

# Distributed Message Service for Kafka

## Pasos iniciales

Edición 01  
Fecha 2023-04-26




**Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2023. Todos los derechos reservados.**

Quedan terminantemente prohibidas la reproducción y/o la divulgación totales y/o parciales del presente documento de cualquier forma y/o por cualquier medio sin la previa autorización por escrito de Huawei Cloud Computing Technologies Co., Ltd.

## **Marcas registradas y permisos**



El logotipo  y otras marcas registradas de Huawei pertenecen a Huawei Technologies Co., Ltd. Todas las demás marcas registradas y los otros nombres comerciales mencionados en este documento son propiedad de sus respectivos titulares.

## **Aviso**

Es posible que la totalidad o parte de los productos, las funcionalidades y/o los servicios que figuran en el presente documento no se encuentren dentro del alcance de un contrato vigente entre Huawei Cloud y el cliente. Las funcionalidades, los productos y los servicios adquiridos se limitan a los estipulados en el respectivo contrato. A menos que un contrato especifique lo contrario, ninguna de las afirmaciones, informaciones ni recomendaciones contenidas en el presente documento constituye garantía alguna, ni expresa ni implícita.

Huawei está permanentemente preocupada por la calidad de los contenidos de este documento; sin embargo, ninguna declaración, información ni recomendación aquí contenida constituye garantía alguna, ni expresa ni implícita. La información contenida en este documento se encuentra sujeta a cambios sin previo aviso.

---

# Índice

---

<b>1</b>	<b>Introducción.....</b>	<b>1</b>
<b>2</b>	<b>Paso 1: Preparar el entorno.....</b>	<b>3</b>
<b>3</b>	<b>Paso 2: Crear una instancia de Kafka.....</b>	<b>6</b>
<b>4</b>	<b>(Opcional) Paso 3: Crear un tema.....</b>	<b>11</b>
<b>5</b>	<b>Paso 4: Conectarse a una instancia de Kafka para crear y recuperar mensajes.....</b>	<b>13</b>
5.1	Conexión a una instancia sin SASL.....	13
5.2	Conexión a una instancia con SASL.....	15
<b>6</b>	<b>Paso 5: Configurar reglas de alarma.....</b>	<b>20</b>

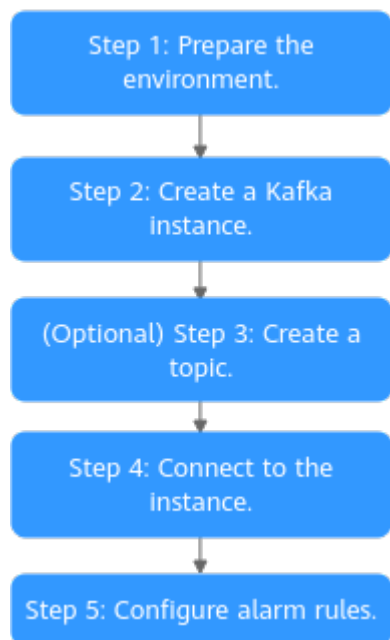
# 1 Introducción

Este documento proporciona las instrucciones para comenzar a usar Distributed Message Service (DMS) for Kafka, incluida la creación de una instancia de Kafka en la consola y la conexión a una instancia de Kafka por un Elastic Cloud Server (ECS).

También puede [crear una instancia de Kafka invocando a una API](#) y [conectarse a la instancia en su código de servicio](#).

## Procedimiento

**Figura 1-1** Procedimiento para usar DMS for Kafka



### 1. Preparar el entorno.

Una instancia de Kafka se ejecuta en una nube privada virtual (VPC). Antes de crear una instancia de Kafka, asegúrese de que una VPC esté disponible.

Después de crear una instancia de Kafka, descargue e instale el cliente de código abierto de Kafka en su ECS antes de crear y recuperar mensajes.

2. **Crear una instancia de Kafka.**

Al crear una instancia, puede elegir si desea habilitar SASL. Si SASL está habilitado, los datos se cifran para su transmisión, lo que mejora la seguridad de los datos. El ajuste de SASL solo se puede configurar cuando se crea una instancia. Después de crear una instancia, no se puede cambiar el ajuste de SASL.

3. (Opcional) **Crear un tema.**

Si la creación automática de temas no está habilitada durante la creación de instancias de Kafka, debe crear manualmente los temas para crear y recuperar mensajes.

4. Conectarse a la instancia.

Puede conectarse a una instancia de Kafka con o sin SASL.

- **Sin SASL:** Soporta el acceso a red privada y el acceso a red pública.
- **Con SASL:** Soporta el acceso a red privada y el acceso a red pública.

5. **Configurar reglas de alarma.**

Configure las reglas de alarma para una instancia de Kafka para supervisar el estado de ejecución del servicio.

 **NOTA**

Para obtener detalles sobre los conceptos de Kafka, consulte [Conceptos básicos](#).

# 2 Paso 1: Preparar el entorno

## VPC

Una VPC proporciona una red virtual aislada para sus instancias de Kafka. Puede configurar y gestionar la red según sea necesario.

**Paso 1** Antes de crear una instancia de Kafka, asegúrese de que una VPC y una subred estén disponibles.

Para obtener más información, consulte la sección [Creación de una VPC](#). Si ya tiene una VPC y una subred disponibles, no es necesario crear otras nuevas.

Tenga en cuenta lo siguiente al crear una VPC y una subred:

- La VPC y la instancia de Kafka deben estar en la misma región.
- Utilice la configuración predeterminada al crear una VPC y una subred.
- Utilice una subred que no esté habilitada con IPv6. El acceso público a la instancia no estará disponible si la instancia de Kafka está en una subred habilitada con IPv6.

