ApsaraDB for MongoDB

User Guide

User Guide

Preface

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 the MongoDB console and familiarizes you with the features and functions of ApsaraDB for MongoDB.

If you need help, click **Ticket Service** > **Submit Ticket** on the MongoDB console.

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 is irregularly updated. Make sure that the document version is consistent with the corresponding software version.

Quick start

If you are using ApsaraDB for MongoDB for the first time, see 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

Log on and log out

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

Prerequisites

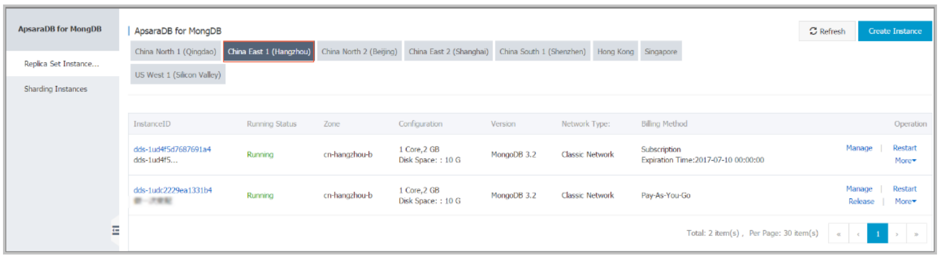
Before logging on to the MongoDB console, you must buy a MongoDB instance. For more information about purchasing, see Purchase. For more information about billing details, see ApsaraDB for MongoDB pricing.

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

Log on to MongoDB console

Use the account that purchased ApsaraDB for MongoDB to log on to the 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-1ud4f5d7687691a4 dds-1ud4f5...	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-1udc2229ea1331b4 [redacted]	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

Total: 2 item(s) , Per Page: 30 item(s) « ‹ 1 › »

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

Log out of MongoDB console

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

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

- Close the web browser.

Manage instances

Release an instance

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 is locked and cannot be read or written. You must renew your subscription to continue using the instance. If the subscription is not renewed, the instance is 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.

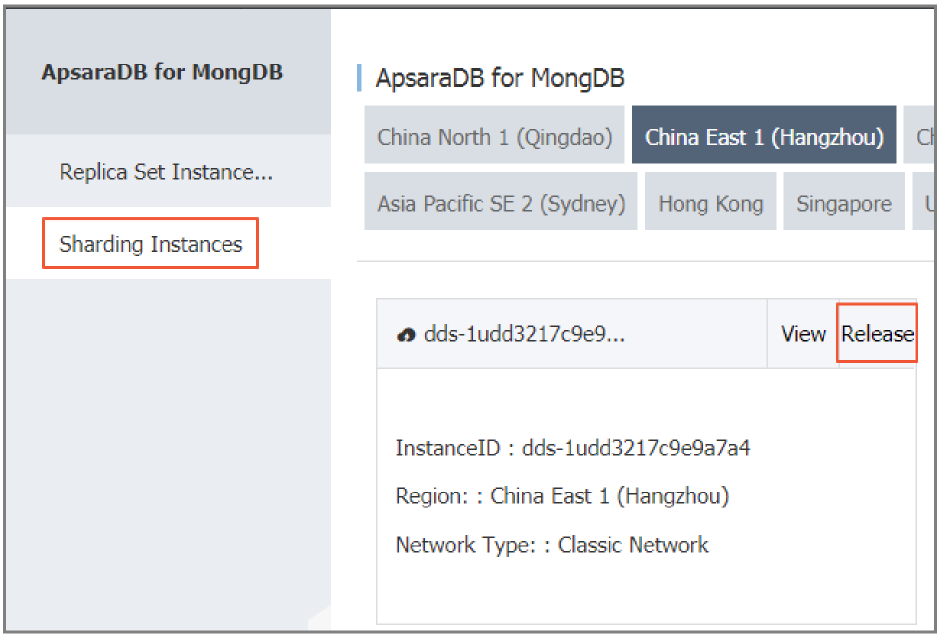
- Pay-As-You-Go: This type of instances can be voluntarily released.

Procedure

- Log on to the 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.

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. See the following figure.



