Document Database Service

trouble-dds

Issue	01
Date	2026-09-23

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 Overview

You can use Mongo Shell, program code, or other tools to connect to a **DDS** instance.

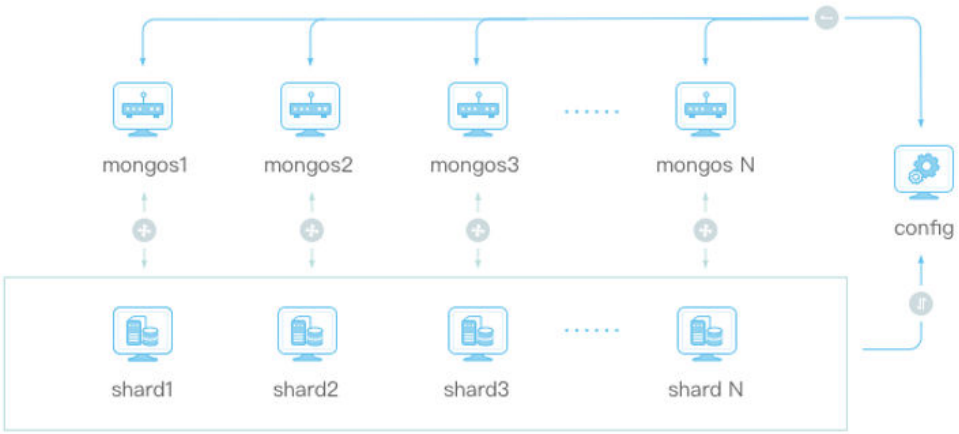
This section describes typical issues that may occur when connecting to a DDS database instance and provides the corresponding solutions.

2 DDS Instance Node Fault Handling Mechanism

Cluster Instance

The shard and config nodes of the cluster instance use the three-node replica set architecture. When a node is faulty, the system uses another normal node to replace the faulty node to continue providing services. In addition, the system checks and rectifies the faulty node. This process is transparent to users and may cause intermittent disconnection within 30 seconds. You are advised to enable automatic reconnection on your application.

Figure 2-1 Cluster instance diagram



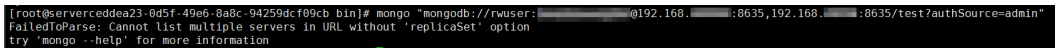
The dds mongos node of a cluster instance uses the single-node architecture. When a dds mongos node is faulty, services on the node become unavailable. You are advised to use Connection String URI to connect to all dds mongos nodes instead of a single dds mongos node. If a dds mongos node becomes faulty, the client can automatically perform failover and distribute requests to normal dds mongos nodes. Command example:

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

NOTICE

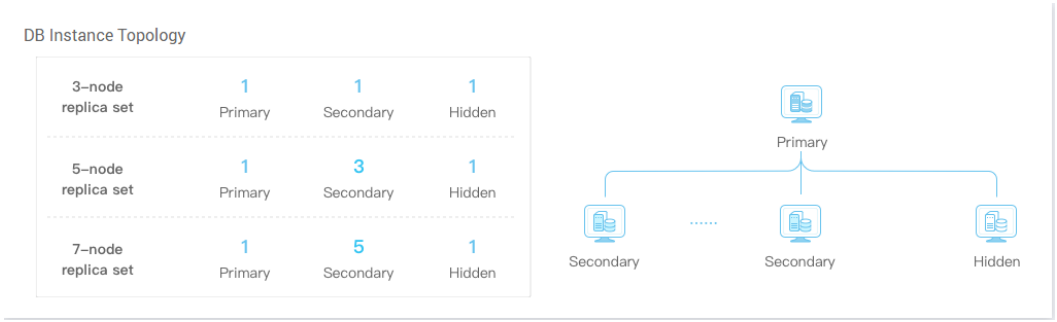
If you use Connection String URI to connect to a cluster instance that is compatible with MongoDB 3.4, you are advised to use a MongoDB client later than 4.0. Otherwise, an error is reported.

Figure 2-2 Error message



Replica Set Instance

Figure 2-3 Replica set instance diagram



A replica set instance consists of two nodes. When a node is faulty, the system uses the other node to continue providing services. In addition, the system checks and rectifies the faulty node. This process is transparent to users and may cause intermittent disconnection within 30 seconds. You are advised to enable automatic reconnection on your application.

