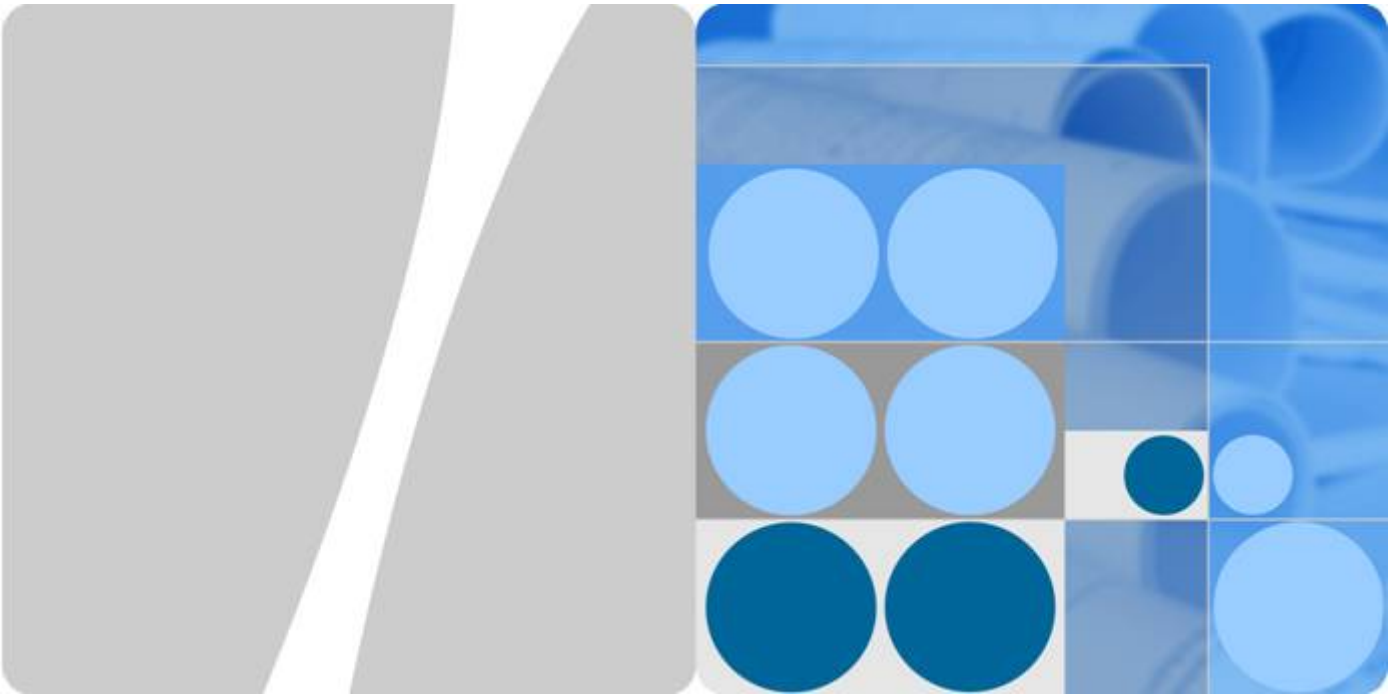


Distributed Message Service

FAQs

Issue 01

Date 2020-12-08

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

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.

Contents

1 Does DMS Support FIFO Delivery?..... 1
2 Does DMS Support "At Least Once" Message Delivery?..... 2
3 How Long Can a Message be Retained in a Queue?..... 3
4 What Is the Maximum Size of a Message?..... 4
5 Does DMS Guarantee Zero Message Repetition?..... 5
6 How Does DMS Ensure Message Security in a Queue?..... 6
7 How Many Queues Can Be Created Under a Project?..... 7
8 How Many Consumer Groups Can Be Created in Each Queue?..... 8
9 Why Can't I Retrieve the Chosen Number of Messages from a Queue That Contains Only a Few Messages?..... 9
10 Why Do Consumers Need to Acknowledge Messages?..... 11
11 Will Duplicate Messages Be Retrieved After "Delay Message Delivery" Is Enabled?..... 12
12 Will Duplicate Messages Be Retrieved After Redelivery?..... 13
13 What Are the Differences Between Kafka Queues and Kafka Premium Instances?..... 14
14 Do RabbitMQ or Kafka Premium Instances Support Cross-VPC Access?..... 15
15 Do RabbitMQ or Kafka Premium Instances Support Cross-Subnet Access?..... 16
16 How to Select and Configure a Security Group?..... 17
17 Can I Access DMS Over a Public Network?..... 20
18 Where Does a Newly Created Consumer Group Start Message Retrieval?..... 21
19 How Is the Performance of Global FIFO Queues?..... 22
20 Why Can't I View the Subnet and Security Group Information When Creating a DMS Instance?..... 23
21 What If One RabbitMQ VM Fails to Be Restarted When a Cluster RabbitMQ Instance Is Being Restarted?..... 24

