Data Encryption Workshop

Guía del usuario de

Edición 26

Fecha 2021-10-26

HUAWEI

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Marcas registradas y permisos

El logotipo 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

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Índice

1 Key Management Service 1
1.1 Tipos de claves 1
1.2 Creación de un CMK 2
1.3 Creación de CMK mediante materiales de clave importados 5
1.3.1 Descripción general 5
1.3.2 Importación de materiales de clave 6
1.3.3 Eliminación de materiales de clave 13
1.4 Gestión de CMK 14
1.4.1 Consulta de un CMK 14
1.4.2 Habilitación de uno o más CMK 16
1.4.3 Deshabilitación de uno o más CMK 17
1.4.4 Programación de la eliminación de uno o más CMK 18
1.4.5 Cancelación de la eliminación programada de uno o más CMK 19
1.4.6 Adición de una clave a un proyecto 20
1.5 Uso de la herramienta en línea para cifrar y descifrar datos de tamaño pequeño 21
1.6 Gestión de etiquetas 22
1.6.1 Adición de una etiqueta 22
1.6.2 Búsqueda de un CMK por etiqueta 24
1.6.3 Modificación de valores de etiqueta 26
1.6.4 Eliminación de etiquetas 26
1.7 Rotación de CMKs 27
1.7.1 Acerca de rotación de clave 27
1.7.2 Habilitación de la rotación de clave 29
1.7.3 Deshabilitación de la rotación de clave 32
2 Cloud Secret Management Service 34
2.1 Creación de un Secreto 34
2.2 Gestión de secretos 35
2.2.1 Ver un secreto 36
2.2.2 Eliminación de un secreto 37
2.3 Gestión de versiones de secreto 38
2.3.1 Gestión de valores de secretos 38
2.3.2 Gestión de estados de versión secreta 40
2.4 Gestión de etiquetas 41

2.4.1 Adición de una etiqueta 42
2.4.2 Búsqueda de un secreto por etiqueta 43
2.4.3 Modificación de un valor de etiqueta 44
2.4.4 Eliminación de una etiqueta 45
3 Key Pair Service 47
3.1 Creación de un par de claves 47
3.2 Importación de un par de claves 52
3.3 Actualización de un par de claves 54
3.4 Gestión de pares de claves 56
3.4.1 Vinculación de un par de claves 56
3.4.2 Consulta de un par de claves 59
3.4.3 Restablecimiento de un par de claves 61
3.4.4 Sustitución de un par de claves 62
3.4.5 Desvinculación de un par de claves 64
3.4.6 Eliminación de un par de claves 66
3.5 Gestión de claves privadas 66
3.5.1 Importación de una clave privada 66
3.5.2 Exportación de una clave privada 68
3.5.3 Borrar una clave privada 69
3.6 Uso de una clave privada para iniciar sesión en Linux ECS 70
3.7 Uso de una clave privada para obtener la contraseña de inicio de sesión de Windows ECS 73
4 HSM dedicado 75
4.1 Guía de operación 75
4.2 Compra de una instancia HSM dedicada 78
4.2.1 Ediciones 78
4.2.2 Creación de una instancia HSM dedicada 79
4.2.3 Activación de una instancia HSM dedicada 82
4.3 Consulta de instancias de HSM dedicadas 86
4.4 Uso de instancias de HSM dedicadas 90
5 Registros de auditoría 94
5.1 Operaciones apoyadas por CTS 94
5.2 Uso de CTS para consultar rastros de operación DEW 95
6 Control de permisos 98
6.1 Crear un usuario y autorizar al usuario el permiso para acceder a DEW 98
6.2 Creación de una política de DEW personalizada 103
A Historial de cambios 106

1 Key Management Service

1.1 Tipos de claves

Los CMK se pueden clasificar en claves simétricas y claves asimétricas.

Las claves simétricas se usan comúnmente para la encriptación de datos. Las claves asimétricas se utilizan para la verificación de firma digital o el encriptación de información sensible 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 clave	Descripción	Uso
Symmetric key	AES	AES_256	Clave simétrica de AES	Cifra y descifra una pequeña cantidad de datos o claves de datos.
Asymmetric key	RSA	• RSA_2048 • RSA_3072 • RSA_4096	Contraseña asimétrica de RSA	Cifra y descifra una pequeña cantidad de datos o crea firmas digitales.
	ECC	• EC_P256 • EC_P384	Curva elíptica recomendada por el NIST	Firma digital

1.2 Creación de un CMK

Esta sección describe cómo crear un CMK en la consola KMS.

Los CMK se pueden clasificar en claves simétricas y claves asimétricas.

Prerrequisitos

Ha obtenido una cuenta y su contraseña para iniciar sesión en la consola de gestión.

La cuenta tiene KMS CMKFullAccess o permisos superiores.

Restricciones

- Puede crear hasta 100 CMK, excluyendo las claves maestras predeterminadas.
- Las claves simétricas se crean utilizando el algoritmo de encriptación y desencriptación AES-256. La clave tiene una longitud de 256 bits y se puede utilizar para cifrar y descifrar una pequeña cantidad de datos o claves de datos.
- 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 maestras predeterminadas terminan con **/default**. Por lo tanto, al elegir alias para sus CMK, no utilice alias que terminen con**/default**.
- DEW no limita el número de veces que se puede llamar a un CMK.

Escenarios

- **Encriptar datos en OBS**.
- **Encriptar datos en EVS**.
- **Encriptar datos en IMS**.
- **Encriptar una instancia de RDS DB**.
- Encriptación y desencriptación directo de pequeños volúmenes de datos
- Encriptación y desencriptación de DEK para aplicaciones de usuario
- Las claves asimétricas se pueden utilizar para firmas digitales y verificación de firmas.

Creación de un CMK

Paso 1 **Inicie sesión en la consola de gestión.**

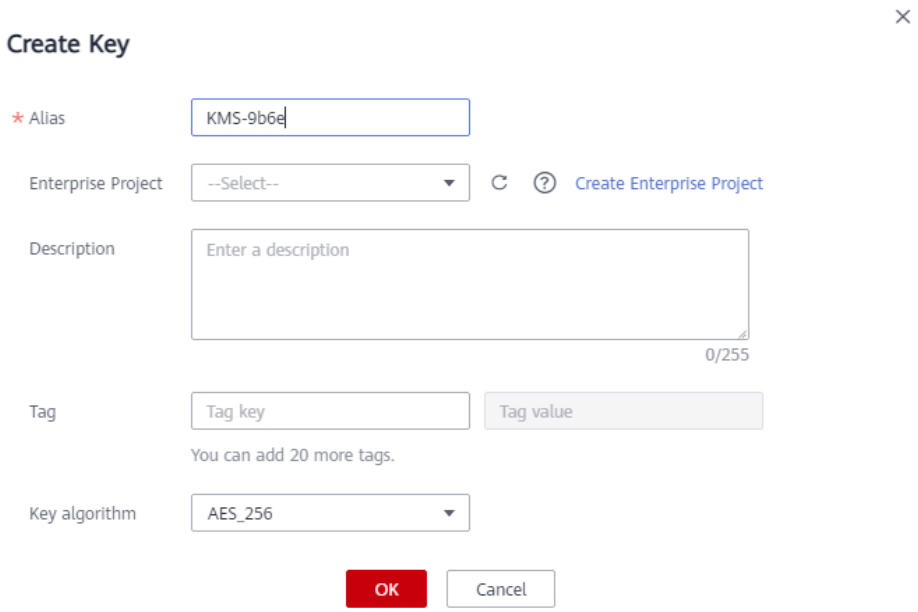
Paso 2 Haga clic en  en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

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

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

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

Figura 1-1 Creación de una clave



- **Alias** es el alias del CMK 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 clave	Descripción	Uso
Symmetric key	AES	AES_256	Clave simétrica de AES	Cifra y descifra una pequeña cantidad de datos o claves de datos.
Asymmetric key	RSA	- RSA_2048 - RSA_3072 - RSA_4096	Contraseña asimétrica de RSA	Cifra y descifra una pequeña cantidad de datos o crea firmas digitales.

Tipo de clave	Tipo de algoritmo	Especificaciones clave	Descripción	Uso
	ECC	- EC_P256 - EC_P384	Curva elíptica recomendada por el NIST	Firma digital

- **Usage**: seleccione **SIGN_VERIFY** o **ENCRYPT_DECRYPT**.
  - Para una clave simétrica, el valor predeterminado es **ENCRYPT_DECRYPT**.
  - 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

  The key usage can only be configured during key creation and cannot be modified afterwards.
- (Opcional) **Description** es la descripción del CMK.
- 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 utilizar proyectos empresariales para gestionar los recursos de la nube y los miembros del proyecto. Para obtener más información acerca de los proyectos de empresa, consulte **Guía de usuario de Enterprise Management**.

  – Para obtener más información acerca de cómo habilitar la función de proyecto de empresa, consulte **Habiltiación del centro de empresa**

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

NOTA

- Cuando se ha creado un CMK sin ninguna etiqueta, puede agregar una etiqueta al CMK más tarde según sea necesario. Haga clic en el alias del CMK, haga clic en la pestaña **Tags** y haga clic en **Add Tag**.
- La misma etiqueta (incluyendo clave de etiqueta y valor de etiqueta) se puede usar para diferentes CMK. Sin embargo, bajo el mismo CMK, una clave de etiqueta puede tener solo un valor de etiqueta.
- Se puede añadir un máximo de 20 etiquetas para un CMK.
- 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 CMK, puede ver las CMK creadas. El estado predeterminado de un CMK es **Enabled**.

----Fin

Operaciones relacionadas

- Para obtener más información acerca de cómo cargar objetos con encriptación del servidor, consulte la sección **Uploading a File with Server-Side Encryption** en la *Object Storage Service Console Operation Guide*.
- 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 **Encriptación de un imagen** en la *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 general

Un CMK contiene metadatos 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 un CMK, el KMS genera automáticamente un material clave para el CMK.
- Si desea utilizar su propio material de clave, puede utilizar la función de importación de clave en la consola de KMS para crear un CMK cuyo material de clave esté vacío e importar el material de clave al CMK.

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.

  Se muestran las diferencias entre el material clave importado y el material clave generado por KMS en **Tabla 1-3**.

