Distributed Cache Service

Troubleshooting Guide

Issue	01
Date	2020-11-04



HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2020. 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


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.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://www.huawei.com

Email: support@huawei.com

Contents

1 Troubleshooting Redis Connection Exceptions.....1
2 Troubleshooting 100% CPU Usage of a DCS Redis Instance.....4
3 Troubleshooting a Jedis Connection Pool Error.....6

 Copyright © Huawei Technologies Co., Ltd.

1 Troubleshooting Redis Connection Exceptions

Overview

This topic describes why Redis connection problems occur and how to solve the problems.

Problem Classification

To troubleshoot abnormal connections to a Redis instance, check the following items:

- **Connection Between the Redis Instance and the ECS**
- **Public Access**
- **Password**
- **Client Connections**
- **Bandwidth**
- **Redis Performance**

Connection Between the Redis Instance and the ECS

The ECS where the client is located must be in the same VPC as the Redis instance and be able to communicate with the Redis instance.

- For a Redis 3.0 instance, check the security group rules of the instance and the ECS.

  Correctly configure security group rules for the ECS and the Redis instance to allow the Redis instance to be accessed. For details, see **How Do I Configure a Security Group?**
- For a DCS Redis 4.0 or 5.0 instance, check the whitelist of the instance.

  If the instance has a whitelist, ensure that the client IP address is included in the whitelist. Otherwise, the connection will fail. For details, see **Managing IP Address Whitelist**. If the client IP address changes, add the new IP address to the whitelist.
- Check the regions of the Redis instance and the ECS.

 Copyright © Huawei Technologies Co., Ltd.

If the Redis instance and the ECS are not in the same region, create another Redis instance in the same region as the ECS and migrate data from the old instance to the new instance by referring to **Data Migration Guide**.

- Check the VPCs of the Redis instance and the ECS.

  Different VPCs cannot communicate with each other. An ECS cannot access a Redis instance if they are in different VPCs. You can establish VPC peering connections to allow the ECS to access the Redis instance across VPCs.

  For more information on how to create and use VPC peering connections, see **VPC Peering Connection**.

Public Access

Before accessing a Redis instance through a public network, ensure that the instance supports public access. For details, see the **public access explanation**.

- **Symptom**: "Error: Connection reset by peer" is displayed or a message is displayed indicating that the remote host forcibly closes an existing connection.
  - **Possible cause 1**: The security group is incorrectly configured.

    Solution: Correctly configure the Redis instance and access the instance by following the **public access instructions**.
  - **Possible cause 2**: SSL encryption has been enabled, but Stunnel is not configured during connection. Instead, the IP address displayed on the console was used for connection.

    Solution: When enabling SSL encryption, install and configure the Stunnel client. For details, see **Enabling SSL Encryption**. In the command for connecting to the Redis instance, the address must be set to the IP address and port number of the Stunnel client. Do not use the public access address and port displayed on the console.
- **Symptom**: Public access has been automatically disabled.

  Cause: The EIP bound to the DCS Redis instance is unbound. As a result, public access is automatically disabled.

  Solution: Enable public access for the instance and bind an EIP to the instance on the management console. Then, try again.

Password

If the instance password is incorrect, the port can still be accessed but the authentication will fail. If you forget the password, you can reset the password. For details, see **Resetting Instance Passwords**.

Client Connections

- If the connection fails when you use redis-cli to connect to a Redis Cluster instance, do as follows:

  Check whether **-c** is added to the connection command. Ensure that the correct connection command is used when connecting to the cluster nodes.
  - Run the following command to connect to a Redis Cluster instance:

    ./redis-cli -h *{dcs_instance_address}* -p 6379 -a *{password}* -c

 Copyright © Huawei Technologies Co., Ltd.

  - Run the following command to connect to a single-node, master/standby, or Proxy Cluster instance:

    ./redis-cli -h *{dcs_instance_address}* -p 6379 -a *{password}*

  For details, see **Access Using redis-cli**.

- If error "Read timed out" or "Could not get a resource from the pool" occurs, do as follows:

  Check if the **KEYS** command has been used. This command consumes a lot of resources and can easily block Redis. Instead, use the **SCAN** command and avoid executing the command frequently.

