

Data Encryption Workshop

Guía del usuario de

Edición 19
Fecha 2024-09-13




Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. 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.

Huawei Cloud Computing Technologies Co., Ltd.

Dirección: Huawei Cloud Data Center Jiaoxinggong Road
Avenida Qianzhong
Nuevo distrito de Gui'an
Gui Zhou, 550029
República Popular China

Sitio web: <https://www.huaweicloud.com/intl/es-us/>

Índice

1 KMS Relacionados.....	1
1.1 ¿Qué es Key Management Service?.....	1
1.2 ¿Qué es una clave maestra del cliente?.....	1
1.3 ¿Qué es una clave predeterminada?.....	2
1.4 ¿Cuáles son las diferencias entre una clave personalizada y una clave predeterminada?.....	2
1.5 What Is a Data Encryption Key?.....	3
1.6 ¿Por qué no puedo eliminar un CMK inmediatamente?.....	3
1.7 ¿Qué servicios en la nube pueden usar KMS para el cifrado?.....	3
1.8 ¿Cómo servicios de Huawei Cloud utilizan KMS para cifrar datos?.....	5
1.9 ¿Cuáles son los beneficios del cifrado de sobres?.....	6
1.10 ¿Hay un límite en el número de claves personalizadas que puedo crear en KMS?.....	6
1.11 ¿Puedo exportar un CMK desde KMS?.....	7
1.12 ¿Puedo descifrar mis datos si elimino permanentemente mi clave personalizada?.....	7
1.13 ¿Cómo uso la herramienta en línea para cifrar o descifrar pequeños volúmenes de datos?.....	7
1.14 ¿Puedo actualizar CMK creados por materiales clave generados por KMS?.....	9
1.15 When Should I Use a CMK Created with Imported Key Materials?.....	9
1.16 ¿Qué debo hacer cuando elimino accidentalmente materiales clave?.....	9
1.17 ¿Cómo se generan las claves predeterminadas?.....	9
1.18 ¿Qué debo hacer si no tengo permisos para realizar operaciones en KMS?.....	10
1.19 ¿Por qué no puedo envolver claves asimétricas usando -id-aes256-wrap-pad en OpenSSL?.....	11
1.20 Algoritmos de clave soportados por KMS.....	12
1.21 ¿Qué debo hacer si no se ha solicitado KMS y se muestra el código de error 401?.....	13
1.22 ¿Cuál es la relación entre el texto cifrado y el texto plano devuelto por la API de encrypt-data?.....	14
1.23 ¿Cómo protego KMS mis claves?.....	14
1.24 ¿Cómo uso una clave asimétrica para verificar el resultado de la firma de un par de claves públicas?.....	14
1.25 ¿Una clave importada admite la rotación?.....	16
2 Credencial Relacionado.....	17
2.1 ¿Por qué no puedo eliminar el estado de versión de un secreto?.....	17
3 KPS Relacionados.....	18
3.1 ¿Cómo creo un par de claves?.....	18
3.2 ¿Qué son un par de claves privadas y un par de claves de cuenta?.....	23
3.3 ¿Cómo puedo manejar un error de importación de un par de claves creado con PuTTYgen?.....	24

3.4 ¿Qué debo hacer cuando no puedo importar un par de claves usando Internet Explorer 9?.....	27
3.5 ¿Cómo inicio sesión en un ECS de Linux con una clave privada?.....	27
3.6 ¿Cómo uso una clave privada para obtener la contraseña para iniciar sesión en un ECS de Windows?.....	29
3.7 ¿Cómo puedo manejar la falla en la vinculación de un par de claves?.....	30
3.8 ¿Cómo manejo el fallo en la sustitución de un par de claves?.....	32
3.9 ¿Cómo puedo manejar la falla en el restablecimiento de un par de claves?.....	33
3.10 ¿Cómo puedo manejar el fallo en la desvinculación de un par de claves?.....	34
3.11 ¿Necesito reiniciar los servidores después de reemplazar su par de claves?.....	35
3.12 ¿Cómo activo el modo de inicio de sesión con contraseña para un ECS?.....	36
3.13 ¿Cómo manejo el fallo al iniciar sesión en ECS después de desvincular el par de claves?.....	38
3.14 ¿Qué debo hacer si se pierde mi clave privada?.....	40
3.15 ¿Cómo convierto el formato de un archivo de clave privada?.....	40
3.16 ¿Puedo cambiar el par de claves de un servidor?.....	42
3.17 ¿Puede un par de claves ser compartido por varios usuarios?.....	42
3.18 ¿Cómo obtengo el archivo de clave pública o privada de un par de claves?.....	42
3.19 ¿Qué puedo hacer si se informa de un error cuando se crea o actualiza una clave de cuenta por primera vez?.....	43
3.20 ¿Se ocupará la cuota del par de claves de cuenta después de que se actualice un par de claves privadas a un par de claves de cuenta?.....	43
4 Relacionado con HSM dedicado.....	44
4.1 ¿Qué es el HSM dedicado?.....	44
4.2 ¿Cómo garantiza el HSM dedicado la seguridad para la generación de claves?.....	44
4.3 ¿El personal de la sala de equipos tiene la función de súper administrador para robar información mediante el uso de un UKey privilegiado?.....	44
4.4 ¿Qué HSM se utilizan para HSM dedicado?.....	45
4.5 ¿Qué API admite HSM dedicado?.....	45
4.6 ¿Cómo habilito el acceso público a una instancia de HSM dedicado?.....	45
5 Precios.....	47
5.1 ¿Cómo se carga el DEW?.....	47
5.2 ¿Cómo renuevo DEW?.....	47
5.3 ¿Cómo me doy de baja de DEW?.....	49
5.4 ¿Se cobrará un CMK después de estar discapacitado?.....	49
5.5 ¿Se facturan las credenciales programadas para eliminarlas?.....	49
5.6 ¿Se cobrará un CMK después de que esté programado para eliminarlo?.....	49
6 General.....	51
6.1 ¿Qué funciones proporciona DEW?.....	51
6.2 ¿Qué algoritmos de criptografía utiliza DEW?.....	52
6.3 ¿En qué regiones están disponibles los servicios DEW?.....	52
6.4 What Is a Quota?.....	53
6.5 ¿Qué es el mecanismo de asignación de recursos de DEW?.....	55
6.6 ¿Qué son las Regiones y las AZ?.....	55
6.7 Can DEW Be Shared Across Accounts?.....	56

6.8 ¿Cómo accedo a las funciones de DEW?..... 56

1 KMS Relacionados

1.1 ¿Qué es Key Management Service?

KMS es un servicio en la nube seguro, confiable y fácil de usar que ayuda a los usuarios a crear, gestionar y proteger claves de manera centralizada.

Utiliza Hardware Security Modules (HSMs) para proteger las claves. Todas las claves están protegidas por claves raíz en HSM para evitar fugas de claves. El módulo HSM cumple con los requisitos de seguridad FIPS 140-2 Nivel 3.

También controla el acceso a las claves y registra todas las operaciones en claves con registros rastreables. Además, proporciona registros de uso de todas las claves, cumpliendo con sus requisitos de auditoría y cumplimiento normativo.

1.2 ¿Qué es una clave maestra del cliente?

Una clave maestra de cliente (CMK) es una clave de cifrado de clave (KEK) creada por un usuario en KMS. Se utiliza para cifrar y proteger los DEK. Se puede usar un CMK para cifrar uno o más DEK.

Los CMK se clasifican en claves personalizadas y claves predeterminadas.

- Claves personalizadas

Claves creadas o importadas por los usuarios en la consola KMS.

- Claves predeterminadas

Cuando un usuario utiliza KMS para la encriptación en un servicio en la nube por primera vez, el servicio en la nube crea automáticamente una clave con el sufijo de alias **/default**.

Puede utilizar la consola de gestión para realizar consultas, pero no puede deshabilitar ni programar la eliminación de las claves maestras predeterminadas.

Tabla 1-1 Claves maestras predeterminadas

Alias	Servicio en la nube
obs/default	Object Storage Service (OBS)

Alias	Servicio en la nube
evs/default	Elastic Volume Service (EVS)
ims/default	Image Management Service (IMS)
kps/default	Key Pair Service (KPS)
csms/default	Cloud Secret Management Service (CSMS)

1.3 ¿Qué es una clave predeterminada?

Otro servicio en la nube que utiliza KMS crea automáticamente una clave predeterminada, como Object Storage Service (OBS). El alias de una clave predeterminada termina en / **default**.

Puede utilizar la consola de gestión para realizar consultas, pero no puede deshabilitar ni programar la eliminación de las claves predeterminadas.

Las claves predeterminadas se alojan de forma gratuita y se cobran en función del número de solicitudes de API para ellas. Si las solicitudes de API superan el límite gratuito, se cobrará la parte sobrante.

Tabla 1-2 Claves maestras predeterminadas

Alias	Servicio en la nube
obs/default	Object Storage Service (OBS)
evs/default	Elastic Volume Service (EVS)
ims/default	Image Management Service (IMS)
vbs/default	Volume Backup Service (VBS)
sfs/default	Scalable File Service (SFS)
kps/default	Key Pair Service (KPS)
csms/default	Cloud Secret Management Service (CSMS)

NOTA

Una clave predeterminada se crea automáticamente cuando un usuario utiliza la función de encriptación KMS por primera vez en otro servicio en la nube.

1.4 ¿Cuáles son las diferencias entre una clave personalizada y una clave predeterminada?

En la siguiente tabla se describen las diferencias entre una clave personalizada y una clave predeterminada.

Tabla 1-3 Diferencias entre una clave personalizada y una clave predeterminada

Concepto	Definición	Diferencia
Clave personalizada	Clave de cifrado de clave (KEK) creada con KMS. La clave se utiliza para cifrar y proteger los DEK. Se puede utilizar una clave personalizada para cifrar varios DEK.	<ul style="list-style-type: none"> ● Puede ser deshabilitado y programado para su eliminación. ● Se factura por uso después de ser creado o importado.
Clave predeterminada	El sistema genera automáticamente cuando utiliza KMS para cifrar datos en otro servicio en la nube por primera vez. El sufijo de la clave es /default . Ejemplo: evs/default	<ul style="list-style-type: none"> ● No se puede deshabilitar ni programar su eliminación. ● No se le cobrará cuando utilice el servicio en la nube generado automáticamente por el sistema. Si el número de solicitudes de API es superior a 20,000, se le facturará.

1.5 What Is a Data Encryption Key?

A data encryption key (DEK) is used to encrypt data.

1.6 ¿Por qué no puedo eliminar un CMK inmediatamente?

La decisión de suprimir un CMK debe considerarse con gran cautela. Antes de la eliminación, confirme que se han migrado todos los datos cifrados del CMK. Tan pronto como se elimine el CMK, no podrá descifrar los datos con él. Por lo tanto, KMS ofrece un período especificado por el usuario de 7 a 1096 días para que la eliminación finalmente surta efecto. El día programado de eliminación, el CMK se eliminará permanentemente. Sin embargo, antes del día programado, aún puede cancelar la eliminación pendiente. Este es un medio de precaución dentro de KMS.

1.7 ¿Qué servicios en la nube pueden usar KMS para el cifrado?

Object Storage Service (OBS), Elastic Volume Service (EVS), Image Management Service (IMS), and Relational Database Service (RDS) pueden utilizar KMS para la encriptación.

Tabla 1-4 Lista de servicios en la nube que utilizan encriptación KMS

Nombre del servicio	Descripción
Object Storage Service (OBS)	<p>Puede cargar objetos y descargarlos desde Object Storage Service (OBS) en modo común o en modo de encriptación del servidor. Cuando carga objetos en modo de encriptación, los datos se cifran en el lado del servidor y luego se almacenan de forma segura en OBS en texto de encriptación. Cuando descarga objetos cifrados, los datos en texto cifrado se descifran en el lado del servidor y luego se le proporcionan en texto sin formato. OBS admite la encriptación del lado del servidor con el modo de claves gestionadas por KMS (SSE-KMS). En el modo SSE-KMS, OBS utiliza las claves proporcionadas por KMS para encriptación del lado del servidor.</p> <p>Para obtener detalles acerca de cómo cargar objetos a OBS en modo SSE-KMS, consulte Guía de operación de consola de Object Storage Service.</p>
Elastic Volume Service (EVS)	<p>Si habilita la función de encriptación al crear un disco EVS, el disco se cifrará con el DEK generado mediante el CMK. Los datos almacenados en el disco EVS se cifrarán automáticamente.</p> <p>Para obtener detalles sobre cómo utilizar la función de encriptación de EVS, consulte Guía de usuario de Elastic Volume Service.</p>
Image Management Service (IMS)	<p>Al crear una imagen privada utilizando un archivo de imagen externo, puede activar la función de encriptación de imagen privada y seleccionar un CMK proporcionado por KMS para cifrar la imagen.</p> <p>Para obtener más información acerca de cómo utilizar la función de encriptación de imagen privada del Image Management Service (IMS), consulte Guía de usuario de Image Management Service.</p>
Scalable File Service (SFS)	<p>Al crear un sistema de archivos en SFS, el CMK proporcionado por KMS se puede seleccionar para cifrar el sistema de archivos, de modo que los archivos almacenados en el sistema de archivos se cifran automáticamente.</p> <p>Para obtener más información acerca de cómo utilizar la función de encriptación del sistema de archivos de SFS, consulte Guía de usuario de Scalable File Service.</p>
Relational Database Service (RDS)	<p>Al comprar una instancia de base de datos, puede habilitar la función de encriptación de disco de la instancia de base de datos y seleccionar un CMK creado en KMS para cifrar el disco de la instancia de base de datos. Habilitación de la función de encriptación de disco mejorará la seguridad de los datos.</p> <p>Para obtener detalles acerca de cómo utilizar la función de encriptación de disco de RDS, consulte Guía de usuario de Relational Database Service.</p>
Document Database Service (DDS)	<p>Al comprar una instancia DDS, puede habilitar la función de encriptación de disco de la instancia y seleccionar un CMK creado en KMS para cifrar el disco de la instancia. Habilitación de la función de encriptación de disco mejorará la seguridad de los datos.</p> <p>Para obtener más información acerca de cómo utilizar la función de encriptación de disco de DDS, consulte Pasos iniciales de Document Database Service.</p>

1.8 ¿Cómo servicios de Huawei Cloud utilizan KMS para cifrar datos?