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

Fuente de material de clave	Diferencia
CMK que utilizan materiales de clave importados	● Puede eliminar el material de clave, pero no puede eliminar el CMK 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 el CMK 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. **NOTA** Las claves que utilizan los algoritmos RSA_2048, RSA_3072, RSA_4096, EC_P256 y EC_P384 son válidas permanentemente. Sus materiales de clave no se pueden eliminar manualmente y su tiempo de caducidad no se puede configurar.
CMK que utilizan materiales de clave generados por KMS	● 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 se importa un material de clave a un CMK, el CMK se asocia permanentemente con el material de clave. Otros materiales clave no se pueden importar en el CMK.

- Unicidad

  Si utiliza el CMK creado con el material de clave importado para cifrar datos, los datos cifrados sólo pueden ser descifrados por el CMK que se ha utilizado para cifrar los datos, ya que los metadatos y el material de clave del CMK 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.

Prerrequisitos

- Ha obtenido una cuenta y su contraseña para iniciar sesión en la consola de gestión.
- Ha preparado materiales de clave para importar.

Procedimiento

Paso 1 **Inicie sesión en la consola de gestión.**

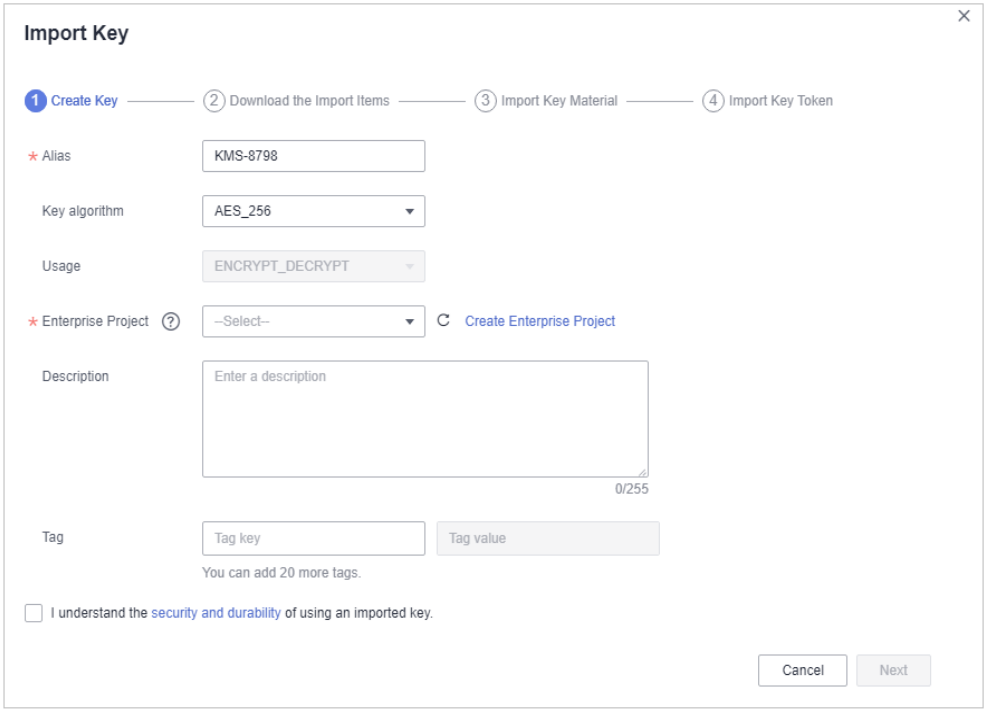
Paso 2 Haga clic en en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

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 del CMK 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 clave	Descripción	Uso
Symmetric key	AES	AES_256	Clave simétrica de AES	Cifra y descifra una pequeña cantidad de datos o claves de datos.
Asymmetric key	RSA	- RSA_2048 - RSA_3072 - RSA_4096	Contraseña asimétrica de RSA	Cifra y descifra una pequeña cantidad de datos o crea firmas digitales.
	ECC	- EC_P256 - EC_P384	Curva elíptica recomendada por el NIST	Firma digital

- **Usage**: seleccione **SIGN_VERIFY** o **ENCRYPT_DECRYPT**.
  - Para una clave simétrica, el valor predeterminado es **ENCRYPT_DECRYPT**.
  - 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

  The key usage can only be configured during key creation and cannot be modified afterwards.
- (Opcional) **Description** es la descripción del CMK.
- 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 utilizar proyectos empresariales para gestionar los recursos de la nube y los miembros del proyecto. Para obtener más información acerca de los proyectos de empresa, consulte **Guía de usuario de Enterprise Management**.
  - Para obtener más información acerca de cómo habilitar la función de proyecto de empresa, consulte **Habiltiación del centro de empresa**

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

NOTA

- Si se creó un CMK sin ninguna etiqueta, puede agregar una etiqueta al CMK más adelante según sea necesario. Haga clic en el alias del CMK, haga clic en la pestaña **Tags** y haga clic en **Add Tag**.
- La misma etiqueta (incluyendo clave de etiqueta y valor de etiqueta) se puede usar para diferentes CMK. Sin embargo, bajo el mismo CMK, una clave de etiqueta puede tener solo un valor de etiqueta.
- Se puede añadir un máximo de 20 etiquetas para cada CMK.
- 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 un CMK 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 1-5**.

Tabla 1-5 Algoritmos de envoltura de claves

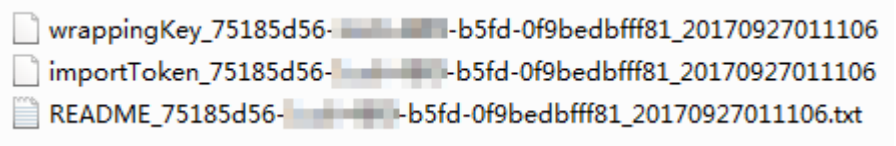
Algoritmo	Descripción	Configuración
RSAES_OAEP_SHA_256	Algoritmo de encriptación RSA que utiliza OAEP y tiene la función hash **SHA-256**	Elija un algoritmo en el cuadro de lista desplegable. Si los HSM soportan el algoritmo **RSAES_OAEP_SHA_256**, utilice **RSAES_OAEP_SHA_256** para cifrar materiales de 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 del CMK requerido e importe material clave en el cuadro de diálogo que se muestra.

Paso 10 Haga clic en **Download**. Se descargan los siguientes archivos: **wrappingKey**, **importToken**, y **README**, como se muestra en **Figura 1-3**.

Figura 1-3 Descarga de archivos



- **wrappingKey_*CMKID_DownloadTime*** es una clave de envoltura utilizada para cifrar materiales de clave.
- **importToken_*CMKID_DownloadTime*** es un token utilizado para importar materiales clave a KMS.

- **README_*CMKID_DownloadTime*** es un archivo de descripción que registra información tal como el número de serie de un CMK, algoritmo de envoltura, nombre de clave de envoltura, nombre de archivo de token, y el tiempo de caducidad del archivo de token y de la clave de envoltura.

AVISO

- **wrappingKey_Key ID**_*Download_time* está codificado en formato binario.
- La clave de embalaje y el token de importación caducan en 24 horas. Si han caducado, descárguelo de nuevo.

También puede obtener la clave de envoltorio y el token de importación a través de la API.

1. Llame a la API **get-parameters-for-import** para obtener la clave de envoltorio y el token de importación.

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

   public_key: contenido de la clave de envoltura (codificación Base-64) devuelta después de la llamada a la API

   import_token: contenido del token de importación (codificación Base-64) devuelto después de la llamada a la API

   - Solicitud de ejemplo

     ```
     {
         "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
     }
     ```

2. 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.

   a. Copie el contenido de la clave de ajuste **public_key**, péguela en el archivo a.txt y guarde el archivo como **PublicKey.b64**.

   b. 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

3. Guarde el token de importación, copie el contenido del token **import_token**, péguelo en un archivo .txt, y guarde el archivo como **ImportToken.b64**.

Paso 11 Utilice el archivo **wrappingKey** para cifrar los materiales de clave que se van a importar.

- 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 cifrar los materiales de clave.

NOTA

Si necesita ejecutar el comando **openssl pkeyutl**, la versión de OpenSSL debe ser 1.0.2 o posterior.

En el ejemplo siguiente se describe cómo utilizar la clave de envoltura descargada para cifrar el material de clave generado (clave simétrica de 256 bits). Siga el siguiente procedimiento:

a. Para generar un material de clave para una clave simétrica de 256 bits usando el algoritmo AES256, en el agente donde se ha instalado OpenSSL, ejecute el siguiente comando para generar el material de clave y guardarlo como **PlaintextKeyMaterial.bin**:

   openssl rand -out *PlaintextKeyMaterial.bin* 32

   Para generar un material de clave para una clave asimétrica RSA o ECC, realice las siguientes operaciones:

   i. Generar una clave hexadecimal AES256.

      openssl rand -out 0xPlaintextKeyMaterial.bin -hex 32

   ii. 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**.

   Replace ***PublicKey.bin*** in the command with the name of the wrapping key *wrappingKey_key ID_download time* downloaded in **Paso 10**.

   Tabla 1-6 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. Para importar una clave asimétrica, genere una clave privada asimétrica y use un material de clave temporal para cifrar la clave privada.

   - Tome el algoritmo RSA4096 como ejemplo. Siga estos pasos:

     1) Generar una clave privada.

        openssl genrsa -out rsa_private_key.pem 4096

     2) Convertir la clave a formato DER.

        openssl pkcs8 -topk8 -inform PEM -outform DER -in rsa_private_key.pem -out rsa_private_key.der -nocrypt

3) Utilice 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 12 Haga clic en **Next** para ir al paso **Import Key Material**.

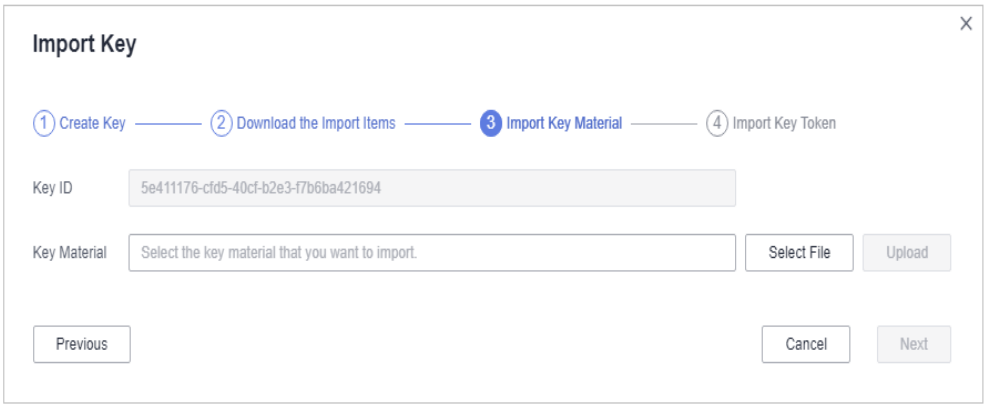
Tabla 1-7 Parámetros para importar materiales de clave (para claves simétricas)

Parámetro	Descripción
Key ID	Random ID of a CMK generated during the CMK creation
Key material	Importar un material de clave.