- If an error occurs when you use the Jedis connection pool, see **Troubleshooting a Jedis Connection Pool Error**.

Bandwidth

If the bandwidth reaches the upper limit of the corresponding instance specifications, Redis connections may time out.

You can view the **Flow Control Times** metric to check whether the bandwidth has reached the upper limit.

Then, check whether the instance has big keys and hot keys. If a single key is too large or overloaded, operations on the key may occupy too many bandwidth resources. For details about big keys and hot keys, see **Analyzing Big Keys and Hot Keys**.

Redis Performance

Connections to an instance may become slow or time out if the CPU usage spikes due to resource-consuming commands such as **KEYS**, or too much memory is used because the expiration time is not set for the instance or expired keys remain in the memory. In these cases, do as follows:

- Use the **SCAN** command instead of the **KEYS** command, or disable the **KEYS** command.
- Check the monitoring data and configure alarm rules. For details, see **Setting Alarm Rules for Critical Metrics**.

  For example, you can view the **Memory Usage** and **Used Memory** metrics to keep track of the instance memory usage, and view the **Connected Clients** metric to determine whether the instance connections limit has been reached.
- Check whether the instance has big keys and hot keys.

  For details about the operations of big key and hot key analysis, see **Analyzing Big Keys and Hot Keys**.

 Copyright © Huawei Technologies Co., Ltd.

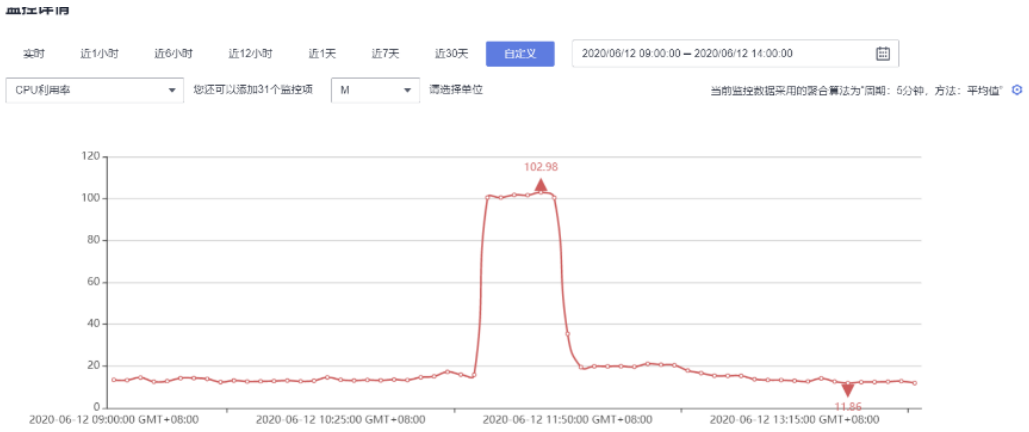
2 Troubleshooting 100% CPU Usage of a DCS Redis Instance

Symptom

The CPU usage of a Redis instance spikes to 100% within a short period of time.

Fault Locating

Step 1 Check the monitoring data generated during the period when the problem occurred.



Redis is single-threaded. If CPU usage suddenly surges at a specific point in time, an operation may have blocked the thread. In this case, check whether the slow log exists.

Step 2 Go to the **Performance Monitoring** page of the instance and check **Slow Query Logs** metric.

If the slow log exists, check the slow log.

Step 3 Go to the **Slow Log** page of the instance and check the slow log generated during the specified period.

 Copyright © Huawei Technologies Co., Ltd.



The **KEYS** command may have caused the slow log. Running the **KEYS** command will initiate the search for all keys that meet the conditions, which occupies an excessive amount of CPU resources and may deteriorate performance. Instead, you can run the **SCAN** command or disable the **KEYS** command.

----End

 Copyright © Huawei Technologies Co., Ltd.

3 Troubleshooting a Jedis Connection Pool Error

The error message that will possibly be displayed when you use the Jedis connection pool is as follows:

```
redis.clients.jedis.exceptions.JedisConnectionException: Could not get a resource from the pool
```

If this error message is displayed, check whether your instance is running properly. If it is running properly, perform the following checks:

Step 1 Check the network.

