

ApsaraDB for MongoDB

User Guide

User Guide

Document overview

ApsaraDB for MongoDB is fully compatible with the MongoDB protocol and can provide stable, reliable, and automatically scalable database service. It offers a full range of database solutions, such as disaster recovery, backup, recovery, monitoring, and alarms.

This document describes how to use ApsaraDB for MongoDB on MongoDB Console and familiarizes you with the features and functions of ApsaraDB for MongoDB.

If you need help, click **Ticket Service** > **Submit Ticket** on MongoDB Console or **Click Here** to submit a ticket.

For more information about ApsaraDB for MongoDB functions and pricing, go to the **official website** of ApsaraDB for MongoDB.

Statement

Some product features or services described in this document may be out of your scope of purchase or use. Follow the actual commercial contracts and conditions and terms. This document is only for guidance. No content in this document shall constitute any express or implied warranty. Due to product version upgrades or other reasons, the content of this document will be irregularly updated. Ensure that the document version is consistent with the corresponding software version.

If you are using ApsaraDB for MongoDB for the first time, refer to the related quick start documentation to understand ApsaraDB for MongoDB and to learn how to migrate your local database to ApsaraDB for MongoDB.

Replica set quick start

Cluster version quick start

You can manage MongoDB instances on MongoDB Console. This chapter describes how to log in/out of MongoDB Console.

Prerequisites

Before logging on to MongoDB Console, you need to buy a MongoDB instance. For details about purchasing, refer to [Purchase](#). For billing details, refer to [ApsaraDB for MongoDB pricing details](#).

The following steps use a replica set instance as an example to describe how to log in/out of MongoDB Console. The log in/out procedures for cluster version instances are similar to those for replica set. For details, refer to the corresponding console operation interface.

Log in MongoDB Console

Use the account that purchased ApsaraDB for MongoDB to log in to MongoDB Console.

When the system displays the MongoDB **Instance List** interface, select the region where the instance is located, as shown in the following figure.

InstanceID	Running Status	Zone	Configuration	Version	Network Type	Billing Method	Operation
dds-lx4H5d7687691a4 dds-lx4H5...	Running	cn-hangzhou-b	1 Core, 2 GB Disk Space: 10 G	MongoDB 3.2	Classic Network	Subscription Expiration Time: 2017-07-10 00:00:00	Manage Restart More
dds-lx4k2228ea133104 88--12302	Running	cn-hangzhou-b	1 Core, 2 GB Disk Space: 10 G	MongoDB 3.2	Classic Network	Pay-As-You-Go	Manage Restart Release More

Click the instance ID or **Manage** to go to the **Basic Information** page, where you can manage the instance account and white list and set instance parameters.

Log out of MongoDB Console

Use either of the following methods to log out of MongoDB Console:

Click user information in the upper-right corner. In the displayed menu, click **Sign out**.

Close the web browser.

Manage instances

Background information

MongoDB instances support two billing methods: Subscription and Pay-As-You-Go.

Subscription: Instances paid by yearly or monthly subscriptions cannot be voluntarily deleted or released. When the purchased MongoDB instance expires, it will be locked and cannot be read or written. You must renew your subscription to continue using the instance (How to Renew). If the subscription is not renewed, the instance will be automatically and irrecoverably deleted 7 days after the end of the service period. Before this happens, back up your data and migrate it from ApsaraDB for MongoDB to avoid data loss.

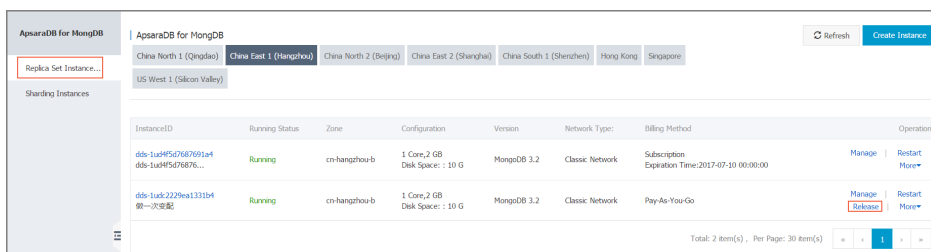
Pay-As-You-Go: This type of instances can be voluntarily released.

