

Data Encryption Workshop

Guía del usuario de

Edición 26
Fecha 2024-09-13



Copyright © Huawei Technologies Co., Ltd. 2024. Todos los derechos reservados.

Quedan terminantemente prohibidas la reproducción y la divulgación del presente documento en todo o en parte, de cualquier forma y por cualquier medio, sin la autorización previa de Huawei Technologies Co., Ltd. otorgada por escrito.

Marcas y permisos



HUAWEI 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

Las funciones, los productos y los servicios adquiridos están estipulados en el contrato celebrado entre Huawei y el cliente. Es posible que la totalidad o parte de los productos, las funciones y los servicios descritos en el presente documento no se encuentren dentro del alcance de compra o de uso. A menos que el contrato especifique lo contrario, ninguna de las afirmaciones, informaciones ni recomendaciones contenidas en este documento constituye garantía alguna, ni expresa ni implícita.

La información contenida en este documento se encuentra sujeta a cambios sin previo aviso. En la preparación de este documento se realizaron todos los esfuerzos para garantizar la precisión de sus contenidos. Sin embargo, ninguna declaración, información ni recomendación contenida en el presente constituye garantía alguna, ni expresa ni implícita.

Huawei Technologies Co., Ltd.

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

Sitio web: <https://www.huawei.com>

Email: support@huawei.com

Índice

1 Key Management Service.....	1
1.1 Tipos de claves.....	1
1.2 Creación de una clave.....	2
1.3 Creación de CMK mediante materiales de clave importados.....	6
1.3.1 Descripción.....	6
1.3.2 Importación de materiales de clave.....	7
1.3.3 Eliminación de materiales de clave.....	16
1.4 Gestión de CMK.....	16
1.4.1 Consulta de un CMK.....	17
1.4.2 Habilidadación de uno o más CMK.....	19
1.4.3 Deshabilitación de uno o más CMK.....	19
1.4.4 Eliminación de uno o más CMK.....	20
1.4.5 Cancelación de la eliminación programada de uno o más CMK.....	22
1.4.6 Adición de una clave a un proyecto.....	22
1.5 Búsqueda de una clave.....	23
1.6 Uso de la herramienta en línea para cifrar y descifrar datos de tamaño pequeño.....	24
1.7 Gestión de etiquetas.....	26
1.7.1 Adición de una etiqueta.....	26
1.7.2 Modificación de valores de etiqueta.....	28
1.7.3 Eliminación de etiquetas.....	29
1.8 Rotación de CMKs.....	30
1.8.1 Acerca de rotación de clave.....	30
1.8.2 Habilidadación de la rotación de clave.....	32
1.8.3 Deshabilitación de la rotación de clave.....	35
1.9 Managing a Grant.....	36
1.9.1 Creación de una concesión.....	36
1.9.2 Consulta de una concesión.....	40
1.9.3 Revocación de una concesión.....	41
2 Cloud Secret Management Service.....	43
2.1 Creación de un secreto.....	43
2.1.1 Creación de un secreto compartido.....	43
2.2 Gestión de secretos.....	45
2.2.1 Ver un secreto.....	45

2.2.2 Búsqueda de secretos por evento.....	46
2.2.3 Eliminación de un secreto.....	47
2.3 Gestión de versiones de secreto.....	48
2.3.1 Guardar y ver valores secretos.....	48
2.3.2 Gestión de estados de versión de secreto.....	49
2.3.3 Setting the Version Expiration Time.....	51
2.4 Gestión de etiquetas.....	52
2.4.1 Adición de una etiqueta.....	52
2.4.2 Búsqueda de un secreto por etiqueta.....	54
2.4.3 Modificación de un valor de etiqueta.....	55
2.4.4 Eliminación de una etiqueta.....	56
2.5 Creación de un evento.....	56
2.6 Gestión de eventos.....	58
2.6.1 Consulta de eventos.....	58
2.6.2 Edición de un evento.....	60
2.6.3 Habilitación de un evento.....	60
2.6.4 Desactivación de un evento.....	61
2.6.5 Eliminación de un evento.....	62
2.7 Consulta de notificaciones.....	63
3 Key Pair Service.....	65
3.1 Creación de un par de claves.....	65
3.2 Importación de un par de claves.....	70
3.3 Actualización de un par de claves.....	74
3.4 Gestión de pares de claves.....	75
3.4.1 Vinculación de un par de claves.....	75
3.4.2 Vinculación de pares de clave en lotes.....	78
3.4.3 Consulta de un par de claves.....	81
3.4.4 Restablecimiento de un par de claves.....	84
3.4.5 Sustitución de un par de claves.....	85
3.4.6 Desvinculación de un par de claves.....	87
3.4.7 Eliminación de un par de clave.....	90
3.5 Gestión de claves privadas.....	90
3.5.1 Importación de una clave privada.....	90
3.5.2 Exportación de una clave privada.....	92
3.5.3 Borrar una clave privada.....	94
3.6 Uso de una clave privada para iniciar sesión en Linux ECS.....	94
3.7 Uso de una clave privada para obtener la contraseña de inicio de sesión de Windows ECS.....	97
4 HSM dedicado.....	99
4.1 Guía de operación.....	99
4.2 Compra de una instancia de HSM dedicado.....	101
4.2.1 Creación de una instancia de HSM dedicado.....	102
4.2.2 Activación de una instancia de HSM dedicado.....	104

4.3 Consulta de instancias de HSM dedicado.....	108
4.4 Gestión de etiquetas.....	111
4.4.1 Adición de una etiqueta.....	111
4.4.2 Búsqueda de una instancia de HSM dedicado por etiqueta.....	113
4.4.3 Modificación de un valor de etiqueta.....	114
4.4.4 Eliminación de una etiqueta.....	115
4.5 Uso de instancias de HSM dedicado.....	116
5 Gestión de etiquetas.....	119
5.1 Descripción.....	119
5.2 Creating a Tag Policy.....	121
5.3 Creating a Tag.....	124
5.4 Búsqueda de una clave personalizada por etiqueta.....	126
5.5 Modificación de un valor de etiqueta.....	128
5.6 Deleting a Tag.....	128
6 Registros de auditoría.....	130
6.1 Operaciones apoyadas por CTS.....	130
6.2 Uso de CTS para consultar rastros de operación de DEW.....	133
7 Control de permisos.....	134
7.1 Crear un usuario y autorizar al usuario el permiso para acceder a DEW.....	134
7.2 Creación de una política de DEW personalizada.....	140

1 Key Management Service

1.1 Tipos de claves

Los CMK incluyen claves personalizadas y claves predeterminadas. Esta sección describe cómo crear, ver, habilitar, deshabilitar, programar la eliminación y cancelar la eliminación de claves personalizadas.

Las claves personalizadas se pueden clasificar en claves simétricas y asimétricas.

Las claves simétricas se utilizan más comúnmente para la protección de la encriptación de datos. Las claves asimétricas se utilizan para la verificación de firma digital o la encriptación de información confidencial en sistemas donde la relación de confianza no es mutua. Una clave asimétrica consiste en una clave pública y una clave privada. La clave pública se puede enviar a cualquier persona. La clave privada debe estar almacenada de forma segura y solo accesible para usuarios de confianza.

Se puede usar una clave asimétrica para generar y verificar una firma. Para transferir datos de forma segura, un firmante envía la clave pública a un receptor, utiliza la clave privada para firmar datos y, a continuación, envía los datos y la firma al receptor. El receptor puede usar la clave pública para verificar la firma.

Tabla 1-1 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

Tipo de clave	Tipo de algoritmo	Especificaciones de clave	Descripción	Uso
Clave simétrica	SM3	HMAC_SM3	Clave simétrica de SM3	Genera y verifica un código de autenticación de mensaje
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

1.2 Creación de una clave

Esta sección describe cómo crear una clave personalizada en la consola KMS.

Las claves personalizadas se pueden clasificar en claves simétricas y asimétricas.

Prerrequisitos

La cuenta tiene KMS CMKFullAccess o permisos superiores.

Restricciones

- Puede crear hasta 20 claves personalizadas, excluidas las claves predeterminadas. Las claves de réplica ocupan la cuota de claves personalizadas en la región.
- Las claves simétricas se crean utilizando la clave AES. La clave AES-256 se puede utilizar para cifrar y descifrar una pequeña cantidad de datos o claves de datos. La clave HMAC se utiliza para generar y verificar códigos de autenticación de mensajes.
- Las claves asimétricas se crean utilizando algoritmos RSA o ECC. Las claves RSA se pueden utilizar para encriptación, desencriptación, la firma digital y la verificación de firmas. Las claves ECC solo se pueden utilizar para la firma digital y la verificación de firmas.
- Los alias de las claves predeterminadas terminan con **/default**. Al elegir alias para las claves personalizadas, no utilice alias que terminen con **/default**.
- Las claves DEW se pueden invocar a través de API para 20,000 veces de forma gratuita al mes.


Escenarios

- [Cifrar datos en OBS](#)
- [Cifrar datos en EVS](#)
- [Cifrar datos en IMS](#)

- **Cifrar una instancia de base de datos de RDS**
- Utilice claves personalizadas para cifrar y descifrar directamente pequeños volúmenes de datos.
- Encriptación y descryptación de DEK para aplicaciones de usuario
- Generación y verificación de código de autenticación de mensajes
- Las claves asimétricas se pueden utilizar para firmas digitales y verificación de firmas.

Creación de una clave

Paso 1 Inicie sesión en la consola de gestión.

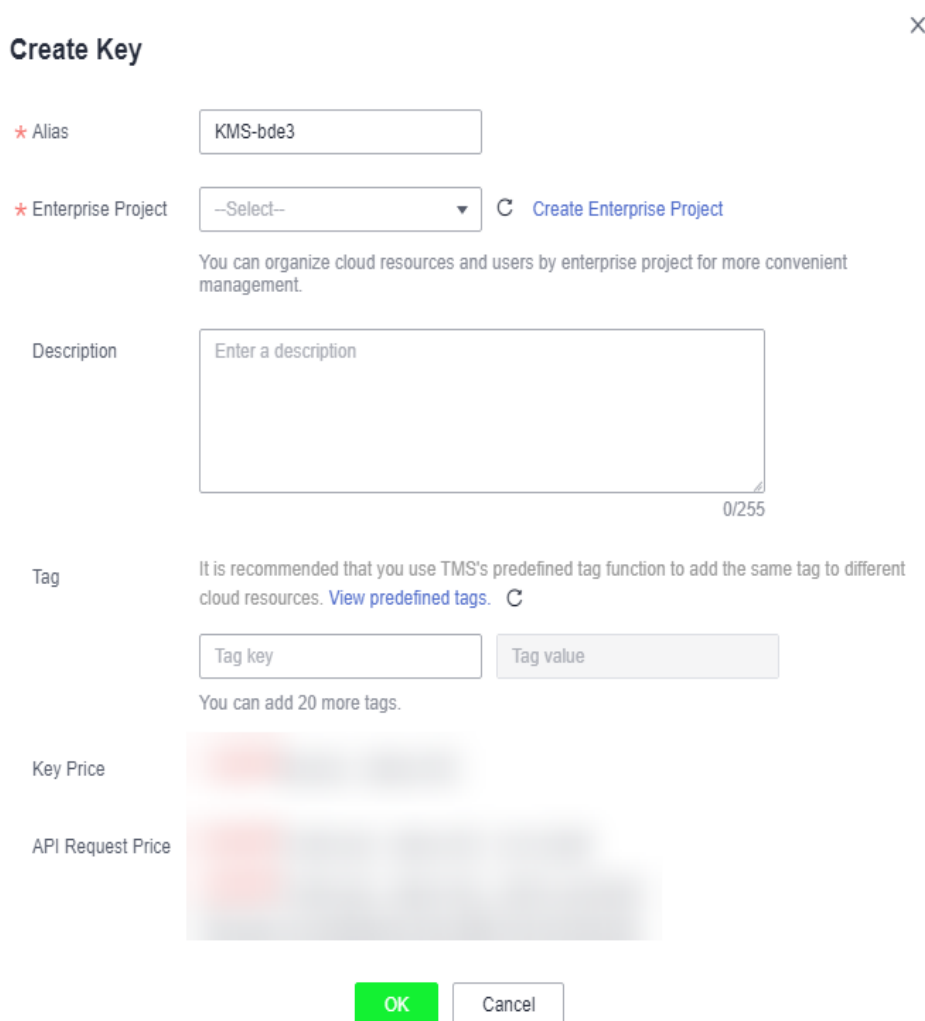
Paso 2 Haga clic en  en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

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

Paso 4 Haga clic en **Create Bucket** en la esquina superior derecha.

Paso 5 Configure los parámetros en el cuadro de diálogo **Create Key**.

Figura 1-1 Creación de una clave



Create Key ×

* Alias

* Enterprise Project [Create Enterprise Project](#)

You can organize cloud resources and users by enterprise project for more convenient management.

Description 0/255

Tag
 It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. [View predefined tags](#). [C](#)

You can add 20 more tags.

Key Price

API Request Price

- **Alias** es el alias de la clave que se va a crear.

 **NOTA**

- Puede introducir dígitos, letras, guiones bajos (_), guiones, dos puntos (:), y barras diagonales (/).
 - Puede introducir hasta 255 caracteres.
- **Key Algorithm:** Seleccione un algoritmo de clave. Para obtener más información, consulte [Tabla 1-2](#).

Tabla 1-2 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
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

- **Usage:** Seleccione **SIGN_VERIFY**, **ENCRYPT_DECRYPT** o **GENERATE_VERIFY_MAC**.
 - Para una clave simétrica AES_256, el valor predeterminado es **ENCRYPT_DECRYPT**.
 - Para una clave simétrica HMAC, el valor por defecto es **GENERATE_VERIFY_MAC**.

- Para claves asimétricas RSA, seleccione **ENCRYPT_DECRYPT** o **SIGN_VERIFY**. El valor predeterminado es **SIGN_VERIFY**.
- Para una clave asimétrica ECC, el valor predeterminado es **SIGN_VERIFY**.

 **NOTA**

El uso de la clave solo se puede configurar durante la creación de la clave y no se puede modificar posteriormente.

- (Opcional) **Description** es la descripción de la clave personalizada.
- El parámetro **Enterprise Project** debe establecerse solo para usuarios empresariales. Si es un usuario de empresa y ha creado un proyecto de empresa, seleccione el proyecto de empresa necesario en la lista desplegable. El proyecto predeterminado es **default**. Si no se muestran opciones de **Enterprise Management**, no es necesario configurarlas.

 **NOTA**

- Puede usar proyectos empresariales para gestionar recursos en la nube y miembros del proyecto. Para obtener más información sobre proyectos empresariales, consulte [¿Qué es Enterprise Project Management Service?](#)
- Para obtener más información acerca de cómo habilitar la función de proyecto de empresa, consulte [Habilitación de Centro de empresa](#).

Paso 6 (Opcional) Agregue etiquetas a la clave personalizada según sea necesario e introduzca la clave de etiqueta y el valor de etiqueta.

 **NOTA**

- Después de crear un CMK, puede hacer clic en el alias del CMK para ir a la página de detalles del CMK y agregar una etiqueta al CMK.
- La misma etiqueta (incluidas clave de etiqueta y valor de etiqueta) se puede utilizar para diferentes claves personalizadas. Sin embargo, bajo la misma clave personalizada, una clave de etiqueta puede tener solo un valor de etiqueta.
- Se puede agregar un máximo de 20 etiquetas para una clave personalizada.
- Si desea eliminar una etiqueta de la lista de etiquetas al agregar varias etiquetas, puede hacer clic en **Delete** en la fila donde se encuentra la etiqueta que se va a agregar para eliminarla.

Paso 7 Haga clic en **OK**. Aparece un mensaje en la esquina superior derecha de la página, indicando que la clave se ha creado correctamente.

En la lista de claves, puede ver la clave creada. El estado predeterminado de una clave es **Enabled**.

----Fin

Operaciones relacionadas

- Para obtener más información sobre cómo cargar objetos con encriptación del lado del servidor, consulte la sección "Cargar un archivo con encriptación del lado del servidor" en *Guía de usuario de Object Storage Service*.
- Para obtener más información sobre cómo cifrar datos en discos EVS, consulte la sección **Compra de un disco EVS** en la *Guía del usuario de Elastic Volume Service*.
- Para obtener más información acerca de cómo cifrar imágenes privadas, consulte la sección *Guía de usuario de Image Management Service*.

- Para obtener detalles acerca de cómo cifrar discos para una instancia de base de datos en RDS, consulte la sección "Compra de una instancia" en la *Guía de usuario de Relational Database Service*.
- Para obtener más información sobre cómo crear un DEK y un DEK sin texto plano, consulte las secciones "Creación de un DEK" y "Creación de un DEK sin texto plano" en la *Referencia de API de Data Encryption Workshop*.
- Para obtener detalles sobre cómo cifrar y descifrar un DEK para una aplicación de usuario, consulte las secciones "Encriptación de un DEK" y "Desencriptación de un DEK" en la *Referencia de API de Data Encryption Workshop*.

1.3 Creación de CMK mediante materiales de clave importados

1.3.1 Descripción

Una clave personalizada contiene metadatos de clave (ID de clave, alias de clave, descripción, estado de clave y fecha de creación) y materiales clave utilizados para cifrar y descifrar datos.

- Cuando un usuario utiliza la consola KMS para crear una clave personalizada, KMS genera automáticamente un material de clave para la clave personalizada.
- Si desea utilizar su propio material de clave, puede utilizar la función de importación de clave en la consola de KMS para crear una clave personalizada cuyo material de clave esté vacío e importar el material de clave a la clave personalizada.

Notas importantes

- Seguridad
Debe asegurarse de que las fuentes aleatorias cumplan con sus requisitos de seguridad cuando las utilice para generar materiales clave. Cuando utilice la función de importación de claves, debe ser responsable de la seguridad de sus materiales de claves. Guarde la copia de respaldo original del material de clave para que el material de clave de copia de respaldo se pueda importar al KMS a tiempo cuando el material de clave se elimine accidentalmente.
- Disponibilidad y durabilidad
Antes de importar el material clave en KMS, debe garantizar la disponibilidad y durabilidad del material clave.
Tabla 1-3 muestra las diferencias entre el material clave importado y el material clave generado por KMS.

Tabla 1-3 Diferencias entre el material de clave importado y el material clave generado por KMS

Fuente de material de clave	Diferencia
Claves importadas	<ul style="list-style-type: none"> ● Puede eliminar el material de clave, pero no puede eliminar la clave personalizada y sus metadatos. ● Tales claves no se pueden girar. ● Al importar el material de clave, puede establecer el tiempo de caducidad del material de clave. Después de que el material de clave caduca, el KMS elimina automáticamente el material de clave en 24 horas, pero no elimina la clave personalizada y sus metadatos. Se recomienda que guarde una copia del material en su dispositivo local, ya que puede usarse para volver a importar en casos de materiales clave no válidos o de eliminación errónea de materiales de clave. <p>NOTA Las claves que usan los algoritmos RSA_2048, RSA_3072, RSA_4096, EC_P256 y EC_P384 son válidas permanentemente. Sus materiales clave no se pueden eliminar manualmente y su tiempo de caducidad no se puede configurar.</p>
Claves creadas en KMS	<ul style="list-style-type: none"> ● El material de clave no se puede eliminar manualmente. ● Las claves simétricas se pueden girar. ● No se puede establecer el tiempo de caducidad para el material de clave.

- **Asociación**
 Cuando un material de clave se importa a una clave personalizada, la clave personalizada se asocia permanentemente con el material de clave. No se pueden importar otros materiales clave a la clave personalizada.
- **Singularidad**
 Si utiliza la clave personalizada creada con el material de clave importado para cifrar datos, los datos cifrados sólo se pueden descifrar mediante la clave personalizada que se ha utilizado para cifrar los datos, ya que los metadatos y el material de clave de la clave personalizada deben ser coherentes.

1.3.2 Importación de materiales de clave

Si desea utilizar sus propios materiales de clave en lugar de los materiales generados por KMS, puede utilizar la consola para importar sus materiales clave a KMS. Los CMK creados con materiales importados y los materiales generados por KMS son gestionados conjuntamente por KMS.


En esta sección se describe cómo importar materiales de clave en la consola de KMS.

Restricciones

- El algoritmo de clave HMAC no admite la importación de materiales clave.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

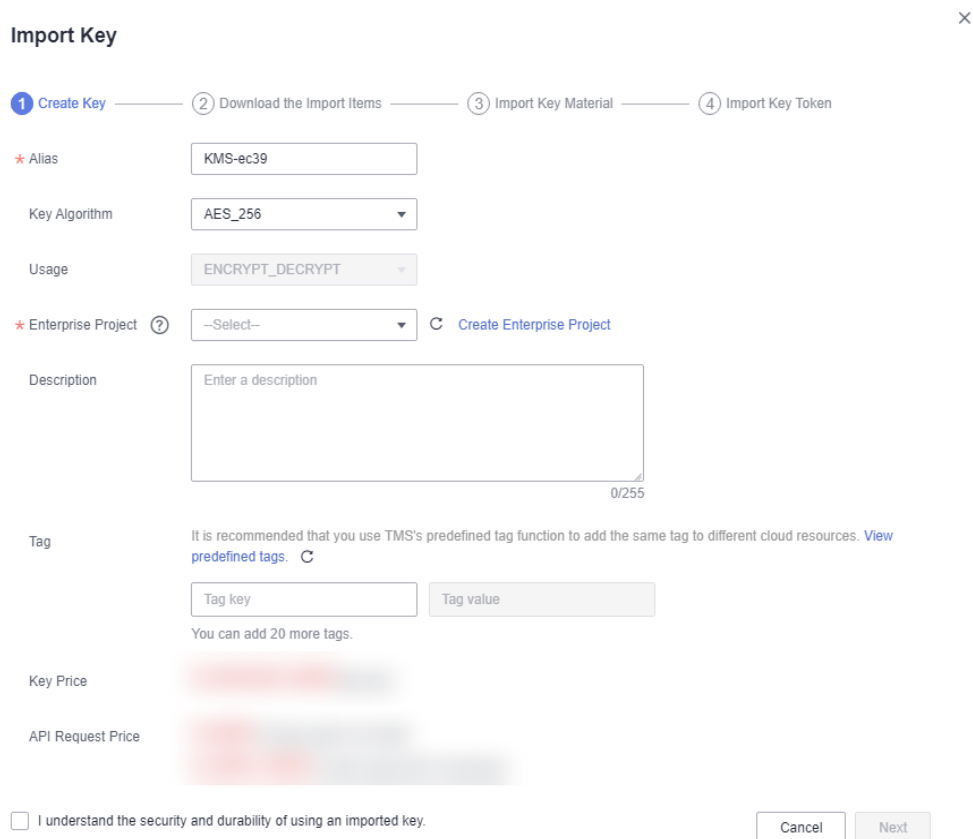
Paso 2 Haga clic en  en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

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

Paso 4 Haga clic en **Import Key**. Aparece el cuadro de diálogo **Import Key**.

Paso 5 Configurar parámetros de clave.

Figura 1-2 Creación de una clave vacía



- **Alias** es el alias de la clave que se va a crear.

NOTA

- Puede introducir dígitos, letras, guiones bajos (_), guiones, dos puntos (:), y barras diagonales (/).
 - Puede introducir hasta 255 caracteres.
- **Key Algorithm:** Seleccione un algoritmo de clave. Para obtener más información, consulte [Tabla 1-4](#).

Tabla 1-4 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 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

- **Usage:** Seleccione **SIGN_VERIFY**, **ENCRYPT_DECRYPT** o **GENERATE_VERIFY_MAC**.
 - Para una clave simétrica AES_256, el valor predeterminado es **ENCRYPT_DECRYPT**.
 - Para una clave simétrica HMAC, el valor por defecto es **GENERATE_VERIFY_MAC**.
 - Para claves asimétricas RSA, seleccione **ENCRYPT_DECRYPT** o **SIGN_VERIFY**. El valor predeterminado es **SIGN_VERIFY**.
 - Para una clave asimétrica ECC, el valor predeterminado es **SIGN_VERIFY**.

📖 NOTA

El uso de la clave solo se puede configurar durante la creación de la clave y no se puede modificar posteriormente.

- (Opcional) **Description** es la descripción de la clave personalizada.
- El parámetro **Enterprise Project** debe establecerse solo para usuarios empresariales. Si es un usuario de empresa y ha creado un proyecto de empresa, seleccione el proyecto de empresa necesario en la lista desplegable. El proyecto predeterminado es **default**. Si no se muestran opciones de **Enterprise Management**, no es necesario configurarlas.

📖 NOTA

- Puede usar proyectos empresariales para gestionar recursos en la nube y miembros del proyecto. Para obtener más información sobre proyectos empresariales, consulte [¿Qué es Enterprise Project Management Service?](#)
- Para obtener más información acerca de cómo habilitar la función de proyecto de empresa, consulte [Habilitación de Centro de empresa](#).

Paso 6 (Opcional) Agregue etiquetas a la clave personalizada según sea necesario e introduzca la clave de etiqueta y el valor de etiqueta.

NOTA

- Si se ha creado una clave personalizada sin ninguna etiqueta, puede agregar una etiqueta a la clave personalizada más adelante según sea necesario. Haga clic en el alias de la clave personalizada, haga clic en la pestaña **Tags** y haga clic en **Add Tag**.
- La misma etiqueta (incluidas clave de etiqueta y valor de etiqueta) se puede utilizar para diferentes claves personalizadas. Sin embargo, bajo la misma clave personalizada, una clave de etiqueta puede tener solo un valor de etiqueta.
- Se puede añadir un máximo de 20 etiquetas para una clave personalizada.
- Si desea eliminar una etiqueta de la lista de etiquetas al agregar varias etiquetas, puede hacer clic en **Delete** en la fila donde se encuentra la etiqueta que se va a agregar para eliminarla.

Paso 7 Haga clic en **security and durability** para comprender la seguridad y durabilidad de la clave importada.

Paso 8 Seleccione **I understand the security and durability of using an imported key** y cree una clave personalizada cuyo material de clave esté vacío.

Paso 9 Haga clic en **Next** para ir al paso **Download the Import Items**. Seleccione un algoritmo de ajuste de clave basado en **Tabla 1-6**. Seleccione un algoritmo de ajuste de claves basado en **Tabla 1-5**.

Figura 1-3 Obtención de la clave de embalaje y el token de importación

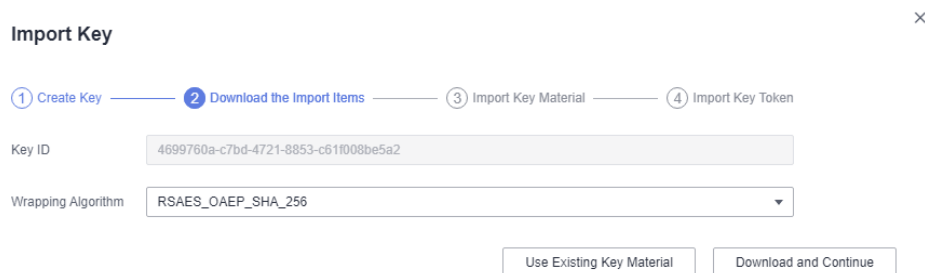


Tabla 1-5 Key wrapping algorithms

Algorithm	Description	Configuration
RSAES_OAEP_SHA_256	RSA algorithm that uses OAEP and has the SHA-256 hash function	Select an algorithm based on your HSM functions. 1. If the HSMs support the RSAES_OAEP_SHA_256 algorithm, use RSAES_OAEP_SHA_256 to encrypt key materials.
RSAES_OAEP_SHA_1	RSA algorithm that uses Optimal Asymmetric Encryption Padding (OAEP) and has the SHA-1 hash function	2. If the HSMs do not support OAEP , use RSAES_PKCS1_V1_5 to encrypt key materials. AVISO The RSAES_OAEP_SHA_1 algorithm is no longer secure. Exercise caution when performing this operation.

Tabla 1-6 Algoritmos de envoltura de claves

Algoritmo	Descripción	Configuración
RSAES_OAEP_SHA_256	Algoritmo RSA que utiliza OAEP y tiene la función hash SHA-256	Seleccione un algoritmo basado en sus funciones HSM. Si los HSM admiten el algoritmo RSAES_OAEP_SHA_256 , utilice RSAES_OAEP_SHA_256 para cifrar materiales clave.

 **NOTA**

Si detiene un proceso de importación de material clave y desea volver a intentarlo, haga clic en **Import Key Material** en la fila de la clave personalizada necesaria e importe el material clave en el cuadro de diálogo que se muestra.

Paso 10 Obtenga la clave de ajuste y el token de importación. Si ya tiene un material clave, omita este paso.

1. Obtenga la clave de ajuste y el token de importación.
 - Método 1: Haga clic en **Download and Continue**, como se muestra en [Figura 1-4](#).

Figura 1-4 Archivo descargado



- **wrappingKey_KeyID** es la clave de envoltura. Se codifica en formato binario y se utiliza para cifrar la clave de envoltura del material de clave.
- Import token: No es necesario descargarlo. El asistente de importación transfiere automáticamente el token de importación. Si cierra el asistente antes de completar la importación, el token no será válido automáticamente.

AVISO

La clave de envoltura caduca en 24 horas. Si la clave de envoltura no es válida, descárguela de nuevo.

El asistente de importación transfiere automáticamente el token de importación. Si cierra el asistente antes de completar la importación, el token no será válido automáticamente. Para volver a intentar importar, vuelva a abrir el asistente de importación.

- Método 2: Obtener la clave de envoltura e importar el token invocando a las API.
 - i. Llame a la API **get-parameters-for-import** para obtener la clave de envoltura y el token de importación.
 - **public_key**: contenido de la clave de envoltura (codificación Base-64) devuelta después de la invocación a la API
 - **import_token**: contenido del token de importación (codificación Base-64) devuelto después de la invocación a la API

En el siguiente ejemplo se describe cómo obtener la clave de ajuste y el token de importación de un CMK (ID: **43f1ffd7-18fb-4568-9575-602e009b7ee8**; algoritmo: **RSAES_OAEP_SHA_256**).

- Parámetros de respuesta

```
{
  "key_id": "43f1ffd7-18fb-4568-9575-602e009b7ee8",
  "wrapping_algorithm": "RSAES_OAEP_SHA_256"
}
```

- Ejemplo de respuesta

```
{
  "key_id": "43f1ffd7-18fb-4568-9575-602e009b7ee8",
  "public_key": "public key base64 encoded data",
  "import_token": "import token base64 encoded data",
  "expiration_time": 1501578672
}
```

- ii. Guarde la clave de ajuste y convierta su formato. Solo el material de clave cifrado con la clave de ajuste convertida se puede importar a la consola de gestión.
 - 1) Copie el contenido de la clave de ajuste **public_key**, péguela en el archivo `.txt` y guarde el archivo como **PublicKey.b64**.
 - 2) Utilice OpenSSL para ejecutar el siguiente comando para realizar la codificación Base-64 en el contenido del archivo **PublicKey.b64** para generar datos binarios y guardar el archivo convertido como **PublicKey.bin**:
openssl enc -d -base64 -A -in PublicKey.b64 -out PublicKey.bin
 - iii. Guarde el token de importación, copie el contenido del token **import_token**, péguelo en un archivo `.txt`, y guarde el archivo como **ImportToken.b64**.
2. Utilice la clave de ajuste para cifrar el material de la clave.

NOTA

Después de realizar este paso, obtendrá cualquiera de los siguientes archivos:

Escenario clave simétrico: **EncryptedKeyMaterial.bin** (material de clave)

Escenario de clave asimétrica: **EncryptedKeyMaterial.bin** (clave de material temporal) y **out_rsa_private_key.der** (texto cifrado de clave privada)

Método 1: Utilice la clave de envoltura descargada para cifrar los materiales de clave en su HSM. Para obtener más información, consulte la guía de operación de su HSM.

Método 2: Utilice OpenSSL para generar un material de clave y utilice la clave de envoltura descargada para cifrar el material de clave.

NOTA

Si necesita ejecutar el comando **openssl pkeyutl**, asegúrese de que su versión de OpenSSL es 1.0.2 o posterior.

- a. Genere un material clave (clave simétrica de 256 bits) y guárdelo como **PlaintextKeyMaterial.bin**.
 - Si se utiliza el algoritmo de clave simétrica AES256, ejecute el siguiente comando en el cliente donde se ha instalado la herramienta OpenSSL:
openssl rand -out PlaintextKeyMaterial.bin 32
 - Si se utilizan los algoritmos de clave asimétrica RSA y ECC, ejecute el siguiente comando en el cliente donde se ha instalado la herramienta OpenSSL:

- 1) Generar una clave hexadecimal AES256.
openssl rand -out 0xPlaintextKeyMaterial.bin -hex 32
 - 2) Convierta la clave hexadecimal AES256 al formato binario.
cat 0xPlaintextKeyMaterial.bin | xxd -r -ps > PlaintextKeyMaterial.bin
- b. Utilice la clave de envoltura descargada para cifrar el material de la clave y guardar el material de la clave cifrada como **EncryptedKeyMaterial.bin**.
 Si la clave de envoltura se descargó de la consola, reemplace **PublicKey.bin** en el siguiente comando con el nombre de clave de envoltura *wrappingKey_keyID*.

