the Maven repository. Click Add Maven Dependency. The following page is displayed.

Figure 2-31 Maven page

In the list shown in Figure 2-31, the first column indicates the cluster version, and the second column indicates the version number of the DWS JDBC driver package. Select the driver package based on the cluster version and go to the following page:
Copy the Maven repository information and add it to the `pom.xml` file. For example, add the following code configuration to the `pom.xml` file:

```xml
<dependency>
    <groupId>com.huaweicloud.dws</groupId>
    <artifactId>huaweicloud-dws-jdbc</artifactId>
    <version>1.3.1</version>
</dependency>
```

### ODBC Driver

Select Microsoft Windows x86/x64 or Linux x64 and click Download to download the ODBC driver matching the current cluster version. If clusters of different versions are available, you will download the ODBC driver matching the earliest cluster version after clicking Download. If there is no cluster, you will download the ODBC driver of the earliest version after clicking Download. DWS clusters are compatible with earlier versions of ODBC drivers.

Click Historical Version to download the corresponding ODBC driver version. You are advised to download the ODBC driver based on the cluster version.

The ODBC driver is applicable to the following operating systems only:

- Windows Server 2008 or later or Windows 7 or later
- RHEL 6.4/6.5/6.6/6.7/7.1/7.2
- CentOS 6.4/6.5/6.6/6.7
- EulerOS 2.0 SP2
- SUSE 11 SP1/11 SP2/11 SP3/11 SP4

**NOTE**

Windows drivers can only be 32-bit and can be used in 32-bit or 64-bit operating systems. However, the applications must be 32-bit.

---End
2.9.3 Using a JDBC Driver to Connect to the Database

In DWS, you can use a JDBC driver to connect to database on Linux or Windows. The drivers can connect to the database through the ECS in the public cloud or over the Internet.

When using the JDBC driver to connect to the data warehouse cluster, determine whether to enable SSL authentication. SSL authentication is used to encrypt communication data between the client and the server. It safeguards sensitive data transmitted over the Internet. You can download a self-signed certificate file on the DWS management console. To make the certificate take effect, you must configure the client program using the OpenSSL tool and the Java keytool.

**NOTE**

The SSL connection mode delivers higher security than the common mode. You are advised to use SSL connection when using JDBC to connect to the cluster.

For details about how to use the JDBC interface, see the official document.

**Prerequisites**

- You have installed JDK 1.6 or later and configured environment variables.
- You have downloaded the JDBC driver. For details, see Downloading the JDBC or ODBC Driver.
- DWS also supports open-source JDBC driver: PostgreSQL JDBC 9.3-1103 or later.
- You have downloaded the SSL certificate file. For details, see (Optional) Downloading SSL Certificate.

**Using a JDBC Driver to Connect to the Database**

The procedure for connecting to the database using a JDBC driver in a Linux environment is similar to that in a Windows environment. The following describes the connection procedure in a Windows environment.

**Step 1** Determine whether you want to use the SSL mode to connect to the data warehouse cluster.

- If you use the SSL mode:
  a. Enable SSL connection for the data warehouse cluster. SSL connection is enabled by default. For details, see (Optional) Configuring SSL Connection.
  b. Determine whether you want to perform authentication using a certificate or password.
     - If certificate authentication is configured, go to **Step 2**.
     - If password authentication is configured, go to **Step 4**.

- If you do not use the SSL mode:
  a. Disable SSL connection for the data warehouse cluster. SSL connection is enabled by default. For details, see (Optional) Configuring SSL Connection.
  b. Go to **Step 4**.

**Step 2** If the Linux environment is used, use WinSCP to upload the downloaded SSL certificate file to the Linux environment.

**Step 3** Configure the certificate to enable Secure Sockets Layer (SSL) connection.
1. Decompress the package to obtain the certificate file. Assume that the decompression path is $SSL_PATH.
   You are advised to store the certificate file in a path of the English version and can specify the actual path when configuring the certificate. If the path is incorrect, a message stating that the file does not exist will be prompted.

2. Open the Command Prompt program and switch to the $SSL_PATH\dws_ssl_cert\sslcert path. Run the following commands to import the root license to the TrustStore:
   ```
   openssl x509 -in cacert.pem -out cacert.crt.der -outform der
   keytool -keystore mytruststore -alias cacert -import -file cacert.crt.der
   - cacert.pem indicates the root certificate obtained after decompression.
   - cacert.crt.der indicates the generated intermediate file. You can store the file to another path and change the file name to your desired one.
   - mytruststore indicates the generated TrustStore name and cacert indicates an alias user. You can change the values of mytruststore and cacert as needed.
   ```
   Enter the TrustStore password that you set as prompted and type y to confirm the password. For example, after entering password truststore123, type y.

3. Run the following command to convert the format of the client private key:
   ```
   openssl pkcs12 -export -out client.pkcs12 -in client.crt -inkey client.key
   Enter the private key password of the client, for example, Gauss@MppDB. Then enter your self-defined private key password, for example, key123 and confirm it.
   ```

4. Run the following command to import the private key to KeyStore:
   ```
   keytool -importkeystore -deststorepass Gauss@MppDB -destkeystore client.jks -srckeystore client.pkcs12 -srcstorepass key123 -srcstoretype PKCS12 -alias 1
   ```

**Step 4** Decompress the downloaded JDBC driver to obtain gsjdbc4.jar.

**Step 5** Add the JAR file to the application project so that applications can reference the JAR file.
   Take the Eclipse project as an example. Store the JAR file to the project directory, for example, the lib directory in the project directory. In the Eclipse project, right-click the JAR file in the lib directory and select Build Path to reference the JAR file.
Alternatively, you can use another method. In the Maven project, you can directly add the DWS JDBC driver as a dependency item to the POM file. The configuration is as follows:

```
<dependency>
  <groupId>com.huaweicloud.dws</groupId>
  <artifactId>huaweicloud-dws-jdbc</artifactId>
  <version>1.0.0</version>
</dependency>
```

**Step 6** Load the driver.

The following methods are available:

- Using a code: `Class.forName("org.postgresql.Driver");`
- Using a parameter during the JVM startup: `java -Djdbc.drivers=org.postgresql.Driver jdbctest`

**Step 7** Invoke the DriverManager.getConnection() method of JDBC to connect to the DWS database.

The JDBC interface does not provide the connection retry capability. You need to implement the retry processing in the service code.

The DriverManager.getConnection() method supports following:

- `DriverManager.getConnection(String url);`
- `DriverManager.getConnection(String url, Properties info);`
DriverManager.getConnection(String url, String user, String password);

### Table 2-8 Database connection parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| url       | Specifies the database connection descriptor, which can be viewed on the management console. For details, see [Obtaining the Cluster Connection Address](#). The formats of URL are as follows: jdbc:postgresql://host:port/database
|           | **NOTE** |
|           | • *database* indicates the name of the database to which you want to connect. |
|           | • *host* indicates the name of the database server. |
|           | • *port* indicates the port number of the database server. |
|           | By default, the code tries to connect to the database on **localhost** through port **8000**. |
| info      | Specifies database connection properties. Common properties include the following: |
|           | • *user*: a string type. It indicates the database user who creates the connection task. |
|           | • *password*: a string type. It indicates the password of the database user. |
|           | • *ssl*: a Boolean type. It indicates whether the SSL connection is used. |
|           | • *loglevel*: an Integer type. It determines the log volume of the DriverManager class recorded by the LogStream or LogWriter object. Currently, only `com.edb.Driver.DEBUG` and `com.edb.Driver.INFO` are supported. If you set *loglevel* to INFO, only a limited amount of log information is recorded. If you set *loglevel* to DEBUG, detailed log information is recorded. |
|           | • *charSet*: a string type. It indicates character sets used when data is sent from the database or the database receives data. |
|           | • *prepareThreshold*: an Integer type. It is used to determine the execution times of PreparedStatement before the information is converted into prepared statements on the server. The default value is **5**. |
| user      | Specifies the database user. |
| password  | Specifies the password of the database user. |

The following describes the sample code used to encrypt the connection using the SSL certificate:

```java
// The following code obtains the database SSL connection operation and encapsulates the operation as an interface.

public static Connection GetConnection(String username, String passwd) {
    // Define the driver class.
    String driver = "org.postgresql.Driver";
    // Set keyStore.
    System.setProperty("javax.net.ssl.trustStore", "mytruststore");
    System.setProperty("javax.net.ssl.keyStore", "client.jks");
    // Other connections...
}
```
System.setProperty("javax.net.ssl.trustStorePassword", "password");
System.setProperty("javax.net.ssl.keyStorePassword", "password");

Properties props = new Properties();
props.setProperty("user", username);
props.setProperty("password", passwd);
props.setProperty("ssl", "true");

String url = "jdbc:postgresql://" + "10.10.0.13" + ':'
+ "8000" + '/'
+ "postgres";
Connection conn = null;

try {
    //Load the driver.
    Class.forName(driver);
} catch( Exception e ) {
    e.printStackTrace();
    return null;
}

try {
    //Create a connection.
    conn = DriverManager.getConnection(url, props );
    System.out.println("Connection succeed!");
} catch(Exception e) {
    e.printStackTrace();
    return null;
}

return conn;

The following describes the sample code used to encrypt the connection using the SSL password:

public static Connection GetConnection(String username, String passwd) {
    //Define the driver class.
    String driver = "org.postgresql.Driver";

    Properties props = new Properties();
    props.setProperty("user", username);
    props.setProperty("password", passwd);
    String url = "jdbc:postgresql://" + "10.10.0.13" + ':'
    + "8000" + '/'
    + "postgres";
    Connection conn = null;

    try {
        //Load the driver.
        Class.forName(driver);
    } catch( Exception e ) {
        e.printStackTrace();
        return null;
    }

    try {
        //Create a connection.
        conn = DriverManager.getConnection(url, props );
        System.out.println("Connection succeed!");
    } catch(Exception e) {
        e.printStackTrace();
        return null;
    }

    return conn;
}
Step 8 Run the following command to execute SQL statements:

1. Run the following command to create a statement object:
   ```java
   Statement stmt = con.createStatement();
   ```

2. Run the following command to execute the statement object:
   ```java
   int rc = stmt.executeUpdate("CREATE TABLE tab1(id INTEGER, name VARCHAR(32));");
   ```

3. Run the following command to release the statement object:
   ```java
   stmt.close();
   ```

Step 9 Invoke `close()` to close the connection.

---End

Sample Code

This sample code illustrates how to develop applications based on the JDBC interface provided by DWS.

```java
//DBtest.java
//Demonstrate the main steps for JDBC development, including creating databases,
creating tables, and inserting data.

import java.sql.Connection;
import java.sql.DriverManager;
import java.sql.PreparedStatement;
import java.sql.SQLException;
import java.sql.Statement;
import java.sql.CallableStatement;

public class DBTest {

    //Create a database connection.
    public static Connection GetConnection(String username, String passwd) {
        String driver = "org.postgresql.Driver";
        String sourceURL = "jdbc:postgresql://10.10.0.13:8000/postgres";
        Connection conn = null;
        try {
            // Load the database driver.
            Class.forName(driver).newInstance();
        } catch (Exception e) {
            e.printStackTrace();
            return null;
        } finally {
            try {
                //Create a database connection.
                conn = DriverManager.getConnection(sourceURL, username, passwd);
            } catch (Exception e) {
                e.printStackTrace();
                return null;
            }
        }
    }

    public static void main(String[] args) {
        String username = "admin";
        String passwd = "admin123456";
        Connection conn = GetConnection(username, passwd);
        Statement stmt = conn.createStatement();
        try {
            String SQL = "CREATE TABLE tab1(id INTEGER, name VARCHAR(32));";
            int rc = stmt.executeUpdate(SQL);
            System.out.println("Table created successfully.");
        } catch (SQLException e) {
            System.out.println("SQLException: ");
            e.printStackTrace();
        } finally {
            try {
                //Close the database connection.
                conn.close();
            } catch (SQLException e) {
                System.out.println("SQLException: ");
                e.printStackTrace();
            }
        }
    }
}
```
return conn;
};

//Run the common SQL statements to create table customer_t1.
public static void CreateTable(Connection conn) {
    Statement stmt = null;
    try {
        stmt = conn.createStatement();
        //Run the common SQL statements.
        int rc = stmt.executeUpdate("CREATE TABLE customer_t1(c_customer_sk INTEGER,
            c_customer_name VARCHAR(32));");
        stmt.close();
    } catch (SQLException e) {
        if (stmt != null) {
            try {
                stmt.close();
            } catch (SQLException e1) {
                e1.printStackTrace();
            }
        }
        e.printStackTrace();
    }
}

//Run the prepared statements and insert data in batches.
public static void BatchInsertData(Connection conn) {
    PreparedStatement pst = null;
    try {
        //Generate the prepared statements.
        pst = conn.prepareStatement("INSERT INTO customer_t1 VALUES (?,?)");
        for (int i = 0; i < 3; i++) {
            //Add parameters.
            pst.setInt(1, i);
            pst.setString(2, "data " + i);
            pst.addBatch();
        }
        //Execute batch processing.
        pst.executeBatch();
        pst.close();
    } catch (SQLException e) {
        if (pst != null) {
            try {
                pst.close();
            } catch (SQLException e1) {
                e1.printStackTrace();
            }
        }
        e.printStackTrace();
    }
}

//Run the precompiled statement to update the data.
public static void ExecPreparedSQL(Connection conn) {
    PreparedStatement pstmt = null;
    try {
        pstmt = conn.prepareStatement("UPDATE customer_t1 SET c_customer_name = ? WHERE c_customer_sk = 1");
        pstmt.setString(1, "new Data");
        int rowcount = pstmt.executeUpdate();
        pstmt.close();
    } catch (SQLException e) {
        if (pstmt != null) {
            try {
                pstmt.close();
            } catch (SQLException e1) {
                e1.printStackTrace();
            }
        }
        e.printStackTrace();
    }
}
//Execute the storage procedure.
public static void ExecCallableSQL(Connection conn) {
    CallableStatement cst = null;
    try {
        cst = conn.prepareCall("? = CALL TESTPROC(?,?,?)");
        cst.setInt(2, 50);
        cst.setInt(1, 20);
        cst.setInt(3, 90);
        cst.registerOutParameter(4, Types.INTEGER);  //Register a parameter of
        //the out type. Its value is an integer.
        cst.execute();
        int out = cst.getInt(4);  //Obtain the out parameter.
        System.out.println("The CallableStatement TESTPROC returns:"+out);
        cst.close();
    } catch (SQLException e) {
        if (cst != null) {
            try {
                cst.close();
            } catch (SQLException e1) {
                e1.printStackTrace();
            }
        }
        e.printStackTrace();
    }
}

/**
 * Main program, which gradually invokes each static method.
 * @param args
 */
public static void main(String[] args) {
    //Create a database connection.
    Connection conn = GetConnection("tester", "Password1234");
    //Create a table.
    CreateTable(conn);
    //Insert data in batches.
    BatchInsertData(conn);
    //Run the precompiled statement to update the data.
    ExecPreparedSQL(conn);
    //Execute the storage procedure.
    ExecCallableSQL(conn);
    //Close the database connection.
    try {
        conn.close();
    } catch (SQLException e) {
        e.printStackTrace();
    }
}
2.9.4 Using an ODBC Driver to Connect to the Database

In DWS, you can use an ODBC driver to connect to database either through an ECS in the public cloud or over the Internet.

For details about how to use the ODBC interface, see the official document.

Prerequisites

- You have downloaded ODBC driver packages dws_odbc_driver_for_linux.tar.gz (for Linux) and dws_odbc_driver_for_windows.tar.gz (for Windows). For details, see Downloading the JDBC or ODBC Driver.
- DWS also supports open-source ODBC driver: PostgreSQL ODBC 09.01.0200 or later.
- You have downloaded the open source unixODBC code file 2.3.0 from https://sourceforge.net/projects/unixodbc/files/unixODBC/2.3.0/unixODBC-2.3.0.tar.gz/download.
- You have downloaded the SSL certificate file. For details, see (Optional) Downloading SSL Certificate.

Using an ODBC Driver to Connect to a Database (Linux)

**Step 1**  Upload the ODBC package and code file to the Linux environment and decompress them to the specified directory.

**Step 2**  Log in to the Linux environment as user root.

**Step 3**  Prepare unixODBC.

1. Decompress the unixODBC code file.
   
   ```
   tar -xvf unixODBC-2.3.0.tar.gz
   ```

2. Modify the configuration.

   ```
   cd unixODBC-2.3.0
   vi configure
   ```

   Change the value of LIB_VERSION to the following. Save the change and exit.

   ```
   LIB_VERSION="1:0:0"
   ```

3. Compile the code file and install the driver.

   ```
   ./configure --enable-gui=no
   make
   make install
   ```

**Step 4**  Replace the driver file.

1. Decompress dws_odbc_driver_for_linux.tar.gz.

   ```
   tar -xvf dws_odbc_driver_for_linux.tar.gz
   ```

2. Copy all files in the lib directory to /usr/local/lib. If there are files with the same name, overwrite them.

3. Copy psqlodbcw.la and psqlodbcw.so in the odbc/lib directory to /usr/local/lib.

**Step 5**  Run the following command to modify the configuration of the driver file:

   ```
   vi /usr/local/etc/odbcinst.ini
   ```
Copy the following content to the file:

```plaintext
[DWS]
Driver64=/usr/local/lib/psqlodbcw.so
```

The parameters are as follows:

- **[DWS]**: indicates the driver name. You can customize the name.
- **Driver64 or Driver**: indicates the path where the dynamic library of the driver resides. For a 64-bit operating system, search for **Driver64** first. If **Driver64** is not configured, search for **Driver**.

**Step 6** Run the following command to modify the data source file:

```bash
vi /usr/local/etc/odbc.ini
```

Copy the following content to the configuration file, save the modification, and exit.

```plaintext
[DWSODBC]
Driver=DWS
Servername=10.10.0.13
Database=postgres
Username=dbadmin
Password=Abcd@123
Port=8000
Sslmode=allow
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>[DSN]</td>
<td>Data source name.</td>
<td>[DWSODBC]</td>
</tr>
<tr>
<td>Driver</td>
<td>Driver name, corresponding to <strong>DriverName</strong> in <strong>odbcinst.ini</strong>.</td>
<td>Driver=DWS</td>
</tr>
<tr>
<td>Servername</td>
<td>Server IP address.</td>
<td>Servername=10.10.0.13</td>
</tr>
<tr>
<td>Database</td>
<td>Name of the database to be connected to.</td>
<td>Database=postgres</td>
</tr>
<tr>
<td>Username</td>
<td>Database username.</td>
<td>Username=dbadmin</td>
</tr>
<tr>
<td>Password</td>
<td>Database user password.</td>
<td>Password=Abcd@123</td>
</tr>
<tr>
<td>Port</td>
<td>Port number of the server.</td>
<td>Port=8000</td>
</tr>
</tbody>
</table>
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
</table>
| Sslmode   | SSL certification mode. This parameter is enabled for the cluster by default. Values and meanings:  
  - **disable**: only tries to establish a non-SSL connection.  
  - **allow**: tries to establish a non-SSL connection first, and then an SSL connection if the first attempt fails.  
  - **prefer**: tries to establish an SSL connection first, and then a non-SSL connection if the first attempt fails.  
  - **require**: only tries to establish an SSL connection. If there is a CA file, perform the verification according to the scenario in which the parameter is set to **verify-ca**.  
  - **verify-ca**: tries to establish an SSL connection and check whether the server certificate is issued by a trusted CA.  
  - **verify-full**: DWS does not support this mode.  

**NOTE**  
The SSL connection mode delivers higher security than the common mode. You are advised to use SSL connection when using ODBC to connect to the cluster. |
|           | Sslmode=allow |               |

---

**NOTE**

You can view the values of **Servername** and **Port** on the DWS management console. Log in to the DWS management console and click **Connection Management**. In the **Data Warehouse Connection String** area, select the target cluster and obtain **Private Network Address** or **Public Network Address**. For details, see *Obtaining the Cluster Connection Address*.

**Step 7** Configure environment variables.