22 How Are Requests Evenly Distributed to Each VM of a Cluster RabbitMQ Instance?..... 25

23 Do Queues Inside a Cluster RabbitMQ Instance Have Any Redundancy Backup?..... 26

24 DMS Password Complexity Requirements..... 27

1 Does DMS Support FIFO Delivery?

Yes. When creating a queue, you can select **Standard** and then **Global FIFO**. In a global FIFO queue, messages are retrieved in the order they were sent. Global FIFO queues are applicable to scenarios where the order of messages is important. In a partition-level FIFO queue, messages might be retrieved in an order different from which they were sent. Partition-level FIFO queues are applicable to scenarios where high concurrency is important.

2 Does DMS Support "At Least Once" Message Delivery?

Yes. DMS stores message copies in multiple servers to achieve message backup and high availability. In rare cases, a server storing message replicas may be unavailable when you request or delete messages. If this happens, the message replicas will not be deleted from that server and may be sent when the connection is restored. This process is called "at-least-once" delivery. To avoid any adverse impact from processing the same message multiple times, ensure that your application processes messages idempotently.

3 How Long Can a Message be Retained in a Queue?

In standard queues, messages are retained for at least 72 hours and will be deleted 72 hours later. In Kafka queues, messages are retained for 1 to 72 hours, depending on what you choose when creating a queue. In Kafka premium instances, messages are retained for 1 to 168 hours, depending on what you choose when creating a topic.

4 What Is the Maximum Size of a Message?

The size of each message, including the message body, labels and attributes, cannot exceed 512 KB.

On the DMS console, only one message can be sent at a time. The **Message Body** input box displays the remaining number of bytes allowed in a message as you are creating the message. If the message size exceeds 512 KB, you cannot click **OK** to create the message.

Multiple messages can be sent at a time through APIs, but the aggregated message size cannot exceed 512 KB. If the aggregated message size exceeds 512 KB, messages fail to be created and the API caller receives the error message "The message size is {message size}, larger than the size limit {max allowed size}".

If a Kafka SDK API is used to create messages in a Kafka queue, the maximum size of a single message is 10 MB. If the DMS console is used to create messages in a Kafka queue, the maximum size of a single message is 512 KB.

5 Does DMS Guarantee Zero Message Repetition?

DMS does not guarantee zero message repetition. Messages may be sent more than once if network exceptions occur.

6 How Does DMS Ensure Message Security in a Queue?

DMS uses a reliable authentication mechanism to prevent unauthorized access to messages to ensure queue security.

DMS queues:

- Before you manage messages on the DMS console, you must complete your identity authentication.
- If you use APIs to send and retrieve messages, you must obtain a token, and add the obtained token to the API request header. In addition, the API request must be signed using the access key ID/secret access key (AK/SK pair), so that this API request can be sent through the API gateway. For details on how to obtain a token and AK/SK, see the *Distributed Message Service API Reference*.

Kafka premium instances:

- For intra-VPC access, the client and the server must be in the same VPC and have been configured with correct security group rules. You can enable SASL authentication to encrypt data before transmission for higher security.
- For public access, enable SASL authentication.

7 How Many Queues Can Be Created Under a Project?

You can create multiple projects. By default, 30 queues can be created under a project. To create more queues, contact customer service to increase your quota.