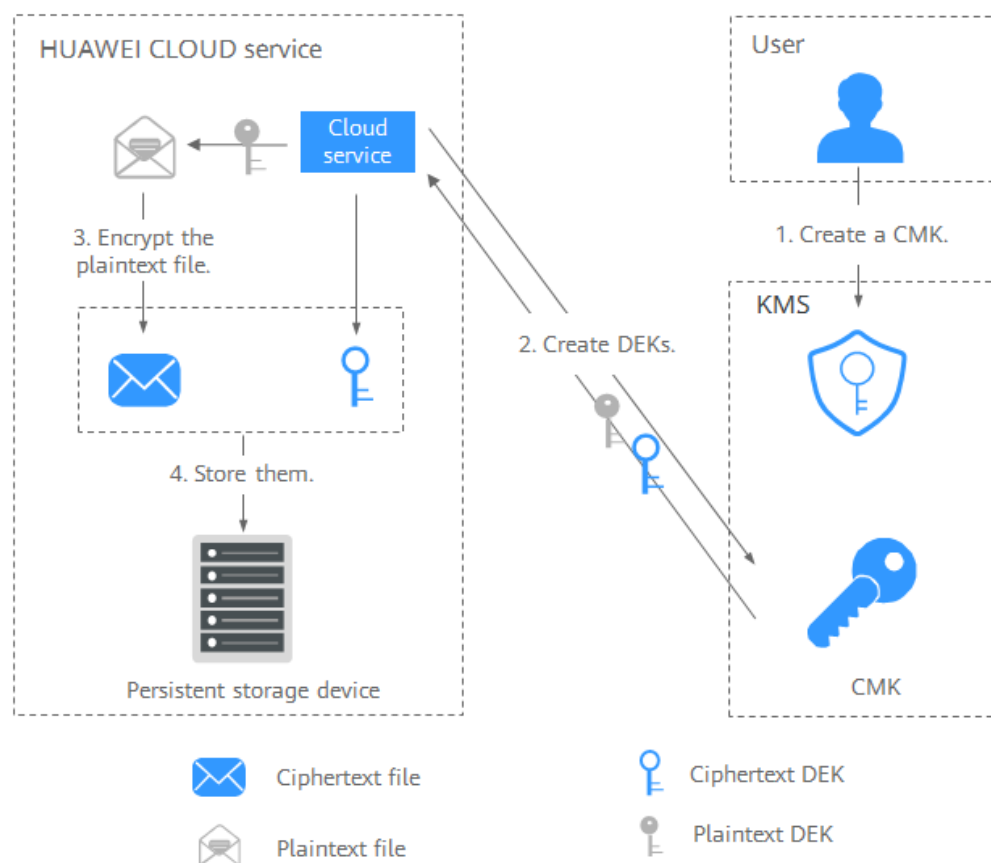
Los servicios de Huawei Cloud (incluidos OBS, IMS, EVS y RDS) utilizan la encriptación de sobre proporcionado por **KMS** para proteger los datos.

📖 NOTA

La encriptación de sobres es un método de encriptación que permite que los DEK se almacenen, transmitan y utilicen en "sobres" de CMK. Como resultado, los CMK no cifran y descifran datos directamente.

- Cuando utiliza un servicio de Huawei Cloud para cifrar datos, debe especificar un CMK en KMS. El servicio de Huawei Cloud genera un DEK de texto sin formato y un DEK de texto cifrado. El DEK de texto cifrado se genera cifrando el DEK de texto sin formato usando el CMK especificado. El servicio de Huawei Cloud utiliza el DEK de texto sin formato para cifrar datos y almacena los datos de texto cifrado y el DEK de texto cifrado en el servicio de Huawei Cloud. Vea la siguiente figura.

Figura 1-1 Cómo Huawei Cloud utiliza KMS para encriptación



- Cuando los usuarios descargan los datos de Huawei Cloud, el servicio utiliza el CMK especificado por KMS para descifrar el DEK de texto cifrado, utilizar el DEK descifrado para descifrar los datos y, a continuación, proporcionar los datos descifrados para que los usuarios los descarguen.

1.9 ¿Cuáles son los beneficios del cifrado de sobres?

La encriptación de sobres es la práctica de cifrar datos con un DEK y luego cifrar el DEK con una clave root que puede gestionar completamente. En este caso, los CMK no son necesarios para la encriptación o desencriptación.

Beneficios:

- **Ventajas sobre la encriptación CMK en KMS**

Los usuarios pueden usar CMK para cifrar y descifrar datos en la consola de KMS o invocando a las API de KMS.

Un CMK puede cifrar y descifrar datos no más de 4 KB. Un sobre puede cifrar y descifrar grandes volúmenes de datos.

Los datos cifrados con sobres no necesitan ser transferidos. Solo es necesario transferir los DEK al servidor KMS.
- **Ventajas sobre la encriptación mediante el uso de servicios en la nube**
 - **Seguridad**

Los datos transferidos a la nube para su encriptación están expuestos a riesgos como la interceptación y el phishing.

Durante la encriptación de sobres, KMS utiliza módulos de seguridad de hardware (HSM) para proteger las claves. Todas las CMK están protegidas por claves root en HSM para evitar fugas de claves.
 - **Confiabilidad**

Usted se preocupará por la seguridad de los datos en la nube. También es difícil para los servicios en la nube demostrar que nunca hacen uso indebido o divulgan dichos datos.

Si elige la encriptación de sobres, KMS controlará el acceso a las claves y registrará todos los usos y operaciones de las claves con registros rastreables, cumpliendo con sus requisitos de auditoría y cumplimiento normativo.
 - **Rendimiento y coste**

Para cifrar o descifrar datos utilizando un servicio en la nube, debe enviar los datos al servidor de encriptación y recibir los datos procesados. Este proceso afecta seriamente el rendimiento de su servicio y conlleva altos costos.

La encriptación de sobres le permite generar DEKs en línea invocando a las API de algoritmos criptográficos de KMS, y cifrar una gran cantidad de datos locales con los DEK.

1.10 ¿Hay un límite en el número de claves personalizadas que puedo crear en KMS?

Sí.

Puede crear un máximo de 20 claves personalizadas, incluidas las que estén habilitadas, deshabilitadas y pendientes de eliminación. Las claves predeterminadas no están incluidas.

1.11 ¿Puedo exportar un CMK desde KMS?

No.

Para garantizar la seguridad de CMK, los usuarios solo pueden crear y usar CMK en KMS.

1.12 ¿Puedo descifrar mis datos si elimino permanentemente mi clave personalizada?

No.


Si ha eliminado permanentemente su clave personalizada, los datos cifrados con ella no se pueden descifrar. Antes de la fecha de eliminación programada de la clave personalizada, puede cancelar la eliminación programada.

1.13 ¿Cómo uso la herramienta en línea para cifrar o descifrar pequeños volúmenes de datos?

Puede utilizar la herramienta en línea para cifrar o descifrar datos en los siguientes procedimientos:

Encriptación de datos

Paso 1 [Inicie sesión en la consola de gestión.](#)

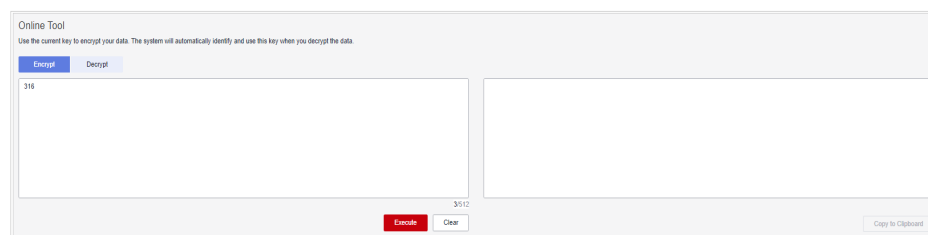
Paso 2 Haga clic en  en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

Paso 3 Haga clic en . Elija **Security & Compliance > Data Encryption Workshop**.

Paso 4 Haga clic en el alias de una clave personalizada para ver sus detalles y vaya a la herramienta en línea para el cifrado y descifrado de datos.

Paso 5 Haga clic en **Encrypt**. En el cuadro de texto de la izquierda, introduzca los datos que se van a cifrar. Para más detalles, consulte [Figura 1-2](#).

Figura 1-2 Encriptación de datos



Paso 6 Haga clic en **Execute**. El texto cifrado de los datos se muestra en el cuadro de texto de la derecha.

 **NOTA**

- Utilice el CMK actual para cifrar los datos.
- Puede hacer clic en **Clear** para borrar los datos introducidos.
- Puede hacer clic en **Copy to Clipboard** para copiar el texto cifrado y guardarlo en un archivo local.

----Fin

 **NOTA**

Introduzca el texto sin formato en la consola, el texto se codificará en formato Base64 antes de la encriptación.

El resultado de descifrado devuelto a través de API estará en formato Base64. Realice la decodificación Base64 para obtener el texto sin formato introducido en la consola.

Desencriptación de datos

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en . Elija **Security & Compliance > Data Encryption Workshop**.

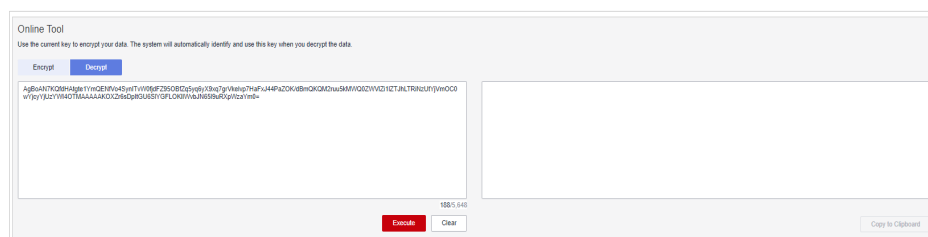
Paso 3 Puede hacer clic en cualquier clave no predeterminada en estado de **Enabled** para ir a la página de encriptación y descifrado de la herramienta en línea.

Paso 4 Haga clic en **Decrypt**. En el cuadro de texto de la izquierda, introduzca los datos que se van a descifrar. Para más detalles, consulte [Figura 1-3](#).

 **NOTA**

- La herramienta identificará el CMK de encriptación original y lo utilizará para descifrar los datos.
- Sin embargo, si el CMK se ha eliminado, el descifrado falla.

Figura 1-3 Desencriptación de datos



Paso 5 Haga clic en **Execute**. El texto sin formato de los datos se muestra en el cuadro de texto de la derecha.

 **NOTA**

- Puede hacer clic en **Copy to Clipboard** para copiar el texto sin formato y guardarlo en un archivo local.

----Fin

1.14 ¿Puedo actualizar CMK creados por materiales clave generados por KMS?

No.

Las claves creadas con materiales generados por KMS no se pueden actualizar. Solo puede utilizar KMS para crear nuevos CMK para cifrar y descifrar datos.

1.15 When Should I Use a CMK Created with Imported Key Materials?

- If you do not want to use KMS-generated key materials, you can import your own key materials to create a CMK. Such a CMK allows deletion of only the key materials when you do not need it. In addition, when you find that the key materials are mis-deleted, you can import the same materials to the CMK.
- You can also import off-cloud key materials to KMS when you want to use the same keys on and off the cloud. This practice has proved useful when users migrate local encrypted data onto cloud.

1.16 ¿Qué debo hacer cuando elimino accidentalmente materiales clave?

Puede importar de nuevo los materiales de la clave de copia de respaldo desde su dispositivo local.

AVISO

Antes de importar materiales clave, se recomienda realizar una copia de respaldo de los materiales. Los materiales a reimportar deben ser consistentes con los materiales mal eliminados.

1.17 ¿Cómo se generan las claves predeterminadas?

Las claves predeterminadas se generan automáticamente.

Cuando un usuario utiliza KMS para la encriptación en un servicio en la nube por primera vez, el servicio en la nube crea automáticamente una clave con el sufijo de alias **/default**.

Puede utilizar la consola de gestión para realizar consultas, pero no puede deshabilitar ni programar la eliminación de las claves maestras predeterminadas.

Las claves predeterminadas se alojan de forma gratuita y se cobran en función del número de solicitudes de API para ellas. Si las solicitudes de API superan el límite gratuito, se cobrará la parte sobrante.

Tabla 1-5 Claves maestras predeterminadas

Alias	Servicio en la nube
obs/default	Object Storage Service (OBS)
evs/default	Elastic Volume Service (EVS)
ims/default	Image Management Service (IMS)
kps/default	Key Pair Service (KPS)
csms/default	Cloud Secret Management Service (CSMS)

1.18 ¿Qué debo hacer si no tengo permisos para realizar operaciones en KMS?

Síntoma

Se muestra un mensaje que indica la falta de permisos cuando intenta realizar operaciones en claves, como ver, crear o importar claves.

Causas posibles

Su cuenta no está asociada a las políticas del sistema KMS requeridas.

Solución

Paso 1 Compruebe si su cuenta está asociada a las políticas de **KMS Administrator** y **KMS CMKFullAccess**.

Para obtener más información sobre cómo verificar los grupos de usuarios y permisos, consulte [Grupos de usuario y autorización](#).

Si su cuenta está asociada a las políticas del sistema KMS requeridas, vaya a **Paso 2**.

Paso 2 Asocie su cuenta con las políticas del sistema requeridas.

- Para obtener más información acerca de cómo agregar permisos de administrador, consulte [Grupos de usuario y autorización](#).
- Para obtener más información sobre cómo agregar una política personalizada, consulte [Creación de una política personalizada de DEW](#).

----Fin

1.19 ¿Por qué no puedo envolver claves asimétricas usando `-id-aes256-wrap-pad` en OpenSSL?

Síntoma

Por defecto, el algoritmo `-id-aes256-wrap-pad` no está habilitado en OpenSSL. Para envolver una clave, actualice OpenSSL a la versión más reciente y parchearlo primero.

Solución

Utilice los comandos bash para crear una copia local del OpenSSL existente. No es necesario eliminar o modificar las configuraciones predeterminadas de instalación del cliente OpenSSL.

Paso 1 Cambie al usuario `root`.

```
sudo su -
```

Paso 2 Ejecute el siguiente comando y registre la versión de OpenSSL:

```
openssl version
```

Paso 3 Ejecute los siguientes comandos para crear el directorio `/root/build`. Este directorio se utilizará para almacenar el último archivo binario OpenSSL.

```
mkdir $HOME/build
```

```
mkdir -p $HOME/local/ssl
```

```
cd $HOME/build
```

Paso 4 Descargue la última versión de OpenSSL desde <https://www.openssl.org/source/>.

Paso 5 Descargue y descomprima el archivo binario.

Paso 6 Sustituya `openssl-1.1.1d.tar.gz` con la última versión de OpenSSL descargada en [paso 4](#).

```
curl -O https://www.openssl.org/source/openssl-1.1.1d.tar.gz
```

```
tar -zxf openssl-1.1.1d.tar.gz
```

Paso 7 Utilice la herramienta `gcc` para parchear la versión y compilar el archivo binario descargado.

```
yum install patch make gcc -y
```

NOTA

Si está utilizando una versión que no sea OpenSSL-1.1.1d, es posible que tenga que cambiar el directorio y los comandos utilizados, o es posible que este parche no funcione correctamente.

Paso 8 Ejecute los siguientes comandos:

```
sed -i "/BIO_get_cipher_ctx(benc, &ctx);/a\ EVP_CIPHER_CTX_set_flags(ctx, EVP_CIPHER_CTX_FLAG_WRAP_ALLOW);" $HOME/build/openssl-1.1.1d/apps/enc.c
```

Paso 9 Ejecute los siguientes comandos para compilar el archivo `enc.c` de OpenSSL:

```
cd $HOME/build/openssl-1.1.1d/
```

```
./config --prefix=$HOME/local --openssldir=$HOME/local/ssl
```



```
make -j$(grep -c ^processor /proc/cpuinfo)
```

```
make install
```

Paso 10 Configure la variable de entorno **LD_LIBRARY_PATH** para asegurarse de que las bibliotecas requeridas estén disponibles para OpenSSL. La última versión de OpenSSL se ha vinculado dinámicamente al archivo binario en el directorio **\$HOME/local/ssl/lib/**, y no se puede ejecutar directamente en shell.

