

Document Database Service User Guide

dds_faq

Issue 01
Date 2023-01-30



Copyright © Huawei Technologies Co., Ltd. 2023. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Contents

1 Product Consulting	1
1.1 What Is the Relationship Between DDS and MongoDB Community Edition?	1
1.2 What Are the Differences Between DDS and GaussDB(for Mongo)?	1
1.3 What Precautions Should Be Taken When Using DDS?	2
1.4 What Is the Availability of DDS DB Instances?	2
1.5 Will My DDS DB Instances Be Affected by Other Users' DDS DB Instances?	2
1.6 Does DDS Support Multi-AZ Deployment?	2
1.7 Can I Change the VPC for a Created Instance?	3
1.8 Can I Change the Region for a Created Instance?	3
1.9 What Is Hidden Node?	3
2 Database Versions	4
2.1 Does DDS Support Version Upgrade?	4
3 Resource and Disk Management	5
3.1 Which Items Occupy the Storage Space of DDS Instances?	5
3.2 Which Types of Logs and Files Occupy DDS DB Instance Storage Space?	5
3.3 Why Is the Storage Space Usage Displayed on the GUI Smaller Than the Actual Usage?	6
3.4 Why Does Available Disk Space Not Increase After Data Is Deleted?	6
3.5 Why Is the Resident Memory of a 4 vCPUs/8 GB Memory Replica Set Instance Only 4 GB?	6
4 Capacity Expansion and Specification Changes	7
4.1 Can a DDS Instance Type Be Changed?	7
4.2 Can Nodes Be Added to DDS Instances?	7
4.3 Is DDS Available When Nodes Are Being Added?	8
5 Database Performance	9
5.1 When Will a Primary/Standby Switchover Be Triggered for a Cluster or Replica Set?	9
5.2 High Storage Usage	10
5.3 What Is the Time Delay for Primary/Secondary Synchronization in a Replica Set?	12
5.4 How Is Data Transferred Between the Primary and Secondary Nodes of a Replica Set?	12
5.5 How Do I Clear an Alarm Saying the Shard Memory Usage Exceeds 90%?	12
5.6 What Can I Do If a Query Error Is Reported After Data Is Written Into the DDS Cluster?	12
6 Database Permissions	14
6.1 What Permissions Does User root Have?	14

7 Creation and Deletion	15
7.1 How Do I Select Instance Specifications and Nodes?	15
7.2 Why Is an Instance Not Displayed on the Console After It Is Created?	15
7.3 Can I Use a Template to Create DDS DB Instances?	16
7.4 Why Is Data Missing from My Database?	16
7.5 Will My Backups Be Deleted If I Delete My Cloud Account?	16
7.6 What Are the Differences Between Instance Deletion and Unsubscription?	16
8 Database Connection	18
8.1 What Should I Do If I Fail to Connect to a DDS Instance?	18
8.2 What Can I Do If the Number of Connections of an Instance Reaches Its Maximum?	26
8.3 How Do I Query and Limit the Number of Connections?	28
8.4 What Should I Do If the ECS and DDS Are Deployed in Different VPCs and They Cannot Communicate with Each Other?	30
8.5 Do Applications Need to Support Automatic Reconnecting to the DDS Database?	30
8.6 How Do I Create and Log In to an ECS?	30
9 Installing a Client	31
9.1 How Can I Install a MongoDB Client?	31
9.2 How Do I Install Robo 3T?	33
10 Database Usage	36
10.1 How Do I View the Primary/Standby Nodes of a Replica Set Instance?	36
10.2 Can I Delete an Index That Fails to Be Created in DDS?	37
10.3 Does DDS Delete Expired Data Using TTL Indexes?	37
10.4 How Do I Use MapReduce Commands?	37
10.5 Does DDS Support the \$round Function?	38
10.6 How Do I Manage Balancers?	38
11 Database Migration	39
11.1 Does DDS Support Cross-Region Migration?	39
11.2 How Do I Migrate DDS Databases Between Different Accounts?	39
12 Database Storage	40
12.1 How Does DDS Store Data?	40
12.2 What Should I Do If My Data Exceeds the Database Storage Space of a DDS Instance?	40
12.3 Why Does a DDS DB Instance Become Read-only?	40
13 Database Parameters	42
13.1 Can I Change the Time Zone of a DDS Instance?	42
13.2 What DB Instance Monitoring Metrics Do I Need to Pay Attention To?	42
13.3 How Do I Enable JavaScript?	42
13.4 Does DDS Support Majority Read Concern?	42
14 Backup and Restoration	44
14.1 Will I Be Charged for Manual Backups of Deleted DB Instances?	44
14.2 How Do I Back Up DDS Databases to an ECS?	44

14.3 How Long Does DDS Store Backup Data For?.....	44
14.4 How Do I Retrieve Lost DDS Backup Data?.....	44
15 Network Security.....	45
15.1 What Security Protection Policies Does DDS Have?.....	45
15.2 Do I Need to Use DDS in a VPC?.....	45
15.3 How Do I Ensure the Security of DDS in a VPC?.....	45
15.4 Does DDS Support IPv6 Subnets?.....	45
16 Monitoring and Alarm.....	46
16.1 What DB Instance Monitoring Metrics Do I Need to Pay Attention To?.....	46
16.2 What Should I Do If I Cannot Find Common Monitoring Items When Configuring DDS Alarm Rules?	47
16.3 How Often Does DDS Collect Metrics?.....	48
A Change History (FAQs) Europe Site.....	49

1 Product Consulting

1.1 What Is the Relationship Between DDS and MongoDB Community Edition?

DDS is fully compatible with MongoDB Community Edition 3.4, 4.0, and 4.2, and partially compatible with MongoDB Community Edition 4.4. For details, see [Version Compatibility](#).

DDS supports most of MongoDB commands. Any client compatible with MongoDB can connect to DDS for data storage and execution of related operations.

You can learn more about the advantages of DDS by [comparing DDS with on-premises databases](#).

For details about DDS, see [What Is DDS?](#)

1.2 What Are the Differences Between DDS and GaussDB(for Mongo)?

Document Database Service (DDS) is a high performance high availability MongoDB-compatible database service that is secure and scalable. It provides a variety of functions including instance creation in just a few clicks, capacity scaling, disaster recovery, backup, restoration, and instance monitoring. For more information about DDS, see [DDS Overview](#).

GaussDB(for Mongo), also called enhanced MongoDB, is a distributed NoSQL database service from Huawei with decoupled compute and storage. GaussDB(for Mongo) is fully compatible with MongoDB APIs and provides high-performance, high-reliability, and enterprise-class services. For more information about GaussDB(for Mongo), see [Overview](#).

1.3 What Precautions Should Be Taken When Using DDS?

1. Failover
DDS uses multiple mongos, replica sets, and shards to ensure data reliability. When a mongos is faulty, the other mongos takes over services immediately to ensure service continuity. A replica set contains multiple secondary nodes. When the primary node is faulty, DDS selects a secondary node as the new primary within 30 seconds.
2. ECSs used for instances are invisible to you. Your applications can access only the IP addresses and ports corresponding to the database.
3. Backup files stored on OBS are invisible to you. They are only visible in the DDS backend management system.
4. With DDS, you do not need to perform basic database O&M operations, such as enabling HA and installing security patches, but you should still note:
 - a. Whether the vCPUs, IOPS, and storage space for DDS DB instances are sufficient. If any of them is insufficient, optimize or upgrade the related configuration.
 - b. Whether DDS DB instances have performance issues, whether there are a large number of , whether SQL statements need to be optimized, and whether there are redundant or missing indexes.

1.4 What Is the Availability of DDS DB Instances?

Formula for calculating the DDS DB instance availability:

DDS DB instance availability = $(1 - \text{Failure duration} / \text{Total service duration}) \times 100\%$

1.5 Will My DDS DB Instances Be Affected by Other Users' DDS DB Instances?

No. Your DDS DB instances and resources are isolated from others.

1.6 Does DDS Support Multi-AZ Deployment?

You can deploy a cluster or replica set instance across up to three AZs.

- Cluster instance:
For details, see "Creating a Cluster Instance Across Multiple AZs".
- Replica set instance:
For details, see "Creating a Replica Set Instance Across Multiple AZs".

1.7 Can I Change the VPC for a Created Instance?

After a DDS instance is created, the VPC of the instance cannot be changed on the DDS console. Execution caution when you select a VPC during instance creation.

1.8 Can I Change the Region for a Created Instance?

After a DDS instance is created, the region of the instance cannot be changed on the DDS console.

1.9 What Is Hidden Node?

Hidden nodes in DDS are used for backing up data of cluster and replica set instances.

Hidden nodes are the same as other backup nodes except that they have different names and cannot function as primary nodes.

2 Database Versions

2.1 Does DDS Support Version Upgrade?

Major Version Upgrade

DDS does not support major engine version upgrade on the console. You can use DRS to migrate data as required. For details, see [Upgrading a Major Version](#).

Minor Version Upgrade

DDS supports automatic and manual minor version upgrades, which can improve performance, add new functions, and fix bugs.

For details, see [Upgrading a Minor Version](#).

3 Resource and Disk Management

3.1 Which Items Occupy the Storage Space of DDS Instances?

The following types of data will occupy the storage space:

- The storage space you applied for will contain the system overhead required for inode, reserved block, and database operation.
- User data (backups not included)
- Data required to ensure instances run properly, such as system database data, rollback logs, and search indexes.
- Log output files that are generated by DDS ensure the stable operating of DDS instances. For example, Oplogs occupy 10% of storage space and cannot be resized.

3.2 Which Types of Logs and Files Occupy DDS DB Instance Storage Space?

Logs and files listed in the following table occupy storage space.

Database Type	File Type
DDS	Log files: mongod.log, mongos.log, configsvr.log and mongod_error.log
	Data files: database content and index file
	Other files: DDS temporary files and YAML configuration files.