**Paso 2** Antes de crear una instancia de Kafka, asegúrese de que hay un grupo de seguridad disponible.

Para obtener más información, consulte la sección [Creación de un grupo de seguridad](#). Si ya tiene un grupo de seguridad disponible, no es necesario crear uno nuevo.

Tenga en cuenta lo siguiente al crear un grupo de seguridad:

- Establezca **Template** en **Custom**.
- Para usar las instancias de Kafka, agregue las reglas de grupo de seguridad descritas en [Tabla 2-1](#). Se pueden agregar otras reglas en función de los requisitos del sitio.

**Tabla 2-1** Reglas de grupos de seguridad

Dirección	Protocolo	Puerto	Origen	Descripción
Inbound	TCP	9094	0.0.0.0/0	Acceda a Kafka a través de la red pública (sin cifrado SSL).

Dirección	Protocolo	Puerto	Origen	Descripción
Inbound	TCP	9092	0.0.0.0/0	Acceda a Kafka dentro de una VPC (sin encriptación SSL).
Inbound	TCP	9095	0.0.0.0/0	Acceda a Kafka a través de la red pública (con cifrado SSL).
Inbound	TCP	9093	0.0.0.0/0	Acceda a Kafka dentro de una VPC (con encriptación SSL).
Inbound	TCP	9999	0.0.0.0/0	Acceda a Kafka Manager.

 **NOTA**

Después de crear un grupo de seguridad, tiene una regla de entrada predeterminada que permite la comunicación entre los ECS dentro del grupo de seguridad y una regla de salida predeterminada que permite todo el tráfico de salida. Si accede a su instancia de Kafka dentro de una VPC, no es necesario agregar las reglas descritas en [Tabla 2-1](#).

---Fin

## (Opcional) EIP

Para acceder a una instancia de Kafka a través de una red pública, prepare una dirección IP elástica (EIP) por adelantado.


Para obtener más información, consulte la sección [Asignación de una EIP](#).

Tenga en cuenta lo siguiente al crear las EIP:

- Las EIP deben crearse en la región en la que se encuentra la instancia de Kafka.
- El número de EIP debe ser el mismo que el número de brokers de la instancia de Kafka.
- **La consola de Kafka no puede identificar las EIP de IPv6.**

## ECS

Antes de conectarse a una instancia de Kafka, asegúrese de haber comprado un ECS, instalado el JDK, configurado las variables de entorno y descargado un cliente de Kafka de código abierto. Los siguientes pasos describen cómo completar estas preparaciones. Un ECS de Linux se toma como ejemplo. Para obtener más información sobre cómo instalar JDK y configurar las variables de entorno para un ECS de Windows, busque en Internet.

**Paso 1** Inicie sesión en la consola de gestión. En la esquina superior izquierda, pase el puntero del mouse sobre . En **Compute**, haga clic en **Elastic Cloud Server** y, a continuación, cree un ECS.

Para más detalles, véase la sección [Compra de un ECS](#). Si ya tiene un ECS disponible, omite este paso.

**Paso 2** Inicie sesión en el ECS.

**Paso 3** Instale JDK o JRE y agregue el siguiente contenido a `.bash_profile` en el directorio principal para configurar las variables de entorno `JAVA_HOME` y `PATH`. En este comando, `/opt/java/jdk1.8.0_151` es la ruta de instalación del JDK. Cámbielo a la ruta donde instale JDK o JRE.

```
export JAVA_HOME=/opt/java/jdk1.8.0_151
export PATH=$JAVA_HOME/bin:$PATH
```

Ejecute el comando `source.bash_profile` para que la modificación surta efecto.

#### NOTA

Utilice JDK de Oracle en lugar del JDK predeterminado de ECS (por ejemplo, OpenJDK), porque el JDK predeterminado de ECS puede que no sea adecuado. Obtenga Oracle JDK 1.8.111 o posterior desde el [sitio web oficial de Oracle](#).

**Paso 4** Descargue un cliente de Kafka de código abierto.

Si la versión de la instancia de Kafka es 1.1.0, descargue el cliente en [https://archive.apache.org/dist/kafka/1.1.0/kafka\\_2.11-1.1.0.tgz](https://archive.apache.org/dist/kafka/1.1.0/kafka_2.11-1.1.0.tgz).

```
wget https://archive.apache.org/dist/kafka/1.1.0/kafka_2.11-1.1.0.tgz
```

Si la versión de la instancia de Kafka es 2.3.0, descargue el cliente en [https://archive.apache.org/dist/kafka/2.3.0/kafka\\_2.11-2.3.0.tgz](https://archive.apache.org/dist/kafka/2.3.0/kafka_2.11-2.3.0.tgz).

```
wget https://archive.apache.org/dist/kafka/2.3.0/kafka_2.11-2.3.0.tgz
```

Si la versión de la instancia de Kafka es 2.7, descargue el cliente en [https://archive.apache.org/dist/kafka/2.7.2/kafka\\_2.12-2.7.2.tgz](https://archive.apache.org/dist/kafka/2.7.2/kafka_2.12-2.7.2.tgz).

```
wget https://archive.apache.org/dist/kafka/2.7.2/kafka_2.12-2.7.2.tgz
```

**Paso 5** Ejecute el siguiente comando para descomprimir el paquete:

```
tar -zxvf ${kafka_tar}
```

En el comando anterior, `kafka_tar` indica el nombre del paquete de cliente. Por ejemplo:

```
tar -zxvf kafka_2.12-2.7.2.tgz
```

---Fin

## Acciones de seguimiento

### [Paso 2: Crear una instancia de Kafka](#)



# 3 Paso 2: Crear una instancia de Kafka

---

## Requisitos previos

Asegúrese de que hay una VPC disponible. Para obtener más información sobre cómo crear una VPC, consulte la [Guía del usuario de Virtual Private Cloud](#).