```
vi ~/.bashrc
```

Add the following information to the configuration file:

```
export LD_LIBRARY_PATH=/usr/local/lib/:$LD_LIBRARY_PATH
export ODBC_SYSINI=/usr/local/etc
export ODBCINI=/usr/local/etc/odbc.ini
```
Step 8 Import environment variables.

source ~/.bashrc

Step 9 Run the following commands to connect to the database:

/usr/local/bin/isql -v DWSODBC

If the following information is displayed, the connection is successful:

```
+---------------------------------------+
| Connected!                           |
|                                       |
| sql-statement                         |
| help [tablename]                      |
| quit                                  |
|                                       |
+---------------------------------------+

SQL>

----End

Using an ODBC Driver to Connect to a Database (Windows)

Step 1 Decompress ODBC driver package dws_odbc_driver_for_windows.tar.gz (for Windows) and install psqlodbc.msi.

Step 2 Decompress the SSL certificate package to obtain the certificate file.

You can choose to automatically or manually deploy the certificate based on your needs.

Automatic deployment:

Double-click the sslcert_env.bat file. The certificate is automatically deployed to a default location.

Manual deployment:

1. Create a new folder named postgresql in the %APPDATA%\postgresql directory.
2. Copy files client.crt, client.key, client.key.cipher, and client.key.rand to the %APPDATA%\postgresql directory and change client in the file name to postgres. For example, change the name of client.key to postgres.key.
3. Copy cacert.pem to %APPDATA%\postgresql and change the name of cacert.pem to root.crt.

Step 3 Open Driver Manager.

Currently, because DWS only provides a 32-bit ODBC driver, it only supports 32-bit application development. Use the 32-bit Driver Manager when you configure the data source. (Assume the Windows system drive is drive C. If another disk drive is used, modify the path accordingly.)

• In a 64-bit Windows operating system, open C:\Windows\SysWOW64\odbcad32.exe.

Do not open Driver Manager by choosing Control Panel > System and Security > Administrative Tools > Data Sources (ODBC).
NOTE

WOW64 is the acronym for Windows 32-bit on Windows 64-bit. C:\Windows\SysWOW64\ stores the 32-bit environment on a 64-bit system. C:\Windows\System32\ stores the environment consistent with the current operating system. For technical details, see the Windows technical documents.

In a 32-bit Windows operating system, open C:\Windows\System32\odbcad32.exe. You can also open Driver Manager by choosing Control Panel > System and Security > Administrative Tools > Data Sources (ODBC).

Step 4 Configure a data source to be connected to.

1. On the User DSN tab, click Add, and choose PostgreSQL Unicode for setup.

Figure 2-34 Configuring a data source to be connected to

You can view the values of Server and Port on the DWS management console. Log in to the DWS management console and click Connection Management. In the Data Warehouse Connection String area, select the target cluster and obtain Private Network Address or Public Network Address. For details, see Obtaining the Cluster Connection Address.

2. Click Test to verify that the connection is correct. If Connection successful is displayed, the connection is correct.

Step 5 Compile an ODBC sample program to connect to the data source.

The ODBC interface does not provide the database connection retry capability. You need to implement the connection retry processing in the service code.

The sample code is as follows:

```c
// This example shows how to obtain DWS data through the ODBC driver.
// DBtest.c (compile with: libodbc.so)
#include <stdlib.h>
#include <stdio.h>
#include <sqlext.h>
#ifdef WIN32
# include <windows.h>
#endif
SQLHENV       V_OD_Env;        // Handle ODBC environment
```
// Handle statement
V_OD_hstmt;      // Handle statement
SQLHDBC         V_OD_hdbc;       // Handle connection
typename[100];  // Handle statement

// 1. Allocate environment handles.
if ((V_OD_erg != SQL_SUCCESS) && (V_OD_erg != SQL_SUCCESS_WITH_INFO))
    printf("Error AllocHandle\n");
    exit(0);

// 2. Set environment attributes (version information).
if ((V_OD_erg != SQL_SUCCESS) && (V_OD_erg != SQL_SUCCESS_WITH_INFO))
    SQLFreeHandle(SQL_HANDLE_ENV, V_OD_Env);
    exit(0);

// 3. Allocate connection handles.
if ((V_OD_erg != SQL_SUCCESS) && (V_OD_erg != SQL_SUCCESS_WITH_INFO))
    printf("Error SQLConnect %d\n", V_OD_erg);
    SQLFreeHandle(SQL_HANDLE_ENV, V_OD_Env);
    exit(0);

// 4. Set connection attributes.
if ((V_OD_erg != SQL_SUCCESS) && (V_OD_erg != SQL_SUCCESS_WITH_INFO))
    printf("Error SetConnAttr\n");
    SQLFreeHandle(SQL_HANDLE_ENV, V_OD_Env);
    exit(0);

// 5. Connect to a data source. You do not need to enter the username and
// password if you have configured them in the odbc.ini file. If you have not
// configured them, specify the name and password of the user who wants to connect
// to the database in the SQLConnect function.
V_OD_erg = SQLConnect(V_OD_hdbc, (SQLCHAR*) "gaussdb", SQL_NTS,
                     (SQLCHAR*) "", SQL_NTS, (SQLCHAR*) "", SQL_NTS);
if ((V_OD_erg != SQL_SUCCESS) && (V_OD_erg != SQL_SUCCESS_WITH_INFO))
    printf("Error SQLConnect \d\n", V_OD_erg);
    SQLFreeHandle(SQL_HANDLE_ENV, V_OD_Env);
    exit(0);

printf("Connected !\n");
if ((V_OD_erg != SQL_SUCCESS) && (V_OD_erg != SQL_SUCCESS_WITH_INFO))
    printf("Error SetStmtAttr\n");
    SQLFreeHandle(SQL_HANDLE_STMT, V_OD_hstmt);

if ((V_OD_erg != SQL_SUCCESS) && (V_OD_erg != SQL_SUCCESS_WITH_INFO))
    SQLFreeHandle(SQL_HANDLE_STMT, V_OD_hstmt);

// 8. Execute SQL statements.
V_OD_erg = SQLExecDirect(V_OD_hstmt,"drop table IF EXISTS testtable",SQL_NTS);
V_OD_erg = SQLExecDirect(V_OD_hstmt,"create table testtable(id int)",SQL_NTS);
V_OD_erg = SQLExecDirect(V_OD_hstmt,"insert into testtable values(25)",SQL_NTS);
if ((V_OD_erg != SQL_SUCCESS) && (V_OD_erg != SQL_SUCCESS_WITH_INFO))
    printf("Error SQLExecDirect\n");
    SQLFreeHandle(SQL_HANDLE_STMT, V_OD_hstmt);

if ((V_OD_erg != SQL_SUCCESS) && (V_OD_erg != SQL_SUCCESS_WITH_INFO))
    printf("Error SQLPrepare\n");
    SQLFreeHandle(SQL_HANDLE_STMT, V_OD_hstmt);

if ((V_OD_erg != SQL_SUCCESS) && (V_OD_erg != SQL_SUCCESS_WITH_INFO))
    printf("Error SQLBindParameter\n");
    SQLFreeHandle(SQL_HANDLE_STMT, V_OD_hstmt);

// 11. Execute prepared statements.
if ((V_OD_erg != SQL_SUCCESS) && (V_OD_erg != SQL_SUCCESS_WITH_INFO))
    SQLFreeHandle(SQL_HANDLE_STMT, V_OD_hstmt);

// 12. Obtain attributes of a specific column in the result set.
if ((V_OD_erg != SQL_SUCCESS) && (V_OD_erg != SQL_SUCCESS_WITH_INFO))
    SQLFreeHandle(SQL_HANDLE_STMT, V_OD_hstmt);

// 13. Bind the result set.
if ((V_OD_erg != SQL_SUCCESS) && (V_OD_erg != SQL_SUCCESS_WITH_INFO))
    SQLFreeHandle(SQL_HANDLE_STMT, V_OD_hstmt);

// 14. Obtain data in the result set by executing SQLFetch.
if ((V_OD_erg != SQL_SUCCESS) && (V_OD_erg != SQL_SUCCESS_WITH_INFO))
    SQLFreeHandle(SQL_HANDLE_STMT, V_OD_hstmt);

// 15. Obtain and return data by executing SQLGetData.
while(V_OD_erg != SQL_NO_DATA)
2.10 Using the Third-Party Function Library psycopg2 of Python to Connect to a Cluster

After creating a data warehouse cluster and using the third-party function library psycopg2 to connect to the cluster, you can use Python to access DWS and perform various operations on data tables.

Preparations Before Connecting to a Cluster

- An EIP has been bound to the data warehouse cluster.
- You have obtained the administrator username and password for logging in to the database in the data warehouse cluster.
- You have obtained the public network address, including the IP address and port number in the data warehouse cluster. For details, see Obtaining the Cluster Connection Address.
- You have installed the third-party function library psycopg2. The link for downloading psycopg2 is https://pypi.org/project/psycopg2/.

Using the Third-Party Function Library psycopg2 to Connect to a Cluster (Linux)

Step 1  Log in to the Linux environment as user root.

Step 2  Run the following command to create the python_dws.py file and copy the following content to the file:

```python
#!/usr/bin/python
# -*- coding: UTF-8 -*-
import psycopg2

def CreateTable(connection):
    print "Begin to create table"
    try:
        cursor = connection.cursor()
        cursor.execute('''drop table if exists test;create table test(id int,name text);''')
    #print "Table created successfully"
        connection.commit()
    except psycopg2.ProgrammingError,e:
        print e
    else:
        print "Table created successfully"
```

----End
def InsertData(connection):
    print "Begin to insert data"
    try:
        cursor = connection.cursor()
        cursor.execute("insert into test values(1,'number1');")
        cursor.execute("insert into test values(2,'number2');")
        cursor.execute("insert into test values(3,'number3');")
        connection.commit()
    except psycopg2.ProgrammingError,e:
        print e
    else:
        print "Insert data successfully"
        cursor.close()

def UpdateData(connection):
    print "Begin to update data"
    try:
        cursor = connection.cursor()
        cursor.execute("update test set name = 'numberupdated' where id=1;")
        connection.commit()
        print "Total number of rows updated :", cursor.rowcount
        cursor.execute("select * from test;")
        rows=cursor.fetchall()
        for row in rows:
            print "id = ", row[0]
            print "name = ", row[1], "\n"
    except psycopg2.ProgrammingError,e:
        print e
    else:
        print "After Update, Operation done successfully"

def DeleteData(connection):
    print "Begin to delete data"
    try:
        cursor = connection.cursor()
        cursor.execute("delete from test where id=3;")
        connection.commit()
        print "Total number of rows deleted :", cursor.rowcount
        cursor.execute("select * from test;")
        rows=cursor.fetchall()
        for row in rows:
            print "id = ", row[0]
            print "name = ", row[1], "\n"
    except psycopg2.ProgrammingError,e:
        print e
    else:
        print "After Delete, Operation done successfully"

def SelectData(connection):
    print "Begin to select data"
    try:
        cursor = connection.cursor()
        cursor.execute("select * from test;")
        rows=cursor.fetchall()
        for row in rows:
            print "id = ", row[0]
            print "name = ", row[1], "\n"
    except psycopg2.ProgrammingError,e:
        print e
    else:
        print "Operation failed"
    else:
        print "Operation done successfully"
        cursor.close()
if __name__ == '__main__':
    try:
        connection = psycopg2.connect(host='10.154.70.231', port='8000',
                                       database='postgres', user='dbadmin', password='Bigdata_2013')
        except psycopg2.DatabaseError, e:
            print e
            print "Connect database failed"
    else:
        print "Opened database successfully"
        CreateTable(connection)
        InsertData(connection)
        SelectData(connection)
        UpdateData(connection)
        DeleteData(connection)
        connection.close()

Step 3  Change the public network address, cluster port number, database name, database username,
and database password in the python_dws.py file based on the actual cluster information.

The psycopg2 interface does not provide the connection retry capability. You need to
implement the retry processing in the service code.

connection = psycopg2.connect(host='10.154.70.231', port='8000',
                                  database='postgres', user='dbadmin', password='Bigdata_2013')

Step 4  Run the following command to connect to the cluster using the third-party function library
psycopg:

python python_dws.py

----End

Using the Third-Party Function Library psycopg2 to Connect to a Cluster
(Windows)

Step 1  In the Windows operating system, click the Start button, enter cmd in the search box, and
click cmd.exe in the result list to open the CLI.

Step 2  On the CLI, run the following command to create the python_dws.py file and copy the
following content to the file:

type nul> python_dws.py
#!/usr/bin/python
# -*- coding: UTF-8 -*-
import psycopg2

def CreateTable(connection):
    print "Begin to create table"
    try:
        cursor = connection.cursor()
        cursor.execute('''drop table if exists test;create table test(id int,
name text);''')
        #print "Table created successfully"
        connection.commit()
    except psycopg2.ProgrammingError,e:
        print e
    else:
        print "Table created successfully"
        cursor.close()

def InsertData(connection):
    print "Begin to insert data"
    try:
cursor = connection.cursor()
cursor.execute("insert into test values(1,'number1');")
cursor.execute("insert into test values(2,'number2');")
cursor.execute("insert into test values(3,'number3');")
connection.commit()
except psycopg2.ProgrammingError,e:
  print e
else:
  print "Insert data successfully"
cursor.close()

def UpdateData(connection):
  print "Begin to update data"
  try:
    cursor = connection.cursor()
    cursor.execute("update test set name = 'numberupdated' where id=1;")
    connection.commit()
    print "Total number of rows updated :", cursor.rowcount
    cursor.execute("select * from test;")
    rows=cursor.fetchall()
    for row in rows:
      print "id = ", row[0]
      print "name = ", row[1], "\n"
  except psycopg2.ProgrammingError,e:
    print e
  else:
    print "After Update, Operation done successfully";

def DeleteData(connection):
  print "Begin to delete data"
  try:
    cursor = connection.cursor()
    cursor.execute("delete from test where id=3;")
    connection.commit()
    print "Total number of rows deleted :", cursor.rowcount
    cursor.execute("select * from test;")
    rows=cursor.fetchall()
    for row in rows:
      print "id = ", row[0]
      print "name = ", row[1], "\n"
  except psycopg2.ProgrammingError,e:
    print e
  else:
    print "After Delete, Operation done successfully";

def SelectData(connection):
  print "Begin to select data"
  try:
    cursor = connection.cursor()
    cursor.execute("select * from test;")
    rows=cursor.fetchall()
    for row in rows:
      print "id = ", row[0]
      print "name = ", row[1], "\n"
  except psycopg2.ProgrammingError,e:
    print e
  except 
    print "select failed"
  else:
    print "Operation done successfully";
cursor.close()
Step 3  Change the public network address, cluster port number, database name, database username, and database password in the `python_dws.py` file based on the actual cluster information.

```python
connection = psycopg2.connect(host='10.154.70.231', port='8000',
database='postgres', user='dbadmin', password='Bigdata_2013')
connection.close()
```

Step 4  In the CLI, run the following command to use psycopg to connect to the cluster:

```
python python_dws.py
```

---End

### 2.11 Connecting to a Cluster Using IAM Authentication

#### 2.11.1 Overview

DWS allows you to access databases using IAM authentication. When you use the JDBC application program to connect to a cluster, set the IAM username, credential, and other information as you configure the JDBC URL. After doing this, when you try to access a database, the system will automatically generate a temporary credential and a connection will be set up.

**NOTE**

Currently, only clusters whose version is 1.3.1 or later (including 1.3.1) and corresponding JDBC driver provided by DWS can access the databases in IAM authentication mode.

IAM supports two types of user credential: password and Access Key ID/Secret Access Key (AK/SK). JDBC connection requires latter.

The IAM account you use to access a database must be granted with the **DWS Database Access** permission. Only users with both the **DWS Administrator** and **DWS Database Access** permissions connect to DWS databases using the temporary database user credentials generated based on IAM users.

The process of accessing a database is as follows:

1. **Granting an IAM Account the DWS Database Access Permission**
2. **Creating an IAM User Credential**
3. **Configuring the JDBC Connection to Connect to a Cluster Using IAM Authentication**

#### 2.11.2 Granting an IAM Account the DWS Database Access Permission

The IAM account you use to access a database must be granted with the **DWS Database Access** permission. Only users with both the **DWS Administrator** and **DWS Database Access** permissions...
Access permissions can connect to DWS databases using the temporary database user credentials generated based on IAM users. Using the DWS Database Access permission helps to control access to databases.

The DWS Database Access permission can only be granted to user groups. Ensure that your IAM account is in a user group with this permission.

On IAM, only users in the admin group have the permissions to manage users. This requires that your IAM account be in the admin user group. Otherwise, contact the administrator to grant your IAM account this permission.

Procedure

Step 1 Log in to the public cloud management console and choose Service List > Mgmt & Deployment > Identity and Access Management to enter the IAM management console.

Step 2 Modify the user group to which your IAM user belongs. Set a policy for, grant the DWS Database Access permission to, and add your IAM user to it.

Only users in the admin user group of IAM can perform this step. In IAM, only users in the admin user group can manage users, including creating user groups and users and setting user group rights.

For details, see Viewing or Modifying User Group Information in the Identity and Access Management User Guide.

You can also create an IAM user group, and set a policy for, grant the DWS Administrator and DWS Database Access permissions to, and add your IAM user to it. For details, see Creating a User Group and Assigning Permissions in the Identity and Access Management User Guide.

---End

2.11.3 Creating an IAM User Credential

You can log in to the management console to create an Access Key ID (AK)/Secret Access Key (SK) pair or use an existing one.

Creating an AK/SK Pair

Log in to the management console, move your cursor over the username in the upper right corner, and choose My Credential. Click the Access Keys tab. On the Access Keys tab page, you can view the existing AKs or click Create Access Key to create an AK/SK pair.

The AK/SK pair is so important that you can download the private key file containing the AK/SK information only when you create the pair. On the management console, you can only view the AKs. If you have not downloaded the file, obtain it from your administrator or create an AK/SK pair again.

NOTE

Each user can create a maximum of two AK/SK pairs, which are valid permanently. To ensure account security, change your AK/SK pairs periodically and keep them safe.
2.11.4 Configuring the JDBC Connection to Connect to a Cluster
Using IAM Authentication

When you use the JDBC application program to connect to a cluster, set the IAM username, credential, and other information as you configure the JDBC URL. After doing this, when you try to access a database, the system will automatically generate a temporary credential and a connection will be set up.

**NOTE**

Currently, only clusters whose version is 1.3.1 or later (including 1.3.1) and corresponding JDBC driver provided by DWS can access the databases in IAM authentication mode. Download the JDBC driver. For details, see [Downloading the JDBC or ODBC Driver](#).