Paso 11 Cree un script llamado **openssl.sh** para cargar la ruta **\$HOME/local/ssl/lib/** antes de ejecutar el archivo binario.

```
cd $HOME/local/bin/
```

```
echo -e '#!/bin/bash \nenv LD_LIBRARY_PATH=$HOME/local/lib/ $HOME/local/bin/openssl "$@"' > ./openssl.sh
```

Paso 12 Ejecute el siguiente comando para configurar un bit de ejecución en el script:

```
chmod 755 ./openssl.sh
```

Paso 13 Ejecute el siguiente comando para iniciar la versión parcheada de OpenSSL:

```
$HOME/local/bin/openssl.sh
```

```
---Fin
```

1.20 Algoritmos de clave soportados por KMS

Tabla 1-6 Algoritmos de clave soportados por KMS

Tipo de clave	Tipo de algoritmo	Especificaciones de clave	Descripción	Uso
Clave simétrica	AES	AES_256	Clave simétrica de AES	Cifra y descifra una pequeña cantidad de datos o claves de datos.
Clave simétrica	AES	<ul style="list-style-type: none"> ● HMAC_256 ● HMAC_384 ● HMAC_512 	Clave simétrica de HMAC	Genera y verifica un código de autenticación de mensaje
Clave simétrica	SM3	HMAC_SM3	Clave simétrica de SM3	Genera y verifica un código de autenticación de mensaje

Tipo de clave	Tipo de algoritmo	Especificaciones de clave	Descripción	Uso
Clave asimétrica	RSA	<ul style="list-style-type: none"> ● RSA_2048 ● RSA_3072 ● RSA_4096 	Contraseña asimétrica de RSA	Cifra y descifra una pequeña cantidad de datos o crea firmas digitales.
	ECC	<ul style="list-style-type: none"> ● EC_P256 ● EC_P384 	Curva elíptica recomendada por NIST	Firma digital

1.21 ¿Qué debo hacer si no se ha solicitado KMS y se muestra el código de error 401?

Síntomas

Se notifica un error cuando se solicita KMS o se habilita la función de encriptación del servicio en la nube.

Información del error: **httpcode=401,code=APIGW.0301,Msg=Incorrect IAM authentication information: current ip:xx.xx.xx.xx refused**

Causas posibles

El control de acceso se configura en IAM.


De forma predeterminada, IAM permite el acceso desde cualquier dirección IP. Si configura ACL, las direcciones IP y los segmentos de red fuera del rango especificado no pueden acceder a KMS ni utilizar la función de encriptación en la nube.

Solución

- Para acceder a KMS a través de la consola de servicios en la nube (por ejemplo, para fines de encriptación de OBS), permita el acceso desde los segmentos de red 10.0.0.0/8, 11.0.0.0/8 y 26.0.0.0/8.
- Para invocar a KMS a través de la API, permita el acceso desde las direcciones IP de origen.

Permitir el acceso desde direcciones IP específicas

Paso 1 [Inicie sesión en la consola de gestión.](#)

Paso 2 Haga clic en  en la izquierda de la página y elija **Management & Governance > Identity and Access Management**. Se muestra la página **Users**.

Paso 3 Elija **Security Settings** y haga clic en la pestaña **ACL**. Compruebe si **IP Address Ranges** y **IPv4 CIDR Blocks** están configurados correctamente.

 **NOTA**

La dirección IP de origen que utilice debe especificarse en las pestañas **Console Access** y **API Access**.

----Fin

1.22 ¿Cuál es la relación entre el texto cifrado y el texto plano devuelto por la API de encrypt-data?

La longitud básica del texto cifrado devuelto por la API de datos cifrados es de 124 bytes. El texto cifrado consta de múltiples campos, incluidos el ID de clave, algoritmo de encriptación, versión de clave y resumen de texto cifrado.

El texto sin formato tiene 16 bytes en cada bloque. Un bloque con menos de 16 bytes se rellena. Longitud de texto cifrado = $124 + \text{Ceil}(\text{longitud de texto plano}/16) \times 16$. El resultado de la conversión se codifica usando Base64.

Tome como ejemplo la entrada de texto sin formato de 4 bytes. El resultado del cálculo es $124 + \text{Ceil}(4/16) \times 16 = 140$. Los 140 bytes se convierten en 188 bytes después de la codificación Base64.

 **NOTA**

Ceil es una función de redondeo. $\text{Ceil}(a) = 1$. El intervalo de valores de **a** es (0,1].

1.23 ¿Cómo protege KMS mis claves?

El mecanismo de KMS impide que cualquier persona acceda a sus claves en texto plano. KMS se basa en módulos de seguridad de hardware (HSM) que protegen la confidencialidad e integridad de sus claves. Las claves KMS de texto plano siempre están cifradas por los HSM y nunca se almacenan en ningún disco. Estas claves solo se utilizan dentro de la memoria volátil de los HSM durante el tiempo necesario para realizar la operación criptográfica que ha solicitado.

1.24 ¿Cómo uso una clave asimétrica para verificar el resultado de la firma de un par de claves públicas?

En escenarios en los que se usan pares de claves públicas y privadas, la clave privada se usa para la firma y la clave pública se usa para la verificación de la firma. La clave pública se puede distribuir al sujeto de servicio que necesita usar la clave pública. El sujeto del servicio verifica la firma de los datos de clave. KMS proporciona la API **get-publickey** para obtener claves públicas.

El CMK **RSA_3072** en este caso se utiliza para verificar las firmas. Puedes usar KMS para firmar las API. El cuerpo de solicitud es el siguiente:

```
{
  "key_id": "key_id_value",
  "message": "MTIzNA==",
  "signing_algorithm": "RSASSA_PSS_SHA_256",
  "message_type": "RAW"
}
```

El resultado es el siguiente:

```
{
  "key_id": "key_id_value",
  "signature": "xxx"
}
```

Después de obtener la clave pública, asegúrese de que se verifica la firma.

```
public class RawDataVerifyExample {

    /**
     * Basic authentication information:
     * - ACCESS_KEY: access key of the Huawei Cloud account
     * - SECRET_ACCESS_KEY: Huawei Cloud account secret access key, which is
     sensitive information. Store this in ciphertext.
     * - IAM_ENDPOINT: endpoint for accessing IAM. For details, see https://
     developer.huaweicloud.com/intl/en-us/endpoint?IAM.
     * - KMS_REGION_ID: regions supported by KMS. For details, see https://
     developer.huaweicloud.com/intl/en-us/endpoint?DEW.
     * - KMS_ENDPOINT: endpoint for accessing KMS. For details, see https://
     developer.huaweicloud.com/intl/en-us/endpoint?DEW.
     */
    private static final String ACCESS_KEY = System.getenv("HUAWEICLOUD_SDK_AK");
    private static final String SECRET_ACCESS_KEY =
System.getenv("HUAWEICLOUD_SDK_SK");
    private static final String IAM_ENDPOINT = "https://<IamEndpoint>";
    private static final String KMS_REGION_ID = "<RegionId>";
    private static final String KMS_ENDPOINT = "https://<KmsEndpoint>";

    private static final int SALT_LENGTH = 32;
    private static final int TRAILER_FIELD = 1;
    public static final String RSA_PUBLIC_KEY_BEGIN = "-----BEGIN PUBLIC KEY-----
\n";
    public static final String RSA_PUBLIC_KEY_END = "-----END PUBLIC KEY-----";

    // Sample signature data in Base64 encoding format. The original text is 1234.
    private static final String RWA_DATA = "MTIzNA==";

    // Signature value obtained through the sign API of KMS
    private static final String SIGN = "xxx";
    public static void main(String[] args) throws Exception {

        final String keyId = args[0];

        publicKeyVerify(keyId);
    }
    public static void publicKeyVerify(String keyId) throws Exception {

        // 1. Prepare the authentication information for accessing HUAWEI CLOUD.
        final BasicCredentials auth = new BasicCredentials()
            .withIamEndpoint(IAM_ENDPOINT).withAk(ACCESS_KEY).withSk(SECRET_AC
CESS_KEY);

        // 2. Initialize the SDK and transfer the authentication information and
the address for the KMS to access the client.
        final KmsClient kmsClient = KmsClient.newBuilder()
            .withRegion(new Region(KMS_REGION_ID,
KMS_ENDPOINT)).withCredential(auth).build();

        // 3. Obtain the public key information. The returned information is in
PKCS8 format.
        final ShowPublicKeyRequest showPublicKeyRequest = new
ShowPublicKeyRequest()
            .withBody(new OperateKeyRequestBody().withKeyId(keyId));
        final ShowPublicKeyResponse showPublicKeyResponse =
kmsClient.showPublicKey(showPublicKeyRequest);

        // 4. Obtain the public key string.
        final String publicKeyStr =
```

```
showPublicKeyResponse.getPublicKey().replace(RSA_PUBLIC_KEY_BEGIN, "")
    .replaceAll("\n", "").replace(RSA_PUBLIC_KEY_END, "");

    // 5. Parse the public key.
    final X509EncodedKeySpec keySpec = new
X509EncodedKeySpec(Base64.getDecoder().decode(publicKeyStr));
    final KeyFactory keyFactory = KeyFactory.getInstance("RSA", new
BouncyCastleProvider());
    final PublicKey publicKey = keyFactory.generatePublic(keySpec);

    // 6. Verify the signature.
    final Signature signature = getSignature();
    signature.initVerify(publicKey);
    signature.update(commonHash(Base64.getDecoder().decode(RWA_DATA)));

    // 7. Obtain the verification result.
    assert signature.verify(Base64.getDecoder().decode(SIGN));

}
private static Signature getSignature() throws Exception {
    Signature signature= Signature.getInstance("NONEwithRSASSA-PSS", new
BouncyCastleProvider());
    MGF1ParameterSpec mgfParam = new MGF1ParameterSpec("SHA256");
    PSSParameterSpec pssParam = new PSSParameterSpec("SHA256", "MGF1",
mgfParam, SALT_LENGTH, TRAILER_FIELD);
    signature.setParameter(pssParam);
    return signature;
}
private static byte[] commonHash(byte[] data) {
    byte[] digest;
    try {
        MessageDigest md = MessageDigest.getInstance("SHA256",
BouncyCastleProvider.PROVIDER_NAME);
        md.update(data);
        digest = md.digest();
    } catch (Exception e) {
        throw new RuntimeException("Digest failed.");
    }
    return digest;
}
}
```

1.25 ¿Una clave importada admite la rotación?

Las claves importadas no admiten rotación. Después de eliminar los materiales de clave importado, asegúrese de que se importan los mismos materiales de clave.

2 Credencial Relacionado

2.1 ¿Por qué no puedo eliminar el estado de versión de un secreto?


`SYSCURRENT` y `SYSPREVIOUS` son estados preconfigurados y no se pueden eliminar.


3 KPS Relacionados

3.1 ¿Cómo creo un par de claves?

Creación de un par de claves mediante la consola de gestión

Paso 1 [Inicie sesión en la consola de gestión.](#)

Paso 2 Haga clic en  en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

Paso 3 Haga clic en  a la izquierda, elija **Security & Compliance > Data Encryption Workshop**, se mostrará la página de gestión de claves.

Paso 4 En el panel de navegación de la izquierda, haga clic en **Key Pair Service**.

Paso 5 Haga clic en **Create Key Pair**.

Paso 6 En el cuadro de diálogo **Create Key Pair**, escriba un nombre para el par de claves que se va a crear, como se muestra en [Figura 3-1](#).

Figura 3-1 Creación de un par de claves

Create Key Pair ×

Key pairs are free but there is a quota for how many you can have.

* Key Pair Name

Type

⚠ If you have not enabled your account key pair, this parameter is invalid. An SSH_RSA_2048 key pair will be created by default. Currently, only the RSA algorithm can be used with Windows.

I agree to host the private key of the key pair. [Learn more](#)

I have read and agree to the [Key Pair Service Disclaimer](#)

Paso 7 (Opcional) Seleccione un tipo de par de claves. Si no hay un par de claves habilitado para su cuenta, se creará un par de claves SSH_RSA_2048 por defecto.

📖 NOTA

Actualmente, solo se puede utilizar el algoritmo RSA con Windows.

Paso 8 Si desea que se administre su clave privada, lea y confirme **I agree to host the private key of the key pair.** Seleccione una clave de encriptación en el cuadro de lista desplegable de **KMS encryption**. Omite este paso si no necesita gestionar la clave privada.

📖 NOTA

- KPS utiliza la clave de encriptación proporcionada por KMS para cifrar las claves privadas. Cuando el usuario utiliza la función de encriptación KMS del par de claves, KMS crea automáticamente una clave predeterminada **kps/default** para la encriptación del par de claves.
- Al seleccionar una clave de encriptación, puede seleccionar una clave de encriptación existente o hacer clic en **View Key List** para crear una clave de encriptación.

Figura 3-2 Gestión de claves privadas

Create Key Pair ×

Key pairs are free but there is a quota for how many you can have.

* Key Pair Name

Type

! If you have not enabled your account key pair, this parameter is invalid. An SSH_RSA_2048 key pair will be created by default. Currently, only the RSA algorithm can be used with Windows.

* KMS Encryption [View Key List](#)

Key ID f1528a05-27fa-4576-aa15-7ce6fb7a1b0f

I agree to host the private key of the key pair. [Learn more](#)

! What you use beyond the free API request quota given by KMS will be billed. [Pricing details](#)

I have read and agree to the [Key Pair Service Disclaimer](#)

Paso 9 Lea el *Key Pair Service Disclaimer* y seleccione **I have read and agree to the Key Pair Service Disclaimer**.

Paso 10 Haga clic en **OK**. El navegador descarga automáticamente la clave privada. Cuando se descarga la clave privada, se muestra un cuadro de diálogo.

Paso 11 Guarde la clave privada según lo indique el cuadro de diálogo.

AVISO

- Si la clave privada no se administra, solo se puede descargar una vez. Guárdelo correctamente. Si se pierde la clave privada, puede vincular un par de claves al ECS nuevamente restableciendo la contraseña o el par de claves. Para obtener más información, consulte [¿Cómo manejo el error al iniciar sesión en ECS después de desvincular el par de claves?](#)
- Si ha autorizado a Huawei Cloud para gestionar la clave privada, puede exportar la clave privada en cualquier momento según sea necesario.

Paso 12 Después de guardar la clave privada, haga clic en **OK**. El par de claves se crea correctamente.