Tabla 1-7 Encriptación del material de clave generado usando la clave de envoltura descargada

Algoritmo de clave de envoltura	Encriptación de material de clave
RSAES_OAEP_SHA_256	openssl pkeyutl -in PlaintextKeyMaterial.bin -inkey PublicKey.bin -out EncryptedKeyMaterial.bin -keyform der -pubin -encrypt -pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256

- c. (Opcional) Para importar una clave asimétrica, genere una clave privada asimétrica, use el material de clave temporal (**EncryptedKeyMaterial.bin**) para cifrar la clave privada e importe el archivo cifrado como el texto cifrado de clave privada.
- Tome el algoritmo RSA4096 como ejemplo. Realice las siguientes operaciones:
 - 1) Generar una clave privada.
openssl genrsa -out pkcs1_rsa_private_key.pem 4096
 - 2) Convertir el formato a PKCS8.
openssl pkcs8 -topk8 -inform PEM -in pkcs1_rsa_private_key.pem -outform pem -nocrypt -out rsa_private_key.pem
 - 3) Convertir el formato PKCS8 al formato DER.
openssl pkcs8 -topk8 -inform PEM -outform DER -in rsa_private_key.pem -out rsa_private_key.der -nocrypt
 - 4) Utilizar un material de clave temporal para cifrar la clave privada.
openssl enc -id-aes256-wrap-pad -K \$(cat 0xPlaintextKeyMaterial.bin) -iv A65959A6 -in rsa_private_key.der -out out_rsa_private_key.der

 **NOTA**

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. Para obtener más información, consulte las preguntas frecuentes.

Paso 11 Si ya tiene el material de clave, haga clic en **Existing Key Material**. Se muestra la página **Import Key Material**.

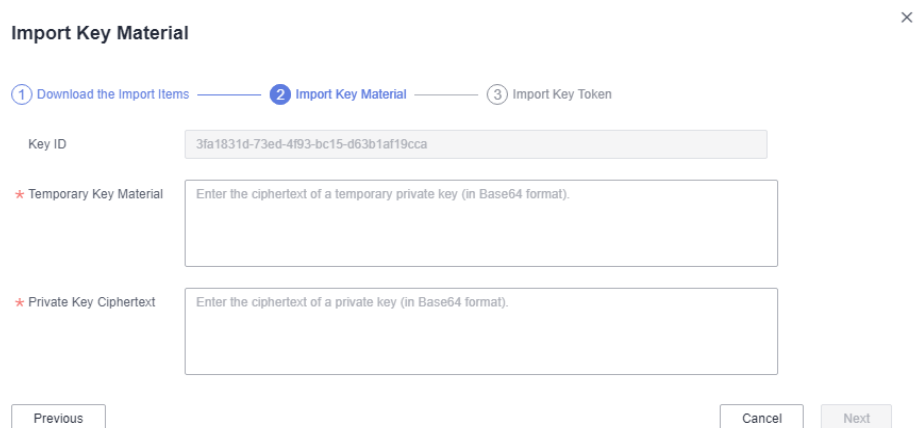
Tabla 1-8 Parámetros para importar materiales de clave (para claves simétricas)

Parámetro	Descripción
Key ID	ID aleatorio de un CMK generado durante la creación del CMK
Key material	Importar un material de clave. Por ejemplo, utilice el archivo EncryptedKeyMaterial.bin de Paso 10.2.b .

Tabla 1-9 Parámetros para importar materiales de clave (para claves asimétricas)

Parámetro	Descripción
Key ID	ID aleatorio de un CMK generado durante la creación del CMK
Temporary key material	Importar un material de clave temporal. Por ejemplo, seleccione el archivo EncryptedKeyMaterial.bin de Paso 10.2.b .
Private key ciphertext	Seleccionar texto cifrado de clave privada. Por ejemplo, seleccione el archivo out_rsa_private_key.der de Paso 10.2.c .

Figura 1-5 Importación de materiales de clave



Import Key Material ×

① Download the Import Items — ② **Import Key Material** — ③ Import Key Token

Key ID: 3fa1831d-73ed-4f93-bc15-d63b1af19cca

* Temporary Key Material: Enter the ciphertext of a temporary private key (in Base64 format).

* Private Key Ciphertext: Enter the ciphertext of a private key (in Base64 format).

Previous Cancel Next

Paso 12 Haga clic en **Next** para ir al paso **Import Key Token**. Configure los parámetros como se describe en el documento **Tabla 1-10**.

Figura 1-6 Importación de un token de clave

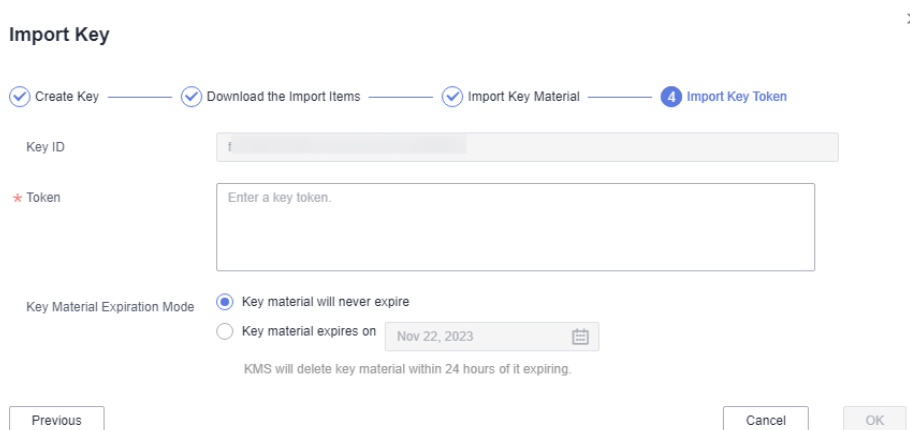


Tabla 1-10 Parámetros para importar un token de clave

Parámetro	Descripción
Key ID	ID aleatorio de un CMK generado durante la creación del CMK
Key import token	Seleccione el token de importación obtenido a través de la API en 12.b .
Key material expiration mode	<ul style="list-style-type: none"> ● Key material will never expire: Utiliza esta opción para especificar que los materiales clave no caducarán después de la importación. ● Key material will expire: Utiliza esta opción para especificar el tiempo de caducidad de los materiales de clave. De forma predeterminada, los materiales de clave caducan en 24 horas después de la importación. Después de que el material de clave caduca, el sistema elimina automáticamente el material de clave en un plazo de 24 horas. Una vez que se elimina el material de la clave, la clave no se puede utilizar y su estado cambia a Pending import.

Paso 13 Haga clic en **OK**. Cuando se muestra el mensaje **Key imported successfully** en la esquina superior derecha, se importan los materiales.

AVISO

Los materiales de clave se pueden importar correctamente cuando coinciden con el ID de CMK y el token correspondientes.

Los materiales importados se muestran en la lista de CMK. El estado predeterminado de un CMK importado es **Enabled**.

----**Fin**

1.3.3 Eliminación de materiales de clave

Al importar materiales de clave, puede especificar su tiempo de caducidad. Después de que el material de clave caduca, KMS lo elimina y el estado de la clave personalizada cambia a **Pending import**. Puede eliminar manualmente los materiales clave según sea necesario. El efecto de la expiración del material clave es el mismo que el de la eliminación manual del material de clave.

En esta sección se describe cómo eliminar materiales clave importados en la consola de KMS.

Prerrequisitos


- Ha importado materiales clave para un CMK.
- La fuente material de la CMK es **External**.
- El estado CMK es **Enabled** o **Disabled**.

Restricciones

- Para volver a importar un material de clave eliminado, asegúrese de que el material importado es el mismo que el eliminado.
- Los datos cifrados mediante un CMK no se pueden descifrar si se eliminó el material de clave de la clave personalizada. Para descifrar los datos, vuelva a importar el material de clave.
- Después de la eliminación, el CMK no estará disponible y su estado cambiará a **Pending import**.
- Los materiales de clave de las claves asimétricas no se pueden eliminar directamente. Para eliminarlos, siga las instrucciones de [Eliminación de uno o más CMK](#).

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 . Elija **Security & Compliance > Data Encryption Workshop**.

Paso 4 En la fila que contiene el CMK deseado, haga clic en **Delete Key Material**.

Paso 5 En el cuadro de diálogo que se muestra, haga clic en **OK**. Cuando **Key material deleted successfully** se muestra en la esquina superior derecha, los materiales clave se eliminan correctamente.

Después de la eliminación, el CMK no estará disponible y su estado cambiará a **Pending import**.

----Fin


1.4 Gestión de CMK

1.4.1 Consulta de un CMK

En esta sección se describe cómo ver la información sobre la clave personalizada en la consola de KMS, incluidos el alias de clave, el estado, el ID y la hora de creación. El estado de una clave puede ser **Enabled**, **Disabled**, **Scheduled deletion** o **Pending import**.

Procedimiento

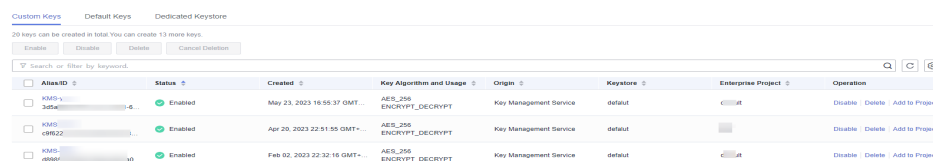
Paso 1 Inicie sesión en la consola de gestión.

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 . Elija **Security & Compliance > Data Encryption Workshop**.

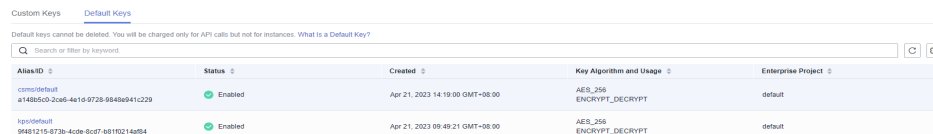
Paso 4 Compruebe la lista de claves. [Tabla 1-11](#) describe los parámetros.

Figura 1-7 Claves personalizadas



AliasID	Status	Created	Key Algorithm and Usage	Origin	Keystore	Enterprise Project	Operation
KMS-23dfe...	Enabled	May 23, 2023 16:55:37 GMT...	AES_256 ENCRYPT_DECRYPT	Key Management Service	default	cliat	Disable Delete Add to Proje
KMS-c9822...	Enabled	Apr 29, 2023 22:51:55 GMT*	AES_256 ENCRYPT_DECRYPT	Key Management Service	default		Disable Delete Add to Proje
KMS-0996...	Enabled	Feb 02, 2023 22:32:16 GMT...	AES_256 ENCRYPT_DECRYPT	Key Management Service	default	cliat	Disable Delete Add to Proje

Figura 1-8 Claves predeterminadas



AliasID	Status	Created	Key Algorithm and Usage	Enterprise Project
cmisdefault a148b50-2a6-4616-9728-9848a941c229	Enabled	Apr 21, 2023 14:19:00 GMT-08:00	AES_256 ENCRYPT_DECRYPT	default
ipisdefault 96481215-873b-4c0e-8c07-9819214a884	Enabled	Apr 21, 2023 09:49:21 GMT-08:00	AES_256 ENCRYPT_DECRYPT	default

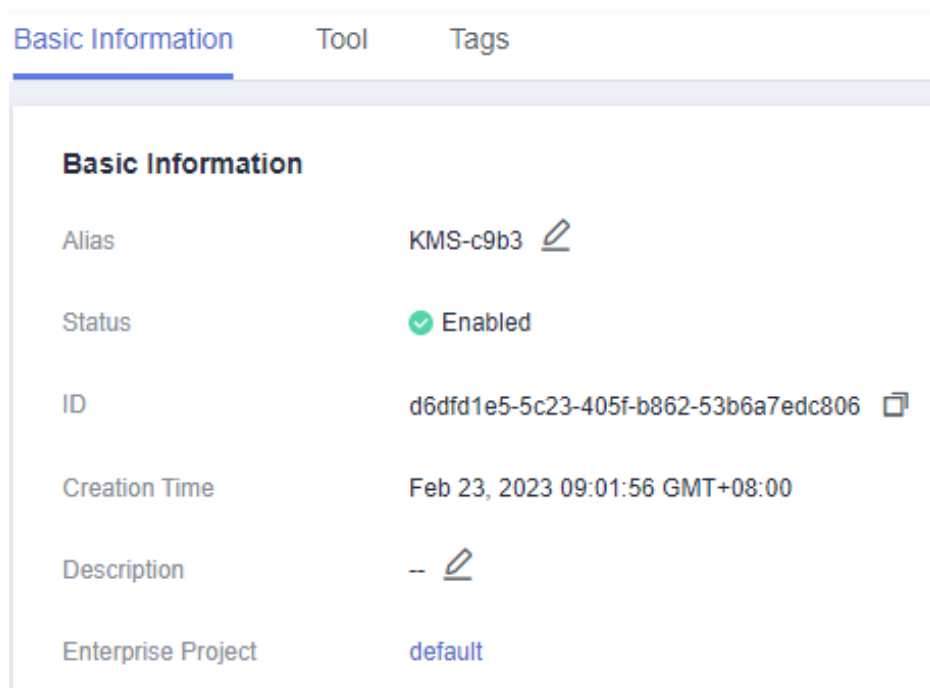
Tabla 1-11 Parámetros de lista de clave

Parámetro	Descripción
Alias/ID	<p>Alias de una clave y el ID aleatorio de una clave generada durante su creación.</p> <p>NOTA Utilice este ID como valor de Path de acceso si está creando una política personalizada en IAM y ha seleccionado Specify resource path para KeyId.</p>
Status	<p>Estado de un CMK, que puede ser uno de los siguientes:</p> <ul style="list-style-type: none"> ● Enabled El CMK está habilitado. ● Disabled El CMK está deshabilitado. ● Pending deletion El CMK está programado para su eliminación. ● Pending import Si su CMK no tiene materiales, su estado es Pending import.


Parámetro	Descripción
Creation Time	Tiempo de creación del CMK
Key Algorithm and Usage	Algoritmo de clave seleccionado durante la creación de clave y su uso
Origin	Origen del material clave, que puede ser uno de los siguientes: <ul style="list-style-type: none"> ● External La clave se importa al KMS desde un sistema externo. ● Key Management Service La clave es una clave predeterminada o creada en KMS.
Enterprise Project	Proyecto de empresa para el que se utiliza el CMK

Paso 5 Puede hacer clic en el alias de una clave para ver sus detalles, como se muestra en el documento **Figura 1-9**.

Figura 1-9 Detalles de CMK



NOTA

Para cambiar el alias o la descripción del CMK, haga clic en  junto al valor de **Alias** o **Description**.

- Una clave predeterminada (cuyo sufijo de alias es el **/default**) no permite cambios de alias y descripción.
- El alias y la descripción de un CMK no se pueden cambiar si el CMK está en estado de **Pending deletion**.

----Fin

1.4.2 Habilitación de uno o más CMK


En esta sección se describe cómo utilizar la consola KMS para habilitar una o más claves personalizadas. Solo se pueden utilizar las claves personalizadas habilitadas para cifrar o descifrar datos. Una nueva clave personalizada está en el estado **Enabled** de forma predeterminada.

Prerrequisitos

La clave personalizada que desea habilitar está en estado **Disabled**.

Procedimiento

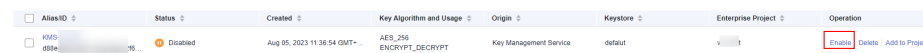
Paso 1 Inicie sesión en la consola de gestión.

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 . Elija **Security & Compliance > Data Encryption Workshop**.

Paso 4 En la fila que contiene la clave personalizada deseada, haga clic en **Enable**.

Figura 1-10 Habilitar una clave



AliasID	Status	Created	Key Algorithm and Usage	Origin	Keystore	Enterprise Project	Operation
alias- alias-	Disabled	Aug 05, 2023 11:36:54 GMT-	AES_256 ENCRYPT_DECRYPT	Key Management Service	default		Enable Delete Add to Project

Paso 5 En el cuadro de diálogo que se muestra, haga clic en **OK** para activar la clave.

NOTA

Para habilitar varios CMK a la vez, selecciónelos y haga clic en **Enable** en la esquina superior izquierda de la lista.

----Fin

1.4.3 Deshabilitación de uno o más CMK

Esta sección describe cómo utilizar la consola KMS para deshabilitar una o más claves personalizadas, protegiendo así los datos en casos urgentes.

Una vez deshabilitada, no se puede utilizar una clave personalizada para cifrar o descifrar ningún dato. Antes de utilizar un CMK deshabilitado para cifrar o descifrar datos, debe habilitarlo siguiendo las instrucciones en [Habilitación de uno o más CMK](#).

Prerrequisitos


El CMK que desea deshabilitar está en estado **Enabled**.

Restricciones

- Las claves predeterminadas creadas por KMS no se pueden deshabilitar.
- Un CMK deshabilitado todavía es facturable. Dejará de incurrir en cargos si se elimina.

Procedimiento

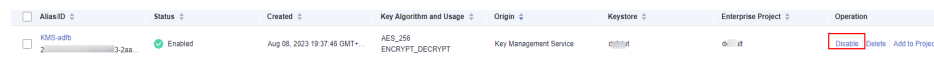
Paso 1 [Inicie sesión en la consola de gestión.](#)

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 . Elija **Security & Compliance > Data Encryption Workshop.**

Paso 4 En la fila que contiene el CMK deseado, haga clic en **Disable**.

Figura 1-11 Deshabilitación de un CMK



AliasID	Status	Created	Key Algorithm and Usage	Origin	Keystore	Enterprise Project	Operation
KMS-akdb-2	Enabled	Aug 08, 2023 19:37:49 GMT+	AES_256 ENCRYPT_DECRYPT	Key Management Service	akdb	akdb	Disable Delete Add to Project

Paso 5 En el cuadro de diálogo que se muestra, seleccione **I understand the impact of disabling keys** y haga clic en **OK**.

NOTA

Para deshabilitar varios CMK a la vez, selecciónelos y haga clic en **Disable** en la esquina superior izquierda de la lista.

----Fin

1.4.4 Eliminación de uno o más CMK

Antes de eliminar el CMK, confirme que no está en uso y que no se utilizará. Puede comprobar el uso de la clave de cualquiera de las siguientes maneras:

- Compruebe el permiso CMK para determinar su posible alcance de uso. Para obtener más información, véase [Consulta de una concesión](#).
- Compruebe los registros de auditoría para determinar el uso real.

Prerrequisitos

- La clave que se va a eliminar está en estado **Enabled**, **Disabled** o **Pending import**.

Restricciones


- Una clave no se eliminará hasta que expire su período de eliminación programado. Puede establecer el período en un valor dentro del intervalo de 7 a 1096 días.

Antes de la fecha de eliminación especificada, puede cancelar la eliminación si desea utilizar el CMK. Una vez que la eliminación programada haya entrado en vigor, el CMK se eliminará permanentemente y no podrá descifrar los datos cifrados por el CMK. Tenga cuidado cuando realice esta acción.

- Para obtener detalles sobre la información de facturación sobre un CMK programado para eliminarse, consulte [¿Se cargará un CMK después de que esté programado para eliminarlo?](#)
- Las claves predeterminadas creadas por KMS no se pueden programar para su eliminación.

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 . Elija **Security & Compliance > Data Encryption Workshop**.

Paso 4 En la fila que contiene el CMK deseado, haga clic en **Delete** en la columna **Operation**.

Figura 1-12 Programación de la eliminación de una CMK

AliasID	Status	Created	Key Algorithm and Usage	Origin	Keystore	Enterprise Project	Operation
KMS-alias 27c473c7-c9e-4b23-a9b3-2aa...	Enabled	Aug 08, 2023 19:37:46 GMT+	AES_256 ENCRYPT_DECRYPT	Key Management Service	it		Disable Delete Add to Project

Paso 5 En el cuadro de diálogo de eliminación de teclas, escriba el tiempo de retardo de eliminación.

Figura 1-13 Introducir el período después del cual desea que la eliminación surta efecto

Waiting Period (days):

Delete Key

The following 1 keys will be deleted.
 After the key is deleted, the data encrypted using the key cannot be decrypted. The key will be deleted seven or more days from now, and will not incur charges during the waiting period.

Alias	Status	ID
KMS-8299	Enabled	00-2021

To confirm deletion, enter 'DELETE' below:

OK Cancel

NOTA

- Una clave no se eliminará hasta que expire su período de eliminación programado. Puede establecer el período en un valor dentro del intervalo de 7 a 1096 días. Antes de la fecha de eliminación especificada, puede cancelar la eliminación si desea utilizar el CMK.
- Para obtener detalles sobre la información de facturación sobre un CMK programado para eliminarse, consulte [¿Se cargará un CMK después de que esté programado para eliminarlo?](#)

Paso 6 En el cuadro de diálogo de confirmación, escriba **DELETE** y haga clic en **OK**. Se muestra un mensaje que indica que la tarea de eliminación de clave se ha entregado correctamente.

Paso 7 Si se utiliza una clave para cifrar DDS, RDS o NoSQL, después de hacer clic en **OK** aparecerá el mensaje "Key XXX is being used by XXX. Are you sure you want to delete it." se muestra, como se muestra en [Confirmar la eliminación](#). Necesita hacer clic en **Yes**.

Figura 1-14 Confirmar la eliminación



----Fin

NOTA

Para programar la eliminación de varios CMK a la vez, selecciónelos y haga clic en **Delete** en la esquina superior izquierda de la lista.

1.4.5 Cancelación de la eliminación programada de uno o más CMK


En esta sección se describe cómo utilizar la consola KMS para cancelar la eliminación programada de una o más claves personalizadas antes de la ejecución de la eliminación. Después de la cancelación, la clave está en estado **Disabled**.

Prerrequisitos

El CMK para el que desea cancelar la eliminación programada está en estado de **Pending deletion**.

Procedimiento

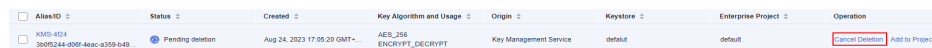
Paso 1 Inicie sesión en la consola de gestión.

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 . Elija **Security & Compliance > Data Encryption Workshop**.

Paso 4 En la fila que contiene el CMK deseado, haga clic en **Cancel Deletion**.

Figura 1-15 Cancelación de la eliminación programada de un CMK



AliasID	Status	Created	Key Algorithm and Usage	Origin	Keystore	Enterprise Project	Operation
KMS-424 3005244-908f-4eac-a359-b49...	Pending deletion	Aug 24, 2023 17:05:29 GMT+	AES_256 ENCRYPT_DECRYPT	Key Management Service	default	default	Cancel Deletion Add to Project

Paso 5 En el cuadro de diálogo que se muestra, haga clic en **OK** para cancelar la eliminación programada.

- Si se crea una clave en la consola KMS, el estado de la clave cambia a **Disabled** después de cancelar su eliminación programada. Para obtener más información acerca de cómo habilitar la clave, consulte [Habilitación de uno o más CMK](#).
- Si el CMK se crea utilizando materiales importados, su estado se convierte en **Disabled** después de la cancelación. Para habilitar el CMK, consulte [Habilitación de uno o más CMK](#).
- Si el CMK se crea utilizando materiales importados y no se han importado materiales clave para él, su estado se convierte en **Pending import** después de la cancelación. Para utilizar el CMK, realice [Creación de CMK mediante materiales de clave importados](#).

NOTA

Para cancelar la eliminación de varios CMK a la vez, selecciónelos y haga clic en **Cancel Deletion** en la esquina superior izquierda de la lista.

----Fin

1.4.6 Adición de una clave a un proyecto

Proyecto empresarial es una plataforma de gobierno en la nube que coincide con la estructura organizativa y el modelo de gestión de servicios de su empresa. Le ayuda a gestionar proyectos empresariales, recursos, personal, finanzas y aplicaciones en la nube en función de la estructura jerárquica de la organización (empresas, departamentos y proyectos) y la estructura del servicio del proyecto.


Si ha habilitado la gestión de proyectos de empresa, puede agregar claves personalizadas especificadas a proyectos de empresa en la consola de KMS.

Restricciones

- Se ha habilitado la función de gestión de proyectos empresariales.
Si no ha habilitado la función de gestión de proyectos de empresa, la opción **Proyecto empresarial** no se muestra en la consola de forma predeterminada y no puede agregar claves a un proyecto. Para obtener más información acerca de cómo habilitar la función de proyecto de empresa, consulte [Habilitación de Centro de empresa](#).
- No se puede cambiar el proyecto de empresa de las claves predeterminadas.

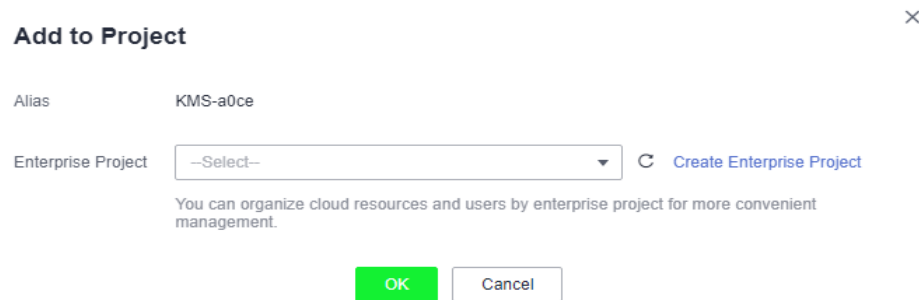
Procedimiento

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 la fila que contiene la clave de destino, haga clic en **Add to Project**.

Figura 1-16 Adición de una clave a un proyecto



NOTA

Si no es usuario de empresa, la opción **Add to Project** no se muestra en la columna de operación.

Para obtener más información acerca de cómo habilitar la función de proyecto de empresa, consulte [Habilitación de Centro de empresa](#).

Paso 4 Seleccione un proyecto.

Paso 5 Haga clic en **OK**.


----Fin

1.5 Búsqueda de una clave

En esta sección se describe cómo buscar una clave personalizada especificando atributos en la página KMS.

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 . Elija **Security & Compliance > Data Encryption Workshop**.

Paso 4 Haga clic en la barra de búsqueda y seleccione los criterios para las claves de filtrado, como se muestra en [Figura 1-17](#). Buscar una clave especificando atributos.

Figura 1-17 Barra de búsqueda



NOTA

- Puede buscar claves por alias de clave, ID, estado, tiempo de creación, algoritmo, uso, tiempo de caducidad del material, origen de material, y proyecto empresarial.
- Puede buscar claves por combinación de atributos. Por ejemplo, si **Status** se establece en **Enabled** y **Key Algorithm** en **AES_256**, se mostrarán todas las claves personalizadas que cumplan los criterios.

----Fin

1.6 Uso de la herramienta en línea para cifrar y descifrar datos de tamaño pequeño

Esta sección describe cómo utilizar la herramienta en línea para cifrar o descifrar datos de tamaño pequeño (4 KB o menos) en la consola KMS.

Prerrequisitos


La clave personalizada está en estado **Enabled**.

Restricciones

- Las claves predeterminadas no se pueden utilizar para cifrar o descifrar dichos datos con la herramienta.
- Las claves asimétricas no se pueden utilizar para cifrar o descifrar dichos datos con la herramienta.
- Puede invocar a una API para usar una clave predeterminada para cifrar o descifrar pequeños volúmenes de datos. Para obtener más información, consulte la *Referencia de API de Data Encryption Workshop*.
- Utilice el CMK actual para cifrar los datos.
- Tenga cuidado al eliminar un CMK. La herramienta en línea no puede descifrar datos si se ha eliminado el CMK utilizado para la encriptación.

Encriptación de datos

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

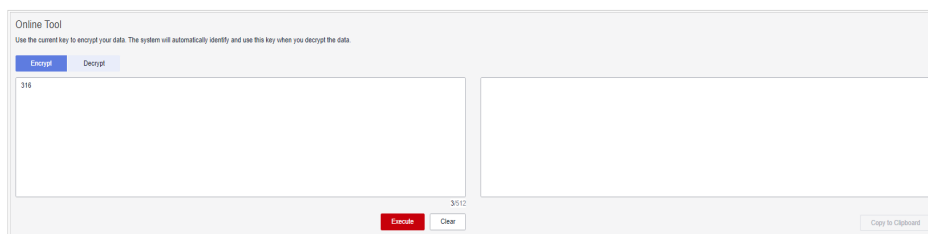
Paso 2 Haga clic en  en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

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 1-18](#).

Figura 1-18 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

Desencriptación de datos

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

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

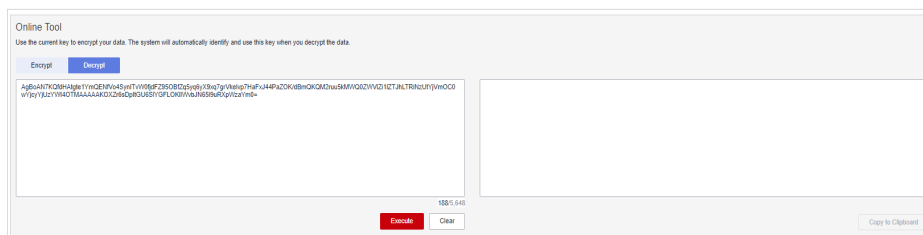
Paso 3 Puede hacer clic en cualquier clave no predeterminada en estado de **Enabled** para ir a la página de encriptación y descifrado de la herramienta en línea.

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 1-19](#).

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 1-19 Descriptación 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

1.7 Gestión de etiquetas

1.7.1 Adición de una etiqueta


Las etiquetas se utilizan para identificar claves. Puede agregar etiquetas a las claves personalizadas para que pueda clasificarlas, rastrearlas y recopilar su estado de uso según las etiquetas.

Restricciones

No se pueden agregar etiquetas a las claves predeterminadas.

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 . Elija **Security & Compliance > Data Encryption Workshop**.

Paso 4 Haga clic en el alias de la clave personalizada deseada para ver sus detalles.

Paso 5 Haga clic en **Tags** para ir a la página de gestión de etiquetas.

Paso 6 Haga clic en **Add Tag**. En el cuadro de diálogo **Add Tag**, escriba la clave de etiqueta y el valor de etiqueta. [Tabla 1-12](#) describe los parámetros.

Figura 1-20 Adición de una etiqueta

Add Tag ×

It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. [View predefined tags.](#) ↻

kcs	01	Delete
Tag key	Tag value	

You can add 18 more tags.

OK Cancel

NOTA

- Si desea utilizar la misma etiqueta para identificar varios recursos en la nube, puede crear etiquetas predefinidas en el TMS. De esta manera, se puede seleccionar la misma etiqueta para todos los servicios. Para obtener más información acerca de las etiquetas predefinidas, consulte la *Guía de usuario de Tag Management Service*.
- Si desea eliminar una etiqueta que se agregará al agregar varias etiquetas, puede hacer clic en **Delete** en la fila donde se encuentra la etiqueta que se agregará para eliminar la etiqueta.

Tabla 1-12 Parámetros de etiqueta

Parámetro	Descripción	Valor	Valor de ejemplo
Tag key	<p>Nombre de una etiqueta.</p> <p>La misma etiqueta (incluidas clave de etiqueta y valor de etiqueta) se puede utilizar para diferentes claves personalizadas. Sin embargo, bajo la misma clave personalizada, una clave de etiqueta puede tener solo un valor de etiqueta.</p> <p>Se puede añadir un máximo de 20 etiquetas para una clave personalizada.</p>	<ul style="list-style-type: none"> ● Obligatorio. ● La clave de etiqueta debe ser única para la misma clave personalizada. ● Límite de 128 caracteres. ● El valor no puede comenzar ni finalizar con un espacio. ● No se puede iniciar con _sys_. ● Se permiten los siguientes tipos de caracteres: <ul style="list-style-type: none"> – Chino – Inglés – Números – Espacio – Caracteres especiales: <code>./=+-@</code> 	cost
Tag value	Valor de la etiqueta	<ul style="list-style-type: none"> ● Este parámetro puede estar vacío. ● Límite de 255 caracteres. ● Se permiten los siguientes tipos de caracteres: <ul style="list-style-type: none"> – Chino – Inglés – Números – Espacio – Caracteres especiales: <code>./=+-@</code> 	100

Paso 7 Haga clic en **OK** para completar.


---Fin

1.7.2 Modificación de valores de etiqueta

En esta sección se describe cómo modificar los valores de etiqueta en la consola KMS.

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.

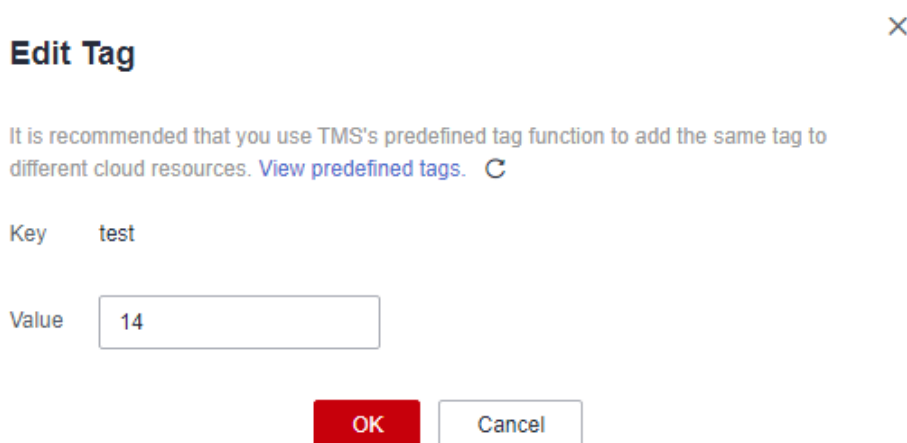
Paso 3 Haga clic en . Elija **Security & Compliance > Data Encryption Workshop**.

Paso 4 Haga clic en el alias de la clave personalizada deseada para ver sus detalles.

Paso 5 Haga clic en **Tags** para ir a la página de gestión de etiquetas.

Paso 6 Haga clic en **Edit** de la etiqueta de destino y aparecerá el cuadro de diálogo **Edit Tag**.