You are advised to use Connection String URI to connect to the nodes. Do not directly connect to the primary node of a replica set instance. If Connection String URI is used and a node becomes faulty, the read and write operations will not be affected by the failover. Command example:

mongo "mongodb://
rwuser:xxxxxxxx@192.168.168.116:8635,192.168.200.147:8635/test?
authSource=admin&replicaSet=replica"

For best practices of connecting replica set instances, see **Connecting to a Replica Set Instance for Read and Write Separation and High Availability**.

Single-Node Instance

Figure 2-4 Single-node instance diagram

As the name implies, single-node instance provides only one node for users to access. When a node is faulty, the system checks and rebuilds the faulty node. In the meanwhile, services on the node become unavailable.

Single-node instances apply to scenarios such as testing, training, and non-core services. You are advised to use cluster instances or replica set instances in the production environment to ensure high service availability.

3 Connection Failure Message: network error while attempting to run command 'isMaster'

Symptom

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

./mongo --host 192.168.168.182 --port 8635 -u rwuser -p *xxxxxxxxxx* **--authenticationDatabase admin**

Figure 3-1 Connection failed

```
[root@ecs-liuwai bin]# ./mongo --host 192.168.168.182 --port 8635 -u rwuser -p --authenticationDatabase admin
MongoDB shell version v3.4.0
Enter password:
connecting to: mongodb://192.168.168.182:8635/
2019-01-10T09:28:27.002+0800 E QUERY    [main] Error: network error while attempting to run command 'isMaster' on host '192.168.
168.182:8635'  :
connect@src/mongo/shell/mongo.js:234:13
@(connect):1:6
exception: connect failed
[root@ecs-liuwai bin]#
```

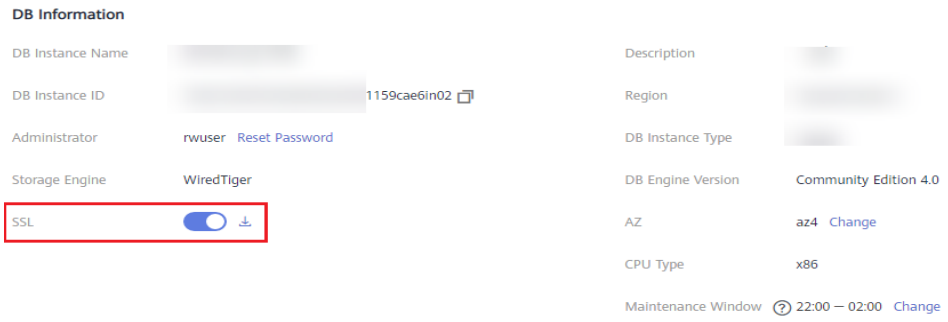
Possible Cause

This preceding command is used to connect to a DB instance in non-SSL mode. If the SSL connection is enabled, an error is reported when you run this command.

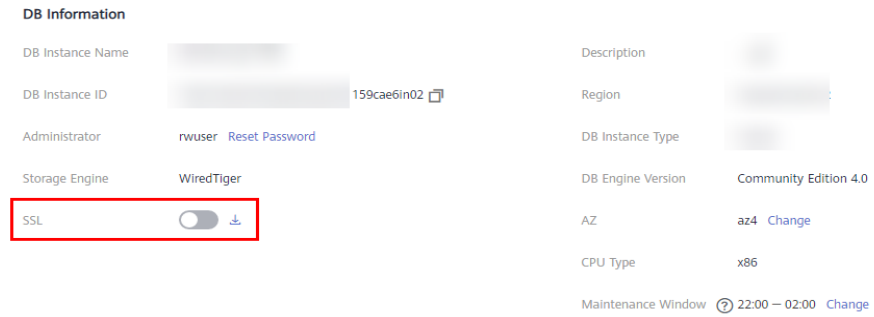
Fault Locating

On the DDS console, click the instance name. On the **Basic Information** page, check whether SSL is enabled.

- If SSL is enabled, connect to the instance in SSL mode using commands.