3.3 Why Is the Storage Space Usage Displayed on the GUI Smaller Than the Actual Usage?

Data stored on DDS disks is compressed before being stored, so the storage usage displayed on the GUI is less than the amount of data stored.

3.4 Why Does Available Disk Space Not Increase After Data Is Deleted?

Operations such as write, update, and delete (including index insert and delete) are actually converted to write operations in the background. When data of an instance in use is deleted, the disk space is not reclaimed. Such unreclaimed disk space is called disk fragments. When new data is inserted, these fragments are reused without applying for new disk space. Different underlying storage engines (RocksDB and WiredTiger) vary according to specific scenarios.

After deleting data, RocksDB directly converts the **delete** operation to append write. After a certain amount of redundant data is accumulated, the background compact thread is automatically triggered to merge and aggregate data of multiple versions to release redundant disk space. You are advised to wait for the system to automatically reclaim the disk space. If the disk space usage is high and close to the threshold, contact Huawei technical support.

After deleting data, WiredTiger merges and aggregates data of multiple versions, causing disk space fragments. However, WiredTiger does not return the disk space to the operating system. WiredTiger marks the disk space for subsequent writes of the current collection, the reserved disk space is preferentially used for subsequent writes of the collection. To release the disk space, run the **compact** command. (Note: This command blocks normal services and is disabled by default.)

3.5 Why Is the Resident Memory of a 4 vCPUs/8 GB Memory Replica Set Instance Only 4 GB?

If 100% of the resident memory is occupied, the system is stuck and services cannot run properly.

4 Capacity Expansion and Specification Changes

4.1 Can a DDS Instance Type Be Changed?

The instance type cannot be changed, but you can use Data Replication Service (DRS) to migrate data between different types of instances.

For example, if you want to change a replica set instance to a cluster instance, you can purchase a cluster instance and use DRS to migrate data from the existing replica set instance to the cluster instance.

For details about data migration, see [Migrating Data Using DRS](#).

4.2 Can Nodes Be Added to DDS Instances?

You can add nodes to cluster and replica set instances. Single-node instances do not support adding nodes.

- Cluster instance
A cluster instance consists of mongos, and config, and shard nodes. Additional shard and mongos nodes can be added, but the number of config nodes is fixed.
For details, see [Adding Cluster Instance Nodes](#).
- Replica set instance
A replica set consists of the primary node, secondary node, and hidden node. By default, the system provides a three-node replica set. You can add nodes to a five-node or seven-node replica set as required. The newly added nodes are all secondary nodes.
For details, see [Adding Replica Set Instance Nodes](#).

4.3 Is DDS Available When Nodes Are Being Added?

Yes. Services are not affected by adding shard nodes. The existing shard nodes are not affected.

5 Database Performance

5.1 When Will a Primary/Standby Switchover Be Triggered for a Cluster or Replica Set?

Causes

The trigger for a switchover depends on the architectures: cluster or replica set.

- Cluster consists of three nodes: mongos, shard, and config. The shard and config nodes use a three-node replica-set architecture. If a primary node becomes faulty, it triggers a switchover.
- In a replica-set architecture there are also three nodes: primary, secondary, and hidden. The primary and secondary nodes provide IP addresses for external access. The primary node of a replica set instance is not fixed. If the configuration of the replica set instance changes, or if the primary node fails, or a switchover is triggered. A secondary node is promoted to primary, and the originally primary node is demoted to secondary.
- If the memory usage is too high, the instance is under heavy load and primary/standby switchover will occur.

For more information, see [Cluster Architecture](#) and [Replica Set Architecture](#).

Impacts

- If a primary node fails, the system selects a standby node as the new primary within 30 seconds.
- If your applications are connected to a primary node that is demoted to standby due to a primary/standby switchover, the read and write operations on services will be affected.

Service Deployment Suggestion

Ensure that your application supports automatic reconnection, so the application can be automatically reconnected to the instance and avoid write errors in the event of a brief disconnects.

- It is recommended that you use URLs to connect the cluster and replica set instances. When a node is faulty, the primary/standby switchover does not affect service read and write operations. For details, see [Connecting to a Cluster Instance](#) and [Connecting to a Replica Set Instance for Read and Write Separation and High Availability](#).
- If an instance is under heavy load, you can change the instance class. Take a cluster instance as an example. For details, see [Changing a Cluster Instance Class](#).

5.2 High Storage Usage

If the storage usage of a DDS instance is too high or fully used, the instance becomes unavailable.

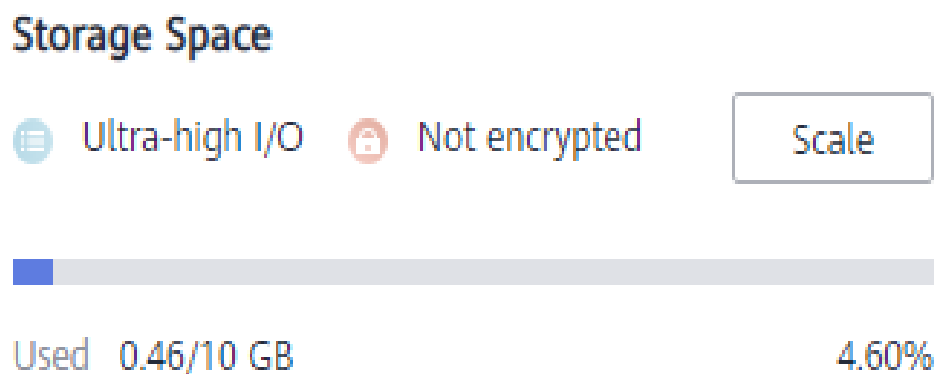
This section describes how to analyze and fix high storage usage.

Checking the Storage Usage

DDS provides the following two methods to check the storage usage of an instance:

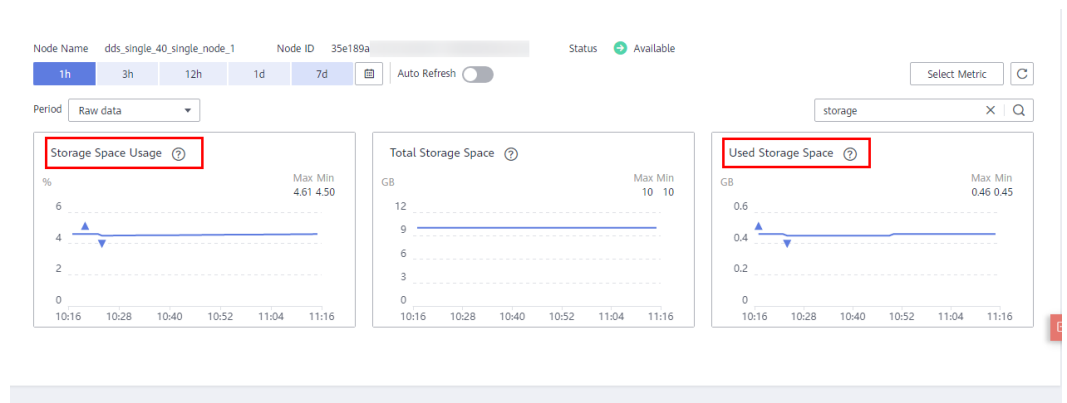
1. Check the storage usage on the DDS console.
You can log in to the DDS console and click the instance. On the **Basic Information** page, you can view the storage space of the instance in the **Storage Space** area.

Figure 5-1 Checking the storage usage



2. View the monitoring metrics (storage usage and used storage).
To view monitoring metrics, see [Viewing Monitoring Metrics](#).

Figure 5-2 Checking the storage usage



Solution

- For cluster instances, data may be unevenly distributed because the database collection is not properly sharded. As a result, the storage usage is high. Shard the database collection properly.
- As service data increases, the original database storage is insufficient. You can expand the storage space to fix this problem.
 - To scale up storage for cluster instances, see [Scaling Up a Cluster Instance](#).
 - To scale up storage for replica set instances, see [Scaling Up a Replica Set Instance](#).
 - To scale up storage for single node instances, see [Scaling Up a Single Node Instance](#).

If the storage space has reached the upper limit of your instance class, change the instance class first.

- To change the cluster instance class, see [Changing a Cluster Instance Class](#).
 - To change the replica set instance class, see [Changing a Replica Set Instance Class](#).
 - To change the single node instance class, see [Changing a Single Node Instance Class](#).
- If a large number of expired files occupy the storage space, delete the expired files in time. For example, if the entire database is no longer used, run **dropDatabase** to delete it.
 - The background data processing mechanism is faulty.

In this case, operations such as write, update, and delete (including index insertion and deletion) are actually converted to write operations in the background. The underlying storage engines (WiredTiger and RocksDB) use appendOnly. Only when the internal data status of the storage engine meets certain conditions, the compaction operation is triggered to compress data and release storage space.

That is why sometimes the disk usage seems greater than the actual data volume, but your services are not affected. The internal data compression operations will not be executed immediately. As data continues to be written, compression is triggered in the background to clear the space.

5.3 What Is the Time Delay for Primary/Secondary Synchronization in a Replica Set?

The delay for primary/secondary synchronization cannot be calculated using a formula. The delay is affected by the following factors:

1. Network communication status
2. Transaction pressure on the primary node, that is, transactions per second (TPS) of the primary node
3. Transaction size executed by the primary node, that is, the duration of a transaction execution
4. Load of the secondary node

If the primary node bears heavy pressure within a period and executes a large number of transactions per second, the synchronization to the secondary node is delayed.

You can view metric "Delay Between Primary and Secondary Nodes" of the secondary node on the Cloud Eye console to know the synchronization delay.

5.4 How Is Data Transferred Between the Primary and Secondary Nodes of a Replica Set?

Data between the primary and secondary nodes is transferred in asynchronous mode.

5.5 How Do I Clear an Alarm Saying the Shard Memory Usage Exceeds 90%?

You can change the value of `enableMajorityReadConcern` to `false` and then restart the node.

