Distributed Message Service for Kafka

Getting Started

Issue 01

Date 2025-02-13

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Contents

1 Getting Started with Kafka for Message Production and Consumption

This section takes the example of creating a Kafka instance (ciphertext access and SASL_SSL) and accessing it on the client (private network, within a virtual private cloud (VPC)) for message production and consumption to get you quickly started with Distributed Message Service (DMS) for Kafka.

Figure 1-1 Procedure for using DMS for Kafka
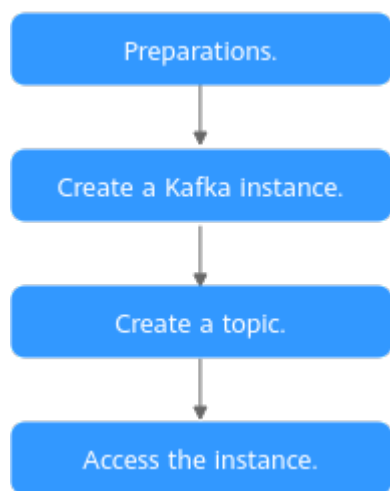
1. **Step 1: Preparations**

   A Kafka instance runs in a virtual private cloud (VPC). Before creating a Kafka instance, ensure that a VPC is available.

   After a Kafka instance is created, download and install the Kafka open-source client on your ECS before producing and consuming messages.

2. **Step 2: Create a Kafka Instance**

   You can select the specification and quantity, and enable ciphertext access and SASL_SSL when creating a Kafka instance.

   When connecting to a Kafka instance with SASL_SSL enabled, SASL is used for authentication. Data is encrypted with SSL certificates for high-security transmission.

3. **Step 3: Create a Topic**

   Topics store messages created by producers and subscribed by consumers.

   This section uses the example of creating a topic on the console.

4. **Step 4: Connect to a Kafka Instance to Produce and Consume Messages**

   Before connecting to a Kafka instance with SASL_SSL enabled, download the certificate and configure the connection in the client configuration file.

Step 1: Preparations

Step 1   Register a HUAWEI ID.

Before creating a Kafka instance, register a HUAWEI ID. For details, see **Signing Up for a HUAWEI ID and Enabling Huawei Cloud Services**.

If you already have a HUAWEI ID, skip this step.

Step 2   Grant Kafka instance permissions.

To achieve fine-grained management of your cloud resources, create Identity and Access Management (IAM) user groups and users and grant specified permissions to the users. For more information, see **Creating a User and Granting DMS for Kafka Permissions**.

Step 3   Create a VPC and subnet.

Before creating a Kafka instance, ensure that a VPC and a subnet are available. For details about how to create a VPC and a subnet, see **Creating a VPC and Subnet**.

The VPC **must** be created in the **same** region as the Kafka instance.

Step 4   Create a security group and add security group rules.

Before creating a Kafka instance, ensure that a security group is available. For details about how to create a security group, see **Creating a Security Group**.

The security group **must** be created in the **same** region as the Kafka instance.

To connect to Kafka instances, add the security group rules described in **Table 1-1**. Other rules can be added based on site requirements.

Table 1-1 Security group rules

Direction	Protocol	Port	Source address	Description
Inbound	TCP	9093	0.0.0.0/0	Accessing a Kafka instance over a private network within a VPC (in ciphertext)

> **NOTE**
>
> After a security group is created, it has a default inbound rule that allows communication among ECSs within the security group and a default outbound rule that allows all outbound traffic. If you access your Kafka instance using the private network within a VPC, you do not need to add the rules described in **Table 1-1**.

Step 5 Construct a client for message production and consumption.

This section uses a Linux elastic cloud server (ECS) as the client. Before creating a Kafka instance, create an ECS with an EIP, install the JDK, configure environment variables, and download an open-source Kafka client.

1. Log in to the console, click ☰ in the upper left corner, click **Elastic Cloud Server** under **Computing**, and then create an ECS.

   For details about how to create an ECS, see **Purchasing a Custom ECS**. If you already have an available ECS, skip this step.

2. Log in to an ECS as user **root**.

3. Install Java JDK and configure the environment variables **JAVA_HOME** and **PATH**.

   a. Download a JDK.