Figura 1-21 Edición de una etiqueta



Paso 7 En el cuadro de diálogo **Edit Tag**, escriba un valor de etiqueta y haga clic en **OK** para completar la edición.


----Fin

1.7.3 Eliminación de etiquetas

En esta sección se describe cómo eliminar etiquetas en la consola KMS.

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 . Elija **Security & Compliance > Data Encryption Workshop**.

Paso 4 Haga clic en el alias de la clave personalizada deseada para ver sus detalles.

Paso 5 Haga clic en **Tags** para ir a la página de gestión de etiquetas.

Paso 6 Haga clic en **Delete** de la etiqueta de destino y aparecerá el cuadro de diálogo **Delete Tag**.

Paso 7 En el cuadro de diálogo **Delete Tag**, haga clic en **Confirm**.

----Fin

1.8 Rotación de CMKs

1.8.1 Acerca de rotación de clave

Propósito de la rotación de clave

Las claves que se usan amplia o repetidamente son inseguras. Para mejorar la seguridad de las claves de encriptación, se recomienda rotar periódicamente las claves y cambiar sus materiales de claves.

Los propósitos de la rotación de claves son:

- Para reducir la cantidad de datos cifrados por cada clave.
Una clave será insegura si se utiliza para cifrar un gran número de datos. La cantidad de datos cifrados por una clave se refiere al número total de bytes o mensajes cifrados mediante la clave.
- Mejorar la capacidad de responder a eventos de seguridad.
En el diseño inicial de su sistema de seguridad, diseñará la función de rotación de teclas y la utilizará para O&M de rutina, de modo que estará a mano cuando ocurra una emergencia.
- Para mejorar la capacidad de aislamiento de datos.
Los datos de texto cifrado generados antes y después de la rotación de clave se aislarán. Puede identificar el alcance de impacto de un evento de seguridad basándose en la clave involucrada y tomar las medidas correspondientes.

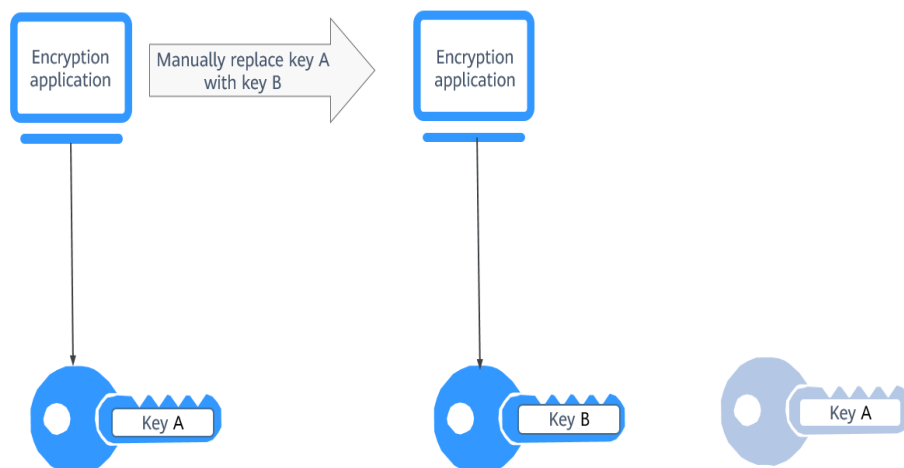
Métodos de rotación de claves

Puede utilizar cualquiera de los siguientes métodos de rotación de claves:

- Rotación manual de clave
Método 1: Crear una clave B para reemplazar la clave A utilizada actualmente.
Método 2: Modificar la clave A y usarla.

Tomemos OBS como ejemplo. Para girar manualmente una clave, cree una nueva clave personalizada en la consola de KMS. Reemplace la antigua clave personalizada por la nueva en la consola OBS.

Figura 1-22 Rotación manual de clave



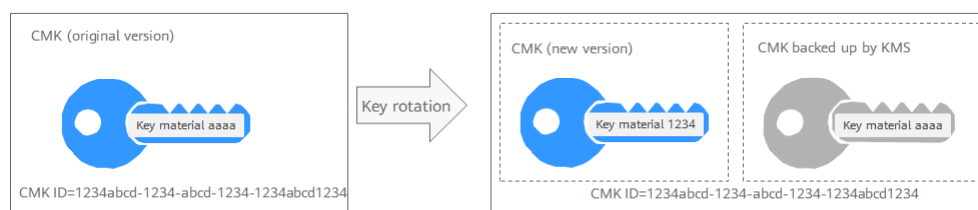
- Rotación automática de clave

KMS rota automáticamente las clave según el período de rotación configurado (365 días por defecto). El sistema genera automáticamente una nueva clave para reemplazar la clave en uso. La rotación automática de clave solo cambia el material de clave de un CMK. Los atributos lógicos de la clave no cambiarán, incluidos su ID de clave, alias, descripción y permisos.

La rotación automática de la llave tiene las siguientes características:

- Habilitar la rotación de una clave personalizada existente. KMS generará automáticamente nuevos materiales clave para la clave personalizada.
- Los datos no se vuelven a cifrar en una rotación de clave automática. El DEK generado con el CMK no se gira automáticamente y los datos que se han cifrado con el CMK no se cifrarán de nuevo. Si se ha producido una fuga de DEK, la rotación automática no puede contener el impacto de la fuga.

Figura 1-23 Rotación de clave



NOTA

KMS conserva todas las versiones de una clave personalizada, para que pueda descifrar cualquier texto cifrado mediante la clave personalizada.

- KMS utiliza la última versión de la clave personalizada para cifrar datos.
- Al descifrar datos, KMS utiliza la versión de clave personalizada que se usó para cifrar los datos.

Modos de rotación

Tabla 1-13 Modos de rotación de clave

Tipo de clave	Modo de rotación
Clave predeterminada	No se puede girar.
Clave personalizada	Las claves se pueden girar de forma automática o manual, dependiendo del tipo de algoritmo de clave. <ul style="list-style-type: none"> ● Clave simétrica: Se puede girar automática o manualmente. ● Clave asimétrica: solo se puede girar manualmente.
CMK deshabilitado	Los CMK deshabilitados no se rotan. KMS mantiene su estado de rotación sin cambios. Después de habilitar una clave personalizada, si se ha utilizado durante más tiempo que el período de rotación, KMS rotará inmediatamente las claves. Si la clave personalizada se ha utilizado durante un período más corto que el período de rotación, KMS implementará el plan de rotación original. Para obtener más información, consulte Deshabilitación de uno o más CMK .
CMK en estado de eliminación pendiente	KMS no rota los CMK en estado de eliminación pendiente. Después de cancelar la eliminación de un CMK, se restaurará el estado de rotación de clave anterior. Si la clave personalizada se ha utilizado durante más tiempo que el período de rotación, KMS rotará inmediatamente las claves. Si el CMK se ha utilizado durante un período de rotación más corto, KMS implementará el plan de rotación original. Para obtener más información, consulte Programación de la eliminación de una o más claves .

NOTA

Puede consultar los detalles de rotación en la página **Rotation Policy**, incluido el tiempo de última rotación y el número de rotaciones.

Precios para rotación de claves

Habilitación de la rotación de clave puede incurrir en cargos adicionales. Para obtener más información, consulte [Descripción de facturación](#).

1.8.2 Habilitación de la rotación de clave

Esta sección describe cómo habilitar la rotación de una clave en la consola KMS.

De forma predeterminada, la rotación automática de clave está deshabilitada para una clave personalizada. Cada vez que habilita la rotación de teclas, KMS gira automáticamente las claves personalizadas en función del período de rotación que establezca.

Prerrequisitos


- La clave está habilitada.
- El **Origin** de la clave es **KMS**.
- Solo se pueden girar las claves simétricas.

Restricciones

- Una clave personalizada deshabilitada nunca se rota, incluso si la rotación está habilitada para ella.
KMS reanuda la rotación cuando esta clave personalizada está habilitada. Si habilita esta clave personalizada una vez transcurrido un período de rotación, KMS la rotará en un plazo de 24 horas.
- Solo se pueden rotar CMK.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

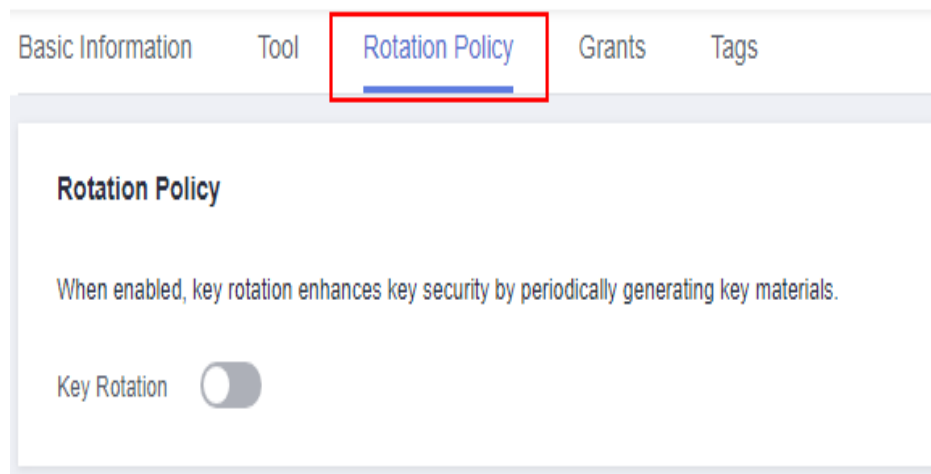
Paso 2 Haga clic en  en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

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

Paso 4 Haga clic en el alias de la clave personalizada deseada para ver sus detalles.

Paso 5 Haga clic en la pestaña **Rotation Policy**. El interruptor de rotación se muestra, como se muestra en **Figura 1-24**.

Figura 1-24 Rotación de clave



Paso 6 Haga clic en  para activar la rotación de clave.

Paso 7 Configure el período de rotación y haga clic en **OK**, como se muestra en **Figura 1-25**. Para obtener más información, consulte **Tabla 1-14**.

Figura 1-25 Habilitación de la rotación de clave

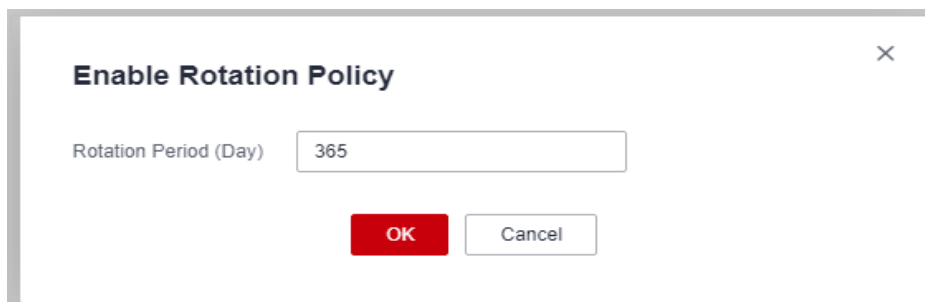



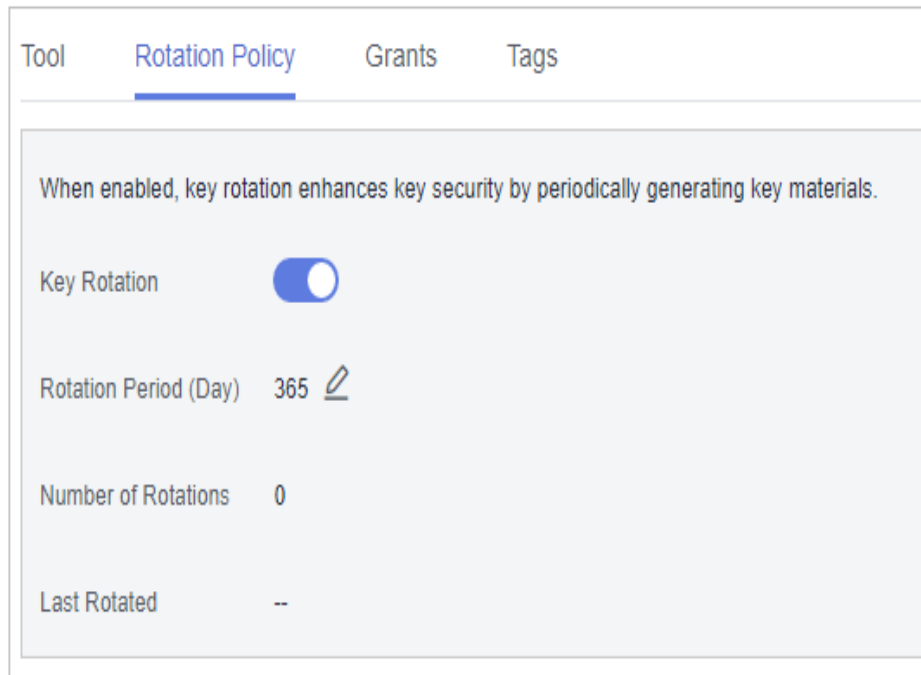


Tabla 1-14 Parámetros de rotación de clave


Parámetro	Descripción
Key rotation	<p>Conmutador de rotación. El estado predeterminado es .</p> <p> : deshabilitado</p> <p> : habilitado</p> <p>Después de activar la rotación, la clave se rotará en función del período establecido.</p> <p>NOTA Una clave personalizada deshabilitada nunca se rota, incluso si la rotación está habilitada para ella. KMS reanuda la rotación cuando esta clave personalizada está habilitada. Si habilita esta clave personalizada una vez transcurrido un período de rotación, KMS la rotará en un plazo de 24 horas.</p>
Rotation Period (day)	<p>Período de rotación (día). El valor es un entero que oscila entre 30 y 365. El valor predeterminado es 365.</p> <p>Configure el período en función de la frecuencia con la que se utilice una clave personalizada. Si se utiliza con frecuencia, configure un período corto; de lo contrario, establezca uno largo.</p>

Paso 8 Compruebe los detalles de rotación, como se muestra en la siguiente figura.

Figura 1-26 Detalles de rotación de claves



 **NOTA**

Puede hacer clic en  para cambiar el período de rotación. Después de cambiar el período, KMS rota la clave por el nuevo período.

----Fin

1.8.3 Deshabilitación de la rotación de clave


Esta sección describe cómo deshabilitar la rotación de una clave en la consola KMS.

Prerrequisitos

- La clave está habilitada.
- El **Origin** de la clave es **KMS**.
- Se ha habilitado la rotación de clave.

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 . Elija **Security & Compliance > Data Encryption Workshop**.

Paso 4 Haga clic en el alias de una clave simétrica.

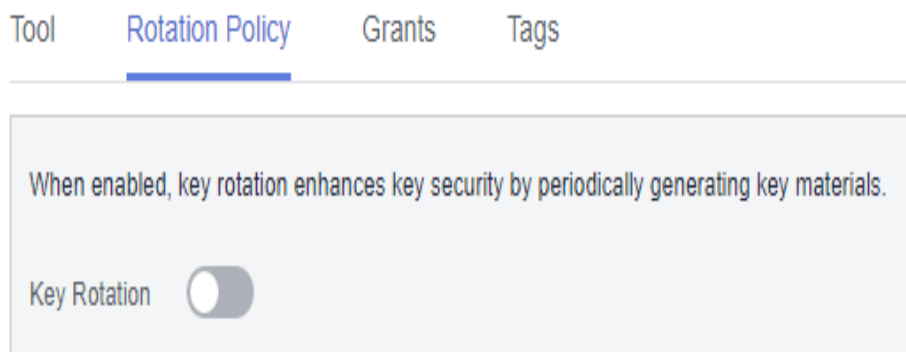
Paso 5 Haga clic en **Rotation Policy** y aparecerá el cuadro de diálogo.

Paso 6 Haga clic en  para desactivar la rotación de clave.

Paso 7 En el cuadro de diálogo de confirmación que se muestra, haga clic en **OK**.

Paso 8 Compruebe el estado de rotación, como se muestra en **Figura 1-27**.

Figura 1-27 Deshabilitación de la rotación de clave



---Fin

1.9 Managing a Grant

1.9.1 Creación de una concesión

Puede crear concesiones para que otros usuarios o cuentas de IAM utilicen la clave personalizada. Puede crear un máximo de 100 concesiones en una clave personalizada.

Prerrequisitos

- Usted ha obtenido el ID del concesionario (usuario al que se autorizarán los permisos).
- La clave personalizada deseada está en estado **Enabled**.

Restricciones

- El propietario de una clave personalizada puede crear una concesión para la clave personalizada en la consola de KMS o invocando a las API. Los usuarios o cuentas de IAM que tienen el permiso de creación de concesión asignado por el propietario de la clave personalizada solo pueden crear concesiones para la clave personalizada invocando a las API.
- Se puede crear un máximo de 100 subvenciones para una clave personalizada.

Procedimiento

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



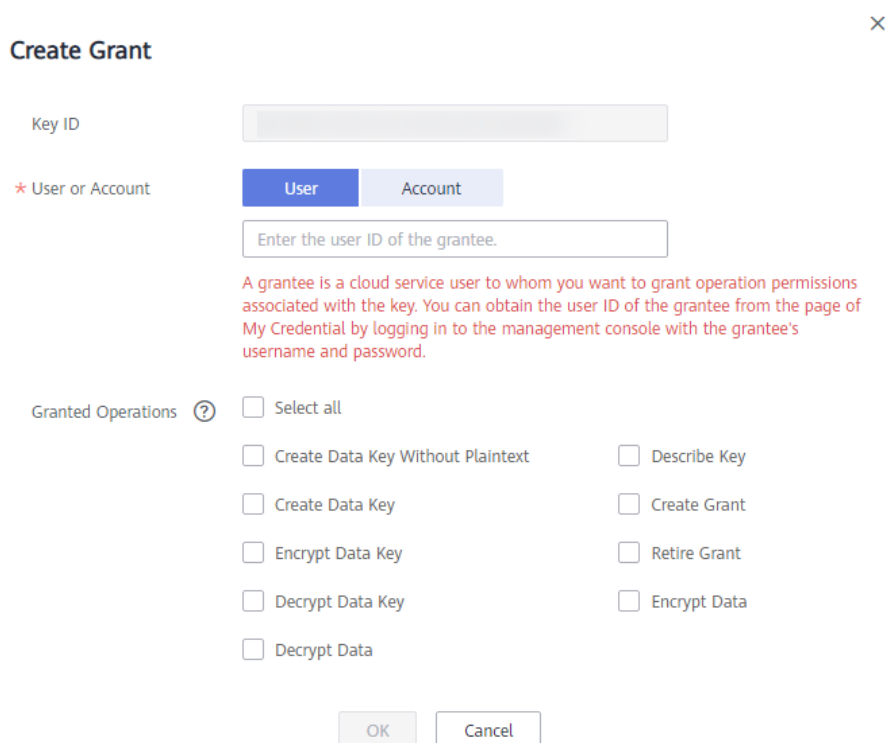
- Paso 2** Haga clic en  en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.
- Paso 3** Haga clic en . Elija **Security & Compliance > Data Encryption Workshop**.
- Paso 4** Haga clic en el alias de la clave personalizada deseada para ir a su página de detalles y crear una concesión en ella.
- Paso 5** Haga clic en la pestaña **Grants**.
- Paso 6** Haga clic en **Create Grant**. Aparece el cuadro de diálogo **Create Grant**.

Figura 1-28 Creación de una concesión (para un usuario)



Create Grant ×

Key ID

* User or Account User Account

A grantee is a cloud service user to whom you want to grant operation permissions associated with the key. You can obtain the user ID of the grantee from the page of My Credential by logging in to the management console with the grantee's username and password.

Granted Operations ?

<input type="checkbox"/> Select all	<input type="checkbox"/> Describe Key
<input type="checkbox"/> Create Data Key Without Plaintext	<input type="checkbox"/> Create Grant
<input type="checkbox"/> Create Data Key	<input type="checkbox"/> Retire Grant
<input type="checkbox"/> Encrypt Data Key	<input type="checkbox"/> Encrypt Data
<input type="checkbox"/> Decrypt Data Key	
<input type="checkbox"/> Decrypt Data	

Figura 1-29 Creación de una concesión (para una cuenta)

The screenshot shows a 'Create Grant' dialog box. At the top right is a close button (X). The main title is 'Create Grant'. Below the title is a 'Key ID' field. Underneath is a section for 'User or Account' with two tabs: 'User' and 'Account'. The 'Account' tab is selected, and below it is a text input field with the placeholder 'Enter a account ID.' and a red note below it: 'A account ID is displayed on the tenant's My Credentials page.' Below this is the 'Granted Operations' section, which includes a help icon (?) and a 'Select all' checkbox. There are ten checkboxes for specific operations: 'Create Data Key Without Plaintext', 'Describe Key', 'Create Data Key', 'Create Grant', 'Encrypt Data Key', 'Retire Grant', 'Decrypt Data Key', 'Encrypt Data', and 'Decrypt Data'. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Paso 7 En el cuadro de diálogo que se muestra, introduzca el ID del usuario que se va a autorizar y seleccione los permisos que se van a conceder. Para obtener más información, consulte [Tabla 1-15](#).

AVISO

Un concesionario puede realizar las operaciones autorizadas solo invocando a las API necesarias. Para obtener más información, consulta la *Referencia de API de Key Management Service*.

Tabla 1-15 Descripción del parámetro

Parámetro	Descripción	Valor de ejemplo
Key ID	ID de una clave personalizada (leída automáticamente por el sistema)	-

Parámetro	Descripción	Valor de ejemplo
User or Tenant	<p>Si un usuario o una cuenta está autorizado.</p> <ul style="list-style-type: none"> ● Usuario ID de usuario: Ingrese el ID de usuario de IAM. Para obtener el ID, haga clic en el nombre de usuario en la esquina superior derecha de la página y elija My Credentials. Elija API Credentials en el panel de navegación y copie el valor de IAM User ID. <p>Una vez completada la autorización, el usuario de IAM puede utilizar las claves especificadas.</p> ● Cuenta ID de cuenta: Ingrese el ID de usuario de IAM. Para obtener el ID, haga clic en el nombre de usuario en la esquina superior derecha de la página y elija My Credentials. Elija API Credentials en el panel de navegación y copie el valor de Account ID. <p>Una vez completada la autorización, todos los usuarios de IAM bajo la cuenta pueden utilizar las claves especificadas.</p> 	<p>d9a6b2bdaedd4b a586cabe6372d1 b312</p>
Grant Name	Puedes nombrar la concesión.	test

Parámetro	Descripción	Valor de ejemplo
Operations	<p>Se pueden autorizar los siguientes permisos:</p> <p>NOTA</p> <ul style="list-style-type: none"> ● Puede crear varias concesiones en una clave personalizada para proporcionar diferentes permisos al mismo usuario. Los permisos del usuario en la clave personalizada son la combinación de todas las concesiones. ● Este parámetro es obligatorio. ● No se permite seleccionar solo Create Grant. ● Crear clave de datos sin texto sin formato ● Crear clave de datos ● Encriptar clave de datos ● Desencriptar clave de datos ● Consultar información de clave ● Crear concesión ● Retirar concesión <ul style="list-style-type: none"> – Un concesionario puede retirar una concesión si el concesionario no necesita ese permiso. – Si, antes de retirar una concesión, el beneficiario ha concedido el permiso a otro usuario, el permiso de ese usuario no se verá afectado por la retirada de la concesión. ● Encriptar datos ● Desencriptar datos 	-

Paso 8 Haga clic en **OK**. Cuando se muestra el mensaje **Grant created successfully** en la esquina superior derecha, se ha creado la concesión.

En la lista de concesiones, puede ver el nombre de la concesión, el ID de concesión, el tipo de concesión, el ID del concesionario, la operación concedida y el tiempo de creación de la concesión.

---Fin

1.9.2 Consulta de una concesión


En esta sección se describe cómo ver los detalles sobre una concesión de clave personalizada en la consola KMS, como el ID de concesión, el ID de usuario del concesionario, la operación concedida y el tiempo de creación.

Prerrequisitos

Usted ha creado una concesión.

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 . Elija **Security & Compliance > Data Encryption Workshop**.

Paso 4 Haga clic en el alias de la clave personalizada deseada para ver sus detalles.

Paso 5 Haga clic en **Grant** para ver la información de concesión de la clave personalizada actual. [Tabla 1-16](#) describe los parámetros.

Tabla 1-16 Descripción del parámetro

Parámetro	Descripción
Grant Name	Nombre de la concesión cuando se crea
Grant ID	Identificación única generada aleatoriamente de una concesión
Granted To	Si se conceden permisos a un usuario o cuenta.
Grantee ID	ID del usuario o cuenta autorizado.
Granted Operations	Operaciones autorizadas (como Create Data Key) en la clave personalizada
Created	Hora de creación de la concesión
Operation	Operaciones que se pueden realizar en una concesión. Por ejemplo, puede revocar una concesión.


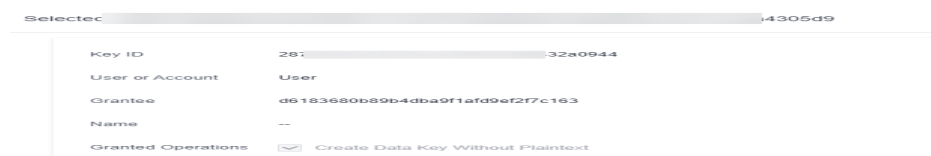
Paso 6 Seleccione la concesión de destino y haga clic en  en la esquina inferior derecha para ver los detalles de la concesión, como se muestra en [Figura 1-30](#).

Figura 1-30 Consulta de los detalles de la concesión



----Fin

1.9.3 Revocación de una concesión

Puede revocar una concesión en la consola KMS en cualquiera de los siguientes escenarios:

- Un concesionario no necesita la concesión de clave personalizada. (El concesionario puede decirle al usuario que ha creado la concesión que revoque la concesión o invocar a la API necesaria para revocar la concesión directamente.)

- Usted no desea que el concesionario tenga la concesión.

Cuando se revoca una concesión, el concesionario ya no tiene el permiso correspondiente. Sin embargo, si el concesionario ha creado la misma concesión a otro usuario, el permiso de ese usuario no se verá afectado.


Esta sección describe cómo revocar una concesión en la consola KMS.

Prerrequisitos

Usted ha creado una concesión.

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 . Elija **Security & Compliance > Data Encryption Workshop**.

Paso 4 Haga clic en el alias de la clave personalizada deseada para ver sus detalles.

Paso 5 En la fila de un concesionario, haga clic en **Revoke Grant**.

Paso 6 En el cuadro de diálogo que se muestra, haga clic en **OK**. Si aparece **Grant *grant ID* revoked successfully** en la esquina superior derecha, la concesión ha sido revocada.

----Fin

2 Cloud Secret Management Service

2.1 Creación de un secreto

2.1.1 Creación de un secreto compartido

Esta sección describe cómo crear un secreto en la consola CSMS.


Puede crear un secreto y almacenar su valor en su versión inicial, que está marcada como **SYSCURRENT**.


Restricciones

- Un usuario puede crear un máximo de 200 secretos.
- De forma predeterminada, la clave predeterminada **csms/default** creada por CSMS se utiliza como clave de encriptación del secreto actual. También puede crear una clave simétrica definida por el usuario y utilizar una clave de encriptación definida por el usuario en la consola de KMS.

Creación de un secreto

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, elija **Cloud Secret Management Service**.

Paso 5 Haga clic en **Create Secret**. Configure los parámetros en el cuadro de diálogo **Create Secret** como se muestra en el documento [Figura 2-1](#). Para obtener más información, consulte [Tabla 2-1](#).

Figura 2-1 Creación de un secreto

Tabla 2-1 Parámetros de secreto

Parámetro	Descripción
Type	Tipo de secreto. El valor predeterminado es Shared secret .
Secret Name	Nombre de secreto
Enterprise Project	Proyecto empresarial al que se debe vincular el secreto
Secret Value	Par de clave/valor de secreto y el secreto en texto plano que se va a cifrar
Description	Descripción de un secreto

Parámetro	Descripción
KMS Encryption Key	Seleccione la clave predeterminada csms/default o una clave personalizada creada en KMS. NOTA De forma predeterminada, la clave predeterminada csms/default creada por CSMS se utiliza como la clave maestra de encriptación del secreto actual. También puede crear una clave o utilizar una clave personalizada en la consola de KMS. Para más detalles, consulte Creación de una clave .
Associated Event	Al crear un secreto, puede asociarlo con un evento secreto. Puede agregar, eliminar, modificar y consultar versiones secretas en la página de notificación de eventos.

Paso 6 Haga clic en **Next** y establezca el período de rotación.

Paso 7 Haga clic en **Next** y confirme la información de creación.

Paso 8 Haga clic en **OK**.

En la lista de secretos, puede ver los secretos creados. El estado predeterminado de un secreto es **Enabled**.

---Fin


2.2 Gestión de secretos


2.2.1 Ver un secreto

Esta sección describe cómo comprobar nombres secretos, estados y tiempo de creación en la consola de CSMS. El estado de secreto puede ser **Enabled** o **Pending deletion**.

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, elija **Security & Compliance > Data Encryption Workshop**, se mostrará la página de gestión de claves.

Paso 4 En el panel de navegación, elija **Cloud Secret Management Service**.

Paso 5 Revise la lista de secreto. Para obtener más información, consulte [Tabla 2-2](#).

Figura 2-2 Lista de secretos

Secret Name ID	Status	Type	Associated Event	Created	Enterprise Project	Operation
ac0177db-102224	Enabled	Shared secret	-	Dec 27, 2022 01:50:10 GMT+08:00	default	Download Backup Delete
ad01380b61afa	Enabled	Shared secret	-	Jun 28, 2023 14:40:31 GMT+08:00	default	Download Backup Delete

Tabla 2-2 Parámetros de lista de secreto

Parámetro	Descripción
Secret Name/ID	Nombre de secreto
Status	Estado de un secreto. El valor puede ser Enabled o Pending deletion .
Type	Tipo de secreto, incluidos secretos compartidos y secretos de instancia de base de datos de RDS.
Created	Tiempo en que se crea un secreto
Enterprise Project	Proyecto empresarial al que se debe vincular el secreto
Operation	Puede gestionar los secretos en la columna Operation , por ejemplo, descargar una copia de respaldo secreta, eliminar secretos y cancelar la eliminación de secretos.

Paso 6 Haga clic en un secreto para ver sus detalles. Véase [Figura 2-3](#).

Figura 2-3 Detalles de secretos

Secret Details		Basic Information	
Name	[Redacted]	Secret ID	50bb760a-0458-4f6c-8a9a-1155b1f6770a
Type	Shared secret	Status	Enabled
Created	Oct 27, 2023 16:06:50 GMT+0...	Encryption Key	6452d410-dbb7-4700-9c10-9f1d470e132
Updated	Nov 20, 2023 14:25:16 GMT+0...	Description	—
Enterprise Project	default	Associated Event	—

NOTA

- Puede hacer clic en **Edit** para modificar la clave de encriptación y la descripción de un secreto.
- Puede hacer clic en **Refresh** para actualizar la información secreta.

----Fin

2.2.2 Búsqueda de secretos por evento


Busque secretos por evento asociado en la página de gestión de secretos.


Prerrequisitos

El secreto que desea buscar se ha asociado con un evento.

Procedimiento

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

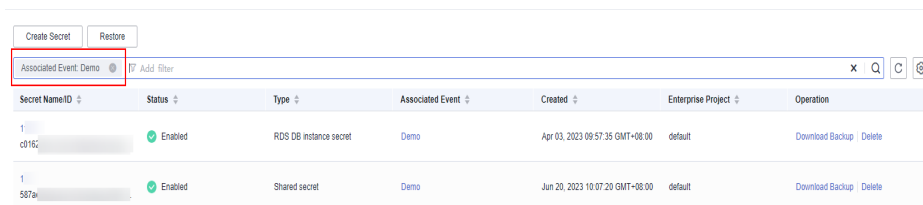
Paso 2 Haga clic en  en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

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

Paso 4 En el panel de navegación, elija **Cloud Secret Management Service**.

Paso 5 Haga clic en la barra de búsqueda y seleccione el **Associated Event** como la condición de filtrado secreto, como se muestra en **Figura 2-4**. Busque un secreto especificando el evento asociado.

Figura 2-4 Búsqueda de un secreto



----Fin

2.2.3 Eliminación de un secreto

Antes de eliminar un secreto, confirme que no está en uso y que no se utilizará.

Prerrequisitos


El secreto que se va a eliminar está en estado **Enabled**.


Restricciones

- Un secreto no se eliminará hasta que expire su período de eliminación programado. Puede establecer el período en un valor dentro del rango de 7 a 30 días. Antes de la fecha de eliminación especificada, puede cancelar la eliminación si desea utilizar el secreto. Si el período de eliminación programado de un secreto expira, el secreto se eliminará y no se podrá restaurar.
- Para obtener detalles sobre la información de facturación sobre un secreto que se va a eliminar, consulte [¿Las credenciales están programadas para ser eliminadas?](#)
- Si elimina un secreto inmediatamente, puede restaurarlo utilizando la copia de respaldo secreta que ha descargado por adelantado. Tenga cuidado cuando realice esta acción.

Eliminación de un secreto

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, elija **Cloud Secret Management Service**.

Paso 5 En la fila de un secreto, haga clic en **Delete**.

Figura 2-5 Eliminación de un secreto

Secret Name/ID	Status	Type	Associated Event	Created	Enterprise Project	Operation
abc177db-22224	Enabled	Shared secret	-	Dec 27, 2022 01:59:10 GMT+08:00	default	Download Backup Delete
abc138ba6c-1afa	Enabled	Shared secret	-	Jun 28, 2023 14:40:31 GMT+08:00	default	Download Backup Delete

Paso 6 En la página mostrada, seleccione un modo de eliminación. Si desea eliminar el secreto en un momento específico, establezca **Schedule deletion**.