5.6 What Can I Do If a Query Error Is Reported After Data Is Written Into the DDS Cluster?

Symptom

Data is continuously written into the DDS cluster. After the data is written into the DDS cluster, an error is reported during query.

Example:

```
W SHARDING [Balancer] Failed to enforce tag ranges :: caused by :: ExceededTimeLimit: Unable to obtain shard utilization information for shard01 due to Operation timed out, request was RemoteCommand xxx --target: 192.168.*.*:8635, db: admin, cmd:{ getShardStatistics: 1, maxTimeMS: 30000 }
```

Possible Cause

Data is continuously written into the storage system, causing chunk splitting timeout in the background.

Solution

This is a normal warning error and does not affect operations. You can try again later.

6 Database Permissions

6.1 What Permissions Does User root Have?

After an instance is created, DDS creates a user **root** in the **admin** database. This user has the built-in root permission of MongoDB. For details about MongoDB built-in roles, see [Built-In Roles](#).

You can log in to the instance and run the following commands to view the permissions of current users:

show users

show roles

7 Creation and Deletion

7.1 How Do I Select Instance Specifications and Nodes?

- Higher specifications can provide better performance. For details about the instance specifications supported by DDS, see [Instance Specifications](#).
- For any given set of instance specifications, more nodes provide better performance. For details about performance, see [Performance White Paper](#).
- Select specifications that can meet your service requirements based on test data and reserve some extra resources for reliability and future service growth.

NOTE

- For a cluster instance with one vCPU, select 16 GB of memory for better performance.
- For replica sets and single node instances, the most popular configurations are listed as recommended for your convenience. For details, see [Buying a Replica Set Instance](#) and [Buying a Single Node Instance](#).

7.2 Why Is an Instance Not Displayed on the Console After It Is Created?

If a DDS instance you created is not displayed on the console, there are a couple of possibilities:

- Insufficient permissions
Your account may not have the required [permissions](#). You can [create a user and grant DDS permissions to the user](#).
- Incorrect region
You can view the created instance only in the region where the instance is located.


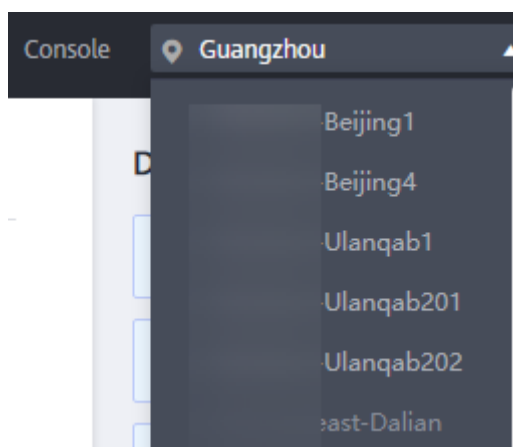
You can click  in the upper left corner of the management console and select the region and project where the instance is located.

Figure 7-1 Selecting a region



7.3 Can I Use a Template to Create DDS DB Instances?

You do not need a template to create DDS DB instances. When you create a DB instance, DDS provides different DB instance specifications which are similar to templates.

7.4 Why Is Data Missing from My Database?

DDS does not delete or perform any operations on any user data. If this problem occurs, check whether a misoperation has been performed. Restore the data using backup files, if necessary.

Solution:

- Restore a DB instance from a backup. For details, see [Backup and Restoration](#).
- Import a backup to a DB instance. For details, see [Data Migration](#).

7.5 Will My Backups Be Deleted If I Delete My Cloud Account?

If your cloud account is deleted, both your automated and manual backups are deleted.

7.6 What Are the Differences Between Instance Deletion and Unsubscription?

The method of releasing resources varies depending on the DB instance billing mode.

- For a DB instance billed in pay-per-use mode, no order is generated after you purchase it. To release resources based on service requirements, manually delete the DB instance on the **Instance Management** page.

- For a yearly/monthly DB instance, an order is generated after you purchase it. You need to unsubscribe from the order to release the DB instance resources. For details, see [Unsubscribing from a Yearly/Monthly DB Instance](#).

8 Database Connection

8.1 What Should I Do If I Fail to Connect to a DDS Instance?

Possible Causes

Locate the fault from the following aspects:

1. **Check whether the DB instance is available.**

For example, if the system is faulty, a DB instance is abnormal, or a DB instance or a table is locked.

2. **(Common) Check whether the client connection is correct.**

- Download the database installation package from the official website. For details, see [How Can I Install a MongoDB Client?](#)
- Use a MongoDB client 4.0 or later to connect to the DB instance.
- If you connect to a DB instance over a private network, ensure that the DB instance and ECS are in the same region and VPC.
- If you connect to a DB instance over a public network, bind an EIP to the DB instance and then connect to the DB instance through the EIP.

3. **Check the connection method.**

Run the following commands to enable and disable SSL on the console:
Example:

- Enable SSL: `./mongo --host<DB_HOST>--port<DB_PORT>-u<DB_USER>-p--authenticationDatabaseadmin--ssl --sslCAFile<FILE_PATH> --sslAllowInvalidHostnames`
- Disable SSL: `./mongo --host<DB_HOST>--port<DB_PORT>-u<DB_USER>-p --authenticationDatabase admin`

4. **Check whether the parameters in the connection command are correct.**

Check whether the following parameters are configured correctly: connection address, port number, username, password, and connection method.

5. **(Common) Check whether the network connectivity is normal.**

Private network connection

- a. Ensure that the ECS and DDS instance are in the same region and VPC.
- b. Check security group rules.
 - i. To access a cluster instance in a different security group from the ECS, [add an inbound rule](#) for the security group.
- c. On the ECS, check whether the DB instance port can be connected.

Public network connection

- a. Check security group rules.
 - i. To access a cluster instance in a different security group from the ECS, [add an inbound rule](#) for the security group.
- b. Check network ACL rules.
- c. Ping the ECS to the DB instance in the same region.

Cross-CIDR block access (configuring IP address mapping)

If a client and a replica set instance are deployed in different CIDR blocks and the client is not in 192.168.0.0/16, 172.16.0.0/24, or 10.0.0.0/8, configure Cross-CIDR Access for the instance to communicate with the client.

- a. Ensure that the source ECS can communicate with the instance node. If the network is abnormal, configure the network settings.
- b. For details about how to configure cross-CIDR block access, see [Configuring Cross-CIDR Access](#).

6. [\(Common\) Check whether the number of connections to the DB instance reaches the upper limit.](#)

If there is an excessive number of database connections, applications may fail to be connected.

7. [\(Common\) Check whether the disk is full.](#)

If the instance disk usage is too high, the instance status is abnormal and the instance cannot be connected.

8. [Check whether the CPU usage is too high.](#)

The CPU usage is high or close to 100%. As a result, data read/write processing is slow, connections cannot be obtained, and errors are reported, affecting service running.

9. [View the common connection error messages](#)

Find corresponding solutions based on connection error messages.

Fault Locating

1. [Check whether the DB instance is available.](#)

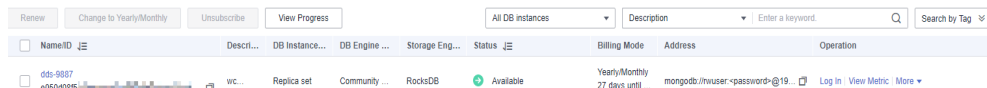
Check method: Check whether the database instance status is **Available** on the console.

Possible cause: The DDS system is faulty, the instance status is abnormal, or the instance or table is locked.

Solution

- If the DDS instance status is abnormal, contact O&M personnel.
- If the system is faulty or the instance or table is locked, restart the instance. For details, see [Restarting an Instance](#).

Figure 8-1 Checking the instance status



2. **Check whether the client connection is correct.**

You are advised to use a MongoDB client of version 4.0 or later to connect to the instance. For details about how to install a MongoDB client, see [How Can I Install a MongoDB Client?](#)

The following uses connecting to a cluster as an example:

- a. For details about how to connect to a DB instance over a private network, see [Connecting to a DB Instance Over Private Networks](#).
- b. For details about how to connect to a DB instance over a public network, see [Connecting to a DB Instance Over Public Networks](#).

Table 8-1 Connection methods

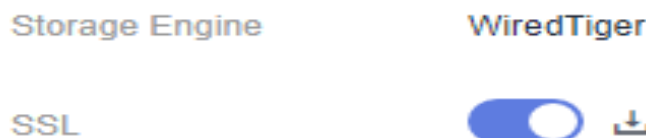
Method	Scenario
Private network	DDS provides a private IP address by default. If your applications are deployed on an ECS that is in the same region and VPC as the DB instance, you are advised to connect to the ECS and DB instance through a private IP address.
Public network	If you cannot access the DB instance over a private IP address, you are advised to bind an EIP to the DB instance and then connect to the DB instance through the EIP. For EIP pricing details, see EIP billing details .

3. **Check the connection method.**

- a. SSL connection is recommended. Enable SSL on the **Connections** page and upload the certificate to the ECS.

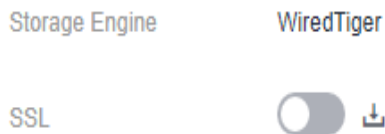
```
./mongo --host<DB_HOST>--port<DB_PORT>-u<DB_USER>-p--authenticationDatabaseadmin--ssl --sslCAFile<FILE_PATH> --sslAllowInvalidHostnames
```

Figure 8-2 Enabling SSL



- b. Unencrypted connection: Disable SSL on the **Connections** page.

```
./mongo --host<DB_HOST>--port<DB_PORT>-u<DB_USER>-p --authenticationDatabase admin
```

Figure 8-3 Disabling SSL

4. **Check whether the parameters in the connection command are correct.**

Ensure that the connection address, port, username and password are correct, and try to connect to the DB instance again in SSL mode.

SSL private network connection example:
`./mongo mongod --rwuser:<password>@<DB_HOST>:<DB_PORT>,<DB_HOST>:<DB_PORT>/test?authSource=admin --ssl --sslCAFile <FILE_PATH> --sslAllowInvalidHostnames`

– Connection address

The connection information can be obtained in the **Address** column on the **Instances** page.