      > **NOTE**
      >
      > Use Oracle JDK instead of ECS's default JDK (for example, OpenJDK), because ECS's default JDK may not be suitable. Obtain Oracle JDK 1.8.111 or later from **Oracle's official website**.

   b. Decompress the JDK.
      ```
      tar -zxvf jdk-8u321-linux-x64.tar.gz
      ```
      Change **jdk-8u321-linux-x64.tar.gz** to your JDK version.

   c. Open the **.bash_profile** file.
      ```
      vim ~/.bash_profile
      ```

   d. Add the following content:
      ```
      export JAVA_HOME=/root/jdk1.8.0_321
      export PATH=$JAVA_HOME/bin:$PATH
      ```
      Change **/root/jdk1.8.0_321** to the path where you install JDK.

   e. Press **Esc**. Enter the following line and press **Enter**. Save the **.bash_profile** file and exit.
      ```
      :wq
      ```

   f. Run the following command to make the change take effect:
      ```
      source .bash_profile
      ```

   g. Check whether the JDK is installed.
      ```
      java -version
      ```
      If the following message is returned, the JDK is installed.
      ```
      java version "1.8.0_321"
      ```

4. Download an open-source Kafka client.
   ```
   wget https://archive.apache.org/dist/kafka/2.7.2/kafka_2.12-2.7.2.tgz
   ```

5. Run the following command to decompress the package:
   ```
   tar -zxf kafka_2.12-2.7.2.tgz
   ```

----End

Step 2: Create a Kafka Instance

Step 1 Go to the **Buy Instance page**.

Step 2 On the **Quick Config** tab page, set basic instance configurations shown in **Figure 1-2**. **Table 1-2** lists the configuration details.

Table 1-2 Setting basic instance configurations

Parameter	Description
Billing Mode	Select **Pay-per-use**, which is a postpaid mode. You can pay after using the service, and will be billed for your usage duration. The fees are calculated in seconds and settled by hour.
Region	DMS for Kafka in different regions cannot communicate with each other over an intranet. Select a nearest location for low latency and fast access. Select AP-Singapore.
AZ	An AZ is a physical region where resources use independent power supply and networks. AZs are physically isolated but interconnected through an internal network. Select **AZ1**, **AZ2**, and **AZ3**.

Figure 1-2 Setting basic instance configurations

Step 3 Set the instance specifications and storage space, as shown in **Figure 1-3**. For details, see **Table 1-3**.

Table 1-3 Setting the instance specifications and storage space

Parameter	Description
Bundle	Choose **Recommended** > **Starter**. This entry level can be managed, compatible with open-source Kafka. Ideal for cost-sensitive services or test environments that are tolerant to limited performance and latency.
Storage Space per Broker	Select the disk type and specify the disk size as required. Total storage space = Storage space per broker × Broker quantity. After the instance is created, you cannot change the disk type. Select **Ultra-high I/O** and enter **100**.

**Figure 1-3** Setting the instance specifications and storage space
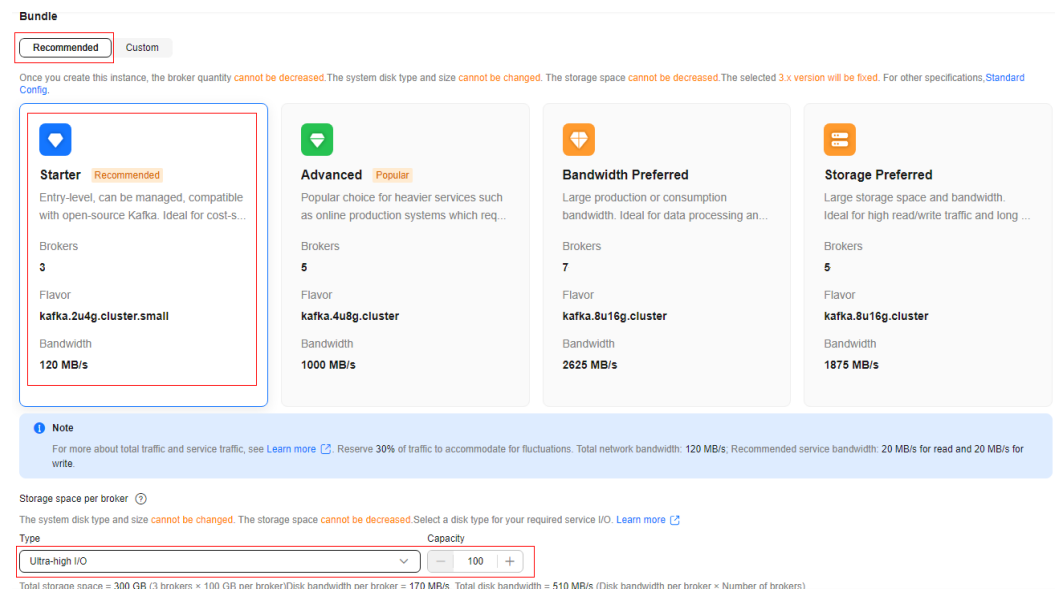
Step 4 Configure the instance network as shown in **Figure 1-4**. For details, see **Table 1-4**.