Tabla 1-8 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.
Private key ciphertext	Seleccionar texto cifrado de clave privada.

Figura 1-4 Importación de materiales de clave



Paso 13 Haga clic en **Next** para ir al paso **Import Key Token**. Configure los parámetros como se describe en **Tabla 1-9**.

Tabla 1-9 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 descargado en **Paso 10**.
Key material expiration mode	● **Key material will never expire**: utilice esta opción para especificar que los materiales clave no caducarán después de la importación. ● **Key material will expire**: Utilice esta opción para especificar el tiempo de caducidad de los materiales 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 14 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 CMK 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 obtenido una cuenta y su contraseña para iniciar sesión en la consola de gestión.
- 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 del CMK. 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, realice las instrucciones en **Programación de la 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 maestra en la consola KMS, incluidos el alias de clave, el estado, el ID y la hora de creación. El estado de un CMK puede ser **Enabled**, **Disabled**, 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 . Elija **Security & Compliance** > **Data Encryption Workshop**.

Paso 4 Compruebe la lista de claves. **Tabla 1-10** describe los parámetros.

Figura 1-5 Claves personalizadas

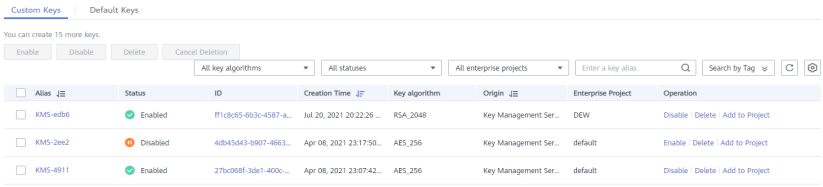


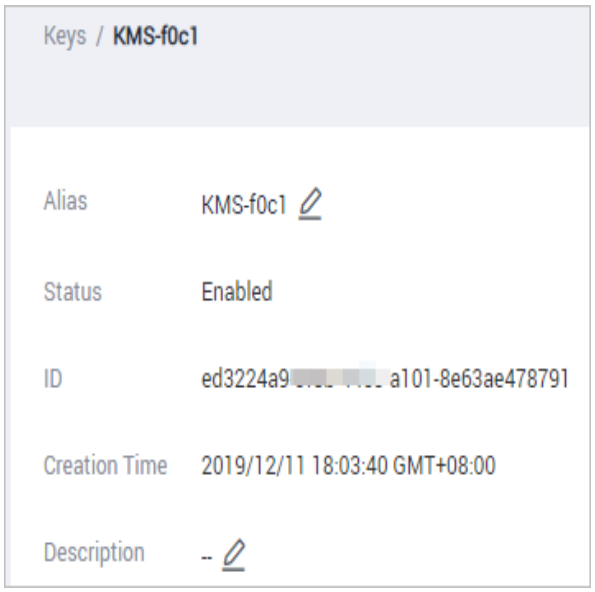
Figura 1-6 Claves predeterminadas

Tabla 1-10 Parámetros de lista de clave

Parámetro	Descripción
Alias	Alias de un CMK
Status	Estado de un CMK, que puede ser uno de los siguientes: ● **Enabled** El CMK está habilitado. ● **Disabled** El CMK está deshabilitado. ● **Pending deletion** El CMK está programado para su eliminación.
ID	ID aleatorio de un CMK generado durante la creación del CMK **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**.
Creation Time	Tiempo de creación del CMK
Key Algorithm and Usage	Algoritmo de clave seleccionado durante la creación de clave y su uso
Enterprise Project	Proyecto de empresa para el que se utiliza el CMK

Paso 5 Puede hacer clic en el alias de un CMK para ver sus detalles, como muestra en **Figura 1-7**.

Figura 1-7 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 maestra predeterminada (cuyo sufijo de alias es **/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 uno o más CMK. Solo se pueden utilizar CMK habilitados para cifrar o descifrar datos. Un nuevo CMK está en el estado **Enabled** de forma predeterminada.

Prerrequisitos

- Ha obtenido una cuenta y su contraseña para iniciar sesión en la consola de gestión.
- El CMK que desea habilitar está en estado **Disabled**.

Procedimiento

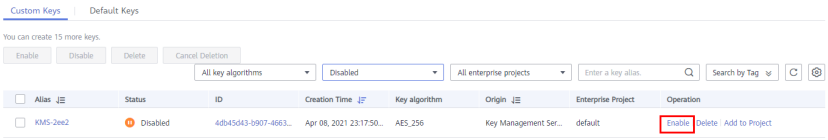
Paso 1 **Inicie sesión en la consola de gestión.**

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 el CMK deseado, haga clic en **Enable**.

Figura 1-8 Habilitación de una CMK



Paso 5 En el cuadro de diálogo que se muestra, haga clic en **Yes** para habilitar el CMK.

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 uno o más CMK, protegiendo así los datos en casos urgentes.

Una vez deshabilitado, no se puede utilizar un CMK 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

- Ha obtenido una cuenta y su contraseña para iniciar sesión en la consola de gestión.
- El CMK que desea deshabilitar está en estado **Enabled**.

Restricciones

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

Procedimiento

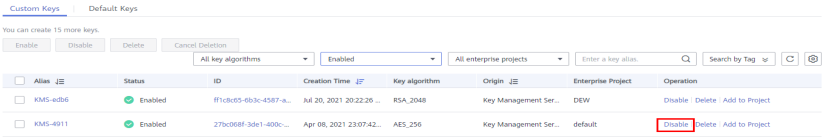
Paso 1 **Inicie sesión en la consola de gestión.**

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 1-9 Deshabilitación de un CMK



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

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 Programación de la 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 en los registros de auditoría.

Prerrequisitos

- Ha obtenido una cuenta y su contraseña para iniciar sesión en la consola de gestión.
- El CMK para el que desea programar la eliminación está en estado **Enabled** o **Disabled**.

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 ha entrado en vigor, el CMK se eliminará permanentemente y no podrá descifrar los datos cifrados por él. Por lo tanto, se le aconseja tener precaución al realizar esta operación.
- Default Master Keys creadas por KMS no se pueden programar para su eliminación.
- Un CMK en estado de eliminación pendiente no incurre en cargos. Si cancela la eliminación, el cargo se reanudará a partir del momento en que se programó que se eliminara el CMK.

Procedimiento

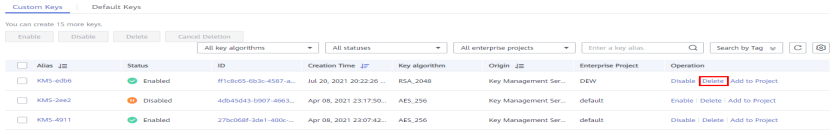
Paso 1 **Inicie sesión en la consola de gestión.**

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**.

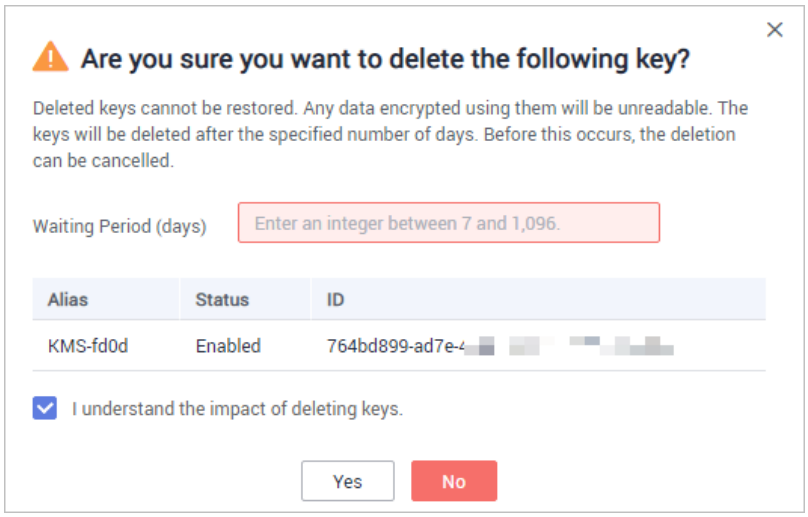
Paso 4 En la fila que contiene el CMK deseado, haga clic en **Delete**.

Figura 1-10 Programación de la eliminación de una CMK



Paso 5 En el cuadro de diálogo que se muestra, escriba el número de días después de los cuales desea que la eliminación surta efecto.

Figura 1-11 Introducir el período después del cual desea que la eliminación surta efecto



Paso 6 En el cuadro de diálogo que se muestra, seleccione **I understand the impact of deleting keys** y haga clic en **Yes**.

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.

----Fin

1.4.5 Cancelación de la eliminación programada de uno o más CMK

Esta sección describe cómo utilizar la consola KMS para cancelar la eliminación programada de uno o más CMK antes de la ejecución de la eliminación. Después de la cancelación, el CMK está en estado **Disabled**.

Prerrequisitos

- Ha obtenido una cuenta y su contraseña para iniciar sesión en la consola de gestión.
- El CMK para el que desea cancelar la eliminación programada está en estado de **Pending deletion**.

Procedimiento

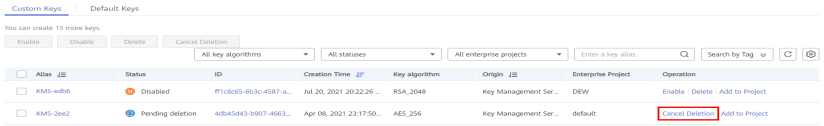
Paso 1 **Inicie sesión en la consola de gestión.**

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 1-12 Cancelación de la eliminación programada de un CMK



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

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

Puede asignar claves a proyectos de empresa en la consola de KMS.

Prerrequisitos

Ha obtenido una cuenta y su contraseña para iniciar sesión en la consola de gestión.