Si ya tiene una VPC disponible, no es necesario crear una nueva.

## Procedimiento

**Paso 1** Inicie sesión en la [consola de Kafka](#) y haga clic en **Buy Instance** en la esquina superior derecha.

**Paso 2** Seleccione un modo de facturación.

**Paso 3** Seleccione una región más cercana a su aplicación para reducir la latencia y acelerar el acceso.

**Paso 4** Seleccione un proyecto en la lista desplegable.

**Paso 5** Seleccione una AZ o al menos tres AZ.

**Paso 6** Especifique el nombre de instancia y el proyecto de empresa.

**Paso 7** Configure los siguientes parámetros de instancia:

1. **Version:** Actualmente, Kafka v1.1.0, v2.3.0, and v2.7 son compatibles. Se recomienda v2.3.0. v2.7 está disponible solo en las regiones CN East-Shanghai1, CN South-Guangzhou, y CN-Hong Kong.
2. **CPU Architecture:** Actualmente, solo se admite la arquitectura x86.
3. Actualmente, hay dos tipos de normas de instancia dependiendo de la región.
  - En regiones distintas de CN East-Shanghai1, CN North-Beijing4, CN South-Guangzhou, AP-Singapore, LA-Mexico City2, LA-Santiago, y AF-Johannesburg, seleccionan un ancho de banda basado en el tráfico de servicio.

Puede ver la cantidad y la norma de ECS, el número máximo de particiones permitidas y el número de grupos de consumidores recomendados para cada opción de ancho de banda.

El parámetro **Maximum Partitions** indica el número máximo de particiones que se pueden crear para una instancia de Kafka. Si la cantidad total de particiones de todos los temas excede este umbral, la creación de temas fallará.

- En las regiones CN East-Shanghai1, CN North-Beijing4, CN South-Guangzhou, AP-Singapore, LA-Mexico City2, LA-Santiago y AF-Johannesburg, seleccionan una norma de corredor basado en los requisitos de servicio. Para **Brokers**, especifique la cantidad de corredor.

Número máximo de particiones por corredores x Número de corredores = Número máximo de particiones de una instancia. Si el número total de particiones de todos los temas excede el número máximo de particiones permitidas para una instancia, la creación del tema fallará.

4. **Storage Space:** espacio total en disco para almacenar los datos de instancia.

El espacio de almacenamiento es el espacio total que consumen todas las réplicas. Especifique el espacio de almacenamiento en función del tamaño esperado del mensaje de servicio y el número de réplicas. Por ejemplo, si el tamaño de disco necesario para almacenar los datos durante el período de retención es de 100 GB, la capacidad del disco debe ser como mínimo: 100 GB x Número de réplicas + 100 GB (reservado).

Los discos se formatean cuando se crea una instancia. Como resultado, el espacio disponible real en disco es del 93% al 95% del espacio total en disco.

- Ancho de banda de 100 MB/s: el rango de valor del **Storage Space** es de 600 - 90,000 GB.
- Ancho de banda de 300 MB/s: el rango de valor del **Storage Space** es de 1200 - 90,000 GB.
- Ancho de banda de 600 MB/s: el rango de valor del **Storage Space** es de 2400 - 90,000 GB.
- Ancho de banda de 1200 MB/s: el rango de valor del **Storage Space** es de 4800 - 90,000 GB.

 **NOTA**

- E/S alta + ancho de banda de 100 MB/s: Si el tamaño promedio del mensaje es de 1 KB, las transacciones por segundo (TPS) pueden alcanzar 100,000 en escenarios de alto rendimiento y 60,000 en escenarios de replicación síncrona.
- E/S alta + ancho de banda de 300 MB/s: Si el tamaño promedio del mensaje es de 1 KB, el TPS puede alcanzar 300,000 en escenarios de alto rendimiento y 150,000 en escenarios de replicación síncrona.
- E/S ultra alta + ancho de banda de 100 MB/s: Si el tamaño promedio del mensaje es de 1 KB, el TPS puede alcanzar 100,000 en escenarios de alto rendimiento y 80,000 en los escenarios de replicación síncrona.
- E/S ultra alta + ancho de banda de 300 MB/s: Si el tamaño promedio del mensaje es de 1 KB, el TPS puede alcanzar 300,000 en escenarios de alto rendimiento y 200,000 en los escenarios de replicación síncrona.
- E/S ultra alta + ancho de banda de 600 MB/s: Si el tamaño promedio del mensaje es de 1 KB, el TPS puede alcanzar 600,000 en escenarios de alto rendimiento y 300,000 en los escenarios de replicación síncrona.
- E/S ultra alta + ancho de banda de 1200 MB/s: Si el tamaño promedio del mensaje es de 1 KB, el TPS puede alcanzar 1,200,000 en escenarios de alto rendimiento y 400,000 en los escenarios de replicación síncrona.

5. **Capacity Threshold Policy:** política utilizada cuando el uso del disco alcanza el umbral. El umbral de capacidad predeterminado es 95%.

- **Automatically delete:** Los mensajes se pueden crear y recuperar, pero el 10% de los mensajes más antiguos se eliminarán para garantizar suficiente espacio en disco. Esta política es adecuada para los escenarios en los que no se puede tolerar ninguna interrupción del servicio. Los datos pueden perderse.

- **Stop production:** no se pueden crear nuevos mensajes, pero los mensajes existentes aún se pueden recuperar. Esta política es adecuada para escenarios en los que no se puede tolerar ninguna pérdida de datos.