8 How Many Consumer Groups Can Be Created in Each Queue?

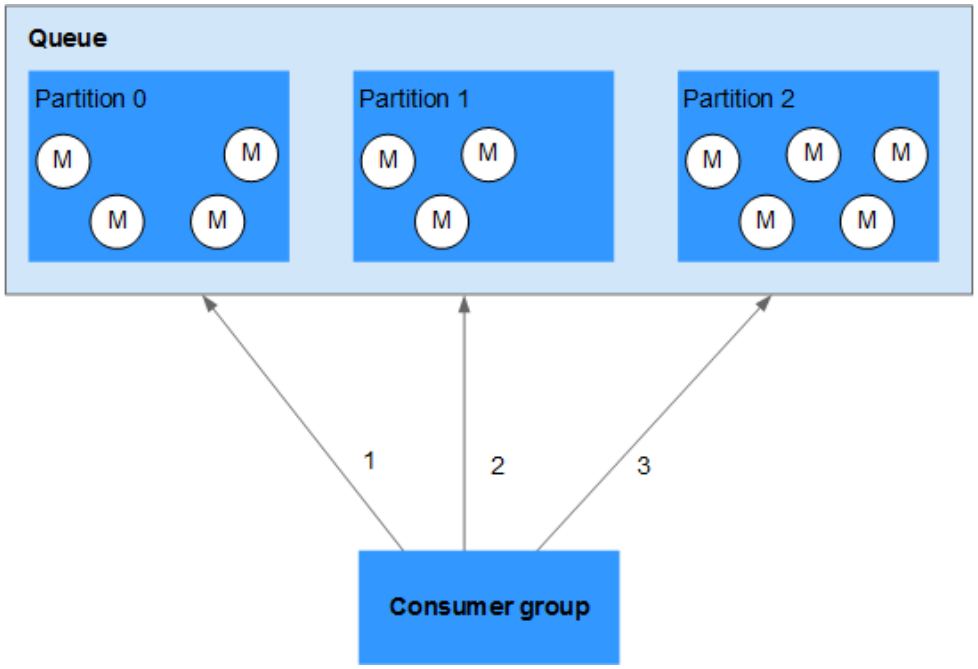
A maximum of three consumer groups can be created in each queue.

9 Why Can't I Retrieve the Chosen Number of Messages from a Queue That Contains Only a Few Messages?

- Messages in a global FIFO queue are stored in a single partition. Upon each retrieval request, the chosen number of messages can be returned, unless the available number of messages in the queue is less than the chosen number of messages.
- Messages in other types of queues are distributed to multiple partitions. This achieves high concurrency, allowing multiple requests from a consumer group to be processed concurrently. To avoid performance loss caused by cross-partition access and management, a single retrieval request from a consumer group returns messages in only one partition. Therefore, when a queue holds a small number of available messages, a single retrieval request may not return the chosen number of messages even if the number of available messages in the queue is greater than the chosen number of messages.

  For example, as shown in **Figure 9-1**, 12 messages exist in the queue and are distributed in three partitions. If the chosen number of messages is **10**, only four messages can be retrieved from **Partition 0**. After retrieval from **Partition 0** is complete, messages are retrieved from **Partition 1** and then from **Partition 2**.

Figure 9-1 A single retrieval request returns messages from only one partition



10 Why Do Consumers Need to Acknowledge Messages?

Messages need to be acknowledged to ensure the reliability of messages. The reliability in sending and retrieving messages is the result of joint efforts from DMS, message producers, and message consumers. DMS considers a message to be retrieved only after a consumer acknowledges the message (that is, acknowledges the message retrieval).

While a message is being retrieved, it remains in the queue. It cannot be retrieved again within 30s since the start of retrieval. If the message is not acknowledged within this period, DMS determines that the message is not successfully retrieved, and the message can be retrieved again.

NOTE

Only messages retrieved using APIs need to be acknowledged. Messages retrieved using the DMS console are automatically acknowledged.

11 Will Duplicate Messages Be Retrieved After "Delay Message Delivery" Is Enabled?

Yes. After Delay Message Delivery is enabled, delivery of messages will be delayed for a specified time period. In the event of a network error, messages may be retrieved in duplicate. To avoid any adverse impact from processing the same message multiple times, ensure that your application processes messages idempotently.

12 Will Duplicate Messages Be Retrieved After Redelivery?

Yes. Messages in standard queues can be flagged to be redelivered during acknowledgment by using an SDK. Redelivered messages can be retrieved a second time.

In the event of a network error, redelivered messages may be retrieved in duplicate. Therefore, set your application as an idempotent application so it is not affected when it processes a message multiple times.

13 What Are the Differences Between Kafka Queues and Kafka Premium Instances?

- Creation:

  When you apply for a Kafka premium instance, an exclusive instance is created and runs on an ECS in a VPC. You can create multiple topics in a Kafka premium instance and customize the number of partitions. A Kafka queue is equivalent to a Kafka topic, and three partitions are configured by default.