Procedure

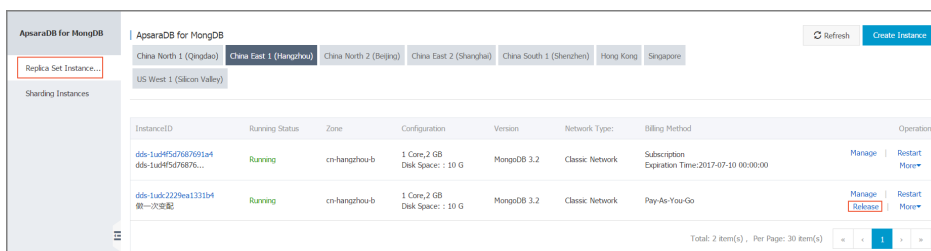
Log on to **MongoDB Console**.

If the target instance is a replica set instance, you can find it on the **Instance List** page.

Click **Release** in the work area and click **OK** in the confirmation box. Refer to the following figure.



If the target instance is a cluster instance, you can find it on the **Instance List** page. Click **Release**, and click **OK** in the confirmation box. Refer to the following figure.

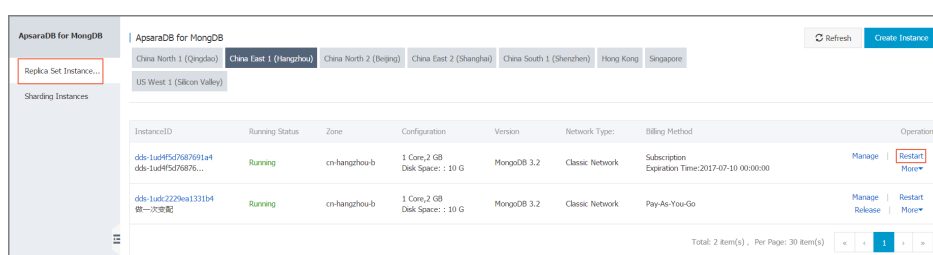


Note: Restarting an instance will cause connection interruption. Exercise caution and take service protection measures before you restart an instance.

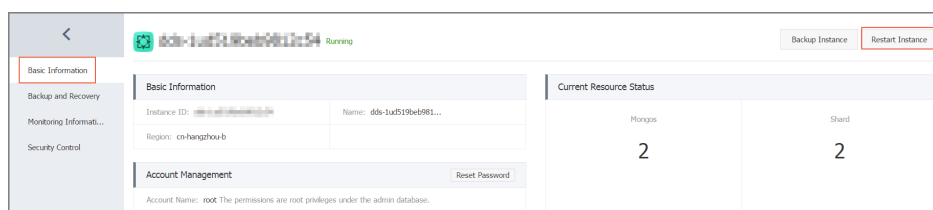
Procedure

Log on to MongoDB Console.

If the target instance is a replica set instance, you can find it on the instance list page. Click **Restart** in the work area and click **OK** in the confirmation box. Refer to the following figure.



If the target instance is a **cluster version instance**, you can find it on the **Instance List** page. Click **Restart**, and click **OK** in the confirmation box. Refer to the following figure.



Manage account

You can reset an instance password if you did not set a password when creating the instance, or if you forgot or need to modify the password.

Note: For data security consideration, it is advised to periodically change your password.

Procedure

Log on to MongoDB Console.

Find the target instance, and click the instance ID or **Manage** to go to the **Basic Information** page.

Click **Reset Instance Password** in the **Account Management** column.

In the **Reset Instance Password** window, enter a new password and click **OK**.

Connect to an instance

Alibaba Cloud intranets are classified into classic network and VPC. Cloud products (such as ECS and ApsaraDB for MongoDB) in the same region can establish cross-zone connection over an intranet. There are two scenarios of intranet-based cross-zone connection between ApsaraDB for MongoDB and ECS:

Connection between an ECS instance and a MongoDB instance that is bought in another zone of the same region as the ECS instance.