– Database port

On the **Private Connection** tab of the **Connections** page, obtain the database port in the **Database Port** field.

– Username and password

If the password of the root administrator is incorrect or you forget the password, [reset the administrator password](#).

– Certificate

Obtain the SSL certificate name from the directory where the command is executed.

SSL public network connection example:
`./mongo mongod --rwuser:<password>@<DB_HOST>:<DB_PORT>/test?authSource=admin --ssl --sslCAFile <FILE_PATH> --sslAllowInvalidHostnames`

– Connection address

Click the instance name. On the **Public Connection** tab of the **Connections** page, obtain the public connection address in the **Public Network Connection Address** field.

– Database port

On the **Public Connection** tab of the **Connections** page, obtain the database port in the **Database Port** field.

– Username and password

If the password of the root administrator is incorrect or you forget the password, [reset the administrator password](#).

– Certificate

Obtain the SSL certificate name from the directory where the command is executed.

5. **Check whether the network connection is normal.**

Private network connection

- a. Check whether the ECS and DDS instance are in the same region and VPC.

- If the ECS and DB instance are in different regions, they cannot communicate with each other. Select a region near to your service area to reduce network latency and experience faster access.
- b. Check security group rules.
To access DB instances in a different security group from the ECS, [add an inbound rule](#) for the security group.
- c. On the ECS, check whether the DB instance port can be connected.

```
telnet <DB instance address> {8635}
```

 - If the connection is normal, the network is normal.
 - If the connection fails, submit a to customer service for assistance.

Public network connection

- a. Check security group rules.
To access DB instances in a different security group from the ECS, [add an inbound rule](#) for the security group.
- b. Check network ACL rules.
 - i. Go to the .
 - ii. Check whether the NIC bound to the EIP is in the subnet associated with the network ACL.
 - iii. Check whether the network ACL is enabled.
The default network ACL rule denies all inbound and outbound packets. After the network ACL is disabled, the default rule still takes effect.
- c. Ping the ECS to the DB instance in the same region.
If you cannot ping the EIP on the original ECS, select another ECS in the same region and ping the EIP again. If the ping is successful, the network is normal. If the ping failed, .

Cross-CIDR block access (configuring IP address mapping)

If a client and a replica set instance are deployed in different CIDR blocks and the client is not in 192.168.0.0/16, 172.16.0.0/24, or 10.0.0.0/8, configure Cross-CIDR Access for the instance to communicate with the client.

- a. Ensure that the source ECS can communicate with the instance node. If the network is abnormal, configure the network settings.
- b. For details about how to configure cross-CIDR block access, see [Configuring Cross-CIDR Access](#).

6. Check whether the number of connections to the DB instance reaches the upper limit.

- a. Check whether the number of connections to the DB instance has reached the upper limit. For details, see [How Do I Query and Limit the Number of Connections?](#)
If the number of instance connections reaches the upper limit, see [What Can I Do If the Number of Connections of an Instance Reaches Its Maximum?](#)
- b. Check whether any metrics are abnormal and whether any alarms are generated on the Cloud Eye console. Cloud Eye monitors database metrics, such as the CPU usage, memory usage, storage space usage, and

database connections, and allows you to set alarm policies to identify risks in advance if any alarms are generated.

7. **Check whether the disk is full.**

Check method: View the storage space usage on the management console or Cloud Eye.

- On the management console
 Locate the target instance and click its name to go to the **Basic Information** page. In the **Storage Space** area, view the storage space usage.
- On Cloud Eye
 Locate the target instance and click **View Metric** in the **Operation** column. On the displayed page, view the storage space usage.

Possible cause: When the instance status is **Storage full**, the instance needs to preserve at least 15% of its capacity to work properly.

Solution:

- As your service data grows, the original storage space may be insufficient. You are advised to scale up storage space. For details, see [Scaling Up Storage Space](#).
- Process expired data files in a timely manner.
- Check whether any metrics are abnormal and whether any alarms are generated on the Cloud Eye console. Cloud Eye monitors database metrics, such as the CPU usage, memory usage, storage space usage, and database connections, and allows you to set alarm policies to identify risks in advance if any alarms are generated.

8. **Check whether the CPU usage is too high.**

The CPU usage is high or close to 100%. As a result, data read/write processing is slow, connections cannot be obtained, and errors are reported, affecting service running.

Solution: For details, see [What Should I Do If CPU Usage Is Unusually High?](#)

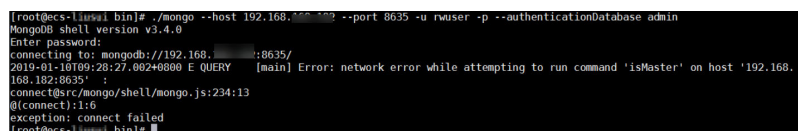
9. **View common connection error messages.**

- Connection failure message: **network error while attempting to run command 'isMaster'**

An error is reported when you run the following command to connect to a DDS DB instance:

```
./mongo --host 192.168.168.182 --port 8635 -u rwuser -p XXXXXXXXXXXX --authenticationDatabase admin
```

Figure 8-4 Connection failed



For details about how to rectify the fault, see [Connection Failure Message: network error while attempting to run command 'isMaster'](#).

- Connection failure messages: **No route to host** and **connection attempt failed**.

An error is reported when you run the following command to connect to a DDS DB instance:

```
mongo --host 192.168.1.6 --port 8635 -u rwuser -p xxxxxxxx --  
authenticationDatabase admin --ssl --sslCAFile /root/ca.crt --  
sslAllowInvalidHostnames
```

Error message:

```
MongoDB shell version v3.4.17  
connecting to: mongod://192.168.1.6:8635/  
2019-09-19T09:38:36.954+0800 W NETWORK [thread1] Failed to connect to 192.168.1.6:8635,  
in(checking socket for error after poll), reason: No route to host  
2019-09-19T09:38:36.954+0800 E QUERY [thread1] Error: couldn't connect to server  
192.168.1.6:8635, connection attempt failed :  
connect@src/mongo/shell/mongo.js:240:13  
@(connect):1:6  
exception: connect failed
```

For details about how to rectify the fault, see [Connection Failure Messages: "No route to host" and "connection attempt failed"](#).

- Connection failure messages: **No route to host** and **connection attempt failed**

An error is reported when you run the following command to connect to a DDS DB instance:

```
mongo --host 192.168.168.116 --port 8635 -u rwuser -p xxxxxxxx --  
authenticationDatabase admin --ssl --sslCAFile /root/ca.crt --  
sslAllowInvalidHostnames
```

Error message:

```
MongoDB shell version v3.4.17  
connecting to: mongod://192.168.168.116:8635/  
2019-09-19T09:39:24.306+0800 W NETWORK [thread1] The server certificate does not match  
the host name. Hostname: 192.168.168.116 does not match CN: 172.16.2.65  
MongoDB server version: 4.0.3  
WARNING: shell and server versions do not match  
2019-09-19T09:39:24.329+0800 E QUERY [thread1] Error: Authentication failed. :  
DB.prototype._authOrThrow@src/mongo/shell/db.js:1461:20  
@(auth):6:1  
@(auth):1:2  
exception: login failed
```

For details about how to rectify the fault, see [Connection Failure Messages: "No route to host" and "connection attempt failed"](#).

- Connection failure message: **couldn't connect to server**.

An error is reported when you run the following command to connect to a DDS DB instance:

```
mongo --host 192.168.64.201 --port 8635 -u rwuser -p xxxxxxxx --  
authenticationDatabase admin --ssl --sslCAFile /root/ca.crt --  
sslAllowInvalidHostnames
```

Error message:

```
MongoDB shell version v3.4.17  
connecting to: mongod://192.168.64.201:8635/  
2019-09-19T09:45:48.168+0800 W NETWORK [thread1] Failed to connect to  
192.168.64.201:8635 after 5000ms milliseconds, giving up.  
2019-09-19T09:45:48.168+0800 E QUERY [thread1] Error: couldn't connect to server  
192.168.64.201:8635, connection attempt failed :  
connect@src/mongo/shell/mongo.js:240:13  
@(connect):1:6  
exception: connect failed
```

For details about how to rectify the fault, see [Connection Failure Message: "couldn't connect to server"](#).

- Connection failure message: **cannot list multiple servers in URL without 'replicaSet' option**

An error is reported when you run the following command to connect to a DDS replica set instance:

```
./mongo mongodb://  
rwuser:xxxxxxxxxx@192.168.168.116:8635,192.168.200.147:8635/test?  
authSource=admin&replicaSet=replica
```

Error message:

```
FailedToParse: Cannot list multiple servers in URL without 'replicaSet' option try 'mongo --help'  
for more information.
```

An error is reported when you run the following command to connect to a DDS DB instance that is compatible with MongoDB 3.4:

```
mongo "mongodb://  
rwuser:xxxxxxxxxx@192.168.95.167:8635,192.168.92.43:8635/test?  
authSource=admin"
```

Error message:

```
FailedToParse: Cannot list multiple servers in URL without 'replicaSet' option  
try 'mongo --help' for more information.
```

For details, see [Connection Failure Message: cannot list multiple servers in URL without 'replicaSet' option](#).

- Connection failure message: **Timeout while receiving message.**

An error is reported when you run the following command to connect to a DDS DB instance through Java driver:

Error message:

```
org.springframework.data.mongodb.UncategorizedMongoDbException: Timeout while receiving  
message; nested exception is com.mongodb.MongoSocketReadTimeoutException: Timeout while  
receiving message
```

For details about how to rectify the fault, see [Connection Failure Message: "Timeout while receiving message"](#).