InstanceID : dds-1udd3217c9e9a7a4

Region: : China East 1 (Hangzhou)

Network Type: : Classic Network

Restart an instance

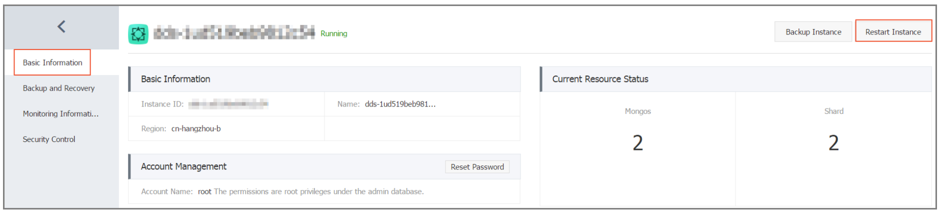
Note: Restarting an instance can cause connection interruption. Exercise caution and take service protection measures before you restart an instance.

Procedure

Log on to the 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.

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



[redacted] Running

Basic Information

Instance ID: [redacted]

Name: dds-1ud519beb981...

Region: cn-hangzhou-b

Account Management

Account Name: root The permissions are root privileges under the admin database.

Current Resource Status

Mongos	Shard
2	2

Manage account

Reset a password

You can reset an instance password if you do not set a password when creating the instance, or if you forget or want to modify the password.

> **Note:** For data security consideration, we recommend you to periodically change your password.

Procedure

Log on to the 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

Intranet-based cross-zone connections between MongoDB and ECS instances

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.

Connect to an instance

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

Set the network type when creating an instance

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 whitelist 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 on-premises IDC with cloud resources in the Alibaba Cloud VPC 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, guarantee 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 more information, see the description about how to change the network type of an existing

MongoDB instance.

Procedure

Create a VPC instance. For more information, see 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 more information, see Create a replica set instance and Create a sharding instance.

Set the network type when creating an instance

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 whitelist 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 on-premises IDC with cloud resources in the Alibaba Cloud VPC 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, guarantee 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 more information, see 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.

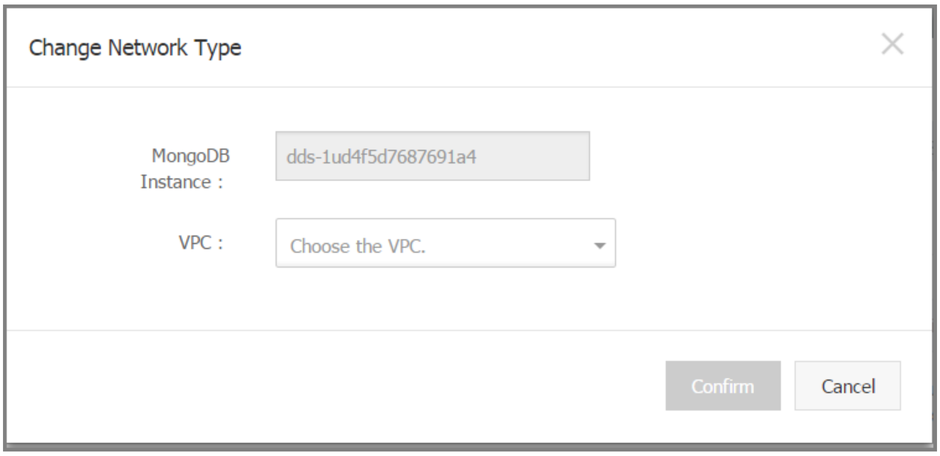
Procedure

Create a VPC instance in the region where the MongoDB instance is located. For more information, see Create VPC.

Log on to the MongoDB console and find the target instance.

In the work area, choose **More** > **Changing the Network Type**.

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



Change Network Type

MongoDB Instance : dds-1ud4f5d7687691a4

VPC : Choose the VPC.

Switch from classic network to VPC

Background

Virtual Private Cloud (VPC) is a private network logically isolated from other virtual networks. Alibaba Cloud VPC allows you to build an isolated network environment with better security and performance than classic network. With these benefits, VPC becomes a preferred networking choice for cloud users. To meet the increasing network migration needs, ApsaraDB for MongoDB adds a new feature called hybrid network access. This feature enables seamless migration from classic network to VPC with no intermittent service interruption or access interruption.

Solution

Previously, when you switch a MongoDB instance from the classic network to VPC, the address of the classic network is released immediately, which causes a transient disconnection shorter than 30s, and cloud products in the classic network, such as ECS, cannot reconnect to the MongoDB instance.

The hybrid access solution allows an MongoDB instance to be connected by ECS instances in a classic network and those in VPC to implement smooth change of network types. When you switch the MongoDB instance from the classic network to VPC, you can choose to retain the address of the classic network (for up to 120 days) while the new VPC connection address is generated. In this way, the instance can be accessed by ECS instances in the classic network and those in VPC during migration.