Configuring JDBC Connection Parameters

**Table 2-9 Database connection parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| url       | gsjdbc4.jar/gsjdbc200.jar database connection descriptor The JDBC interface does not provide the connection retry capability. You need to implement the retry processing in the service code. The URL example is as follows: jdbc:dws:iam://dws-IAM-demo:cn-north-1/postgres?AccessKeyID=XXXXXXXXXXXXXXXXXXXXXXXXXXXXX&SecretAccessKey=XXXXXXXXXXXXXXXXXXXXXXXXXX&DbUser=user_test&AutoCreate=true

**NOTE**

- *jdbc:dws:iam* is a prefix in the URL format.
- *dws-IAM-demo* indicates the name of the cluster containing the database.
- *cn-north-1* is the region where the cluster resides. For details about DWS regions, visit [Regions and Endpoints](#).
- *postgres* indicates the name of the database to which you want to connect.
- *AccessKeyID* and *SecretAccessKey* are the access key ID and secret access key corresponding to the IAM user specified by *DbUser*.
- Set *DbUser* to the IAM username. Note that the current version does not support hyphens (-) in the IAM username.
  - If the user specified by *DbUser* exists in the database, the temporary user credential has the same permissions as the existing user.
  - If the user specified by *DbUser* does not exist in the database and the value of *AutoCreate* is true, a new user named by the value of *DbUser* is automatically created. The created user is a common database user by default.
  - Parameter *AutoCreate* is optional. The default value is false. It indicates whether to automatically create a database user named by the value of *DbUser* in the database.
  - The value true indicates that a user is automatically created. If the user already exists, the user will not be created again.
  - The value false indicates that a user is not created. If the username specified by *DbUser* does not exist in the database, an error is returned.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| info      | Database connection properties. Common properties include the following:  
• **ssl**: a Boolean type. It indicates whether the SSL connection is used.  
• **loglevel**: an Integer type. It sets the log amount recorded in DriverManager for LogStream or LogWriter.  
Currently, `org.postgresql.Driver.DEBUG` and `org.postgresql.Driver.INFO` logs are supported. If the value is 1, only `org.postgresql.Driver.INFO` (little information) is recorded. If the value is greater than or equal to 2, `org.postgresql.Driver.DEBUG` and `org.postgresql.Driver.INFO` logs are printed, and detailed log information is generated. Its default value is 0, which indicates that no logs are printed.  
• **charSet**: a string type. It indicates character sets used when data is sent from the database or the database receives data.  
• **prepareThreshold**: an Integer type. It is used to determine the execution times of PreparedStatement before the information is converted into prepared statements on the server. The default value is 5. |

**Example**

```java
//The following uses gsjdbc4.jar as an example.  
//The following encapsulates the database connection obtaining operations into an interface. You can connect to the database by specifying the region where the cluster is located, cluster name, access key ID, secret access key, and the corresponding IAM username.

public static Connection GetConnection(String clustername, String regionname,  
String AK, String SK, String username)  
{  
    //Driver class  
    String driver = "org.postgresql.Driver";  
    //Database connection descriptor  
    String sourceURL = "jdbc:dws:iam://" + clustername + ":" + regionname + "/postgres?+*AccessKeyId=AK+*SecretAccessKey=SK+*DBUser=username+*autoCreate=true";  
    Connection conn = null;  
    try  
    {  
        //Load the driver.  
        Class.forName(driver);  
    }  
    catch (Exception e)  
    {  
        return null;  
    }  
    try  
    {  
        //Create a connection.  
        conn = DriverManager.getConnection(sourceURL);  
        System.out.println("Connection succeed!");  
    }  
    catch (Exception e)  
    {  
        return null;  
    }
```
2.12 Managing Database Connections

Scenario

This section describes how to manage database connections to optimize database performance when the number of users and applications that can connect to the database is limited.

Viewing the Maximum Number of Connections

**Step 1** Use the SQL client tool to connect to the database in a cluster.

**Step 2** Run the following command:

```
SHOW max_connections;
```

The following information shows that the maximum number of database connections is 200 by default.

```
max_connections
------------
200
(1 row)
```

----End

Viewing the Number of Used Connections

**Step 1** Use the SQL client tool to connect to the database in a cluster.

**Step 2** View the number of connections in scenarios described in Table 2-10.

Table 2-10 Viewing the number of connections

<table>
<thead>
<tr>
<th>Description</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>View the maximum number of sessions connected to a specific user.</td>
<td>Run the following command to view the maximum number of sessions connected to user <code>dbadmin</code>. <code>-1</code> indicates that the number of sessions connected to user <code>dbadmin</code> is not limited.</td>
</tr>
</tbody>
</table>

```sql
postgres=# SELECT ROLNAME, ROLCONNLIMIT FROM PG_ROLES WHERE ROLNAME='dbadmin';
rolname  | rolconnlimit
----------+--------------
dwsadmin |           -1  
(1 row)
```

----End
<table>
<thead>
<tr>
<th>Description</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>View the number of session connections that have been used by a user.</td>
<td>Run the following command to view the number of session connections that have been used by <code>dbadmin</code>. <code>1</code> indicates the number of session connections that have been used by <code>dbadmin</code>.</td>
</tr>
<tr>
<td></td>
<td><code>postgres=# SELECT COUNT(*) FROM V$SESSION WHERE USERNAME='dbadmin';</code></td>
</tr>
<tr>
<td></td>
<td><code>count -------</code></td>
</tr>
<tr>
<td></td>
<td><code>1</code></td>
</tr>
<tr>
<td></td>
<td><code>(1 row)</code></td>
</tr>
<tr>
<td>View the maximum number of sessions connected to a specific database.</td>
<td>Run the following command to view the maximum number of sessions that are allowed to connect to database <code>postgres</code>. <code>-1</code> indicates that the number of sessions connected to database <code>postgres</code> is not limited.</td>
</tr>
<tr>
<td></td>
<td><code>postgres=# SELECT DATNAME,DATCONNLIMIT FROM PG_DATABASE WHERE DATNAME='postgres';</code></td>
</tr>
<tr>
<td></td>
<td>`datname</td>
</tr>
<tr>
<td></td>
<td>`----------</td>
</tr>
<tr>
<td></td>
<td>`postgres</td>
</tr>
<tr>
<td></td>
<td><code>(1 row)</code></td>
</tr>
<tr>
<td>View the number of session connections that have been used by a database.</td>
<td>Run the following command to view the number of session connections that have been used by <code>postgres</code>. <code>1</code> indicates the number of connections that have been used by <code>postgres</code>.</td>
</tr>
<tr>
<td></td>
<td><code>postgres=# SELECT COUNT(*) FROM PG_STAT_ACTIVITY WHERE DATNAME='postgres';</code></td>
</tr>
<tr>
<td></td>
<td><code>count -------</code></td>
</tr>
<tr>
<td></td>
<td><code>1</code></td>
</tr>
<tr>
<td></td>
<td><code>(1 row)</code></td>
</tr>
<tr>
<td>View the number of session connections that have been used by all users.</td>
<td>Run the following command to view the number of session connections that have been used by all users:</td>
</tr>
<tr>
<td></td>
<td><code>postgres=# SELECT COUNT(*) FROM V$SESSION;</code></td>
</tr>
<tr>
<td></td>
<td><code>count -------</code></td>
</tr>
<tr>
<td></td>
<td><code>10</code></td>
</tr>
<tr>
<td></td>
<td><code>(1 row)</code></td>
</tr>
</tbody>
</table>

---End
3 Managing Snapshots

3.1 Overview

A snapshot is a complete backup that records point-in-time configuration data and service data of a data warehouse cluster. You can use it to restore the cluster data backed up during snapshot creation. Snapshots are stored on OBS.

**NOTE**
- DWS provides some free-of-charge storage space for you to store snapshot data. However, when you use more space than the free-of-charge storage space, the excessive space is charged based on the OBS charging rule. For details, see [OBS Pricing Details](#).
- The free-of-charge space is twice the size of the total storage space of your cluster because the snapshot data is stored in dual-copy mode. (Free-of-charge space = Storage space of a single node x Number of nodes x 2)

A snapshot contains the data in databases running in a cluster and the cluster information, including the node quantity, flavor, and administrator username. If you need to restore from a snapshot, DWS creates a new cluster and restores all databases from the snapshot data. The new cluster created from the snapshot has the same configurations (including the number and flavor of nodes) as those of the original cluster. When restoring a snapshot to a new cluster, if you do not specify other values, the parameter settings retain the same as those backed up in the snapshot. For details about how to restore a cluster from a snapshot, see [Restoring a Snapshot](#).

There are two types of snapshots: automated and manual.

**Manual Snapshots**

You can create manual snapshots at any time. Manual snapshots are full backups, so creating them takes a long time. After a manual snapshot is created, it is saved until you delete it from the DWS management console. For details about how to delete a manual snapshot, see [Deleting Manual Snapshots](#).

**Automated Snapshots**

When automated snapshots are enabled for a cluster, DWS periodically takes snapshots of that cluster based on the time and interval you set, usually every eight hours. Automated snapshots
are enabled by default when you create a cluster. The retention period of an automated snapshot can be set to 1 to 10 days. The default retention period is 3 days. The system deletes the snapshot at the end of the retention period. You can set the automated snapshot policy for a cluster on the DWS management console. For details, see Setting the Automated Snapshot Policy.

To disable the automated snapshot policy, turn the switch off. If you disable automated snapshot, DWS stops taking snapshots and deletes existing automated snapshots of the corresponding cluster. Exercise caution when performing this operation.

Only DWS can delete automated snapshots; you cannot delete them manually. DWS deletes automated snapshots at the end of a snapshot's retention period, when you disable automated snapshots, or when you delete the cluster.

If you want to keep an automated snapshot for a longer period, you can create a copy of it as a manual snapshot. The automated snapshot is retained until the end of the retention period, but the corresponding manual snapshot is retained until you manually delete it. For details about how to copy an automated snapshot, see Copying Automated Snapshots.

Backup and Restoration Policies of Automated Snapshots

Automated snapshots adopt differential incremental backups. The automated snapshot created for the first time is a full backup (base version), and then the system creates full backups at a specified interval. Incremental backups are generated between two full backups. The incremental backup records change based on the previous backup. During snapshot restoration, DWS uses all backups between the latest full backup and the current incremental backup to restore the cluster. Therefore, no data loss occurs. To ensure that every incremental snapshot can be used for data restoration, if its retention period exceeds the upper limit, DWS does not delete it immediately. Instead, DWS retains it for next cluster restoration using subsequent incremental snapshots. DWS deletes the previous full snapshot and related incremental snapshots only after a new full snapshot is created. If you disable the automated snapshot function for an existing cluster, all its automated snapshots will be deleted. However, manual snapshots will not be deleted.

3.2 Manually Creating a Snapshot

Scenario

A snapshot is a complete backup that records point-in-time configuration data and service data of a data warehouse cluster. This section describes how to create a snapshot on the Snapshot Management page to back up cluster data.
Impact on the System

A cluster for which a snapshot is being created temporarily cannot provide complete services. For example, you cannot restart the cluster, resize it, reset the password, or modify the cluster configuration information during snapshot creation. To ensure integrity of the snapshot data, stop writing data to the cluster when you are creating a snapshot.

Prerequisites

The cluster for which a snapshot is to be created must be in the Available, Read-only, or Low performance status.

Procedure

Step 1 Log in to the DWS management console.

Step 2 In the navigation tree on the left, click Snapshot Management.

Step 3 Click Create Snapshot.

- **Cluster Name**: Select a data warehouse cluster from the drop-down list. The drop-down list only displays clusters that are in the Available state.
- **Snapshot Name**: Enter a snapshot name. The snapshot name must be 4 to 64 characters in length and start with a letter. It is case-insensitive and contains only letters, digits, hyphens (-), and underscores (_).
- **Snapshot Description**: Enter the snapshot information. This parameter is optional. The snapshot description contains 0 to 256 characters and does not support special characters !<>="&".

Figure 3-1 Creating a snapshot

Step 4 Click OK.
Task status of the cluster for which you are creating a snapshot is **Creating snapshot**. The status of the snapshot that is being created is **Creating**. After the snapshot is created, its status becomes **Available**.

**NOTE**

If the snapshot size is much greater than that of the data stored in the cluster, it is possible that data is labeled with a deletion tag, but is not cleared and reclaimed. Clear the data and create a snapshot again. For details, see [How Can I Clear and Reclaim the Storage Space?](#).

-----End

### 3.3 Setting the Automated Snapshot Policy

This section describes how to set the automated snapshot policy for a cluster. After the automated snapshot policy is enabled, the system automatically creates snapshots based on the preset time and period.

**Setting the Automated Snapshot Policy**

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

**Step 2** In the navigation tree on the left, click **Cluster Management**.

**Step 3** In the cluster list, click the name of the cluster that you want to view. Then click **Snapshots**.

**Step 4** On the **Snapshots** page, click the **Snapshot Policy** switch to enable the policy.

- ![Status](#) indicates that the policy is enabled.
- ![Status](#) indicates that the policy is disabled. By default, the policy is enabled.

**Step 5** On the **Snapshot Policy** page, configure the following parameters:

**Figure 3-2** Configuring the automated snapshot policy
Table 3-1 Parameter description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retention Days</td>
<td>Set the retention days of the snapshots that are automatically created. The value ranges from 1 to 10 days. <strong>NOTE</strong> You cannot delete the snapshots that are automatically created. The system automatically deletes these snapshots when their retention duration expires.</td>
</tr>
<tr>
<td>Execution Period</td>
<td>Set the cycle for creating automated snapshots. You can specify several days in a week for creating snapshots, and set the execution frequency. You can have the system to create a snapshot every day or every several hours each day.</td>
</tr>
</tbody>
</table>

**Step 6** Click OK.

**Step 7** (Optional) Click **Modify Snapshot Policy** to modify the automatic creation policy you have enabled.

----End

### 3.4 Viewing Snapshot Information

This section describes how to view snapshot information on the **Snapshot Management** page.

**Viewing Snapshot Information**

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

**Step 2** In the navigation tree on the left, click **Snapshot Management**.

In the snapshot list, all snapshots are displayed by default. Click next to the snapshot name to display the snapshot details.

**Figure 3-3** Snapshot management

**Step 3** You can view **Snapshot Name**, **Snapshot Status**, **Cluster Name**, **Snapshot Type**, and **Snapshot Created** of snapshots.

You can also enter a snapshot name or cluster name in the upper right corner of the snapshot list and click to search for the specified snapshot. DWS supports fuzzy search.
Table 3-2 describes snapshot status.

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available</td>
<td>Indicates that the existing snapshot works properly.</td>
</tr>
<tr>
<td>Creating</td>
<td>Indicates that a snapshot is being created.</td>
</tr>
<tr>
<td>Unavailable</td>
<td>Indicates that the existing snapshot cannot provide services.</td>
</tr>
</tbody>
</table>

Table 3-3 describes the snapshot types.

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual</td>
<td>Indicates the snapshot that you manually create through the DWS management console or using APIs. You can delete the snapshots that are manually created.</td>
</tr>
<tr>
<td>Automated</td>
<td>Indicates the snapshot that is automatically created after the automatic snapshot backup policy is enabled. You cannot delete the snapshots that are automatically created. The system automatically deletes the snapshots whose retention duration expires.</td>
</tr>
</tbody>
</table>

3.5 Copying Automated Snapshots

This section describes how to copy snapshots that are automatically created to generate manual snapshots for long-term retention.

Copying an Automated Snapshot

Step 1  Log in to the DWS management console.

Step 2  In the navigation tree on the left, click Snapshot Management.

All snapshots are displayed by default. You can copy the snapshots that are automatically created.

Step 3  In the Operation column of the snapshot that you want to copy, click Copy.

- **New Snapshot Name**: Enter a new snapshot name.
  
  The snapshot name must be 4 to 64 characters in length and start with a letter. It is case-insensitive and contains only letters, digits, hyphens (-), and underscores (_).

- **Snapshot Description**: Enter the snapshot information.
  
  This parameter is optional. The snapshot description contains 0 to 256 characters and does not support special characters !<>"=&".
Figure 3-4 Copying a snapshot

Copy Snapshot

* Snapshot Name  dws-dws-12b9-o-20160228015010

* Snapshot Name

Snapshot Description

Step 4  Click OK. The system starts to copy the snapshot for the cluster.

The system displays a message indicating that the snapshot is successfully copied and delivered. After the snapshot is copied, the status of the copied snapshot is Available.

NOTE

If the snapshot size is much greater than that of the data stored in the cluster, it is possible that data is labeled with a deletion tag, but is not cleared and reclaimed. Clear the data and create a snapshot again. For details, see How Can I Clear and Reclaim the Storage Space?.

----End

3.6 Restoring a Snapshot

Scenario

This section describes how to restore a snapshot when you want to check point-in-time snapshot data of the cluster. To ensure that the services of the cluster for which you want to restore the snapshot are uninterrupted, DWS creates a new cluster with the same flavor and node quantity as the original cluster by default and imports the snapshot data.

Prerequisites

- The number of nodes in the cluster for which you want to restore snapshots must be less than or equal to the user's remaining node quota.
- The status of the snapshot is Available.

Restoring a Snapshot to a New Cluster

Step 1  Log in to the DWS management console.
Step 2  In the navigation tree on the left, click **Snapshot Management**. All snapshots are displayed by default.

Step 3  In the **Operation** column of the snapshot that you want to restore, click **Restore**.

Step 4  Configuring parameters for the new cluster.

You can only configure the following parameters. Retain values of other parameters. For details, see **Creating a Cluster**.

- **Region**
- **AZ**
- **Cluster Type**: The parameter can only be viewed by OBT users.
- **Node Flavor**
  - **dws.m3.xlarge** can be restored to **dws.m3.xlarge** or **dws.d2.xlarge**.
  - Other flavor and backup information remains unchanged.
- **Cluster Name**
- **Database Port**
- **VPC**
- **Subnet**
- **Security Group**
- **EIP**
- **Enterprise Project**
- **Advanced Settings**
  - When **Custom** is selected, set the following parameters:
    - **Automated Snapshot**
      - When **Automated Snapshot** is enabled, set the following parameters:
        - **Retention Days**
        - **Execution Period**
    - **Parameter Template**
    - **Tag**
    - **KMS Key**

Step 5  Click **Restore Now**. The **Restore Snapshot to New Cluster** page is displayed.

Step 6  Click **Submit** to restore the snapshot to the new cluster.

**NOTE**

If the number of applied nodes, vCPU (cores), or memory (GB) exceed the user's remaining quota, a warning dialog box is displayed indicating insufficient quota and displaying the detailed remaining quota and the current quota application information. In this case, you can click **Increase quota** in the warning dialog box to submit a service ticket and apply for higher node quota.

For details about quota, see **What Is User Quota?**.

When the status of the new cluster changes to **Available**, the snapshot is restored.

After the snapshot is restored, the private network address and EIP (if **EIP** is set to **Automatically assign**) are automatically assigned.

---End
3.7 Deleting Manual Snapshots

On the Snapshot Management page of the DWS management console, you can delete an unwanted snapshot in the Unavailable state or delete an available snapshot to release the storage space.

Deleted snapshots cannot be recovered. Exercise caution when performing this operation.

Deleting a Snapshot

Step 1   Log in to the DWS management console.

Step 2   In the navigation tree on the left, click Snapshot Management.

All snapshots are displayed by default.