Table 1-4 Configuring instance network

Parameter	Description
VPC	After the Kafka instance is created, its VPC cannot be changed. Select the VPC prepared in **Step 3**.
Subnet	After the Kafka instance is created, its subnet cannot be changed. Select the subnet prepared in **Step 3**.
Security Group	Select the security group prepared in **Step 4**.

Figure 1-4 Configuring instance network
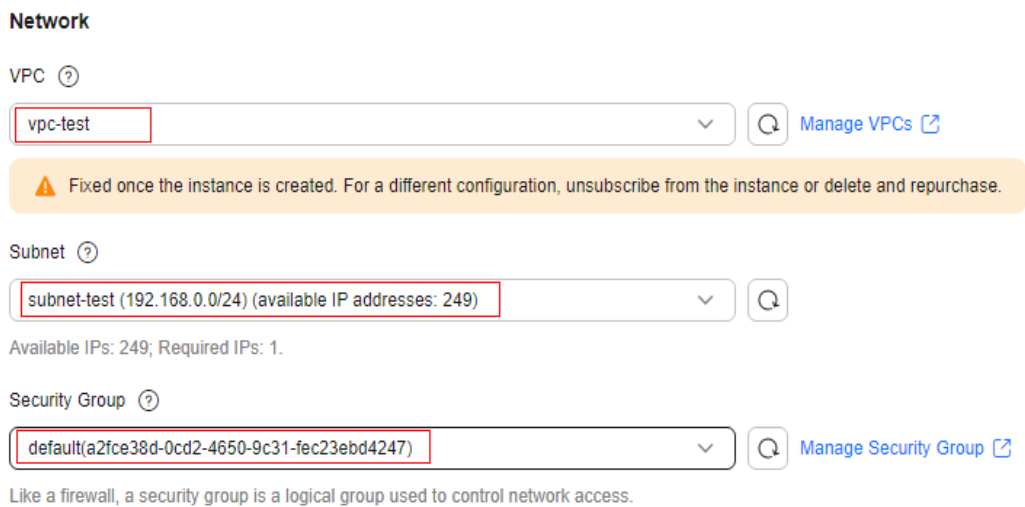
Step 5 Set the instance access mode, as shown in **Figure 1-5**. For details, see **Table 1-5**.

Table 1-5 Configuring the instance access mode

Parameter	Sub-Parameter	Description
Private Network Access	Access Mode	Select **Ciphertext Access**: Clients access a Kafka instance with SASL authentication.
	Security Protocol	Select **SASL_SSL**: SASL is used for authentication. Data is encrypted with an SSL certificate for high-security transmission.
	Private IP Addresses	Select **Auto**: The system automatically assigns IP addresses from the subnet.
	SSL Username	Enter **test**. The username cannot be changed once ciphertext access is enabled. A username should contain 4 to 64 characters, start with a letter, and contain only letters, digits, hyphens (-), and underscores (_).
	Password	A password must meet the following requirements: ● Contains 8 to 32 characters. ● Contains at least three types of the following characters: uppercase letters, lowercase letters, digits, and special characters `~!@#$%^&*()-_=+|[{}];:'",<.>? and spaces, and cannot start with a hyphen (-). ● Cannot be the username spelled forwards or backwards.

Parameter	Sub-Parameter	Description
	SASL/PLAIN	Check **SASL PLAIN**. The SASL/PLAIN setting cannot be changed once ciphertext access is enabled. Enabling SASL/PLAIN supports both SCRAM-SHA-512 (enabled by default) and PLAIN.
Public Network Access	-	Skip it.