During hybrid access to the instance, you can gradually migrate ECS instances and other cloud products in the classic network to VPC to enable intranet-based connection between all products over VPC with improved security.

Limits

During the hybrid access period, switching to classic network is not supported.

Procedure

Log on to the MongoDB console and find the target instance.

In the operation area, choose **More** > **Change network type** to go to the **Change Network Type** page.

Click **Switch to VPC** to go to the **Switch to VPC** confirmation page. Then, select the expected VPC and VSwitch, select **Reserve Original Classic Network**, set the expiration time of the intranet address of the original classic network, and click **OK**.

Migrate data

Data can be imported and exported between ApsaraDB for MongoDB instance and user-created MongoDB instance or between different ApsaraDB for MongoDB instances.If you must migrate your data to ApsaraDB for MongoDB, you can use one of the following two methods:

- Use DTS to import data

- Use the built-in utilities to import data

Back up and recovery

Automatic backup

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

Procedure

- Log on to the 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 left-side navigation pane.

- 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.

Manual backup

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

Procedure

Log on to the 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.

Backup progress cannot be viewed on the console.

Download backup data for sharding instances

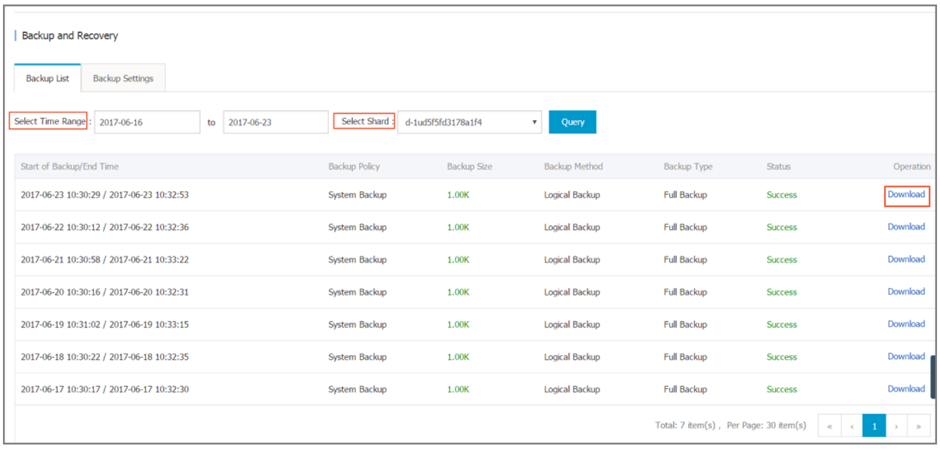
The backups of cluster version instances can be downloaded based on the backup time and shard nodes.

Procedures

Log on to the MongoDB console and find the target instance.

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

Select **Backup and Recovery** in the left-side navigation pane, 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 following 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
```

Download backup data for replica set instances

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

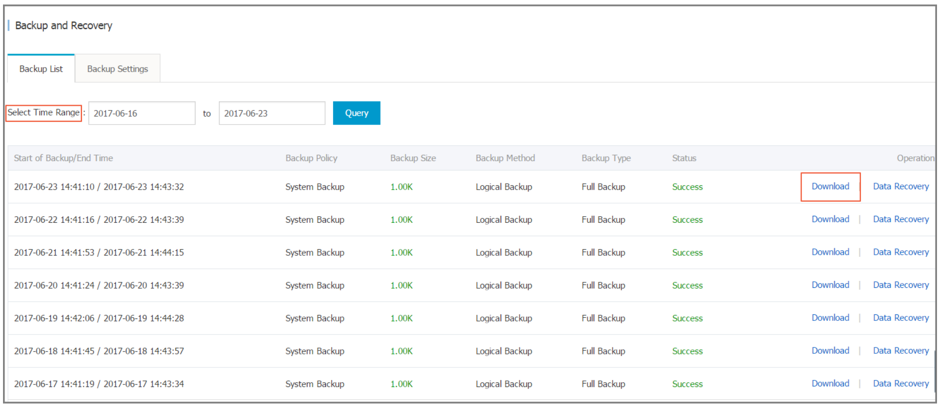
Procedure

Log on to the 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 left-side navigation pane.

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



Select Time Range: 2017-06-16 to 2017-06-23

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.

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

Data recovery

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

Note:

The MongoDB rollback operation overwrites the data. After rollback, the data cannot be restored. Therefore, perform rollback with caution.

If time permits, we recommend that you use 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 the 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 left-side navigation pane.

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.

Physical backup and recovery

Download and decompression

Download the physical backup file and decompress the file to the data directory where MongoDB is located (the data directory must be empty). The following operation assumes that /path/to/mongo is the location directory for MongoDB to be started using the physical backup:

```
cd /path/to/mongo/data/
rm -rf *
tar xzvf hins_xxx.tar.gz
```

Version and configuration requirements for MongoDB startup

MongoDB version: 3.2 or later.

ApsaraDB for MongoDB uses the WiredTiger storage engine by default and enables the directoryPerDB feature. Therefore, select related options in configuration.

The physical backup of ApsaraDB for MongoDB contains the replica set configuration of the original instance. Therefore, MongoDB must be started in single-node mode (the configuration file cannot contain configurations related to replication). Otherwise, access may fail. To start MongoDB in replica set mode, follow these steps after MongoDB is started in single-node mode:

Remove the configurations of the original replica set.

```
  use local
db.system.replset.remove({})
```

Modify the configuration file to add configurations related to replication.

Restart the mongod process.

Reinitialize the replica set.

The physical backup of ApsaraDB for MongoDB contains the user name and password of the original instance. If authentication is enabled in the configuration file, use the user name and password of the original instance for access.

The following is the configuration template that uses the physical backup to start ApsaraDB for MongoDB (authentication is enabled for the single node):

```
  systemLog:
destination: file
path: /path/to/mongo/mongod.log
logAppend: true
security:
authorization: enabled
storage:
dbPath: /path/to/mongo/data
directoryPerDB: true
net:
http:
enabled: false
port: 27017
unixDomainSocket:
enabled: false
processManagement:
fork: true
pidFilePath: /path/to/mongo/mongod.pid
```

Security control

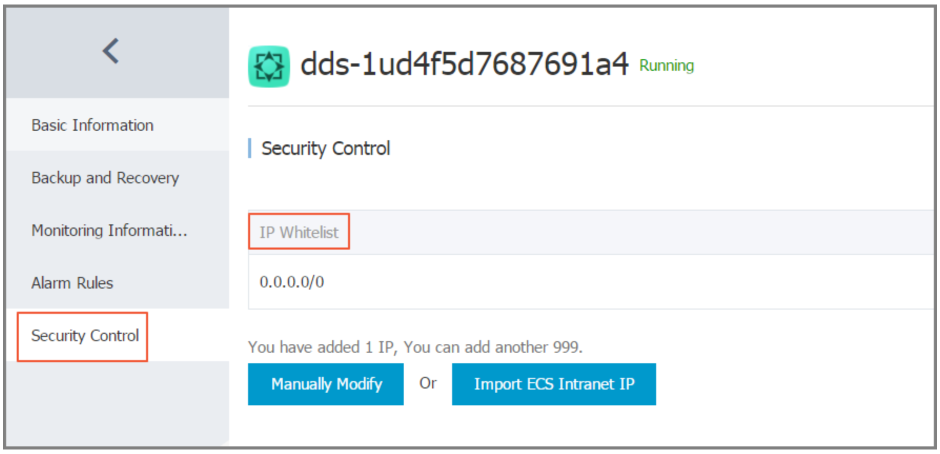
To guarantee database security and stability, ApsaraDB for MongoDB automatically adds the IP address 127.0.0.1 to a whitelist after an instance is created. Therefore, after you create an instance, add the IP addresses or segments that need to access the database to the whitelist. Otherwise, you are not 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 the 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** page, as shown in the following figure.



0.0.0.0/0

You have added 1 IP, You can add another 999.

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 no IP access restriction is in place. In this case, the database may have a high security risk. We recommend that you set the access permission only for the Internet IP address/IP address segment of your Web server.

Monitoring and Alarms

Set alarm rules

MongoDB allows you to set alarm rules based on monitoring items.

For more information about monitoring items, see Monitoring items.