NOTA

No se puede cambiar el proyecto de empresa de las claves maestras predeterminadas.

Procedimiento

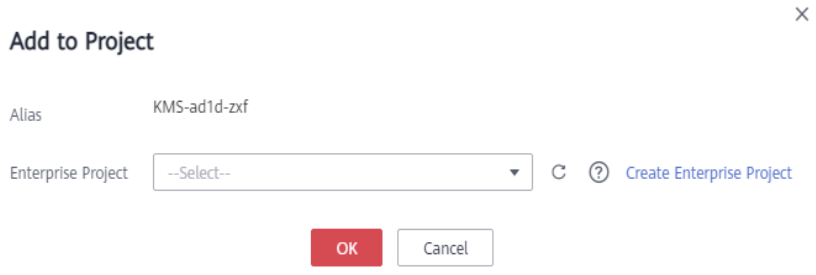
Paso 1 **Inicie sesión en la consola de gestión.**

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

Figura 1-13 Adición de una clave a un proyecto



Paso 5 Seleccione un proyecto.

Paso 6 Haga clic en **OK**.

----Fin

1.5 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

- Ha obtenido una cuenta y su contraseña para iniciar sesión en la consola de gestión.

Restricciones

- Las claves maestras predeterminadas no se pueden utilizar para cifrar o descifrar dichos datos con la herramienta.
- Puede llamar a una API para usar una clave maestra 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.**

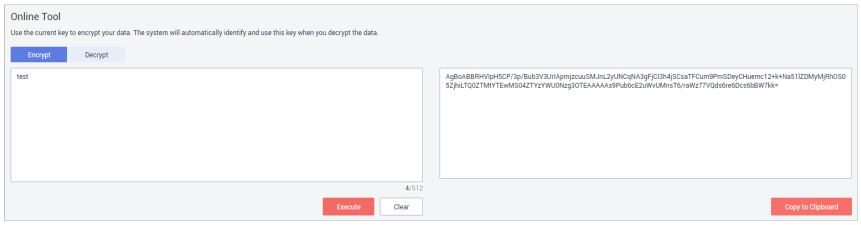
Paso 2 Haga clic en en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

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

Paso 4 Haga clic en el alias del CMK deseado para ver sus detalles, y vaya a la herramienta en línea para el encriptación y desencriptación de datos.

Paso 5 Haga clic en **Encrypt**. En el cuadro de texto de la izquierda, introduzca los datos que se van a cifrar. Consulte **Figura 1-14** para obtener más detalles.

Figura 1-14 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**.

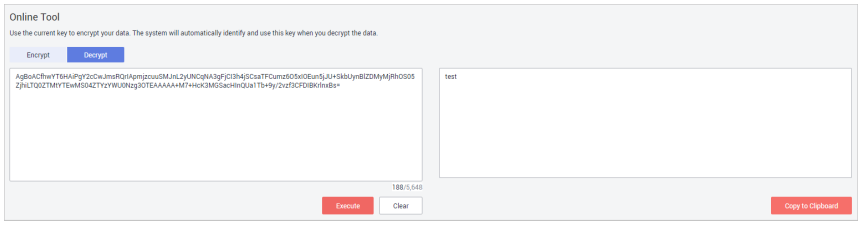
Paso 3 Puede hacer clic en cualquier CMK en estado **Enabled** para ir a la página de encriptación y desencriptación de la herramienta en línea.

Paso 4 Haga clic en **Decrypt**. En el cuadro de texto de la izquierda, introduzca los datos que se van a descifrar. Consulte **Figura 1-15** para obtener más detalles.

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 1-15 Desencriptación de datos



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

NOTA

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

----Fin

1.6 Gestión de etiquetas

1.6.1 Adición de una etiqueta

Las etiquetas se utilizan para identificar CMK. Puede agregar etiquetas a las CMK para que pueda clasificarlas, rastrearlas y recopilar su estado de uso de acuerdo con las etiquetas.

Prerrequisitos

Ha obtenido una cuenta y su contraseña para iniciar sesión en la consola de gestión.

Restricciones

No se pueden agregar etiquetas a las claves maestras 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.

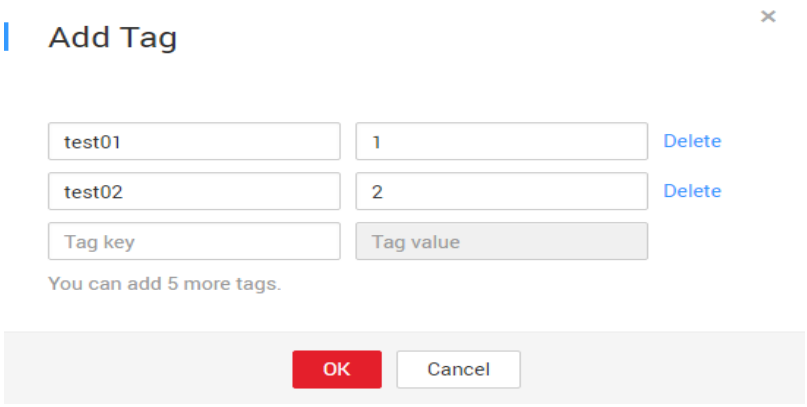
Paso 3 Haga clic en . Elija **Security & Compliance** > **Data Encryption Workshop**.

Paso 4 Haga clic en el alias del CMK deseado 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 1-11** describe los parámetros.

Figura 1-16 Adición de una etiqueta



NOTA

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 1-11 Parámetros de etiqueta

Parámetro	Descripción	Valor	Valor de ejemplo
Tag key	Nombre de una etiqueta. La misma etiqueta (incluyendo clave de etiqueta y valor de etiqueta) se puede usar para diferentes CMK. Sin embargo, bajo el mismo CMK, una clave de etiqueta puede tener solo un valor de etiqueta. Se puede añadir un máximo de 20 etiquetas para un CMK.	● Obligatorio. ● Cada clave de etiqueta debe ser única bajo el mismo CMK. ● Límite de 36 caracteres. ● Se permiten los siguientes tipos de caracteres: – Letras en mayúscula – Letras en minúscula – Dígitos – Caracteres especiales, incluyendo guiones (-) y guiones bajos (_)	cost
Tag value	Valor de la etiqueta	● Este parámetro puede estar vacío. ● Límite de 43 caracteres. ● Se permiten los siguientes tipos de caracteres: – Letras en mayúscula – Letras en minúscula – Dígitos – Caracteres especiales, incluyendo guiones (-) y guiones bajos (_)	100

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

----Fin

1.6.2 Búsqueda de un CMK por etiqueta

Esta sección describe cómo buscar un CMK por etiqueta en un proyecto en la consola KMS.

Prerrequisitos

- Ha obtenido una cuenta y su contraseña para iniciar sesión en la consola de gestión.
- Se han agregado etiquetas.

Restricciones

- Se pueden agregar varias etiquetas en una búsqueda. Se puede añadir un máximo de 20 etiquetas para una búsqueda. Si se buscan varias etiquetas a la vez, cada CMK en el resultado de la búsqueda cumple los criterios de búsqueda combinados.

- Si desea eliminar una etiqueta agregada de los criterios de búsqueda, haga clic en junto a la etiqueta.
- Puede hacer clic en **Reset** para restablecer los criterios de búsqueda.

Procedimiento

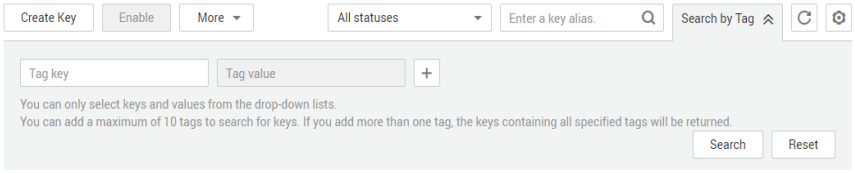
Paso 1 **Inicie sesión en la consola de gestión.**

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 **Search by Tag** para mostrar el cuadro de búsqueda. **Figura 1-17** describe los detalles.

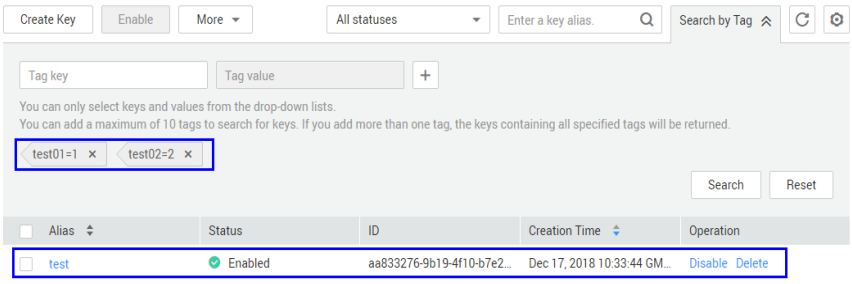
Figura 1-17 Búsqueda de etiquetas



Paso 5 En el cuadro de búsqueda, escriba o seleccione una clave de etiqueta y un valor de etiqueta.

Paso 6 Haga clic para agregar la entrada a los criterios de búsqueda y haga clic en **Search**. La lista muestra las CMK que cumplen los criterios de búsqueda. Para más detalles, consulte **Figura 1-18**.

Figura 1-18 Resultados de búsqueda



NOTA

- Se pueden agregar varias etiquetas en una búsqueda. Se puede añadir un máximo de 20 etiquetas para una búsqueda. Si se buscan varias etiquetas a la vez, cada CMK en el resultado de la búsqueda cumple los criterios de búsqueda combinados.
- Si desea eliminar una etiqueta agregada de los criterios de búsqueda, haga clic en junto a la etiqueta.
- Puede hacer clic en **Reset** para restablecer los criterios de búsqueda.

----Fin

1.6.3 Modificación de valores de etiqueta

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

Prerrequisitos

Ha obtenido una cuenta y su contraseña para iniciar sesión en 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.

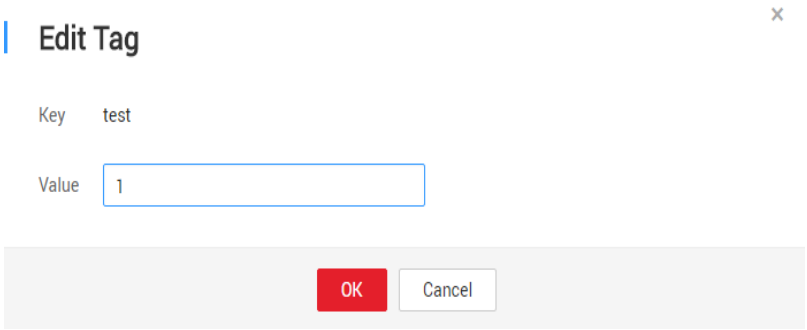
Paso 3 Haga clic en . Elija **Security & Compliance** > **Data Encryption Workshop**.