Figure 1-5 Configuring the instance access mode

Step 6 Configure **Advanced Settings**, as shown in **Figure 1-6**. For details, see **Table 1-6**. Retain default settings for other parameters.

Table 1-6 Configuring instance advanced settings

Parameter	Description
Instance Name	You can customize a name that complies with the rules: 4–64 characters; starts with a letter; can contain only letters, digits, hyphens (-), and underscores (_). Enter **kafka-test**.

Parameter	Description
Enterprise Project	This parameter is for enterprise users. An enterprise project manages project resources in groups. Enterprise projects are logically isolated. Select **default**.
Capacity Threshold Policy	Select **Automatically delete**: When the disk reaches the disk capacity threshold (95%), messages can still be produced and consumed, but the earliest 10% of messages will be deleted to ensure sufficient disk space. Use this policy for services intolerant of interruptions. However, data may be lost.

Figure 1-6 Configuring instance advanced settings
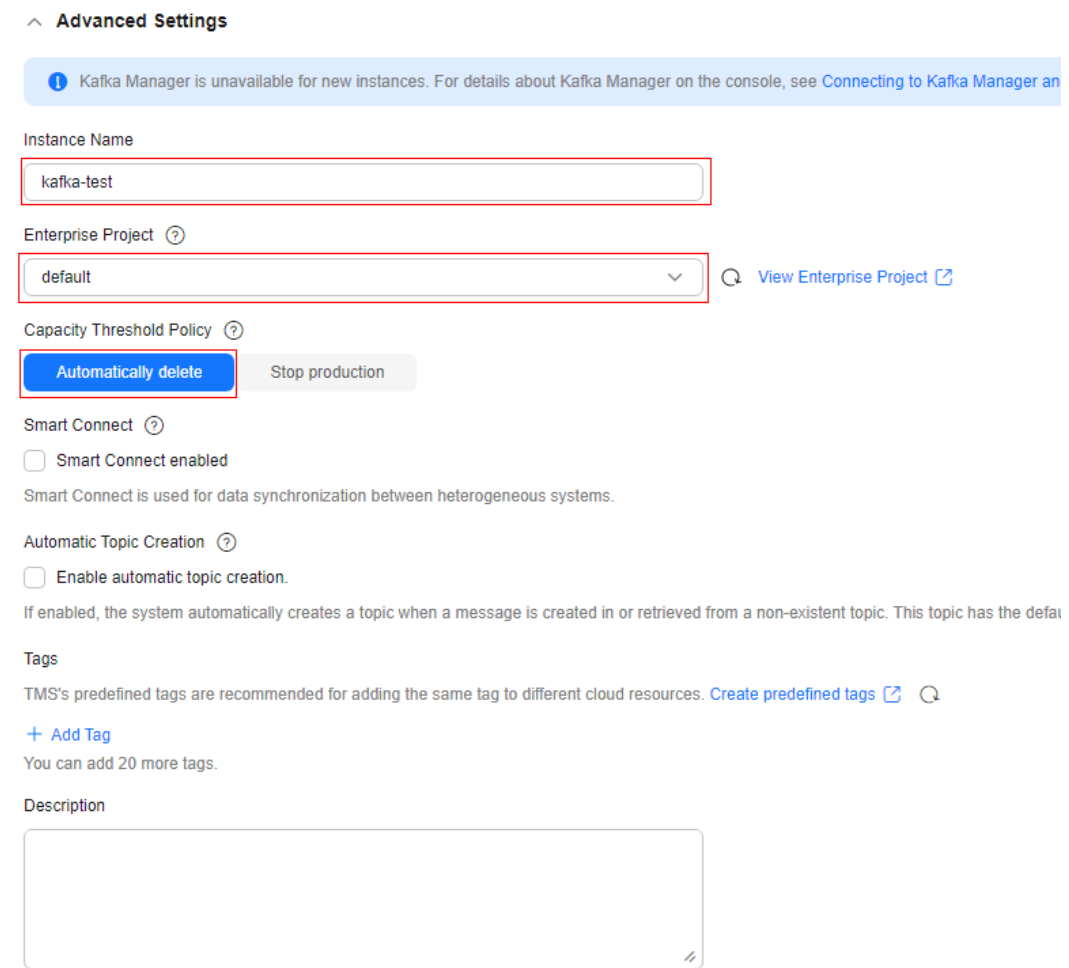
Step 7   Click **Confirm**.