Figura 2-6 Establecer la eliminación de horarios

Paso 7 En el cuadro de diálogo de confirmación, escriba **DELETE** y haga clic en **OK**.

NOTA

- Un secreto no se eliminará hasta que expire su período de eliminación programado. Puede establecer el periodo en un valor dentro del rango de 7 a 30 días. Antes de la fecha de eliminación especificada, puede cancelar la eliminación si desea utilizar el secreto. Si el período de eliminación programado de un secreto expira, el secreto se eliminará y no se podrá restaurar.
- Para obtener detalles sobre la información de facturación sobre un secreto que se va a eliminar, consulte [¿Las credenciales están programadas para ser eliminadas?](#)
- Si elimina un secreto inmediatamente, puede restaurarlo utilizando la copia de respaldo secreta que ha descargado por adelantado. Tenga cuidado cuando realice esta acción.

---Fin

2.3 Gestión de versiones de secreto

2.3.1 Guardar y ver valores secretos

Esta sección describe cómo guardar y ver valores secretos en la consola CSMS.


Puede crear una nueva versión de un secreto para cifrar y mantener un nuevo valor de secreto. De forma predeterminada, la última versión secreta en estado **SYSCURRENT**. La versión anterior está en el estado **SYSPREVIOUS**.


Restricciones

- Un secreto puede tener hasta 20 versiones.
- Las versiones secretas se numeran v1, v2, v3, y así sucesivamente en función de su tiempo de creación.

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.

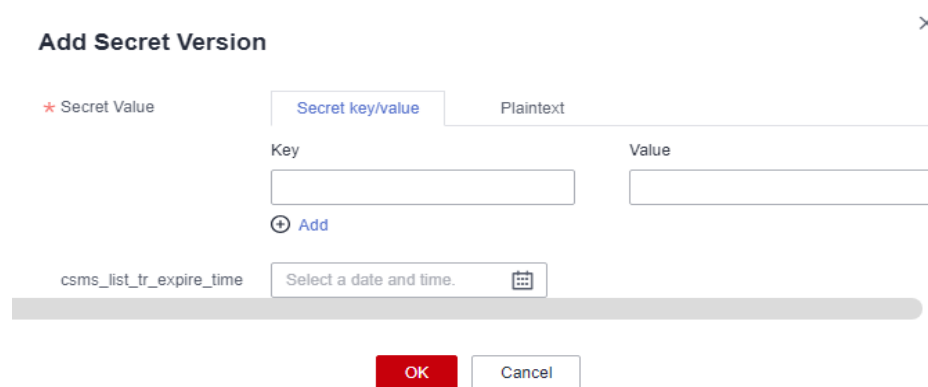
Paso 3 Haga clic en  a la izquierda, elija **Security & Compliance > Data Encryption Workshop**, se mostrará la página de gestión de claves.

Paso 4 En el panel de navegación, elija **Cloud Secret Management Service**.

Paso 5 Haga clic en un nombre secreto para ir a la página de detalles.

Paso 6 En el área **Version List**, haga clic en **Add Secret Version**. Configure la clave de secreto y el valor en el cuadro de diálogo que se muestra.

Figura 2-7 Adición de un valor de secreto



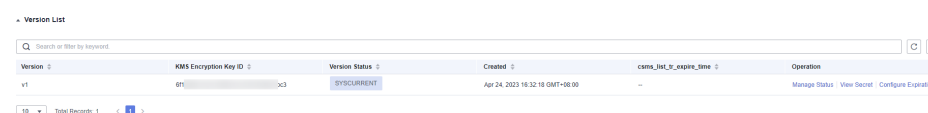
Paso 7 Puede seleccionar un tiempo de caducidad para el valor secreto almacenado. El tiempo puede ser específico para segundos. Una vez completada la configuración, puede ver el tiempo de caducidad en la lista de versiones secretas. Por ejemplo, el 30 de junio de 2023 19:52:59.

Paso 8 Haga clic en **OK**. Se muestra un mensaje en la esquina superior derecha de la página, indicando que el valor se ha añadido correctamente.

Vea el último valor secreto en la lista de versiones secretas.

Paso 9 En el área **Version List**, haga clic en **View Secret** en la columna **Operation** de un secreto.

Figura 2-8 Lista de versiones secreta



Paso 10 Vea el valor secreto y haga clic en **OK**.

----Fin

2.3.2 Gestión de estados de versión de secreto

Esta sección describe cómo agregar, cambiar y eliminar estados de versiones de secreto.


Los valores de secreto se cifran y se almacenan en versiones de secreto. Una versión puede tener varios estados. Las versiones sin ningún estado se consideran obsoletas y pueden ser eliminadas automáticamente por CSMS.


Restricciones

- La versión inicial se marca con la etiqueta de estado **SYSCURRENT**.
- Puede marcar una versión con una etiqueta creada en el servicio o una etiqueta personalizada. Una versión puede tener varias etiquetas de estado, pero una etiqueta de estado solo se puede usar para una versión. Por ejemplo, si agrega la etiqueta de estado utilizada por la versión A a la versión B, la etiqueta se moverá de la versión A a la versión B.
- Un secreto puede tener hasta 12 estados de versión. Un estado solo se puede usar para una versión.
- **SYSCURRENT** y **SYSPREVIOUS** son estados preconfigurados y no se pueden eliminar.

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.

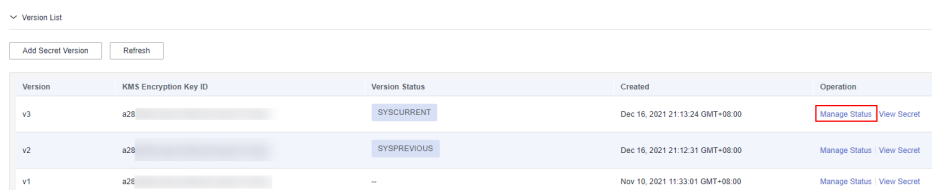
Paso 3 Haga clic en  a la izquierda, elija **Security & Compliance > Data Encryption Workshop**, se mostrará la página de gestión de claves.

Paso 4 En el panel de navegación, elija **Cloud Secret Management Service**.

Paso 5 Haga clic en un nombre de secreto para ir a la página de detalles.

Paso 6 En el área **Version List**, haga clic en **Manage Status** en la columna **Operation**.

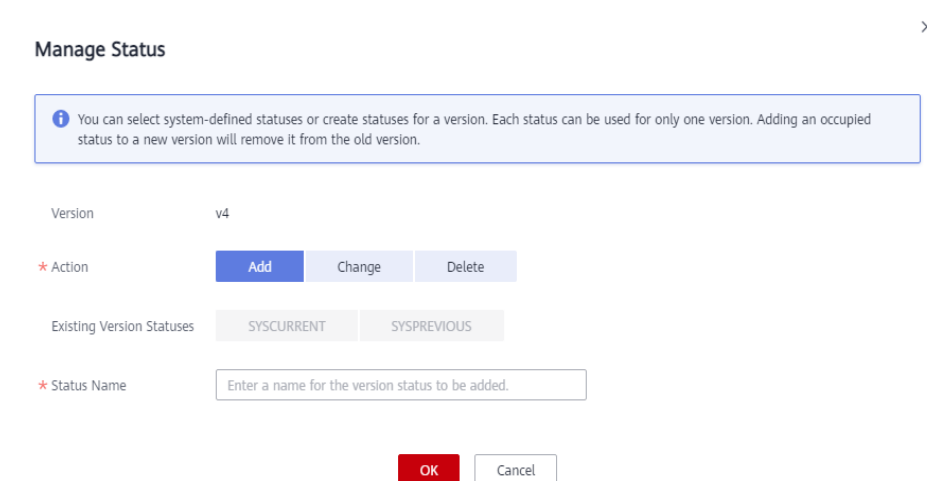
Figura 2-9 Lista de versiones de secreto



Version	KMS Encryption Key ID	Version Status	Created	Operation
v3	a26	SYSCURRENT	Dec 16, 2021 21:13:24 GMT+08:00	Manage Status View Secret
v2	a26	SYSPREVIOUS	Dec 16, 2021 21:12:31 GMT+08:00	Manage Status View Secret
v1	a26	--	Nov 10, 2021 11:33:01 GMT+08:00	Manage Status View Secret

Paso 7 En el cuadro de diálogo **Manage Status**, agregue, cambie o elimine el estado de una versión de secreto.

Figura 2-10 Gestión de estados



- **Adición de un estado de versión**
En el cuadro de diálogo **Manage Status**, haga clic en **Add** e introduzca un nombre de estado. Haga clic en **OK**.

NOTA

Un secreto puede tener hasta 12 estados de versión. Un estado solo se puede usar para una versión.

- **Actualización del estado de la versión de un secreto**
En el cuadro de diálogo **Manage Status**, haga clic en **Change** y seleccione un estado de versión existente. Haga clic en **OK**.
- **Eliminación del estado de versión de un secreto**
En el cuadro de diálogo **Manage Status**, haga clic en **Delete** y seleccione un estado de versión. Haga clic en **OK**.

NOTA



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

----Fin

2.3.3 Setting the Version Expiration Time

This section describes how to set the version expiration time on the secret details page.

Procedure

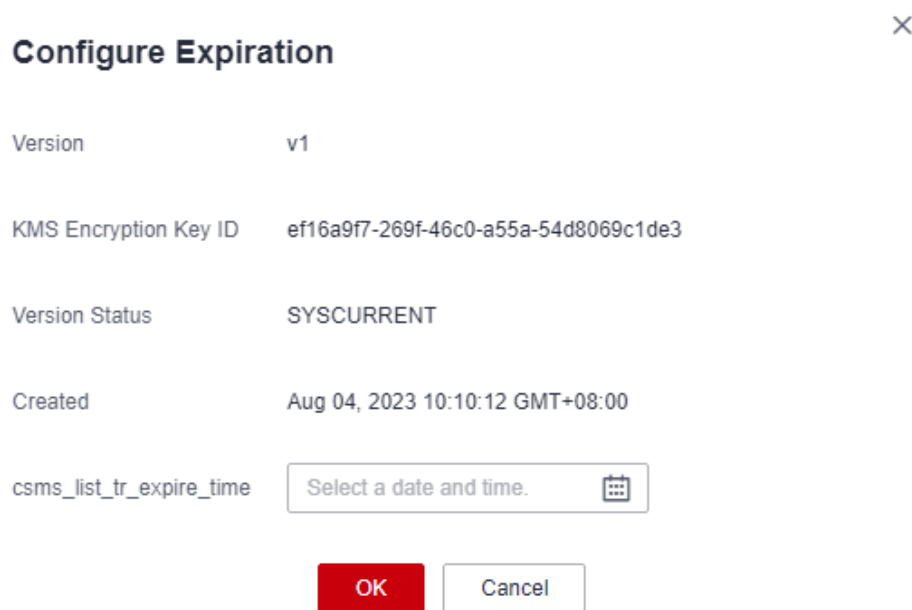
- Paso 1** **Inicie sesión en la consola de gestión.**
- Paso 2** Haga clic en  en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.
- Paso 3** Haga clic en  a la izquierda, elija **Security & Compliance > Data Encryption Workshop**, se mostrará la página de gestión de claves.
- Paso 4** En el panel de navegación, elija **Cloud Secret Management Service**.

Paso 5 Click a secret name to go to the details page.

Paso 6 In the **Current Version** area, click **Configure Expiration** of the target secret version.

Paso 7 On the displayed page, set an expiration time, and click **OK**.

Figura 2-11 Setting an expiration time



---Fin


2.4 Gestión de etiquetas


2.4.1 Adición de una etiqueta

Las etiquetas se utilizan para identificar secretos. Puede clasificar y rastrear fácilmente los secretos usando etiquetas.

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.

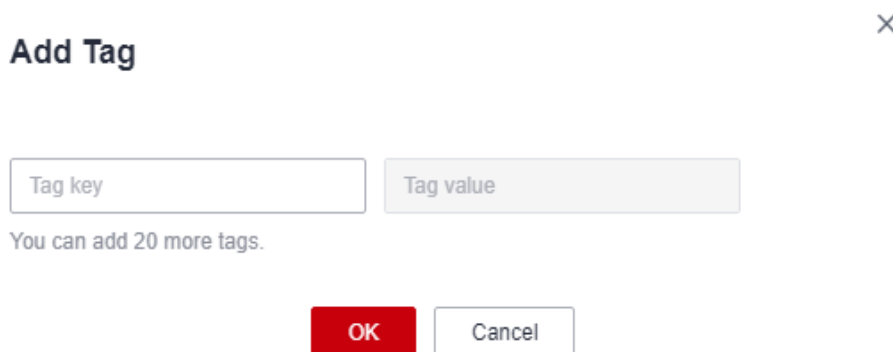
Paso 3 Haga clic en  a la izquierda, elija **Security & Compliance > Data Encryption Workshop**, se mostrará la página de gestión de claves.

Paso 4 En el panel de navegación, elija **Cloud Secret Management Service**.

Paso 5 Haga clic en un nombre secreto para ir a la página de detalles.

Paso 6 En el área **Tags**, haga clic en **Add Tag**. En el cuadro de diálogo **Add Tag**, escriba la clave de etiqueta y el valor de etiqueta. [Tabla 2-3](#) describe los parámetros.

Figura 2-12 Agregar una etiqueta



NOTA

- Si desea utilizar la misma etiqueta para identificar varios recursos en la nube, puede crear etiquetas predefinidas en el TMS. De esta manera, se puede seleccionar la misma etiqueta para todos los servicios. Para obtener más información acerca de las etiquetas predefinidas, consulte la *Guía de usuario de Tag Management Service*.
- Para eliminar una etiqueta, haga clic en **Delete** junto a ella.

Tabla 2-3 Parámetros de etiqueta

Parámetro	Descripción	Observaciones
Tag key	<p>Nombre de la etiqueta.</p> <p>Las claves de etiqueta de un secreto no pueden tener valores duplicados. Se puede usar una clave de etiqueta para múltiples secretos.</p> <p>Un secreto puede tener hasta 20 etiquetas.</p>	<ul style="list-style-type: none"> ● Obligatorio. ● La clave de etiqueta debe ser única para la misma clave personalizada. ● Límite de 128 caracteres. ● El valor no puede comenzar ni finalizar con un espacio. ● No se puede iniciar con <code>_sys_</code>. ● Se permiten los siguientes tipos de caracteres: <ul style="list-style-type: none"> – Chino – Inglés – Números – Espacio – Caracteres especiales: <code>./=+-@</code>

Parámetro	Descripción	Observaciones
Tag value	Valor de la etiqueta	<ul style="list-style-type: none"> ● Opcional ● Límite de 255 caracteres. ● Se permiten los siguientes tipos de caracteres: <ul style="list-style-type: none"> – Chino – Inglés – Números – Espacio – Caracteres especiales: ./=@+-

Paso 7 Haga clic en **OK**.

----Fin

2.4.2 Búsqueda de un secreto por etiqueta


Esta sección describe cómo buscar un secreto por etiqueta en un proyecto en la consola CSMS.


Prerrequisitos

Se han agregado etiquetas.

Procedimiento

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

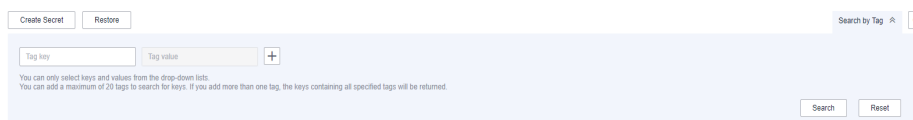
Paso 2 Haga clic en  en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

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

Paso 4 En el panel de navegación, elija **Cloud Secret Management Service**.

Paso 5 Click **Search by Tag** to show the search box, as shown in [Figura 2-13](#).

Figura 2-13 Search box



Paso 6 In the search box, enter or select a tag key and a tag value.


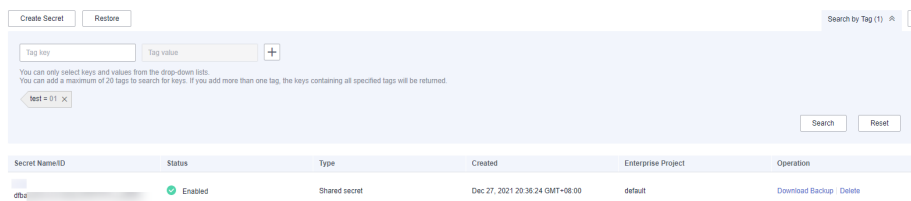

Paso 7 Haga clic en  para agregar la entrada a los criterios de búsqueda y haga clic en **Search**. Como se muestra en [Figura 2-14](#).

Figura 2-14 Resultado de la búsqueda



NOTA

- Se pueden agregar varias etiquetas para una búsqueda. Se puede agregar un máximo de 20 etiquetas para una búsqueda. Cada resultado de búsqueda cumple con todos los criterios de búsqueda.
- Para eliminar una etiqueta de los criterios de búsqueda, haga clic en  junto a la etiqueta.
- Puede hacer clic en **Reset** para restablecer los criterios de búsqueda.


----Fin


2.4.3 Modificación de un valor de etiqueta

Esta sección describe cómo modificar los valores de etiqueta en la consola CSMS.

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.

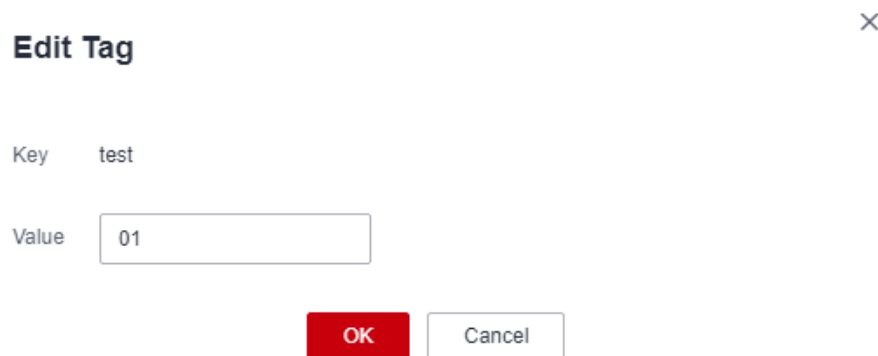
Paso 3 Haga clic en  a la izquierda, elija **Security & Compliance > Data Encryption Workshop**, se mostrará la página de gestión de claves.

Paso 4 En el panel de navegación, elija **Cloud Secret Management Service**.

Paso 5 Haga clic en un nombre de secreto para ir a la página de detalles.

Paso 6 En el área **Tags**, haga clic en **Edit**.

Figura 2-15 Edición de una etiqueta



Edit Tag ×

Key test

Value 01

OK Cancel

Paso 7 En el cuadro de diálogo **Edit Tag**, escriba un valor de etiqueta y haga clic en **OK**.


----Fin


2.4.4 Eliminación de una etiqueta

Esta sección describe cómo eliminar etiquetas en la consola CSMS.

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, elija **Security & Compliance > Data Encryption Workshop**, se mostrará la página de gestión de claves.

Paso 4 En el panel de navegación, elija **Cloud Secret Management Service**.

Paso 5 Haga clic en un nombre secreto para ir a la página de detalles.

Paso 6 En el área **Tags**, haga clic en **Delete**.

Paso 7 En el cuadro de diálogo **Delete Tag**, haga clic en **Yes**.

----Fin

2.5 Creación de un evento

En esta sección se describe cómo crear un evento en la página **Events**.

Al crear un evento, puede establecer el tipo de evento en **Version creation**, **Version expiry**, **Secret rotation** y **Secret deletion** nuevo.

Restricciones

Puede crear un máximo de 30 eventos.

Procedimiento



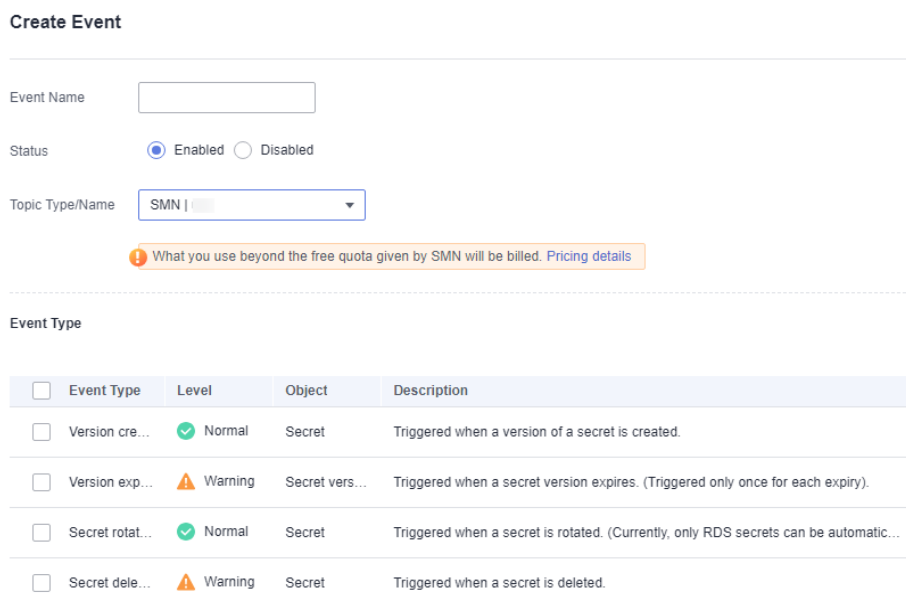
- Paso 1** [Inicie sesión en la consola de gestión.](#)
- Paso 2** Haga clic en  en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.
- Paso 3** Haga clic en  a la izquierda, elija **Security & Compliance > Data Encryption Workshop**, se mostrará la página de gestión de claves.
- Paso 4** En el panel de navegación de la izquierda, elija **Cloud Secret Management Service > Events**. Se muestra la página **Events**.
- Paso 5** Haga clic en **Create Event** en la esquina superior derecha. Se muestra la página para crear un evento, como se muestra en [Creación de un evento](#).

Figura 2-16 Creación de un evento



Event Type	Level	Object	Description
<input type="checkbox"/> Version cre...	Normal	Secret	Triggered when a version of a secret is created.
<input type="checkbox"/> Version exp...	Warning	Secret vers...	Triggered when a secret version expires. (Triggered only once for each expiry).
<input type="checkbox"/> Secret rotat...	Normal	Secret	Triggered when a secret is rotated. (Currently, only RDS secrets can be automatic...
<input type="checkbox"/> Secret dele...	Warning	Secret	Triggered when a secret is deleted.

Tabla 2-4 Parámetros para crear un evento

Parámetro	Descripción
Event Name	Nombre del evento que se va a crear.
Status	Las opciones son Enabled y Disabled . De forma predeterminada, se selecciona Enabled .
Topic Type/Name	Tipo de tema: se selecciona SMN de forma predeterminada. Nombre del tema: nombre del tema creado en SMN.
Event Type	Tipos de eventos compatibles, incluidos Version creation , Version expiry , Secret rotation y Secret deletion .

Paso 6 Haga clic en **OK**.

Paso 7 Vea el evento creado en la lista de eventos, como se muestra en **Figura 2-17**. El estado predeterminado del evento es **Enabled**.

Figura 2-17 Lista de eventos

Event Name	Status	Subscription	Topic Type Name	Created	Operation
Demo	Enabled	Version creation Secret rotation Secret ...	SMN	Jun 07, 2023 16:16:47 GMT+08:00	Edit Delete
demo01	Enabled	Version creation Version expiry Secret ...	SMN	Jun 12, 2023 11:37:26 GMT+08:00	Edit Delete
demo010	Enabled	Version creation Version expiry Secret ...	SMN	Jun 12, 2023 14:38:29 GMT+08:00	Edit Delete
demo02	Enabled	Version creation Version expiry Secret ...	SMN	Jun 12, 2023 11:38:19 GMT+08:00	Edit Delete
demo03	Enabled	Secret rotation	SMN	Jun 12, 2023 11:38:32 GMT+08:00	Edit Delete
demo04	Enabled	Secret deletion	SMN	Jun 12, 2023 11:38:50 GMT+08:00	Edit Delete
demo05	Enabled	Version creation	SMN	Jun 12, 2023 11:39:09 GMT+08:00	Edit Delete
demo06	Enabled	Secret deletion	SMN	Jun 12, 2023 11:39:29 GMT+08:00	Edit Delete
demo09	Enabled	Secret rotation	SMN	Jun 12, 2023 11:39:57 GMT+08:00	Edit Delete
lytest	Enabled	Version creation Version expiry Secret ...	SMN	Jul 05, 2023 11:12:37 GMT+08:00	Edit Delete

----Fin


2.6 Gestión de eventos


2.6.1 Consulta de eventos

En esta sección se describe cómo ver la información sobre los eventos creados en la página **Events**, incluidos el nombre del evento, el estado, el tipo de evento de suscripción, el tipo/ nombre de tema y la hora de creación.

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, elija **Security & Compliance > Data Encryption Workshop**, se mostrará la página de gestión de claves.

Paso 4 En el panel de navegación de la izquierda, elija **Cloud Secret Management Service > Events**. Se muestra la página **Events**.

Paso 5 En la lista de eventos, vea la información del evento. **Tabla 2-5** describe los parámetros de la lista de eventos.

Figura 2-18 Lista de eventos

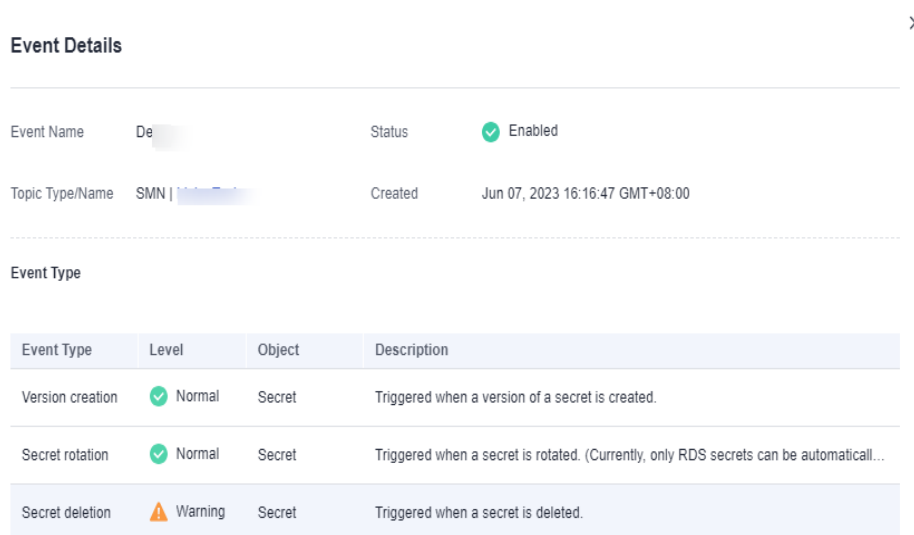
Event Name	Status	Subscription	Topic Type Name	Created	Operation
Demo	Enabled	Version creation Secret rotation Secret ...	SMN	Jun 07, 2023 16:16:47 GMT+08:00	Edit Delete
demo01	Enabled	Version creation Version expiry Secret ...	SMN	Jun 12, 2023 11:37:26 GMT+08:00	Edit Delete
demo010	Enabled	Version creation Version expiry Secret ...	SMN	Jun 12, 2023 14:38:29 GMT+08:00	Edit Delete
demo02	Enabled	Version creation Version expiry Secret ...	SMN	Jun 12, 2023 11:38:19 GMT+08:00	Edit Delete
demo03	Enabled	Secret rotation	SMN	Jun 12, 2023 11:38:32 GMT+08:00	Edit Delete
demo04	Enabled	Secret deletion	SMN	Jun 12, 2023 11:38:50 GMT+08:00	Edit Delete
demo05	Enabled	Version creation	SMN	Jun 12, 2023 11:39:09 GMT+08:00	Edit Delete
demo06	Enabled	Secret deletion	SMN	Jun 12, 2023 11:39:29 GMT+08:00	Edit Delete
demo09	Enabled	Secret rotation	SMN	Jun 12, 2023 11:39:57 GMT+08:00	Edit Delete
lytest	Enabled	Version creation Version expiry Secret ...	SMN	Jul 05, 2023 11:12:37 GMT+08:00	Edit Delete

Tabla 2-5 Parámetros en la lista de eventos

Parámetro	Descripción
Event Name	Nombre de un evento
Status	Estado del evento, incluidos: <ul style="list-style-type: none"> ● Enabled El evento está habilitado. ● Disabled El evento está desactivado.
Subscription	Tipo de evento seleccionado durante la creación del evento. Las opciones son las siguientes: <ul style="list-style-type: none"> ● Version creation ● Version expiry ● Secret rotation ● Secret deletion
Topic Type/Name	Tipo de tema: se selecciona SMN de forma predeterminada. Nombre del tema: nombre del tema creado en SMN.
Created	Hora en que se crea el evento
Operation	Puede editar o eliminar un evento en la columna Operation .

Paso 6 Haga clic en el nombre de un evento para ver los detalles del evento, como se muestra en [Figura 2-19](#).

Figura 2-19 Detalles del evento



----Fin

2.6.2 Edición de un evento

En esta sección se describe cómo modificar un tipo de evento en la página **Events**.

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, elija **Security & Compliance > Data Encryption Workshop**, se mostrará la página de gestión de claves.
- Paso 4** En el panel de navegación de la izquierda, elija **Cloud Secret Management Service > Events**. Se muestra la página **Events**.
- Paso 5** Haga clic en **Edit** en la columna **Operation** del evento de destino. Se muestra la página **Edit Event**.
- Paso 6** Seleccione el tipo de evento de destino, como se muestra en [Figura 2-20](#).

Figura 2-20 Edición de un evento

Event Type

<input type="checkbox"/>	Event Type	Level	Object	Description
<input checked="" type="checkbox"/>	Version creation	 Normal	Secret	Triggered when a version of a secret is created.
<input type="checkbox"/>	Version expiry	 Warning	Secret version	Triggered when a secret version expires. (Triggered only once for each expiry).
<input checked="" type="checkbox"/>	Secret rotation	 Normal	Secret	Triggered when a secret is rotated. (Currently, only RDS secrets can be automatic
<input checked="" type="checkbox"/>	Secret deletion	 Warning	Secret	Triggered when a secret is deleted.

- Paso 7** Haga clic en **OK**.

----Fin

2.6.3 Habilitación de un evento


En esta sección se describe cómo habilitar un evento deshabilitado en la página **Events**.


Prerrequisitos

El evento que se va a habilitar debe estar en el estado **Disabled**.

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, elija **Security & Compliance > Data Encryption Workshop**, se mostrará la página de gestión de claves.

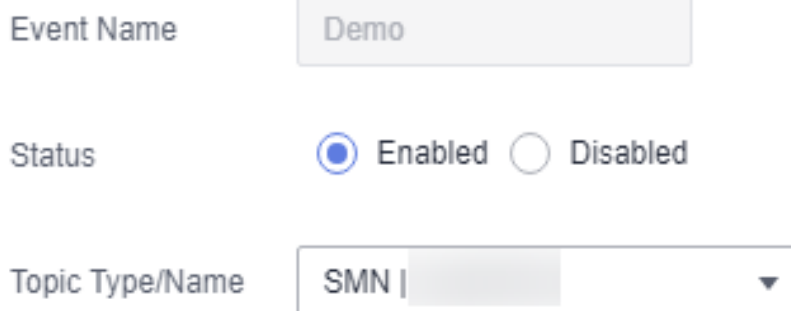
Paso 4 En el panel de navegación de la izquierda, elija **Cloud Secret Management Service > Events**. Se muestra la página **Events**.

Paso 5 Haga clic en **Edit** en la columna **Operation** del evento de destino. Se muestra la página **Edit Event**.

Paso 6 Seleccione **Enabled** para **Status**.

Figura 2-21 Habilitación de un evento

Edit Event



Event Name

Status Enabled Disabled

Topic Type/Name

Paso 7 Haga clic en **OK**. En la esquina superior derecha de la página aparece un mensaje que indica que el estado del evento se ha actualizado correctamente.

----Fin

2.6.4 Desactivación de un evento

En esta sección se describe cómo deshabilitar un evento habilitado en la página **Events**.

Prerrequisitos

El evento que se va a deshabilitar debe estar en el estado **Enabled**.

Procedimiento



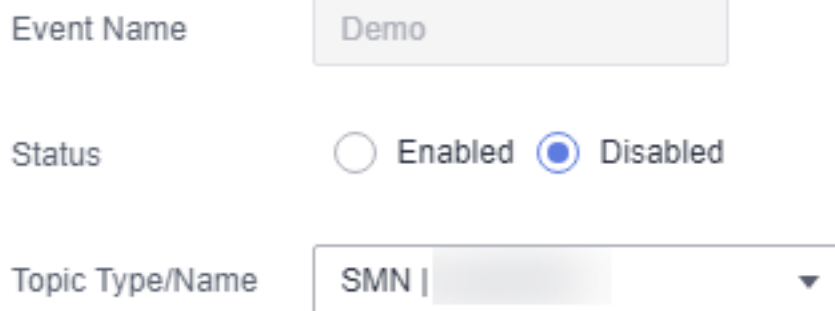
- Paso 1** Inicie sesión en la consola de gestión.
- Paso 2** Haga clic en  en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.
- Paso 3** Haga clic en  a la izquierda, elija **Security & Compliance > Data Encryption Workshop**, se mostrará la página de gestión de claves.
- Paso 4** En el panel de navegación de la izquierda, elija **Cloud Secret Management Service > Events**. Se muestra la página **Events**.
- Paso 5** Haga clic en **Edit** en la columna **Operation** del evento de destino. Se muestra la página **Edit Event**.
- Paso 6** Seleccione **Disabled** para **Status**.