6. Seleccione una VPC y una subred.

Una VPC proporciona una red virtual aislada para sus instancias de Kafka. Puede configurar y gestionar la red según sea necesario.

**NOTA**

Después de crear la instancia de Kafka, su VPC y subred no se pueden cambiar.

7. Seleccione un grupo de seguridad.

Un grupo de seguridad es un conjunto de reglas que controlan el acceso a Elastic Cloud Servers (ECSs). Proporciona políticas de acceso para ECSs de confianza mutua con los mismos requisitos de protección de seguridad en la misma VPC.

Puede hacer clic en **Manage Security Group** para ver o crear grupos de seguridad en la consola de red.

**Figura 3-1** Comprar una instancia de Kafka

The screenshot shows the configuration interface for purchasing a Kafka instance. It includes the following sections:

- Version:** Radio buttons for 2.3.0 (selected) and 1.1.0.
- CPU Architecture:** Radio button for x86 (selected).
- Specifications:** A table with columns: Bandwidth (MB/s), Number of Nodes, ECS Flavor, Maximum Partitions, and Recommended Consumer Group.
 

	Bandwidth (MB/s)	Number of Nodes	ECS Flavor	Maximum Partitions	Recommended Consumer G...
<input checked="" type="radio"/>	100	3	c6.large.2	300	60
<input type="radio"/>	300	3	c6.xlarge.2	900	300
<input type="radio"/>	600	4	c6.2xlarge.2	1,800	600
<input type="radio"/>	1,200	8	c6.2xlarge.2	1,800	600
- Storage Space:** A dropdown menu set to 'Ultra-high I/O' and a numeric input set to '600' GB.
- Capacity Threshold Policy:** Radio buttons for 'Automatically delete' (selected) and 'Stop production'.
- VPC:** Two dropdown menus, the first set to 'vpc-kafka' and the second to 'subnet-kafka'.
- Security Group:** A dropdown menu set to 'Sys-default'.

**Paso 8** Configure los parámetros de red de instancia.

1. Seleccione una VPC y una subred.

**NOTA**

Después de crear la instancia de Kafka, su VPC y subred no se pueden cambiar.

2. Seleccione un grupo de seguridad.

Un grupo de seguridad es un conjunto de reglas para acceder a una instancia de Kafka. Puede hacer clic en **Manage Security Group** para ver o crear grupos de seguridad en la consola de red.

**Paso 9** Configure el nombre de usuario y la contraseña para iniciar sesión en Kafka Manager. **El nombre de usuario de Kafka Manager no se puede cambiar una vez que se crea una instancia.**

Kafka Manager es una herramienta de código abierto para la gestión de clústeres de Kafka. Después de crear una instancia de Kafka, puede ir a la página de detalles de la instancia para obtener la dirección para iniciar sesión en Kafka Manager. En Kafka Manager, puede ver las estadísticas de monitoreo y la información del broker de sus clústeres de Kafka.

**Paso 10** Seleccione la duración deseada.

Este parámetro solo se muestra si el modo de facturación es anual/mensual.

**Paso 11** Haga clic en **More Settings** para configurar más parámetros.

1. Configure **Public Access**.

El acceso público está deshabilitado de forma predeterminada. Puede activarla o mantenerla deshabilitada según sea necesario. Una vez habilitado el acceso público, configure un IPv4 EIP para cada broker.

**Figura 3-2** Configuración del acceso público



#### **NOTA**

El acceso público es compatible en la región AP-Jakarta.

2. Configure **Kafka SASL\_SSL**.

Este parámetro indica si se debe habilitar la autenticación SSL cuando un cliente se conecta a la instancia. Si habilita **Kafka SASL\_SSL**, los datos se cifrarán antes de la transmisión para mejorar la seguridad.

**Esta configuración no se puede cambiar después de crear la instancia.** Si desea utilizar una configuración SASL\_SSL diferente después de crear la instancia, debe crear una nueva instancia.

Si habilita **Kafka SASL\_SSL**, también debe establecer el nombre de usuario y la contraseña para acceder a la instancia.

3. Configure **Automatic Topic Creation**.

Esta configuración está deshabilitada de forma predeterminada. Puede activarlo o desactivarlo según sea necesario.

Si se habilita la creación automática de temas, el sistema crea automáticamente un tema cuando se crea o se recupera un mensaje de un tema que no existe. Este tema tiene la siguiente configuración predeterminada: 3 particiones, 3 réplicas, tiempo de caducidad 72 horas y replicación y vaciado sincrónicos deshabilitados.

Después de cambiar el valor del parámetro **log.retention.hours**, **default.replication.factor** o **num.partitions**, los temas creados automáticamente posteriormente utilizan el nuevo valor. Por ejemplo, si **num.partitions** se establece en **5**, un tema creado automáticamente tendrá la siguiente configuración: 5 particiones, 3 réplicas, tiempo de envejecimiento 72 horas y replicación y vaciado sincrónicos deshabilitados.

4. Especifique las etiquetas.

Las etiquetas se utilizan para identificar los recursos de la nube. Cuando tiene muchos recursos de nube del mismo tipo, puede usar etiquetas para clasificar los recursos de nube por dimensión (por ejemplo, por uso, propietario o entorno).

- Si ha creado etiquetas predefinidas, seleccione un par predefinido de clave y valor de etiqueta. Puede hacer clic en **View predefined tags** para ir a la consola del Tag Management Service (TMS) a ver o crear etiquetas.
- También puede crear nuevas etiquetas ingresando **Tag key** y **Tag value**.