- Connection failure messages: **exception: login failed and U_STRINGPREP_PROHIBITED_ERROR**

An error is reported when you run the following command to connect to a DDS DB instance:

```
./mongo "mongodb://  
rwuser:xxxxxx@192.168.0.45:8635,192.168.0.96:8635/test?  
authSource=admin&replicaSet=replica"
```

Error message:

```
MongoDB shell version v4.0.3  
connecting to: mongodb://192.168.0.45:8635,192.168.0.96:8635/test?  
authSource=admin&replicaSet=replica  
2021-11-05T05:52:53.717+0000 I NETWORK [js] Starting new replica set monitor for replica/  
192.168.0.45:8635,192.168.0.96:8635  
2021-11-05T05:52:53.718+0000 I NETWORK [ReplicaSetMonitor-TaskExecutor] Successfully  
connected to 192.168.0.45:8635 (1 connections now open to 192.168.0.45:8635 with a 5 second  
timeout)  
2021-11-05T05:52:53.718+0000 I NETWORK [js] Successfully connected to 192.168.0.96:8635 (1  
connections now open to 192.168.0.96:8635 with a 5 second timeout)  
Implicit session: session { "id" : UUID("5945d2a5-8275-4e3c-b06f-632f062a2ead") }  
MongoDB server version: 4.0.3  
2021-11-05T05:52:53.722+0000 I NETWORK [js] Marking host 192.168.0.96:8635 as failed ::  
caused by :: Location50692: can't authenticate against replica set node 192.168.0.96:8635 ::  
caused by :: Error preflighting normalization: U_STRINGPREP_PROHIBITED_ERROR  
2021-11-05T05:52:53.722+0000 I NETWORK [js] Successfully connected to 192.168.0.45:8635 (1
```

```
connections now open to 192.168.0.45:8635 with a 0 second timeout)
2021-11-05T05:52:53.723+0000 I NETWORK [js] Marking host 192.168.0.45:8635 ::
caused by :: Location50692: can't authenticate against replica set node 192.168.0.45:8635 ::
caused by :: Error preflighting normalization: U_STRINGPREP_PROHIBITED_ERROR
2021-11-05T05:52:53.724+0000 I NETWORK [js] Marking host 192.168.0.96:8635 as failed ::
caused by :: Location50692: can't authenticate against replica set node 192.168.0.96:8635 ::
caused by :: Error preflighting normalization: U_STRINGPREP_PROHIBITED_ERROR
2021-11-05T05:52:53.725+0000 I NETWORK [js] Marking host 192.168.0.45:8635 as failed ::
caused by :: Location50692: can't authenticate against replica set node 192.168.0.45:8635 ::
caused by :: Error preflighting normalization: U_STRINGPREP_PROHIBITED_ERROR
2021-11-05T05:52:53.725+0000 E QUERY [js] Error: can't authenticate against replica set node
192.168.0.45:8635 :: caused by :: Error preflighting normalization:
U_STRINGPREP_PROHIBITED_ERROR :
DB.prototype._authOrThrow@src/mongo/shell/db.js:1685:20
@(auth):6:1
@(auth):1:2
exception: login failed
```

For details about how to rectify the fault, see [Connection Failure Messages: exception: login failed and U_STRINGPREP_PROHIBITED_ERROR](#).

10. If the problem persists, to contact Huawei Cloud customer service for assistance.

8.2 What Can I Do If the Number of Connections of an Instance Reaches Its Maximum?

The number of connections indicates the number of applications that can be simultaneously connected to the database. The number of connections is irrelevant to the maximum number of users allowed by your applications or websites.

- For a cluster instance, the number of connections is the number of connections between the client and the mongos.
- For a replica set instance, the number of connections is the number of connections between the client and the primary and secondary nodes.
- For a single-node instance, the number of connections is the number of connections between the client and the node.

When the number of connections to a DDS instance reaches the maximum supported, new connection requests cannot be responded to, and the connection attempt fails.

Symptom

Some common errors:

- If the following information is displayed when you use Mongo Shell to connect to an instance, no more connections can be established.

Figure 8-5 Message displayed

```
[root@623- ~]# mongo "mongodb://rwuser:192.168.0.180:8635,192.168.0.50:8635/test?authSource=admin&replicaSet=replica"
MongoDB shell version v3.4.17
connecting to: mongodb://rwuser:623_Huawei@192.168.0.180:8635,192.168.0.50:8635/test?authSource=admin&replicaSet=replica
2019-10-16T17:43:45.203+0800 I NETWORK [thread1] Starting new replica set monitor for replica/192.168.0.180:8635,192.168.0.50:8635
2019-10-16T17:43:45.205+0800 W NETWORK [ReplicaSetMonitor-TaskExecutor-0] No primary detected for set replica
2019-10-16T17:43:45.205+0800 I NETWORK [ReplicaSetMonitor-TaskExecutor-0] All nodes for set replica are down. This has happened for 1 check
s in a row.
2019-10-16T17:43:45.708+0800 W NETWORK [thread1] No primary detected for set replica
2019-10-16T17:43:45.708+0800 I NETWORK [thread1] All nodes for set replica are down. This has happened for 2 checks in a row.
2019-10-16T17:43:46.210+0800 I NETWORK [thread1] No primary detected for set replica
2019-10-16T17:43:46.210+0800 I NETWORK [thread1] All nodes for set replica are down. This has happened for 3 checks in a row.
2019-10-16T17:43:46.712+0800 W NETWORK [thread1] No primary detected for set replica
2019-10-16T17:43:46.712+0800 I NETWORK [thread1] All nodes for set replica are down. This has happened for 4 checks in a row.
2019-10-16T17:43:47.215+0800 W NETWORK [thread1] No primary detected for set replica
2019-10-16T17:43:47.215+0800 I NETWORK [thread1] All nodes for set replica are down. This has happened for 5 checks in a row.
2019-10-16T17:43:47.717+0800 W NETWORK [thread1] No primary detected for set replica
2019-10-16T17:43:47.717+0800 I NETWORK [thread1] All nodes for set replica are down. This has happened for 6 checks in a row.
2019-10-16T17:43:48.218+0800 W NETWORK [thread1] No primary detected for set replica
2019-10-16T17:43:48.218+0800 I NETWORK [thread1] All nodes for set replica are down. This has happened for 7 checks in a row.
2019-10-16T17:43:48.721+0800 W NETWORK [thread1] No primary detected for set replica
2019-10-16T17:43:48.721+0800 I NETWORK [thread1] All nodes for set replica are down. This has happened for 8 checks in a row.
2019-10-16T17:43:49.222+0800 W NETWORK [thread1] No primary detected for set replica
2019-10-16T17:43:49.222+0800 I NETWORK [thread1] All nodes for set replica are down. This has happened for 9 checks in a row.
2019-10-16T17:43:49.724+0800 W NETWORK [thread1] No primary detected for set replica
2019-10-16T17:43:49.724+0800 I NETWORK [thread1] All nodes for set replica are down. This has happened for 10 checks in a row.
2019-10-16T17:43:50.226+0800 W NETWORK [thread1] No primary detected for set replica
2019-10-16T17:43:50.226+0800 I NETWORK [thread1] All nodes for set replica are down. This has happened for 11 checks in a row.
2019-10-16T17:43:50.727+0800 W NETWORK [thread1] No primary detected for set replica
2019-10-16T17:43:51.230+0800 W NETWORK [thread1] No primary detected for set replica
2019-10-16T17:43:51.731+0800 W NETWORK [thread1] No primary detected for set replica
```

- If the following information is displayed when you use Python to connect to an instance, the number of connections reaches its maximum.
`pymongo.errors.ServerSelectionTimeoutError: connection closed, connection closed`

Handling Method

1. Check what applications are connected, optimize the connections, and release any that are not necessary.
2. Check the value of the **net.maxIncomingConnections** parameter and the instance specifications. Change the parameter value or the database specifications.
3. Check for abnormal metrics and alarms on the Cloud Eye console. Cloud Eye monitors database metrics, such as the CPU usage, memory usage, storage space usage, and database connections, and allows you to set alarm policies to identify risks in advance if any alarms are generated. For details, see the *Cloud Eye User Guide*.

Solution

1. Release unnecessary connections.
 - a. You can restart the instance to release all of the connections. For details, see [Restarting an Instance or a Node](#).
 - b. You can query the current number of connections on a node and the connection source, analyze the number of connections established between each client and the instance, and adjust the number of connections. For details, see [How Do I Query and Limit the Number of Connections?](#)
2. Change parameter values or database specifications.

You can change the maximum number of connections of a DB instance by modifying the **net.maxIncomingConnections** parameter. Then, restart the DB instance for the modification to take effect. For details about how to change parameter values, see [Editing a Parameter Template](#).

 - If the value is **default**, the maximum number of connections is the default value and is related to the instance specifications. For details, see [Instance Specifications](#).

- If there are too many connections, the service may break down. In this case, you can increase the number of connections by changing the instance specifications. For details, see [Changing a Cluster Instance Class](#).

NOTE

If a default parameter template is used, you cannot change its settings. You can create a parameter template and change the corresponding parameter values. After the change, associate the new parameter template with the instance.

3. Check whether there are . You can add indexes to improve queries.

8.3 How Do I Query and Limit the Number of Connections?

The following uses a replica set instance as an example to describe how to query the connection status and set the number of connections in the connection pool.

Querying the Number of Connections

The maximum number of connections varies according to the instance specifications.

NOTE

The maximum number of connections refers to the maximum number of connections of each node in an instance.

Example: If a replica set instance has two vCPUs and 4 GB memory for each node, the maximum number of connections of the primary and secondary nodes is 1000 respectively. The hidden node does not provide services because of its architecture features.

Use Mongo Shell to connect to the primary node, and run the **db.serverStatus().connections** command to query the number of connections on the node.

```
replica:PRIMARY> db.serverStatus().connections
{ "current" : 7, "available" : 398, "totalCreated" : 818364 }
```

Pay attention to the following parameters and their values:

- **current**: Existing connections
- **available**: Number of available connections.