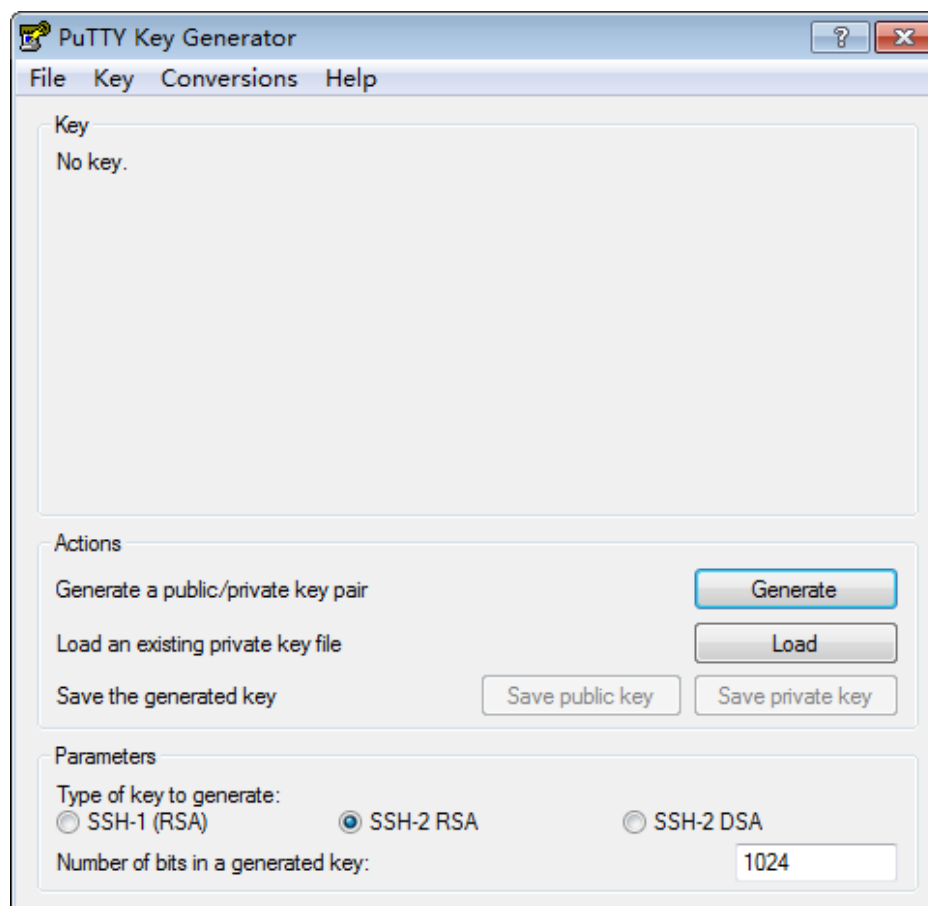
Después de crear el par de claves, puede verlo en la lista de pares de claves. La lista muestra información como el nombre del par de claves, la huella dactilar, la clave privada y la cantidad.

----**Fin**

Creación de un par de claves con PuTTYgen

Paso 1 Generar las claves públicas y privadas. Haga doble clic en **PuTTYgen.exe**. Se muestra la página **PuTTY Key Generator**, como se muestra en **Figura 3-3**.

Figura 3-3 Generador de claves de PuTTY



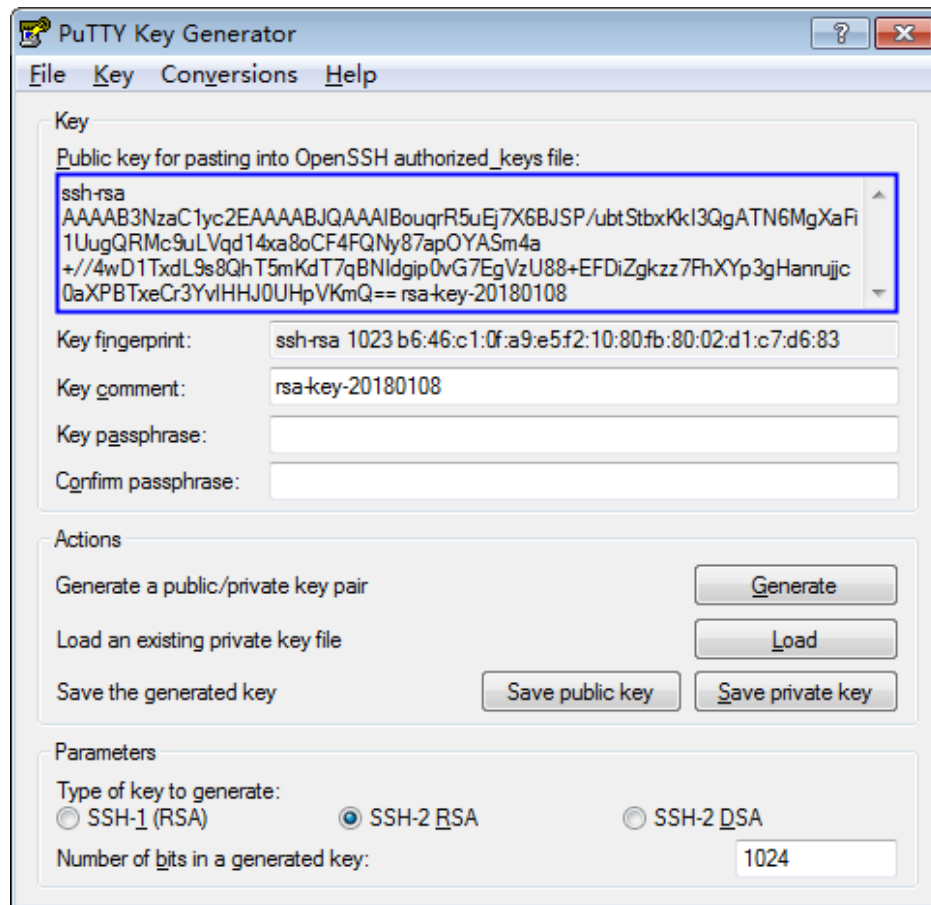
Paso 2 Configure los parámetros como se describe en el documento **Tabla 3-1**.

Tabla 3-1 Descripción del parámetro

Parámetro	Descripción
Type of key to generate	Algoritmo de cifrado y descifrado de pares de claves para importar a la consola de gestión. Actualmente, solo se admite SSH-2 RSA .
Number of bits in a generated key	Longitud de un par de claves que se va a importar a la consola de gestión. Actualmente, se admiten los siguientes valores de longitud: 1024 , 2048 , y 4096 .

Paso 3 Haga clic en **Generate** para generar una clave pública y una clave privada. Véase **Figura 3-4**.
El contenido resaltado por el cuadro de línea azul muestra una clave pública generada.

Figura 3-4 Obtención de las claves públicas y privadas



Paso 4 Copie la información en el cuadrado azul y guárdela en un archivo local .txt.

AVISO

No guarde la clave pública haciendo clic en **Save public key**. Guardar una clave pública haciendo clic en **Save public key** de PuTTYgen cambiará el formato del contenido de la clave pública. Dicha clave no se puede importar a la consola de gestión.

Paso 5 Guarde la clave privada en formato PPK o PEM.

AVISO

Por motivos de seguridad, la clave privada solo se puede descargar una vez. Manténgalo seguro.

Tabla 3-2 Formato de un archivo de clave privada

Formato de archivo de clave privada	Escenario de uso de clave privada	Método de ahorro
PEM	<ul style="list-style-type: none"> ● Utilizar la herramienta Xshell para iniciar sesión en el servidor en la nube que ejecuta el sistema operativo Linux. ● Gestionar la clave privada en la consola de gestión. 	<ol style="list-style-type: none"> 1. Elija Conversions > Export OpenSSH key. 2. Guarde la clave privada, por ejemplo, kp-123.pem, en un directorio local.
	Obtenga la contraseña de un servidor en la nube que ejecuta el sistema operativo Windows.	<ol style="list-style-type: none"> 1. Elija Conversions > Export OpenSSH key. <p>NOTA No introduzca la información de Key passphrase. De lo contrario, no se puede obtener la contraseña.</p> <ol style="list-style-type: none"> 2. Guarde la clave privada, por ejemplo, kp-123.pem, en un directorio local.
PPK	Utilizar la herramienta PuTTY para iniciar sesión en el servidor en la nube que ejecuta el sistema operativo Linux.	<ol style="list-style-type: none"> 1. En la página PuTTY Key Generator, elija File > Save private key. 2. Guarde la clave privada, por ejemplo, kp-123.ppk, en un directorio local.

Después de guardar correctamente la clave pública y la clave privada, puede importar el par de claves a la consola de gestión.

----Fin

3.2 ¿Qué son un par de claves privadas y un par de claves de cuenta?

Un par de claves privadas puede ser visto o utilizado solo por la cuenta actual.

Todos los usuarios de la cuenta pueden ver o usar un par de claves de cuenta.

Un par de claves privadas se puede actualizar a un par de claves de cuenta. Para obtener más información, consulte [Actualización de un par de claves](#).

3.3 ¿Cómo puedo manejar un error de importación de un par de claves creado con PuTTYgen?

Síntoma

Cuando un par de claves creado con PuTTYgen se importó a la consola de gestión, el sistema mostró un mensaje que indica que la importación de la clave pública falló.

Causas posibles

El formato del contenido de clave pública no cumple con los requisitos del sistema.

Almacenar una clave pública haciendo clic en **Save public key** cambiará el formato del contenido de la clave pública. La importación de dicha clave pública fallará porque la clave no pasa la verificación de formato por el sistema.

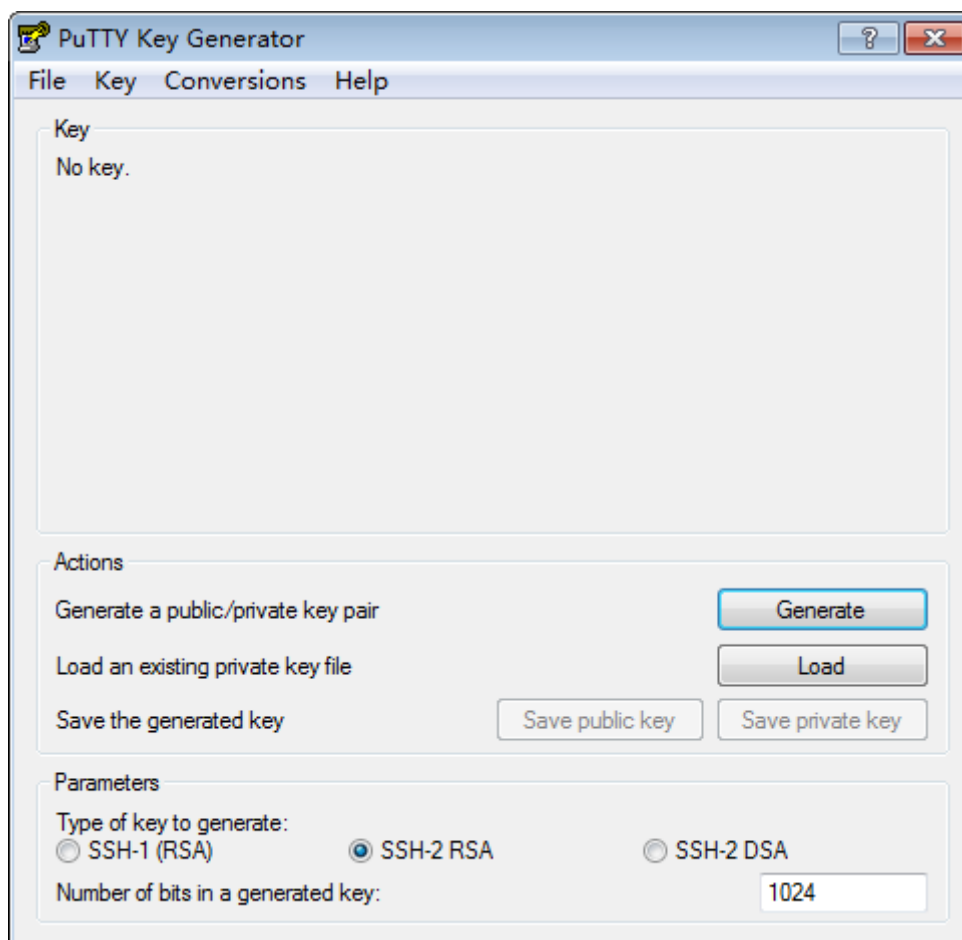
Procedimiento

Utilice la clave privada y **PuTTY Key Generator** almacenados localmente para restaurar el formato del contenido de la clave pública. A continuación, importe la clave pública a la consola de gestión.

Paso 1 Restaurar el archivo de clave pública en el formato correcto.

1. Haga doble clic en **PuTTYgen.exe**. Se muestra la página **PuTTY Key Generator**, como se muestra en [Figura 3-5](#).

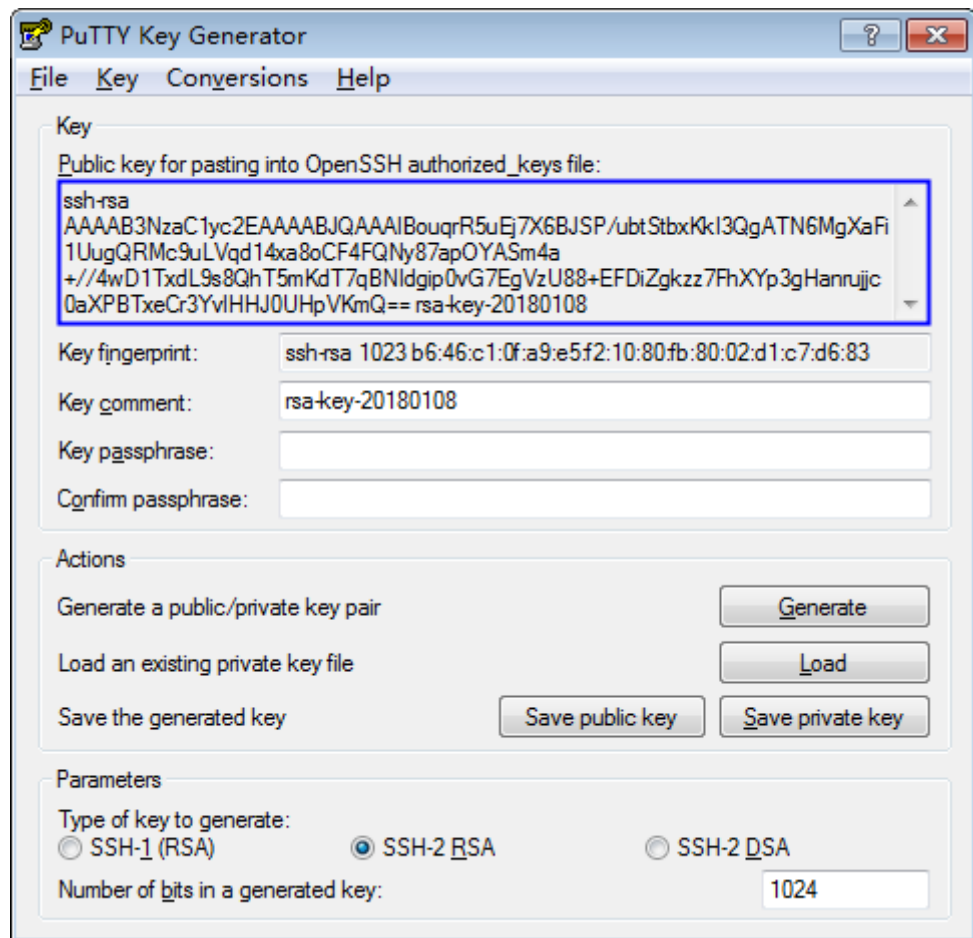
Figura 3-5 Interfaz principal del PuTTY Key Generator



2. Haga clic en **Load** y seleccione la clave privada.

El sistema carga automáticamente la clave privada y restaura el formato del contenido de la clave pública de **PuTTY Key Generator**. El contenido del cuadro rojo de **Figura 3-6** es la clave pública con el formato que cumple los requisitos del sistema.