Paso 4 Haga clic en el alias del CMK deseado 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 1-19 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

1.6.4 Eliminación de etiquetas

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

Prerrequisitos

Ha obtenido una cuenta y su contraseña para iniciar sesión en 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 . Elija **Security & Compliance** > **Data Encryption Workshop**.

Paso 4 Haga clic en el alias del CMK deseado 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 **Yes** para completar la eliminación.

----Fin

1.7 Rotación de CMKs

1.7.1 Acerca de rotación de clave

Propósito de la rotación de clave

Las claves que se usan ampliamente 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

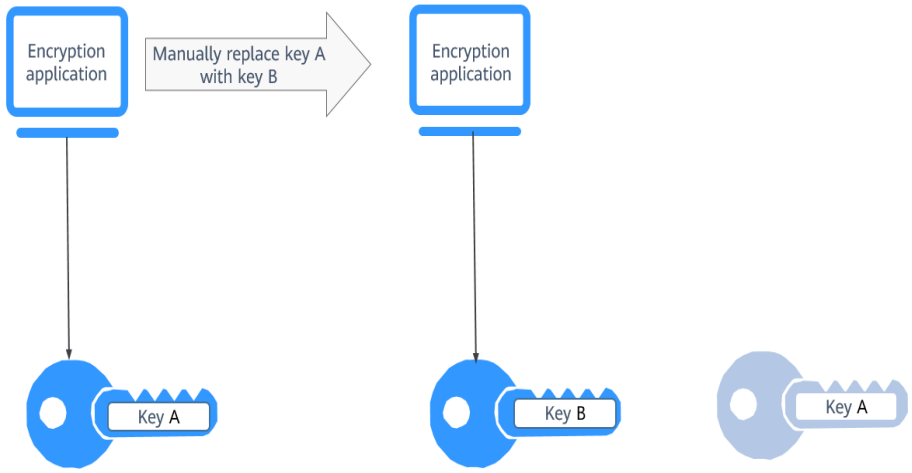
Puede utilizar cualquiera de los siguientes métodos de rotación de claves:

- Rotación manual de clave

  Reemplace la clave en uso por una nueva clave. Por ejemplo, si la clave A está en uso, puede crear la clave B utilizando un nuevo material de encriptación y reemplazar la clave A por la clave B. Esto logra el mismo resultado que cambiar el material clave de la clave A.

Tomemos OBS como ejemplo. Para girar manualmente una clave, cree un nuevo CMK en la consola KMS. Reemplace el antiguo CMK por el nuevo en la consola OBS.

Figura 1-20 Rotación manual de clave



- Rotación automática de clave

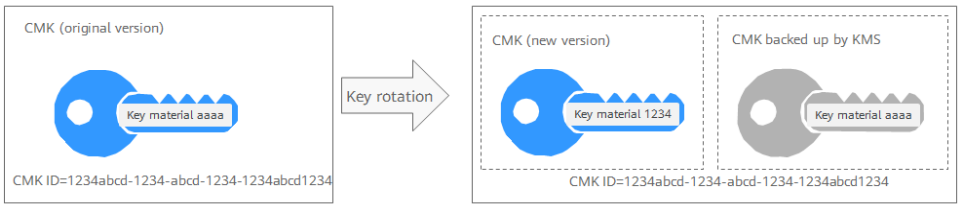
  KMS rota automáticamente las clave según el período de rotación configurado (365 días por defecto). El sistema genera automáticamente una nueva clave para reemplazar la clave en uso. La rotación automática de clave solo cambia el material de clave de un CMK. Los atributos lógicos del CMK no cambiarán,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

  La rotación automática de la llave tiene las siguientes características:

  a. Habilitar la rotación de un CMK existente. KMS generará automáticamente nuevos materiales clave para el CMK.

  b. 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 1-21 Rotación de clave



NOTA

KMS conserva todas las versiones de un CMK, por lo que puede descifrar cualquier texto cifrado mediante el CMK.

- KMS utiliza la última versión del CMK para cifrar datos.
- Al descifrar datos, KMS utiliza la versión CMK que se utilizó para cifrar los datos.

Modos de rotación

Tabla 1-12 Modos de rotación de clave

Tipo de clave	Modo de rotación
Default master key	No se puede girar.
User-defined key (imported CMK)	Solo se puede girar manualmente. Para obtener más información acerca de las claves definidas por el usuario, vea **Descripción general de CMK**.
Symmetric key	Se puede girar automática o manualmente.
Asymmetric key	Solo se puede girar manualmente.
Disabled CMK	Los CMK deshabilitados no se rotan. KMS mantiene su estado de rotación sin cambios. Después de activar un CMK, si se ha utilizado durante más tiempo que el período de rotación, KMS girará inmediatamente calves. 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 **Deshabilitación de uno o más CMK**.
CMKs in pending deletion state	Los CMK deshabilitados no se rotan. KMS mantiene su estado de rotación sin cambios. Después de activar un CMK, si se ha utilizado durante más tiempo que el período de rotación, KMS girará inmediatamente calves. 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.

1.7.2 Habilitación de la rotación de clave

Esta sección describe cómo habilitar la rotación para un CMK en la consola KMS.

De forma predeterminada, la rotación automática de teclas está deshabilitada para un CMK. Cada vez que habilita la rotación de teclas, KMS rota automáticamente las CMK en función del período de rotación establecido.

Prerrequisitos

- Ha obtenido una cuenta y su contraseña para iniciar sesión en la consola de gestión.
- El CMK está habilitado.
- El **Origin** de la CMK es **KMS**.

Restricciones

Un CMK deshabilitado nunca se rota, incluso si la rotación está habilitada para él.

KMS reanuda la rotación cuando este CMK está habilitado. Si habilita esta CMK después de que haya pasado un período de rotación, KMS la rotará dentro de las 24 horas.

Procedimiento

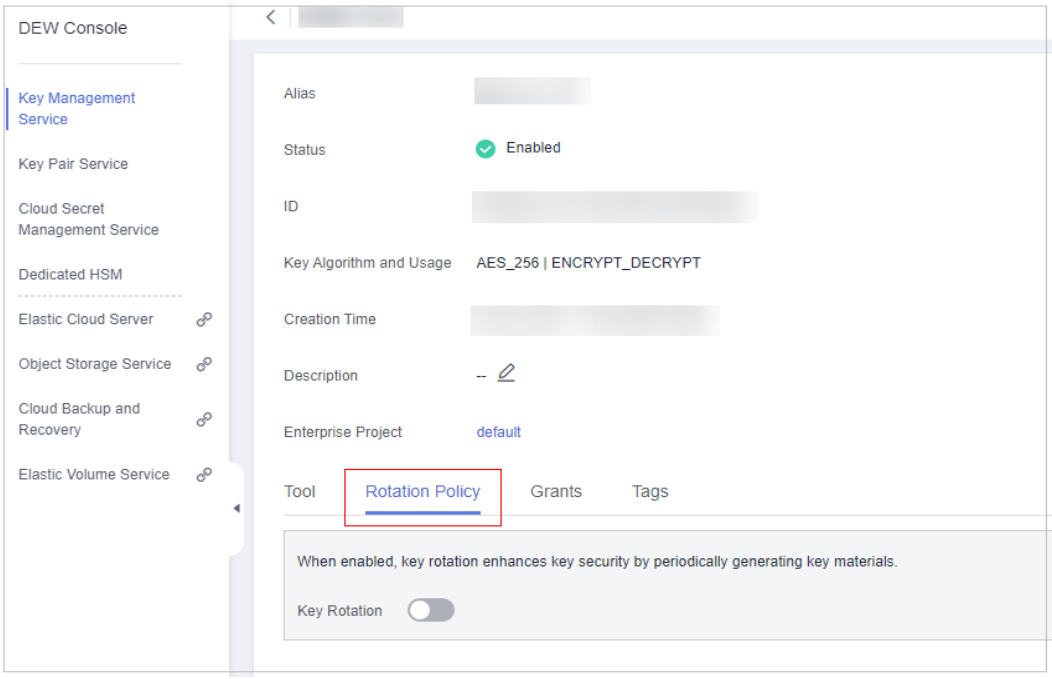
Paso 1 **Inicie sesión en la consola de gestión.**

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**.

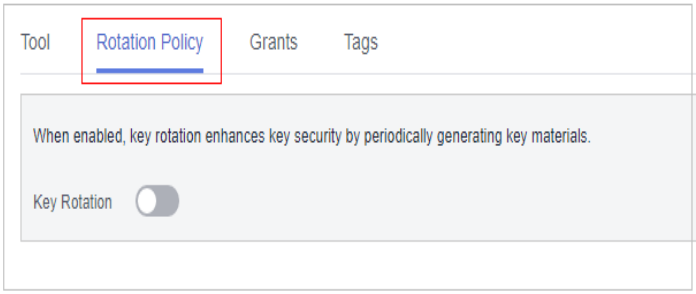
Paso 4 Haga clic en el alias del CMK deseado para ver sus detalles.

Figura 1-22 Detalles de CMK



Paso 5 Haga clic en la pestaña **Rotation Policy**. Se muestra el conmutador de rotación, como se muestra en **Figura 1-23**.

Figura 1-23 Rotación de CMK:



Paso 6 Haga clic en para habilitar la rotación de teclas.

Paso 7 Configure el período de rotación y haga clic en **OK**, como se muestra en **Figura 1-24**. Para obtener más información, consulte **Tabla 1-13**.