Figura 2-22 Desactivar un evento

Edit Event



Event Name

Status Enabled Disabled

Topic Type/Name

- Paso 7** Haga clic en **OK**. Se muestra un mensaje en la esquina superior derecha de la página, indicando que el evento está deshabilitado correctamente.

---Fin

2.6.5 Eliminación de un evento

En esta sección se describe cómo eliminar un evento creado en la página **Events**. Antes de eliminar un evento, asegúrese de que el evento ya no se usa.

Restricciones

Las notificaciones de eventos solo se pueden eliminar después de que se hayan cancelado todos los secretos asociados. Si el secreto asociado no se cancela, la eliminación fallará.

Procedimiento



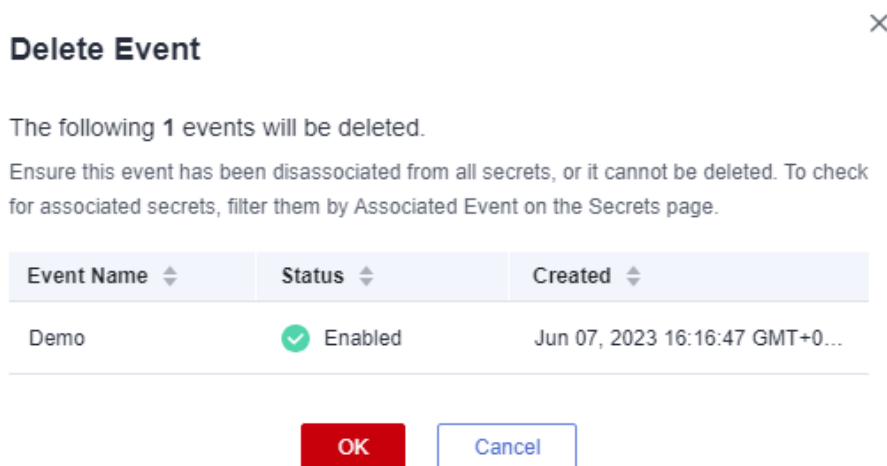
- Paso 1** [Inicie sesión en la consola de gestión.](#)
- Paso 2** Haga clic en  en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.
- Paso 3** Haga clic en  a la izquierda, elija **Security & Compliance > Data Encryption Workshop**, se mostrará la página de gestión de claves.
- Paso 4** En el panel de navegación de la izquierda, elija **Cloud Secret Management Service > Events**. Se muestra la página **Events**.
- Paso 5** Haga clic en **Delete** en la columna **Operation** del evento de destino. Aparece el cuadro de diálogo **Delete Event**.

Figura 2-23 Eliminación de un evento





- Paso 6** Haga clic en **OK**.

----Fin

2.7 Consulta de notificaciones

En esta sección se describe cómo ver las notificaciones de eventos.

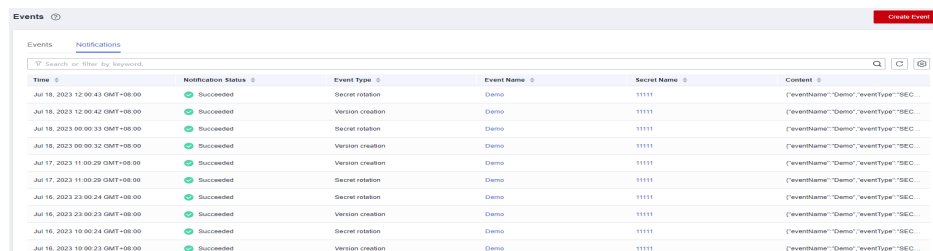
Procedimiento

- 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, elija **Security & Compliance > Data Encryption Workshop**, se mostrará la página de gestión de claves.

Paso 4 En el panel de navegación de la izquierda, elija **Cloud Secret Management Service > Events**. Se muestra la página **Events**.

Paso 5 Haga clic en la pestaña **Notifications**. Se muestra la página para ver las notificaciones, como se muestra en **Figura 2-24**.

Figura 2-24 Consulta de notificaciones



The screenshot shows the 'Notifications' tab in the Cloud Secret Management Service interface. It displays a table with columns for Time, Notification Status, Event Type, Event Name, Secret Name, and Content. The table lists several events, all with a 'Succeeded' status, involving 'Secret rotation' and 'Version creation' for a secret named 'Demo'.

Time	Notification Status	Event Type	Event Name	Secret Name	Content
Jul 18, 2023 12:00:43 GMT+08:00	Succeeded	Secret rotation	Demo	11111	["eventName":"Demo","eventType":"SEC...
Jul 18, 2023 12:00:42 GMT+08:00	Succeeded	Version creation	Demo	11111	["eventName":"Demo","eventType":"SEC...
Jul 18, 2023 00:00:33 GMT+08:00	Succeeded	Secret rotation	Demo	11111	["eventName":"Demo","eventType":"SEC...
Jul 18, 2023 00:00:32 GMT+08:00	Succeeded	Version creation	Demo	11111	["eventName":"Demo","eventType":"SEC...
Jul 17, 2023 11:00:29 GMT+08:00	Succeeded	Version creation	Demo	11111	["eventName":"Demo","eventType":"SEC...
Jul 17, 2023 11:00:29 GMT+08:00	Succeeded	Secret rotation	Demo	11111	["eventName":"Demo","eventType":"SEC...
Jul 16, 2023 23:00:24 GMT+08:00	Succeeded	Secret rotation	Demo	11111	["eventName":"Demo","eventType":"SEC...
Jul 16, 2023 23:00:23 GMT+08:00	Succeeded	Version creation	Demo	11111	["eventName":"Demo","eventType":"SEC...
Jul 16, 2023 10:00:24 GMT+08:00	Succeeded	Secret rotation	Demo	11111	["eventName":"Demo","eventType":"SEC...
Jul 16, 2023 10:00:23 GMT+08:00	Succeeded	Version creation	Demo	11111	["eventName":"Demo","eventType":"SEC...

Paso 6 En la página de pestaña **Notifications**, puede ver los cambios realizados en los secretos de los eventos asociados.

----Fin

3 Key Pair Service

3.1 Creación de un par de claves

Por motivos de seguridad del sistema, se recomienda utilizar el modo de autenticación de par de claves para autenticar al usuario que intenta iniciar sesión en un ECS.

Puede crear un par de claves y usarlo para la autenticación al iniciar sesión en su ECS.

NOTA

Si ya ha creado un par de claves, no es necesario volver a crear.

Puede crear un par de claves utilizando cualquiera de los métodos siguientes:

- Creación de un par de claves en la consola de gestión

La clave pública se guarda automáticamente en Huawei Cloud. La clave privada se puede descargar y guardar en su host local. También puede guardar sus claves privadas en Huawei Cloud y gestionarlas con KPS en función de sus necesidades. Huawei Cloud utiliza claves de encriptación proporcionadas por KMS para cifrar sus claves privadas para garantizar un almacenamiento y acceso seguros. Para obtener más información, véase [Creación de un par de claves mediante la consola de gestión](#).

NOTA

- El par de claves creado en la consola de gestión utiliza el algoritmo de encriptación y desencriptación **SSH-2 (RSA, 2048)**.
- Los pares de claves creados por un usuario de IAM en la consola de gestión solo pueden ser utilizados por el usuario. Si varios usuarios de IAM necesitan usar el mismo par de claves, puede crear un par de claves de cuenta.
- Creación de un par de claves con la herramienta PuTTYgen

Tanto la clave pública como la clave privada se pueden almacenar en el host local. Para obtener más información, véase [Creación de un par de claves con PuTTYgen](#).

NOTA


PuTTYgen es una herramienta para generar claves públicas y privadas. Puede obtener la herramienta de <https://www.putty.org/>.


Prerrequisitos

Cuando se crea un par de claves de cuenta por primera vez, es necesario obtener un usuario con el rol del sistema Administrador del Tenant.

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.

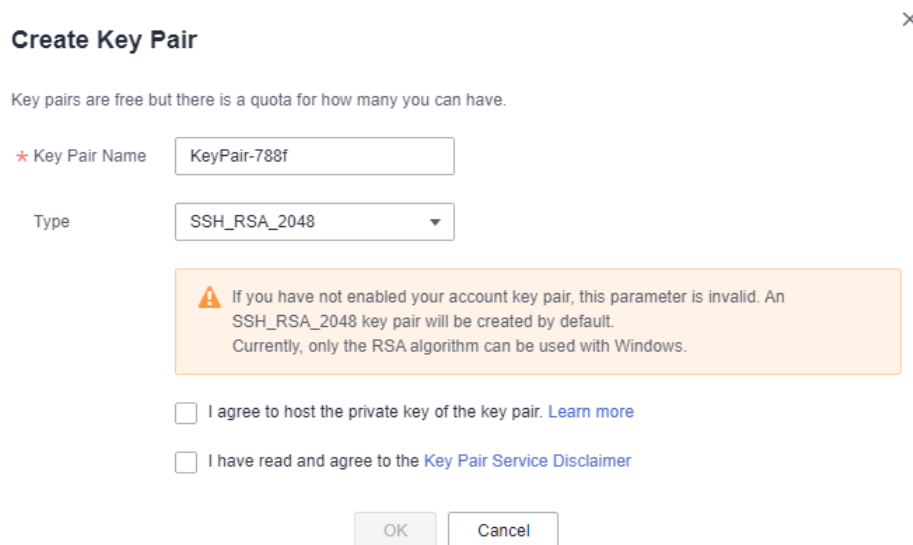
Paso 3 Haga clic en  a la izquierda, elija **Security & Compliance > Data Encryption Workshop**, se mostrará la página de gestión de claves.

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



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

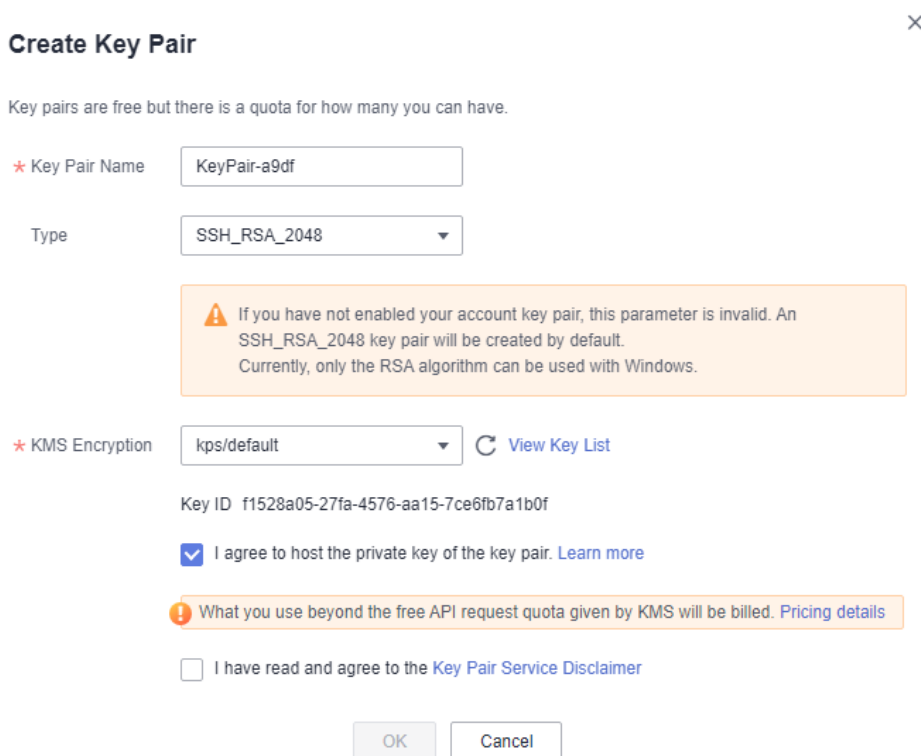
Actualmente, solo se puede utilizar el algoritmo RSA con Windows.

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**. Omita 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.

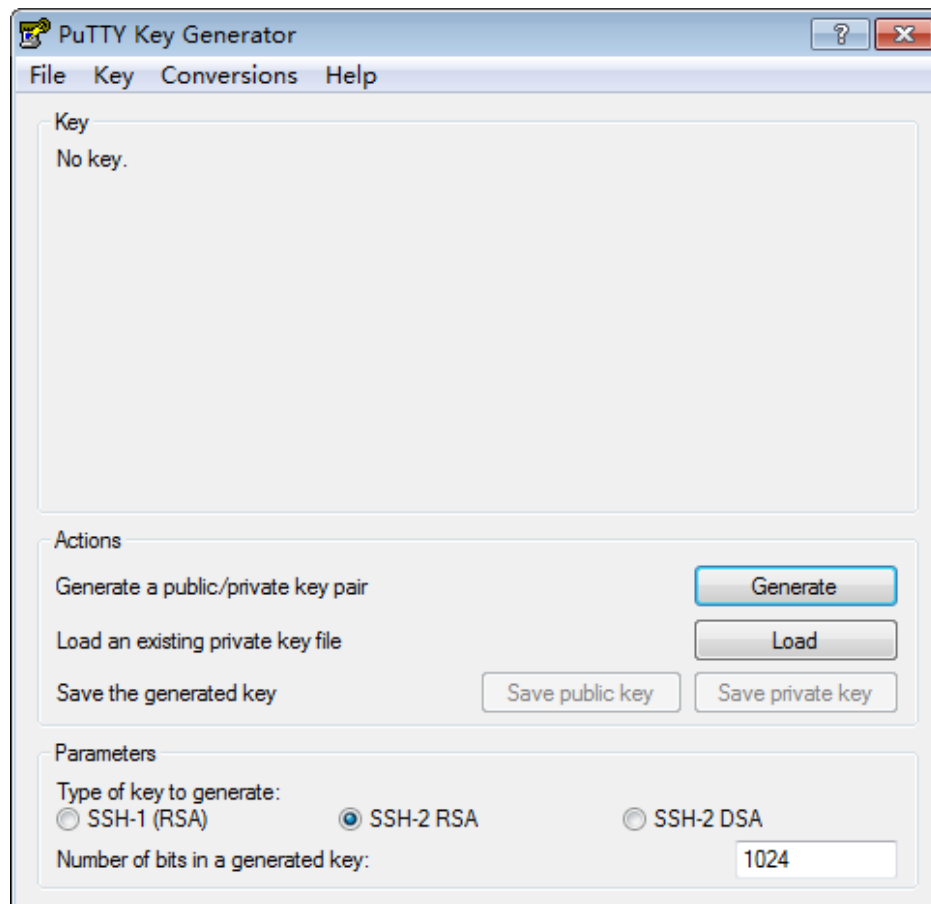
Después de crear el par de claves, puede verlo en la lista de pares de claves. La lista muestra información como el nombre del par de claves, la huella dactilar, la clave privada y la cantidad.

---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

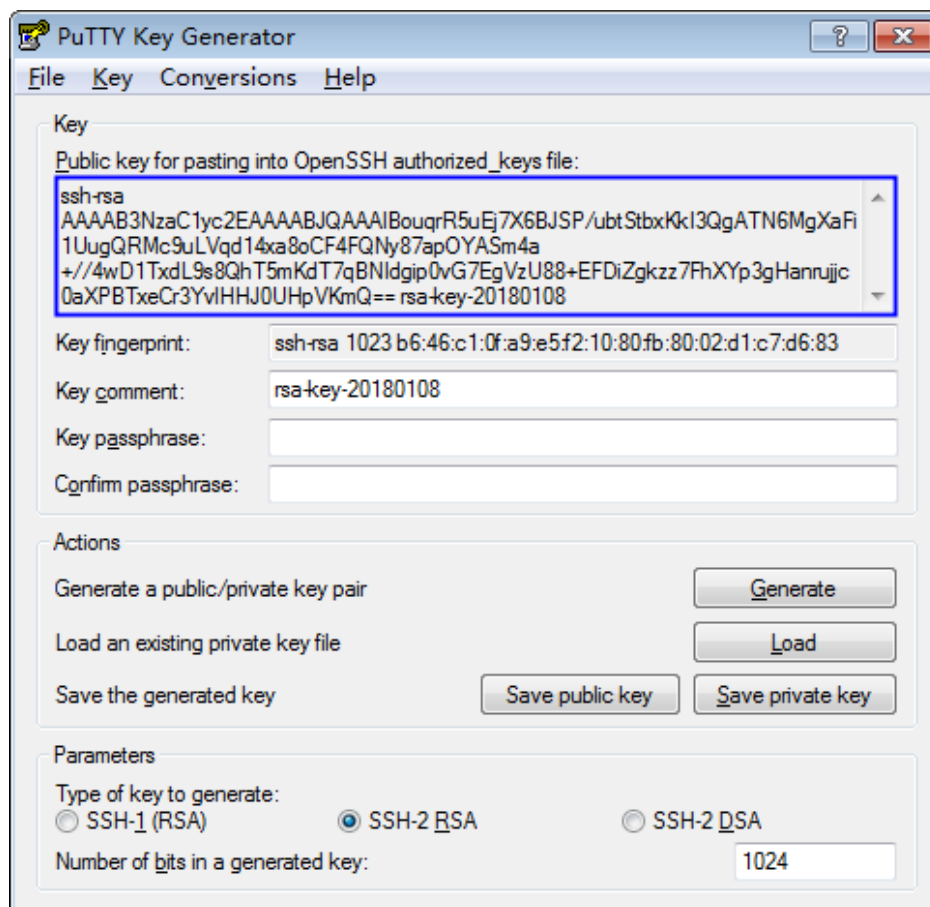
Parámetro	Descripción
Type of key to generate	Algoritmo de cifrado y descifrado de pares de claves para importar a la consola de gestión. Actualmente, solo se admite SSH-2 RSA .

Parámetro	Descripción
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 Importación de un par de claves

Si necesita usar su propio par de claves (por ejemplo, usando el par de claves creado por la herramienta PuTTYgen), puede importar la clave pública a la consola de gestión y utilizar su clave privada para iniciar sesión de forma remota en un ECS. También puede gestionar la clave privada en la consola de gestión de Huawei Cloud según sea necesario.

Si varios usuarios de IAM necesitan usar el mismo par de claves, utilice otra herramienta (como PuTTYgen) para crear un par de claves e importarlo para cada uno de los usuarios de IAM por separado.

Prerrequisitos


- Los archivos de clave pública y privada del par de claves a importar están listos.
- El par de claves importadas es un par de claves de cuenta. Si se ha creado un par de claves privadas con el mismo nombre, el sistema muestra un mensaje que indica que el nombre del par de claves ya existe al importar el par de claves de cuenta.
- Cada usuario de IAM no tiene un par de claves privadas con el mismo nombre.


Restricciones

- 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.
- El formato del archivo de clave privada que se puede importar es PEM.
Si el archivo está en formato .ppk, conviértelo en un archivo .pem. Para obtener más información, consulte [¿Cómo convierto el formato de un archivo de clave privada?](#)

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, 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 **Import Key Pair**.

Paso 6 En el cuadro de diálogo **Import Key Pair**, haga clic en **Select File** e importe un archivo de clave pública o copie y pegue claves públicas en el cuadro de texto **Public Key Content**, como se muestra en [Figura 3-5](#).

Figura 3-5 Importación de un par de claves

Import Key Pair ×

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

To import a public key, use either of the following methods:
1. Click Select File to import a public key file. You can change the key name if necessary.
2. Copy the content of a public key file to the Public Key Content field and enter a name in the Name field.
Notes: Only RSA keys are supported. The key file size must be 1024, 2048, or 4096 bits.

* Key Pair Name

Public Key No file is selected.

* Public Key Content

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

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

NOTA

- Puede personalizar el nombre de un par de claves importadas.
- Si el sistema muestra un mensaje que indica que el nombre ya existe, debe cambiar el nombre del par de claves porque el nombre ha sido creado por otro usuario de IAM.

Paso 7 Si desea que se gestione su clave privada, lea y confirme **I agree to host the private key of the key pair.**, como se muestra en el documento [Figura 3-6](#). Omita este paso si no necesita gestionar la clave privada.

Figura 3-6 Gestión de claves privadas

1. Haga clic en **Select File**, seleccione el archivo de clave privada **.pem** que desea importar. También puede copiar y pegar el contenido de clave privada en el cuadro de texto **Private Key Content**.
2. Seleccione una clave de encriptación en el cuadro de lista desplegable de **KMS encryption**.

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 maestra predeterminada **kps/default** para la encriptación del par de claves.
- Puede seleccionar una clave de encriptación existente o hacer clic en **View Key List** para crear una.

Paso 8 Lea el *Key Pair Service Disclaimer* y seleccione **I have read and agree to the Key Pair Service Disclaimer**.

Paso 9 Haga clic en **OK** para importar el par de claves.

----Fin

3.3 Actualización de un par de claves

Para permitir que todos los usuarios de su cuenta usen sus pares de claves, puede actualizar los pares de claves a pares de claves de cuenta.

Prerrequisitos


- Se ha creado o importado un par de claves.
- Los usuarios con el rol de sistema de 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.
- Se ha manejado el ticket de servicio para la actualización de clave.


Restricciones

- Los pares de claves que utilizan los mismos nombres que los pares de claves de cuenta existentes u los pares de claves privadas de otros usuarios no se pueden actualizar.
- 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.

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.

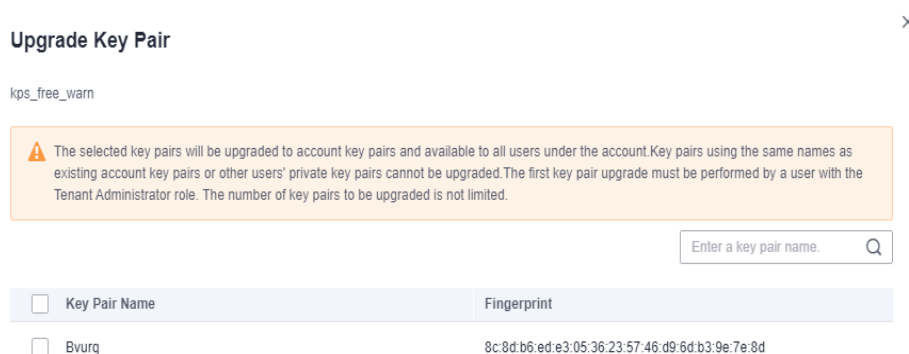
Paso 3 Haga clic en  a la izquierda, elija **Security & Compliance > Data Encryption Workshop**, se mostrará la página de gestión de claves.

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

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

Paso 6 En el cuadro de diálogo que se muestra, seleccione el par de teclas que desea actualizar y haga clic en **OK**, como se muestra en [Figura 3-7](#).

Figura 3-7 Actualización de un par de claves



 **NOTA**

Los pares de claves actualizados se muestran en la lista de pares de claves de cuenta.

----Fin

3.4 Gestión de pares de claves

3.4.1 Vinculación de un par de claves

Si establece el modo de inicio de sesión en **Password** al comprar un ECS que ejecuta Linux, puede vincular un par de claves al ECS en la consola KPS. KPS configurará el par de claves y, a continuación, el modo de inicio de sesión de ECS se cambiará a **Key Pair**. Una vez enlazado el par de claves, puede utilizar la clave privada para iniciar sesión en el ECS.

Esta sección describe cómo vincular un par de claves a un ECS en la consola KPS.

Prerrequisitos


- El ECS debe estar en el estado **Running** o **Shut down**.
- El ECS no se ha vinculado a un par de claves.
- El ECS cuyo par de claves debe restablecerse utiliza la imagen pública proporcionada por Huawei Cloud.
- Para enlazar a un par de claves, puede escribir la clave pública del usuario en el archivo **root/.ssh/authorized_keys** en el servidor. Asegúrese de que el archivo no se modifica antes de vincularlo al par de claves. De lo contrario, la vinculación no será posible.


Restricciones

- En la consola de gestión, los pares de claves no se pueden vincular a los ECS que ejecutan Windows.
- Los pares de claves no se pueden vincular a imágenes públicas que ejecuten CoreOS, OpenEuler o FreeBSD (Otros), Kylin V10 de 64 bits o UnionTech servidor 20 Euler del sistema operativo de 64 bits.

Vinculación de un par de claves

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 **ECS List** para ver los ECS, como se muestra en el documento [Figura 3-8](#).

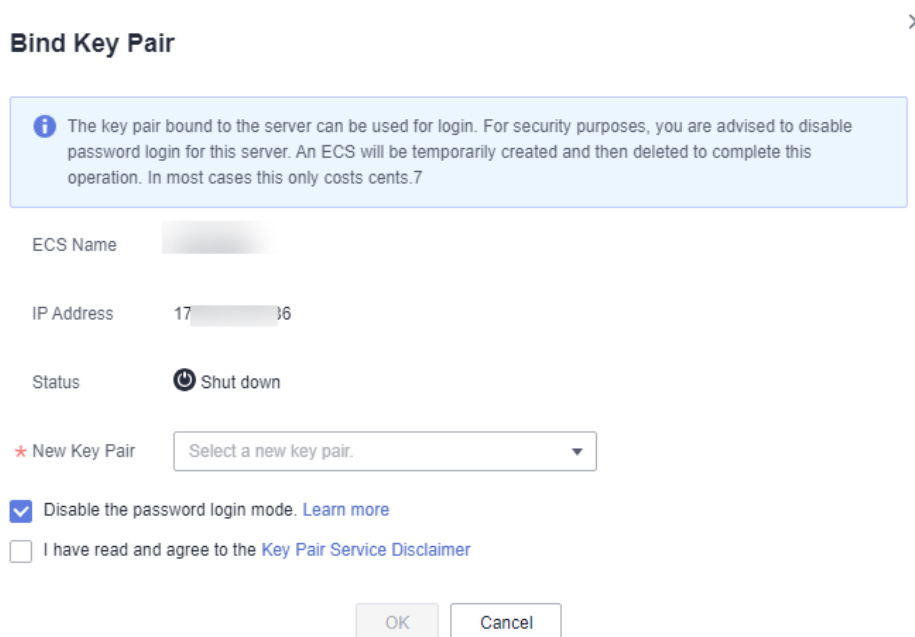
Figura 3-8 Vinculación



Paso 6 Haga clic en **Bind** en la fila de un ECS para abrir el cuadro de diálogo **Bind Key Pair**.

- Si el ECS está apagado, se mostrará un cuadro de diálogo, como se muestra en **Figura 3-9**.

Figura 3-9 Vinculación de un par de claves (1)



- Si el ECS se está ejecutando, debe proporcionar la contraseña raíz. Para más detalles, véase **Figura 3-10**.

Figura 3-10 Vinculación de un par de claves (2)

Bind Key Pair ×

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 c... 2

IP Address 1... 2

Status Running

* New Key Pair

* Root Password

* Port

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

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

NOTA

- Si tiene la contraseña raíz del ECS, puede ingresar directamente la contraseña para vincular el par de claves al ECS.
- Si no tiene la contraseña raíz del ECS, puede apagar el ECS y vincular el par de claves cuando el ECS está en el estado de apagado.

Paso 7 Seleccione un nuevo par de claves en el cuadro de lista desplegable de **New Key Pair**.

Paso 8 El número de puerto predeterminado es 22 y se puede modificar.

NOTA

Antes de utilizar el puerto definido por el usuario, asegúrese de que:

- El par de claves se puede conectar al ECS mediante el puerto. Para obtener más información acerca de cómo modificar la configuración del grupo de seguridad de un ECS, consulte [Configuración de las reglas del grupo de seguridad](#).
- Modifique el puerto predeterminado del ECS y asegúrese de que el puerto esté habilitado. Para obtener más información, consulte [Mejora de la seguridad para los inicios de sesión de SSH a los ECS de Linux](#).

Paso 9 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, consulte [¿Cómo activo el modo de inicio de sesión con contraseña para un ECS?](#)

Paso 10 Seleccione **I have read and agree to the Key Pair Service Disclaimer**.

Paso 11 Haga clic en **OK** para completar la operación.

- Si el ECS no se apaga, utilice la contraseña raíz para vincular el par de claves. Se tarda unos 30 segundos en completarse.
- Si el ECS se apaga, la operación de enlace puede tardar unos cinco minutos.

----Fin

3.4.2 Vinculación de pares de clave en lotes

Cuando ECS está en el estado **Running**, puede vincular pares de claves en lotes en la consola.

Esta sección describe cómo vincular pares de claves en lotes en la consola de KMS.

Escenario de aplicación

- Si varios ECS a vincular tienen la misma contraseña, puede ingresar la contraseña y seleccionar el par de claves con solo unos pocos clics.
- Si las contraseñas de los ECS que se van a vincular son diferentes, puede introducir sus contraseñas y seleccionar el mismo par de claves para vincular.

Prerrequisitos


- El ECS debe estar en el estado de **Running**.
- El ECS no se ha vinculado a un par de claves.


Restricciones

- En la consola de gestión, los pares de claves no se pueden vincular a los ECS que ejecutan Windows.
- Los pares de claves no se pueden vincular a imágenes públicas que ejecuten CoreOS, OpenEuler, FreeBSD (Other), Kylin V10 64-bit, o UnionTech OS Server 20 Euler 64-bit.
- Puede vincular pares de claves a un máximo de 10 ECS a la vez.

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, 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 **ECS List**. La página de lista de ECS se muestra, como se muestra en **Figura 3-11**.

Figura 3-11 Lista de ECS

ECS NameID	Status	Private IP Address	Elastic IP Address	Associated Key Pair	Operation
eci-c228020e-870a-4171-81a8-cc90114bc936	Running	172.16.255.104	100.93.13.190	--	Bind
oyy-dc05d553-9e43-4e6a-9e55-aa19811168d3	Running	172.19.16.232	--	--	Bind
oyy-9a6010c-844a-4966-8d63-59af009a3b6d	Running	172.16.159.166	--	--	Bind
imsg-b0400b0d-4228-42c7-bd73-0a99c0affc59	Running	192.168.3.47	100.93.2.122	--	Bind
eci-6662e722-8259-4256-8875-1c6cc481e0...	Shut down	172.27.225.97	100.93.3.159	--	Bind
imsg-6662e722-8259-4256-8875-1c6cc481e0...	Running	192.168.3.24	100.85.119.17	2	Replace Reset Unbind
eci-18a0247-495c-4592-8a1d-087586ac482c	Running	172.19.176.149	100.85.127.239	KeyPair-nq	Replace Reset Unbind

Paso 6 Seleccione los servidores que se van a enlazar en lotes y haga clic en **Bind** encima del cuadro de búsqueda, como se muestra en **Vinculación de pares de claves en lotes**. Para más detalles, consulte **Figura 3-12**.

Figura 3-12 Vinculación de pares de clave en lotes

ECS NameID	Status	Private IP Address	Elastic IP Address	Associated Key Pair	Operation
eci-c228020e-870a-4171-81a8-cc90114bc936	Running	172.16.255.104	100.93.13.190	--	Bind
oyy-dc05d553-9e43-4e6a-9e55-aa19811168d3	Running	172.19.16.232	--	--	Bind
oyy-9a6010c-844a-4966-8d63-59af009a3b6d	Running	172.16.159.166	--	--	Bind
imsg-b0400b0d-4228-42c7-bd73-0a99c0affc59	Running	192.168.3.47	100.93.2.122	--	Bind
eci-6662e722-8259-4256-8875-1c6cc481e0...	Shut down	172.27.225.97	100.93.3.159	--	Bind
imsg-6662e722-8259-4256-8875-1c6cc481e0...	Running	192.168.3.24	100.85.119.17	2	Replace Reset Unbind
eci-18a0247-495c-4592-8a1d-087586ac482c	Running	172.19.176.149	100.85.127.239	KeyPair-nq	Replace Reset Unbind

Paso 7 Haga clic en **Bind**. Aparece el cuadro de diálogo **Bind Key Pair to ECS**.

- Si las contraseñas de los ECS que se van a vincular son las mismas, puede seleccionar un par de claves con un solo clic e introducir la contraseña para vincular el par de claves. Para más detalles, consulte **Figura 3-13**.

Figura 3-13 Vinculación unificada

X

Bind Key Pair to ECS

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.

Operation Type: **Unified bind** | Separate bind

Bind multiple ECSs with the same root password to the same key pair.

* Key Pair: Select a new key pair. ▾

* Root Password:

* Port [?]: 22

ECS Name	IP Address	Status	Key Pair	Root Password	Port	Disable P...
ecs-8544	172.16.255.104	Running	Select a new key ... ▾	<input type="password"/>	22	<input checked="" type="checkbox"/>
cyy-testforbi...	172.19.16.232	Running	Select a new key ... ▾	<input type="password"/>	22	<input checked="" type="checkbox"/>

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

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

OK Cancel

- Si las contraseñas de los ECS que se van a vincular son diferentes, puede vincularlas por separado. Para más detalles, consulte [Figura 3-14](#).

Figura 3-14 Vinculación separada

X

Bind Key Pair to ECS

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.

Operation Type: Unified bind | **Separate bind**

Bind ECSs with different root passwords to the same key pair.

* Key Pair: KeyPair-4083 ▾

ECS Name	IP Address	Status	Key Pair	Root Password	Port	Disable P...
1f...	192.168.36	Running	KeyPair-4083 ▾	<input type="password"/>	22	<input checked="" type="checkbox"/>
...	192.168.36	Running	KeyPair-4083 ▾	<input type="password"/>	22	<input checked="" type="checkbox"/>

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

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

OK Cancel

NOTA

Si selecciona **Unified bind**, solo se puede utilizar el mismo par de claves para la vinculación.