Figura 3-6 Restaurar el formato del contenido de clave pública




3. Copie la información en el cuadrado azul y guárdela en un archivo local **.txt**.

AVISO

No guarde la clave pública haciendo clic en **Save public key**. Guardar una clave pública haciendo clic en **Save public key** de PuTTYgen cambiará el formato del contenido de la clave pública. Dicha clave no se puede importar a la consola de gestión.

Paso 2 Importe el archivo de clave pública en el formato correcto a la consola de KPS.

1. Inicie sesión en la consola de gestión.
2. Haga clic en  a la izquierda, elija **Security & Compliance > Data Encryption Workshop**, se mostrará la página de gestión de claves.
3. En el panel de navegación, haga clic en **Key Pair Service**.
4. En la página **Servicio de par de claves**, haga clic en **Import Key Pair**.
5. Haga clic en **Select File** y seleccione el archivo de clave pública **.txt** o copie y pegue el contenido de clave pública en el cuadro de texto del contenido de clave pública.
6. Haga clic en **OK** para importar el archivo de clave pública.


----Fin

3.4 ¿Qué debo hacer cuando no puedo importar un par de claves usando Internet Explorer 9?

Síntomas

La importación de un par de claves puede fallar si se utiliza Internet Explorer 9.

Procedimiento

- Paso 1** Haga clic en  en la esquina superior derecha del navegador.
- Paso 2** Seleccione **Internet Options**.
- Paso 3** Haga clic en la pestaña **Security** del cuadro de diálogo mostrado.
- Paso 4** Haga clic en **Internet**.
- Paso 5** Si el nivel de seguridad indica **Custom**, haga clic en **Default Level** para restaurar la configuración predeterminada.
- Paso 6** Mueva la barra de desplazamiento para establecer el nivel de seguridad en **Medium** y haga clic en **Apply**.
- Paso 7** Haga clic en **Custom Level**.
- Paso 8** Ajusta **Initialize and script ActiveX controls not marked as safe for scripting** a **Prompt**.
- Paso 9** Haga clic en **Yes**.

----Fin

3.5 ¿Cómo inicio sesión en un ECS de Linux con una clave privada?

Escenario

Después de crear o importar un par de claves en la consola KMS, seleccione el par de claves como modo de inicio de sesión al comprar un ECS y seleccione el par de claves creado o importado.

Después de comprar un ECS, puede utilizar la clave privada del par de claves para iniciar sesión en el ECS.

Prerrequisitos

- La conexión de red entre la herramienta de inicio de sesión (como PuTTY y XShell) y el ECS de destino es normal.
- Usted ha vinculado una EIP al ECS.
- Usted ha obtenido el archivo de clave privada del ECS.

Inicio de sesión desde un equipo con Windows

Para iniciar sesión en Linux ECS desde un equipo con Windows, realice las operaciones descritas en esta sección.

Método 1: Utilice PuTTY para iniciar sesión en el ECS.

Las siguientes operaciones utilizan PuTTY para iniciar sesión en ECS. Antes de iniciar sesión, debe obtener el formato de clave privada en el formato .ppk.

Paso 1 Haga doble clic en **PuTTY.EXE**. Se muestra la página **PuTTY Configuration**.

Paso 2 Elija **Connection > Data**. Ingrese el nombre de usuario de la imagen en **Auto-login username**.

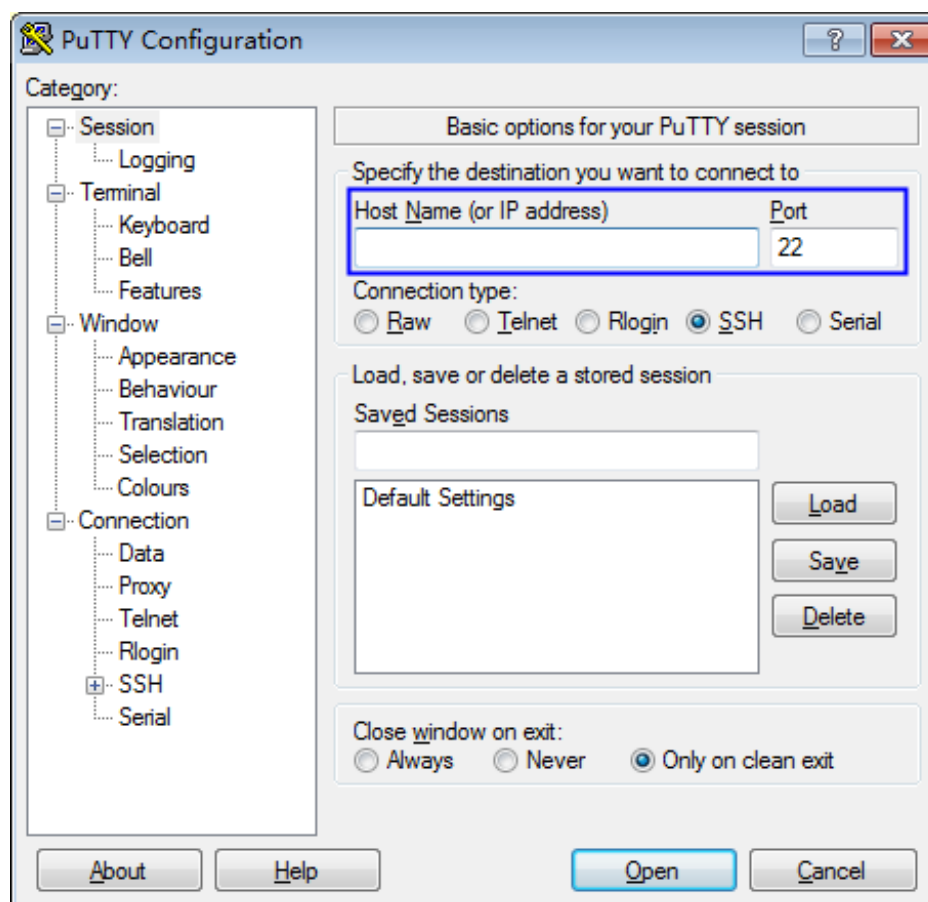
📖 NOTA

- Si se utiliza la imagen pública de **CoreOS**, el nombre de usuario de la imagen es **core**.
- Para una imagen pública de **non-CoreOS**, el nombre de usuario de la imagen es **root**.

Paso 3 Elija **Connection > SSH > Auth**. En **Private key file for authentication**, haga clic en **Browse** y seleccione un archivo de clave privada (en el formato .ppk).

Paso 4 Haga clic en **Session** e ingrese la EIP del ECS en **Host Name (o IP address)**

Figura 3-7 Configuración de la EIP



Paso 5 Haga clic en **Open** para iniciar sesión en el ECS.

----Fin

Método 2: Utilice Xshell para iniciar sesión en el ECS.

Paso 1 Inicie la herramienta Xshell.

Paso 2 Ejecute el siguiente comando para iniciar sesión remotamente en el ECS a través de SSH:

```
ssh Username@EIP
```

Un comando de ejemplo se proporciona de la siguiente manera:

```
ssh root@192.168.1.1
```

Paso 3 (Opcional) Si el sistema muestra el cuadro de diálogo **SSH Security Warning**, haga clic en **Accept & Save**.

Paso 4 Seleccione **Public Key** y haga clic en **Browse** junto al cuadro de texto CMK.

Paso 5 En el cuadro de diálogo mostrado, haga clic en **Import**.

Paso 6 Seleccione el archivo de clave almacenado localmente (en el formato **.pem**) y haga clic en **Open**.

Paso 7 Haga clic en **OK** para iniciar sesión en el ECS.

----Fin

Inicio de sesión desde un computador Linux

Para iniciar sesión en el ECS Linux desde un computador Linux, realice las operaciones que se describen a continuación: El siguiente procedimiento utiliza el archivo de clave privada **kp-123.ppk** como ejemplo para iniciar sesión en el ECS. El nombre de su archivo de clave privada puede diferir.

Paso 1 En la CLI de Linux, ejecute el siguiente comando para cambiar los permisos de operación:

```
chmod 600 /path/kp-123.ppk
```

 **NOTA**

En el comando anterior, **path** es la ruta donde se guarda el archivo de clave.

Paso 2 Ejecute el siguiente comando para iniciar sesión en ECS:

```
ssh -i /path/kp-123 root@EIP
```

 **NOTA**

- En el comando anterior, **path** es la ruta donde se guarda el archivo de clave.
- **EIP** es la EIP vinculada al ECS.

----Fin

3.6 ¿Cómo uso una clave privada para obtener la contraseña para iniciar sesión en un ECS de Windows?

Escenario

Se requiere una contraseña cuando inicia sesión en un ECS de Windows. En primer lugar, debe obtener la contraseña de administrador (contraseña del **administrador** de la cuenta u

otra cuenta establecida en Cloudbase-Init) generado durante la instalación inicial del ECS a partir del archivo de clave privada descargado al crear el ECS. Esta contraseña se genera aleatoriamente, ofreciendo una alta seguridad.

Puede obtener la contraseña para iniciar sesión en un ECS de Windows a través de la consola de gestión

NOTA

- Después de obtener la contraseña inicial, se recomienda borrar la información de contraseña registrada en el sistema para aumentar la seguridad del sistema.

El borrado de la información de contraseña inicial no afecta a la operación o inicio de sesión de ECS. Una vez borrada, la contraseña no se puede recuperar. Antes de eliminar una contraseña, se recomienda registrarla. Para obtener más información, consulte *Guía del usuario de Elastic Cloud Server*.


- También puede invocar a la API para obtener la contraseña inicial del ECS de Windows. Para obtener más información, consulte la *Referencia de API de Elastic Cloud Server*.


Prerrequisitos

Ha obtenido el archivo de clave privada (en formato **.pem**) para iniciar sesión en el ECS.

Obtención de una contraseña

Paso 1 [Inicie sesión en la consola de gestión](#).

Paso 2 Haga clic en  en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

Paso 3 Haga clic en  y seleccione **Compute > Elastic Cloud Server**.

Paso 4 En la lista de ECS, seleccione el ECS cuya contraseña desea obtener.

Paso 5 En la columna **Operation**, haga clic en **More** y elija **Get Password**.

Paso 6 Utilice uno de los métodos siguientes para obtener la contraseña:

- Haga clic en **Select File** y cargue el archivo clave desde un directorio local.
- Copie el contenido del archivo clave en el campo de texto.

Paso 7 Haga clic en **Get Password** para obtener una nueva contraseña aleatoria.

----Fin

3.7 ¿Cómo puedo manejar la falla en la vinculación de un par de claves?

Síntoma

Error al vincular el par de claves al ECS.

NOTA

- El cuadro de diálogo **Failed Key Pair Task** sólo registra y muestra las operaciones de par de claves fallidas en los ECS, que no afectan al estado ECS ni a las operaciones posteriores. Puede hacer clic en **Delete** en la fila del registro de error para eliminarlo, o puede hacer clic en **Delete All** para eliminar todos los registros de error.
- Haga clic en **Learn more** para ver documentos relacionados.

Causas posibles

- Se ha proporcionado una contraseña incorrecta o no válida.
- Se ha cambiado el grupo de permisos o propietarios del archivo de clave pública.
- Se ha modificado la configuración SSH del ECS.
- La dirección de entrada del puerto 22 del grupo de seguridad ECS no está abierta a 100.125.0.0/16.
- El ECS se ha apagado, iniciado o se ha separado un disco durante el proceso de vincular el par de claves al ECS.
- La conexión de red es defectuosa.
- Las reglas de firewall se han configurado para el ECS.

Procedimiento de manejo

Paso 1 Compruebe el estado de ECS.

- Si se está ejecutando, vaya a [Paso 2](#).
- Si está cerrado, vaya a [Paso 5](#).

Paso 2 Utilice la contraseña para iniciar sesión en el ECS para comprobar si la contraseña es correcta.

- Si es correcto, vaya a [Paso 4](#).
- Si no es correcto, utilice la contraseña correcta para volver a vincular el par de claves.

Paso 3 Compruebe si se han modificado la ruta de acceso de permisos y el grupo de propietarios del archivo `/root/.ssh/authorized_keys` en ECS.

- Si es así, restaure el permiso a lo siguiente:
 - El grupo propietario de cada nivel tiene el permiso **root:root**.
 - El permiso para el archivo `.ssh` es 700.
 - El permiso para **authorized_keys** es 600.
- Si no, vaya a [Paso 4](#).

Paso 4 Compruebe si el archivo `/root/.ssh/authorized_keys` del ECS ha sido modificado.

- En caso afirmativo, restaure el contenido original del archivo `/root/.ssh/authorized_keys` según los requisitos del sitio.
- Si no, vaya a [Paso 5](#).

Paso 5 Compruebe si la dirección de entrada del puerto 22 del grupo de seguridad ECS está abierta a 100.125.0.0/16. Es decir, 100.125.0.0/16 puede conectarse remotamente a los ECS de Linux a través de SSH.

- En caso afirmativo, vaya a [Paso 6](#).
- Si no, agregue la siguiente regla de grupo de seguridad y vuelva a vincular el par de claves. Para obtener más información sobre cómo agregar un grupo de seguridad, vea [Adición de una regla de grupo de seguridad](#).

Dirección	Protocolo/ Aplicación	Puerto	Origen
Inbound	SSH (22)	22	0.0.0.0/0

Paso 6 Compruebe si el ECS se puede encender, apagar e iniciar sesión.

- En caso afirmativo, vuelva a vincular el par de claves.
- Si no, vaya a [Paso 7](#).

Paso 7 Compruebe si la red está defectuosa.

- En caso afirmativo, póngase en contacto con el soporte técnico para verificar y localizar la falla.
- Si no, vuelva a vincular el par de claves.

----Fin

3.8 ¿Cómo manejo el fallo en la sustitución de un par de claves?

Síntoma

Error al reemplazar el par de claves en el ECS.

NOTA

El cuadro de diálogo **Failed Key Pair Task** sólo registra y muestra las operaciones de par de claves fallidas en los ECS, que no afectan al estado ECS ni a las operaciones posteriores. Puede hacer clic en **Delete** en la fila del registro de error para eliminarlo, o puede hacer clic en **Delete All** para eliminar todos los registros de error.

Causas posibles

- Se ha proporcionado una clave privada incorrecta o no válida.
- La dirección de entrada del puerto 22 del grupo de seguridad ECS no está abierta a 100.125.0.0/16.
- Se ha modificado la configuración SSH del ECS.
- El ECS se ha apagado, iniciado o se ha separado un disco durante el proceso de sustitución del par de claves para el ECS.
- La conexión de red es defectuosa.
- Las reglas de firewall se han configurado para el ECS.

Procedimiento de manejo

Paso 1 Utilice el par de claves SSH para iniciar sesión en el ECS y compruebe si la clave privada es correcta.

- Si es correcto, vaya a [Paso 2](#).
- Si no es correcto, utilice la clave privada correcta para reemplazar el par de claves.

Paso 2 Compruebe si el archivo `/root/.ssh/authorized_keys` del ECS ha sido modificado.

- En caso afirmativo, restaure el contenido original del archivo `/root/.ssh/authorized_keys` según los requisitos del sitio.
- Si no, vaya a **Paso 3**.

Paso 3 Compruebe si la dirección de entrada del puerto 22 del grupo de seguridad ECS está abierta a 100.125.0.0/16. Es decir, 100.125.0.0/16 puede conectarse remotamente a los ECS de Linux a través de SSH.