Step 3   In the Operation column of the snapshot that you want to copy, click Delete.

  ▶️ NOTE

You can delete snapshots that are manually created only.

Step 4   In the dialog box that is displayed, click Yes to delete the snapshot.

----End
Managing Parameter Templates

To facilitate database parameter configuration, DWS provides the parameter template function. A parameter template contains some common database parameters. You can manage parameter templates on the DWS management console. After applying a parameter template to a cluster, you can modify parameters on the parameter modification page of the cluster.

The following parts are included in this section:

- Parameter Template Overview
- Parameter Description
- Creating a Parameter Template
- Modifying a Parameter Template
- Applying a Parameter Template to the Cluster
- Deleting a Parameter Template

Parameter Template Overview

A parameter template is a set of parameters applicable to data warehouses. All parameters in the template have default values. The parameters include the session timeout interval, date, and time format. For details, see Parameter Description. You can adjust parameter values to better adapt the database to actual services. When creating a cluster, you can specify a parameter template for it. Parameters in the template will be applied to all databases in the cluster. If you do not specify a parameter template, the system applies the default parameter template to the cluster. After a cluster is created, you can modify the parameters on the Parameter Modifications page. Alternatively, select an existing parameter template or create a parameter template on the Parameter Template Management page and apply it to the cluster.

DWS presets a default parameter template to data warehouses of each version. The default parameter template cannot be deleted and modified. If you want to modify parameter values in the template, create a customized parameter template. The parameters in the customized template can be modified. After a user-defined parameter template is applied to a cluster, it is not associated with the cluster. If you modify the parameter values in the template, the modifications will not be synchronized to the cluster. You need to apply the template to the cluster again, and then the modified parameter values can be applied to the cluster. Similarly, if you modify parameters on the cluster details page, the modifications will not be synchronized to the parameter template.
## Parameter Description

### Table 4-1 Parameter description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>session_timeout</td>
<td>Sets the timeout interval of an idle session. The value 0 indicates that the timeout limit is disabled. The unit is second. The value ranges from 0 to 86400.</td>
<td>600</td>
</tr>
<tr>
<td>datestyle</td>
<td>Sets the display format for date and time.</td>
<td>ISO,MDY</td>
</tr>
<tr>
<td>failed_login_attempts</td>
<td>Sets the number of consecutive incorrect password attempts after which the account is locked. The value 0 indicates that the number of incorrect password attempts is not limited. The value ranges from 0 to 1000.</td>
<td>10</td>
</tr>
<tr>
<td>timezone</td>
<td>Sets the time zone displayed in the time stamps.</td>
<td>UTC</td>
</tr>
<tr>
<td>log_timezone</td>
<td>Sets the time zone for timestamps in the server log.</td>
<td>UTC</td>
</tr>
<tr>
<td>enable_resource_record</td>
<td>Enables or disables the resource recording function. If the actual execution time of an SQL statement is greater than the value of <em>resource_track_duration</em> (the default value is 60s; customizable), the monitoring information will be archived. This function will cause storage space expansion and slightly affect system performance. Disable it when it is not required.</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE**

- Archiving: The monitoring information is stored in the history view and archived in the info table. The archiving time is 3 minutes. After the archiving, records in the history view are cleared.
- History view
  - GS_WLM_SESSION_HISTORY;
  - GS_WLM_SESSION_INFO
- History view
  - GS_WLM_OPERATOR_HISTORY;
  - GS_WLM_OPERATOR_INFO

- off
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>resource_track_cost</td>
<td>Sets the minimum execution cost for resource monitoring on statements. The value <code>-1</code> indicates that resource monitoring is disabled (execution cost less than 10). If the value is greater than or equal to 0, and the cost of executing statements exceeds the value and is greater than or equal to 10, resource monitoring is performed. You can run the SQL command <em>Explain</em> to query the estimated execution cost of an SQL statement. This parameter is valid only when the cluster version is 1.5.0 or later.</td>
<td>100000</td>
</tr>
<tr>
<td>resource_track_duration</td>
<td>Sets the minimum time for archiving executed statements recorded during real-time monitoring.</td>
<td>60</td>
</tr>
<tr>
<td>password_effect_time</td>
<td>Sets the validity period of the account password. When the password is about to expire or has expired, the system prompts the user to change the password. The value ranges from 0 to 999, in days. If this parameter is set to 0, the function is disabled. This parameter is valid only when the cluster version is 1.5.0 or later.</td>
<td>90</td>
</tr>
<tr>
<td>update_lockwait_timeout</td>
<td>Sets the maximum duration that a lock waits for concurrent updates on a row to complete. If the lock waiting time exceeds the specified value, an error is reported. The value 0 indicates that an error is reported when there is a lock without waiting for a period of time. The default value is 120000, in milliseconds. This parameter is valid only when the cluster version is 1.5.100 or later.</td>
<td>120000</td>
</tr>
</tbody>
</table>
Creating a Parameter Template

If parameters in the default parameter template cannot meet service requirements, you can customize a parameter template and modify the parameter values to better adapt to services.

To create a parameter template, perform the following steps:

**Step 1**  Log in to the management console at https://console.huaweicloud.com/dws/?locale=en-us.

**Step 2**  In the navigation tree on the left, click Parameter Template Management.

**Step 3**  Click Create Parameter Template and set the following parameters:

- **Database Engine**: Select a database engine.
- **Database Version**: Select a database version.
- **Name**: Enter the name of the new parameter template. Enter 4 to 64 characters. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed. The value must start with a letter. Letters are case-insensitive.
- **Description**: Enter the description of the new parameter template. This parameter is optional.
  
  The parameter template description contains 0 to 256 characters and does not support special characters !<>'=&".

**NOTE**

The Database Engine and Database Version selected during parameter template creation must be the same as the cluster type and version of the parameter template to be applied.

**Figure 4-1** Creating a parameter template
Modifying a Parameter Template

You can modify the parameter values in a user-defined parameter template but cannot modify the parameter values in the default parameter template.

Step 1  Log in to the management console at https://console.huaweicloud.com/dws/?locale=en-us.

Step 2  In the navigation tree on the left, click Parameter Template Management.

Step 3  In the Name column, click the name of the target parameter template. Its parameter table is displayed.

Step 4  Enter a new value in the Value column of the parameter to be modified. After the modification, click Save.

Step 5  In the Modification Preview dialog box, confirm the settings and modifications and click Save.

Apply a Parameter Template to the Cluster

After a cluster is created, you can apply a new parameter template to the cluster so that the values of all parameters in the parameter template can take effect in the cluster.

To apply a parameter template, perform the following steps:

Step 1  Log in to the management console at https://console.huaweicloud.com/dws/?locale=en-us.

Step 2  In the navigation tree on the left, click Parameter Template Management.

Step 3  Select the target parameter template and click Apply in the Operation column.

Step 4  In the Parameter Template Application dialog box that is displayed, select the target cluster.

You can apply the selected parameter template to the cluster corresponding to the parameter template version.

Figure 4-2 Parameter template application
Step 5 Click OK.

If some parameter values in the newly applied parameter template are different from the original parameter values in the cluster, the system will prompt the differences.

----End

Deleting a Parameter Template

You can delete an unnecessary parameter template or a parameter template that is no longer used. The default parameter template cannot be deleted. Deleted parameter templates cannot be restored. Exercise caution when performing this operation.

Step 1 Log in to the management console at https://console.huaweicloud.com/dws/?locale=en-us.

Step 2 In the navigation tree on the left, click Parameter Template Management.

Step 3 In the Operation column of the parameter template to be deleted, click Delete.

Step 4 In the displayed dialog box, click Yes.

----End
5 Permissions Management

5.1 Basic Concepts

This chapter describes IAM's fine-grained permissions management for your DWS. With IAM, you can:

- Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has their own security credentials, providing access to DWS resources.
- Grant only the permissions required for users to perform a task.
- Entrust a cloud account or service to perform professional and efficient O&M on your DWS resources.

If your cloud account does not need individual IAM users, then you may skip over this chapter.

The following sections describe the common IAM operations, including creating a user and user group, granting permissions to a user group, and creating a custom policy. For other IAM operations, see the IAM User Guide.

Account

To use the Huawei cloud, you need to register an account using your mobile number. The account owns your Huawei cloud resources and has full access permissions for the resources. You can use the account to reset user passwords and assign permissions. Your account receives and pays all bills generated by your IAM users' use of resources. To log in to the Huawei management console using an account, choose Account Login.

If you forget the password of the account, you can reset it by following the procedure in Resetting Password for a HUAWEI CLOUD Account.
IAM User

IAM users are created by an account to use cloud services. Each IAM user has their own password and access key to access the Huawei cloud using the console or APIs. The users manage cloud resources for the account based on assigned permissions. IAM users do not own resources or make payments. It is the account that controls user permissions and pays the bills. To log in to the Huawei cloud management console as an IAM user, choose IAM User Login.

If you forget the password of an IAM user, you can reset it by following the procedure in Resetting Password for an IAM User.
Relationship Between an Account and Its IAM Users

An account and its IAM users are like a parent and children. The account owns the resources and makes payments for IAM users' resource usage. It has full access permissions for these resources. IAM users are created by the account, and only have the permissions granted by the account. The account can modify or cancel the IAM users' permissions at any time. Fees generated by IAM users' use of resources are paid by the account.
Identity Credentials

Identity credentials are used for authentication when you or your IAM users access the Huawei cloud through the console or APIs. Identity credentials include the password and access keys, which can be managed in IAM.

- **Password**: A common identity credential for logging in to the Huawei cloud management console or calling Huawei cloud APIs.
- **Access key**: An access key ID/secret access key (AK/SK) pair, which is used only for calling Huawei cloud APIs. Each access key provides a signature for cryptographic authentication to ensure that access requests are secret, complete, and correct.

User Group

User groups facilitate centralized user management and streamlined permission management. Users in the same user group have the same permissions. IAM users must be added to a user group to obtain the permissions required for accessing specified resources or cloud services in the account. A user can be added to multiple groups, which allows them to inherit different permissions.
The default user group admin has all of the permissions required to use all of the cloud resources. Users in this group can perform operations on all the resources, including but not limited to creating user groups and users, assigning permissions, and managing resources.

**Figure 5-4** Process for creating a user group and user

![Diagram of user group and user creation process]

**Authorization**

Authorization is the process of granting required permissions for a user to perform a task. After a system or custom policy is assigned to a user group, users in the group inherit the permissions defined by the policy to manage resources. For example, managing ECSs.

**Figure 5-5** Authorization model

![Diagram of authorization model]
**Project**

A project corresponds to a Huawei cloud region. Default projects are defined to group and physically isolate resources (including computing, storage, and network resources) across regions. Users can be granted permissions in a default project to access all resources in the region associated with the project. If you need more refined access control, you can create subprojects under a default project and purchase resources in subprojects. Then you can assign required permissions for users to access only the resources in specific subprojects.

*Figure 5-6 Project isolation model*

---

**5.2 Creating a User and Granting Permissions**

This section describes how to use a group to grant permissions to a user. *Figure 5-7* shows the process for granting permissions.

**Process Flow**

*Figure 5-7 Process Flow*
1. Create a user group and grant permissions to it.
   Create a user group on the IAM console, and assign the DWS Viewer policy to the group.

2. Create a 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 DWS console as the created user, and verify that it only has read permissions for DWS.

Prerequisites

- **DWS Viewer** is a fine-grained policy that can be used only if fine-grained access control is enabled in IAM. For more information, see [Applying for Fine-Grained Access Control](#).

- Before assigning permissions to user groups, you should learn about the system policies listed in [System policy summary](#). For the system policies of other services, see [Permission Policy](#).

Step 1: Create a User Group and Grant Permissions

User groups facilitate centralized user management and streamlined permissions management. Users in the same user group have the same permissions. Users created in IAM inherit permissions from the groups to which they belong. To create a user group and grant it permissions, perform the following steps:

**Step 1** Log in to HUAWEI CLOUD using an account.

![Account Login (China)](image)
Step 2  On the management console, click the username on the upper right corner and then choose Identity and Access Management.

![Management Console Screenshot]

Step 3  On the IAM console, choose User Groups in the navigation pane. Then click Create User Group.

![IAM Console Screenshot]

Step 4  Enter a user group name (for example, Developers), and click OK.

The user group is then displayed in the user group list.

Step 5  In the same row as the user group, choose More > Configure Permission. Then click Configure Policy next to the region for which you want to assign permissions to the user group.

DWS is a project-level service. Therefore, you need to assign permissions in the projects in which users in the group need to access DWS resources.

![IAM Console Screenshot]

Step 6  In the Configure Policy dialog box, search for and select DWS Viewer. For details about the system permissions, see System policy summary.
Step 7  Click OK.

----End

Step 2: Create an IAM User

IAM users can be created for employees or applications of an enterprise. Each IAM user has their own security credentials, and inherits permissions from the groups it is a member of. To create an IAM user, perform the following steps:

Step 1  In the navigation pane of the IAM console, choose Users. Then click Create User.

Step 2  Set user information and click Next.

- **Username**: Used for logging in to HUAWEI CLOUD. For this example, enter James.
- **Credential Type**: Identity credential for authentication. For this example, select Password.
  - **Password**: Used for accessing HUAWEI CLOUD using the console or development tools (including APIs, CLI, and SDKs).
  - **Access Key**: Used for logging in to HUAWEI CLOUD using development tools. This credential type is more secure, and is recommended if the user does not need to use the console.
- **(Optional) User Groups**: Select Developers. The user will inherit the permissions granted to the user group. The default user group is admin, which has the administrator permissions and all of the permissions required to use all cloud resources.
- **(Optional) Description**: Description of the user.

Step 3  On the next page, set a password type, an email address, and a mobile number, and then click OK.

The following password types are available:

- **Set at first login**: Select this option if you are not the entity using user James. James will receive a one-time login URL by email and can set a password at first login.
- **Automatically generated**: Select this option if James accesses HUAWEI CLOUD using a development tool. HUAWEI CLOUD will generate a random 10-digit password.
- **Set manually**: Select this option if you are the entity using user James. Then set a password for login.

----End
Step 3: Log In and Verify Permissions

After the user is created, use the username and identity credential to log in to HUAWEI CLOUD, and verify that the user has the permissions defined by the DWS Viewer policy. For more login methods, see Signing In to HUAWEI CLOUD.

Step 1  On the HUAWEI CLOUD login page, click IAM User Login.

Step 2  Enter the account name, username, and password, and click Log In.

- The account name is the name of the HUAWEI CLOUD account that created the IAM user.
- The username and password are those set by the account when creating the IAM user.

If the login fails, contact the entity owning the account to verify the username and password. Alternatively, you can reset the password by following the procedure in Resetting Password for an IAM User.

Step 3  After successful login, click the region selector in the upper right corner to switch to a region where the user has been granted permissions on the management console. The default region is CN North-Beijing1.

Step 4  Choose Service List > Data Warehouse Service. Then click Create DWS Cluster on the DWS console. If a message appears indicating insufficient permissions to perform the operation, the DWS Viewer policy has already taken effect.
5.3 Creating a Custom Policy

Custom policies can be created as a supplement to the system policies of DWS. For the actions supported for custom policies, see Permissions Policies and Supported Actions. The following is the procedure of creating a custom policy for editing jobs.

Prerequisites

- Fine-grained access control must be enabled in IAM. For more information, see Applying for Fine-Grained Access Control.
- You must be familiar with the JSON policy structure. For more information, see Syntax of Fine-Grained Policies.
- You have a plan for which operations to allow or deny, and have obtained the corresponding actions. For details about the supported actions, see DWS Permissions in Fine-Grained Policies.

Creating Custom Policies

This procedure creates a policy named create cluster that only defines the permissions required for creating data warehouse clusters.

Step 1 On the IAM console, choose Policies in the navigation pane. Then click Create Custom Policy.

Step 2 On the Create Custom Policy page, set the following parameters:
**Policy Name**: Enter `create cluster`.

**Scope**: Select `Project-level service`.

**Policy Information**: Copy the following content to the text box and click **Check Grammar**. The policy defines the permissions for creating a data warehouse cluster.

```json
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "dws:cluster:create",
            "ecs:*:get",
            "ecs:*:list",
            "vpc:*:get",
            "vpc:*:list"
         ]
      }]
}
```

- **Policy Name**: Enter `create cluster`.
- **Scope**: Select `Project-level service`.
- **Policy Information**: Copy the following content to the text box and click **Check Grammar**. The policy defines the permissions for creating a data warehouse cluster.

```json
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "dws:cluster:create",
            "ecs:*:get",
            "ecs:*:list",
            "vpc:*:get",
            "vpc:*:list"
         ]
      }]
}
```
Step 3  Click OK.

Step 4  Assign the policy to a user group so that users in the group can inherit the permissions of the policy.

Step 5  Log in to the DWS console as a user in the group, and check whether the user can create clusters.

After authorization, users in the group can verify their permissions using the console or REST APIs. The following are the steps to be performed on the console.

1. Log in to HUAWEI CLOUD as an IAM user.
   - The account name is the name of the HUAWEI CLOUD account that created the IAM user.
   - The username and password are those set by the account when creating the IAM user.
2. On the DWS console, create a cluster. If the creation is successful, the permissions are correct and have already taken effect.
3. Perform other operations, for example, deleting a cluster.
   If a message appears indicating insufficient permissions to perform the operation, the permissions are correct and have already taken effect.

---End

Example Policies

- Example 1: Allowing users to create/restore, restart, and delete a cluster, set security parameters, and reset passwords.