Se pueden agregar hasta 20 etiquetas a cada instancia de Kafka. Para obtener más información sobre los requisitos de etiquetas, consulte [Gestión de Etiquetas de Instancia](#).

 **NOTA**

Algunas regiones no admiten etiquetas. Para obtener más información, consulte la información que se muestra en la consola.

5. Introduzca una descripción de la instancia.

**Paso 12** Haga clic en **Buy**.

**Paso 13** Confirme la información de la instancia.

**Paso 14** Vuelva a la página **Kafka Premium** y compruebe si se ha creado la instancia.

Se tarda de 3 a 15 minutos en crear una instancia. Durante este período, el estado de la instancia es **Creating**.

- Si la instancia se crea correctamente, su estado cambia a **Running**.
- Si no se puede crear la instancia, vea **Instance Creation Failures**. Elimine la instancia y cree otra instancia. Si la creación de la instancia falla de nuevo, póngase en contacto con el servicio de atención al cliente.

 **NOTA**

Las instancias que no se crean no ocupan otros recursos.

----**Fin**

## Acciones de seguimiento

[\(Opcional\) Paso 3: Crear un tema](#)

# 4 (Opcional) Paso 3: Crear un tema

Un tema es un flujo de mensajes. Si la creación automática de temas no está habilitada durante la creación de instancias de Kafka, debe crear manualmente temas para crear y recuperar mensajes. Si se habilita la creación automática de temas, este paso es opcional. El sistema crea automáticamente un tema cuando se crea un mensaje. Este tema tiene la siguiente configuración predeterminada: 3 particiones, 3 réplicas, tiempo de caducidad 72 horas y replicación y vaciado sincrónicos deshabilitados.

A continuación se describen tres métodos para crear manualmente un tema.

- **Método 1: Creación de un tema en la consola**
- **Método 2: Creación de un tema en Kafka Manager**
- **Método 3: Creación de un tema mediante la CLI de Kafka**

## Método 1: Creación de un tema en la consola

**Paso 1** Inicie sesión en la **consola de Kafka** y seleccione la región donde se encuentra la instancia de Kafka.

**Paso 2** Haga clic en una instancia de Kafka.

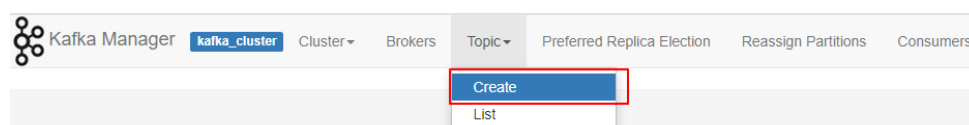
**Paso 3** En la página de ficha **Topics**, haga clic en **Create Topic**.

**Paso 4** Escriba el nombre del tema, especifique otros parámetros y haga clic en **OK**.

----Fin

## Método 2: Creación de un tema en Kafka Manager

Inicie sesión en Kafka Manager, seleccione **Topic > Create** y establezca los parámetros según se le solicite.



#### AVISO

Si el nombre de un tema comienza con un carácter especial, por ejemplo, no se puede mostrar un signo numérico (#), datos de supervisión.

### Método 3: Creación de un tema mediante la CLI de Kafka

Si su cliente es v2.2 o posterior, puede usar **kafka-topics.sh** para crear temas y gestionar parámetros de temas.

#### AVISO

Si el nombre de un tema comienza con un carácter especial, por ejemplo, no se puede mostrar un signo numérico (#), datos de supervisión.

- Si SASL no está habilitado para la instancia de Kafka, ejecute el siguiente comando en el directorio */directory where the CLI is located*/**kafka\_{version}/bin/** para crear un tema:

```
./kafka-topics.sh --create --topic {topic_name} --bootstrap-server  
{broker_ip}:{port} --partitions {partition_num} --replication-factor  
{replication_num}
```

- Si se ha habilitado SASL para la instancia de Kafka, realice los siguientes pasos para crear un tema:
  - a. (Opcional) Si se ha establecido la configuración del certificado SSL, omita este paso. En caso contrario, realice las siguientes operaciones:

Cree el archivo **ssl-user-config.properties** en el directorio **/config** del cliente Kafka y agregue las configuraciones del certificado SSL haciendo referencia a [Conexión a una instancia con SASL](#).
  - b. Ejecute el siguiente comando en el directorio */directory where the CLI is located*/**kafka\_{version}/bin/** para crear un tema:

```
./kafka-topics.sh --create --topic {topic_name} --bootstrap-server  
{broker_ip}:{port} --partitions {partition_num} --replication-factor  
{replication_num} --command-config ./config/ssl-user-config.properties
```

### Acciones de seguimiento

#### [Paso 4: Conectarse a una instancia de Kafka para crear y recuperar mensajes](#)

# 5 Paso 4: Conectarse a una instancia de Kafka para crear y recuperar mensajes

## 5.1 Conexión a una instancia sin SASL

Esta sección describe cómo conectarse a una instancia de Kafka en una red privada o pública mediante una CLI, sin usar los certificados de SASL.

El acceso a la red privada y el acceso a la red pública difieren solo en las direcciones IP y los puertos de conexión. Para el acceso a la red privada, utilice el puerto 9092. Para el acceso a la red pública, utilice el puerto 9094.

A continuación se describe únicamente el procedimiento para el acceso a la red pública. Para el acceso a la red privada, reemplace las direcciones IP por las actuales.

### NOTA

Para las instancias compradas en julio de 2020 y posteriores, cada broker de Kafka permite un máximo de 1000 conexiones desde cada dirección IP de forma predeterminada. Para los casos adquiridos antes de julio de 2020, cada broker de Kafka permite un máximo de 200 conexiones desde cada dirección IP de forma predeterminada. El exceso de conexiones será rechazado. Puede cambiar el límite [modificando los parámetros de Kafka](#).