- En caso afirmativo, vaya a **Paso 4**.
- Si no, agregue la siguiente regla de grupo de seguridad y reemplace el par de claves.

Dirección	Protocolo/ Aplicación	Puerto	Origen
Inbound	SSH (22)	22	0.0.0.0/0

Paso 4 Compruebe si el ECS se puede encender, apagar e iniciar sesión.

- Si es así, vuelva a sustituir el par de claves.
- Si no, vaya a **Paso 5**.

Paso 5 Compruebe si la red está defectuosa.

- En caso afirmativo, póngase en contacto con el soporte técnico para verificar y localizar la falla.
- Si no, vuelva a cambiar el par de claves.

----Fin

3.9 ¿Cómo puedo manejar la falla en el restablecimiento de un par de claves?

Síntoma

Error al restablecer el par de claves en el ECS.

NOTA

El cuadro de diálogo **Failed Key Pair Task** sólo registra y muestra las operaciones de par de claves fallidas en los ECS, que no afectan al estado ECS ni a las operaciones posteriores. Puede hacer clic en **Delete** en la fila del registro de error para eliminarlo, o puede hacer clic en **Delete All** para eliminar todos los registros de error.

Causas posibles

- La dirección de entrada del puerto 22 del grupo de seguridad ECS no está abierta a 100.125.0.0/16.
- El ECS se ha apagado, iniciado o se ha desconectado un disco durante el proceso de restablecer el par de claves para el ECS.
- La conexión de red es defectuosa.
- Las reglas de firewall se han configurado para el ECS.

Procedimiento de manejo

Paso 1 Compruebe si la dirección de entrada del puerto 22 del grupo de seguridad ECS está abierta a 100.125.0.0/16. Es decir, 100.125.0.0/16 puede conectarse remotamente a ECSs de Linux a través de SSH.

- En caso afirmativo, vaya a **Paso 2**.
- Si no, agregue la siguiente regla de grupo de seguridad y restablezca de nuevo el par de claves.

Dirección	Protocolo/ Aplicación	Puerto	Origen
Inbound	SSH (22)	22	0.0.0.0/0

Paso 2 Compruebe si el ECS se puede encender, apagar e iniciar sesión.

- Si es así, restablezca de nuevo el par de claves.
- Si no, vaya a **Paso 3**.

Paso 3 Compruebe si la red está defectuosa.

- En caso afirmativo, póngase en contacto con el soporte técnico para verificar y localizar la falla.
- Si no, restablezca de nuevo el par de claves.

----Fin

3.10 ¿Cómo puedo manejar el fallo en la desvinculación de un par de claves?

Síntoma

Error al desvincular el par de claves del ECS.

NOTA

El cuadro de diálogo **Failed Key Pair Task** sólo registra y muestra las operaciones de par de claves fallidas en los ECS, que no afectan al estado ECS ni a las operaciones posteriores. Puede hacer clic en **Delete** en la fila del registro de error para eliminarlo, o puede hacer clic en **Delete All** para eliminar todos los registros de error.

Causas posibles

- Se ha proporcionado una clave privada incorrecta o no válida.
- La dirección de entrada del puerto 22 del grupo de seguridad ECS no está abierta a 100.125.0.0/16.
- Se ha modificado la configuración SSH del ECS.
- El ECS se ha apagado, iniciado o se ha desconectado un disco durante el proceso de desvinculación del par de claves del ECS.
- La conexión de red es defectuosa.

- Las reglas de firewall se han configurado para el ECS.

Procedimiento de manejo

Paso 1 Compruebe el estado de ECS.

- Si se está ejecutando, vaya a **Paso 2**.
- Si está cerrado, vaya a **Paso 4**.

Paso 2 Utilice el par de claves SSH para iniciar sesión en el ECS y compruebe si la clave privada es correcta.

- Si es correcto, vaya a **Paso 4**.
- Si es incorrecto, utilice la clave privada correcta para desvincular el par de claves de nuevo.

Paso 3 Compruebe si el archivo `/root/.ssh/authorized_keys` del ECS ha sido modificado.

- En caso afirmativo, restaure el contenido original del archivo `/root/.ssh/authorized_keys`.
- Si no, vaya a **Paso 4**.

Paso 4 Compruebe si la dirección de entrada del puerto 22 del grupo de seguridad ECS está abierta a 100.125.0.0/16. Es decir, 100.125.0.0/16 puede conectarse remotamente a los ECS de Linux a través de SSH.

- En caso afirmativo, vaya a **Paso 5**.
- Si no, agregue la siguiente regla de grupo de seguridad y desvincule de nuevo el par de claves.

Dirección	Protocolo/ Aplicación	Puerto	Origen
Inbound	SSH (22)	22	0.0.0.0/0

Paso 5 Compruebe si el ECS se puede encender, apagar e iniciar sesión.

- Si es así, desvincule de nuevo el par de claves.
- Si no, vaya a **Paso 6**.

Paso 6 Compruebe si la red está defectuosa.

- En caso afirmativo, póngase en contacto con el soporte técnico para verificar y localizar la falla.
- Si no, desvincule el par de claves de nuevo.

----Fin

3.11 ¿Necesito reiniciar los servidores después de reemplazar su par de claves?

No. El reemplazo del par de claves no afecta a los servicios.

3.12 ¿Cómo activo el modo de inicio de sesión con contraseña para un ECS?

Si desactiva el modo de inicio de sesión con contraseña al vincular un par de claves a un ECS, puede activar el modo de inicio de sesión con contraseña de nuevo más adelante cuando lo necesite.

Procedimiento

En el ejemplo siguiente se describe cómo iniciar sesión en ECS mediante PuTTY y habilitar el modo de inicio de sesión con contraseña.

Paso 1 Haga doble clic en **PuTTY.EXE**. Se muestra la página **PuTTY Configuration**.

Paso 2 Elija **Connection > Data**. Ingrese el nombre de usuario de la imagen en **Auto-login username**.

NOTA

- Si se utiliza la imagen pública de **CoreOS**, el nombre de usuario de la imagen es **core**.
- Para una imagen pública de **non-CoreOS**, el nombre de usuario de la imagen es **root**.

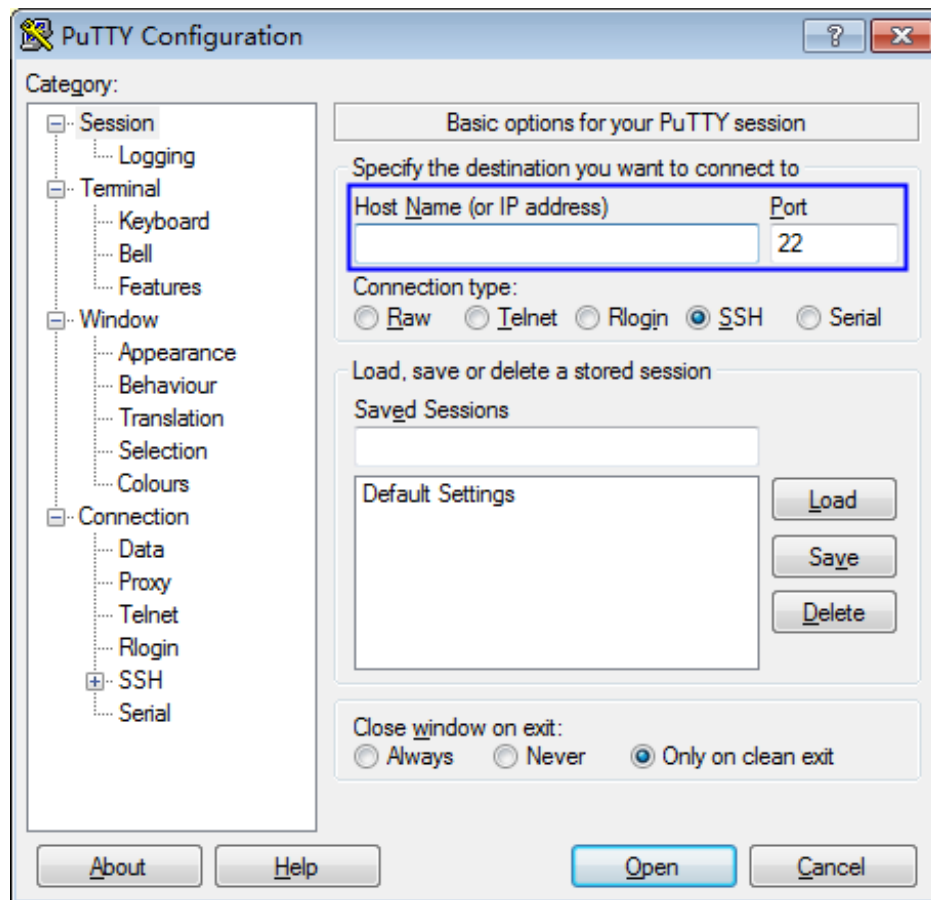
Paso 3 Elija **Connection > SSH > Auth**. En **Private key file for authentication**, haga clic en **Browse** y seleccione un archivo de clave privada (en el formato **.ppk**).

NOTA

Si el archivo está en el formato **.pem**, conviértelo haciendo referencia a [Convertir el archivo de clave privada en el formato .pem al formato .ppk](#).

Paso 4 Haga clic en **Session** e ingrese la EIP del ECS en **Host Name (o IP address)**

Figura 3-8 Configuración de la EIP



Paso 5 Haga clic en **Open** para iniciar sesión en el ECS.

Paso 6 Ejecute el siguiente comando para abrir el archivo `/etc/ssh/sshd_config`:

```
vi /etc/ssh/sshd_config
```

Paso 7 Pulse **i** para entrar en el modo de edición y activar el modo de inicio de sesión con contraseña.

- Para un sistema operativo que no sea SUSE, cambie el valor de **PasswordAuthentication** a **yes**.

```
PasswordAuthentication yes
```

- Para un sistema operativo SUSE, cambie los valores de **PasswordAuthentication** y **UsePAM** a **yes**.

```
PasswordAuthentication yes  
UsePAM yes
```

📖 NOTA

- Non-SUSE OS

Para deshabilitar el inicio de sesión con contraseña, cambie el valor de **PasswordAuthentication** a **no**. Si el parámetro **PasswordAuthentication** no está contenido en el archivo `/etc/ssh/sshd_config` agréguelo y configúrelo en **no**.

- SUSE OS

Para desactivar el inicio de sesión con contraseña, cambie los valores de **PasswordAuthentication** y **UsePAM** a **no**. Si el archivo no contiene los parámetros **PasswordAuthentication** y **UsePAM**, agregue los parámetros y establezca los valores en **no**.

Paso 8 Pulse **Esc** para salir del modo de edición.

Paso 9 Ingrese **:wq** y presione **Enter** para guardar y salir.

Paso 10 Ejecute el siguiente comando para reiniciar el servicio SSH para que la configuración surta efecto:

- Non-Ubuntu14.xx OS
service sshd restart
- Ubuntu14.xx OS
service ssh restart

----Fin

3.13 ¿Cómo manejo el fallo al iniciar sesión en ECS después de desvincular el par de claves?

Síntoma

- Cuando el modo de inicio de sesión para un ECS es el par de claves pero el par de claves inicial ha sido desatado, no hay ninguna contraseña o par de claves disponible para iniciar sesión en el ECS. ¿Cómo puedo solucionar este problema?
- Cuando vinculo un par de claves a un ECS en la consola KPS, desactivo el modo de inicio de sesión con contraseña. Después de que el par de claves esté libre, no tengo contraseña ni par de claves para iniciar sesión en el ECS. ¿Cómo puedo solucionar este problema?

Procedimiento


Método 1: restablecimiento de contraseña


Restablecer la contraseña en la consola de ECS y utilizar la contraseña para iniciar sesión en ECS. Para obtener más información, consulte *Guía del usuario de Elastic Cloud Server*.

Método 2: restablecimiento del par de claves

Apague el ECS, vincule el par de claves al ECS en la consola KPS y use el par de claves para iniciar sesión en el ECS. El procedimiento es el siguiente:

Paso 1 [Inicie sesión en la consola de gestión](#).

Paso 2 Haga clic en  en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

Paso 3 Haga clic en  a la izquierda, elija **Security & Compliance > Data Encryption Workshop**, se mostrará la página de gestión de claves.

Paso 4 Haga clic en **ECS List** para ver los ECS. Para más detalles, consulte [Figura 3-9](#).

Figura 3-9 Lista de ECS

ECS Name/ID	Status	Private IP Address	Elastic IP Address	Associated Key Pair	Operation
ecs-...-windows 0643b313-8b1e-4fe2-873a-1b03053befc6	Running	192.168.0.231	--	--	Bind
ecs-...-pwd3 2625c514-7a29-4b50-a13e-a591610ded9c	Shut down	192.168.0.95	--	--	Bind
ecs-...-euler 984e162e-7f4b-4564-93dc-90043a5dfb8d	Running	192.168.0.27	--	--	Replace Reset

Paso 5 Haga clic en el nombre del ECS de destino. Se muestra la página de detalles de ECS.

Paso 6 Haga clic en **Shut Down** en la esquina superior derecha de la página para cerrar el ECS.

Paso 7 Vuelva a la página de la lista de ECS haciendo referencia al paso **Paso 5**.

Paso 8 Haga clic en **Bind** en la fila del ECS de destino. Aparece el cuadro de diálogo **Bind Key Pair**.

Paso 9 Seleccione un nuevo par de claves en el cuadro de lista desplegable de **New Key Pair**.

Figura 3-10 Vinculación de un par de claves

Bind Key Pair [Close]

i The system will configure the key pair for the server. After this operation, you can use the key to log in to the server. To ensure security, it is recommended that you disable the password login mode of the server and use only the key to log in to the server.

ECS Name: ecs-...-windows

IP Address: 192.168.0.231

Status: Shut down

* New Key Pair: Select a new key pair.

Disable the password login mode. [Learn more](#)

I have read and agree to the [Key Pair Service Disclaimer](#)

[OK] [Cancel]

Paso 10 Puede elegir si desea desactivar el modo de inicio de sesión de contraseña según sea necesario. De forma predeterminada, el modo de inicio de sesión con contraseña está deshabilitado.

NOTA

- Si no deshabilita el modo de inicio de sesión con contraseña, puede usar la contraseña o el par de claves para iniciar sesión en ECS.
- Si el modo de inicio de sesión con contraseña está deshabilitado, solo puede usar el par de claves para iniciar sesión en el ECS. Si necesita utilizar el modo de inicio de sesión con contraseña más adelante, puede activar el modo de inicio de sesión con contraseña de nuevo. Para obtener más información, véase [¿Cómo activo el modo de inicio de sesión con contraseña para un ECS?](#).

Paso 11 Seleccione **I have read and agree to the Key Pair Service Disclaimer**.

Paso 12 Haga clic en **OK**. El par de claves está enlazado. Una vez completado el enlace, puede utilizar el par de claves para iniciar sesión en el ECS.

---Fin

3.14 ¿Qué debo hacer si se pierde mi clave privada?

Para clave privada gestionada en KPS

Puede exportar la clave privada de KPS de nuevo.

Para clave privada no gestionada en KPS

La clave privada no se puede recuperar.