Querying the Source of Connections

Step 1 Use Mongo Shell to connect to the primary node and switch to the **admin** database.

```
replica:PRIMARY> use admin
```

Step 2 Run the **db.runCommand({currentOp: 1, \$all: true})** command to query the connection source.

By analyzing the command output, you can query the source IP address of each connection. In this way, the number of connections between each client and DDS DB instance is obtained.

Figure 8-6 Command output

```

replica:PRIMARY> db.runCommand({currentOp: 1, $all: true})
{
  "inprog" : [
    {
      "desc" : "conn828171",
      "threadId" : "139911043778304",
      "connectionId" : 828171,
      "client" : "192.168.1.116:58096",
      "appName" : "MongoDB Shell",
      "clientMetadata" : {
        "application" : {
          "name" : "MongoDB Shell"
        },
        "driver" : {
          "name" : "MongoDB Internal Client",
          "version" : "3.4.17"
        },
        "os" : {
          "type" : "Linux",
          "name" : "CentOS Linux release 7.4.1708 (Core) ",
          "architecture" : "x86_64",
          "version" : "Kernel 3.10.0-693.11.1.el7.x86_64"
        }
      },
      "active" : true,
      "opid" : 3719193,
      "secs_running" : 0,
      "microsecs_running" : NumberLong(30),
      "op" : "command",
      "ns" : "admin.$cmd",
      "query" : {
        "currentOp" : 1,
        "$all" : true
      },
      "numYields" : 0,
      "locks" : {
      },
      "waitingForLock" : false,
      "lockStats" : {
      }
    }
  ]
}
    
```

----End

Limiting the Number of Connections

DDS allows you to log in to the database using Connection String URI. When logging in to the database using Connection String URI, you can add **&maxPoolSize=<integer>** to the end of the URI to set the number of connections in the connection pool.

Example: When Mongo Shell is used to connect replica set instances, run the following command to set the number of connections in the connection pool to 10:

```

mongo "mongodb://
rwuser:xxxxxxxxxx@192.168.168.116:8635,192.168.200.147:8635/test?
authSource=admin&replicaSet=replica&maxPoolSize=10"
    
```

Figure 8-7 Limiting the number of connections

```

root@serverced4ea23-8d5f-49e6-8a8c-94259dcf89cb ycsbj# mongo "mongodb://rwuser:xxxxxxxxxx@192.168.168.116:8635,192.168.200.147:8635/test?authSource=admin&replicaSet=replica&maxPoolSize=10"
MongoDB shell version v3.4.17
connecting to: mongodb://rwuser:xxxxxxxxxx@192.168.168.116:8635,192.168.200.147:8635/test?authSource=admin&replicaSet=replica&maxPoolSize=10
2019-09-19T11:13:25.634+0800 I NETWORK [thread1] Starting new replica set monitor for replica/192.168.168.116:8635
2019-09-19T11:13:25.654+0800 I NETWORK [thread1] Successfully connected to 192.168.85.63:8635 (1 connections now open to 192.168.168.116:8635 with a 5 second timeout)
2019-09-19T11:13:25.655+0800 I NETWORK [ReplicaSetMonitor-TaskExecutor-0] Successfully connected to 192.168.96.198:8635 (1 connections now open to 192.168.168.116:8635 with a 5 second timeout)
MongoDB server version: 3.4.14
replica:PRIMARY>
    
```

 NOTE

For details about how to limit the number of connection pools on [clients in different languages](#), see the API documents of clients in different languages on the MongoDB official website.

8.4 What Should I Do If the ECS and DDS Are Deployed in Different VPCs and They Cannot Communicate with Each Other?

- Change the VPC hosting the ECS to the same as that hosting the DDS by referring to "Changing a VPC".
- Create a VPC peering connection. For details, see "VPC Peering Connection Overview".

8.5 Do Applications Need to Support Automatic Reconnecting to the DDS Database?

It is recommended that your applications support automatic reconnections to the database. After a database reboot, your applications will automatically reconnect to the database to increase service availability and continuity.

In addition, you are advised to set your applications to connect to the database using a long connection to reduce resource consumption and improve performance.

8.6 How Do I Create and Log In to an ECS?

- The ECS to be created must be in the same VPC with the DDS DB instance to which it connects.
- When you create an ECS, select an OS, such as Red Hat 6.6, and bind an EIP to it.
- Configure the security group to enable the ECS to access the DB instance through the private IP address, that is, the node address in the **Private IP Address** column on the **Basic Information** page.

9 Installing a Client

9.1 How Can I Install a MongoDB Client?

MongoDB official website provides client installation packages for different OSs. Download the official package at <https://www.mongodb.com/download-center#community>.

NOTICE

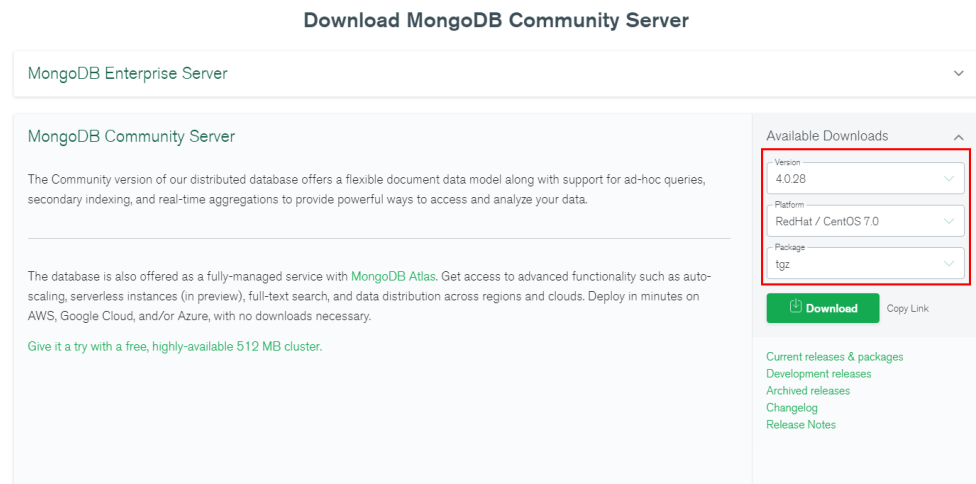
The following uses RedHat/CentOS 7.0 and MongoDB 4.0.28 as examples to describe how to obtain the required installation package and install the MongoDB client.

During the installation, select the client version that matches the instance version.

Procedure

- Step 1** Obtain the installation package.
1. Visit the [MongoDB official website](#).
 2. Select version **4.0.28**, platform **RedHat/CentOS 7.0**, and package **tgz**. [Figure 9-1](#) shows an example.

Figure 9-1 MongoDB official webpage



- Use either of the following methods to upload the installation package to the ECS:

NOTE

For details about how to log in to an ECS, see [How Can I Create and Log In to an ECS?](#)

- Click **Download** to obtain the binary installation package of version 4.0.28. The name of the installation package is **mongodb-linux-x86_64-rhel70-4.0.28.tgz**. Upload the installation package to the ECS.
- Click **Copy Link** to obtain the download address. Log in to the ECS and run the **wget copylink** command.

NOTE

Replace *copylink* with the actual download address.

Step 2 Decompress the installation package on the ECS.

```
tar zxvf mongodb-linux-x86_64-rhel70-4.0.28.tgz
```

Step 3 Access the directory where the installation package is located.

```
cd mongodb-linux-x86_64-rhel70-4.0.28/bin
```

The common tools are as follows:

- MongoDB client **mongo**
- Data export tool **mongoexport**
- Data import tool **mongoimport**

Step 4 Make the packages executable.

- Run the **chmod +x mongo** command to grant a client permission to connect to an instance.
- Run the **chmod +x mongoexport** command to grant a client permission to export data.
- Run the **chmod +x mongoimport** command to grant a client permission to import data.

Step 5 Connect to an instance from the client. For details, see "Connecting to an Instance" in *Getting Started with Document Database Service*.

----End

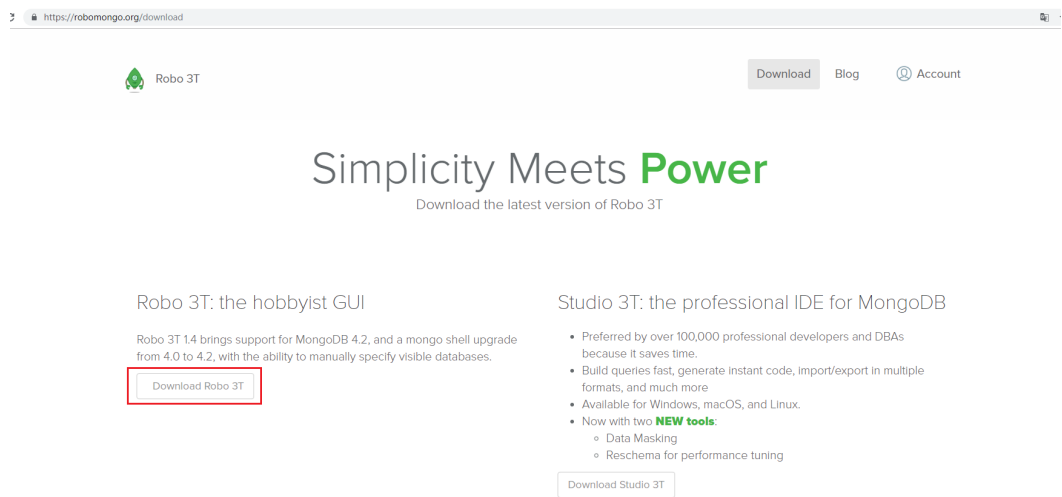
9.2 How Do I Install Robo 3T?

This section describes how to obtain the Robo 3T installation package and install Robo 3T.

Procedure

Step 1 Access the Robo 3T download address <https://robomongo.org/download> and click **Download Robo 3T**.

Figure 9-2 Downloading page



Step 2 In the displayed dialog box, enter the required information and click **Download for Windows** to download the **robo3t-1.4.4-windows-x86_64-e6ac9ec5.zip** package.