Figura 1-24 Habilitación de la rotación de clave

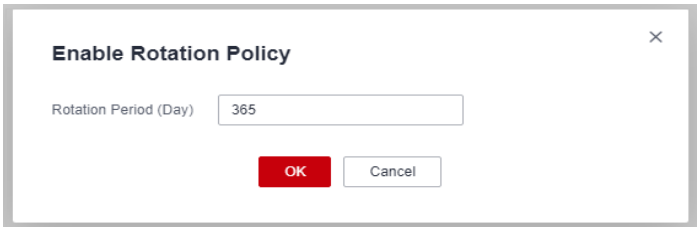
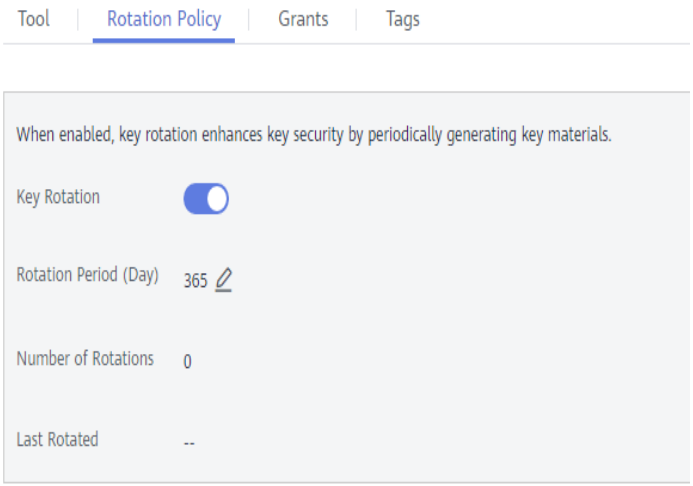


Tabla 1-13 Parámetros de rotación de clave

Parámetro	Descripción
Rotación de CMK:	Conmutador de rotación. El estado predeterminado es . : Dishabilitado : habilitado Después de activar la rotación, el CMK se rotará en función del período establecido. **NOTA** Un CMK deshabilitado nunca se rota, incluso si la rotación está habilitada para él. KMS reanuda la rotación cuando este CMK está habilitado. Si habilita esta CMK después de que haya pasado un período de rotación, KMS la rotará dentro de las 24 horas.
Rotation Period (day)	Período de rotación (día). El valor es un entero que oscila entre 30 y 365. El valor predeterminado es **365**. Configure el período en función de la frecuencia con la que se utilice un CMK. Si se utiliza con frecuencia, configure un período corto; de lo contrario, establezca uno largo.

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

Figura 1-25 Detalles de rotación CMK



NOTA

Puede hacer clic en para cambiar el período de rotación. Después de cambiar el período, KMS gira el CMK por el nuevo período.

----Fin

1.7.3 Deshabilitación de la rotación de clave

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

Prerrequisitos

- Ha obtenido una cuenta y su contraseña para iniciar sesión en la consola de gestión.
- La clave está habilitada.
- El **Origin** de la CMK 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.

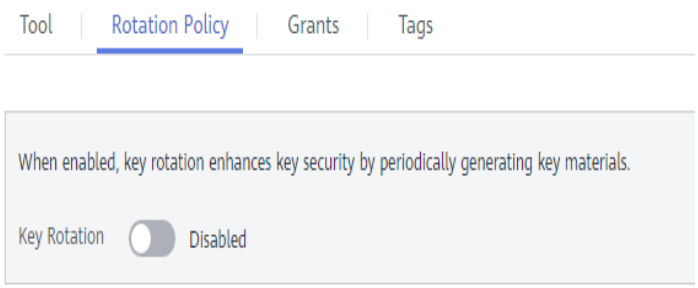
Paso 5 Haga clic en la pestaña **Rotation Policy**. Se muestra el interruptor de rotación, como se muestra en la siguiente figura.

Figura 1-26 Rotación de CMKs

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

Paso 7 Compruebe el estado de rotación, como se muestra en **Figura 1-27**.

Figura 1-27 Deshabilitación de la rotación de clave



----Fin

2 Cloud Secret Management Service

2.1 Creación de un Secreto

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**.

Prerrequisitos

Ha obtenido una cuenta y su contraseña para iniciar sesión en la consola de gestión.

Restricciones

- Un usuario puede crear un máximo de 200 credenciales.
- De forma predeterminada, la clave maestra predeterminada **csms/default** creada por CSMS se utiliza como la clave maestra de encriptación del secreto actual. También puede crear una clave 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.**

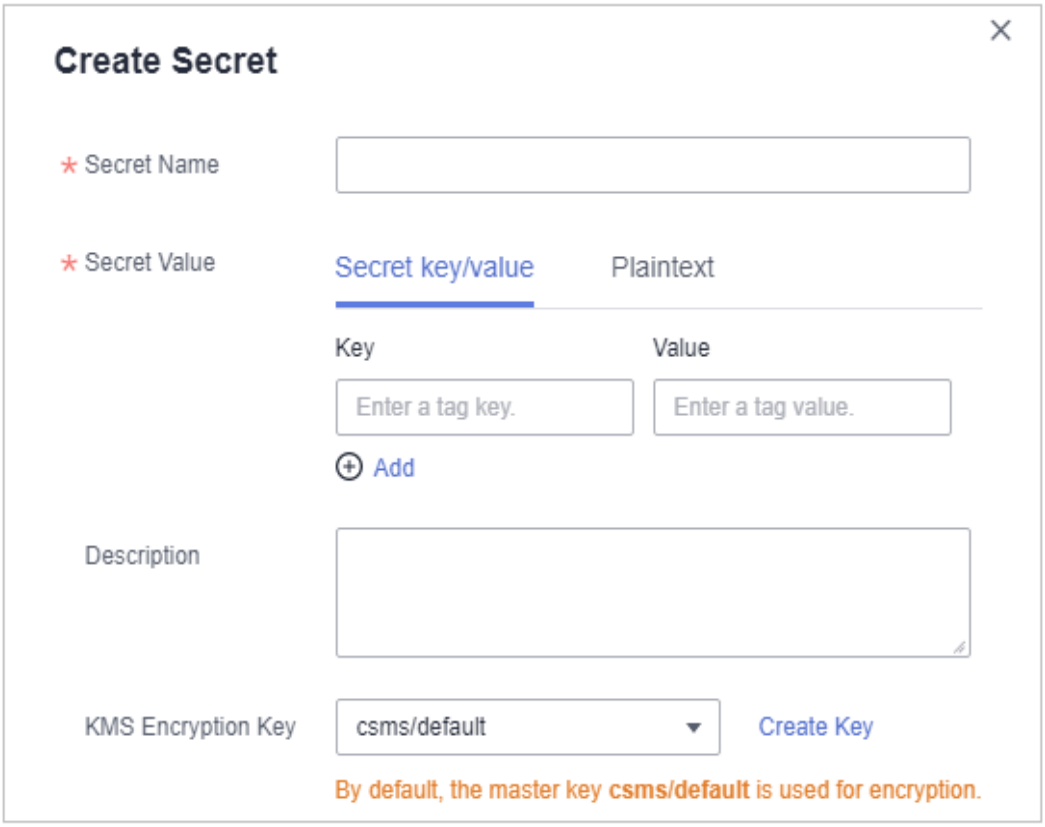
Paso 2 Haga clic en  en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

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

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

Paso 5 Haga clic en **Create Secret**.

Figura 2-1 Creación de un Secreto



Paso 6 En el cuadro de diálogo **Create Secret**, escriba el nombre secreto, el valor, la descripción y seleccione una clave de encriptación KMS.

- **Secret Name**: Ingresar un nombre secreto.
- **Secret Value**: Ingresar la clave/valor secreto o el secreto de texto sin formato.
- **Description**: Ingresar la descripción secreta.
- **KMS Encryption Key**: Seleccionar la clave predeterminada CMK **csms/default** o una clave definida por el usuario en KMS.

  NOTA

  De forma predeterminada, la clave maestra predeterminada **csms/default** creada por CSMS se utiliza como la clave maestra de encriptación del secreto actual. También puede crear una clave y utilizar una clave de encriptación definida por el usuario en la consola de KMS. Para más detalles, consulte **Creación de un CMK**.

Paso 7 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 la credencial puede ser **Enabled** o **Pending deletion**.

Prerrequisitos

Ha obtenido una cuenta y su contraseña para iniciar sesión en 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 . Elija **Security & Compliance** > **Data Encryption Workshop**.

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

Paso 5 Revise la lista secreta. Para obtener más información, consulte **Tabla 2-1**.

Figura 2-2 Lista de secretos

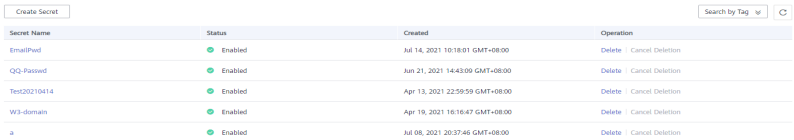
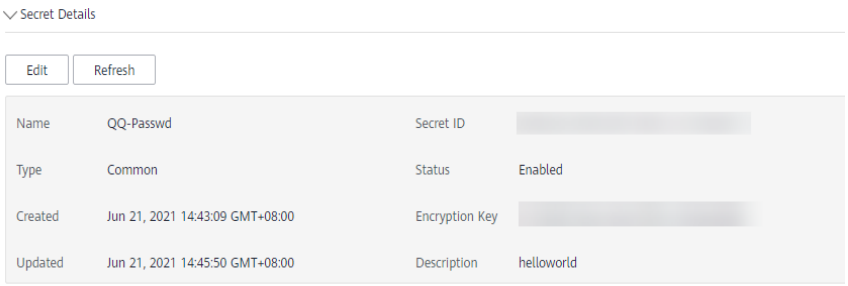


Tabla 2-1 Parámetros de lista secreta

Parámetro	Descripción
Secret Name	Nombre de secreto
Status	Estado de secreto. Puede ser: ● **Enabled** El secreto está habilitado. ● **Pending deletion** El secreto está a la espera de ser eliminado.
Created	Tiempo en que se crea un secreto
Operation	Puede programar o cancelar la eliminación de un secreto en la columna **Operation**.

Paso 6 Haga clic en un secreto para ver sus detalles. Consulte **Figura 2-3**.

Figura 2-3 Detalles de secretos



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 Eliminación de un secreto

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

Prerrequisitos

- Ha obtenido una cuenta y su contraseña para iniciar sesión en la consola de gestión.
- 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.
- Si elige eliminar un secreto inmediatamente, no se puede restaurar. Tenga cuidado al realizar esta operación.