If the ECS instance is a VPC instance, to connect the two instances over the intranet, make sure both instances have the same VPC ID and create a switch in the zone where the MongoDB instance is located.

If the ECS instance belongs to the classic type, to connect the two instances, make sure the MongoDB instance also belongs to the classic type.

Connection between an existing MongoDB instance and ECS instance

In the case that the ECS instance and MongoDB instance are located in the same region:

The two instances can establish connection over the intranet only if both instances belong to the same network type (which is classic or VPC; in the latter case, both instances must have the same VPC ID).

If the two instances belong to different network types, use the **network type change** function provided by ApsaraDB for MongoDB to change the network type of the MongoDB instance before you connect the two instances.

You can use any of the following methods to connect to an ApsaraDB for MongoDB instance:

- Mongo shell connection
- Mongo driver connection
- Internet connection
 - ECS Linux
 - ECS Windows

Set network type

Background information

ApsaraDB supports two types of network: classic and Virtual Private Cloud (VPC). On the Alibaba Cloud platform, a classic network and VPC have the following differences:

Classic network: Cloud services on the classic network are not isolated, and unauthorized access can only be blocked by the security group or white list policy of the cloud services.

VPC: This helps you build an isolated network environment on Alibaba Cloud. You can customize the route table, IP address range, and gateway on the VPC. In addition, you can combine your machine room and cloud resources in the Alibaba Cloud VPC into a virtual machine room through a leased line or VPN to migrate applications to the cloud.

By default, MongoDB uses the classic network type. If you want to use VPC, ensure that the MongoDB and VPC instances are in the same region. You may create a VPC instance in either of the following scenarios:

If no MongoDB instance exists, create a VPC instance and then create a MongoDB instance in VPC. This chapter describes how to create a MongoDB instance.

If a MongoDB instance already exists, create a VPC instance in the region where the MongoDB instance is located and add the MongoDB instance to the VPC instance. For details, refer to the description about how to change the network type of an existing MongoDB instance.

Procedure

Create a VPC instance. For details, refer to [Create VPC](#).

Create a MongoDB instance in the region where the VPC instance is located.

During purchasing, select **VPC** as the network type and select the corresponding VPC instance. For details, refer to [Create a replica set instance](#).

Background information

Note: This document is intended for replica set instances only. Cluster version instances do not support network type change.

ApsaraDB supports two types of network: classic and Virtual Private Cloud (VPC). On the Alibaba Cloud platform, a classic network and VPC have the following differences:

Classic network: Cloud services on the classic network are not isolated, and unauthorized access can only be blocked by the security group or white list policy of the cloud services.

VPC: This helps you build an isolated network environment on Alibaba Cloud. You can customize the route table, IP address range, and gateway on the VPC. In addition, you can combine your machine room and cloud resources in the Alibaba Cloud VPC into a virtual machine room through a leased line or VPN to migrate applications to the cloud.

By default, MongoDB uses the classic network type. If you want to use VPC, ensure that the MongoDB and VPC instances are in the same region. You may create a VPC instance in either of the following scenarios:

If no MongoDB instance exists, create a VPC instance and then create a MongoDB instance in VPC. For details, refer to [Create a MongoDB instance](#).

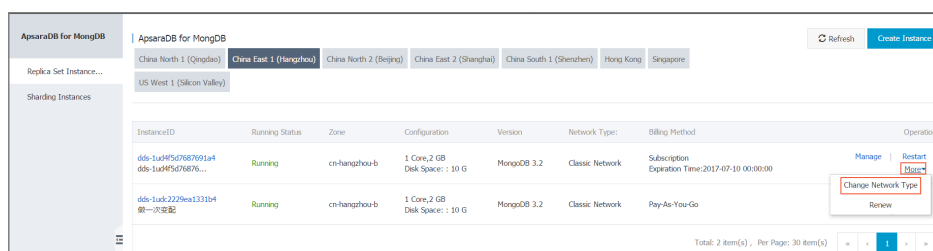
If a MongoDB instance already exists, create a VPC instance in the region where the MongoDB instance is located and add the MongoDB instance to the VPC instance to change the network type of the MongoDB instance. This chapter describes how to change the network type for MongoDB instances.