### Requisitos previos

- Ha configurado correctamente las reglas de grupo de seguridad. Para obtener más información, véase [Tabla 2-1](#).
- Se ha obtenido la dirección de conexión de instancia.
  - Para el acceso intra-VPC, utilice el puerto 9092. Obtenga la dirección de conexión de instancia en la página de detalles de instancia.

**Figura 5-1** Obtención de direcciones de conexión de instancia Kafka para el acceso intra-VPC sin SASL

Instance Address (Private Network) IPv4 192.168.0.24:9092,192.168.0.224:9092,192.168.0.197:9092 

- Para acceso público, utilice el puerto 9094. Obtenga la dirección de acceso a la instancia en la página de detalles de la instancia.



**Figura 5-2** Obtención de direcciones de conexión de instancia Kafka para acceso público sin SASL

Instance Address (Public Network) 139.196.45:9094, 10.78.42.127:9094, 10.4.49.103:9094

- Si la creación automática de temas no está habilitada para la instancia de Kafka, obtenga el nombre del tema.

Puede obtener el nombre del tema creado en **(Opcional) Paso 3: Crear un tema** en la ficha **Topics** de la instancia.

**Figura 5-3** Consulta del nombre del tema

Topic Name	Partitions	Replicas	Aging Time (h)	Synchronous Replic...	Synchronous Plus...	Operation
topic-775891784	3	3	72	No	No	Grant User Permission   Edit   More

- Ha adquirido un ECS, ha instalado el JDK, ha configurado las variables de entorno y ha descargado un cliente de Kafka. Para obtener más información, consulte **Paso 1: Preparar el entorno**.

## Creación de mensajes

Vaya al directorio **/bin** del archivo de cliente de Kafka y ejecute el siguiente comando para crear mensajes:

```
./kafka-console-producer.sh --broker-list ${connection address} --topic ${topic name}
```

Descripción de parámetros:

- *{connection-address}*: la dirección obtenida en **Requisitos previos**
- *{topic-name}*: el nombre del tema creado para la instancia de Kafka

Por ejemplo, 10.3.196.45:9094, 10.78.42.127:9094 y 10.4.49.103:9094 son las direcciones de acceso público de la instancia de Kafka.

Después de ejecutar el comando anterior, puede enviar un mensaje a la instancia de Kafka ingresando la información como se le solicite y presionando **Enter**. El contenido de cada línea se envía como un mensaje.

```
[root@ecs-kafka bin]# ./kafka-console-producer.sh --broker-list
10.3.196.45:9094,10.78.42.127:9094,10.4.49.103:9094 --topic topic-demo
>Hello
>DMS
>Kafka!
>^C[root@ecs-kafka bin]#
```

Para dejar de crear mensajes, presione **Ctrl+C** para salir.

## Recuperación de mensajes

Ejecute el siguiente comando para recuperar mensajes:

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

Descripción de parámetros:

- *{connection-address}*: la dirección obtenida en [Requisitos previos](#)
- *{topic-name}*: el nombre del tema creado para la instancia de Kafka
- *{consumer-group-name}*: el nombre del grupo de consumidores establecido en función de sus requisitos de servicio. **Si se ha especificado un nombre de grupo de consumidores en el archivo de configuración, asegúrese de utilizar el mismo nombre en la línea de comandos. De lo contrario, el consumo puede fallar.** Si el nombre de un grupo de consumidores comienza con un carácter especial, como un signo numérico (#), no se pueden mostrar los datos de supervisión.

A continuación se presenta un ejemplo:

```
[root@ecs-kafka bin]# ./kafka-console-consumer.sh --bootstrap-server
10.3.196.45:9094,10.78.42.127:9094,10.4.49.103:9094 --topic topic-demo --group
order-test --from-beginning
Kafka!
DMS
Hello
^CProcessed a total of 3 messages
[root@ecs-kafka bin]#
```

Para detener la recuperación de mensajes, presione **Ctrl+C** para salir.

## Acciones de seguimiento

Puede configurar las reglas de alarma para monitorear métricas para recibir notificaciones de manera oportuna cuando las instancias, los brokers o los temas son anormales.

### [Paso 5: Configurar reglas de alarma](#)

## 5.2 Conexión a una instancia con SASL

Esta sección describe cómo conectarse a una instancia de Kafka en una red privada o pública con una CLI y certificados de SASL.

El acceso a la red privada y el acceso a la red pública difieren solo en las direcciones IP y los puertos de conexión. Para el acceso intra-VPC, utilice el puerto 9093. Para acceso público, utilice el puerto 9095.

A continuación se describe únicamente el procedimiento para el acceso a la red pública. Para el acceso a la red privada, reemplace las direcciones IP por las actuales.

### NOTA

- Para las instancias compradas en julio de 2020 y posteriores, cada broker de Kafka permite un máximo de 1000 conexiones desde cada dirección IP de forma predeterminada. Para los casos adquiridos antes de julio de 2020, cada broker de Kafka permite un máximo de 200 conexiones desde cada dirección IP de forma predeterminada. El exceso de conexiones será rechazado. Puede cambiar el límite [modificando los parámetros de Kafka](#).

## Requisitos previos

- Ha configurado correctamente las reglas de grupo de seguridad. Para obtener más información, véase [Tabla 2-1](#).
- Se ha obtenido la dirección de conexión de instancia.
  - Para el acceso intra-VPC, utilice el puerto 9093. Obtenga la dirección de conexión de instancia en la página de detalles de instancia.