Procedimiento

Paso 1 **Inicie sesión en la consola de gestión.**

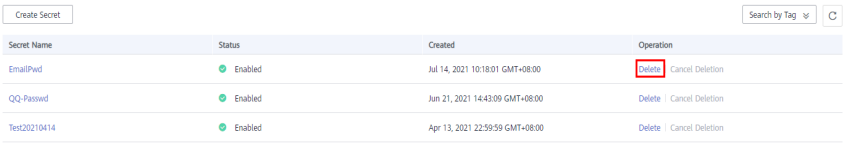
Paso 2 Haga clic en en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

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

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

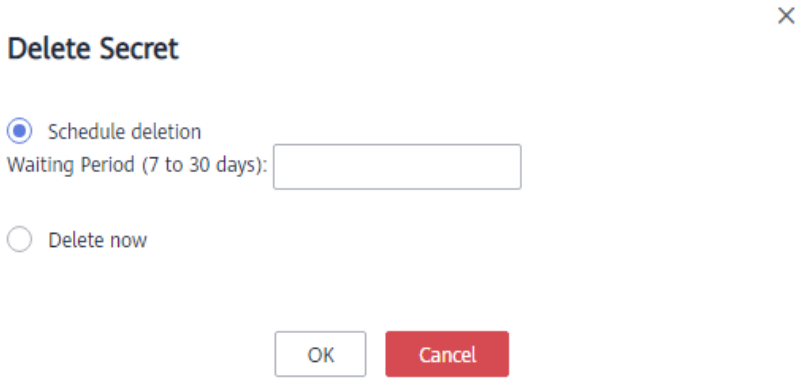
Paso 5 En la fila de un secreto, haga clic en **Delete**.

Figura 2-4 Eliminación de un secreto



Paso 6 En el cuadro de diálogo que se muestra, haga clic en **Schedule deletion** o **Delete now**.

Figura 2-5 Eliminación de un secreto



Paso 7 Haga clic en **OK**.

NOTA

- 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.
- Si elige eliminar un secreto inmediatamente, no se puede restaurar. Tenga cuidado al realizar esta operación.

----Fin

2.3 Gestión de versiones de secreto

2.3.1 Gestión de valores de 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**.

Prerrequisitos

Ha obtenido una cuenta y su contraseña para iniciar sesión en la consola de gestión.

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.

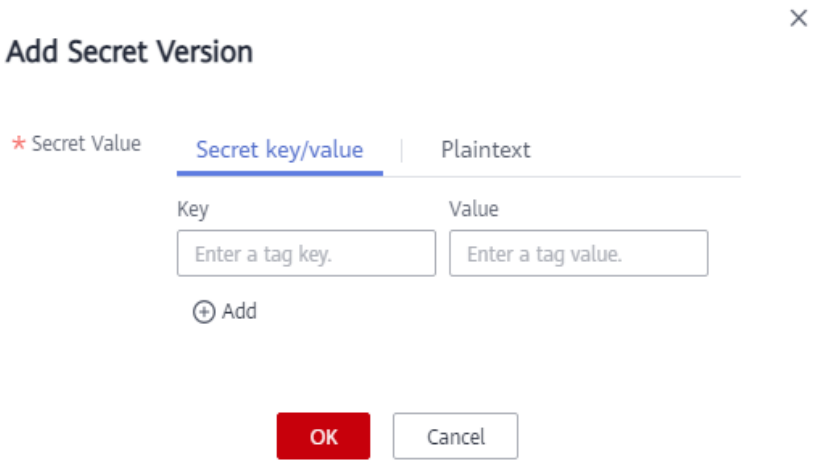
Paso 3 Haga clic en . Elija **Security & Compliance** > **Data Encryption Workshop**.

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 2-6 Adición de un valor de secreto

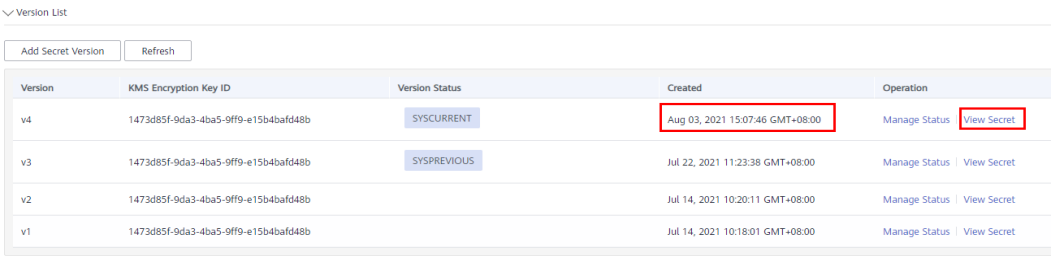


Paso 7 Haga clic en **OK**. Se muestra un mensaje en la esquina superior derecha de la página, indicando que el valor se ha añadido correctamente.

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

Paso 8 En el área **Version List**, haga clic en **View Secret** en la columna **Operation** de un secreto.

Figura 2-7 Lista de versiones secreta



Paso 9 En el cuadro de diálogo **View Secret**, haga clic en **Yes**.

NOTA

Los valores secretos generalmente se obtienen a través de APIs. La comprobación de los valores en la consola conlleva riesgos de seguridad.

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

----Fin

2.3.2 Gestión de estados de versión secreta

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

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

Prerrequisitos

Ha obtenido una cuenta y su contraseña para iniciar sesión en la consola de gestión.

Restricciones

- La versión inicial se marca con la etiqueta de estado **SYSCURRENT**.
- Puede marcar una versión con etiquetas preconfiguradas o definidas por el usuario. 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.

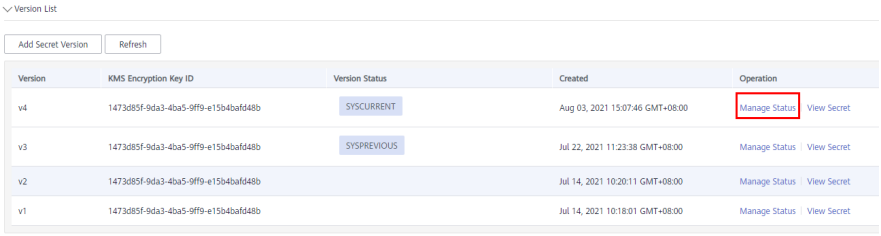
Paso 3 Haga clic en  . Elija **Security & Compliance** > **Data Encryption Workshop**.

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.

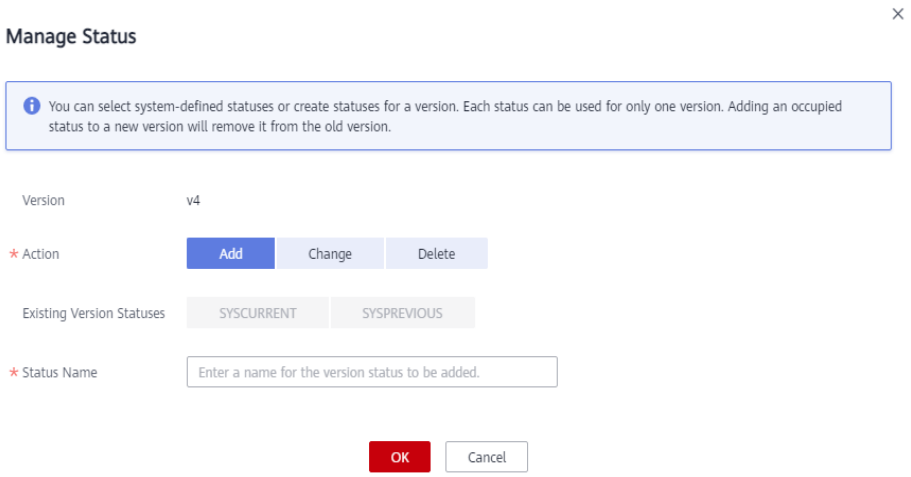
Paso 6 En el área **Version List**, haga clic en **Manage Status** en la columna **Operation**.

Figura 2-8 Lista de versiones secreta



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

Figura 2-9 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

2.4 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.

Prerrequisitos

Ha obtenido una cuenta y su contraseña para iniciar sesión en 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.

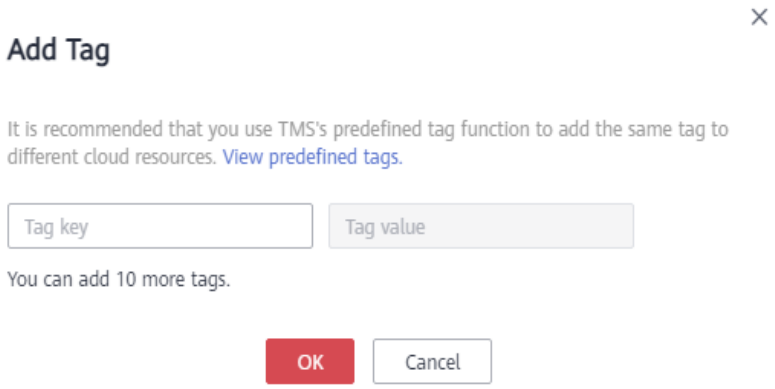
Paso 3 Haga clic en . Elija **Security & Compliance** > **Data Encryption Workshop**.

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 2-2** describe los parámetros.

Figura 2-10 Agregar 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 2-2 Parámetros de etiqueta

Parámetro	Descripción	Comentarios
Tag key	Nombre de la etiqueta. Las claves de etiqueta de un secreto no pueden tener valores duplicados. Se puede usar una clave de etiqueta para múltiples secretos. Un secreto puede tener hasta 10 etiquetas.	● Obligatorio. ● Las claves de etiqueta de un secreto no pueden tener valores duplicados. ● Límite de 36 caracteres. ● Se permiten los siguientes tipos de caracteres: – Letras en mayúscula – Letras en minúscula – Números – Caracteres especiales, incluyendo guiones (-) y guiones bajos (_) – Caracteres chinos
Tag value	Valor de la etiqueta	● Opcional ● Límite de 43 caracteres. ● Se permiten los siguientes tipos de caracteres: – Letras en mayúscula – Letras en minúscula – Números – Caracteres especiales, incluyendo guiones (-) y guiones bajos (_) – Caracteres chinos

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

- Ha obtenido una cuenta y su contraseña para iniciar sesión en la consola de gestión.
- 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 . Elija **Security & Compliance** > **Data Encryption Workshop**.