Paso 8 El número de puerto predeterminado es 22 y se puede modificar.

 **NOTA**

Antes de utilizar el puerto definido por el usuario, asegúrese de que:

- El par de claves se puede conectar al ECS mediante el puerto. Para obtener más información acerca de cómo modificar la configuración del grupo de seguridad de un ECS, consulte [Configuración de las reglas del grupo de seguridad](#).
- Modifique el puerto predeterminado del ECS y asegúrese de que el puerto esté habilitado. Para obtener más información, consulte [Mejora de la seguridad para los inicios de sesión de SSH a los ECS de Linux](#).

Paso 9 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, consulte [¿Cómo activo el modo de inicio de sesión con contraseña para un ECS?](#)

Paso 10 Seleccione **I have read and agree to the Key Pair Service Disclaimer**.

Paso 11 Haga clic en **OK**. Los pares de claves están enlazados por lotes. La unión dura aproximadamente 3 a 5 minutos.


---Fin


3.4.3 Consulta de un par de claves

Esta sección describe cómo ver la información del par de claves, incluidos los nombres, las huellas dactilares, las claves privadas y las claves usadas en la página KPS de la consola DEW.

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, 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**.

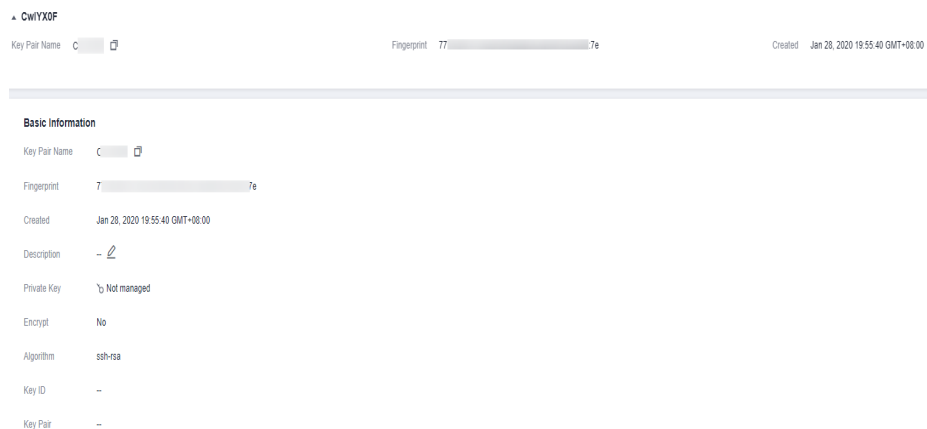
Paso 5 Haga clic en la pestaña **Private Key Pairs** y vea información sobre el par de claves en la lista de pares de claves.

 **NOTA**

La lista describe los nombres, las huellas dactilares, las claves privadas y los estados de los pares de claves.

Paso 6 Haga clic en el nombre del par de claves de destino. Se muestra la información detallada sobre el par de claves y la lista de los ECS que usan el par de claves.

Figura 3-15 Detalles del par de claves



NOTA

Cuando compre un ECS, elija el método de inicio de sesión para usar un par de claves. A continuación, el par de claves se vinculará al ECS después de comprar el ECS.

Enlaza un par de claves a los ECS. Para obtener más información sobre los parámetros, consulte [Tabla 3-3](#).

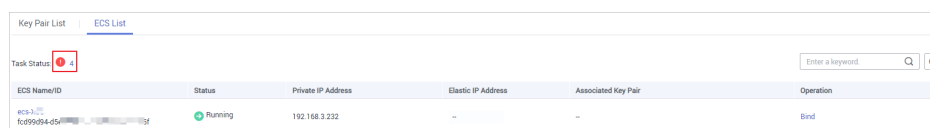
Tabla 3-3 Descripción del parámetro


Parámetro	Descripción
ECS Name/ID	Nombre e ID de un ECS
Status	Los estados de un ECS son los siguientes: <ul style="list-style-type: none"> ● Running ● Creating ● Faulty ● Shut down ● DELETE ● HARD_REBOOT ● MIGRATING ● REBOOT ● RESIZE ● REVERT_RESIZE ● SHELVED ● SHELVED_OFF ● LOADED ● UNKNOWN ● VERIFY_RESIZE

Parámetro	Descripción
Private IP address	Dirección IP privada
EIP	Dirección IP elástica
Bound key pair	Par de claves que se une a la ECS

Paso 7 Haga clic en **ECS List** para ver los ECS.


Figura 3-16 Lista de ECS



Paso 8 Haga clic en el número junto al icono de estado de la tarea  para ver las tareas fallidas, como se muestra en **Figura 3-17**.

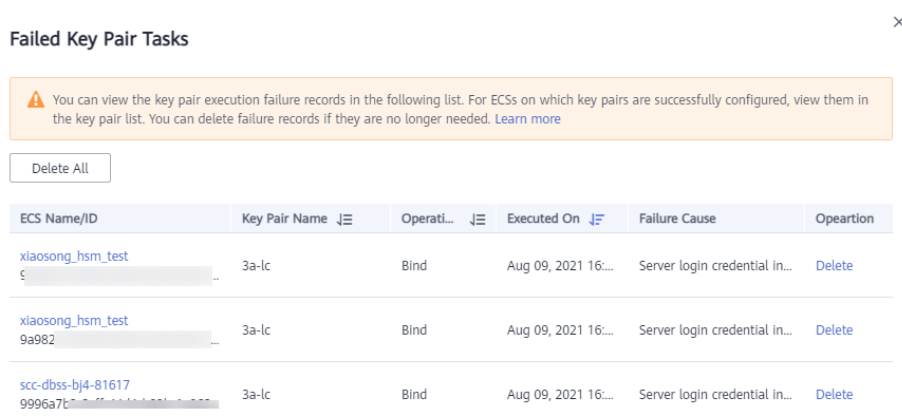
NOTA

Estado de reinicio o sustitución del par de claves:

 : Executing

 : Execution failed

Figura 3-17 Tareas fallidas del par de claves



NOTA

- Puede hacer clic en **Delete** en la fila donde se muestra el par de claves de destino para eliminar la tarea de par de claves fallida. También puede hacer clic en **Delete All** en la parte superior de la lista para eliminar todas las tareas fallidas.
- Haga clic en **Learn more** para ver documentos relacionados.

----Fin

3.4.4 Restablecimiento de un par de claves

Si se pierde su clave privada, puede utilizar un nuevo par de claves para reconfigurar el ECS a través de la consola de gestión. Después de restablecer el par de claves, debe usar la clave privada del nuevo par de claves para iniciar sesión en el ECS, y la clave privada original no se puede usar para iniciar sesión en el ECS.


Esta sección describe cómo restablecer un par de claves en la consola KPS.


Prerrequisitos

- El ECS cuyo par de claves debe restablecerse utiliza la imagen pública proporcionada por Huawei Cloud.
- Para restablecer el par de claves, puede reemplazar la clave pública del usuario modificando el archivo `/root/.ssh/authorized_keys` en el servidor. Asegúrese de que el archivo no se modifica antes de restablecer el par de claves. De lo contrario, el restablecimiento fallará.
- El ECS debe estar en el estado **Shut down**.

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, 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 la pestaña **ECS List**.

Paso 6 Haga clic en **Reset** en la fila de un ECS, como se muestra en [Figura 3-18](#).

Figura 3-18 Restablecimiento de un par de claves

Are you sure you want to reset the key pair of the following server?

The key pair bound to the ECS can be used for login. For security purposes, you are advised to disable password login for this ECS. An ECS will be temporarily created and then deleted to complete this operation. In most cases this generates less than ¥0.1 in incidental charges.

ECS Name: ir-...-219

IP Address: 192...4

Status: Shut down

Key Pair: 2

* New Key Pair: Select a new key pair.

* Port: 22

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

OK Cancel

Paso 7 Seleccione un nuevo par de claves en el cuadro de lista desplegable de **New Key Pair**.

Paso 8 El número de puerto predeterminado es 22 y se puede modificar.

NOTA

Antes de utilizar el puerto definido por el usuario, asegúrese de que:

- El par de claves se puede conectar al ECS mediante el puerto. Para obtener más información acerca de cómo modificar la configuración del grupo de seguridad de un ECS, consulte [Configuración de las reglas del grupo de seguridad](#).
- Modifique el puerto predeterminado del ECS y asegúrese de que el puerto esté habilitado. Para obtener más información, consulte [Mejora de la seguridad para los inicios de sesión de SSH a los ECS de Linux](#).

Paso 9 Seleccione **I have read and agree to the Key Pair Service Disclaimer**.

Paso 10 Haga clic en **OK**. El par de claves de ECS se restablecerá en unos 10 minutos.

----Fin

3.4.5 Sustitución de un par de claves

Si se filtra su clave privada, puede utilizar un nuevo par de claves para reemplazar la clave pública del ECS a través de la consola de gestión. Después de reemplazar el par de claves, debe usar la clave privada del nuevo par de claves para iniciar sesión en el ECS, y la clave privada original no se puede usar para iniciar sesión en el ECS.

Esta sección describe cómo reemplazar un par de claves en la consola KPS.


Prerrequisitos


- El ECS cuyo par de claves debe reemplazarse utiliza la imagen pública proporcionada por Huawei Cloud.

- Para reemplazar el par de claves, puede reemplazar la clave pública del usuario modificando el archivo `/root/.ssh/authorized_keys` en el servidor. Asegúrese de que el archivo no se modifica antes de reemplazar el par de claves. De lo contrario, se producirá un error al reemplazar la clave pública.
- El ECS debe estar en el estado de **Running**.

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, 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**.

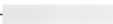




Paso 5 Haga clic en la pestaña **ECS List**.

Paso 6 Haga clic en **Replace** en la fila de un ECS. Establezca los parámetros en el cuadro de diálogo que se muestra. Para más detalles, consulte [Figura 3-19](#).

Figura 3-19 Sustitución de un par de claves

Are you sure you want to replace the key pair of the following server? ×

The system will use the new key pair for the server. After this operation is executed, the existing key pair cannot be used to log in to the server.

ECS Name	image-  19
IP Address	1  4
Status	 Running
Key Pair	2
* New Key Pair	<input type="text" value="Select a new key pair."/>
* Private Key in Use 	No file is selected. <input type="button" value="Select File"/>
	<input type="text" value="Paste the private key file content here."/>
* Port 	<input type="text" value="22"/>

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

Paso 7 Seleccione un nuevo par de claves en el cuadro de lista desplegable de **New Key Pair**.

Paso 8 Haga clic en **Select File** para cargar la clave privada (formato en .pem) del par de claves original o copie el contenido de la clave privada en el cuadro de texto.

NOTA

La clave privada que se va a cargar o copiar en el cuadro de texto debe estar en formato .pem. Si está en formato .ppk, conviértelo haciendo referencia a [¿Cómo convierto el formato de un archivo de clave privada?](#)

Paso 9 El número de puerto predeterminado es 22 y se puede modificar.

NOTA

Antes de utilizar el puerto definido por el usuario, asegúrese de que:

- El par de claves se puede conectar al ECS mediante el puerto. Para obtener más información acerca de cómo modificar la configuración del grupo de seguridad de un ECS, consulte [Configuración de las reglas del grupo de seguridad](#).
- Modifique el puerto predeterminado del ECS y asegúrese de que el puerto esté habilitado. Para obtener más información, consulte [Mejora de la seguridad para los inicios de sesión de SSH a los ECS de Linux](#).

Paso 10 Seleccione **I have read and agree to the Key Pair Service Disclaimer**.

Paso 11 Haga clic en **OK**. El par de claves será reemplazado del ECS en aproximadamente un minuto.

----Fin

3.4.6 Desvinculación de un par de claves

Cuando utiliza un par de claves para iniciar sesión en un ECS, si desea cambiar el modo de par de claves a contraseña, puede desvincular el par de claves en la consola de gestión. El KPS desvinculará el par de claves del ECS. Después de que el par de claves esté libre, puede usar la contraseña para iniciar sesión en el ECS.

Prerrequisitos


- El ECS debe estar en el estado **Running** o **Shut down**.
- El ECS se ha enlazado a un par de claves.
- El ECS que se va a desvincular de su par de claves utiliza la imagen pública proporcionada por Huawei Cloud.
- Para desvincular de un par de claves, puede eliminar la clave pública del usuario del archivo `/root/.ssh/authorized_keys` en el servidor. Asegúrese de que el archivo no se modifica antes de desvincular del par de claves. De lo contrario, la desvinculación fallará.


Restricciones

- Si no ha establecido la contraseña para iniciar sesión en el ECS u olvida la contraseña de inicio de sesión, puede restablecer la contraseña de inicio de sesión del ECS en la consola de ECS. Para obtener más información, consulte *Guía del usuario de Elastic Cloud Server*.
- Si ha habilitado el inicio de sesión de pares de claves para un ECS durante su creación, pero desvincula el par de claves utilizado para el inicio de sesión, para vincular el par de claves de nuevo, apague primero el ECS.
- Después de desvincular un ECS de su par de claves, restablezca la contraseña en la consola ECS de manera oportuna. Para obtener más información, consulte *Guía del usuario de Elastic Cloud Server*.

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, elija **Security & Compliance > Data Encryption Workshop**, se mostrará la página de gestión de claves.

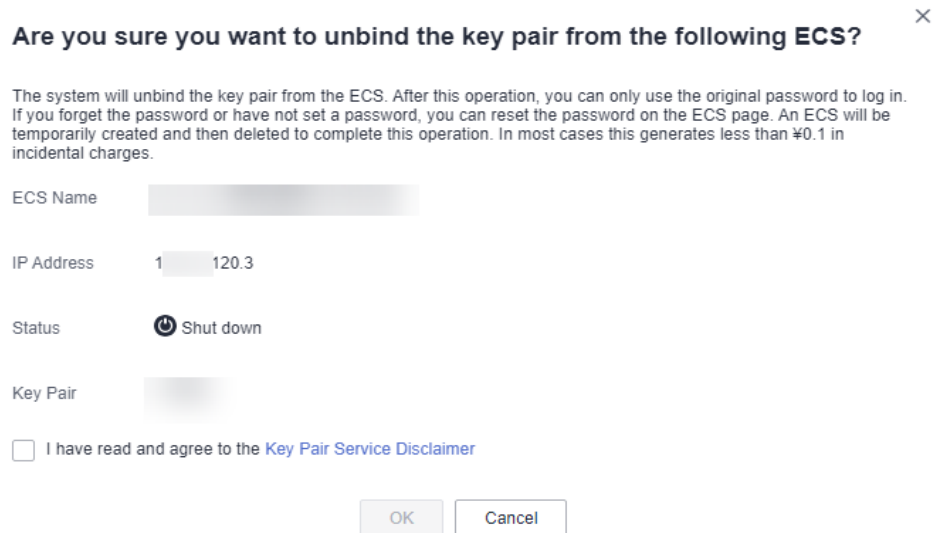
Paso 4 En el panel de navegación de la izquierda, haga clic en **Key Pair Service**.

Paso 5 Haga clic en la pestaña **ECS List**.

Paso 6 Haga clic en **Unbind** en la fila de un ECS.

- Si el ECS está apagado, se mostrará un cuadro de diálogo, como se muestra en [Figura 3-20](#).

Figura 3-20 Desvinculación de un par de claves (1)



- Si el ECS se está ejecutando, se mostrará un cuadro de diálogo.

Figura 3-21 Desvinculación de un par de claves (2)

Are you sure you want to unbind the key pair from the following ECS? ×

The system will unbind the key pair from the ECS. After this operation, you can only use the original password to log in. If you forget the password or have not set a password, you can reset the password on the ECS page.

ECS Name image-9

IP Address 4

Status → Running

Key Pair 2

* Private Key in Use ? No file is selected. Select File

Paste the private key file content here.

* Port ? 22

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

OK Cancel

Paso 7 Si desvincula el par de claves cuando el ECS está en el estado de ejecución, debe cargar la clave privada. Haga clic en **Select file** para cargar la clave privada (en el formato **.pem**) del par de claves existente o copie la clave privada en el cuadro de texto. Si el ECS está apagado, omita este paso.

NOTA

La clave privada que se va a cargar o copiar en el cuadro de texto debe estar en formato **.pem**. Si está en formato **.ppk**, conviértelo haciendo referencia a [¿Cómo convierto el formato de un archivo de clave privada?](#)

Paso 8 El número de puerto predeterminado es 22 y se puede modificar.

NOTA

Antes de utilizar el puerto definido por el usuario, asegúrese de que:

- El par de claves se puede conectar al ECS mediante el puerto. Para obtener más información acerca de cómo modificar la configuración del grupo de seguridad de un ECS, consulte [Configuración de las reglas del grupo de seguridad](#).
- Modifique el puerto predeterminado del ECS y asegúrese de que el puerto esté habilitado. Para obtener más información, consulte [Mejora de la seguridad para los inicios de sesión de SSH a los ECS de Linux](#).

Paso 9 Seleccione **I have read and agree to the Key Pair Service Disclaimer**.

Paso 10 Haga clic en **OK**. El par de claves se separará del ECS en aproximadamente un minuto.

NOTA

Después de desvincular un ECS de su par de claves, restablezca la contraseña en la consola ECS de manera oportuna. Para obtener más información, consulte *Guía del usuario de Elastic Cloud Server*.

----Fin

3.4.7 Eliminación de un par de clave

Puede eliminar un par de clave si ya no se usa.


Esta sección describe cómo eliminar un par de clave en la consola KPS


Restricciones

- No se puede recuperar una clave eliminada. Por lo tanto, realice esta operación con precaución.
- La clave privada importada para un par de claves se eliminará con ella.
- Si elimina la clave pública que se ha enlazado a un ECS en la consola y la clave privada se ha guardado localmente, puede utilizar la clave privada para iniciar sesión en el ECS. La operación de eliminación no afecta al inicio de sesión de ECS.

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, 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 En la fila que contiene el par de claves deseado, haga clic en **Delete**.

NOTA

Si ha actualizado el par de claves a un par de claves de cuenta, realice el siguiente paso en la lista de pares de claves de cuenta.

Paso 6 En el cuadro de diálogo **Delete Key Pair** que se muestra, escriba **DELETE** y haga clic en **OK**. Cuando **Key pair deleted successfully** se muestra en la esquina superior derecha, el par de claves se elimina.

----Fin

3.5 Gestión de claves privadas

3.5.1 Importación de una clave privada

Para facilitar la gestión de claves privadas locales, puede importar la clave privada a la consola de KPS para la gestión centralizada de sus claves privadas. Las claves privadas administradas se cifran mediante las claves proporcionadas por KMS, lo que garantiza la seguridad para el almacenamiento, la importación y la exportación de las claves privadas. Puede descargar las claves privadas desde la consola de gestión siempre que lo necesite. Para garantizar la seguridad de las claves privadas, mantenga las claves privadas descargadas correctamente.

Esta sección describe cómo importar un par de claves en la consola KPS.

Prerrequisitos


Se ha obtenido el archivo de clave privada que coincide con la clave pública.


Restricciones

- Solo la clave privada que coincida con una clave pública se puede importar para la clave pública.
- La clave privada que se va a cargar o copiar en el cuadro de texto debe estar en formato .pem. Si está en formato .ppk, conviértelo haciendo referencia a [¿Cómo convierto el formato de un archivo de clave privada?](#)
- Cuando habilita la función de encriptación para un par de claves, KMS crea automáticamente una clave predeterminada **kps/default** para el 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.

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, 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 **Import Private Key** en la fila donde se encuentra la clave pública de destino. Establezca parámetros en el cuadro de diálogo **Import Private Key**. Para más detalles, consulte [Figura 3-22](#).

Figura 3-22 Importación de una clave privada

Import Private Key [X]

Warning: Private keys are encrypted and hosted on the cloud but can be exported as needed. Your private keys will never be used for any purpose irrelevant to key pair management.

Note: Once the private key is imported successfully, you will be charged for the management service by hour. This function is offered for free now. [Learn more](#)

* Key Pair Name: KeyPair-2a11

Private Key: No file is selected. [Select File]

* Private Key Content: [Empty text area]

* KMS Encryption: kps/default [Refresh]

Key ID: [Redacted]

Warning: If KMS encryption is used, 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](#)

[OK] [Cancel]

Paso 6 Haga clic en **Select File**, seleccione un archivo de clave privada local **.pem**. También puede copiar y pegar el contenido de clave privada en el cuadro de texto **Private Key Content**.

NOTA

- Solo la clave privada que coincida con una clave pública se puede importar a la clave pública.

Paso 7 Seleccione una clave de encriptación en el cuadro de lista desplegable de **KMS encryption**.

NOTA

- Cuando habilita la función de encriptación para un par de claves, KMS crea automáticamente una clave predeterminada **kps/default** para el 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.

Paso 8 Seleccione **I have read and agree to the Key Pair Service Disclaimer**.

Paso 9 Haga clic en **OK** para completar la importación.

----Fin

3.5.2 Exportación de una clave privada

Si tiene las claves privadas gestionadas por la consola de gestión, puede descargar las claves privadas siempre que lo necesite. Para garantizar la seguridad de la clave privada, mantenga la clave privada descargada correctamente.

Prerrequisitos


La clave privada se ha administrado en la consola de gestión.


Restricciones

Una clave privada es cifrada y descifrada usando la misma clave de encriptación. Si se elimina la clave de encriptación, la clave privada no se exportará.

Procedimiento

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

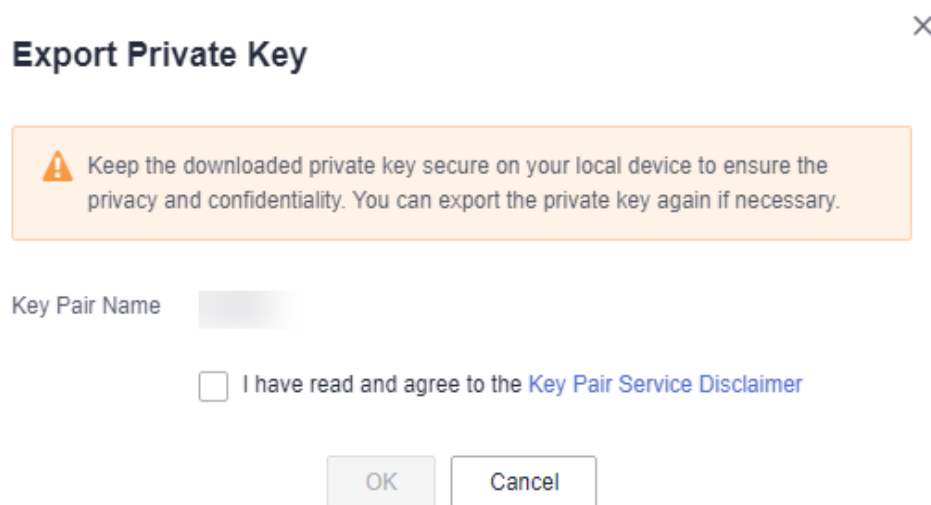
Paso 2 Haga clic en  en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

Paso 3 Haga clic en  a la izquierda, 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 **Export Private Key** en la fila donde reside el par de claves de destino. Se muestra el cuadro de diálogo **Export Private Key**, como se muestra en [Figura 3-23](#).

Figura 3-23 Exportación de una clave privada



Paso 6 Seleccione **I have read and agree to the Key Pair Service Disclaimer**.

Paso 7 Haga clic en **OK**. El navegador descarga automáticamente la clave privada.

AVISO

Al exportar una clave privada, debe utilizar la clave de encriptación que cifra la clave privada para descifrar la clave privada. Si la clave de encriptación se ha eliminado completamente, la exportación de la clave privada fallará.

----Fin

3.5.3 Borrar una clave privada

Si las claves privadas gestionadas por KPS ya no son necesarias, puede borrar las claves privadas gestionadas en la consola de KPS.

Prerrequisitos


La clave privada se ha administrado en la consola de gestión.


Restricciones

Después de borrar la clave privada, no puede obtener la clave privada de Huawei Cloud. Tenga cuidado cuando realice esta acción. Si necesita volver a administrar la clave privada, puede importarla a la consola de gestión.

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, 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 **Clear Private Key** en la fila donde se encuentra la clave pública de destino para borrar la clave privada.

NOTA

Si ha actualizado el par de claves a un par de claves de cuenta, realice los siguientes pasos en la lista de pares de claves de cuenta.

Paso 6 En el cuadro de diálogo **Clear Private Key** que se muestra, haga clic en **OK**.

NOTA

Después de borrar la clave privada, no puede obtener la clave privada de Huawei Cloud. Tenga cuidado cuando realice esta acción. Si necesita volver a administrar la clave privada, puede importarla a la consola de gestión.

----Fin

3.6 Uso de una clave privada para iniciar sesión en Linux ECS

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.

Restricciones

Los formatos de los archivos de clave privada de ECS deben cumplir con los siguientes requisitos.

Tabla 3-4 Formatos de archivo de clave privada

Sistema operativo local	Herramienta de inicio de sesión de Linux ECS	Formato de archivo de clave privada
Windows OS	Xshell	.pem
	PuTTY	.ppk
Linux OS	-	.pem or .ppk

Si su archivo de clave privada no está en el formato requerido, conviértelo haciendo referencia a [¿Cómo convierto el formato de un archivo de clave privada?](#)

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.

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**.

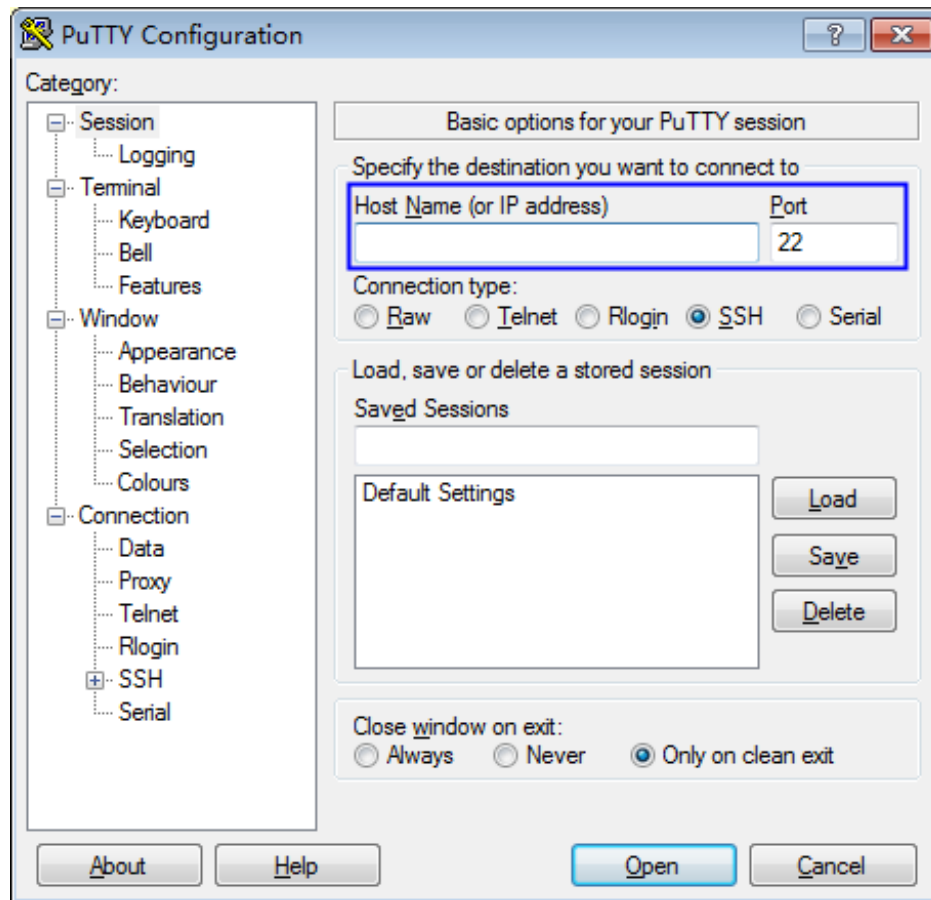
NOTA

- 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 3-24 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

3.7 Uso de una clave privada para obtener la contraseña de inicio de sesión de Windows ECS

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

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

Prerrequisitos

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


Restricciones


- 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 restaurar. 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 *Referencia de API de Elastic Cloud Server*.
- El archivo de clave privada de ECS debe estar en formato in .pem.

Si el archivo está en formato .ppk, conviértelo en un archivo .pem. Para obtener más información, consulte [¿Cómo convierto el formato de un archivo de clave privada?](#)

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  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**

4 HSM dedicado

4.1 Guía de operación

Restricciones

- Las instancias HSM dedicadas deben usarse junto con VPC. Después de crear una instancia HSM dedicada, debe configurar su VPC, grupo de seguridad y NIC en la consola de gestión antes de usarla.
- Por motivos de seguridad, las instancias HSM dedicadas no proporcionan servicios para la red pública. Para gestionar las instancias, implemente su herramienta de gestión en su VPC.

Guía de operación

Para usar HSM dedicado en la nube, puede crear instancias HSM dedicadas a través de la consola de gestión. Después de crear una instancia HSM dedicada, recibirá el UKey enviado por HSM dedicado. Necesita usar el UKey para inicializar y controlar la instancia. Puede utilizar la herramienta de gestión para autorizar a las aplicaciones de servicio el permiso para acceder a instancias de HSM dedicadas. [Figura 4-1](#) ilustra el flujo de operación.

Figura 4-1 Guía de operación

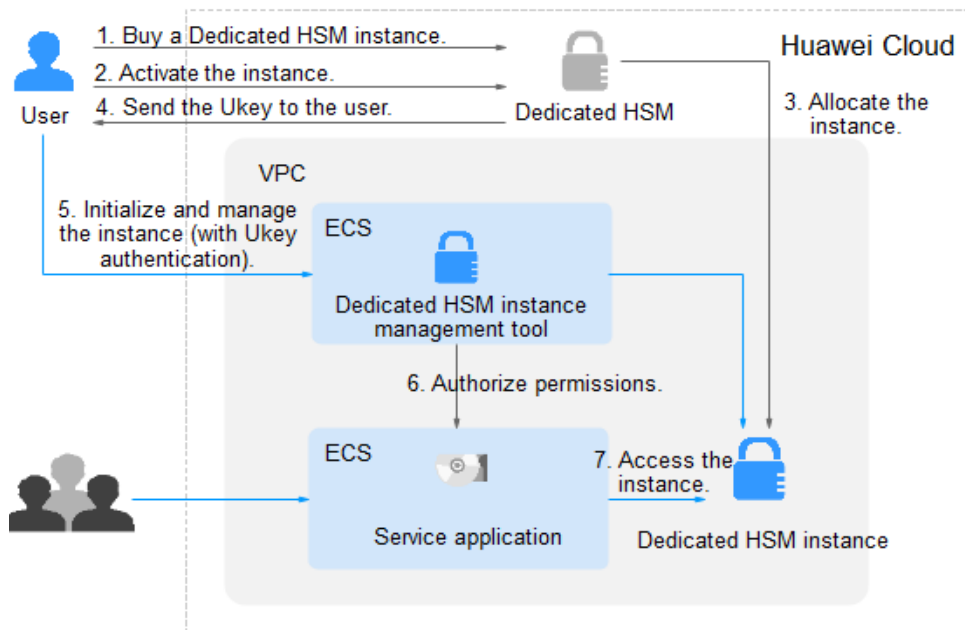


Tabla 4-1 describe la guía de operación.

Tabla 4-1 Descripciones de la guía de operación

No.	Procedimiento	Descripción	Gestionado por
1	Crear una instancia de HSM dedicada.	Cree una instancia en la consola de gestión de HSM dedicada. El equipo de seguridad de Huawei Cloud evaluará sus escenarios de uso para asegurarse de que la instancia cumple con sus requisitos de servicio. A continuación, puede pagar por la instancia solicitada.	Usuario
2	Activar una instancia de HSM dedicada.	Después de comprar una instancia, debe configurar la instancia en la consola de gestión. Debe seleccionar la VPC a la que pertenece la instancia y el tipo de función de la instancia. Para obtener más información, véase Activación de una instancia de HSM dedicado .	Usuario
3	Asignar una instancia HSM dedicada.	Un experto en seguridad se pondrá en contacto con usted a través de la información de contacto que proporcionó y determinará si la instancia solicitada cumple con sus requisitos de servicio. La instancia se asignará después de que el experto revise y confirme su pedido.	Experto dedicado o en seguridad HSM

No.	Procedimiento	Descripción	Gestionado por
4	Obtener el UKey, documentos de inicialización y software.	<ul style="list-style-type: none"> ● Un experto en seguridad envía el Ukey a la dirección de correo electrónico que proporcionó. Un UKey es el único identificador de un usuario HSM dedicado. Guárdelo correctamente. ● Un experto en seguridad le proporcionará el software y la guía para inicializar instancias HSM dedicadas. Si tiene alguna pregunta, póngase en contacto con el experto. <p>NOTA Puede enviar un Ticket de servicio para proporcionar la dirección del destinatario de UKey y ponerse en contacto con expertos en seguridad para obtener orientación.</p>	Experto dedicado en seguridad HSM
5	Inicializar y gestionar instancias (involucrado la autenticación UKey).	<ol style="list-style-type: none"> 1. Instale la herramienta para gestionar instancias de HSM dedicadas en el nodo de gestión de instancias. 2. Utilice UKey y la herramienta de gestión para inicializar la instancia HSM dedicada y registre un administrador para gestionar la instancia HSM dedicada y la clave. <p>Para obtener más información, véase Inicialización de una instancia HSM dedicada.</p>	Usuario
6	Instalar el agente de seguridad y la concesión de permisos de acceso.	<p>Instale e inicialice el agente de seguridad en los nodos de aplicaciones de servicio.</p> <p>Para obtener más información, véase Instalación del agente de seguridad y concesión de permisos de acceso.</p>	Usuario
7	Acceder a la instancia.	Las aplicaciones de servicio acceden a las instancias de HSM dedicadas a través de API o SDK.	Usuario

4.2 Compra de una instancia de HSM dedicado

4.2.1 Creación de una instancia de HSM dedicado

Al crear una instancia de HSM dedicado, debe especificar la región y completar la información de contacto.