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "dws:cluster:create",
        "dws:cluster:restart",
        "dws:cluster:delete",
        "dws:cluster:setParameter",
        "dws:cluster:resetPassword",
        "ecs:*:get*",
        "ecs:*:list*",
        "vpc:*:get*",
        "vpc:*:list*"
      ]
    }
  ]
}
```

- Example 2: Denying cluster deletion

A deny policy must be used in conjunction with other policies to take effect. If the permissions assigned to a user contain both Allow and Deny actions, the Deny actions take precedence over the Allow actions.
The following method can be used if you need to assign permissions of the **DWS Admin** policy to a user but also forbid the user from deleting clusters. Create a custom policy for denying cluster deletion, and assign both policies to the group the user belongs to. Then the user can perform all operations on DWS except deleting clusters. The following is an example deny policy:

```json
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "dws:cluster:delete"
      ]
    }
  ]
}
```

**DWS Permissions in Fine-Grained Policies**

When creating a custom policy on IAM, you can add the operations on DWS resources or the permissions corresponding to RESTful APIs to the action list of the policy authorization statement so that the policy contains the operation permissions. The following table lists the DWS permissions.

- **RESTful APIs**
  For details about DWS RESTful API permissions, see [Permissions Policies and Supported Actions](#).

- **Management console operations**
  Table 5-1 describes the DWS operations on resources and corresponding permissions.

Table 5-1 DWS permissions

<table>
<thead>
<tr>
<th>Operation</th>
<th>Permission</th>
<th>Dependent Permission</th>
<th>Scope</th>
</tr>
</thead>
</table>
| Creating/Restoring clusters | "dws:cluster:create" | "dws:*:get*", "dws:*:list*", "ecs:*:get*", "ecs:*:list*", "ecs:*:create*", "vpc:*:get*", "vpc:*:list*", "vpc:*:create*", "evs:*:get*", "evs:*:list*", "evs:*:create*", | Includes:  
                          - Project  
                          - Enterprise project |

---

For details about DWS RESTful API permissions, see the [Permissions Policies and Supported Actions](#).

Table 5-1 describes the DWS operations on resources and corresponding permissions.
<table>
<thead>
<tr>
<th>Operation</th>
<th>Permission</th>
<th>Dependent Permission</th>
<th>Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtaining the cluster list</td>
<td>&quot;dws:cluster:list&quot;</td>
<td>&quot;dws:<em>:get</em>&quot;,</td>
<td>● Includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;dws:<em>:list</em>&quot;</td>
<td>- Project</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Enterprise project</td>
</tr>
<tr>
<td>Obtaining the details of a cluster</td>
<td>&quot;dws:cluster:getDetail&quot;</td>
<td>&quot;dws:<em>:get</em>&quot;,</td>
<td>● Includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;dws:<em>:list</em>&quot;</td>
<td>- Project</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Enterprise project</td>
</tr>
<tr>
<td>Setting automated snapshot policy</td>
<td>&quot;dws:cluster:setAutomated Snapshot&quot;</td>
<td>&quot;dws:<em>:get</em>&quot;,</td>
<td>● Includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;dws:<em>:list</em>&quot;</td>
<td>- Project</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Enterprise project</td>
</tr>
<tr>
<td>Setting security parameters/parameter</td>
<td>&quot;dws:cluster:setParameter&quot;</td>
<td>&quot;dws:<em>:get</em>&quot;,</td>
<td>● Includes:</td>
</tr>
<tr>
<td>groups</td>
<td></td>
<td>&quot;dws:<em>:list</em>&quot;</td>
<td>- Project</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Enterprise project</td>
</tr>
<tr>
<td>Restarting clusters</td>
<td>&quot;dws:cluster:restart&quot;</td>
<td>&quot;dws:<em>:get</em>&quot;,</td>
<td>● Includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;dws:<em>:list</em>&quot;</td>
<td>- Project</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Enterprise project</td>
</tr>
<tr>
<td>Scaling out clusters</td>
<td>&quot;dws:cluster:scaleOut&quot;</td>
<td>&quot;dws:<em>:get</em>&quot;,</td>
<td>● Includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;dws:<em>:list</em>&quot;,</td>
<td>- Project</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;ecs:<em>:get</em>&quot;,</td>
<td>- Enterprise project</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;ecs:<em>:list</em>&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;ecs:<em>:create</em>&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;vpc:<em>:get</em>&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;vpc:<em>:list</em>&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;vpc:<em>:create</em>&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;evs:<em>:get</em>&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;evs:<em>:list</em>&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;evs:<em>:create</em>&quot;,</td>
<td></td>
</tr>
<tr>
<td>Operation</td>
<td>Permission</td>
<td>Dependent Permission</td>
<td>Scope</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------</td>
<td>----------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Resizing a cluster</td>
<td>dws:openAPICluster:resize</td>
<td>&quot;dws:<em>:get</em>&quot;,</td>
<td>● Includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;dws:<em>:list</em>&quot;,</td>
<td>- Project</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;ecs:<em>:get</em>&quot;,</td>
<td>- Enterprise project</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;ecs:<em>:list</em>&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;ecs:<em>:create</em>&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;vpc:<em>:get</em>&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;vpc:<em>:list</em>&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;vpc:<em>:create</em>&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;evs:<em>:get</em>&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;evs:<em>:list</em>&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;evs:<em>:create</em>&quot;,</td>
<td></td>
</tr>
<tr>
<td>Resetting passwords</td>
<td>&quot;dws:cluster:resetPassword&quot;</td>
<td>&quot;dws:<em>:get</em>&quot;,</td>
<td>● Includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;dws:<em>:list</em>&quot;,</td>
<td>- Project</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;ecs:<em>:get</em>&quot;,</td>
<td>- Enterprise project</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;ecs:<em>:list</em>&quot;,</td>
<td></td>
</tr>
<tr>
<td>Applying parameter templates to</td>
<td>&quot;dws:cluster:changeParameterGroup&quot;</td>
<td>&quot;dws:<em>:get</em>&quot;,</td>
<td>● Includes:</td>
</tr>
<tr>
<td>clusters</td>
<td></td>
<td>&quot;dws:<em>:list</em>&quot;,</td>
<td>- Project</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;ecs:<em>:get</em>&quot;,</td>
<td>- Enterprise project</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;ecs:<em>:list</em>&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;ecs:<em>:delete</em>&quot;,</td>
<td></td>
</tr>
<tr>
<td>Deleting clusters</td>
<td>&quot;dws:cluster:delete&quot;</td>
<td>&quot;dws:<em>:get</em>&quot;,</td>
<td>● Includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;dws:<em>:list</em>&quot;,</td>
<td>- Project</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;ecs:<em>:get</em>&quot;,</td>
<td>- Enterprise project</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;ecs:<em>:list</em>&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;ecs:<em>:delete</em>&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;vpc:<em>:get</em>&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;vpc:<em>:list</em>&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;vpc:<em>:delete</em>&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;evs:<em>:get</em>&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;evs:<em>:list</em>&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;evs:<em>:delete</em>&quot;,</td>
<td></td>
</tr>
<tr>
<td>Configuring maintenance windows</td>
<td>&quot;dws:cluster:setMaintainceWindow&quot;</td>
<td>&quot;dws:<em>:get</em>&quot;,</td>
<td>● Includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;dws:<em>:list</em>&quot;,</td>
<td>- Project</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;ecs:<em>:get</em>&quot;,</td>
<td>- Enterprise project</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;ecs:<em>:list</em>&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;ecs:<em>:delete</em>&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;vpc:<em>:get</em>&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;vpc:<em>:list</em>&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;vpc:<em>:delete</em>&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;evs:<em>:get</em>&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;evs:<em>:list</em>&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;evs:<em>:delete</em>&quot;,</td>
<td></td>
</tr>
<tr>
<td>Operation</td>
<td>Permission</td>
<td>Dependent Permission</td>
<td>Scope</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------</td>
<td>----------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>Binding EIPs</td>
<td>&quot;dws:eip:operate&quot;</td>
<td>&quot;dws::<em>:get</em>'&quot;, &quot;dws::<em>:list</em>'&quot;,</td>
<td>● Includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Project</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Enterprise project</td>
</tr>
<tr>
<td>Unbinding EIPs</td>
<td>&quot;dws:eip:operate&quot;</td>
<td>&quot;dws::<em>:get</em>'&quot;, &quot;dws::<em>:list</em>'&quot;,</td>
<td>● Includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Project</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Enterprise project</td>
</tr>
<tr>
<td>Creating DNS domain names</td>
<td>&quot;dws:dns:create&quot;</td>
<td>&quot;dws::<em>:get</em>'&quot;, &quot;dws::<em>:list</em>'&quot;,</td>
<td>● Includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Project</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Enterprise project</td>
</tr>
<tr>
<td>Releasing DNS domain names</td>
<td>&quot;dws:dns:release&quot;</td>
<td>&quot;dws::<em>:get</em>'&quot;, &quot;dws::<em>:list</em>'&quot;,</td>
<td>● Includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Project</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Enterprise project</td>
</tr>
<tr>
<td>Modifying DNS domain names</td>
<td>&quot;dws:dns:edit&quot;</td>
<td>&quot;dws::<em>:get</em>'&quot;, &quot;dws::<em>:list</em>'&quot;,</td>
<td>● Includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Project</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Enterprise project</td>
</tr>
<tr>
<td>Creating MRS connections</td>
<td>&quot;dws:MRSConnection:create&quot;</td>
<td>&quot;dws::<em>:get</em>'&quot;, &quot;dws::<em>:list</em>'&quot;,</td>
<td>● Includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Project</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Enterprise project</td>
</tr>
<tr>
<td>Updating MRS connections</td>
<td>&quot;dws:MRSConnection:update&quot;</td>
<td>&quot;dws::<em>:get</em>'&quot;, &quot;dws::<em>:list</em>'&quot;,</td>
<td>● Includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Project</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Enterprise project</td>
</tr>
<tr>
<td>Operation</td>
<td>Permission</td>
<td>Dependent Permission</td>
<td>Scope</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------</td>
<td>----------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Deleting MRS connections</td>
<td>&quot;dws:MRSCreation:del   te&quot;</td>
<td>&quot;dws:<em>:get</em>&quot;, &quot;dws:<em>:list</em>&quot;,</td>
<td>• Includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Project</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Enterprise project</td>
</tr>
<tr>
<td>Adding/Deleting tags</td>
<td>&quot;dws:tag:addAndDelete&quot;</td>
<td>&quot;dws:<em>:get</em>&quot;, &quot;dws:<em>:list</em>&quot;,</td>
<td>• Includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Project</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Enterprise project</td>
</tr>
<tr>
<td>Editing tags</td>
<td>&quot;dws:tag:edit&quot;</td>
<td>&quot;dws:<em>:get</em>&quot;, &quot;dws:<em>:list</em>&quot;,</td>
<td>• Includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Project</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Enterprise project</td>
</tr>
<tr>
<td>Creating snapshots</td>
<td>&quot;dws:snapshot:create&quot;</td>
<td>&quot;dws:<em>:get</em>&quot;, &quot;dws:<em>:list</em>&quot;,</td>
<td>• Includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Project</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Enterprise project</td>
</tr>
<tr>
<td>Obtaining the snapshot list</td>
<td>&quot;dws:snapshot:list&quot;</td>
<td>&quot;dws:<em>:get</em>&quot;</td>
<td>• Includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Project</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Enterprise project</td>
</tr>
<tr>
<td>Deleting snapshots</td>
<td>&quot;dws:snapshot:delete&quot;</td>
<td>&quot;dws:snapshot:list&quot;</td>
<td>• Includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Project</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Enterprise project</td>
</tr>
<tr>
<td>Copying snapshots</td>
<td>&quot;dws:snapshot:copy&quot;</td>
<td>&quot;dws:snapshot:list&quot;</td>
<td>• Includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Project</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Enterprise project</td>
</tr>
</tbody>
</table>
### 5.4 Syntax of Fine-Grained Policies

#### Policy Structure

A fine-grained policy consists of a Version and a Statement. Each policy can have multiple statements.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Permission</th>
<th>Dependent Permission</th>
<th>Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating parameter templates</td>
<td>&quot;dws:parameterGroup:create&quot;</td>
<td>&quot;dws:<em>:get</em>&quot;, &quot;dws:<em>:list</em>&quot;</td>
<td>● Includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Project</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Enterprise project</td>
</tr>
<tr>
<td>Deleting parameter templates</td>
<td>&quot;dws:parameterGroup:delete&quot;</td>
<td>&quot;dws:<em>:get</em>&quot;, &quot;dws:<em>:list</em>&quot;</td>
<td>● Includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Project</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Enterprise project</td>
</tr>
<tr>
<td>Changing parameter templates</td>
<td>&quot;dws:parameterGroup:edit&quot;</td>
<td>&quot;dws:<em>:get</em>&quot;, &quot;dws:<em>:list</em>&quot;</td>
<td>● Includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Project</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Enterprise project</td>
</tr>
</tbody>
</table>
Policy Syntax

The **DWS Viewer** policy is used as an example to describe the syntax of fine-grained policies.
**Version**: Distinguishes between role-based access control (RBAC) and fine-grained policies.

- **1.0**: RBAC policies. An RBAC policy consists of permissions for an entire service. Users in a group with such a policy assigned are granted all of the permissions required for that service.

- **1.1**: Fine-grained policies. A fine-grained policy consists of API-based permissions for operations on specific resource types. Fine-grained policies, as the name
suggests, allow for more fine-grained control than RBAC policies. Users granted permissions of such a policy can only perform specific operations on the corresponding service. Fine-grained policies include system and custom policies.

- **Statement**: Permissions defined by a policy, including Effect and Action.
  - **Effect**
    The valid values for Effect are Allow and Deny. System policies contain only Allow statements. For custom policies containing both Allow and Deny statements, the Deny statements take precedence.
  - **Action**
    Permissions in the format of `Service name:Resource type:Operation`. A policy can contain one or more permissions. The wildcard (*) is allowed to indicate all of the services, resource types, or operations depending on its location in the action.
    Example: `dws:cluster:create`, permissions for create data warehouse clusters.

**Multi-Action Policy**

A custom policy can contain actions of multiple services that are all of the global or project-level type. The following is a policy with multiple statements:

```json
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecs:cloudServers:resize",
        "ecs:cloudServers:delete",
        "ecs:cloudServers:rebuild"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "dws:*:get*",
        "dws:*:list*",
        "dws:cluster:create"
      ]
    }
  ]
}
```

**Deny Policy**

A deny policy must be used in conjunction with other policies to take effect. If the permissions assigned to a user contain both Allow and Deny actions, the Deny actions take precedence over the Allow actions.

The following method can be used if you need to assign permissions of the **DWS Admin** policy to a user but also forbid the user from deleting clusters. Create a custom policy for denying cluster deletion, and assign both policies to the group the user belongs to. Then the user can perform all operations on DWS except deleting clusters. The following is an example deny policy:

```json
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
    
```
Authentication Logic

If a user is granted permissions of multiple policies or of only one policy containing both Allow and Deny statements, then authentication starts from the Deny statements. The following figure shows the authentication logic for resource access.

Figure 5-9 Authentication logic

![Authentication Logic Diagram]

**NOTE**

The actions in each policy bear the OR relationship.

1. A user accesses the system and makes an operation request.
2. The system evaluates all the permissions policies assigned to the user.
3. In these policies, the system looks for explicit deny permissions. If the system finds an explicit deny that applies, it returns a decision of Deny, and the authentication ends.
4. If no explicit deny is found, the system looks for allow permissions that would apply to the request. If the system finds an explicit allow permission that applies, it returns a decision of Allow, and the authentication ends.

5. If no explicit allow permission is found, IAM returns a decision of Deny, and the authentication ends.

5.5 RBAC Syntax of RBAC Policies

Policy Structure

An RBAC policy consists of a Version, a Statement, and Depends.

**Figure 5-10** Policy structure

Policy Syntax

The DWS Administrator policy is used as an example to describe the syntax of RBAC policies.
Parameter | Meaning | Value
---|---|---
Version | Policy version | The value is fixed to 1.0.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Meaning</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statement</td>
<td>Action</td>
<td>Operations to be performed on DWS</td>
</tr>
</tbody>
</table>
|           |         | Format: *Service name:Resource type:Operation.*  
|           |         | **DWS:DWS:** Permissions for performing all operations on all resource types in DWS. |
| Effect    |         | Whether the operation defined in an action is allowed  
|           |         | • Allow  
|           |         | • Deny |
| Depends   | catalog | Name of the service to which dependencies of a policy belong |
|           |         | Service name  
|           |         | Example: **BASE** |
|           | display_name | Name of a dependent policy |
|           |         | Policy name  
|           |         | Example: **Server Administrator** |
6 Managing MRS Data Sources

6.1 Importing Data from MRS to DWS

Importing Data from MRS to a Data Warehouse Cluster

MRS is a big data cluster running based on the open source Hadoop ecosystem. It provides the industry's latest cutting-edge storage and analysis capabilities of massive volumes of data, satisfying even the most demanding of your data storage and processing requirements. For details, see the MapReduce Service User Guide.

You can use Hive/Spark (analysis cluster of MRS) to store massive volumes of service data. Hive/Spark data files are stored in HDFS. On DWS, you can connect a data warehouse cluster to MRS clusters, read data from HDFS files, and write the data to DWS when the clusters are on the same network.

Import Process

Perform the following operations to import data from MRS to a data warehouse cluster:

1. In the data warehouse cluster, create an MRS data source connection according to section Creating an MRS Data Source Connection.

NOTE

A connection is also called a foreign server in databases. One data warehouse cluster can connect to multiple MRS clusters, but only one connection can be established between a data warehouse cluster and an MRS cluster.

2. Create an HDFS foreign table for querying data from the MRS cluster over interfaces of a foreign server.

For details, see Importing Data from MRS to a Data Warehouse Cluster in the Data Warehouse Service Database Developer Guide.
6.2 Creating an MRS Data Source Connection

Scenario

Before DWS reads data from MRS HDFS, you need to create an MRS data source connection that functions as a channel of transporting data warehouse cluster data and MRS cluster data.

Impact on the System

- You can create only one MRS data source connection in the data warehouse cluster at a time.
- When an MRS data source connection is being created, the system automatically adds inbound and outbound rules to security groups of the data warehouse cluster and MRS cluster. Nodes in the same subnet can be accessed.
- For the MRS cluster with Kerberos authentication enabled, the system automatically adds a Machine-Machine user that belongs to user group supergroup to the MRS cluster.

Prerequisites

You have created a data warehouse cluster and recorded the AZ, VPC, and subnet where the cluster resides.

Procedure

**Step 1** Log in to the public cloud management console.

**Step 2** Choose Service List > EI Enterprise Intelligence > MapReduce Service to enter the MRS management console and create an MRS cluster.

Configure parameters as required. For details, see Creating a Cluster in the MapReduce Service User Guide.

- The AZ, VPC, and subnet of the MRS cluster must be the same as those of the data warehouse cluster.
- **Cluster Type** must be Analysis Cluster.
- MRS cluster versions are 1.2, 1.3.0, 1.5.0, 1.5.1, 1.6.*, 1.7.*, 1.8.*, and 2.0.*. The asterisk (*) indicates a number.
- In the Components area, select Hive and Spark.

**NOTE**

If you enable Kerberos authentication for an MRS cluster, use MRS Manager to create a user for interconnecting DWS with the system after the MRS cluster is created. The user type must be Human-Machine and the user, user group hadoop, and role Manager_administrator must be bound together. The user password must be changed on the MRS Manager page after the user is created.

If you already have a qualified MRS cluster, skip this step.

**Step 3** Choose Service List > EI Enterprise Intelligence > Data Warehouse Service to enter the DWS management console.
Step 4  On the DWS management console, click **Cluster Management**.

Step 5  In the cluster list, click the name of a cluster. On the page that is displayed, click the **MRS Data Sources** tab.

**Figure 6-1** MRS data sources

Step 6  Click **Create MRS Cluster Connection** and configure parameters.

**Table 6-1** MRS cluster connection parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MRS Data Source</strong></td>
<td>Specifies the MRS cluster to which DWS can connect. By default, all available analytic MRS clusters that are in the same VPC and subnet as the current data warehouse cluster and in the <strong>Available</strong> state are displayed. After you select an MRS cluster, the system automatically displays whether Kerberos authentication is enabled for the selected cluster. This parameter is mandatory.</td>
</tr>
<tr>
<td><strong>MRS Account</strong></td>
<td>Specifies the account used when a data warehouse cluster connects to an MRS cluster. This parameter is available only when Kerberos authentication is selected for the MRS cluster. This parameter is mandatory.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Specifies the password of the connection user. If you change the password, you need to create a new connection. This parameter is available only for clusters with Kerberos authentication enabled. This parameter is mandatory.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Describes the connection. This parameter is optional.</td>
</tr>
</tbody>
</table>

**NOTE**

- If the **MRS Data Source** drop-down list is empty, click **Create MRS Cluster** to create an MRS cluster.
- After selecting an MRS cluster from the **MRS Data Source** drop-down list, click **View MRS Cluster** to view information about the MRS cluster.

Step 7  Click **OK** to save the connection.
Configuration Status turns to Creating. You can view the connection that is successfully created in the MRS data source list and the connection status is Available.

**NOTE**

- In the Operation column, you can click Update Configurations to update MRS Cluster Status and Configuration Status. During configuration update, you cannot create a new connection. The system checks whether the security group rule is correct. If the rule is incorrect, the system rectifies the fault. For details, see Updating the MRS Data Source Configuration.
- In the Operation column, you can click Delete to delete the unnecessary connection. When deleting a connection, you need to manually delete the security group rule.

---

## 6.3 Updating the MRS Data Source Configuration

### Scenario

For MRS, if the following parameter configurations of the HDFS cluster change, data may fail to be imported to the data warehouse cluster from the HDFS cluster. Before importing data using the HDFS cluster, you must update the MRS data source configuration.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dfs.client.read.shortcircuit</td>
<td>Specifies whether to enable the local read function.</td>
</tr>
<tr>
<td>dfs.client.read.shortcircuit.skip.checksum</td>
<td>Specifies whether to skip data verification during the local read.</td>
</tr>
<tr>
<td>dfs.client.block.write.replace-datanode-on-failure.enable</td>
<td>Specifies whether to replace the location storing copies with the new node when data blocks fail to be written to HDFS.</td>
</tr>
<tr>
<td>dfs.encrypt.data.transfer</td>
<td>Specifies whether to enable data encryption. <strong>NOTE</strong> This parameter is available only for clusters with Kerberos authentication enabled.</td>
</tr>
<tr>
<td>dfs.encrypt.data.transfer.algorithm</td>
<td>Specifies the encryption and decryption algorithm for key transmission.</td>
</tr>
<tr>
<td>dfs.encrypt.data.transfer.cipher.suites</td>
<td>Specifies the encryption and decryption algorithm for the transmission of actually stored data.</td>
</tr>
<tr>
<td>dfs.replication</td>
<td>Specifies the default number of data copies.</td>
</tr>
<tr>
<td>dfs.blocksiz</td>
<td>Specifies the default size of a data block.</td>
</tr>
<tr>
<td>hadoop.security.authentication</td>
<td>Specifies the security authentication mode.</td>
</tr>
<tr>
<td>hadoop.rpc.protection</td>
<td>Specifies the RPC communication protection mode.</td>
</tr>
<tr>
<td>dfs.domain.socket.path</td>
<td>Specifies the locally used Domain socket path.</td>
</tr>
</tbody>
</table>
Prerequisites

You have created an MRS data source connection for the data warehouse cluster.

Impact on the System

When you are updating an MRS data source connection, the data warehouse cluster will automatically restart and cannot provide services.

Procedure

Step 1  On the DWS management console, click Cluster Management.

Step 2  In the cluster list, click the name of a cluster. On the page that is displayed, click MRS Data Sources.

Step 3  In the MRS data source list, select the MRS that you want to update. In the Operation column, click Update Configurations.

MRS Cluster Status and Configuration Status of the current connection will be updated. During configuration update, you cannot create a new connection. The system checks whether the security group rule is correct. If the rule is incorrect, the system rectifies the fault.

----End
Function

This section describes how to check cluster metrics on Cloud Eye. By monitoring cluster running metrics, you can identify the time when the database cluster is abnormal and analyze potential activity problems based on the database logs, improving database performance. This section describes the metrics that can be monitored by Cloud Eye as well as their namespaces and dimensions. You can use the management console or APIs provided by Cloud Eye to query the metrics of the monitored objects and alarms generated for DWS.

Namespace

SYS.DWS

Monitoring Metrics of a Cluster

With the DWS monitoring metrics provided by Cloud Eye, you can obtain information about the cluster running status and performance. This information will provide a better understanding of the node-level information.

Table 7-1 describes DWS monitoring metrics.

<table>
<thead>
<tr>
<th>Metric ID</th>
<th>Name</th>
<th>Description</th>
<th>Value Range</th>
<th>Measurement Object &amp; Dimension</th>
<th>Monitoring Period (Raw Data)</th>
</tr>
</thead>
<tbody>
<tr>
<td>shared_buffer_hit_ratio</td>
<td>Shared Memory Hit Ratio</td>
<td>Percentage of data volume obtained from memory, expressed in percentage</td>
<td>0% to 100%</td>
<td>Monitored object: data warehouse cluster Dimension: dws_instance_id</td>
<td>1 minute</td>
</tr>
<tr>
<td>Metric ID</td>
<td>Name</td>
<td>Description</td>
<td>Value Range</td>
<td>Measurement Object &amp; Dimension</td>
<td>Monitoring Period (Raw Data)</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------</td>
<td>--------------------------------------------------</td>
<td>-------------</td>
<td>--------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>in_memory_sort_ratio</td>
<td>In-memory Sort Ratio</td>
<td>Percentage of data volume that is sorted in memory, expressed in percentage</td>
<td>0% to 100%</td>
<td>Monitored object: data warehouse cluster Dimension: dws_instance_id</td>
<td>1 minute</td>
</tr>
<tr>
<td>physical_reads</td>
<td>File Reads</td>
<td>Total number of database file reads</td>
<td>&gt; 0</td>
<td>Monitored object: data warehouse cluster Dimension: dws_instance_id</td>
<td>1 minute</td>
</tr>
<tr>
<td>physical_writes</td>
<td>File Writes</td>
<td>Total number of database file writes</td>
<td>&gt; 0</td>
<td>Monitored object: data warehouse cluster Dimension: dws_instance_id</td>
<td>1 minute</td>
</tr>
<tr>
<td>physical_writes_per_second</td>
<td>File Reads per Second</td>
<td>Number of database file reads per second</td>
<td>≥ 0</td>
<td>Monitored object: data warehouse cluster Dimension: dws_instance_id</td>
<td>1 minute</td>
</tr>
<tr>
<td>physical_reads_per_second</td>
<td>File Writes per Second</td>
<td>Number of database file writes per second</td>
<td>≥ 0</td>
<td>Monitored object: data warehouse cluster Dimension: dws_instance_id</td>
<td>1 minute</td>
</tr>
<tr>
<td>Metric ID</td>
<td>Name</td>
<td>Description</td>
<td>Value Range</td>
<td>Measurement Object &amp; Dimension</td>
<td>Monitoring Period (Raw Data)</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------</td>
<td>----------------------------------------------------------</td>
<td>---------------</td>
<td>-------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>db_size</td>
<td>Data Volume</td>
<td>Total data volume of the database Unit: MB</td>
<td>0 to 36,000 MB</td>
<td>Monitored object: data warehouse cluster Dimension: dws_instance_i d</td>
<td>1 minute</td>
</tr>
<tr>
<td>active_sql_count</td>
<td>Active SQL Count</td>
<td>Number of active SQLs in the database</td>
<td>≥ 0</td>
<td>Monitored object: data warehouse cluster Dimension: dws_instance_i d</td>
<td>1 minute</td>
</tr>
<tr>
<td>session_count</td>
<td>Session Count</td>
<td>Number of sessions that access the database</td>
<td>≥ 0</td>
<td>Monitored object: data warehouse cluster Dimension: dws_instance_i d</td>
<td>1 minute</td>
</tr>
<tr>
<td>cpu_usage</td>
<td>CPU Usage</td>
<td>CPU usages of each node in the cluster, expressed in percentage</td>
<td>0% to 100%</td>
<td>Monitored object: data warehouse cluster Dimension: datastore_id</td>
<td>4 minutes</td>
</tr>
<tr>
<td>mem_usage</td>
<td>Memory Usage</td>
<td>Memory usages of each node in the cluster, expressed in percentage</td>
<td>0% to 100%</td>
<td>Monitored object: data warehouse cluster Dimension: datastore_id</td>
<td>4 minutes</td>
</tr>
<tr>
<td>iops</td>
<td>IOPS</td>
<td>Number of I/O requests processed by each node in the cluster per second</td>
<td>≥ 0</td>
<td>Monitored object: data warehouse cluster Dimension: datastore_id</td>
<td>4 minutes</td>
</tr>
<tr>
<td>Metric ID</td>
<td>Name</td>
<td>Description</td>
<td>Value Range</td>
<td>Measurement Object &amp; Dimension</td>
<td>Monitoring Period (Raw Data)</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------</td>
<td>---------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>bytes_in</td>
<td>Network Input Throughput</td>
<td>Data input to each node in the cluster per second over the network Unit: byte/s</td>
<td>≥ 0 bytes/s</td>
<td>Monitored object: data warehouse Dimension: datastore_id</td>
<td>4 minutes</td>
</tr>
<tr>
<td>bytes_out</td>
<td>Network Output Throughput</td>
<td>Data sent to the network per second from each node in the cluster Unit: byte/s</td>
<td>≥ 0 bytes/s</td>
<td>Monitored object: data warehouse Dimension: datastore_id</td>
<td>4 minutes</td>
</tr>
<tr>
<td>disk_usage</td>
<td>Disk Usage</td>
<td>Disk usages of each node in the cluster, expressed in percentage</td>
<td>0% to 100%</td>
<td>Monitored object: data warehouse Dimension: datastore_id</td>
<td>4 minutes</td>
</tr>
<tr>
<td>disk_total_size</td>
<td>Total Disk Size</td>
<td>Total disk space of each node in the cluster Unit: GB</td>
<td>100 to 2,000 GB</td>
<td>Monitored object: data warehouse Dimension: datastore_id</td>
<td>4 minutes</td>
</tr>
<tr>
<td>disk_used_size</td>
<td>Used Disk Space</td>
<td>Used disk space of each node in the cluster Unit: GB</td>
<td>0 to 3,600 GB</td>
<td>Monitored object: data warehouse Dimension: datastore_id</td>
<td>4 minutes</td>
</tr>
<tr>
<td>disk_read_throughput</td>
<td>Disk Read Throughput</td>
<td>Data volume read from each disk in the cluster per second Unit: byte/s</td>
<td>≥ 0 bytes/s</td>
<td>Monitored object: data warehouse Dimension: datastore_id</td>
<td>4 minutes</td>
</tr>
<tr>
<td>disk_write_throughput</td>
<td>Disk Write Throughput</td>
<td>Data volume written to each disk in the cluster per second Unit: byte/s</td>
<td>≥ 0 bytes/s</td>
<td>Monitored object: data warehouse Dimension: datastore_id</td>
<td>4 minutes</td>
</tr>
</tbody>
</table>
### Metric ID | Name | Description | Value | Measurement Object & Dimension | Monitoring Period (Raw Data)
--- | --- | --- | --- | --- | ---
`avg_disk_seconds_per_read` | Average Time per Disk Read | Average time used each time when a disk reads data | > 0s | Monitored object: data warehouse Dimension: datastore_id | 4 minutes
`avg_disk_seconds_per_write` | Average Time per Disk Write | Average time used each time when data is written to a disk | > 0s | Monitored object: data warehouse Dimension: datastore_id | 4 minutes
`avg_disk_queue_length` | Average Disk Queue Length | Average I/O queue length of a disk | ≥ 0 | Monitored object: data warehouse Dimension: datastore_id | 4 minutes

### Dimension

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>dws_instance_id</td>
<td>Data warehouse cluster</td>
</tr>
<tr>
<td>datastore_id</td>
<td>Data warehouse node</td>
</tr>
</tbody>
</table>

### Viewing Monitoring Information of a Cluster

**Step 1** Log in to the [DWS management console](#) and click **Cluster Management**.

**Step 2** In the cluster list, click **View Metric** in the **Operation** column where a specific cluster resides. The Cloud Eye management console is displayed.

On Cloud Eye, you can view monitoring metrics of data warehouse clusters and monitoring information about each node in the cluster. Additionally, you can specify a specific monitoring metric and the time range to view the performance curve.

Cloud Eye also supports the ability to compare the monitoring metrics of multiple nodes. For details, see [Comparing the Monitoring Metrics of Multiple Nodes](#).

----End
Comparing the Monitoring Metrics of Multiple Nodes

**Step 1** In the navigation tree on the left of the Cloud Eye management console, choose **Dashboard > Monitoring Panels**.

**Step 2** On the **Monitoring Panels** page, click **Create Panel**. In the displayed dialog box, enter the **Name** and click **OK**.

**Step 3** On the **Monitoring Panels** page, click **Add Graph** in the upper right corner.

**Step 4** In the **Add Graph** window, configure the title and monitoring metrics.

**NOTE**

You can add multiple monitoring metrics by clicking **Add Metric**.

![Add Graph Window](image)

The following describes how to set parameters if you want to compare CPU usage of two nodes.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Type</td>
<td>DWS</td>
</tr>
<tr>
<td>Dimension</td>
<td>Data Warehouse Node</td>
</tr>
<tr>
<td>Monitored Object</td>
<td>dws-64a3-dws-cn-cn-1-1, dws-64a3-dws-cn-cn-1-1</td>
</tr>
<tr>
<td>Metric</td>
<td>CPU Usage</td>
</tr>
</tbody>
</table>

**Step 5** Click **OK**.

After the monitoring metrics are added successfully, you can view the corresponding monitoring graph on the **Monitoring Panels** page. Move the cursor to the graph and click in the upper right corner to zoom in the graph and view detailed metric comparison data.

---End
Creating Alarm Rules

Setting DWS alarm rules allows you to customize the monitored objects and notification policies and determine the running status of your DWS at any time.

A DWS alarm rule includes the alarm rule name, monitored object, metric, threshold, monitoring interval, and whether to send a notification. This section describes how to set DWS alarm rules.

Step 1  Log in to the management console at https://console.huaweicloud.com/dws/?locale=en-us.

Step 2  In the navigation tree on the left, click Cluster Management.

Step 3  Locate the row containing the target cluster, click View Metric in the Operation column to enter the Cloud Eye management console and view the DWS monitoring information.

The status of the target cluster must be Available. Otherwise, you cannot create alarm rules.

Step 4  In the left navigation pane of the Cloud Eye management console, choose Alarm Management > Alarm Rules.

Step 5  On the Alarm Rules page, click Create Alarm Rule in the upper right corner.

Step 6  On the Create Alarm Rule page, set parameters as prompted.

1. Configure the rule name and description.
2. Configure the alarm parameters as prompted.

Figure 7-2 Configuring alarm content
### Table 7-3 Configuring alarm content

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Type</td>
<td>Name of the cloud service resource for which the alarm rule is configured.</td>
<td>Data Warehouse Service</td>
</tr>
<tr>
<td>Dimension</td>
<td>Metric dimension of the alarm rule. You can select Data Warehouse Nodes or Data Warehouses.</td>
<td>Data Warehouse Node</td>
</tr>
<tr>
<td>Monitoring Scope</td>
<td>Resource scope to which an alarm rule applies. Select Specific resources and select one or more monitoring objects. Select the ID of the cluster instance or node you have created. Click to synchronize the monitoring objects to the right pane.</td>
<td>Specific resources</td>
</tr>
<tr>
<td>Method</td>
<td>Select Use template or Create manually as required.</td>
<td>Create manually</td>
</tr>
<tr>
<td></td>
<td>- If no alarm template is available, set Method to Create manually and configure related parameters to create an alarm rule.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- If you have available alarm rule templates, set Method to Use template, so that you can use a template to quickly create alarm rules.</td>
<td></td>
</tr>
<tr>
<td>Template</td>
<td>This parameter is valid only when Use template is selected. Select the template to be imported. If no alarm template is available, click Create Custom Template to create one that meets your requirements.</td>