**Figura 5-4** Obtención de direcciones de conexión de instancia Kafka para el acceso intra-VPC con SASL habilitado

Instance Address (Private Network) IPv4 192.168.0.239:9093,192.168.0.182:9093,192.168.0.57:9093

- Para acceso público, utilice el puerto 9095. Obtenga la dirección de acceso a la instancia en la página de detalles de la instancia.

**Figura 5-5** Obtención de direcciones de conexión de instancia Kafka para acceso público con SASL habilitado

Instance Address (Public Network) 139.129.145:9095,122.214.119:9095,119.129:9095

- El mecanismo de SASL en uso es conocido.

En el área **Connection** de la página de detalles de la instancia de Kafka, vea **SASL Mechanism**. Si tanto SCRAM-SHA-512 como PLAIN están habilitados, configure cualquiera de ellos para conexiones. Si **SASL Mechanism** no se muestra, se utiliza PLAIN de forma predeterminada.

**Figura 5-6** Mecanismo de SASL en uso

### Connection

Username test [Reset Password](#)

Kafka SASL\_SSL Enabled **Fixed for this instance**

SASL Mechanism SCRAM-SHA-512,PLAIN

- Si la creación automática de temas no está habilitada para la instancia de Kafka, obtenga el nombre del tema.

Puede obtener el nombre del tema creado en **(Opcional) Paso 3: Crear un tema** en la ficha **Topics** de la instancia.

**Figura 5-7** Consulta del nombre del tema

Partition Usage 0.4% Maximum: 750 Used: 3 Remaining: 747

Topic Name	Partitions	Replicas	Aging Time (h)	Synchronous Replic...	Synchronous Plus...	Operation
topic-775891784	3	3	72	No	No	Grant User Permission Edit More

- Ha adquirido un ECS, ha instalado el JDK, ha configurado las variables de entorno y ha descargado un cliente de Kafka. Para obtener más información, consulte el **Paso 1: Preparar el entorno**.

## Configuración del archivo de ajuste para la creación y recuperación de mensajes

**Paso 1** Inicio de sesión en un ECS de Linux.

**Paso 2** Asigne hosts a direcciones IP en el archivo `/etc/hosts` en ECS, para que el cliente pueda analizar rápidamente los brokers de instancia.

Establezca las direcciones IP en las direcciones de conexión de instancia obtenidas en [Requisitos previos](#). Establezca hosts en los nombres de hosts de instancia. Especifique un nombre único para cada host.

Por ejemplo:

10.154.48.120 server01

10.154.48.121 server02

10.154.48.122 server03

**Paso 3** Descargue **client.truststore.jks**. En la consola de Kafka, Haga clic en la instancia. En la página de detalles de la instancia, haga clic en **Download** junto a **SSL Certificate** en el área **Connection**.

Descomprima el paquete para obtener el archivo de certificado del cliente **client.truststore.jks**.

**Paso 4** Modifique el archivo de configuración de Kafka CLI basado en el [mecanismo de SASL](#).

- **Si se usa PLAIN**, encuentre los archivos **consumer.properties** y **producer.properties** en el directorio **/config** de la CLI de Kafka y agregue el siguiente contenido a los archivos:

```
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=
```

Descripción de parámetros:

- **username** y **password**: nombre de usuario y contraseña que establece al habilitar SASL\_SSL durante la creación de una instancia de Kafka o al crear un usuario SASL\_SSL.
  - **ssl.truststore.location**: ruta de acceso para almacenar el certificado obtenido de [Paso 3](#).
  - **ssl.truststore.password**: contraseña del certificado del servidor, que debe establecerse en **dms@kafka** y no se puede cambiar.
  - **ssl.endpoint.identification.algorithm**: si se debe verificar el nombre de dominio del certificado. **Este parámetro debe dejarse en blanco, lo que indica la desactivación de la verificación del nombre de dominio.**
- **Si se usa SCRAM-SHA-512**, encuentre los archivos **consumer.properties** y **producer.properties** en el directorio **/config** de la CLI de Kafka y agregue el siguiente contenido a los archivos:

```
sasl.jaas.config=org.apache.kafka.common.security.scram.ScramLoginModule
required \
username="*****" \
password="*****";
sasl.mechanism=SCRAM-SHA-512

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

Descripción de parámetros:

- **username** y **password**: nombre de usuario y contraseña que establece al habilitar SASL\_SSL durante la creación de una instancia de Kafka o al crear un usuario SASL\_SSL.
- **ssl.truststore.location**: ruta de acceso para almacenar el certificado obtenido de [Paso 3](#).
- **ssl.truststore.password**: contraseña del certificado del servidor, que debe establecerse en **dms@kafka** y no se puede cambiar.
- **ssl.endpoint.identification.algorithm**: si se debe verificar el nombre de dominio del certificado. **Este parámetro debe dejarse en blanco, lo que indica la desactivación de la verificación del nombre de dominio.**

----Fin

## Creación de mensajes

Vaya al directorio **/bin** del archivo de cliente de Kafka y ejecute el siguiente comando para crear mensajes:

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

Descripción de parámetros:

- *{connection-address}*: la dirección obtenida en [Requisitos previos](#)
- *{topic-name}*: el nombre del tema creado para la instancia de Kafka

Por ejemplo, **10.3.196.45:9095,10.78.42.127:9095,10.4.49.103:9095** son las direcciones de conexión de la instancia de Kafka.

Después de ejecutar el comando anterior, puede enviar un mensaje a la instancia de Kafka ingresando la información como se le solicite y presionando **Enter**. El contenido de cada línea se envía como un mensaje.