La tarifa para una instancia de HSM dedicado en edición platino consta de las dos partes siguientes:

- Tarifa de instalación inicial, que se cobra al crear una instancia de HSM dedicado .
- Cuota anual/mensual, cobrada cuando [Activación de una instancia de HSM dedicado](#).

Prerrequisitos


You have obtained the login account (with the **Ticket Administrator** and **KMS Administrator** permissions) and password for logging in to the management console.


Restricciones

- Al comprar una instancia de HSM dedicada, debe enviar un ticket de servicio para establecer la información del destinatario de UKey. Solo las cuentas con el permiso **Ticket Administrator** pueden enviar tickets de servicio.
- Después de crear una instancia, se enviará un UKey a la dirección que figura en su información de contacto. A continuación, puede utilizar UKey para inicializar y autorizar a sus aplicaciones de servicio para acceder a la instancia.
Necesita activar la instancia antes de usarla.

Procedimiento

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

Paso 2 Click  in the upper left corner of the management console and select a region or project.

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

Paso 4 In the navigation pane, choose **Dedicated HSM**.

Paso 5 Click **Create Dedicated HSM** in the upper right corner of the page.

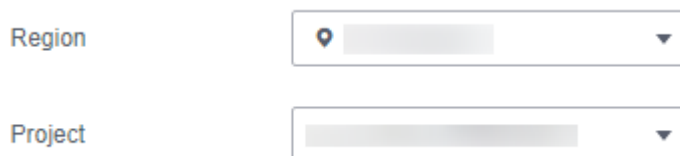
Paso 6 **Billing Mode** can only be set to **Yearly/Monthly**.

Figura 4-2 Billing Mode



Paso 7 Select a region and project.

Figura 4-3 Selecting a region



 **NOTA**

- Select the current region and the default project.
- Only the default project is supported. User-defined projects cannot be created.

Paso 8 Seleccione la edición de servicio para la instancia. Vea **Figura 4-4** para más detalles.. **Tabla 4-2** enumera los parámetros relacionados.

Figura 4-4 Edición platino (fuera de China continental)

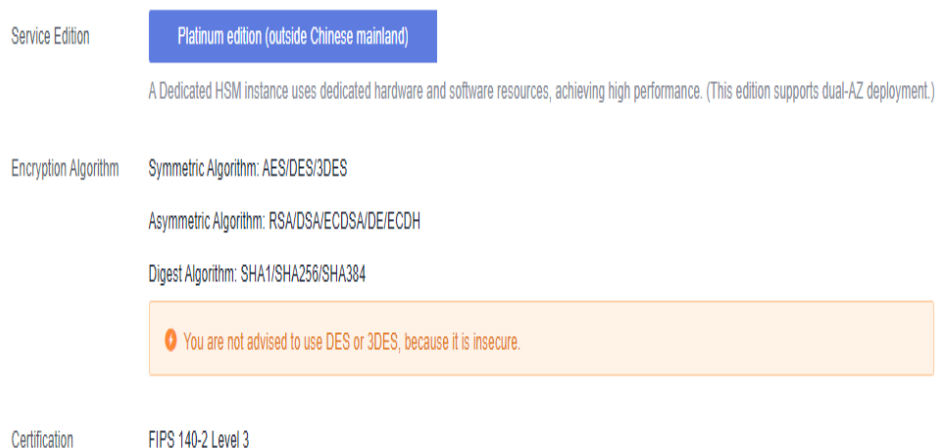


Tabla 4-2 Parámetros de edición

Parámetro	Descripción
Service Edition	Edición platino (fuera de China continental)
Encryption Algorithm	Algoritmo soportado por la instancia de HSM. <ul style="list-style-type: none"> ● Algoritmo simétrico: AES ● Algoritmo asimétrico: RSA, DSA, ECDSA, DE y ECDH ● Algoritmo de resumen: SHA1, SHA256, SHA384
Certification	Certificado FIPS 140-2 nivel 3

Paso 9 Seleccione **Service Tickets > Create Service Ticket**. Nuestros expertos en Huawei Cloud se pondrán en contacto con usted y le proporcionarán un plan de compra personalizado y su presupuesto.

- En la lista desplegable **Case Severity**, seleccione **General guidance**.
- En el cuadro de texto **Problem Description**, escriba **Dedicated HSM Contact Information**.
- **Contact Information**: Ingrese el número de teléfono y la dirección de correo electrónico para recibir la información de progreso del ticket de servicio.

AVISO

Asegúrese de que la información de contacto proporcionada en el cuadro de texto **Confidential Information** es válida para que nuestros expertos en seguridad puedan ponerse en contacto con usted de manera oportuna.

Figura 4-5 Creación de un ticket de servicio

Create Service Ticket

1 Select Service/Product — 2 Select Issue Category — 3 Submit Service Ticket

My Issue: DEW - General Consulting

* Region

* Case Severity

* Problem Description 26/1,200

Upload Attachments

Contact Options

Contact Information

I have read and agree to the [Ticket Service Protocol](#) and [Privacy Statement](#).

Paso 10 Haga clic en **Submit**. El ticket de servicio se muestra en la página **My Service Tickets**.

📖 NOTA

Una vez creado correctamente el ticket de servicio, puede hacer clic en **View Details** en la columna **Operation** para ver los detalles. Puede recordarle al equipo de soporte un ticket de servicio, dejar sus mensajes, cancelar un ticket de servicio o cerrar un ticket de servicio según los estados de los tickets de servicio.

----Fin

4.2.2 Activación de una instancia de HSM dedicado

Necesita activar una instancia de HSM dedicado antes de usarla. El paquete anual o mensual se cargará durante la activación.

Esta sección describe cómo activar una instancia HSM dedicado a través de la consola de gestión.

Prerrequisitos


El estado de la instancia HSM dedicada es **To be activated**.


Restricciones

- El nombre de instancia solo puede contener letras, dígitos, guiones bajos (_), y guiones (-).
- Se crean dos nodos como el grupo de recursos en segundo plano para una instancia de HSM dedicado. Para garantizar una alta disponibilidad de los nodos, se asigna una dirección IP flotante a la instancia.
- Si la instancia no se crea, puede hacer clic en **Delete** en la fila donde se encuentra la instancia para eliminarla. A continuación, solicite un reembolso mediante la presentación de un ticket de servicio.
- Después de crear correctamente una instancia de HSM dedicada, no se puede cambiar a otro tipo. Para utilizar una instancia de HSM dedicada de otro tipo, debe comprar otra.

Procedimiento

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

Paso 2 Click  in the upper left corner of the management console and select a region or project.

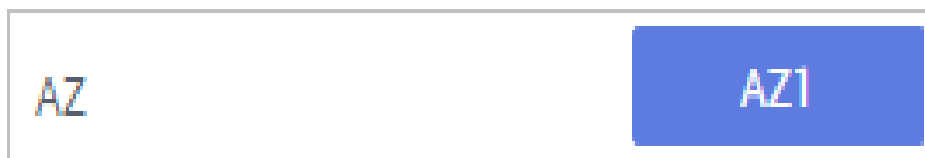
Paso 3 Haga clic en  a la izquierda, elija **Security & Compliance > Data Encryption Workshop**, se mostrará la página de gestión de claves.

Paso 4 In the navigation pane, choose **Dedicated HSM**.

Paso 5 Haga clic en **Activate** en la fila donde se encuentra la instancia de destino.

Paso 6 Seleccione una AZ.

Figura 4-6 Selección de una AZ



Paso 7 Introduzca la información de activación, como se muestra en [Figura 4-7](#). [Tabla 4-3](#) describe los parámetros.

Figura 4-7 Configuración de una instancia de HSM dedicado




Instance Name	<input type="text" value="DedicatedHSM-3f9b-0002"/>
HSM Type	<input type="text" value="Finance"/> <small>Provides key management and cryptographic operation services, including IC card issuing, transaction verification, data encryption, digital signatures, and dynamic password authentication.</small>
VPC 	<input type="text" value="vpc-eb5f"/> <small>You can select an existing VPC or apply for one.</small>
NIC 	<input type="text"/>
Security Group 	<input type="text" value="WorkspaceManagerSecuri..."/>

Tabla 4-3 Parámetros de activación

Parámetro	Descripción	Valor de ejemplo
Instance Name	Nombre de una instancia de HSM dedicado NOTA El nombre de instancia solo puede contener letras, dígitos, guiones bajos (_), y guiones (-).	DedicatedHSM-3c98-0002
Enterprise Project	Proyecto empresarial al que debe vincularse el HSM dedicado	default
HSM Type	Los tipos de HSM disponibles incluyen Finance , Server , y Signature server . <ul style="list-style-type: none"> ● Finance: Proporciona gestión de claves y servicios informáticos de encriptación, incluidas emisión de tarjetas IC, verificación de transacciones, encriptación de datos, firmas digitales y autenticación dinámica de contraseñas. ● Server: Proporciona servicios de gestión de claves seguros y completos y operaciones criptográficas simultáneas de alto rendimiento, como firmas de datos, verificación de firmas y encriptación/descriptación de datos. ● Signature server: Garantiza la integridad, confidencialidad, anti-repudio y trazabilidad post-evento de los datos del usuario mediante el uso de firmas digitales, sobres digitales y compendios digitales. 	Finance
VPC	Puede seleccionar una nube privada virtual (VPC) existente o hacer clic en Apply for VPC para crear una. Para obtener más información acerca de VPC, consulte la <i>Guía del usuario de Virtual Private Cloud</i> .	vpc-test-dhsm
NIC	Todas las subredes disponibles se muestran en la página. El sistema asigna automáticamente tres direcciones IP a la instancia. NOTA Se crean dos nodos como el grupo de recursos en segundo plano para una instancia de HSM dedicado. Para garantizar una alta disponibilidad de los nodos, se asigna una dirección IP flotante a la instancia. Para obtener más información acerca de las subredes, consulte la <i>Guía del usuario de Virtual Private Cloud</i> .	subnet-test-dhsm (192.168.0.0/24)

Parámetro	Descripción	Valor de ejemplo
Security Group	<p>El grupo de seguridad configurado para la instancia se muestra en la página. Una vez que se selecciona un grupo de seguridad para una instancia, la instancia está protegida por las reglas de acceso del grupo de seguridad.</p> <p>Para obtener más información acerca de los grupos de seguridad, consulte la <i>Guía del usuario de Virtual Private Cloud</i>.</p>	WorkspaceUserSecurityGroup

Paso 8 Si ha adquirido una instancia HSM dedicada en la edición estándar:

Haga clic en **Create Now** para volver a la lista de instancias de HSM dedicado. Puede ver información sobre la instancia activada.

Si el estado de la instancia de HSM dedicada es **Creating**, la instancia se activa correctamente.

Paso 9 Si ha adquirido una instancia de HSM dedicado en edición platino:

1. Establezca la duración requerida.

La duración requerida varía de un mes a un año.

 **NOTA**

La opción **Auto-renew** permite al sistema renovar el servicio por el período adquirido cuando el servicio está a punto de caducar.

2. Confirme la configuración y haga clic en **Next**.

Para cualquier duda sobre los precios, haga clic en **Pricing details**.

3. En la página **Order Details**, confirme los detalles del pedido, lea y seleccione **I have read and agree to the Privacy Policy Statement**.

4. Haga clic en **Pay Now** para pagar el paquete anual o mensual.

5. En la página **Pay**, seleccione un método de pago para pagar su pedido.

Después del pago exitoso, puede ver la información sobre la instancia de HSM en la página de lista de instancias de HSM.

Si el **Status** de la instancia es **Creating**, la instancia se ha activado y se le está asignando. Estará disponible en 5 a 10 minutos.

Creating: El sistema le está asignando una instancia. Este proceso suele durar de 5 a 10 minutos.

Después de la asignación, el estado de la instancia puede cambiar a uno de los siguientes:

- **Creation failed**: Una instancia no se puede crear debido a recursos insuficientes o errores de red.

 **NOTA**

Si la instancia no se crea, puede hacer clic en **Delete** en la fila donde se encuentra la instancia para eliminarla. A continuación, solicite un reembolso mediante la presentación de un ticket de servicio.

- **Running**: Se le ha asignado una instancia correctamente y se está ejecutando correctamente.

 **NOTA**

Después de crear correctamente una instancia de HSM dedicado, no se puede cambiar a otro tipo ni se puede reembolsar. Para utilizar una instancia de HSM dedicado de otro tipo, debe comprar otra.

----Fin

4.3 Consulta de instancias de HSM dedicado

Esta sección describe cómo ver la información de la instancia de HSM dedicada, incluidos el nombre/ID, el estado, la versión del servicio, el proveedor del dispositivo, el modelo del dispositivo, la dirección IP y la hora de creación.

Procedimiento

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

Paso 2 Haga clic en . Elija **Security & Compliance > Data Encryption Workshop**. Se mostrará la página **Key Management Service**.

Paso 3 En el panel de navegación, elija **Dedicated HSM**.

Paso 4 En la lista, puede ver la información sobre las instancias de HSM.

[Tabla 4-4](#) describe los parámetros de la lista de instancias de HSM.

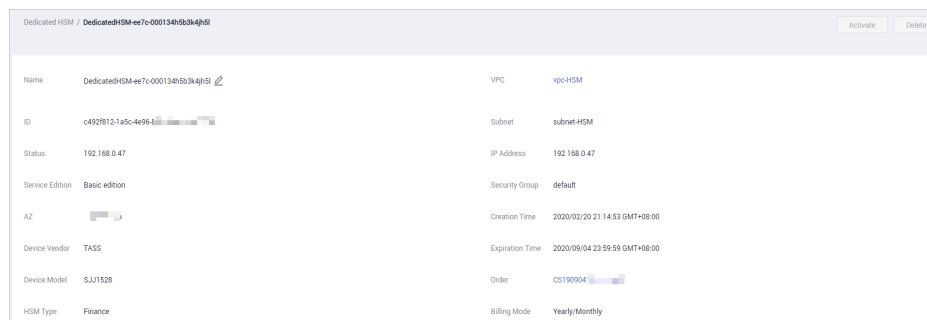
Tabla 4-4 Parámetros de instancia HSM dedicados

Parámetro	Descripción
Name/ID	Nombre e ID de una instancia HSM dedicada

Parámetro	Descripción
Status	<p>Estado de una instancia HSM dedicada:</p> <ul style="list-style-type: none"> ● Installing Después de pagar la tarifa de instalación inicial, se instalará la instancia comprada. El estado de la instancia de HSM dedicada será Installing. ● To be activated El estado de una instancia que ha sido instalada pero no activada es To be activated. ● Creating Después de activar una instancia, el sistema le asignará la instancia según su configuración. La instancia se encuentra en el estado de Creating durante este proceso. ● Creation failed Debido a recursos insuficientes o fallos de red, es posible que no se cree una instancia. En este caso, la instancia estará en el estado de Creation failed. ● Running Después de configurar y asignar una instancia, estará en el estado de Running. ● Frozen Si una instancia no se renueva al expirar, su estado cambia a Frozen.
Service Edition	<p>Edición platino (fuera de China continental)</p> <ul style="list-style-type: none"> ● Edición Platinum (fuera de China continental): Puede utilizar exclusivamente el subastidor HSM, la fuente de alimentación, el ancho de banda de red y los recursos API del HSM. <p>Edición Platinum: Puede utilizar exclusivamente el subrack HSM, la fuente de alimentación, el ancho de banda de la red y los recursos API del HSM.</p>
AZ	Zona de disponibilidad de un dispositivo
Expiration Time	Tiempo de expiración de la instancia de HSM adquirida.

Paso 5 Puede hacer clic en el nombre de una instancia para ver detalles sobre la instancia, como se muestra en [Figura 4-8](#).

Figura 4-8 Detalles acerca de instancias de HSM dedicadas



Para obtener más información, consulte [Tabla 4-5](#).

Tabla 4-5 Descripción del parámetro

Parámetro	Descripción
Name	Nombre de una instancia de HSM dedicado
ID	ID de una instancia
Status	<p>Estado de una instancia HSM dedicada:</p> <ul style="list-style-type: none"> ● Installing Después de pagar la tarifa de instalación inicial, se instalará la instancia comprada. El estado de la instancia de HSM dedicada será Installing. ● To be activated El estado de una instancia que ha sido instalada pero no activada es To be activated. ● Creating Después de activar una instancia, el sistema le asignará la instancia según su configuración. La instancia se encuentra en el estado de Creating durante este proceso. ● Creation failed Debido a recursos insuficientes o fallos de red, es posible que no se cree una instancia. En este caso, la instancia estará en el estado de Creation failed. ● Running Después de configurar y asignar una instancia, estará en el estado de Running. ● Frozen Si una instancia no se renueva al expirar, su estado cambia a Frozen.
Service Edition	Edición Platinum: Puede utilizar exclusivamente el subrack HSM, la fuente de alimentación, el ancho de banda de la red y los recursos API del HSM.
Tipo de HSM	Tipos de HSM de una instancia, incluidos Finance , Server y Signature verification server .

Parámetro	Descripción
VPC	VPC a la que pertenece la instancia Para obtener más información acerca de VPC, consulte <i>Guía del usuario de Virtual Private Cloud</i> .
Subnet	Subred donde se encuentra la instancia. Para obtener más información acerca de las subredes, consulte <i>Guía del usuario de Virtual Private Cloud</i> .
IP Address	Dirección IP flotante de la instancia HSM dedicada
Security Group (SG)	Grupo de seguridad al que pertenece la instancia Para obtener más información acerca de los grupos de seguridad, consulte <i>Guía del usuario de Virtual Private Cloud</i> .
Creation Time	Hora de compra de la instancia
Expiration Time	Hora en que expira la instancia
Order	ID de pedido de la instancia. Puede hacer clic en el número de pedido para consultar los detalles del pedido.
Billing Mode	Paquete prepago anual/mensual

---Fin

4.4 Gestión de etiquetas

4.4.1 Adición de una etiqueta

Puede utilizar etiquetas para identificar instancias de HSM dedicado. Se pueden agregar etiquetas a instancias de HSM dedicado para facilitar la clasificación y consulta de instancias.

Procedimiento



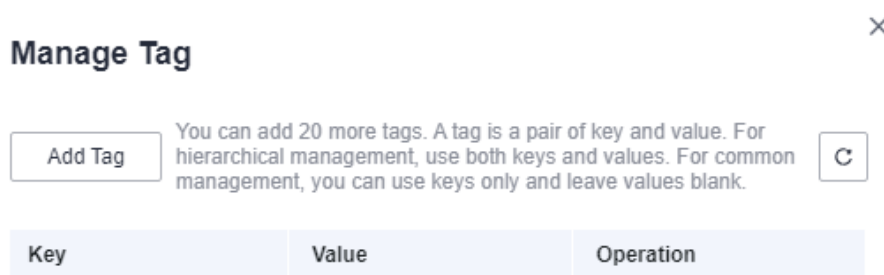
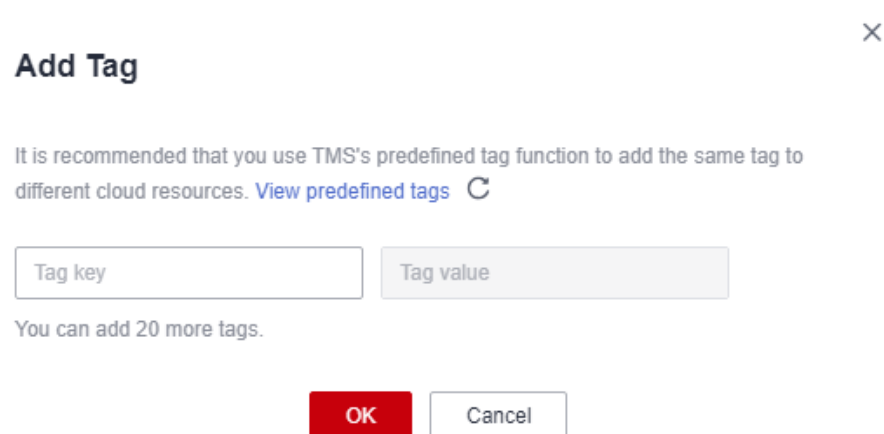
- Paso 1** Haga clic en  en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.
- Paso 2** Haga clic en . Elija **Security & Compliance > Data Encryption Workshop**.
- Paso 3** En el panel de navegación, elija **Dedicated HSM**.
- Paso 4** En la columna **Operation** de una instancia, haga clic en **Manage Tag**. Se muestra la página **Manage Tag**, como se muestra en [Figura 4-9](#).

Figura 4-9 Gestionar etiqueta



Paso 5 Haga clic en **Add Tag**. En el cuadro de diálogo que se muestra, escriba la clave de etiqueta y el valor de etiqueta. Para obtener más información sobre los parámetros, consulte [Tabla 4-6](#).

Figura 4-10 Adición de una etiqueta



NOTA

- Si desea utilizar la misma etiqueta para identificar varios recursos en la nube, puede crear etiquetas predefinidas en el TMS. De esta manera, se puede seleccionar la misma etiqueta para todos los servicios. Para obtener más información acerca de las etiquetas predefinidas, consulte la *Guía de usuario de Tag Management Service*.
- Para eliminar una etiqueta, haga clic en **Delete** junto a ella.

Tabla 4-6 Parámetros de etiqueta

Parámetro	Descripción	Observaciones
Tag key	<p>Nombre de la etiqueta.</p> <p>Las claves de etiqueta de un secreto no pueden tener valores duplicados. Se puede usar una clave de etiqueta para múltiples secretos.</p> <p>Un secreto puede tener hasta 20 etiquetas.</p>	<ul style="list-style-type: none"> ● Obligatorio. ● La clave de etiqueta debe ser única para la misma clave personalizada. ● Límite de 128 caracteres. ● El valor no puede comenzar ni finalizar con un espacio. ● No se puede iniciar con <code>_sys_</code>. ● Se permiten los siguientes tipos de caracteres: <ul style="list-style-type: none"> – Chino – Inglés – Números – Espacio – Caracteres especiales: <code>./=+-@</code>
Tag value	Valor de la etiqueta	<ul style="list-style-type: none"> ● Opcional ● Límite de 255 caracteres. ● Se permiten los siguientes tipos de caracteres: <ul style="list-style-type: none"> – Chino – Inglés – Números – Espacio – Caracteres especiales: <code>./=+-@</code>

Paso 6 Haga clic en **OK**.

----**Fin**

4.4.2 Búsqueda de una instancia de HSM dedicado por etiqueta

Esta sección describe cómo buscar instancias de HSM por etiqueta en el proyecto actual en la página **Instances (New)**.

Prerrequisitos

Se han agregado etiquetas.

Procedimiento



- Paso 1** Haga clic en  en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.
- Paso 2** Haga clic en . Elija **Security & Compliance > Data Encryption Workshop**.
- Paso 3** En el panel de navegación, elija **Dedicated HSM**.
- Paso 4** Haga clic en el cuadro de búsqueda y seleccione una etiqueta como atributo de filtro para buscar instancias HSM dedicadas, como se muestra en el documento [Figura 4-11](#).

Figura 4-11 Búsqueda de una instancia de HSM dedicado



Name/ID	Status	Service Edition	AZ	IP Address	Expiration Time	Enterprise Project	Operation
1c p4	Creating	--	AZ 3	--	9 hours 16 minutes until expi...	default	Manage Tag

----Fin

4.4.3 Modificación de un valor de etiqueta

En esta sección se describe cómo modificar los valores de etiqueta en la página HSM dedicado.

Procedimiento



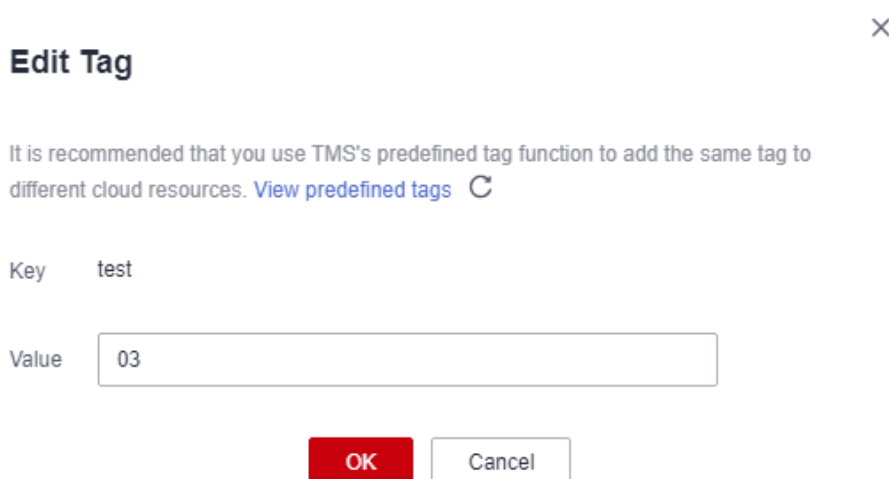
- Paso 1** Haga clic en  en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.
- Paso 2** Haga clic en . Elija **Security & Compliance > Data Encryption Workshop**.
- Paso 3** En el panel de navegación, elija **Dedicated HSM**.
- Paso 4** Haga clic en **Manage Tag** en la fila donde se encuentra la instancia de destino. Aparece el cuadro de diálogo **Manage Tag**.
- Paso 5** Haga clic en **Edit**. Aparece el cuadro de diálogo **Edit Tag**. Después de cambiar el valor de la etiqueta, haga clic en **OK**.

Figura 4-12 Edición de una etiqueta



---Fin

4.4.4 Eliminación de una etiqueta

Esta sección describe cómo eliminar etiquetas en la página HSM dedicado.

Procedimiento



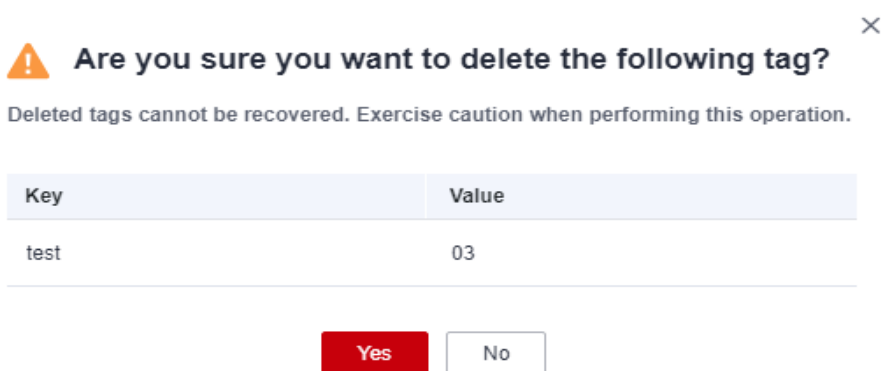
- Paso 1** Haga clic en  en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.
- Paso 2** Haga clic en . Elija **Security & Compliance > Data Encryption Workshop**.
- Paso 3** En el panel de navegación, elija **Dedicated HSM**.
- Paso 4** Haga clic en **Manage Tag** en la fila donde se encuentra la instancia de destino. Aparece el cuadro de diálogo **Manage Tag**.
- Paso 5** En la columna **Operation** de una etiqueta, haga clic en **Delete**.

Figura 4-13 Eliminación de una etiqueta



Paso 6 En el cuadro de diálogo **Delete Tag**, haga clic en **Yes**.

---Fin

4.5 Uso de instancias de HSM dedicado

Después de completar su pago, espere a que enviemos el Ukey utilizado para inicializar la instancia HSM dedicada a su dirección de correo electrónico. Un experto en servicios de HSM dedicado también se pondrá en contacto con usted y le enviará documentos y software relacionados, incluida la herramienta utilizada para administrar instancias de HSM dedicadas, y el agente de seguridad y el SDK utilizados para las llamadas de servicio.

Prerrequisitos

Después de configurar una instancia HSM dedicada, debe inicializar la instancia, instalar el agente de seguridad y conceder permisos de acceso. Se requiere la siguiente información.

Tabla 4-7 Información requerida

Concepto	Descripción	Dónde obtenerlos
Ukey	Almacena la información de gestión de permisos acerca de la instancia.	Una vez que se haya pagado el pedido y se haya configurado la instancia HSM dedicada, el Ukey se enviará a la dirección de correo electrónico del destinatario que haya proporcionado.
Herramienta de gestión de instancias HSM dedicada	Funciona con UKey para gestionar instancias de forma remota.	Un experto en servicio también se pondrá en contacto con usted y le enviará los documentos y el software relacionados.
Documentos dedicados de instancia de HSM	<i>Manual del usuario de la instancia HSM dedicada y Guía de instalación de la instancia HSM dedicada</i>	
Software de agente de seguridad	Establece una conexión segura con la instancia.	
SDK	Proporciona API para HSM dedicado. Puede utilizar el SDK para establecer conexiones seguras con instancias.	
Nodo dedicado de gestión de instancias de HSM (por ejemplo, un ECS)	Ejecute la herramienta de gestión de instancias dedicadas de HSM, que se encuentra en la misma VPC donde reside la instancia dedicada de HSM, y asigne direcciones IP elásticas para conexiones remotas.	

Concepto	Descripción	Dónde obtenerlos
Nodos de aplicación de servicio (por ejemplo, ECS)	Ejecute el software del agente de seguridad y las aplicaciones de servicio de los usuarios, que deben estar en la VPC donde se despliega la instancia de HSM dedicada.	


Inicialización de una instancia HSM dedicada

NOTA

Actualmente, no puede iniciar sesión en instancias de HSM dedicadas a través de SSH. Debe utilizar la herramienta de gestión de instancias dedicadas de HSM para gestionar las instancias.

Supongamos que desea utilizar un ECS de Windows como nodo de gestión de instancias dedicadas de HSM. Realice los siguientes pasos para inicializar la instancia HSM dedicada:

Paso 1 Adquiera un ECS de Windows como nodo de gestión de instancias de HSM dedicadas.

1. Inicie sesión en la consola de gestión.
2. Haga clic en . Elija **Computing > Elastic Cloud Server**.
3. Haga clic en **Buy ECS**.
 - Establezca **Region** y **AZ** en las mismas que las de la instancia de HSM dedicada que compró.
 - Establezca **Image** en una imagen pública de Windows.
 - Establezca la **VPC** en la VPC a la que pertenece la instancia HSM dedicada.
 - Configure **EIP**. Le permite configurar localmente instancias de HSM convenientemente.

NOTA

Después de inicializar la instancia HSM dedicada, puede desvincular de la dirección IP elástica. Las operaciones de vinculación y desvinculación se pueden realizar siempre que sea necesario.

- Establezca otros parámetros en función de los requisitos del sitio.

Paso 2 Inicialice la instancia HSM dedicada utilizando la herramienta de gestión recibida y los documentos relacionados.

Paso 3 Una vez completada la inicialización, puede utilizar la herramienta de gestión para generar, destruir, realizar copias de respaldo y restaurar claves.

NOTA

Si tiene alguna pregunta durante la inicialización y la gestión, consulte al experto en servicio dedicado de HSM.

Para obtener más información, consulte los documentos sobre la instancia HSM dedicada: *Manual del usuario de la instancia HSM dedicada* y *Guía de instalación de la instancia HSM dedicada*.

----Fin

Instalación del agente de seguridad y concesión de permisos de acceso

Debe instalar el agente de seguridad en un nodo de aplicación de servicio para establecer un canal seguro a la instancia HSM dedicada.

- Paso 1** Descargue el certificado para acceder a la instancia HSM dedicada desde la herramienta de gestión.
- Paso 2** Instale el agente de seguridad en el nodo de aplicación de servicio.
- Paso 3** Importe el certificado al agente de seguridad. Otorgue a la aplicación de servicio el permiso para acceder a la instancia HSM dedicada.
- Paso 4** La aplicación de servicio puede acceder a la instancia de HSM dedicada a través de SDK o las API.

NOTA

Puede configurar varias instancias de HSM dedicadas en el agente de seguridad para balancear las cargas.

----**Fin**

5 Gestión de etiquetas

5.1 Descripción

Escenario

Las etiquetas son el identificador de DEW. Agregar etiquetas le permite reconocer y gestionar fácilmente sus recursos de encriptación de datos.

Las etiquetas se pueden agregar durante o después de la creación de recursos.

Reglas de nomenclatura de etiquetas

- Cada etiqueta consiste en un par de clave-valor.
- Puede agregar como máximo 20 etiquetas a un recurso DEW.
- Para cada recurso, una clave de etiqueta debe ser única y solo puede tener un valor de etiqueta.
- Una etiqueta consiste en una clave de etiqueta y un valor de etiqueta. Las reglas de nombres se enumeran en [Tabla 5-1](#).