Procedure

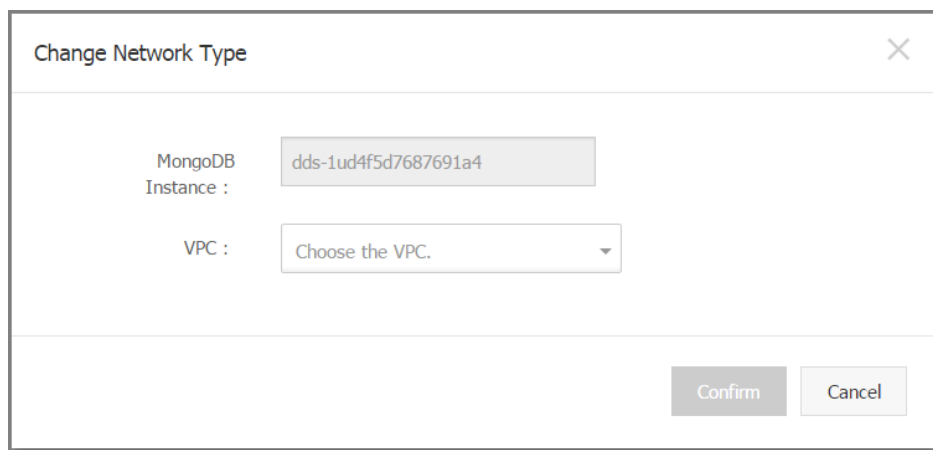
Create a VPC instance in the region where the MongoDB instance is located. For details, refer to [Create VPC](#).

Log on to MongoDB Console and find the target instance.

In the work area, choose **More > Changing the Network Type**, as shown in the following figure.



On the **Switch to VPC** page, select the VPC and VSwitch and click **OK**, as shown in the following figure.



Data can be migrated between ApsaraDB for MongoDB instances and self-built MongoDB instances or between different ApsaraDB for MongoDB instances.

For details, refer to the following documents:

- Replica set data import
- Replica set data migration
- Cluster version data import
- Cluster version data migration

Back up and recovery

Complete the backup settings to enable ApsaraDB for MongoDB to perform automatic backup at selected time points.

Procedure

Log on to MongoDB Console and find the target instance.

Click the instance ID or **Manage** or **View** to go to the **Basic Information** page.

Select **Backup and Recovery** in the navigation bar on the left.

Click **Backup Settings**.

Click **Edit** to customize the automatic backup cycles and times.

Note: By default, backup data is retained for 7 days. This setting cannot be modified.

Click **OK** to complete automatic backup setting.

In addition to the general backup settings, you can initiate a manual backup request on the console at any time.

Procedure

Log on to MongoDB Console and find the target instance.

Click the instance ID or **Manage** or **View** to go to the **Basic Info** page.

Click **Backup Instance** in the upper-right corner.

Click **OK** to back up the instance immediately.

Note: On the **Backup List** page, you can select time ranges and query historical backup data. By default, you can query historical backup data from the past 7 days.

The backups of cluster version instances can be downloaded based on the backup time and shard nodes.

Procedures

Log on to MongoDB Console and find the target instance.

Click the instance ID to go to the **Basic Information** page.

Select **Backup and Recovery** in the navigation bar on the left, as shown in the following figure.

Start of Backup/End Time	Backup Policy	Backup Size	Backup Method	Backup Type	Status	Operation
2017-06-23 10:30:29 / 2017-06-23 10:32:53	System Backup	1.00K	Logical Backup	Full Backup	Success	Download
2017-06-22 10:30:12 / 2017-06-22 10:32:36	System Backup	1.00K	Logical Backup	Full Backup	Success	Download
2017-06-21 10:30:58 / 2017-06-21 10:33:22	System Backup	1.00K	Logical Backup	Full Backup	Success	Download
2017-06-20 10:30:16 / 2017-06-20 10:32:31	System Backup	1.00K	Logical Backup	Full Backup	Success	Download
2017-06-19 10:31:02 / 2017-06-19 10:33:15	System Backup	1.00K	Logical Backup	Full Backup	Success	Download
2017-06-18 10:30:22 / 2017-06-18 10:32:35	System Backup	1.00K	Logical Backup	Full Backup	Success	Download
2017-06-17 10:30:17 / 2017-06-17 10:32:30	System Backup	1.00K	Logical Backup	Full Backup	Success	Download

Total: 7 item(s) . Per Page: 30 item(s)

On the **Backup List** page, select a time range, shard nodes, and the backup data set you want to download, and click **Download**.