Puede restablecer la contraseña o el par de claves enlazadas al ECS. Para más detalles, consulte [¿Cómo manejo el fallo al iniciar sesión en ECS después de desvincular el par de claves?](#)

3.15 ¿Cómo convierto el formato de un archivo de clave privada?

Convertir el archivo de clave privada en el formato .ppk al formato .pem

La clave privada que se va a cargar o copiar en el cuadro de texto debe estar en formato .pem. Si el archivo está en formato .ppk, realice los siguientes pasos:

Paso 1 Visite el siguiente sitio web y descargue PuTTY y PuTTYgen:

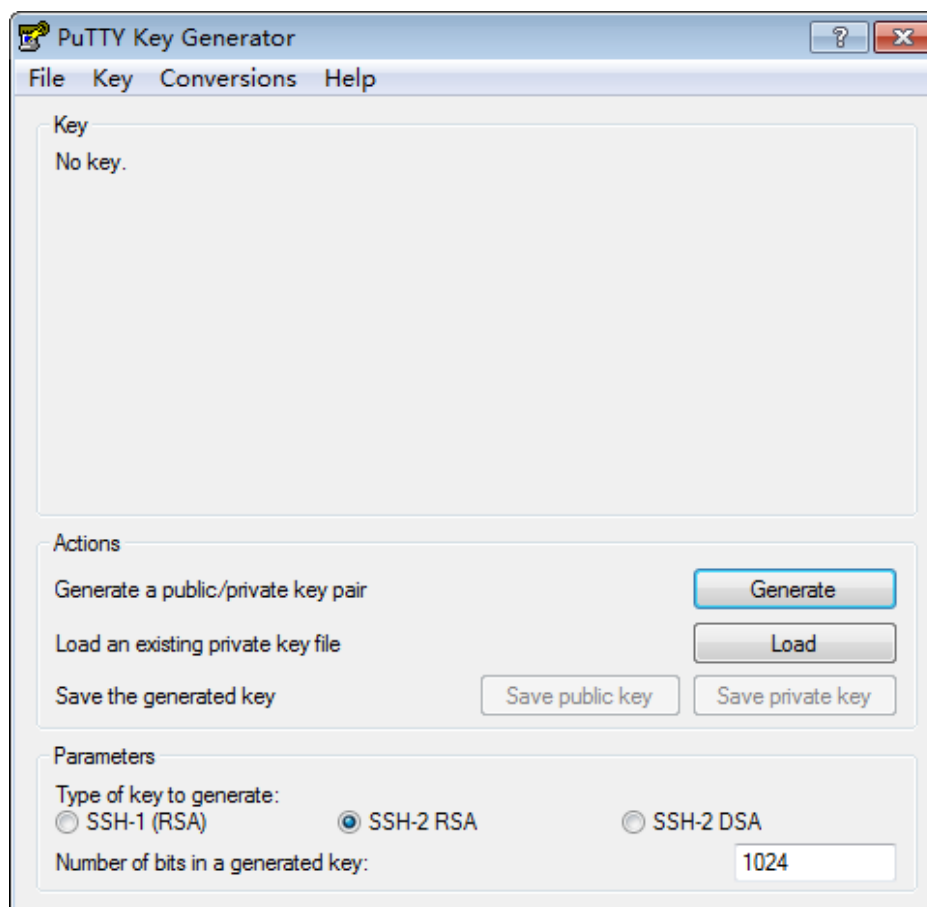
<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

NOTA

PuTTYgen es un generador de claves privadas, que se utiliza para crear un par de claves que consiste en una clave pública y una clave privada para PuTTY.

Paso 2 Haga doble clic en **PuTTYGEN.exe**. Se muestra la página **PuTTY Key Generator**, como se muestra en [Figura 3-11](#).

Figura 3-11 Generador de claves de PuTTY



Paso 3 Elija **Conversions > Import Key** para importar el archivo de clave privada en el formato **.ppk**.

Paso 4 Elija **Conversions > Export OpenSSH Key**, se muestra el cuadro de diálogo **PuTTYgen Warning**.

Paso 5 Haga clic en **Yes** para guardar el archivo en el formato **.pem**.

----Fin

Convertir el archivo de clave privada en el formato **.pem** al formato **.ppk**

Quando utiliza PuTTY para iniciar sesión en un ECS de Linux, la clave privada debe estar en formato **.ppk**. Si el archivo está en formato **.pem**, realice los siguientes pasos para ocultar su formato:

Paso 1 Visite el siguiente sitio web y descargue PuTTY y PuTTYgen:

<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

📖 NOTA

PuTTYgen es un generador de claves privadas, que se utiliza para crear un par de claves que consiste en una clave pública y una clave privada para PuTTY.

Paso 2 Haga doble clic en **PuTTYgen.exe**. Se muestra la ventana **PuTTY Key Generator**.

Paso 3 En el área **Actions**, haga clic en **Load** e importar el archivo de clave privada que almacenó al comprar el ECS.

Asegúrese de que **All files (*.*)** incluya el formato de archivo de clave privada.

Paso 4 Haga clic en **Save private key**.

Paso 5 Guarde la clave privada convertida, por ejemplo **kp-123.ppk** en un directorio local.

---Fin

3.16 ¿Puedo cambiar el par de claves de un servidor?

Sí.

Puede desvincular, restablecer o reemplazar un par de claves según sea necesario. Para obtener más información, consulte [Gestión de pares de clave](#).

3.17 ¿Puede un par de claves ser compartido por varios usuarios?

Los pares de claves no se pueden compartir entre cuentas, pero los usuarios de IAM pueden compartirlos con la misma cuenta de cualquiera de las siguientes maneras:

- Importar un par de claves. Para permitir que varios usuarios de IAM usen el mismo par de claves, puede crear un par de claves (mediante PuTTYgen u otras herramientas) e importarlo como un recurso de usuario de IAM. Para obtener más información, consulte [Importación de un par de clave](#).
- Actualizar un par de claves de usuario a un par de claves de cuenta. Puede [actualizar](#) un par de claves [creado en la consola de gestión](#) o importado a la consola.

3.18 ¿Cómo obtengo el archivo de clave pública o privada de un par de claves?

Obtención de un archivo de clave privada

Cuando [crea un par de claves](#), su archivo de clave privada se descargará automáticamente.

- Si la clave privada no se gestiona, no se puede descargar más tarde. Guárdelo correctamente.
- Si ha autorizado a Huawei Cloud para gestionar claves privadas, puede exportar las claves privadas gestionadas. Para obtener más información, consulte [Exportación de una clave privada](#).

Obtención de un archivo de clave pública

- Si se crea un par de claves en la consola de gestión, su clave pública se almacena automáticamente en Huawei Cloud. Puede presionar **F12** para actualizar la lista de pares de claves y tomar nota del campo **public_key** de la lista.
- Si se creó un par de claves usando PuTTYgen, puede encontrar su clave pública en la ruta de almacenamiento de su PC local.

3.19 ¿Qué puedo hacer si se informa de un error cuando se crea o actualiza una clave de cuenta por primera vez?

Creación de un par de claves de cuenta por primera vez

Al crear un par de claves de cuenta por primera vez, debe usar un usuario con el rol de sistema de administrador de tenant.

Actualización de un par de claves de cuenta por primera vez

Después de actualizar un par de claves a un par de claves de cuenta, todos los usuarios de su cuenta pueden ver y usar el par de claves. Si un nombre de par de claves es el mismo que el nombre de par de claves privadas de otro subusuario, no se puede realizar la actualización. Para actualizar los pares de claves, los usuarios con el rol de sistema administrador de tenant deben realizar la actualización al menos una vez. El número de pares de claves que se van a actualizar no está limitado.

3.20 ¿Se ocupará la cuota del par de claves de cuenta después de que se actualice un par de claves privadas a un par de claves de cuenta?

No.

Si un par de claves privadas se actualiza a un par de claves de cuenta, la cuota de par de claves de cuenta no está ocupada.

4 Relacionado con HSM dedicado

4.1 ¿Qué es el HSM dedicado?

HSM dedicado es un servicio en la nube utilizado para la encriptación, desencriptación, firma, verificación de firmas, generación de claves y almacenamiento seguro de claves.

HSM dedicado proporciona hardware de encriptación, lo que garantiza la seguridad e integridad de los datos en Elastic Cloud Servers (los ECS) y cumple con los requisitos FIPS 140-2. HSM dedicado le ofrece una gestión segura y confiable de las claves generadas por sus instancias, y utiliza múltiples algoritmos para la encriptación y desencriptación de datos.

4.2 ¿Cómo garantiza el HSM dedicado la seguridad para la generación de claves?

- El usuario crea una clave de forma remota. Durante la creación, solo el UKey propiedad del usuario está involucrado en la autenticación.
- La configuración de HSM y la preparación de claves internas se pueden realizar solo después de ser autenticadas usando el UKey como la credencial.

El usuario tiene control total sobre la generación, almacenamiento y acceso de claves. El HSM dedicado solo es responsable de monitorear y gestionar los HSM y las instalaciones de red relacionadas.

4.3 ¿El personal de la sala de equipos tiene la función de súper administrador para robar información mediante el uso de un UKey privilegiado?

Los UKeys son propiedad únicamente de los usuarios que compraron instancias HSM dedicadas. El personal de la sala de equipos no tiene la función de superadministrador.

Los datos confidenciales (claves) se almacenan en chips. Incluso el proveedor de HSM no puede acceder a la información de clave interna.

4.4 ¿Qué HSM se utilizan para HSM dedicado?

HSM dedicado utiliza HSM que han obtenido la certificación de la Administración Estatal de Criptografía de China (CSCA) y la certificación FIPS 140-2 de nivel 3, logrando una alta seguridad.

4.5 ¿Qué API admite HSM dedicado?

HSM dedicado proporciona las mismas funciones e interfaces que los dispositivos criptográficos físicos, lo que le ayuda a migrar fácilmente los servicios a la nube. Las API compatibles incluyen PKCS#11 y CSP.

Para obtener más información, véase [Ediciones](#).

4.6 ¿Cómo habilito el acceso público a una instancia de HSM dedicado?

Puede vincular EIP para acceder a instancias de HSM dedicado desde la red pública.

Prerrequisitos

Tiene una EIP que puede vincularse a la instancia de HSM dedicado.

NOTA


Para obtener más información sobre cómo solicitar una EIP, consulte .


Restricciones

- Después de que una EIP se vincula a una instancia de HSM dedicado, pueden producirse ataques de red pública. Tenga cuidado al vincular una EIP a una instancia HSM dedicado.
- A las EIP se les cobran recursos. Es necesario configurar las EIP según sea necesario. Si no necesita las EIP, desvínculelas oportunamente. Para obtener más información sobre cómo desvincular EIP, consulte . Si la EIP no se libera después de la desvinculación, Huawei Cloud cobrará la tarifa de retención de direcciones IP. Si una EIP de pago por uso facturado por ancho de banda no está vinculado de una instancia, el ancho de banda continuará siendo facturado. Para obtener más información, consulte [¿Por qué me siguen facturando después de que mi EIP se haya liberado o no vinculado?](#)

Procedimiento

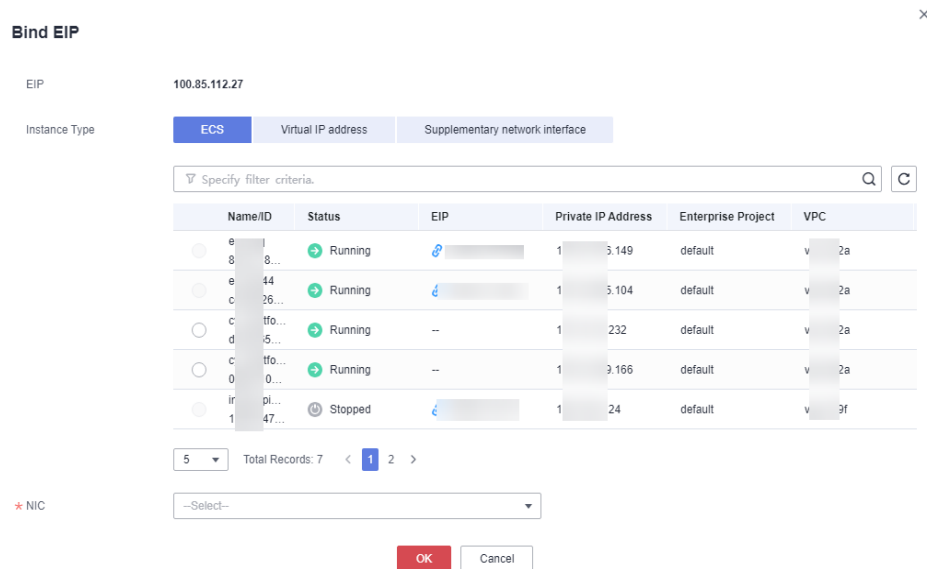
Paso 1 [Inicie sesión en la consola de gestión](#).

Paso 2 Haga clic en  en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

Paso 3 Haga clic en  a la izquierda de la página. Seleccione **Network > EIP**. La página EIP se muestra por defecto.

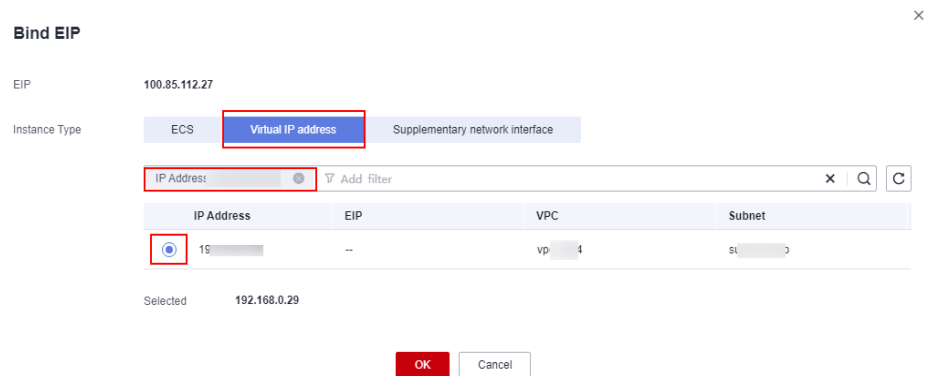
Paso 4 Haga clic en **Bind** en la columna **Operation** de la EIP de destino. Se muestra la página Vinculación, como se muestra en **Figura 4-1**.

Figura 4-1 Vinculación de una EIP



Paso 5 Haga clic en **Virtual IP Address**, introduzca la dirección IPv4 de la instancia que desea enlazar en el cuadro de búsqueda y seleccione el resultado de la búsqueda, como se muestra en **Vinculación de una dirección IP virtual**.

Figura 4-2 Vinculación de una dirección IP virtual



Paso 6 Seleccione la dirección IP correspondiente y haga clic en **OK**.

----Fin

5 Precios

5.1 ¿Cómo se carga el DEW?

Para obtener detalles de precios, consulte [Detalles de precios del producto](#).

KMS

KMS se cobra por uso. No se requiere una tarifa mínima. Una vez que se crea un CMK, se cargará por hora. Usted paga por los CMK que creó y las solicitudes de API que están más allá del rango gratuito.

KPS

- Si no decide dejar que Huawei Cloud gestione sus claves privadas al crearlas o importarlas, no se incurrirá en ningún costo.
- Si tiene sus claves gestionadas por Huawei Cloud, KPS se cobra por hora. En la versión actual, es gratuito.