- Resource allocation:

  Kafka premium instances are a new type of resource provided by DMS. After creating a Kafka premium instance, you can exclusively use physically isolated resources in the instance.

- Client connection:

  Kafka queues require tenant identity authentication for logical isolation. Therefore, token authentication is added to the DMS SDK based on the open-source Kafka SDK. By contrast, Kafka premium instances support client-based access in a VPC. With the secure access control provided by the VPC, you can access Kafka premium instances by using the open-source SDK.

14 Do RabbitMQ or Kafka Premium Instances Support Cross-VPC Access?

Yes. RabbitMQ and Kafka premium instances support cross-VPC access. By establishing a peering connection between two VPCs, ECSs in one VPC can access instances in the other VPC.

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

15 Do RabbitMQ or Kafka Premium Instances Support Cross-Subnet Access?

Yes.

If the client and the instance are in the same VPC, cross-subnet access is supported.

If the client and the instance are in different VPCs, establish a **VPC peering connection**.

You can also access an instance through the elastic IP address bound to the instance.

16 How to Select and Configure a Security Group?

To access a Kafka premium instance or RabbitMQ premium instance within a VPC or over public networks, configure the security group rules as follows (using Kafka instances as an example).

Intra-VPC Access

To access a Kafka premium instance, you must deploy your client on an ECS in the same VPC and subnet as the instance.

In addition, before you can access the instance through your client, you must configure correct rules for the security groups of both the ECS and the Kafka premium instance.

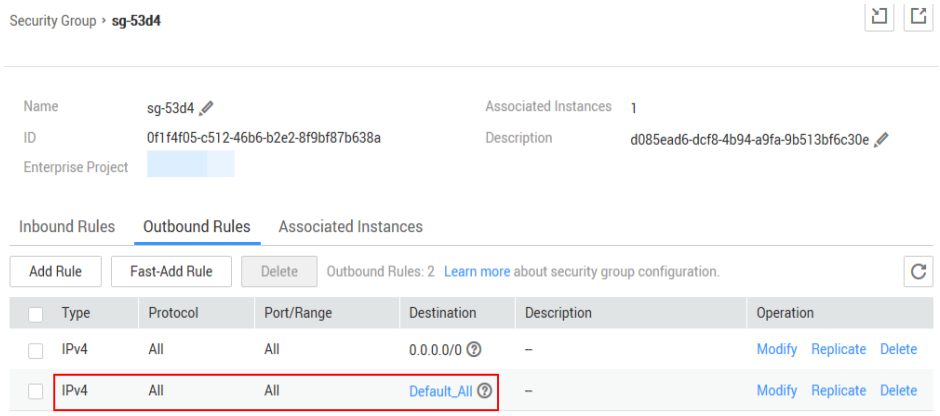
1. You are advised to configure the same security group for the ECS and the Kafka premium instance. After a security group is created, network access in the group is not restricted by default.
2. If the ECS and the instance belong to different security groups, add security group rules to ensure that the ECS and the instance can access each other.

   NOTE

   - Assume that security groups **sg-53d4** and **Default_All** are configured respectively for your ECS and Kafka premium instance.
   - You can specify a security group or IP address as the remote end in the following rules.

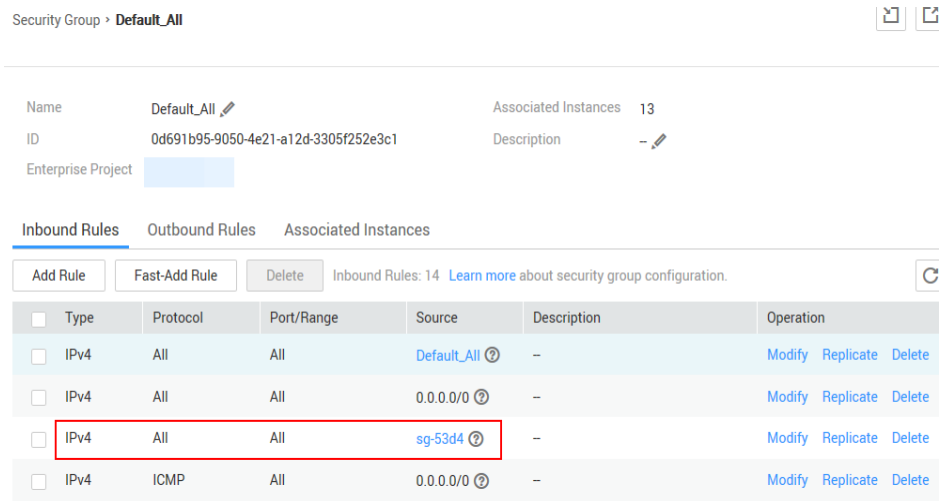
   To ensure that your client can access the instance, add the following rule to the security group configured for the ECS.