Figure 9-3 Downloading Robo 3T

Windows Mac Linux

Robo 3T 1.4.4

Download for Windows

Email*

First name* Last name*

Country code Phone number

Please select ▼

By clicking on the download button, I agree to the 3T Software Labs [Privacy Policy](#).

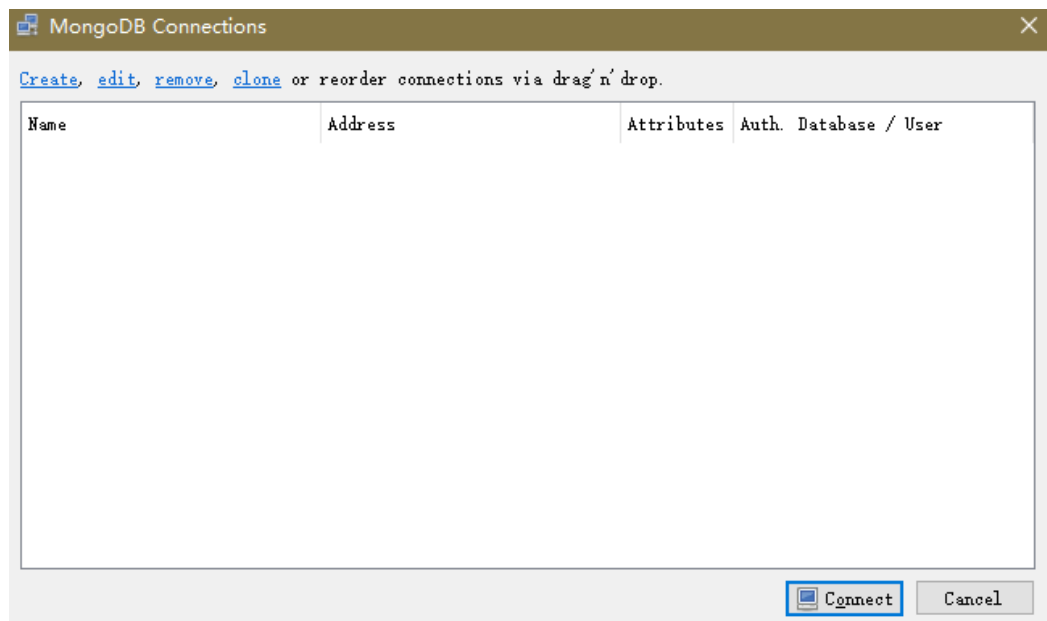
Download for Windows

Close

Step 3 Decompress the downloaded package obtained in [Step 2](#) and double-click the **robo3t.exe** file in the decompressed directory to start the installation.

Step 4 After the installation is complete, start the tool.

Figure 9-4 Main window



- Step 5** Connect to an instance using the tool over a public network. For details, see "Connecting to an Instance" in *Getting Started with Document Database Service*
- End

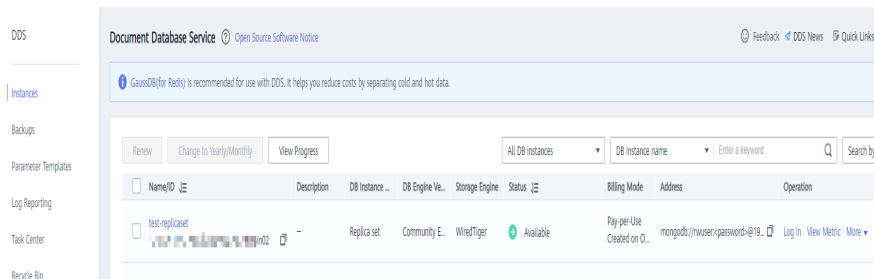
10 Database Usage

10.1 How Do I View the Primary/Standby Nodes of a Replica Set Instance?

You can view node information for the current instance on the DDS console.

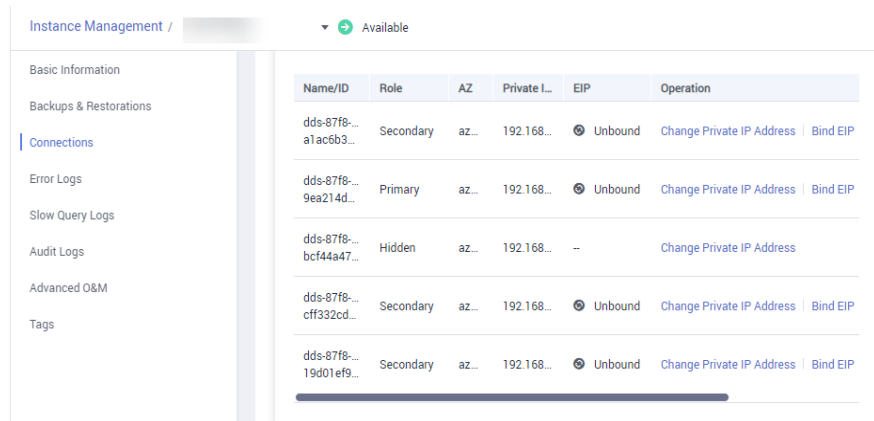
1. Logging In to the DDS Console
2. On the **Instances** page, click the instance name.

Figure 10-1 Instances



3. In the navigation pane on the left, choose **Connections**. The node information is displayed in the right area.

Figure 10-2 Connections



10.2 Can I Delete an Index That Fails to Be Created in DDS?

Run the `db.cooperatorManager_module.stats()` statement to query the indexes that fail to be created in the database and then delete them.

10.3 Does DDS Delete Expired Data Using TTL Indexes?

You can delete expired data using time-to-live (TTL) indexes. For details, see the [official guide](#).

10.4 How Do I Use MapReduce Commands?

Overview

MapReduce commands are used for executing map-reduce operations on big data.

How Do I Enable MapReduce Commands?

The MapReduce command is controlled by the DDS parameter `security.javascriptEnabled`. The default value is `false`, indicating that the `mapReduce` and `group` commands are unavailable. If you need to use the MapReduce command, change the parameter value to `true`. Then, restart the DB instance for the change to take effect.

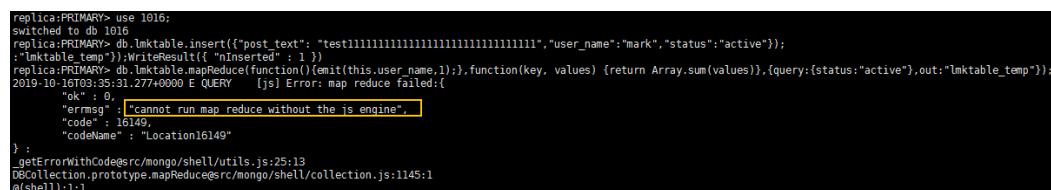
- For a cluster instance, change the parameter values in the parameter template associated with all shard nodes and restart the instance for the change to take effect.
- For a replica set or single-node instance, change the parameter values in the parameter template associated with the instance and restart the instance for the change to take effect.

For details about how to change parameter values, see [Editing a Parameter Template](#).

Common Errors and Handling Methods for MapReduce Command Execution Failures

Error information: cannot run map reduce without the js engine or map is not defined

Figure 10-3 Case 1



```
replica:PRIMARY> use test;
switched to db test
replica:PRIMARY> db.test.insert({"post_text": "testllllllllllllllllllllllllllllllll", "user_name": "mark", "status": "active"});
{"_id": "1", "nInserted": 1}
replica:PRIMARY> db.test.mapReduce(function()emit(this.user_name,1);),function(key, values) {return Array.sum(values)}; {query:{status:"active"},out:"test"});
2019-10-16T03:35:31.277+0000 E QUERY [js] Error: map reduce failed:{"
  "ok" : 0,
  "errmsg" : "cannot run map reduce without the js engine",
  "code" : 13149,
  "codeName" : "Location16149"
} ;
_getErrorWithCode@src/mongo/shell/utils.js:25:13
DBCollection.prototype.mapReduce@src/mongo/shell/collection.js:1145:1
@shell:1:1
```

Figure 10-4 Case 2

```
replica:PRIMARY> db.mythings.find( { age: {$lt: 25} } )
replica:PRIMARY> db.runCommand(
... {
...  mapreduce: 'mythings'
...  ,map: map
...  ,reduce: reduce
...  ,out: 'a'
...  ,keeptemp: false
... }
... )
2019-10-16T03:38:30.420+0000 E QUERY [js] ReferenceError: map is not defined :
@(shell):4:2
```

Possible cause: MapReduce commands are restricted and cannot be used.

Solution: Change the value of **security.javascriptEnabled** in the instance parameter template to **true** and restart the instance for the change to take effect.

NOTE

If a parameter template is a default parameter template, you are not allowed to change its parameter values. You can create a parameter template and change the corresponding parameter values. After the change, associate the new parameter template with the instance. For details, see [Changing the Associated Parameter Template](#).

10.5 Does DDS Support the \$round Function?

DDS supports the \$round function. For details, see [Compatible Aggregate Functions](#).

10.6 How Do I Manage Balancers?

DDS supports balancer management. In some special scenarios, you can enable or disable the balancer and configure the active window.

For details, see the [official document](#).

11 Database Migration

11.1 Does DDS Support Cross-Region Migration?

You can use the Data Replication Service (DRS) to migrate databases across regions on the cloud.

For details, see "Migrating Data Using DRS".

11.2 How Do I Migrate DDS Databases Between Different Accounts?

If you want to migrate DDS instance A of account A to DDS-instance B of account B, you can use DRS to replicate data from instance A to instance B. For details, see "Does DRS Support Cross-Account Cloud Database Migration?"

12 Database Storage

12.1 How Does DDS Store Data?

EVS is used to store DDS instance data. For details about EVS, see *Elastic Volume Service User Guide*.

DDS instance backup data is stored in OBS and does not count towards your DDS storage quota. For details on the DDS instance storage configuration, see the *Object Storage Service User Guide*.