<td>-</td>
</tr>
<tr>
<td>Alarm Policy</td>
<td>This parameter is valid only when Create manually is selected. Set the policy that triggers an alarm. For example, trigger an alarm if the CPU usage equals to or is greater than 80% for 3 consecutive periods. Table 7-1 lists the monitoring metrics supported by DWS.</td>
<td>-</td>
</tr>
<tr>
<td>Alarm Severity</td>
<td>Severity of an alarm. Valid values are Critical, Major, Minor, and Informational.</td>
<td>Major</td>
</tr>
</tbody>
</table>

3. Configure the alarm notification parameters as prompted.
### Figure 7-3 Configuring alarm notification

![Figure 7-3 Configuring alarm notification]

### Table 7-4 Configuring alarm notification

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm Notification</td>
<td>Whether to notify users when alarms are triggered. Notifications can be sent as emails or text messages, or HTTP/HTTPS requests sent to the servers. You can enable (recommended) or disable <strong>Alarm Notification</strong>.</td>
<td>Enable</td>
</tr>
<tr>
<td>Validity Period</td>
<td>Cloud Eye sends notifications only within the validity period specified in the alarm rule. If <strong>Validity Period</strong> is set to <strong>00:00-8:00</strong>, Cloud Eye sends notifications only within <strong>00:00-8:00</strong>.</td>
<td>-</td>
</tr>
<tr>
<td>Topic</td>
<td>Name of the topic to which the alarm notification is sent. If you enable <strong>Alarm Notification</strong>, you need to select a topic. If no desired topics are available, create one first, whereupon the SMN service is invoked. For details about how to create a topic, see the <em>Simple Message Notification User Guide</em>.</td>
<td>-</td>
</tr>
<tr>
<td>Trigger Condition</td>
<td>Condition for triggering the alarm. You can select <strong>Generated alarm</strong>, <strong>Cleared alarm</strong>, or both.</td>
<td>-</td>
</tr>
</tbody>
</table>

4. After the configuration is complete, click **Next**.

After the alarm rule is created, if the metric data reaches the specified threshold, Cloud Eye will immediately inform you that an exception has occurred.

----End
Configuring OBS Transfer

On Cloud Eye, the raw data retention period for each metric is two days. Raw data with a retention period of more than two days will not be saved. You can enable OBS and save the raw data to OBS so that it can be saved for a longer time.

For details about how to configure OBS transfer, see Configuring Data Storage in the Cloud Eye User Guide.
8 Notifying Events

8.1 Event Notification Overview

Overview

DWS uses the Simple Message Notification (SMN) service to send notifications of DWS events. The SMN function is only available by subscription. In a subscription, you need to specify one or more event filtering conditions. When an event that matches all filtering conditions occurs, DWS sends a notification based on the subscription. The filter conditions include the Event Type (for example, Management, Monitoring, or Security), Event Severity (for example, Normal or Warning), and Event Source Category (for example, Cluster or Snapshot).

Supported Event Types and Events

Events are records of changes in the user's cluster status. Events can be triggered by user operations (such as audit events), or may be caused by cluster service status changes (for example, cluster repaired successfully or failed to repair the cluster.) The following tables list the events and event types supported by DWS.

- The following table shows the events whose Event Source Category is Cluster.

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Event Name</th>
<th>Event Severity</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>createClusterFail</td>
<td>Warning</td>
<td>Failed to create cluster.</td>
</tr>
<tr>
<td>Management</td>
<td>createClusterSuccess</td>
<td>Normal</td>
<td>Cluster created successfully.</td>
</tr>
<tr>
<td>Management</td>
<td>createCluster</td>
<td>Normal</td>
<td>Cluster creation started.</td>
</tr>
<tr>
<td>Management</td>
<td>extendCluster</td>
<td>Normal</td>
<td>Cluster scale-out started.</td>
</tr>
<tr>
<td>Event Type</td>
<td>Event Name</td>
<td>Event Severity</td>
<td>Event</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------</td>
<td>----------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Management</td>
<td>extendClusterSuccess</td>
<td>Normal</td>
<td>Cluster scaled out successfully.</td>
</tr>
<tr>
<td>Management</td>
<td>extendClusterFail</td>
<td>Warning</td>
<td>Failed to scale out the cluster.</td>
</tr>
<tr>
<td>Management</td>
<td>deleteClusterFail</td>
<td>Warning</td>
<td>Failed to delete the cluster.</td>
</tr>
<tr>
<td>Management</td>
<td>deleteClusterSuccess</td>
<td>Normal</td>
<td>Cluster deleted successfully.</td>
</tr>
<tr>
<td>Management</td>
<td>deleteCluster</td>
<td>Normal</td>
<td>Cluster deletion started.</td>
</tr>
<tr>
<td>Management</td>
<td>restoreClusterFail</td>
<td>Warning</td>
<td>Failed to restore the cluster.</td>
</tr>
<tr>
<td>Management</td>
<td>restoreClusterSuccess</td>
<td>Normal</td>
<td>Cluster restored successfully.</td>
</tr>
<tr>
<td>Management</td>
<td>restoreCluster</td>
<td>Normal</td>
<td>Cluster restoration started.</td>
</tr>
<tr>
<td>Management</td>
<td>restartClusterFail</td>
<td>Warning</td>
<td>Failed to restart the cluster.</td>
</tr>
<tr>
<td>Management</td>
<td>restartClusterSuccess</td>
<td>Normal</td>
<td>Cluster restarted successfully.</td>
</tr>
<tr>
<td>Management</td>
<td>restartCluster</td>
<td>Normal</td>
<td>Cluster restarted.</td>
</tr>
<tr>
<td>Management</td>
<td>configureMRSExtData-Sources</td>
<td>Normal</td>
<td>Configuration of MRS external data source for the cluster started.</td>
</tr>
<tr>
<td>Management</td>
<td>configureMRSExtData-SourcesFail</td>
<td>Warning</td>
<td>Failed to configure the MRS external data source for the cluster.</td>
</tr>
<tr>
<td>Management</td>
<td>configureMRSExtData-SourcesSuccess</td>
<td>Normal</td>
<td>MRS external data source configured successfully for the cluster.</td>
</tr>
<tr>
<td>Management</td>
<td>deleteMRSExtData-Sources</td>
<td>Normal</td>
<td>Deletion of MRS external data source for the cluster started.</td>
</tr>
<tr>
<td>Management</td>
<td>deleteMRSExtData-SourcesFail</td>
<td>Warning</td>
<td>Failed to delete the MRS external data source for the cluster.</td>
</tr>
<tr>
<td>Event Type</td>
<td>Event Name</td>
<td>Event Severity</td>
<td>Event</td>
</tr>
<tr>
<td>-------------</td>
<td>----------------------------------</td>
<td>----------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Management</td>
<td>deletedMRSExtData-SourcesSuccess</td>
<td>Normal</td>
<td>MRS external data source deleted successfully for the cluster.</td>
</tr>
<tr>
<td>Management</td>
<td>bindEipToCluster</td>
<td>Normal</td>
<td>Bound an EIP to the cluster.</td>
</tr>
<tr>
<td>Management</td>
<td>bindEipToClusterFail</td>
<td>Warning</td>
<td>Failed to bind an EIP to the cluster.</td>
</tr>
<tr>
<td>Management</td>
<td>unbindEipToCluster</td>
<td>Normal</td>
<td>Unbound an EIP from the cluster.</td>
</tr>
<tr>
<td>Management</td>
<td>unbindEipToClusterFail</td>
<td>Warning</td>
<td>Failed to unbind an EIP from the cluster.</td>
</tr>
<tr>
<td>Management</td>
<td>refreshEipToCluster</td>
<td>Normal</td>
<td>Refreshed the cluster's EIP.</td>
</tr>
<tr>
<td>Management</td>
<td>refreshEipToClusterFail</td>
<td>Warning</td>
<td>Failed to refresh the cluster's EIP.</td>
</tr>
<tr>
<td>Management</td>
<td>changeExpressFlagSuccess</td>
<td>Normal</td>
<td>Acceleration enabled successfully.</td>
</tr>
<tr>
<td>Management</td>
<td>disableExpressSuccess</td>
<td>Normal</td>
<td>Acceleration disabled successfully.</td>
</tr>
<tr>
<td>Security</td>
<td>resetPasswordFail</td>
<td>Warning</td>
<td>Failed to reset the password.</td>
</tr>
<tr>
<td>Security</td>
<td>resetPasswordSuccess</td>
<td>Normal</td>
<td>Password of the cluster reset successfully.</td>
</tr>
<tr>
<td>Security</td>
<td>updateConfiguration</td>
<td>Normal</td>
<td>Updating security parameters of the cluster started.</td>
</tr>
<tr>
<td>Security</td>
<td>updateConfigurationFail</td>
<td>Warning</td>
<td>Failed to update security parameters of the cluster.</td>
</tr>
<tr>
<td>Monitoring</td>
<td>repairCluster</td>
<td>Normal</td>
<td>The node is faulty. Repairing the cluster starts.</td>
</tr>
<tr>
<td>Monitoring</td>
<td>repairClusterFail</td>
<td>Warning</td>
<td>Failed to repair the cluster.</td>
</tr>
</tbody>
</table>
The following table shows the events whose **Event Source Category** is **Snapshot**.

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Event Name</th>
<th>Event Severity</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring</td>
<td>repairClusterSuccess</td>
<td>Normal</td>
<td>Cluster repaired successfully.</td>
</tr>
</tbody>
</table>

### Table 8-2 Events whose **Event Source Category** is **Snapshot**

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Event Name</th>
<th>Event Severity</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>deleteBackup</td>
<td>Normal</td>
<td>Snapshot deleted successfully.</td>
</tr>
<tr>
<td>Management</td>
<td>deleteBackupFail</td>
<td>Warning</td>
<td>Failed to delete the snapshot.</td>
</tr>
<tr>
<td>Management</td>
<td>createBackup</td>
<td>Normal</td>
<td>Snapshot creation started.</td>
</tr>
<tr>
<td>Management</td>
<td>createBackupSuccess</td>
<td>Normal</td>
<td>Snapshot created successfully.</td>
</tr>
<tr>
<td>Management</td>
<td>createBackupFail</td>
<td>Warning</td>
<td>Failed to create the snapshot.</td>
</tr>
</tbody>
</table>

## 8.2 Subscribing to Event Notification

After subscribing to DWS event notification, you will receive notifications by email or phone when management, monitoring, or security events occur in a specific cluster or snapshot.

### Creating a Subscription

**Step 1** Log in to the management console at [https://console.huaweicloud.com/dws/?locale=en-us](https://console.huaweicloud.com/dws/?locale=en-us).

**Step 2** In the navigation tree on the left, click **Event Management**.

**Step 3** On the **Event Management** page, choose **Subscription > Create Subscription**.

**Step 4** In the **Subscription Settings** area, set basic subscription information and event filtering.

The **Subscribed Event List** area displays the events filtered by the system based on the subscription settings.
Figure 8-1 Subscription Settings

![Subscription Settings](image)

Table 8-3 Subscription parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable/Disable Notification</td>
<td>Enable or disable event subscription.</td>
</tr>
<tr>
<td>Subscription Name</td>
<td>Enter the name of a subscription.</td>
</tr>
<tr>
<td>Event Type</td>
<td>Select the type of the event to be subscribed. Possible values are Management, Monitoring, and Security.</td>
</tr>
<tr>
<td>Event Severity</td>
<td>Select the alarm severity of the event. Possible values are Normal and Warning.</td>
</tr>
<tr>
<td>Event Source Category</td>
<td>Select the event source category. Possible values are Cluster and Snapshot.</td>
</tr>
</tbody>
</table>

Step 5  Select a message notification topic from the Message Notification Topic drop-down list.

You can perform the following operations to create a message notification topic as required.

1. Click Create Topic. The Topic page of SMN is displayed. You can click Create Topic in the upper right corner to create a topic. For details, see Topic Management > Creating a Topic in the Simple Message Notification User Guide.
Figure 8-2 Creating a topic

2. In the row containing the created topic, choose More > Configure Topic Policy and select DWS under Services that can publish messages to enable message notification for DWS.

Figure 8-3 Configuring topic policy

Step 6 Click OK to complete the subscription.

----End

Modifying the Subscription

Step 1 On the Event Management page of the DWS management console, click the Subscription tab.

Step 2 In the Operation column of the row containing the specified subscription, click Edit to enter the Edit Subscription page.

Figure 8-4 Clicking Edit
Step 3  On the Edit Subscription page, set the parameters to be modified. For details, see Step 4 and Step 6 in section “Creating a Subscription”.

----End

Deleting the Subscription

Step 1  On the Event Management page of the DWS management console, click the Subscription tab.

Step 2  In the Operation column of the row containing the specified subscription, click Delete. The Delete Subscription dialog box is displayed.

Step 3  Click Yes to delete the subscription.

----End

8.3 Viewing Events

This section describes how to search for events that occur in a cluster or snapshot.

Step 1  Log in to the management console at https://console.huaweicloud.com/dws/?locale=en-us.

Step 2  In the navigation tree on the left, click Event Management to enter the Events tab page.

In the event list, all events occurring in the cluster or snapshot are displayed by default.

By clicking next to field Time in the table header, you can list the events in chronological order or reverse order.

You can click next to fields (excluding Time) in the table header to select corresponding filtering criteria in the pop-up menu to filter events.

Figure 8-5 Event page

----End
9 Audit Logs

9.1 Viewing Audit Logs of Key Operations on the Management Console

DWS uses CTS to record key operation events on the DWS management console. The generated logs can be used in scenarios such as security analysis, compliance audit, resource tracing, and problem locating. This section is organized as follows:

- Enabling the Audit Service
- Disabling the Audit Log Function
- Key Operations
- Viewing Traces

Enabling the Audit Service

A tracker will be automatically created after CTS is enabled. All traces recorded by CTS are associated with a tracker. Currently, only one tracker can be created for each account.

**Step 1** On the DWS management console, choose Service List > Management & Deployment > Cloud Trace Service. The CTS management console is displayed.

**Step 2** In the navigation tree on the left, click Trackers.

**Step 3** Enable CTS.

If you are a first-time CTS user and do not have any created trackers in the tracker list, enable CTS first. For details, see Enabling CTS in the Cloud Trace Service Getting Started.

If you have enabled CTS, the system has automatically created a management tracker. Only one management tracker can be created and it cannot be deleted. You can also manually create a data tracker. For details, see Creating a Tracker in the Cloud Trace Service User Guide.

----End

Disabling the Audit Log Function

If you want to disable the audit log function, disable the tracker in CTS.
Step 1 On the DWS management console, choose Service List > Management & Deployment > Cloud Trace Service. The CTS management console is displayed.

Step 2 In the navigation pane on the left, click Trackers.

Step 3 In the tracker list, locate the tracker to be disabled and click Disable in the corresponding row.

Step 4 In the displayed dialog box, click Yes.

After the tracker is disabled, the Disable button in the Operation column is switched to Enable. To enable the tracker again, click Enable and then click Yes. The system will start recording operations again.

After the tracker is disabled, the system will stop recording operations, but you can still view existing operation records.

---End

Key Operations

With CTS, you can record operations associated with DWS for later query, audit, and backtrack operations.

Table 9-1 DWS operations that can be recorded by CTS

<table>
<thead>
<tr>
<th>Operation</th>
<th>Resource</th>
<th>Event Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating/Restoring a cluster</td>
<td>cluster</td>
<td>createCluster</td>
</tr>
<tr>
<td>Deleting a cluster</td>
<td>cluster</td>
<td>deleteCluster</td>
</tr>
<tr>
<td>Scaling out a cluster</td>
<td>cluster</td>
<td>growCluster</td>
</tr>
<tr>
<td>Restarting a cluster</td>
<td>cluster</td>
<td>rebootCluster</td>
</tr>
<tr>
<td>Creating a snapshot</td>
<td>backup</td>
<td>createBackup</td>
</tr>
<tr>
<td>Deleting a snapshot</td>
<td>backup</td>
<td>deleteBackup</td>
</tr>
<tr>
<td>Setting security parameters</td>
<td>configurations</td>
<td>updateConfigurations</td>
</tr>
<tr>
<td>Creating an MRS data source</td>
<td>dataSource</td>
<td>createExtDataSource</td>
</tr>
<tr>
<td>Deleting an MRS data source</td>
<td>dataSource</td>
<td>deleteExtDataSource</td>
</tr>
<tr>
<td>Updating an MRS data source</td>
<td>dataSource</td>
<td>updateExtDataSource</td>
</tr>
</tbody>
</table>

Viewing Traces

Step 1 On the DWS management console, choose Service List > Management & Deployment > Cloud Trace Service. The CTS management console is displayed.
Step 2  In the navigation pane on the left, choose Trace List.

Step 3  In the upper right corner of the trace list, click Filter to set the search criteria.

The following filters are available:

- **Trace Source, Resource Type, and Search By**
  - **Trace Source**: Select DWS.
  - **Resource Type**: Select All resource types or specify a resource type.
  - **Search By**: Select All filters or any of the following options:
    - **Trace name**: If you select this option, you also need to select a specific trace name.
    - **Resource ID**: If you select this option, you also need to select or enter a specific resource ID.
    - **Resource name**: If you select this option, you also need to select or enter a specific resource name.

- **Operator**: Select a specific operator (at user level rather than tenant level).

- **Trace Status**: Available options include All trace statuses, normal, warning, and incident. You can only select one of them.

- **Start Date** and **End Date**: You can specify the time period to query traces.

![Querying traces](image)

Step 4  Click Query.

Step 5  Click on the left of the trace to be queried to extend its details.

![Traces](image)

Step 6  Locate the row containing the target trace and click View Trace in the Operation column.
9.2 Configuring the Database Audit Log

Scenario

DWS allows you to record the audit log of specific operations, involving audit log retention policy, unauthorized access and DML, SELECT COPY, and DDL operations performed on the stored procedures and database objects.

After configuring the audit log, you can query the audit information to locate the fault cause or the historical operation record as needed when a data warehouse cluster is abnormal.

For details about how to view the audit log information, see Viewing the Auditing Information in the Data Warehouse Service Database Developer Guide.

Prerequisites

Database audit logs are configured on the Security Settings page. You can change security settings only when Cluster Status is Available and Low performance and Task Information cannot be Creating snapshot, Scaling out, Configuring, or Restarting.

Procedure

Step 1  Log in to the DWS management console.

Step 2  Click Cluster Management.

Step 3  In the cluster list, click the name of a cluster. On the page that is displayed, click Security Settings.
By default, **Configuration Status** is **Synchronized**, which indicates that the latest database result is displayed.

**Step 4** In the **Audit Settings** area, set the audit log retention policy.

**Figure 9-4 Audit log retention policy**

![Audit log retention policy](image)

**Table 9-2** describes the detailed information.

**Table 9-2 Audit log retention policy**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Log Retention Policy</td>
<td>Specifies the audit log retention policy. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Space priority</strong>: Audit logs will be automatically deleted if the size of audit logs on a single node exceeds 1 GB.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Time priority</strong>: Audit logs will be retained within the minimum retention period. After this period expires, audit logs will be</td>
</tr>
<tr>
<td></td>
<td>automatically deleted if the size of audit logs on a single node exceeds 1 GB.</td>
</tr>
<tr>
<td></td>
<td><strong>Space priority</strong> is preferred.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong></td>
</tr>
<tr>
<td></td>
<td>Clusters 1.0.0 and 1.1.0 do not support the audit log retention policy.</td>
</tr>
<tr>
<td>Minimum Retention Period</td>
<td>This parameter is valid when <strong>Audit Log Retention Policy</strong> is set to <strong>Time priority</strong>. The value ranges from 0 to 730 days. The default</td>
</tr>
<tr>
<td>(Day)</td>
<td>value is 90 days.</td>
</tr>
</tbody>
</table>

**Step 5** Enable the audit function for the following operations if necessary.

![Audit function enabled](image) indicates that the audit function is enabled. ![Audit function disabled](image) indicates that the audit function is disabled.
Table 9-3 describes the detailed information about the audit items.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Unauthorized Access</td>
<td>Specifies whether to record unauthorized operations. This parameter is disabled by default.</td>
</tr>
<tr>
<td>Audit DML Execution</td>
<td>Specifies whether to record INSERT, UPDATE, and DELETE operations on tables. This parameter is disabled by default.</td>
</tr>
<tr>
<td>Audit SELECT Execution</td>
<td>Specifies whether to record the SELECT operation. This parameter is disabled by default.</td>
</tr>
<tr>
<td>Audit Stored Procedure Execution</td>
<td>Specifies whether to record operations when executing the stored procedure or user-defined functions. This parameter is disabled by default.</td>
</tr>
<tr>
<td>Audit COPY Execution</td>
<td>Specifies whether to record the COPY operation. This parameter is disabled by default.</td>
</tr>
<tr>
<td>Audit DDL Objects</td>
<td>Specifies whether to record the CREATE, DROP, and ALTER operations of specified database objects. Database, Schema, and User are selected by default. Other objects are not selected by default.</td>
</tr>
</tbody>
</table>

Except audit items listed in Table 9-3, key audit items in Table 9-4 are enabled by default in DWS.

Table 9-4 Key audit items

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key audit items</td>
<td>Records successful and failed login and deregistration information.</td>
</tr>
</tbody>
</table>
### 9.3 Dumping the Database Audit Log

DWS records information (audit logs) about connections and user activities in your database. With the information, you can monitor the database to ensure security and facilitate fault troubleshooting and historical operation record locating. These audit logs are stored in the database by default. You can also dump them to OBS so that users who are responsible for monitoring the database can view the logs more conveniently.

You can perform the following operations on the DWS console:
- **Enabling Audit Log Dump**
- **Modifying Audit Log Dump Configurations**
- **Viewing Audit Log Dump Records**
- **Disabling Audit Log Dump**

#### Enabling Audit Log Dump

After a data warehouse cluster is created, you can enable audit log dump for it to dump audit logs to OBS.