Note: Run the below command to import data to a user-created database after the backup file is downloaded.

```
cat xx.ar| mongorestore -h xxx --port xxx -u xxx -p xxx --drop --gzip --archive -vvvv --stopOnError
```

The backups of three-node replica set instances can be downloaded based on the backup time.

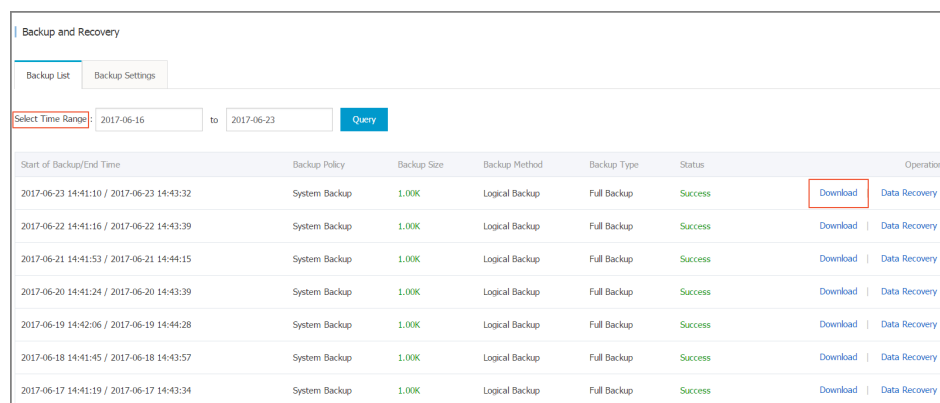
Procedure

Log on to MongoDB Console and find the target instance.

Click the instance ID or **Manage** to go to the **Basic Information** page.

Select **Backup and Recovery** in the navigation bar on the left.

On the **Backup List** page, select a time range and the backup data set you want to download, and click **Download**. Refer to the following figure.



Start of Backup/End Time	Backup Policy	Backup Size	Backup Method	Backup Type	Status	Operation
2017-06-23 14:41:10 / 2017-06-23 14:43:32	System Backup	1.00K	Logical Backup	Full Backup	Success	Download Data Recovery
2017-06-22 14:41:16 / 2017-06-22 14:43:39	System Backup	1.00K	Logical Backup	Full Backup	Success	Download Data Recovery
2017-06-21 14:41:53 / 2017-06-21 14:44:15	System Backup	1.00K	Logical Backup	Full Backup	Success	Download Data Recovery
2017-06-20 14:41:24 / 2017-06-20 14:43:39	System Backup	1.00K	Logical Backup	Full Backup	Success	Download Data Recovery
2017-06-19 14:42:06 / 2017-06-19 14:44:28	System Backup	1.00K	Logical Backup	Full Backup	Success	Download Data Recovery
2017-06-18 14:41:45 / 2017-06-18 14:43:57	System Backup	1.00K	Logical Backup	Full Backup	Success	Download Data Recovery
2017-06-17 14:41:19 / 2017-06-17 14:43:34	System Backup	1.00K	Logical Backup	Full Backup	Success	Download Data Recovery

Note: You can run the following command to import data to a user-created database after the backup file is downloaded.

```
```java
cat xx.ar| mongorestore -h xxx --port xxx -u xxx -p xxx --drop --gzip --archive -vvvv --stopOnError
```
```

The data recovery function can minimize the damage caused by database misoperations. Currently, ApsaraDB for MongoDB supports data recovery via backup.

Note: The MongoDB rollback operation will overwrite the data. After rollback, the data cannot be restored. Therefore, perform rollback with caution. If time permits, we suggest using the instance creation method from backup points. This method creates a Pay-As-You-Go instance based on the backup set to be recovered. After verifying that the data is correct, you can recover the data to the original instance.