Procedure

Log on to the MongoDB console and locate the target instance.

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

In the left-side navigation pane, click **Alarm Rules**.

Click **Set Alarm Rule** to go to the CloudMonitor console.

Click **Replica Set Instance List** or **Cluster Instance List**, select one or more instances, and click **Set Alarm Rules**.

Set the parameters in the **Set Alarm Rules** and **Notification Method** areas.

Click **Confirm**.

> **Note**: To view the alarm history of an alarm rule, click **View** of an alarm on the **Alarm Rules** tab page.

View monitoring information

The MongoDB console provides various performance monitoring metrics so that you can analyze the running status of the instance.

Note:

The system collects monitoring data every five minutes.

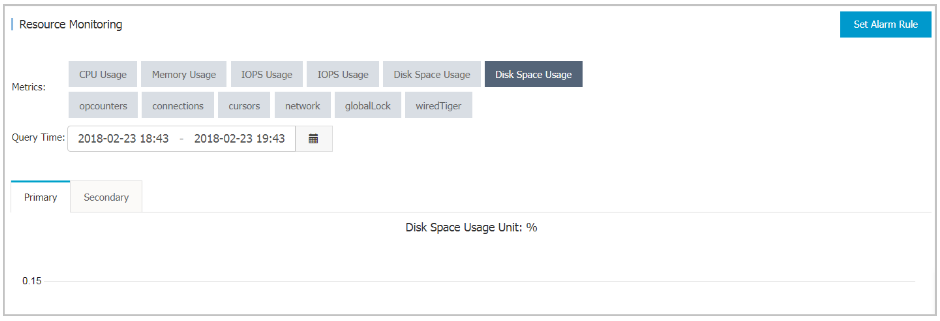
You can query monitoring data of the last 30 days.

Procedure

Log on to the MongoDB console.

Locate the target instance and click its ID or **Manage** in the operation column to display the **Basic Information** page.

In the left-side navigation pane, click **Monitoring Information**.



Query Time: 2018-02-23 18:43 - 2018-02-23 19:43

You can set the time range and select a monitoring metric.

Monitoring metrics

Monitoring metric	Description
CPU Usage	CPU usage of the instance
Memory Usage	Memory usage of the instance
IOPS Usage	Used IOPS, including: - Data disk IOPS - Log disk IOPS
IOPS Usage	Ratio of used IOPS to maximum available IOPS
Disk Space Usage	Occupied disk space, including: - Total used space - Occupied data disk space - Occupied log disk space
Disk space usage	Ratio of total used space to maximum available space
opcounters	Number of performed operations per second, including: - Number of insert operations - Number of queries - Number of delete operations - Number of update operations - Number of getmore operations - Number of commands
connections	Number of current connections
cursors	Number of cursors, including: - Number of open cursors - Number of timed out cursors
network	Network traffic, including: - Received traffic - Sent traffic - Number of handled requests
globalLock	Number of operations queued waiting for the lock - Number of operations that are currently queued and waiting for the read lock - Number of operations that are currently queued and waiting for the write lock - Total number of operations queued waiting for the lock
wiredTiger	wiredTiger engine cache data, including: - Volume of data read into the cache - Volume of data written from the cache - Maximum cache size

Audit logs