Tabla 5-1 Parámetros de etiqueta

Parámetro	Reglas	Ejemplo
Tag key	<ul style="list-style-type: none"> ● Este parámetro es obligatorio. ● La clave de etiqueta debe ser única para la misma clave personalizada. ● El valor puede contener un máximo de 128 caracteres. ● El valor no puede comenzar ni finalizar con un espacio. ● El valor no puede comenzar por <code>_sys_</code>. ● Se permiten los siguientes tipos de caracteres: <ul style="list-style-type: none"> – Chino – Inglés – Dígitos – Espacio – Caracteres especiales: <code>./=+</code> 	cost
Tag value	<ul style="list-style-type: none"> ● Este parámetro se puede dejar vacío. ● El valor puede contener un máximo de 255 caracteres. ● Se permiten los siguientes tipos de caracteres: <ul style="list-style-type: none"> – Chino – Inglés – Dígitos – Espacio – Caracteres especiales: <code>./=+-@</code> 	100

5.2 Creating a Tag Policy

Introduction

Tag policies are a type of policy that can help you standardize tags across resources in your organization's accounts. A tag policy is only applied to tagged resources and tags that are defined in that policy.

For example, a tag policy can specify that a tag attached to a resource must use the case treatment and tag values defined in the tag policy. If the case and value of the tag do not comply with the tag policy, the resource will be marked as non-compliant.

You can use tag policies as detective or preventive guardrails:

1. **Detective guardrails:** If a resource tag violates the tag policy, the resource will appear as noncompliant in the compliance result.
2. **Preventive guardrails:** If enforcement is enabled for a tag policy, non-compliant tagging operations will be prevented from being performed on specified resource types.

Constraints


Only organization administrators can create a tag policy.

NOTA

Before you create a tag policy and add it to the organization unit and account, a tag policy must be enabled by the administrator account. For details, see [Enabling or Disabling the Tag Policy Type](#).

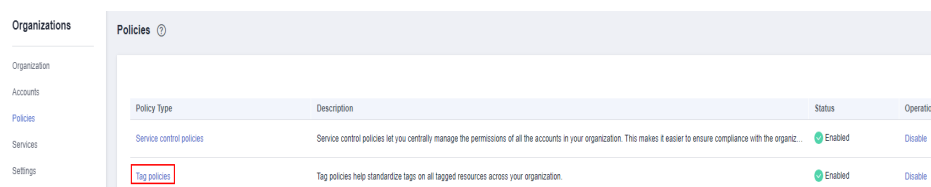
Procedure

Paso 1 Log in to Huawei Cloud as an organization administrator or an administrator account.

Paso 2 Click  on the left, choose **Management & Governance > Organizations**. The organization management page is displayed.

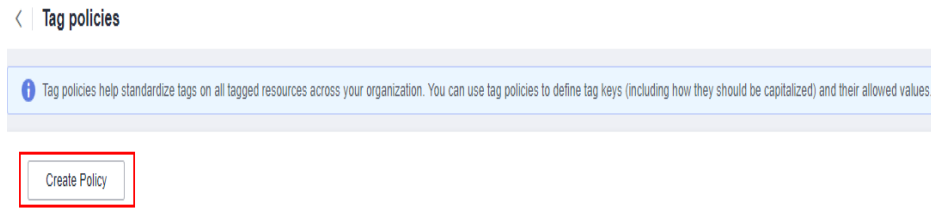
Paso 3 Click **Policies** on the left to go to the policy management page and click **Tag policies**.

Figura 5-1 Accessing the **Tag policies** page



Paso 4 Click **Create Policy**.

Figura 5-2 Creating a policy



Paso 5 Enter a policy name. Ensure that you are entering a unique policy name, different from any existing name.

Paso 6 Set a policy according to **Tag Policy Syntax**. The system automatically verifies the syntax. If the syntax is incorrect, modify it as prompted.

Figura 5-3 Setting a policy tag

Policy Syntax

```
Visual Editor  JSON
1  {
2    "tags": {
3      "abc": {
4        "tag_key": {
5          "@@assign": "abc"
6        },
7        "tag_value": {
8          "@@assign": [
9            "xxx*"
10         ]
11       },
12       "enforced_for": {
13         "@@assign": [
14           "DHSM:hsm",
15           "KMS:cmk"
16         ]
17       }
18     }
19   }
20 }
```

Current location: JSON Ln5,Col25 Policy size: 132/10000

Paso 7 (Optional) Add one or more tags to the policy. Enter a tag key and a tag value, and click **Add**.

Paso 8 Click **Save** in the lower right corner. If the tag policy is created successfully, it will be added to the list.

📖 NOTA

To update or delete a tag policy, see [Updating or Deleting a Tag Policy](#).

To attach or detach a tag policy, see [Attaching or Detaching a Tag Policy](#).

----Fin

5.3 Creating a Tag


This section describes how to add tags for existing keys, secrets, and Dedicated HSM instances.

Constraints

Tags cannot be added to default keys.

Key Management

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.

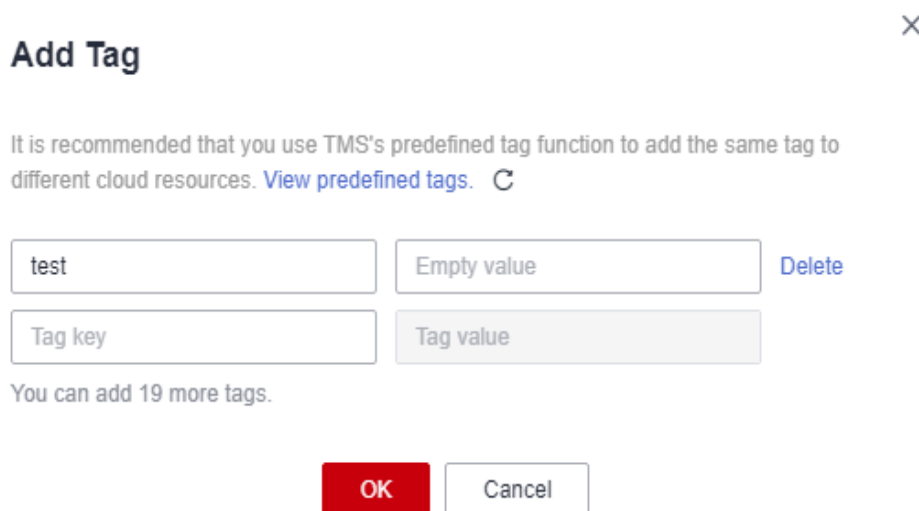
Paso 3 Haga clic en . Elija **Security & Compliance > Data Encryption Workshop.**

Paso 4 Click the alias of the desired custom key to view its details.

Paso 5 Click **Tags** to go to the tag management page.

Paso 6 Click **Add Tag**. On the displayed dialog box, set **Tag key** and **Tag value**.

Figura 5-4 Adding a tag



Add Tag ×

It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. [View predefined tags.](#) Ⓞ

test	Empty value	Delete
Tag key	Tag value	

You can add 19 more tags.

OK Cancel

NOTA

To delete a tag, click **Delete** next to it.


- If you want to use the same tag to identify multiple cloud resources, you can create predefined tags in the TMS. In this way, the same tag can be selected for all services. For more information about predefined tags, see the *Tag Management Service User Guide*.
- To delete a tag, click **Delete** next to it.


Paso 7 Click **OK** to complete.

----Fin

CSMS

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.

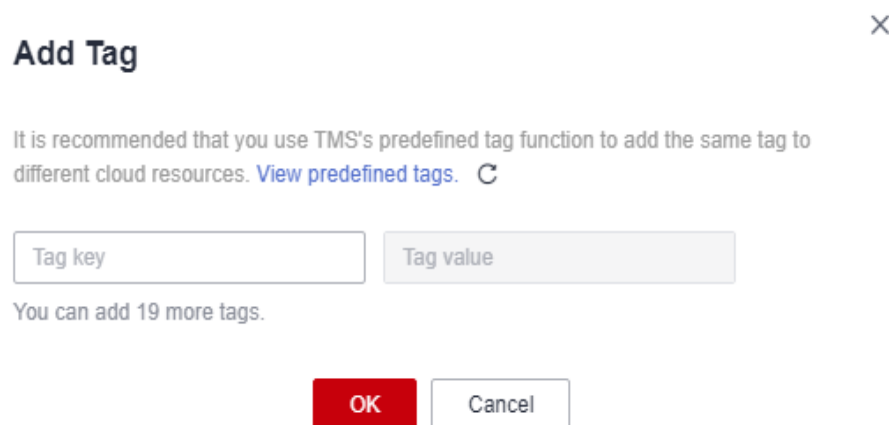
Paso 3 Haga clic en  a la izquierda, elija **Security & Compliance > Data Encryption Workshop**, se mostrará la página de gestión de claves.

Paso 4 En el panel de navegación, elija **Cloud Secret Management Service**.

Paso 5 Click a secret name to go to the details page.

Paso 6 Click **Add Tag**. On the displayed dialog box, set **Tag key** and **Tag value**.

Figura 5-5 Adding a tag




NOTA

- If you want to use the same tag to identify multiple cloud resources, you can create predefined tags in the TMS. In this way, the same tag can be selected for all services. For more information about predefined tags, see the *Tag Management Service User Guide*.
- To delete a tag, click **Delete** next to it.

Paso 7 Click **OK**.

----Fin

Dedicated HSM

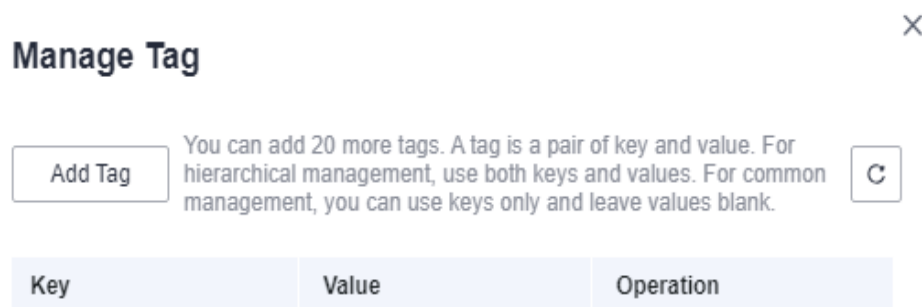
Paso 1 Click  in the upper left corner of the management console and select a region or project.

Paso 2 Click . Choose **Security & Compliance > Data Encryption Workshop**.

Paso 3 In the navigation pane, choose **Dedicated HSM**.

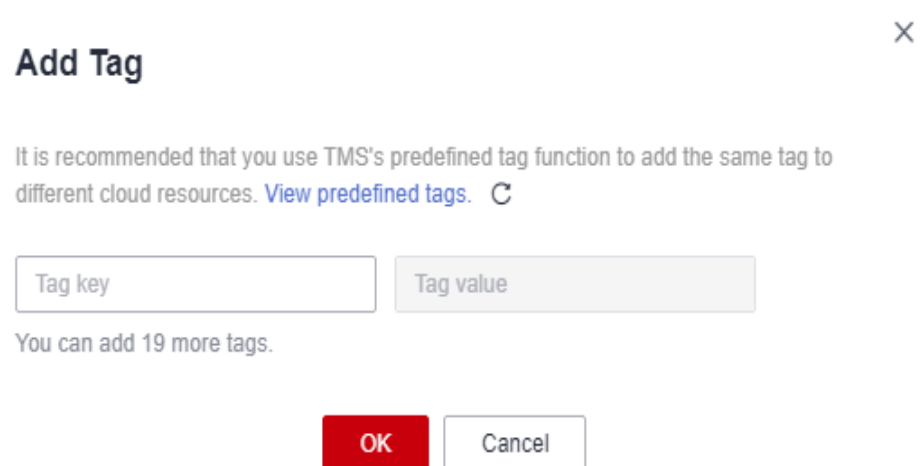
Paso 4 In the **Operation** column of an instance, click **Manage Tag**. The **Manage Tag** page is displayed, as shown in **Figura 5-6**.

Figura 5-6 Manage Tag



Paso 5 Click **Add Tag**. On the displayed dialog box, set **Tag key** and **Tag value**.

Figura 5-7 Adding a tag



NOTA

- If you want to use the same tag to identify multiple cloud resources, you can create predefined tags in the TMS. In this way, the same tag can be selected for all services. For more information about predefined tags, see the *Tag Management Service User Guide*.
- To delete a tag, click **Delete** next to it.

Paso 6 Click **OK**.

----Fin


5.4 Búsqueda de una clave personalizada por etiqueta

Esta sección describe cómo buscar una clave personalizada por etiqueta en un proyecto en la consola de KMS.

Prerrequisitos


Se han agregado etiquetas.

Restricciones

- Se pueden agregar varias etiquetas en una búsqueda. Se puede agregar un máximo de 20 etiquetas para una búsqueda. Si se buscan varias etiquetas a la vez, solo se mostrarán en el resultado de la búsqueda claves personalizadas que cumplan los criterios de búsqueda combinados.
- Si desea eliminar una etiqueta agregada de los criterios de búsqueda, haga clic en  junto a la etiqueta.

Procedimiento

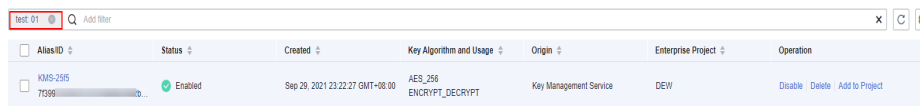
Paso 1 [Inicie sesión en la consola de gestión.](#)

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 . Elija **Security & Compliance > Data Encryption Workshop.**

Paso 4 Haga clic en el cuadro de búsqueda e introduzca la clave de etiqueta y el valor de etiqueta del recurso que desea buscar. Se muestran las teclas personalizadas que cumplen los criterios de búsqueda, como se muestra en el documento [Figura 5-8](#).

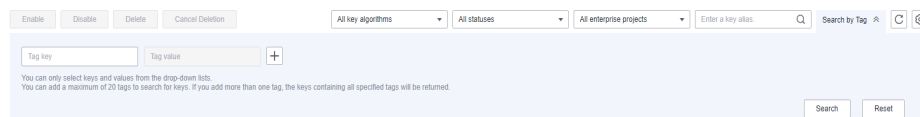
Figura 5-8 Resultado de la búsqueda



Alias ID	Status	Created	Key Algorithm and Usage	Origin	Enterprise Project	Operation
KMS-2395 7599	Enabled	Sep 29, 2021 23:22:27 GMT+08:00	AES_256 ENCRYPT_DECRYPT	Key Management Service	DEW	Disable Delete Add to Project

Paso 5 Haga clic en **Search by Tag** para mostrar el cuadro de búsqueda, como se muestra en [Figura 5-9](#).

Figura 5-9 Búsqueda de etiquetas





Enable Disable Delete Cancel Deletion All key algorithms All statuses All enterprise projects Enter a key alias Search by Tag

Tag key Tag value +

You can only select keys and values from the drop-down lists.
You can add a maximum of 20 tags to search for keys. If you add more than one tag, the keys containing all specified tags will be returned.

Search Reset

NOTA

- Se pueden agregar varias etiquetas en una búsqueda. Se puede agregar un máximo de 20 etiquetas para una búsqueda. Si se buscan varias etiquetas a la vez, solo se mostrarán en el resultado de la búsqueda claves personalizadas que cumplan los criterios de búsqueda combinados.
- Si desea eliminar una etiqueta agregada de los criterios de búsqueda, haga clic en   junto a la etiqueta.

----Fin

5.5 Modificación de un valor de etiqueta

En esta sección se describe cómo modificar una etiqueta de secreto creada.

Procedimiento



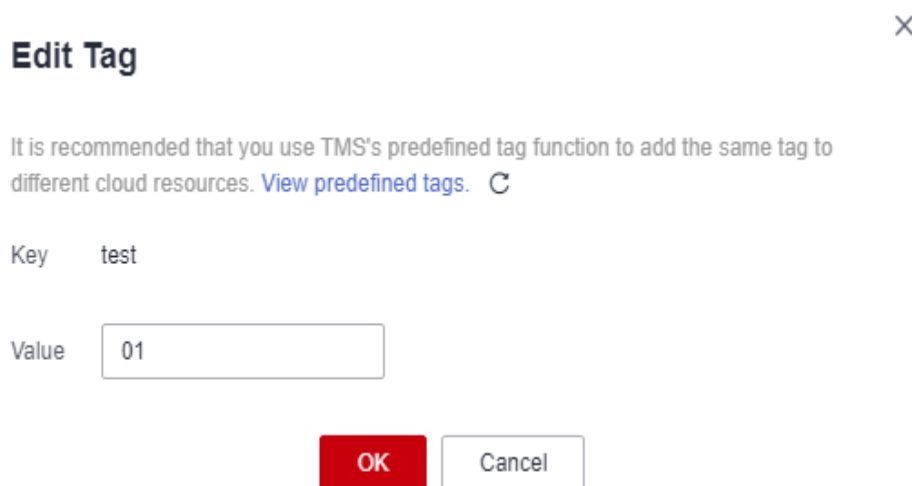

- Paso 1** Haga clic en  en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.
- Paso 2** Haga clic en . Elija **Security & Compliance > Data Encryption Workshop**.
- Paso 3** Elija el servicio de la izquierda, haga clic en la instancia cuya etiqueta debe modificarse y vaya a la página de detalles.
- Paso 4** Seleccione las etiquetas correspondientes, haga clic en **Edit** y aparecerá el cuadro **Edit Tag**. Después de cambiar el valor de la etiqueta, haga clic en **OK**.

Figura 5-10 Edición de una etiqueta



Edit Tag ×

It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. [View predefined tags.](#) 

Key test

Value



OK Cancel

----Fin

5.6 Deleting a Tag

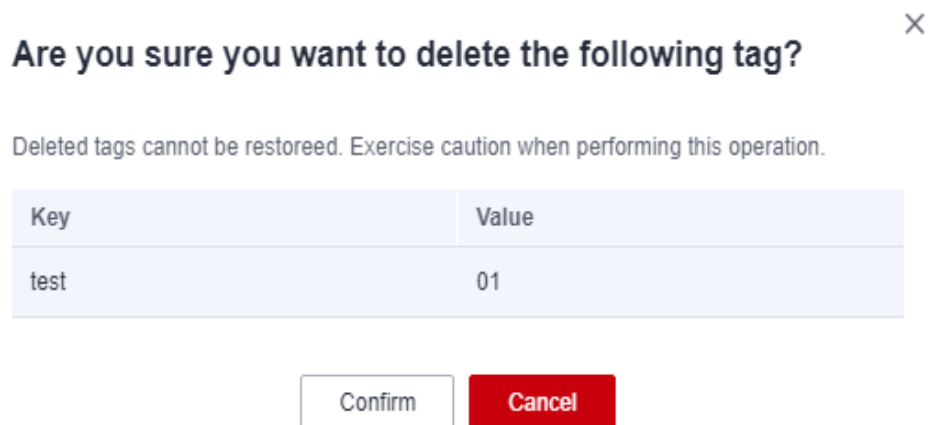
This section describes how to delete a created secret tag.

Procedure

- Paso 1** Click  in the upper left corner of the management console and select a region or project.
- Paso 2** Click . Choose **Security & Compliance > Data Encryption Workshop**.
- Paso 3** Choose the service from the left, click the instance whose tag need to be deleted, and go to the details page.

Paso 4 In the **Operation** column of a tag, click **Delete**.

Figura 5-11 Delete a tag



Paso 5 In the **Delete Tag** dialog box, click **Yes**.

----**Fin**

6 Registros de auditoría

6.1 Operaciones apoyadas por CTS

Las tablas de esta sección describen las operaciones DEW soportadas por CTS.

Tabla 6-1 Operaciones KMS registradas por CTS

Operación	Tipo de recurso	Nombre del rastro
Crear una clave	cmk	createKey
Crear un DEK	cmk	createDataKey
Crear un DEK sin texto sin formato	cmk	createDataKeyWithoutPlaintext
Habilitar una clave	cmk	enableKey
Deshabilitar una clave	cmk	disableKey
Cifrar un DEK	cmk	encryptDatakey
Descifrar un DEK	cmk	decryptDatakey
Programar eliminación de clave	cmk	scheduleKeyDeletion
Cancelar la eliminación de clave programada	cmk	cancelKeyDeletion
Generar números aleatorios	rng	genRandom
Modificar un alias de clave	cmk	updateKeyAlias
Modificar descripción de clave	cmk	updateKeyDescription
Riesgos inmediatos sobre la eliminación de CMK	cmk	deleteKeyRiskTips

Operación	Tipo de recurso	Nombre del rastro
Importar materiales de clave	cmk	importKeyMaterial
Eliminar materiales de clave	cmk	deleteImportedKeyMaterial
Crear una concesión	cmk	createGrant
Retirar una concesión	cmk	retireGrant
Revocar una concesión	cmk	revokeGrant
Cifrar datos	cmk	encryptData
Descifrar datos	cmk	decryptData
Agregar una etiqueta	cmk	createKeyTag
Eliminar una etiqueta	cmk	deleteKeyTag
Añadir etiquetas en lotes	cmk	batchCreateKeyTags
Eliminar etiquetas en lotes	cmk	batchDeleteKeyTags
Habilitar la rotación de clave	cmk	enableKeyRotation
Modificar intervalo de rotación de clave	cmk	updateKeyRotationInterval

Tabla 6-2 Operaciones KMS registradas por CSMS

Operación	Tipo de recurso	Nombre del rastro
Crear un secreto	csms	createSecret
Actualizar un secreto	csms	updateSecret
Eliminar un secreto	csms	forceDeleteSecret
Programar la eliminación de un secreto	csms	scheduleDelSecret
Cancelar la eliminación secreta programada	csms	restoreSecretFromDeleted-Status
Crear un estado secreto	csms	createSecretStage
Actualizar un estado secreto	csms	updateSecretStage
Eliminar un estado secreto	csms	deleteSecretStage
Crear una versión secreta	csms	createSecretVersion
Descargar una copia de respaldo secreta	csms	backupSecret

Operación	Tipo de recurso	Nombre del rastro
Restaurar una copia de respaldo secreta	csms	restoreSecretFromBackup-Blob
Actualizar la versión secreta	csms	putSecretVersion
Iniciar la rotación secreta	csms	rotateSecret
Crear un evento secreto	csms	createSecretEvent
Actualizar un evento secreto	csms	updateSecretEvent
Eliminar un evento secreto	csms	deleteSecretEvent
Crear una etiqueta de recurso	csms	createResourceTag
Eliminar una etiqueta de recurso	csms	deleteResourceTag

Tabla 6-3 Operaciones de KMS registradas por KPS

Operación	Tipo de recurso	Nombre del rastro
Crear o importar un par de claves SSH	keypair	createOrImportKeypair
Eliminar un par de claves SSH	keypair	deleteKeypair
Importar una clave privada	keypair	importPrivateKey
Exportar una clave privada	keypair	exportPrivateKey
Vincular un par de claves SSH	keypair	bindKeypair
Desvincular un par de claves SSH	keypair	unbindKeypair
Borrar claves privadas	keypair	clearPrivateKey

Tabla 6-4 Operaciones KMS grabadas por HSM dedicado

Operación	Tipo de recurso	Nombre del rastro
Comprar una instancia de HSM	hsm	purchaseHsm
Configurar una instancia de HSM	hsm	createHsm

Operación	Tipo de recurso	Nombre del rastro
Eliminar una instancia de HSM	hsm	deleteHsm

6.2 Uso de CTS para consultar rastros de operación de DEW

Una vez habilitado el CTS, el sistema inicia las operaciones de grabación en KMS. Los registros de operación de los últimos 7 días se almacenan en la consola CTS.

Para obtener más información acerca de cómo ver los registros de auditoría, consulte [Consulta de trazas en tiempo real](#).

7 Control de permisos

7.1 Crear un usuario y autorizar al usuario el permiso para acceder a DEW

Esta sección describe cómo usar **IAM** para implementar un control de permisos detallado para los recursos de DEW. Con IAM, usted puede:

- Crear usuarios de IAM para empleados en función de la estructura organizativa de su empresa. Cada usuario de IAM tiene sus propias credenciales de seguridad para acceder a los recursos de DEW.
- Otorgar a los usuarios sólo los permisos necesarios para realizar una tarea.
- Delegar una cuenta de Huawei o un servicio en la nube de confianza para realizar operaciones profesionales y eficientes en sus recursos de DEW.

Si su cuenta de Huawei no requiere usuarios individuales de IAM, omite este capítulo.

En esta sección se describe el procedimiento para conceder permisos (consulte [Figura 7-1](#)).

Prerrequisitos

Antes de conceder permisos a un grupo de usuarios, debe comprender los permisos de DEW disponibles y conceder permisos basados en el escenario de la vida real. En las tablas siguientes se describen los permisos admitidos en DEW.

Para ver las directivas del sistema de otros servicios, consulte [Permisos de sistema](#).

Tabla 7-1 Políticas del sistema KMS

Rol/Política	Descripción	Tipo	Dependencia
KMS Administrator	Todos los permisos de KMS	Rol	Ninguna

Rol/Política	Descripción	Tipo	Dependencia
KMS CMKFullAccess	Todos los permisos para las claves de KMS. Los usuarios con estos permisos pueden realizar todas las operaciones permitidas por las políticas.	Política	Ninguna
KMS CMKReadOnlyAccess	Permisos de sólo lectura para las claves de KMS. Los usuarios con estos permisos pueden realizar todas las operaciones permitidas por las políticas.	Política	Ninguna

Tabla 7-2 Políticas del sistema KPS

Rol/Política	Descripción	Tipo	Dependencia
DEW KeypairFullAccess	Todos los permisos para KPS. Los usuarios con estos permisos pueden realizar todas las operaciones permitidas por las políticas.	Política del sistema	Ninguna
DEW KeypairReadOnlyAccess	Permisos de solo lectura para el servicio de par de claves (KPS) en DEW. Los usuarios con este permiso sólo pueden ver los datos de KPS.	Política del sistema	Ninguna

Tabla 7-3 Políticas del sistema CSMS

Rol/Política	Descripción	Tipo	Dependencia
CSMS FullAccess	Todos los permisos para Cloud Secret Management Service (CSMS) en DEW. Los usuarios con estos permisos pueden realizar todas las operaciones permitidas por las políticas.	Política del sistema	Ninguna
CSMS ReadOnlyAccess	Permisos de solo lectura para Cloud Secret Management Service (CSMS) en DEW. Los usuarios con estos permisos pueden realizar todas las operaciones permitidas por las políticas.	Política del sistema	Ninguna

Tabla 7-4 describe las operaciones comunes soportadas por cada permiso definido por el sistema de DEW. Seleccione los permisos necesarios.

Tabla 7-4 Operaciones comunes respaldadas por cada política o función definida por el sistema

Operación	KMS Administrator	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
Creación de una clave	√	√	x	x
Habilitar una clave	√	√	x	x
Deshabilitar una clave	√	√	x	x
Programar eliminación de clave	√	√	x	x
Cancelar la eliminación de clave programada	√	√	x	x
Modificar un alias de clave	√	√	x	x
Modificar descripción de clave	√	√	x	x
Generar un número aleatorio	√	√	x	x
Crear un DEK	√	√	x	x
Crear un DEK sin texto sin formato	√	√	x	x
Cifrar un DEK	√	√	x	x
Descifrar un DEK	√	√	x	x
Obtener parámetros para importar una clave	√	√	x	x
Importar materiales de clave	√	√	x	x

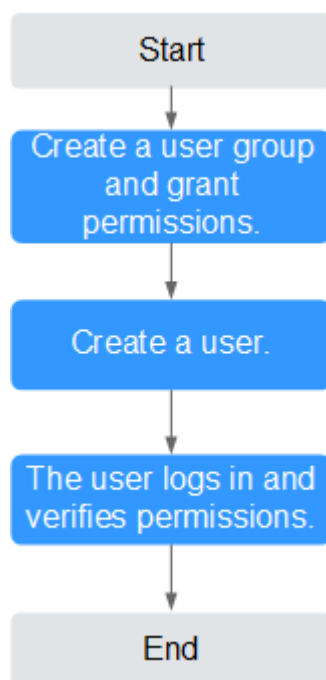
Operación	KMS Administrator	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairRead OnlyAccess
Eliminar materiales de clave	√	√	x	x
Crear una concesión	√	√	x	x
Revocar una concesión	√	√	x	x
Retirar una concesión	√	√	x	x
Consultar la lista de concesiones	√	√	x	x
Consultar concesiones retirables	√	√	x	x
Cifrar datos	√	√	x	x
Descifrar datos	√	√	x	x
Enviar mensajes de firma	√	√	x	x
Autenticar firma	√	√	x	x
Habilitación de la rotación de clave	√	√	x	x
Modificar intervalo de rotación de clave	√	√	x	x
Deshabilitación de la rotación de clave	√	√	x	x
Consultar estado de rotación de clave	√	√	x	x
Consultar instancias de CMK	√	√	x	x

Operación	KMS Administrator	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairRead OnlyAccess
Consultar etiquetas de clave	√	√	x	x
Consultar etiquetas de proyecto	√	√	x	x
Agregar o eliminar etiquetas de clave por lotes	√	√	x	x
Agregar etiquetas a una clave	√	√	x	x
Eliminar etiquetas de clave	√	√	x	x
Consultar la lista de clave	√	√	x	x
Consultar detalles de clave	√	√	x	x
Consultar clave pública	√	√	x	x
Cantidad de instancia de consulta	√	√	x	x
Cuotas de consulta	√	√	x	x
Consultar la lista de pares de claves	x	x	√	√
Crear o importar un par de claves	x	x	√	x
Consultar pares de claves	x	x	√	√
Eliminar un par de claves	x	x	√	x

Operación	KMS Administrator	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairRead OnlyAccess
Actualizar descripción del par de claves	x	x	√	x
Vincular un par de claves	x	x	√	x
Desvincular un par de claves	x	x	√	x
Consultar una tarea de vinculación	x	x	√	√
Consultar tareas fallidas	x	x	√	√
Eliminar todas las tareas con error	x	x	√	x
Eliminar una tarea fallida	x	x	√	x
Consultar tareas en ejecución	x	x	√	√

Proceso de autorización

Figura 7-1 Autorización del permiso de acceso DEW a un usuario



1. **Crear un grupo de usuario y asignar permisos**
Cree un grupo de usuarios en la consola de IAM y conceda al grupo de usuarios el permiso **KMS CMKFullAccess** (que indica permisos completos para las claves).
2. **Creación de un usuario de IAM**
Cree un usuario en la consola de IAM y agregue el usuario al grupo de usuarios creado en **1**.
3. **Iniciar sesión** y verificar los permisos.
Inicie sesión en la consola como usuario recién creado y compruebe que el usuario solo tiene permisos de lectura para DEW.
 - Elija **Service List > Data Encryption Workshop**. En el panel de navegación, elija **Key Pair Service**. Si aparece un mensaje que indica la falta de permisos, la política **KMS CMKFullAccess** tiene efecto.
 - Haga clic en **Service List** y seleccione un servicio que no sea DEW. Si se muestra un mensaje que indica que no tiene permiso para acceder al servicio, la política **KMS CMKFullAccess** tiene efecto.

7.2 Creación de una política de DEW personalizada

Las políticas personalizadas se pueden crear como un suplemento a las políticas del sistema de DEW. Para obtener más información sobre las acciones admitidas por las políticas personalizadas, consulte [Políticas de permisos y acciones admitidas](#).

Puede crear las políticas personalizadas de cualquiera de las siguientes maneras:

- Editor visual: Puede seleccionar configuraciones de política sin necesidad de conocer la sintaxis de política.

Parámetros de política de KMS personalizados:

- **Select service:** Seleccione **Key Management Service**.
 - **Select action:** Defina como sea necesario.
 - **(Optional) Select resource:** Establezca **Resources** en **Specific** y **KeyId** en **Specify resource path**. En el cuadro de diálogo que se muestra, establezca **Path** en el ID generado al crear la clave. Para obtener más información sobre cómo obtener el ID, consulte "Ver un CMK".
- JSON: Edite las políticas de JSON desde cero o basándose en una política existente. Para obtener más información acerca de cómo crear políticas personalizadas, consulte [Creación de una política personalizada](#).

Ejemplo de políticas personalizadas

- Ejemplo: autorizar a los usuarios a crear e importar claves

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:cmk:create",
        "kms:cmk:getMaterial",
        "kms:cmkTag:create",
        "kms:cmkTag:batch",
        "kms:cmk:importMaterial"
      ]
    }
  ]
}
```

- Ejemplo: denegar la eliminación de etiquetas clave

Una política de denegación debe usarse junto con otras políticas para que surtan efecto. Si los permisos asignados a un usuario contienen acciones Allow y Deny, las acciones Deny tienen prioridad sobre las acciones Allow.

El siguiente método se puede utilizar si necesita asignar permisos de la política **KMS Administrator** a un usuario, pero también prohibir que el usuario elimine etiquetas clave (**kms:cmkTag:delete**). Cree una política personalizada con la acción de eliminar etiquetas clave, establezca su **Effect** en **Deny** y asigne esta política y las políticas de **KMS Administrator** al grupo al que pertenece el usuario. A continuación, el usuario puede realizar todas las operaciones excepto eliminar las etiquetas de clave. La siguiente es una política para denegar etiquetas de par de claves.

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "kms:cmkTag:delete"
      ]
    }
  ]
}
```

- Ejemplo: autorizar a los usuarios a usar claves

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
```

```
        "kms:dek:crypto",  
        "kms:cmk:get",  
        "kms:cmk:crypto",  
        "kms:cmk:generate",  
        "kms:cmk:list"  
    ]  
  }  
]  
}
```

- **Ejemplo: política multi-acción**

Una política personalizada puede contener acciones de varios servicios que son todos de tipo global o de nivel de proyecto. La siguiente es una política con varias sentencias:

```
{  
  "Version": "1.1",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "rds:task:list"  
      ]  
    },  
    {  
      "Effect": "Allow",  
      "Action": [  
        "kms:dek:crypto",  
        "kms:cmk:get",  
        "kms:cmk:crypto",  
        "kms:cmk:generate",  
        "kms:cmk:list"  
      ]  
    }  
  ]  
}
```