HSM dedicado

HSM dedicado ofrece paquetes mensuales y anuales basados en la edición y los modelos de dispositivos de las instancias que ha comprado.

CSMS

Se le cobra en función del número de secretos, la duración del uso y el número de solicitudes de API.

5.2 ¿Cómo renuevo DEW?

En esta sección se describe cómo renovar KMS o una instancia de HSM dedicado. Después de la renovación, puede seguir utilizando la instancia de KMS y HSM dedicado.

- Renovación automática

Si ha seleccionado y aceptado la renovación automática de KMS o HSM dedicado, el sistema genera automáticamente un pedido de renovación y renueva la suscripción según el período de suscripción original antes de que expire el servicio.

- **Renovación manual**

Antes de que caduque el servicio, el sistema enviará un mensaje SMS o correo electrónico para recordarle que debe renovarlo.

Si no renueva el servicio antes de que caduque, entrará en el período de retención.

 **NOTA**

Si no renueva su suscripción antes de que caduque, se aplicará un período de retención. El período de retención varía según los niveles de cliente. Para obtener más información, consulte [Período de retención](#).

Tabla 5-1 Período de retención

Servicio	Edición	Período de retención
KMS	Standard	Las claves están congeladas. Active las claves congeladas recargando la cuenta.
Dedicado HSM	-	<ul style="list-style-type: none"> ● Dentro del período de retención, las instancias de HSM dedicado no se pueden usar, pero están reservadas para usted. ● Si el período de retención expira, se liberarán las instancias de HSM dedicadas.

 **NOTA**

- Las claves congeladas no se pueden usar para cifrado o descifrado. Para evitar pérdidas innecesarias, se recomienda que renueve el servicio a tiempo.
- Los datos relacionados con las instancias de HSM dedicadas se perderán cuando se publiquen las instancias. Para evitar pérdidas innecesarias, se recomienda renovar el servicio o recargar la cuenta a tiempo.

Prerrequisitos


Ha obtenido la cuenta de inicio de sesión (con los permisos **BSS Administrator** y **KMS Administrator**) y la contraseña para iniciar sesión en la consola de gestión.


 **NOTA**

Una cuenta con el permiso **BSS Administrator** puede realizar cualquier operación en todos los elementos del menú en el centro de cuentas, el centro de facturación y el centro de recursos.

Procedimiento

Paso 1 [Inicie sesión en la consola de gestión](#).

Paso 2 Haga clic en  en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

Paso 3 En el panel de navegación de la izquierda, haga clic en  y elija **Security & Compliance > Data Encryption Workshop**.

Paso 4 En la esquina superior derecha, haz clic en **Renew**.

Paso 5 En la página de gestión de renovación, complete la renovación según se le indique.

Para obtener más información, consulte [Renovación manual de un recurso](#).

----Fin

5.3 ¿Cómo me doy de baja de DEW?

DEW no admite la cancelación de la suscripción.

NOTA

Si no puede crear una instancia HSM dedicada, puede hacer clic en **Delete** en la fila donde se encuentra la instancia fallida para eliminarla. A continuación, puede enviar un ticket de servicio para solicitar el reembolso.

Enlaces útiles

- [Reglas de cancelación de suscripción](#)
- [Lista de productos de servicios en la nube de los que no puede darse de baja](#)
- [Creación de un ticket de servicio](#)

5.4 ¿Se cobrará un CMK después de estar discapacitado?

Sí.

KMS conserva y mantiene una CMK deshabilitada. Puede habilitarlo siempre que lo necesite. Por lo tanto, un CMK deshabilitado todavía es facturable. Solo los CMK eliminados no se cobran.

5.5 ¿Se facturan las credenciales programadas para eliminarlas?

No.

Una credencial en estado de eliminación pendiente no incurre en cargos.

Si cancela la eliminación, el cargo se reanudará a partir del momento en que se programó la eliminación de la credencial.

5.6 ¿Se cobrará un CMK después de que esté programado para eliminarlo?

No.

El período pendiente de un CMK desde su programación hasta su eliminación no se cobra.

Sin embargo, si cancela la eliminación programada, el cargo se reanudará a partir del momento en que el CMK está programado para ser eliminado.

6 General

6.1 ¿Qué funciones proporciona DEW?

Key Management Service

- En la consola KMS, puede:
 - Crear, consultar, habilitar y deshabilitar CMK, así como programar y cancelar la eliminación de CMK.
 - Modificar el alias y las descripciones de los CMK.
 - Utilizar la herramienta en línea para cifrar y descifrar datos de pequeño tamaño.
 - Agregar, buscar, editar y eliminar etiquetas.
 - Crear, cancelar y consultar concesiones.

- Puedes usar las API para:
 - Crear, cifrar o descifrar DEK.
 - Retirar concesiones.
 - Firmar o verificar la firma de los mensajes o resúmenes de mensajes.
 - Generar y verificar códigos de autenticación de mensajes.

Para obtener más información, consulta la *Referencia de la API de Data Encryption Workshop*.

- Generar hardware verdaderos números aleatorios.
Puede generar números aleatorios de 512 bits basados en hardware mediante la API de KMS. Los números aleatorios verdaderos de 512 bits se pueden usar como base para materiales clave y parámetros de encriptación. Para obtener más información, consulta la *Referencia de la API de Data Encryption Workshop*.

Key Pair Service

Con la consola de KPS o las API, puede realizar las siguientes operaciones en pares de claves:

- Creación, importación, visualización y eliminación de pares de claves
- Restablecimiento, sustitución, vinculación y desvinculación de pares de claves
- Gestión, importación, exportación y borrado de claves privadas

HSM dedicado

En la página **Dedicated HSM** de la consola de gestión, puede comprar instancias HSM dedicadas

6.2 ¿Qué algoritmos de criptografía utiliza DEW?

Algoritmos criptográficos soportados por KPS

- Los pares de claves SSH creados en la consola de gestión admiten los siguientes algoritmos criptográficos:
 - SSH-ED25519
 - ECDSA-SHA2-NISTP256
 - ECDSA-SHA2-NISTP384
 - ECDSA-SHA2-NISTP521
 - SSH_RSA: The length can be 2048, 3072, and 4096 bits.
- Las claves SSH importadas a la consola KPS admiten los siguientes algoritmos criptográficos:
 - SSH-DSS
 - SSH-ED25519
 - ECDSA-SHA2-NISTP256
 - ECDSA-SHA2-NISTP384
 - ECDSA-SHA2-NISTP521
 - SSH_RSA: La longitud puede ser de 2048, 3072, 4096 bits.

Algoritmos de criptografía compatibles

Puede utilizar algoritmos criptográficos chinos y algunos algoritmos criptográficos internacionales comunes para satisfacer diversos requisitos del usuario.

Tabla 6-1 Algoritmos de criptografía compatibles

Categoría	Algoritmo criptográfico común
Algoritmo criptográfico simétrico	AES
Algoritmo criptográfico asimétrico	RSA, DSA, ECDSA, DH, y ECDH
Algoritmo de codificación	SHA1, SHA256 y SHA384

6.3 ¿En qué regiones están disponibles los servicios DEW?

Los servicios DEW están disponibles en las siguientes regiones:

- KMS

- CN-Hong Kong
- AP-Bangkok
- AP-Singapore
- AF-Johannesburg
- LA-Mexico City1
- LA-Mexico City2
- LA-Santiago
- LA-Sao Paulo1
- KPS
 - CN-Hong Kong
 - AP-Bangkok
 - AP-Singapore
 - LA-Sao Paulo1
- CSMS
 - CN-Hong Kong
 - AP-Bangkok
 - AP-Singapore
 - LA-Sao Paulo1
- HSM dedicado
 - CN-Hong Kong
 - AP-Bangkok
 - AP-Singapore
 - LA-Santiago

6.4 What Is a Quota?

What Is a Quota?

Quotas are enforced for service resources on the platform to prevent unforeseen spikes in resource usage. Quotas can limit the number or amount of resources available to users. For example, the maximum number of CMKs that you can create.

If the existing resource quota cannot meet your service requirements, you can apply for a higher quota.

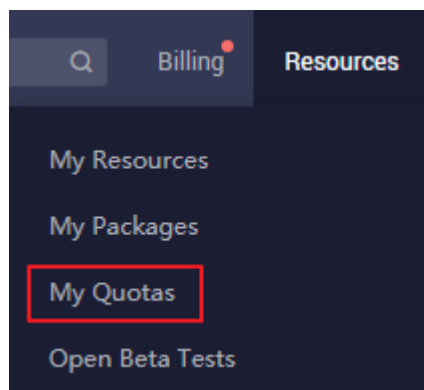
How Do I View My Quota?

Paso 1 Log in to the management console.

Paso 2 In the upper right corner of the page, choose **Resources > My Quotas**.

The **Service Quota** page is displayed.

Figura 6-1 My quotas



Paso 3 View the used and total quota of each type of resources on the displayed page.

Paso 4 If a quota cannot meet your service requirements, click **Increase Quota** to change it.

----Fin

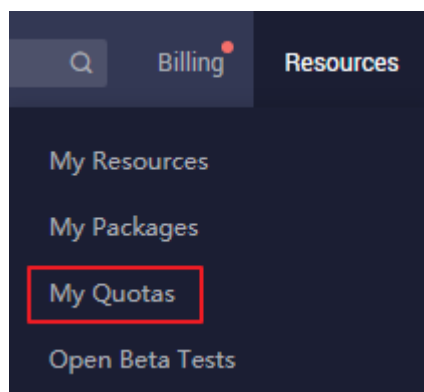
How Do I Increase a Quota?

Paso 1 Log in to the management console.

Paso 2 In the upper right corner of the page, choose **Resources > My Quotas**.

The **Service Quota** page is displayed.

Figura 6-2 My quotas



Paso 3 Click **Increase Quota**.

Paso 4 On the **Create Service Ticket** page, configure parameters as required.

In the **Problem Description** area, fill in the content and reason for the increase.

Paso 5 After all mandatory parameters are configured, select **I have read and agree to the Tenant Authorization Letter and Privacy Statement** and click **Submit**.

----Fin

6.5 ¿Qué es el mecanismo de asignación de recursos de DEW?

DEW utiliza regiones como grandes grupos de recursos y recursos o servicios independientes de cada cliente como pequeños grupos de recursos. El fondo tiene límites de tráfico por defecto. Para un solo usuario, si el tráfico excede el umbral, la velocidad de servicio es lenta. En el caso de clientes con grandes necesidades de tráfico, los recursos de fondo pueden modificarse en función de la situación y las necesidades reales.

Si su volumen de tráfico excede el límite, puede enviar un ticket de servicio para aumentar la cuota. DEW ajustará su límite en segundo plano para admitir el aprovisionamiento de clústeres de configuración dedicados y garantizar una ejecución estable del servicio.

6.6 ¿Qué son las Regiones y las AZ?

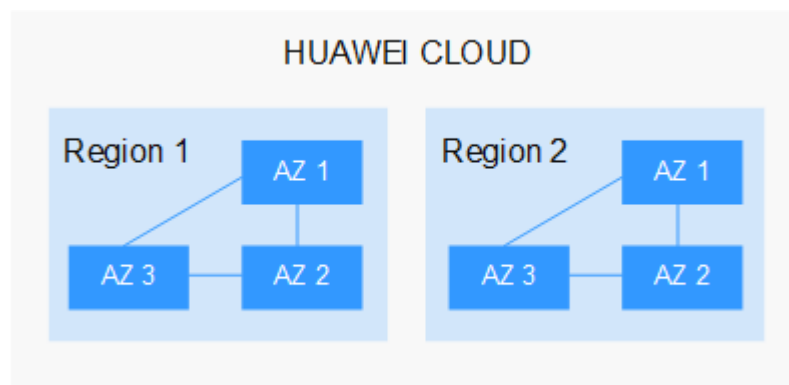
Conceptos

Una región y una zona de disponibilidad (AZ) identifican la ubicación de un centro de datos. Puede crear recursos en una región específica y AZ.

- Las regiones se dividen de las dimensiones de la ubicación geográfica y la latencia de la red. Los servicios públicos, como Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP) e Image Management Service (IMS), se comparten dentro de la misma región. Las regiones se clasifican como regiones universales y regiones dedicadas. Una región universal proporciona servicios en la nube universales para los tenants estándares. Una región dedicada proporciona servicios del mismo tipo solo o para tenants específicos.
- Una AZ contiene uno o más centros de datos físicos. Cada AZ cuenta con instalaciones independientes de electricidad, de refrigeración, de extinción de incendios y a prueba de humedad. Dentro de una AZ, los recursos de computación, red, almacenamiento y otros se dividen de forma lógica en múltiples clústeres. Las AZ dentro de una región están interconectadas mediante fibras ópticas de alta velocidad para permitirle construir sistemas de alta disponibilidad entre AZ.

Figura 6-3 muestra la relación entre las regiones y las zonas de disponibilidad.

Figura 6-3 Región y AZ



Huawei Cloud ofrece servicios en muchas regiones de todo el mundo. Puede seleccionar una región y una AZ según sea necesario.

Selección de una región

Al seleccionar una región, tenga en cuenta los siguientes factores:

- Localización

Se recomienda seleccionar una región cercana a usted o a sus usuarios objetivo. Esto reduce la latencia de la red y mejora la velocidad de acceso.

- Si usted o sus usuarios se encuentran en la región Asia Pacífico y fuera de China continental, seleccione la región **CN-Hong Kong**, **AP-Bangkok** o **AP-Singapore**.
- Si usted o sus usuarios están en África, seleccione la región **AF-Johannesburg**.
- Si usted o sus usuarios están en América Latina, seleccione la región **LA-Santiago**.

- Precio del recurso

Los precios de los recursos pueden variar en diferentes regiones. Para obtener más información, consulte [Detalles de precios del producto](#).

Selección de una AZ

Al determinar si se deben desplegar recursos en la misma AZ, tenga en cuenta los requisitos de recuperación ante desastres (DR) y latencia de red de sus aplicaciones.

- Para una alta capacidad de DR, despliegue recursos en diferentes AZ en la misma región.
- Para una baja latencia de red, implemente recursos en la misma AZ.

Regiones y puntos de conexión

Antes de usar una API para invocar a recursos, especifique su región y punto de conexión. Para obtener más información, consulte [Regiones y puntos de conexión](#).

6.7 Can DEW Be Shared Across Accounts?


No. Currently, a user can only use and manage their own keys and key pairs.

6.8 ¿Cómo accedo a las funciones de DEW?

Puede usar DEW en la consola web o invocar a las funciones de DEW mediante API basadas en HTTPS.

- Consola

Si se ha registrado en la nube pública, puede iniciar sesión en la consola de gestión

directamente. En la esquina superior izquierda de la consola, haga clic en . Elija **Security & Compliance > Data Encryption Workshop**.

- API

Puedes acceder a DEW usando la API. Para obtener más información, consulte la *Referencia de la API de Data Encryption Workshop*.

DEW admite las API de REST, lo que le permite invocar a las API mediante HTTPS. Puede utilizar las API proporcionadas para realizar operaciones en claves y pares de claves, como crear, consultar y eliminar claves.

Las API de DEW utilizan el protocolo HTTPS para cifrar y proteger la transmisión, evitando ataques man-in-the-middle.