Background

The audit log function records operations performed on the databases in the instance. You can use the audit logs for fault analysis, behavior analysis, and security audit. Audit logs are generally becoming an essential regulatory requirement of Finance Cloud and other mission-critical services.

Note:MongoDB audit logs currently record only the following operations:

- auth, admin, slow, insert, update, delete, command
- slow queries that last over 100 msCommon queries are not recorded.

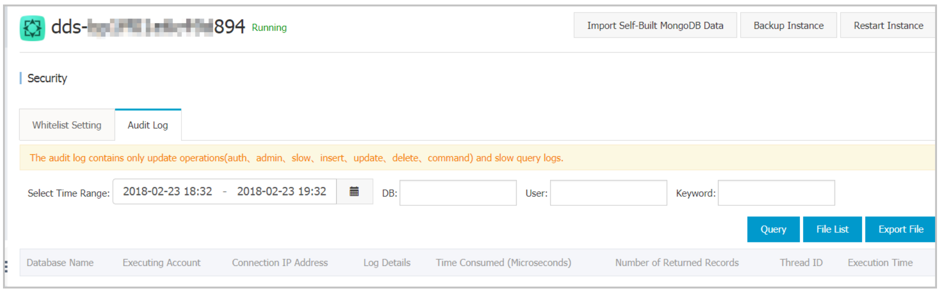
Procedure

Log on to the MongoDB console.

Locate the target instance and click its ID or **Manage** in the operation column to display the **Basic Information** page.

In the left-side navigation pane, click **Data Security**.

Click the **Audit log** tab. The following figure shows the audit log page of a replica set instance.



dds-[redacted]894 Running

Security

The audit log contains only update operations(auth、admin、slow、insert、update、delete、command) and slow query logs.

Select Time Range: 2018-02-23 18:32 - 2018-02-23 19:32 DB: User: Keyword:

Database Name	Executing Account	Connection IP Address	Log Details	Time Consumed (Microseconds)	Number of Returned Records	Thread ID	Execution Time

You can perform the following operations:

- Set the time range, database name, database user name, or other keywords, and

click **Query**.
- Click **File List** to display exported audit log files.
- Click **Export File** to export audit logs.

Upgrade the database version

ApsaraDB for MongoDB delivers higher performance and security in version 3.4 compared to version 3.2.
To upgrade ApsaraDB for MongoDB from version 3.2 to 3.4, follow these steps:

Note:

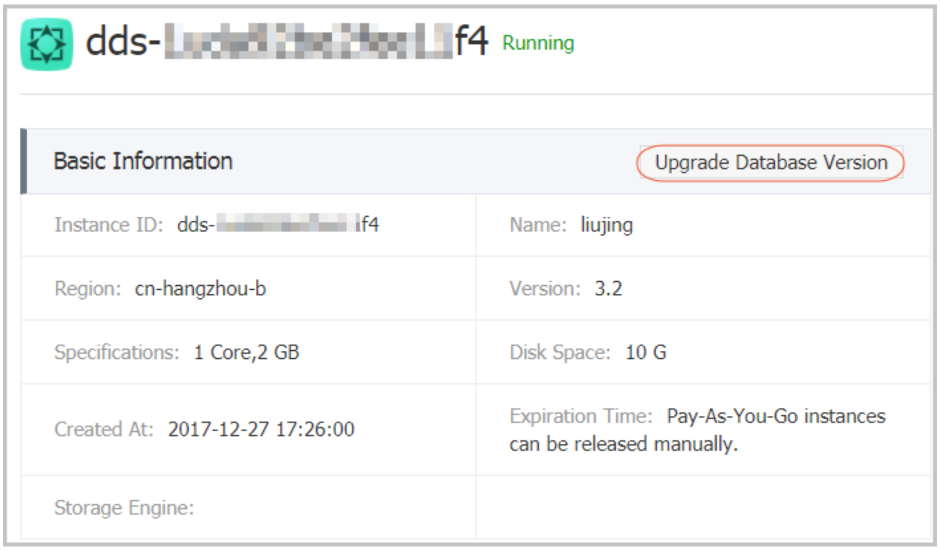
- Perform the upgrade during off-peak hours, because the instance will restart during the upgrade.
- The instance cannot be downgraded after being upgraded.

Procedure

Log on to MongoDB console and find the target instance.

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

Click **Upgrade Database Version**.

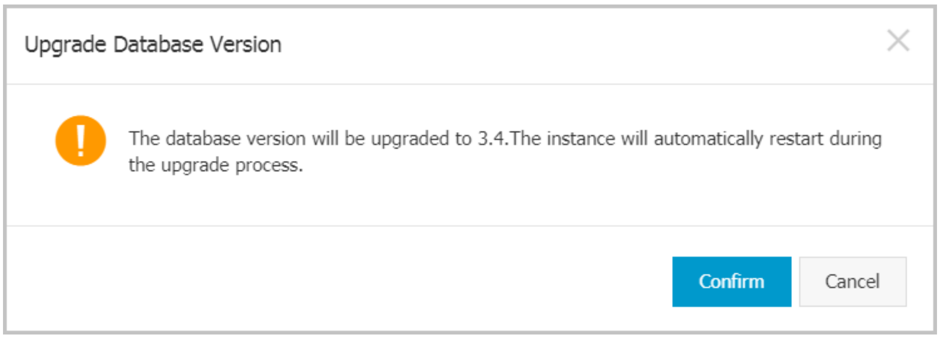


dds-[redacted]f4 Running

Basic Information

Instance ID: dds-[redacted]f4	Name: liujing
Region: cn-hangzhou-b	Version: 3.2
Specifications: 1 Core,2 GB	Disk Space: 10 G
Created At: 2017-12-27 17:26:00	Expiration Time: Pay-As-You-Go instances can be released manually.
Storage Engine:	

In the **Upgrade Database Version** window, click **Confirm** to start the upgrade.


Upgrade Database Version

The database version will be upgraded to 3.4.The instance will automatically restart during the upgrade process.