1. Check the IP address configurations.

   Check whether the IP address configured on the Jedis client is the same as the subnet address configured for your DCS instance. If public access is enabled for your instance, check whether the IP address configured on the Jedis client is the same as the EIP bound to your instance. If they are inconsistent, modify the IP address configuration and then try again.

2. Test the network.

   Use the ping command and telnet on the client to test the network.

   - If the network cannot be pinged:
     - For intra-VPC access, ensure that the client and your DCS instance belong to the same VPC and security group, or the **security group of your DCS instance allows access through port 6379**.
     - For public access with SSL encryption, ensure that you have configured the security group of your DCS instance, **allowing access through port 36379**.
     - For public access without SSL encryption, ensure that you have configured the security group of your DCS instance, **allowing access through port 6379**.
   - If the IP address can be pinged but telnet failed, restart your instance. If the problem persists after the restart, contact technical support.

Step 2 Check the number of connections.

Check whether the number of established network connections exceeds the upper limit configured for the Jedis connection pool. If the number of established

 Copyright © Huawei Technologies Co., Ltd.

connections approaches the configured upper limit, restart the DCS service and check whether the problem persists. If the number of established connections is far below the upper limit, continue with the following checks.

In Unix or Linux, run the following command to query the number of established network connections:

netstat -an | grep 6379 | grep ESTABLISHED | wc -l

In Windows, run the following command to query the number of established network connections:

netstat -an | find "6379" | find "ESTABLISHED" /C

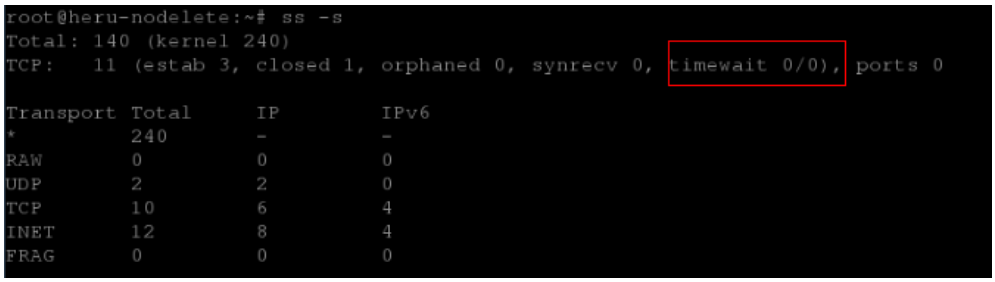
Step 3 Check the JedisPool code.

If the number of established connections approaches the upper limit, determine whether the problem is caused by service concurrency or incorrect usage of JedisPool.

When using JedisPool, you must call **jedisPool.returnResource()** or **jedis.close()** (recommended) to release the resources after you call **jedisPool.getResource()**.

Step 4 Check the number of TIME_WAIT connections.

Run the **ss -s** command to check whether there are too many **TIME_WAIT** connections on the client.



If there are too many **TIME_WAIT** connections, modify the kernel parameters by running the **/etc/sysctl.conf** command as follows:

```
##Uses cookies to prevent some SYN flood attacks when the SYN waiting queue overflows.
net.ipv4.tcp_syncookies = 1
##Reuses TIME_WAIT sockets for new TCP connections.
net.ipv4.tcp_tw_reuse = 1
##Enables quick reclamation of TIME_WAIT sockets in TCP connections.
net.ipv4.tcp_tw_recycle = 1
##Modifies the default timeout time of the system.
net.ipv4.tcp_fin_timeout = 30
```

After the modification, run the **/sbin/sysctl -p** command for the modification to take effect.

Step 5 If the problem persists after you perform the preceding checks, perform the following steps.

Capture packets and send packet files along with the time and description of the exception to technical support for analysis.

Run the following command to capture packets:

tcpdump -i eth0 tcp and port 6379 -n -nn -s 74 -w dump.pcap

 Copyright © Huawei Technologies Co., Ltd.

In Windows, you can also install the Wireshark tool to capture packets.

NOTE

For public access, change the port number to **36379**.

Replace the NIC name to the actual one.

----End

 Copyright © Huawei Technologies Co., Ltd.