Figure 16-1 Configuring rules for the security group of the ECS



To ensure that your client can access the Kafka premium instance, add the following rule to the security group configured for the instance:

Figure 16-2 Configuring rules for the security group of the Kafka premium instance



Public Access

A client can access a Kafka premium instance only if rules have been correctly configured for the security group of the instance.

For example, for security group **sg-Kafka**, you need to configure either of the following rules in the inbound direction:

- Protocol: **TCP**; port number: **9094**; source IP address: **0.0.0.0/0**
- Protocol: **Any**; source IP address: **0.0.0.0/0**

The following figures show the rules.

Figure 16-3 Rule 1 for the security group

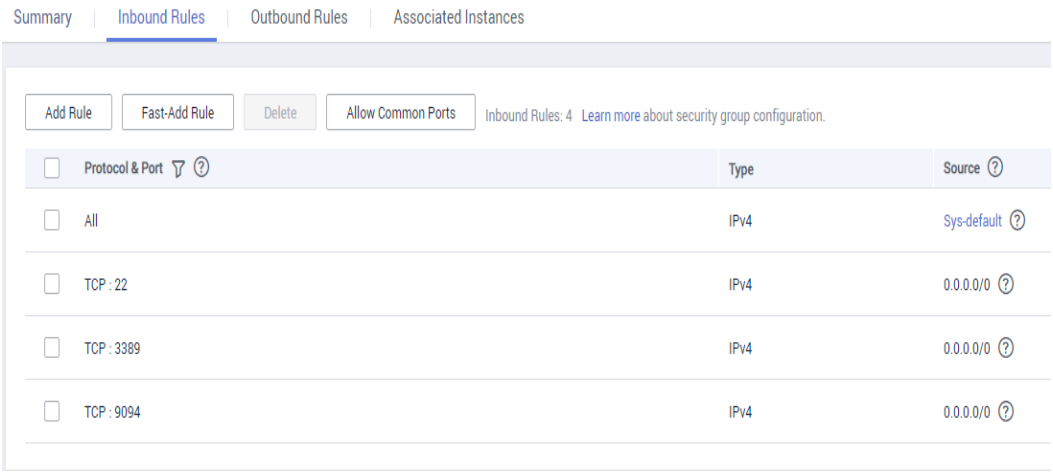
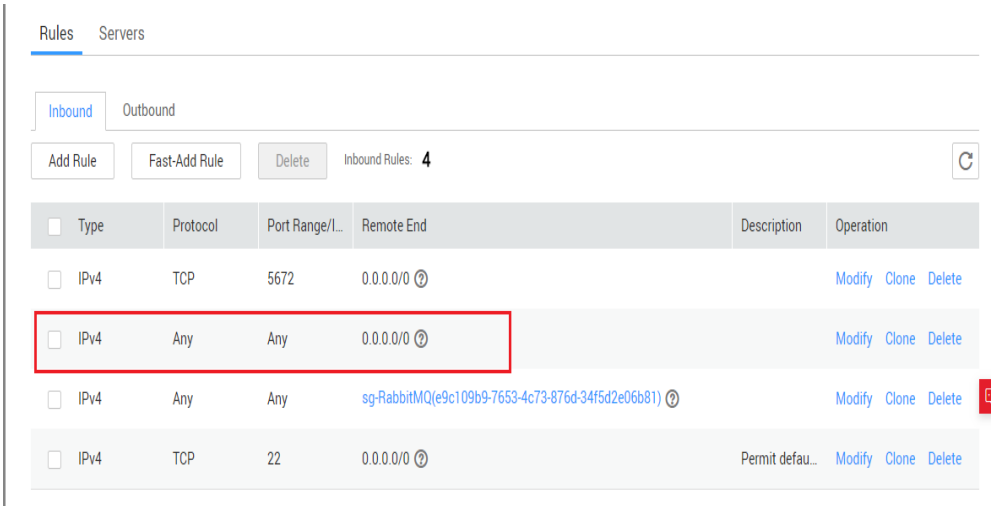


Figure 16-4 Rule 2 for the security group



17 Can I Access DMS Over a Public Network?

Whether you can access DMS over a public network depends on the queue type and access mode.