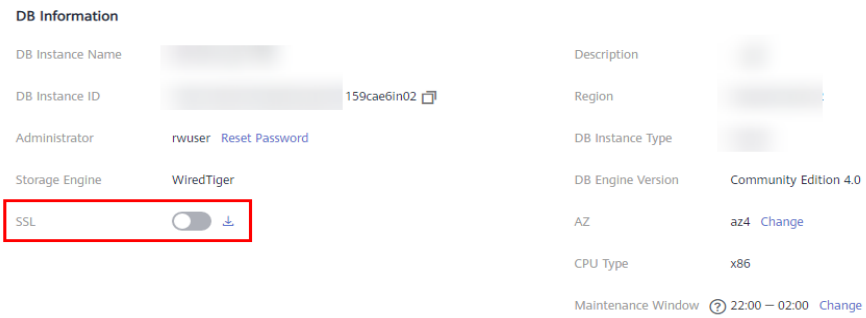
- If SSL is disabled, connect to the instance over an unencrypted connection using commands.



Solution

Method 1: Run the following command disable SSL and use an unencrypted connection to connect to the instance:

./mongo --host 192.168.168.182 --port 8635 -u rwuser -p *xxxxxxxxxx* **--authenticationDatabase admin**



Method 2: Connect to the instance using SSL.

To connect to the instance using SSL, download the SSL certificate, upload the certificate to the ECS directory (for example, **/root/ca.crt**), and run the command in SSL mode to connect to the instance.

NOTE

You can click the instance name on the DDS console, click next to **SSL** on the **Connections** page, and download the SSL certificate.

./mongo --host 192.168.168.182 --port 8635 -u rwuser -p *xxxxxxxxxx* **--authenticationDatabase admin --ssl --sslCAFile /root/ca.crt --sslAllowInvalidHostnames**

Figure 3-2 Connection succeeded

4 Connection Failure Messages: No route to host and connection attempt failed

Symptom

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

./mongo --host 192.168.1.6 --port 8635 -u rwuser -p *xxxxxxxxx* **--authenticationDatabase admin --ssl --sslCAFile /root/ca.crt –sslAllowInvalidHostnames**

Error message:

```
MongoDB shell version v3.4.17
connecting to: mongodb://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
```

Possible Cause

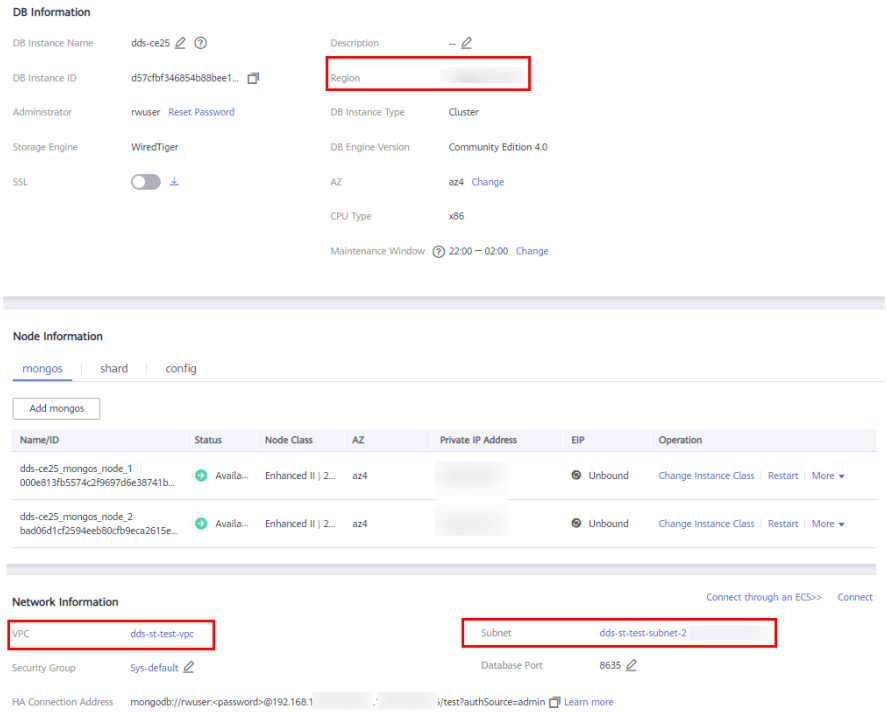
- The instance port is incorrect.
- The DDS instance and ECS are not in the same region.
- The DDS instance and ECS are not in the same subnet.