```
[root@ecs-kafka bin]# ./kafka-console-producer.sh --broker-list 10.3.196.45:9095,10.78.42.127:9095,10.4.49.103:9095 --topic topic-demo --producer.config ../config/producer.properties
>Hello
>DMS
>Kafka!
>^C[root@ecs-kafka bin]#
```

Para dejar de crear mensajes, presione **Ctrl+C** para salir.

## Recuperación de mensajes

Ejecute el siguiente comando para recuperar mensajes:

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

Descripción de parámetros:

- *{connection-address}*: la dirección obtenida en [Requisitos previos](#)
- *{topic-name}*: el nombre del tema creado para la instancia de Kafka
- *{consumer-group-name}*: el nombre del grupo de consumidores establecido en función de sus requisitos de servicio. **Si se ha especificado un nombre de grupo de consumidores en el archivo de configuración, asegúrese de utilizar el mismo nombre**

**en la línea de comandos. De lo contrario, el consumo puede fallar.** Si el nombre de un grupo de consumidores comienza con un carácter especial, como un signo numérico (#), no se pueden mostrar los datos de supervisión.

A continuación se presenta un ejemplo:

```
[root@ecs-kafka bin]# ./kafka-console-consumer.sh --bootstrap-server 10.xxx.xxx.202:9095,10.xxx.xxx.197:9095,10.xxx.xxx.68:9095 --topic topic-demo --group order-test --from-beginning --consumer.config ../config/consumer.properties
Hello
Kafka!
DMS
^CProcessed a total of 3 messages
[root@ecs-kafka bin]#
```

Para detener la recuperación de mensajes, presione **Ctrl+C** para salir.

## Acciones de seguimiento

Puede configurar las reglas de alarma para monitorear métricas para recibir notificaciones de manera oportuna cuando las instancias, los brokers o los temas son anormales.

### **Paso 5: Configurar reglas de alarma**

# 6 Paso 5: Configurar reglas de alarma

Esta sección describe las reglas de alarma de algunas métricas y cómo configurarlas. En los servicios reales, se recomienda configurar las reglas de alarma para métricas basadas en las siguientes políticas de alarma.

## NOTA



**Límite superior de aproximación** en la siguiente tabla se indica si el rendimiento del recurso actual está cerca del límite superior. Si el rendimiento está cerca del límite superior, el rendimiento soportado por el recurso actual es el umbral de alarma establecido en la política de alarma. Si el rendimiento continúa aumentando, los servicios pueden volverse anormales.

**Tabla 6-1** Métricas de instancia de Kafka para configurar reglas de alarma para

Métrica	Rango normal	Política de alarmas	Límite superior de aproximación	Descripción de métrica y manejo de alarmas
Disk Capacity Usage	0 - 100	Umbral de alarma: valor original > 85 Número de períodos consecutivos: 3 Severidad de la alarma: crítica	Sí	Descripción métrica: uso del disco de la máquina virtual Kafka. Unidad: % Manejo de alarmas: cuando se genera una alarma para esta métrica, modifique el espacio de almacenamiento de la instancia. Para obtener más información, consulte <a href="#">Modificación de las especificaciones de instancias</a> .

Métrica	Rango normal	Política de alarmas	Límite superior de aproximación	Descripción de métrica y manejo de alarmas
Average Load per CPU Core	0 - 2	Umbral de alarma: valor original > 1.5 Número de períodos consecutivo s: 3 Severidad de la alarma: mayor	Sí	Descripción métrica: carga media de cada núcleo de CPU de la máquina virtual Kafka. Manejo de alarmas: Cuando se genera una alarma para esta métrica, modifique el <b>ancho de banda</b> de la instancia. Para obtener más información, consulte <a href="#">Modificación de las especificaciones de instancias</a> .
Uso de memoria	0 - 100	Umbral de alarma: valor original > 85 Número de períodos consecutivo s: 3 Severidad de la alarma: crítica	Yes	Descripción métrica: uso de memoria de la máquina virtual Kafka. Unidad: % Manejo de alarmas: Cuando se genera una alarma para esta métrica, modifique el <b>ancho de banda</b> de la instancia. Para obtener más información, consulte <a href="#">Modificación de las especificaciones de instancias</a> .

## Procedimiento

- Paso 1** Inicie sesión en la [consola de Kafka](#) y seleccione la región donde se encuentra la instancia de Kafka.
- Paso 2** Haga clic en  junto al nombre de instancia de Kafka para ir a la página de supervisión de instancia de la consola de Cloud Eye.
- Paso 3** Pase el puntero del mouse sobre una métrica y haga clic en  para crear una regla de alarma para la métrica.
- Paso 4** Especifique los detalles de la alarma.

Para obtener más información sobre cómo crear reglas de alarma, consulte [Crear reglas de alarma](#).



1. Establezca el nombre y la descripción de la alarma.
2. Especifique la política de alarma y la gravedad de la alarma.

Como se muestra en la siguiente figura, si el uso de la capacidad original del disco supera el 85% durante tres periodos consecutivos, se genera una alarma. Si la alarma no se maneja a tiempo, se envía una notificación de alarma.

**Figura 6-1** Configuración de la política de alarma y la gravedad de la alarma

\* Method Configure manually

\* Alarm Policy

Metric Name	Alarm Policy	Alarm Severity	Operation
Consumer Available ...	Raw d... 3 consecuti... >= 500 Count	One day	Major

⊕ Add Alarm Policy You can add 0 more.

3. Establezca las configuraciones de notificación de alarma. Si habilita **Alarm Notification**, establezca el período de validez, el objeto de notificación y la condición del activador.
4. Haga clic en **Create**.

----**Fin**