Step 8   Confirm the instance information, read and agree to the *Huawei Cloud Customer Agreement*, and then submit the request.

Step 9   Click **Back to Kafka Instance List** and check whether the instance has been created.

It takes 3 to 15 minutes to create an instance. During this period, the instance status is **Creating**.

- If the instance is created successfully, its status changes to **Running**.
- If the instance is in the **Failed** state, delete it and try creating another one. If the instance creation fails again, contact customer service.
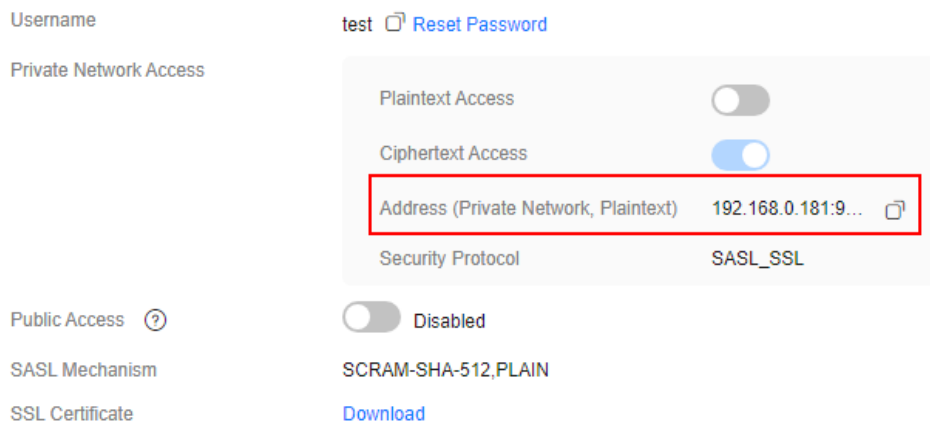
📖 **NOTE**

Instances that fail to be created do not occupy other resources.

Step 10 After the instance is created, click its name to go to the instance details page.

Step 11 In the **Connection** area, view and record the connection address.

Figure 1-7 Kafka instance addresses (private network) for intra-VPC access

----End

Step 3: Create a Topic

Step 1 On the **Kafka Instances** page, click a Kafka instance.

Step 2 In the navigation pane, choose **Topics**.

Step 3 Click **Create Topic**.

Step 4 Enter the topic name, specify other parameters by referring to **Table 1-7**, and click **OK**.

Table 1-7 Topic parameters

Parameter	Description
Topic Name	Customize a name that contains 3 to 200 characters, starts with a letter or underscore (_), and contains only letters, digits, periods (.), hyphens (-), and underscores (_). The name must be different from preset topics: ● __consumer_offsets ● __transaction_state ● __trace ● __connect-status ● __connect-configs ● __connect-offsets Cannot be changed once the topic is created. Enter **topic-01**.
Partitions	If the number of partitions is the same as that of consumers, the larger the partitions, the higher the consumption concurrency. Enter **3**.
Replicas	Data is automatically backed up to each replica. When one Kafka broker becomes faulty, data is still available. A higher number of replicas delivers higher reliability. Enter **3**.
Aging Time (h)	How long messages will be preserved in the topic. Messages older than this period cannot be consumed. They will be deleted, and can no longer be consumed. Enter **72**.
Synchronous Replication	Skip it. When this option is disabled, leader replicas are independent from follower replica synchronization. They receive messages and write them to local logs, then immediately send the successfully written ones to the client.
Synchronous Flushing	Skip it. When this option is disabled, messages are produced and stored in memory instead of written to the disk immediately.
Message Timestamp	Select **CreateTime**: time when the producer created the message.
Max. Message Size (bytes)	Maximum batch processing size allowed by Kafka. If message compression is enabled in the client configuration file or code of producers, this parameter indicates the size after compression. Enter **10,485,760**.

Parameter	Description
Description	Skip it.

Figure 1-8 Creating a topic

----**End**

Step 4: Connect to a Kafka Instance to Produce and Consume Messages

Step 1 Prepare the file for production and consumption configuration.