Before enabling audit log dump, ensure that the following conditions are met:
- You have created an OBS bucket for storing the audit logs. For details, see [Creating a Bucket](#) in the *Object Storage Service Console Operation Guide*.

The procedure is as follows:

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

**Step 2** In the navigation tree on the left, click **Cluster Management**.

**Step 3** In the cluster list, click the name of the cluster for which you want to enable audit log dump. On the page that is displayed, click **Security Settings**.

---

### Parameter Table

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Records database startup, stop, recovery, and failover audit information.</td>
</tr>
<tr>
<td></td>
<td>Records a user's lock and unlock information.</td>
</tr>
<tr>
<td></td>
<td>Records the grants and reclaims of a user's permission.</td>
</tr>
<tr>
<td></td>
<td>Records the audit function of the SET operation.</td>
</tr>
</tbody>
</table>

---

**Step 6** Click **Apply**.

Click ▶️. If **Configuration Status** is **Applying**, the system is saving the settings.

Wait for a moment and then refresh **Configuration Status**. When **Configuration Status** is **Synchronized**, the configuration is saved and takes effect.

----End
Step 4  In the **Audit Settings** area, enable **Audit Log Dump**.

[Image]

---

<table>
<thead>
<tr>
<th>Audit Log Dump</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OBS Bucket</strong></td>
</tr>
<tr>
<td><strong>OBS Path</strong></td>
</tr>
<tr>
<td><strong>Dump Interval (Minute)</strong></td>
</tr>
</tbody>
</table>

- **OBS Bucket**: Name of the OBS bucket used to store the audit data. If no OBS bucket is available, click **View OBS Bucket** to access the OBS console and create one. For details, see **Creating a Bucket** in the *Object Storage Service Console Operation Guide*.
- **OBS Path**: User-defined directory on OBS for storing audit files. Different directory levels are separated by forward slashes (/). The value is a string containing 1 to 50 characters, which cannot start with a forward slash (/). If the entered OBS path does not exist, the system creates one and dumps data to it.
- **Dump Interval (Minute)**: Interval based on which DWS periodically dumps data to OBS. The value ranges from 5 to 43200. The unit is minute.

Step 5  Click **Apply**.

If **Configuration Status** is **Applying**, the system is saving the settings.

Wait for a moment and then refresh **Configuration Status**. When **Configuration Status** is **Synchronized**, the configuration is saved and takes effect.

---End---

**Modifying Audit Log Dump Configurations**

After audit log dump is enabled, you can modify the dump configurations, for example, modifying the OBS bucket, path, and dump interval.

The procedure is as follows:

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

**Step 2**  In the navigation tree on the left, click **Cluster Management**.

**Step 3**  In the cluster list, click the name of the cluster for which you want to modify the audit log dump configurations. On the page that is displayed, click **Security Settings**.

**Step 4**  In the **Audit Settings** area, modify the **Audit Log Dump** configurations.

**Step 5**  Click **Apply**.

If **Configuration Status** is **Applying**, the system is saving the settings.
Wait for a moment and then refresh **Configuration Status**. When **Configuration Status** is **Synchronized**, the configuration is saved and takes effect.

---End

**Viewing Audit Log Dump Records**

After audit log dump is enabled, you can view the dumped audit logs on OBS.

The procedure is as follows:

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

**Step 2** In the navigation tree on the left, click **Cluster Management**.

**Step 3** In the cluster list, click the name of the target cluster. On the page that is displayed, click **Security Settings**.

**Step 4** In the **Audit Settings** area, click **View Dump Record**.

**Step 5** In the **Audit Log Dump Records** dialog box, click **View OBS Bucket**. The OBS console page is displayed.

**Step 6** Select the OBS bucket and folder where the logs are stored to view the log files.

You can download and decompress the files to view. The fields of audit log files are described as follows:

**Table 9-5 Log file fields**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>time</td>
<td>Indicates the operation time.</td>
</tr>
<tr>
<td>type</td>
<td>Indicates the operation type.</td>
</tr>
<tr>
<td>result</td>
<td>Indicates the operation result.</td>
</tr>
<tr>
<td>username</td>
<td>Indicates the name of the user who initiates the operation.</td>
</tr>
<tr>
<td>database</td>
<td>Indicates the database name.</td>
</tr>
<tr>
<td>client_conninfo</td>
<td>Indicates the client connection information.</td>
</tr>
<tr>
<td>object_name</td>
<td>Indicates the operation object name.</td>
</tr>
<tr>
<td>detail_info</td>
<td>Indicates the detailed information about the operation.</td>
</tr>
<tr>
<td>node_name</td>
<td>Indicates the node name.</td>
</tr>
<tr>
<td>thread_id</td>
<td>Indicates the thread ID.</td>
</tr>
<tr>
<td>local_port</td>
<td>Indicates the local port.</td>
</tr>
<tr>
<td>remote_port</td>
<td>Indicates the remote port.</td>
</tr>
</tbody>
</table>

---End
Disabling Audit Log Dump

You can disable audit log dump if you do not want to dump audit logs to OBS any more.

The procedure is as follows:

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

**Step 2** In the navigation tree on the left, click Cluster Management.

**Step 3** In the cluster list, click the name of the cluster for which you want to disable audit log dump. On the page that is displayed, click Security Settings.

**Step 4** In the Audit Settings area, disable audit log dump.

- [ ] indicates that the function is enabled. [ ] indicates that the function is disabled.

**Step 5** Click Apply.

If Configuration Status is Applying, the system is saving the settings.

Wait for a moment and then refresh Configuration Status. When Configuration Status is Synchronized, the configuration is saved and takes effect.

----End
If errors occur when DWS operation requests submitted on the management console are being processed, error information is displayed on the management console. The error information includes the returned error code and description.

Error Code Description

If an error occurs, find the error code and perform the corresponding operations listed in Table 10-1.

Table 10-1 Error codes

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Error Information</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>DWS.6000</td>
<td>Failed to create the cluster. Contact the customer service or try again later.</td>
<td>Check the remaining resource quota of the account. If the remaining resource quota is greater than the requested resources, contact the customer service or technical support engineers.</td>
</tr>
<tr>
<td>DWS.6001</td>
<td>Failed to scale out the cluster. Contact the customer service or try again later.</td>
<td>Check the remaining node quota of the account. If the remaining node quota is greater than the number of requested nodes, contact the customer service or technical support engineers.</td>
</tr>
<tr>
<td>DWS.6002</td>
<td>Failed to restart the cluster. Contact the customer service or try again later.</td>
<td>Contact the customer service or try again later.</td>
</tr>
<tr>
<td>DWS.6003</td>
<td>Failed to restore the cluster. Contact the customer service or try again later.</td>
<td>Check the remaining quota of the account. If the remaining quota is greater than the requested quota, contact the customer service or technical support engineers.</td>
</tr>
<tr>
<td>Error Code</td>
<td>Error Information</td>
<td>Recommended Action</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DWS.6004</td>
<td>Failed to create a DWS node. This is caused by an ECS exception and the error code is ${\text{FailureReason}}$. Contact the customer service or try again later.</td>
<td>For details about the ECS error codes and recommended actions, see <a href="#">How Do I Handle Error Messages Displayed on the Management Console?</a> in the Elastic Cloud Server FAQs. You can also select another region, AZ, or node flavor to create a cluster.</td>
</tr>
<tr>
<td>DWS.6005</td>
<td>Failed to bind an EIP to a data warehouse cluster. This is caused by a VPC exception and the error code is ${\text{FailureReason}}$. Contact the customer service or try again later.</td>
<td>For details about the VPC error codes, see <a href="#">Error Codes</a> in the Virtual Private Cloud API Reference.</td>
</tr>
<tr>
<td>DWS.6006</td>
<td>Failed to bind the EIP. The error code is ${\text{FailureReason}}$.</td>
<td>For details about the VPC error codes, see <a href="#">Error Codes</a> in the Virtual Private Cloud API Reference.</td>
</tr>
<tr>
<td>DWS.6007</td>
<td>The EIP has been bound to other VMs. The error code is ${\text{FailureReason}}$.</td>
<td>Select another unbound EIP.</td>
</tr>
<tr>
<td>DWS.6008</td>
<td>Failed to create the private network domain name. The error code is ${\text{FailureReason}}$.</td>
<td>For details about the DNS error codes, see <a href="#">Public Parameters &gt; Error Code</a> in the Domain Name Service API Reference.</td>
</tr>
</tbody>
</table>
### A Change History

<table>
<thead>
<tr>
<th>Release Date</th>
<th>What's New</th>
</tr>
</thead>
</table>
| 2019-10-30   | This issue is the twenty-second official release. The following topic is modified:  
  * Monitoring a Cluster |
| 2019-08-08   | This is the twenty-first official release. The following topic is added:  
  * Modifying Parameters  
  The following topics are modified:  
  * Creating a Cluster  
  * Buying Yearly/Monthly Packages  
  * Resizing a Cluster: Before resizing a cluster, DWS automatically creates a snapshot for it.  
  * Overview  
  * Setting the Automated Snapshot Policy: Increased the frequency of automated snapshots.  
  * Managing Parameter Templates: Added the `update_lockwait_timeout` parameter.  
  * Using the Data Studio GUI Client to Connect to a Cluster: For Data Studio 18.2.0 SPC1 and later versions, the client SSL key can only be in the PK8 format. |
| 2019-06-17   | This issue is the twentieth official release. The following topic is added:  
  * Overview  
  The following topics are modified:  
  * Creating a Cluster  
  * Dumping the Database Audit Log  
  The following topic is deleted: Creating a DWS Agency on the IAM Console |
<table>
<thead>
<tr>
<th>Release Date</th>
<th>What's New</th>
</tr>
</thead>
</table>
| 2019-05-24   | This issue is the nineteenth official release.  
The following topic is added:  
  - Permissions Management  
The following topics are modified:  
  - Creating a Cluster  
  - Managing Enterprise Projects  
  - Database Encryption Overview |
| 2019-04-17   | This issue is the eighteenth official release.  
The following topics are added:  
  - Dumping the Database Audit Log  
  - Creating a DWS Agency on the IAM Console  
The following topics are modified:  
  - Creating a Cluster  
  - Resizing a Cluster  
  - Managing Parameter Templates |
| 2019-02-28   | This issue is the seventeenth official release.  
The following topics are modified:  
  - Creating a Cluster  
  - Querying Cluster Status Information  
  - Managing Parameter Templates |
| 2019-02-01   | This issue is the sixteenth official release.  
The following topics are added:  
  - Managing Enterprise Projects  
  - Database Encryption Overview  
  - Rotating Encryption Keys  
The following topics are modified:  
  - Creating a Cluster  
  - Querying Cluster Status Information  
  Deleted the following content from this document. To learn the related information, see Data Import in the Data Warehouse Service Database Developer Guide.  
  - Importing and Exporting Data |
| 2018-11-24   | This issue is the fifteenth official release.  
The following topics are modified:  
  - Buying Yearly/Monthly Packages  
  - Downloading the JDBC or ODBC Driver |
<table>
<thead>
<tr>
<th>Release Date</th>
<th>What's New</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018-11-08</td>
<td>This issue is the fourteenth official release. &lt;br&gt;The following topic is added: &lt;br&gt;• <strong>Buying Yearly/Monthly Packages</strong> &lt;br&gt;• <strong>Methods of Connecting to a Cluster</strong> &lt;br&gt;The following topics are modified: &lt;br&gt;• <strong>Creating a Cluster</strong> &lt;br&gt;• <strong>Manually Creating a Snapshot</strong> &lt;br&gt;• (Optional) <strong>Configuring SSL Connection</strong> &lt;br&gt;• (Optional) <strong>Downloading SSL Certificate</strong></td>
</tr>
<tr>
<td>2018-09-30</td>
<td>This is the thirteenth official release. &lt;br&gt;The following topics are added: &lt;br&gt;• <strong>Establishing Secure TCP/IP Connections in SSL Mode</strong> &lt;br&gt;• <strong>Overview</strong> &lt;br&gt;• <strong>Granting an IAM Account the DWS Database Access Permission</strong> &lt;br&gt;• <strong>Creating an IAM User Credential</strong> &lt;br&gt;• <strong>Configuring the JDBC Connection to Connect to a Cluster Using IAM Authentication</strong> &lt;br&gt;The following topic is modified: &lt;br&gt;• <strong>Using the gsql Client to Connect to a Cluster</strong></td>
</tr>
<tr>
<td>2018-08-30</td>
<td>This issue is the twelfth official release. &lt;br&gt;The following topic is modified: &lt;br&gt;• <strong>Creating a Cluster</strong>: Added regions.</td>
</tr>
<tr>
<td>2018-07-30</td>
<td>This issue is the eleventh official release. &lt;br&gt;The following topics are added: &lt;br&gt;• <strong>Upgrading a Cluster</strong> &lt;br&gt;• <strong>Managing Parameter Templates</strong> &lt;br&gt;• <strong>Preparing an ECS as the gsql Client Host</strong> &lt;br&gt;The following topics are modified: &lt;br&gt;• <strong>Creating a Cluster</strong>: Added the parameter group. &lt;br&gt;• <strong>Restoring a Snapshot</strong>: Added the parameter group.</td>
</tr>
<tr>
<td>Release Date</td>
<td>What's New</td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
</tr>
<tr>
<td>2018-07-10</td>
<td>This issue is the tenth official release. The following topics are added:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Using the Third-Party Function Library psycopg2 of Python to Connect to a Cluster</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Viewing Audit Logs of Key Operations on the Management Console</strong></td>
</tr>
<tr>
<td></td>
<td>The following topics are modified:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Querying Cluster Status Information</strong>: Modified the description of the cluster's access addresses.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Obtaining the Cluster Connection Address</strong>: Modified the description of the cluster's access addresses.</td>
</tr>
<tr>
<td>2018-05-15</td>
<td>This issue is the ninth official release. The following topics are added:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Tag Management</strong>: Added the functions of adding tags to a cluster and searching for a cluster by tag.</td>
</tr>
<tr>
<td></td>
<td>• <strong>7.3.5-Using the gsql Client to Connect to a Cluster (SSL)</strong>: Added the procedure for connecting the gsql to the cluster in SSL mode.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Using the Data Studio GUI Client to Connect to a Cluster</strong>: Added the function of connecting to a cluster through the Data Studio GUI client.</td>
</tr>
<tr>
<td></td>
<td>• Added the functions of adding extended applications and using extended applications to connect to a cluster.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Managing Extended Applications</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Using Extended Application pgAdmin4 to Connect to the Cluster</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Restrictions on Using pgAdmin4</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Development Specifications</strong>: Added the development specifications for connecting to a cluster using code.</td>
</tr>
<tr>
<td></td>
<td>• Added the function of notifying users of events.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Event Notification Overview</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Subscribing to Event Notification</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Viewing Events</strong></td>
</tr>
<tr>
<td></td>
<td>The following topics are modified:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Creating a Cluster</strong>: Added the function of adding tags and specifying the EIP bandwidth during cluster creation.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Using the gsql Client to Connect to a Cluster</strong>: Added the procedure for connecting to a cluster in non-SSL mode.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Using a JDBC Driver to Connect to the Database</strong>: Added the function of delivering the JAR file of the JDBC driver to users in Maven mode.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Monitoring a Cluster</strong>: Added the description of creating alarm rules.</td>
</tr>
<tr>
<td>Release Date</td>
<td>What's New</td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
</tr>
<tr>
<td>2018-3-31</td>
<td>This is the eighth official release. The following topics are modified:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Creating a Cluster</strong>: Added the quota verification description.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Resizing a Cluster</strong>: Added the quota verification description.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Restoring a Snapshot</strong>: Added the quota verification description.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Using a JDBC Driver to Connect to the Database</strong>: Added the sample code that illustrates how to develop applications based on the JDBC interface provided by DWS.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Monitoring a Cluster</strong>: Added the description of creating alarms and configuring OBS transfer.</td>
</tr>
<tr>
<td></td>
<td>The following topics are added:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Setting the Automated Snapshot Policy</strong>: Added automatic snapshot policy setting.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Using pgAdmin to Connect to a Cluster</strong>: Added the description of using pgAdmin to connect to the database.</td>
</tr>
<tr>
<td>2018-03-02</td>
<td>This issue is the seventh official release. The following topics are modified:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Creating a Cluster</strong>: Modified the node flavor.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Querying Cluster Status Information</strong>: Added the procedure of view <strong>Connection Address</strong>, including the domain name of the existing cluster on the <strong>Cluster Details</strong> page.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Configuring the Database Audit Log</strong>: Added the method of viewing the audit log.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Obtaining the Cluster Connection Address</strong>: Added the procedure of viewing the cluster connection address on the <strong>Cluster Details</strong> page.</td>
</tr>
<tr>
<td></td>
<td>The following topic is added:</td>
</tr>
<tr>
<td></td>
<td><strong>Setting the Automated Snapshot Policy</strong>: Added the description of copying a snapshot.</td>
</tr>
<tr>
<td>Release Date</td>
<td>What's New</td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
</tr>
</tbody>
</table>
| 2018-02-12   | This is the sixth official release.  
The following topics are modified:  
- **Resizing a Cluster**: Optimized the description of prerequisites.  
- **Restarting a Cluster**: Optimized the impact of cluster restart on the system.  
- **Creating a Cluster**: Added the procedure of creating a default security group for a cluster.  
- **Configuring the Database Audit Log**: Added the procedure of auditing the log retention policy.  
- **Downloading Clients**: Added the third-party open-source PostgreSQL client.  
Deleted the following content from this document. If you want to know more about the following content, see the *Data Warehouse Service Database Developer Guide*:  
- Managing Database Users  
- Managing Database Audit  
- Importing Data from OBS to a Data Warehouse Cluster  
- Exporting Data from a Data Warehouse Cluster to OBS  
- SQL on OBS  
- Clearing and Reclaiming the Storage Space |
| 2017-12-27   | This is the fifth official release.  
The following topics are modified:  
- **Creating a Cluster**  
- **Separating Rights of Roles**  
- Introduction to SQL |
<table>
<thead>
<tr>
<th>Release Date</th>
<th>What's New</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-11-24</td>
<td>This is the fourth official release.</td>
</tr>
<tr>
<td></td>
<td>• The following topics are added:</td>
</tr>
<tr>
<td></td>
<td>- Managing Clusters That Fail to Be Created</td>
</tr>
<tr>
<td></td>
<td>- Resetting Passwords</td>
</tr>
<tr>
<td></td>
<td>- Using a JDBC Driver to Connect to the Database</td>
</tr>
<tr>
<td></td>
<td>- Introduction to SQL</td>
</tr>
<tr>
<td></td>
<td>- Updating the MRS Data Source Configuration</td>
</tr>
<tr>
<td></td>
<td>- Error Code Reference</td>
</tr>
<tr>
<td></td>
<td>• The following topics are modified:</td>
</tr>
<tr>
<td></td>
<td>- Managing Clusters</td>
</tr>
<tr>
<td></td>
<td>- Manually Creating a Snapshot</td>
</tr>
<tr>
<td></td>
<td>- Restoring a Snapshot</td>
</tr>
<tr>
<td></td>
<td>- Using the gsql Client to Connect to a Cluster</td>
</tr>
<tr>
<td></td>
<td>- Importing Data from OBS to a Data Warehouse Cluster</td>
</tr>
<tr>
<td></td>
<td>- Importing Data</td>
</tr>
<tr>
<td></td>
<td>- Exporting Data from a Data Warehouse Cluster to OBS</td>
</tr>
<tr>
<td></td>
<td>- Exporting Data</td>
</tr>
<tr>
<td>2017-08-25</td>
<td>This is the third official release.</td>
</tr>
<tr>
<td></td>
<td>• The following topics are added:</td>
</tr>
<tr>
<td></td>
<td>- Resizing a Cluster</td>
</tr>
<tr>
<td></td>
<td>- Separating Rights of Roles</td>
</tr>
<tr>
<td></td>
<td>- (Optional) Configuring SSL Connection</td>
</tr>
<tr>
<td></td>
<td>- Managing Database Audit</td>
</tr>
<tr>
<td></td>
<td>- Importing Data from MRS to DWS</td>
</tr>
<tr>
<td></td>
<td>- Creating an MRS Data Source Connection</td>
</tr>
<tr>
<td></td>
<td>- Updating the MRS Data Source Configuration</td>
</tr>
<tr>
<td></td>
<td>• The following topics are modified:</td>
</tr>
<tr>
<td></td>
<td>- Creating a Cluster</td>
</tr>
<tr>
<td>2017-06-09</td>
<td>This is the second official release.</td>
</tr>
<tr>
<td></td>
<td>The following topics are modified:</td>
</tr>
<tr>
<td></td>
<td>Supported the ability to create nodes with ultra-high I/Os in Creating a</td>
</tr>
<tr>
<td></td>
<td>Cluster.</td>
</tr>
<tr>
<td>2017-05-04</td>
<td>This is the first official release.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>