Fault Locating

Step 1 Check whether the DDS instance and ECS are in the same region, security group, and subnet.

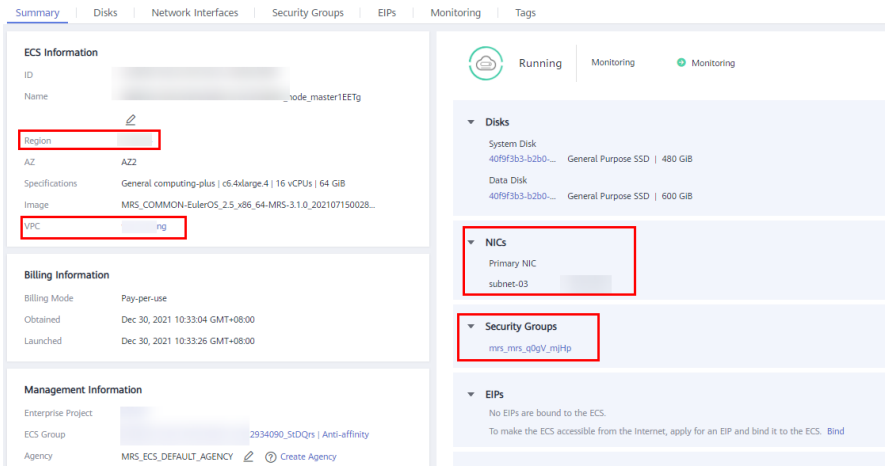
1. Log in to the DDS console, click the instance name, and view information about the region, VPC, security group, and subnet on the **Basic Information** page.

Figure 4-1 Viewing instance network information



2. Log in to the ECS console and click the ECS name. On the **Basic Information** page, view the region, VPC, security group, and subnet.

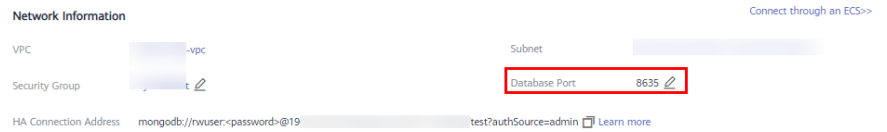
Figure 4-2 Viewing ECS network information



Step 2 Check whether the instance port is correct and run the curl command to check whether the port is available.

1. Click the instance name. On the **Basic Information** page, view the port of the instance.

Figure 4-3 Viewing instance port



2. Run the curl command to check whether the port is available. The following is an example:

   curl 192.168.1.6:8635

   If the message "It looks like you are trying to access MongoDB over HTTP on the native driver port." is displayed, the IP address can be connected and port 8635 can be used for communication.

   Figure 4-4 Command output

----End

Solution

- Select an ECS that is in the same region, VPC, and subnet as the DDS instance to be connected. Alternatively, you can bind an EIP to the instance and connect to the instance over a public network.
- Ensure that the entered port is the same as the actual port displayed on the console.

Background Information

- If you connect to an instance over a private network, ensure that the region, VPC subnet, and security group of the ECS are the same as those of the DDS instance to be connected.
- If you cannot connect to an instance over a private network, you can bind an EIP to the instance and connect to the instance over a public network.

5 Connection Failure Message: Authentication failed

Symptom

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

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

Error message:

```
MongoDB shell version v3.4.17
connecting to: mongodb://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
```

Possible Cause

When connecting to a DDS instance, you need to enter the administrator password. If the entered password is incorrect, the message "Authentication failed" is displayed.