1. Log in to a Linux ECS.

2. Download the **client.jks** certificate and upload it to the **/root** directory on the ECS.

To obtain the certificate: On the Kafka console, click the Kafka instance to go to the **Basic Information** page. Click **Download** next to **SSL Certificate** in the **Connection** area. Decompress the package to obtain the client certificate file **client.jks**.

📖 NOTE

/root is the path for storing the certificate. Change it to the actual path if needed.

3. Go to the **/config** directory on the Kafka client.
```
cd kafka_2.12-2.7.2/config
```

4. Add the following commands in both the **consumer.properties** and **producer.properties** files (PLAIN is used as an example).
```
sasl.jaas.config=org.apache.kafka.common.security.plain.PlainLoginModule required \
username="**********" \
password="**********";
sasl.mechanism=PLAIN

security.protocol=SASL_SSL
ssl.truststore.location={ssl_truststore_path}
ssl.truststore.password=dms@kafka
ssl.endpoint.identification.algorithm=
```

Description:

- **username** and **password** are specified when enabling ciphertext access during instance creation.

- **ssl.truststore.location** is the path for storing the certificate obtained in **Step 1.2**.

- **ssl.truststore.password** is certified by the server, which must be set to **dms@kafka** and cannot be changed.

- **ssl.endpoint.identification.algorithm** decides whether to verify the certificate domain name. In this example, **leave this parameter blank, which indicates disabling domain name verification**.

Step 2 Go to the **/bin** directory on the Kafka client.
```
cd ../bin
```

Step 3 Produce messages.
```
./kafka-console-producer.sh --broker-list ${connection address} --topic ${topic name} --producer.config ../config/producer.properties
```

Description:

- *{connection address}*: the connection address obtained in **Step 11**

- *{topic name}*: the topic name obtained in **Step 4**

For example, **192.xxx.xxx.xxx:9093**, **192.xxx.xxx.xxx:9093**, **192.xxx.xxx.xxx:9093** are the connection addresses of the Kafka instance.

After running this command, you can send messages to the Kafka instance by entering the information as prompted and pressing **Enter**. Each line of content will be sent as a message.

```
[root@ecs-kafka bin]#./kafka-console-producer.sh --broker-list
192.xxx.xxx.xxx:9093,192.xxx.xxx.xxx:9093,192.xxx.xxx.xxx:9093  --topic topic-01 --producer.config ../config/
producer.properties
>Hello
>DMS
>Kafka!
>^C[root@ecs-kafka bin]#
```

Press **Ctrl+C** to cancel.

Step 4 Consume messages.

```
./kafka-console-consumer.sh --bootstrap-server ${connection address} --topic ${topic name} --from-beginning  --consumer.config ../config/consumer.properties
```

Description:

- *{connection address}*: the connection address obtained in **Step 11**
- *{topic name}*: the topic name obtained in **Step 4**

Sample:

```
[root@ecs-kafka bin]#  ./kafka-console-consumer.sh --bootstrap-server
192.xxx.xxx.xxx:9093,192.xxx.xxx.xxx:9093,192.xxx.xxx.xxx:9093 --topic topic-01 --from-beginning --consumer.config ../config/consumer.properties
Hello
Kafka!
DMS
^CProcessed a total of 3 messages
[root@ecs-kafka bin]#
```

Press **Ctrl+C** to cancel.

----End

Related Information

- Learn more about the **basic concepts of Kafka**.
- Learn more about **Distributed Message Service for Kafka Pricing**.
- To view messages on the console, see **Viewing Kafka Messages**.
- To view consumption offsets, see **Viewing and Resetting Kafka Consumption Offsets**.
- To view monitoring metrics of a Kafka instance, see **Viewing Kafka Monitoring Metrics**.

2 Common Practices

You can use the common practices provided by DMS for Kafka to meet your service requirements.

Table 2-1 Common practices

Practice	Description
Using MirrorMaker to Synchronize Data Across Clusters	MirrorMaker can synchronize data from the source cluster to the target cluster.
Configuring an Alarm Rule for Accumulated Messages	Configure an alarm rule so that the SMN service will notify you by SMS or email when the number of accumulated messages in a consumer group exceeds the threshold.