12.2 What Should I Do If My Data Exceeds the Database Storage Space of a DDS Instance?

For details about the files that occupy the storage space, see [Which Items Occupy the Storage Space of DDS Instances?](#)

If the storage required by your applications exceeds the maximum allocated capacity, you can [scale up the storage](#).

For a cluster instance, you can also add shard nodes to increase storage. For details, see [Adding Nodes](#).

12.3 Why Does a DDS DB Instance Become Read-only?

To ensure that a DB instance can still be used if the storage space is about to be used up, databases running on the instance are set to read-only, and data cannot be modified. If this happens, you can [add more storage](#) to restore the database to read/write status.

Detailed rules are as follows:

- If the storage space you purchased exceeds 600 GB and the remaining storage space is 18 GB, the DB instance becomes **Read-only**.
- If the storage space you purchased is less than 600 GB and the storage space usage reaches 97%, the DB instance becomes **Read-only**.

- If the storage space you purchased exceeds 600 GB and the remaining available storage space is greater than 90 GB, the read-only state is automatically canceled.
- If the storage space you purchased is less than or equal to 600 GB and the used storage space is less than 85% of the total storage space, the read-only state is automatically canceled.

You are advised to remove unnecessary resources or expand the storage space.

13 Database Parameters

13.1 Can I Change the Time Zone of a DDS Instance?

The server time is in UTC format and cannot be changed. You are advised to control the data insertion time on the application.

13.2 What DB Instance Monitoring Metrics Do I Need to Pay Attention To?

Related parameters are described as follows:

- For details on parameter descriptions, visit [MongoDB official website](#).
- The default value of the **net.maxIncomingConnections** parameter varies according to DB instance specifications. Therefore, this parameter is set to **default** before being specified.
- **disableJavaScriptJIT** and **security.javascriptEnabled** are used together to set the statistical function.
 - **disableJavaScriptJIT**: The default value is **true**, indicating that the JavaScriptJIT compiler is disabled.
 - **security.javascriptEnabled**: The default value is **false**, indicating that JavaScript cannot be executed on mongod and the mapReduce and group commands cannot be used.

13.3 How Do I Enable JavaScript?

For security purposes, DDS restricts the execution of JavaScript code. If you need to execute JavaScript, you can change the value of **security.javascriptEnabled** to **true** on the DDS console. For details, see [Editing a Parameter Template](#).

13.4 Does DDS Support Majority Read Concern?

Write concern and read concern respectively specify the write and read policies for MongoDB.

If read concern is set to majority, data read by users has been written to a majority of nodes and will not be rolled back to avoid dirty reads.

DDS does not support majority read concern.

To meet this requirement, set write concern to majority. In this way, data is written to a majority of nodes, ensuring data consistency. Then, by reading data from a single node, it can be ensured that data read by the user can be written to a majority of nodes, and such data is not rolled back to avoid dirty read.

14 Backup and Restoration

14.1 Will I Be Charged for Manual Backups of Deleted DB Instances?

Yes. Manual backups are retained by default after your DB instances are deleted. The manual backups are billed based on the OBS pricing.

14.2 How Do I Back Up DDS Databases to an ECS?

You can store DDS backup data on an ECS using [mongoexport](#). However, you are not advised to use an ECS as backup space.

For the best reliability and service assurance, [store backups](#) in Object Storage Service (OBS) buckets.

14.3 How Long Does DDS Store Backup Data For?

The automated backup retention period is 7 days by default. You can set a backup retention period from 1 to 732 days. There is no limit on the manual backup retention period. You can delete manual backup files as needed.

14.4 How Do I Retrieve Lost DDS Backup Data?

If Cloud Trace Service (CTS) is not enabled, you cannot query operation records.

To query backup deletion records, you can enable CTS. For details, see [Querying Traces](#).

15 Network Security

15.1 What Security Protection Policies Does DDS Have?

DDS allows you to set the VPC which DDS DB instances belong to, ensuring that the DDS DB instances are isolated from other services. In addition, the IAM service is provided, achieving access control over DDS resources.

15.2 Do I Need to Use DDS in a VPC?

A VPC allows you to create virtual network environment in a private and isolated network to control the private IP address range, subnets, route tables, and network gateways. The VPC also allows you to define the virtual network topology and network configuration to make the network similar to the traditional IP network you are operating in the data center.

You may need to use DDS in the VPC in the following cases:

You want to run Internet-oriented web applications and retain the backend server that the public cannot access. To do so, you can create an ECS and a DDS DB instance in the same VPC, allocate a public IP address for the ECS, and deploy a web server on the ECS.

15.3 How Do I Ensure the Security of DDS in a VPC?

The VPC security group helps ensure the security of DDS in a VPC. In addition, ACL can be used to allow or reject I/O network traffic for each subnet. Use the internal security infrastructure (including the network firewall, intrusion detection, and protection system) to monitor all IPsec VPN connection-based input and output network traffic for VPC.

15.4 Does DDS Support IPv6 Subnets?

If you selected an IPv6 subnet, you cannot associate it with your instance. Select an IPv4 subnet.

16 Monitoring and Alarm

16.1 What DB Instance Monitoring Metrics Do I Need to Pay Attention To?

You need to focus on the CPU, memory, and storage space usage.

For more information about monitoring indicators, see [DDS Metrics](#).

You can configure DDS to report alarms as needed. If an alarm is reported, you can take proper measures to clear it.

Configuration examples:

- Configure DDS to report alarms to Cloud Eye if CPU utilization reaching or exceeding a certain value (90% for example) for multiple times (3 for example) within a period of time (5 minutes for example).
- Configure DDS to report alarms to Cloud Eye if its memory utilization reaches or exceeds a specific value (for example, 90%) multiple times (for example, 4 times) within a set period (for example, 5 minutes).
- Configure DDS to report alarms to Cloud Eye if its storage utilization reaches or exceeds a specific value (for example, 85%) multiple times (for example, 5 times) within a set period (for example, 5 minutes).

NOTE

For details on Cloud Eye alarm configuration, see "Alarm Rule Management" in *Cloud Eye Service User Guide*.

If the CPU and memory usage stay high for a long time and the disk capacity cannot be expanded, you can change the CPU and memory specifications.

Measures:

If a storage usage alarm is reported, perform either of the following operations:

- Check the storage space consumption and see whether any space can be freed up by deleting data from DB instances or dumping the data to another system.
- Scale up the storage space. For details, see [Scaling Up Storage Space](#).

16.2 What Should I Do If I Cannot Find Common Monitoring Items When Configuring DDS Alarm Rules?

Symptom

When a DDS alarm rule is configured, some common monitoring metrics, such as the CPU usage, memory usage, and storage space usage, are not displayed.

Possible Causes

When you configure alarm rules on the Cloud Eye console, the configured monitoring dimensions are inconsistent with the dimensions supported by the monitoring metric. As a result, the monitoring metrics are not displayed.

For example, if the objects whose CPU usage you want to monitor are mongos nodes or primary/standby nodes, the monitoring dimension you configure for an alarm rule on the Cloud Eye console must be at the node-level.

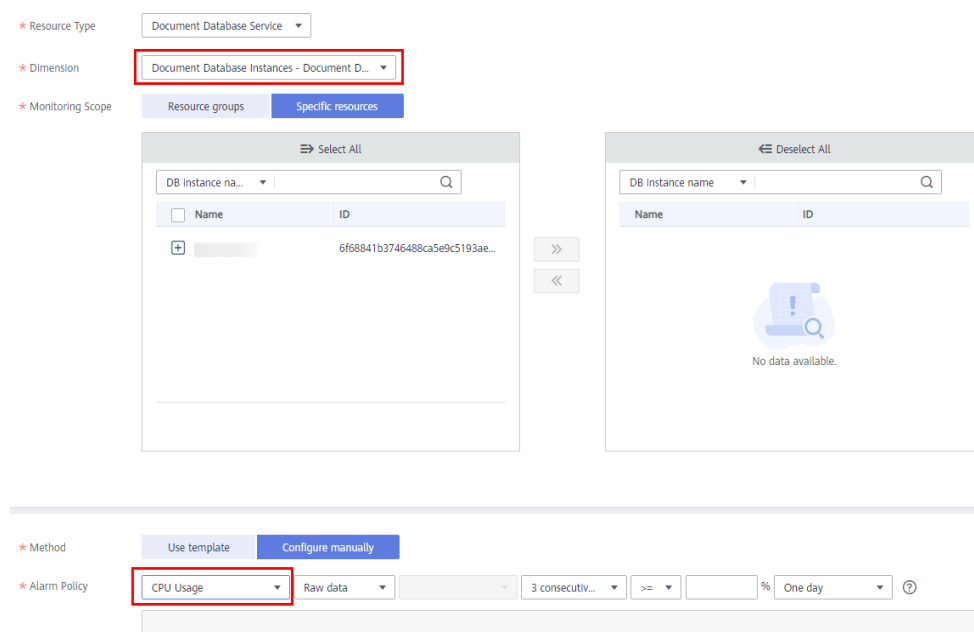
Solution

DDS supports instance-level and node-level metric monitoring. Set dimensions supported by monitoring metrics on the alarm rule page. Different metrics have different dimensions. For details, see [Supported DDS Metrics](#).

For example, the monitored objects of CPU usage can be mongos nodes of a DDS cluster instance, or the primary and standby nodes of a DDS DB instance.

When configuring alarm rules on the Cloud Eye console, select **Document Database Instances - Document Database Node** for **Dimension**. Then, you can view the CPU usage in the alarm policy.

Figure 16-1 Configuring monitoring dimension



16.3 How Often Does DDS Collect Metrics?

The default monitoring interval is 1 minute. To improve the instantaneous accuracy of monitoring metrics, you can set the monitoring interval to 5 seconds.

For details, see [Configuring Monitoring by Seconds](#).

A Change History (FAQs) Europe Site

Released On	Description
2022-09-30	This issue is the first official release.