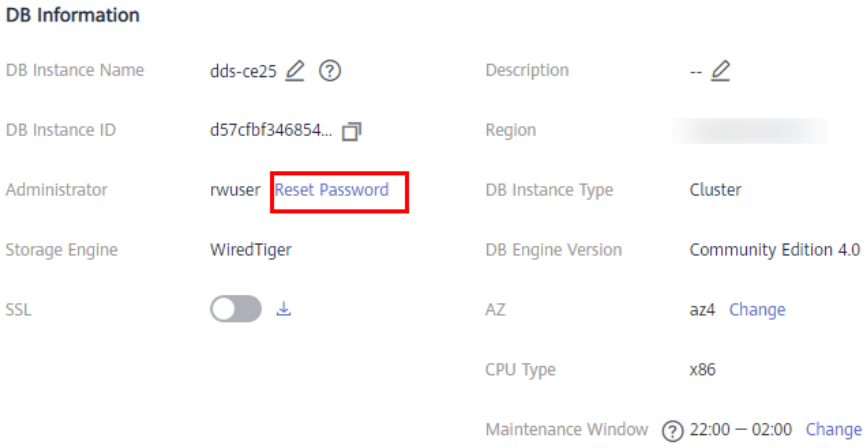
Fault Locating

Check whether the administrator password in the command for connecting to the DDS instance is correct.

Solution

- Enter the correct administrator password.
- If you forget your password, click the DB instance. On the displayed **Basic Information** page, click **Reset Password** in the **Administrator** field to reset the password.

Figure 5-1 Resetting a password



6 Connection Failure Message: couldn't connect to server

Symptom

An error is reported when you run the following command to connect to a DDS 3.4 instance:

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

Error message:

```
MongoDB shell version v3.4.17
connecting to: mongodb://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
```

Possible Cause

The security group policy is not correctly configured, which means that the security group rules do not allow traffic to access the DDS instance.

Fault Locating

Check whether the security group policy of the DDS instance is correctly configured. If the security group policy settings are incorrect, you cannot access DDS from outside the security group.

Solution

Set the security group policy. For details, see **Setting a Security Group**.

7 Connection Failure Message: cannot list multiple servers in URL without 'replicaSet' option

Symptom

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

./mongo mongodb://
rwuser:*xxxxxxxxxxx***@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.
```

Possible Cause

- The versions of the client and server are inconsistent.
- The command format is incorrect.

Fault Locating

- Check whether the versions of the client and server are the same.
- Check whether the format of the entered command is correct.

Solution

- The versions of the client and server must be consistent.
- **replicaSet** is specified in the URL command. (The name of **replicaSet** in DDS is fixed at **replica**.)
- The URL command is enclosed in double quotation marks.

8 Connection Failure Message: Timeout while receiving message

Symptom

An error is reported when a Java driver is used to connect to a DDS instance. The error information is as follows:

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

Possible Cause

- Slow queries occupy instance resources, causing the CPU usage to increase sharply or even reach the peak value.
- The connection pool of the application is incorrectly configured. As a result, the number of connections increases sharply and reaches the maximum number of connections supported by the DDS instance.

Fault Locating

- Check whether slow queries occupy instance resources.
- Check whether the configuration of the application connection pool is correct.

Solution

- Check whether slow queries exist. You can add indexes to optimize queries.
- Check whether the client uses the connection pool properly.
- Change the maximum number of connections supported by a DDS instance.

Background Information

The maximum number of connections depends on the instance specifications. When the maximum number of clients connected to an instance is reached, new client connection requests will be rejected.

9 Connection Failure Message: exception: login failed and U_STRINGPREP_PROHIBITED_ERROR

Symptom

An error is reported when you run the following command to connect to a DDS 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 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
2021-11-05T05:52:53.724+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
```


Possible Cause

The instance password is incorrect.

Fault Locating

- Check whether the DDS instance password contains the at sign (@), percent sign (%), and exclamation mark (!). If yes, escape them.
- DDS instances support the following special characters: ~!@#%^*-_=+?, in which % and @ must be escaped.

Solution

Method 1: Change the password of the DDS instance. The new password cannot contain the at sign (@), percent sign (%), and exclamation mark (!).

Method 2: When connecting to a DDS instance, escape the at sign (@), percent sign (%), and exclamation mark (!) and replace them with hexadecimal URL codes (ASCII codes) %40, %25, and %21.

For example, if the password is ******@ %***!**, the corresponding URL code is ****** %40%25*** %21**.

Background Information

The at sign (@), percent sign (%), and exclamation mark (!) are processed as special characters when you connect to a DDS instance. If these characters are used, they must be escaped when you use the HA connection address to connect to the DDS instance, otherwise, the password cannot be parsed.