- RESTful API

  Public access is supported. You can access standard and Kafka queues over a public network by using a RESTful API.

- TCP API

  Public access is not supported. To access DMS by using a TCP API, you must deploy your message client on an ECS.

- Open-source Kafka API

  Public access is supported. Alternatively, you can access DMS from an ECS. Note that the DMS endpoints differ by access mode.

18 Where Does a Newly Created Consumer Group Start Message Retrieval?

- Kafka API
  - When a newly created consumer group starts message retrieval for the first time, it ignores all messages that have already been sent, and only retrieves messages sent after its creation. To set the message retrieval start position to the earliest message, change the default value of **auto.offset.reset** from **latest** to **earliest** in the **Consumer** configuration on your Kafka client.
  - When the consumer group starts message retrieval for a second time, it retrieves messages starting from the last retrieval position.
  - To start message retrieval from a specific position, reset the retrieval start position on the DMS console as required. The reset takes effect only for the queue of the configured consumer group, and does not affect other consumer groups.
- RESTful API / TCP API
  - When a consumer group starts message retrieval for the first time, it retrieves messages starting from the earliest in the queue.
  - When the consumer group starts message retrieval for a second time, it retrieves messages starting from the last retrieval position.
  - To start message retrieval from a specific position, reset the retrieval start position on the DMS console as required. The reset takes effect only for the queue of the configured consumer group, and does not affect other consumer groups.

19 How Is the Performance of Global FIFO Queues?

Compared with partition-level FIFO queues, global FIFO queues have restrictions in application, deteriorating their performance. For example, to ensure that messages are globally retrieved in the order they were sent, you cannot configure multiple partitions to improve concurrent message retrieval.

In global FIFO queue mode, the message retrieval order is ensured by DMS queues, and places requirements on your service.

- Messages must be created in order and then sent to message queues in synchronous mode, which is less efficient than asynchronous message transmission mode.
- Messages must be retrieved and acknowledged in order, and messages in a queue cannot be concurrently consumed using multiple clients or threads.

You are advised to use the global FIFO queue mode in scenarios with high requirements for ordered message processing, such as processing transactions or financial transaction messages.

20 Why Can't I View the Subnet and Security Group Information When Creating a DMS Instance?

This may be because you do not have the permissions of the server administrator and VPC administrator. For details on how to add user permissions, see **Adding Users to a User Group**.

21 What If One RabbitMQ VM Fails to Be Restarted When a Cluster RabbitMQ Instance Is Being Restarted?

Restarting a RabbitMQ instance will restart only the RabbitMQ process instead of VMs on which the instance runs.

For a cluster RabbitMQ instance, if the RabbitMQ process fails to be restarted on one VM, the instance will be still in the **Running** state after the restart and a message is displayed indicating that some nodes are faulty. A RabbitMQ daemon process runs on each VM and periodically checks whether the RabbitMQ process exists. If the RabbitMQ process does not exist, the RabbitMQ process will be automatically started.

If a RabbitMQ instance exception lasts for more than 1 minute, an alarm will be reported, and HUAWEI CLOUD technical support will take follow-up actions.

22 How Are Requests Evenly Distributed to Each VM of a Cluster RabbitMQ Instance?

A cluster uses Linux virtual servers (LVSs) inside for load balancing, which evenly distribute requests to each VM.

23 Do Queues Inside a Cluster RabbitMQ Instance Have Any Redundancy Backup?

Whether queue mirroring (that is, redundancy backup) is implemented depends on your service requirements. If you configure mirroring, queue replicas are stored on multiple VMs in a cluster. When a VM is faulty, queue data is synchronized to this VM from another normal VM.

24 DMS Password Complexity Requirements

The passwords must meet the following requirements:

- Cannot be left blank.
- Must be 8 to 32 characters long.
- Contain at least three of the following character types:
  - Lowercase letters
  - Uppercase letters
  - Digits
  - Special characters (`~!@#$%^&*()-_=+\|[{}]:'",<.>/?)
- Cannot start with a hyphen (-).
- Cannot be the username or the username spelled backwards.