Procedure

Log on to MongoDB Console and find the target instance.

Click the instance ID in the ReplicaSet instance list or **Manage** to go to the **Basic Information** page.

Select **Backup and Recovery** in the navigation bar on the left.

On the **Backup List** page, select the time range for recovery and click **Query**.

Find the target backup file and click **Data Recovery**.

In the **Data Recovery** window, select **OK** to directly recover the data of the original instance.

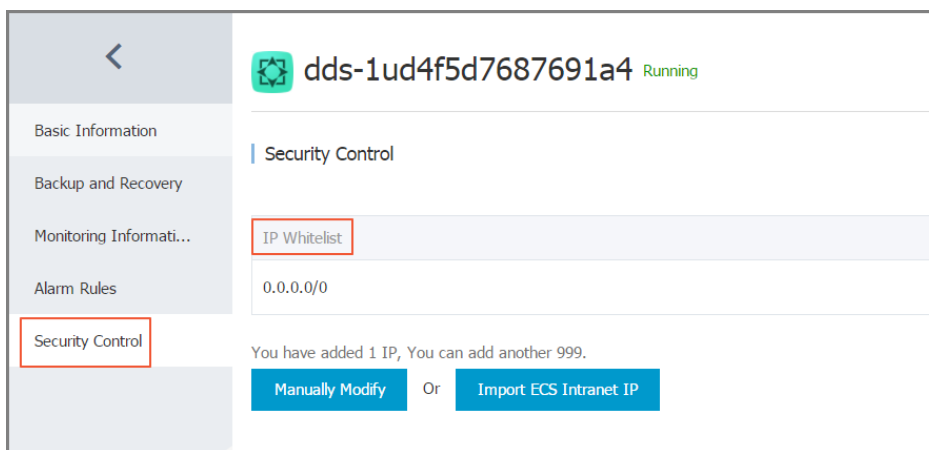
To ensure database security and stability, ApsaraDB for MongoDB automatically adds the IP address 127.0.0.1 to a white list after an instance is created. Therefore, after you create an instance, add the IP addresses or segments that need to access the database to the white list. Otherwise, you will not be able to view the instance connection address on the **Basic Information** page of the instance. MongoDB allows you to add up to 1,000 IP addresses.

Add an IP whitelist

Log on to MongoDB Console and find the target instance.

Click the instance ID or **Manage** or **View** to go to the **Basic Information** page.

Click **Security Control** to go to the IP whitelist setting, as shown in the following figure.



Click **Manually Modify** to manually enter IP addresses or segments. You can also click **Import ECS Intranet IP** to enable the system to automatically add activated intranet IP addresses of ECS.

Note:

Separate the IP addresses by commas (,). You can add up to 1,000 unique IP addresses/IP segments. Supported IP address formats include 0.0.0.0/0, 10.23.12.24 (IP), and 10.23.12.24/24 (CIDR mode; classless inter-domain routing; /24 indicates the length of the prefix in the IP address; the prefix length ranges from 1 to 32).

0.0.0.0/0 and a blank field indicates that there is no IP access restriction. In this case, the database may have a high security risk. It is advised to set the access permission only for the Internet IP address/IP address segment of your Web server.

MongoDB provides 12 monitor groups for you to create custom metrics as needed.

Note: Cluster version instances do not support this feature.

Metric descriptions

Refer to Cloud Service Monitor Document.

Set alert policies

Log on to **MongoDB Console** and find the target instance.

Click the instance ID or **Manage** to go to the **Basic Information** page.

Select **Alert Policies** in the navigation bar on the left.

Click **Set Alert Policies** to go to CloudMonitor Console.

On the **Instance List** page, select one or more instance IDs and click **Set Alert Policies** to go to the **Batch Set Alert Policies** window.

Add alert policies as needed in the instance dimension.

Click **Next** to set the notification object.

Click **OK** to complete alert policy setting.

Note: After setting alert polices, you can view the alert history and modify the alert policy status on the alert policy page of CloudMonitor Console.