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

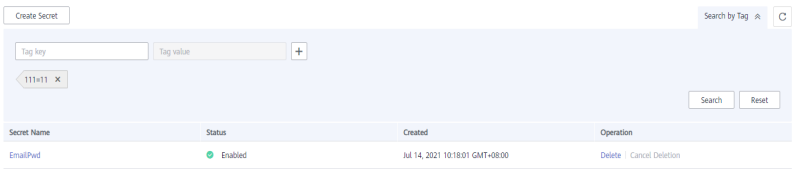
Paso 5 Haga clic en **Search by Tag** para mostrar el cuadro de búsqueda.

Figura 2-11 Cuadro de búsqueda

Paso 6 En el cuadro de búsqueda, escriba o seleccione una clave de etiqueta y un valor de etiqueta.

Paso 7 Haga clic en para agregar la entrada a los criterios de búsqueda y haga clic en **Search**.

Figura 2-12 Resultados de la búsqueda



NOTA

- Se pueden agregar varias etiquetas para una búsqueda. Se puede añadir un máximo de 10 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.

Prerrequisitos

Ha obtenido una cuenta y su contraseña para iniciar sesión en 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.

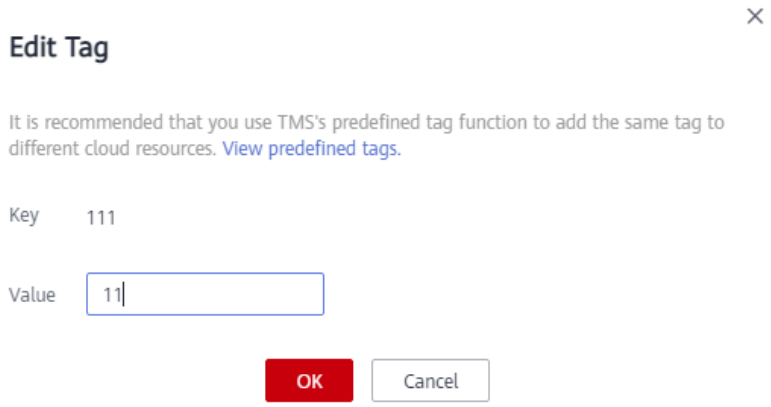
Paso 3 Haga clic en . Elija **Security & Compliance** > **Data Encryption Workshop**.

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 **Edit**.

Figura 2-13 Edición de una etiqueta



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.

Prerrequisitos

Ha obtenido una cuenta y su contraseña para iniciar sesión en 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.

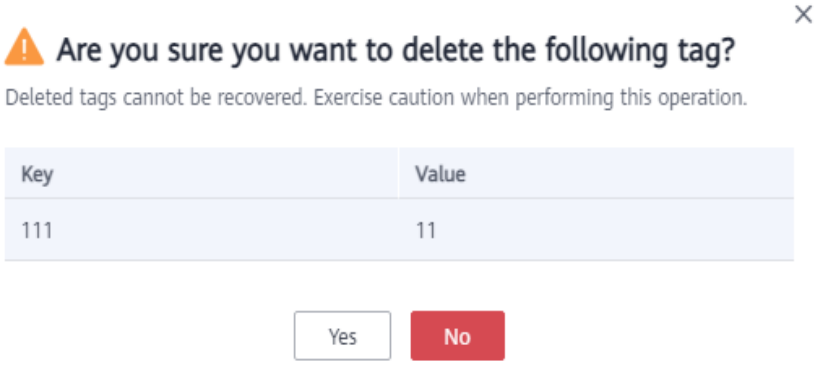
Paso 3 Haga clic en . Elija **Security & Compliance** > **Data Encryption Workshop**.

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**.

Figura 2-14 Eliminación de una etiqueta



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

----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 según sus necesidades. Huawei Cloud utiliza claves de encriptación proporcionadas por KMS para cifrar sus claves privadas y garantizar un almacenamiento y acceso seguros. Para más detalles, consulte **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 más detalles, consulte **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

Ha obtenido el nombre de usuario y la contraseña para iniciar sesión en la consola de gestión, y se ha vinculado al usuario un método de pago.

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.

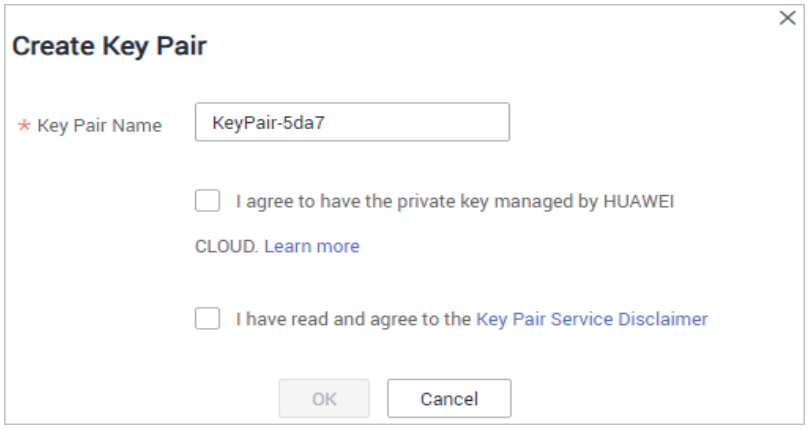
Paso 3 Haga clic en . Elija **Security & Compliance** > **Data Encryption Workshop**.

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.

Figura 3-1 Creación de un par de claves

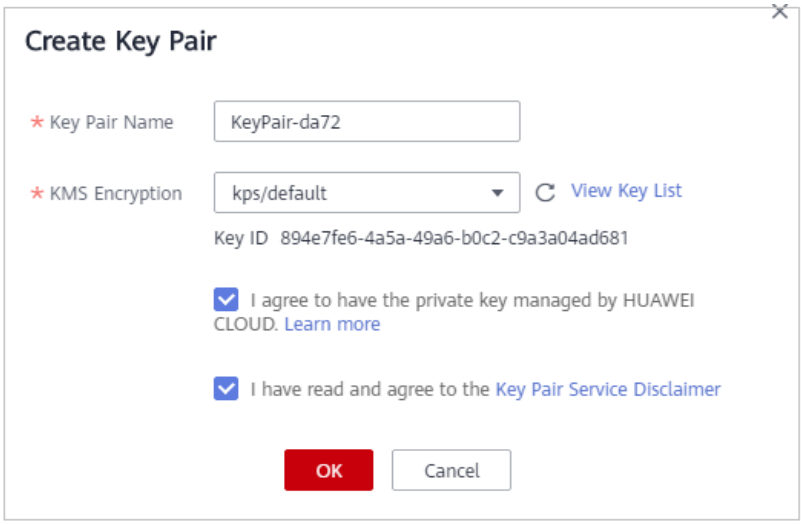


Paso 7 Si desea que su clave privada sea administrada por Huawei Cloud, lea y confirme **I agree to have the private key managed by HUAWEI CLOUD**. Seleccione una clave de encriptación en el cuadro de lista desplegable de **KMS encryption**. Omita este paso si no necesita tener la clave privada gestionada por Huawei Cloud.

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.
- 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



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**. El navegador descarga automáticamente la clave privada. Cuando se descarga la clave privada, se muestra un cuadro de diálogo.

Paso 10 Guarde la clave privada según lo indique el cuadro de diálogo.

AVISO

- Si la clave privada no es gestionada por Huawei Cloud, solo se puede descargar una vez. Mantener en buen estado. 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 11 Después de guardar la clave privada, haga clic en **OK**. El par de claves se crea correctamente.

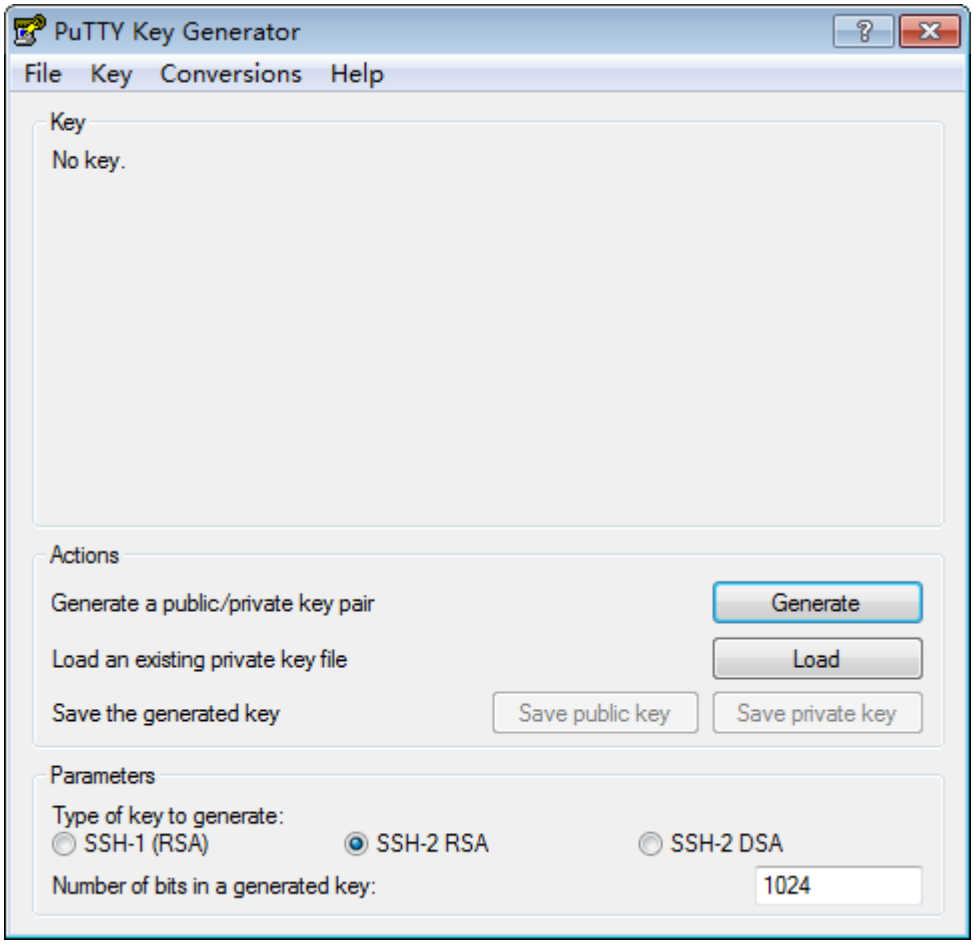
Después de crear el par de claves, puede verlo en la lista de pares de claves. La lista muestra información como el nombre del par de claves, la huella dactilar, la clave privada y la cantidad.

----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 **Tabla 3-1**.

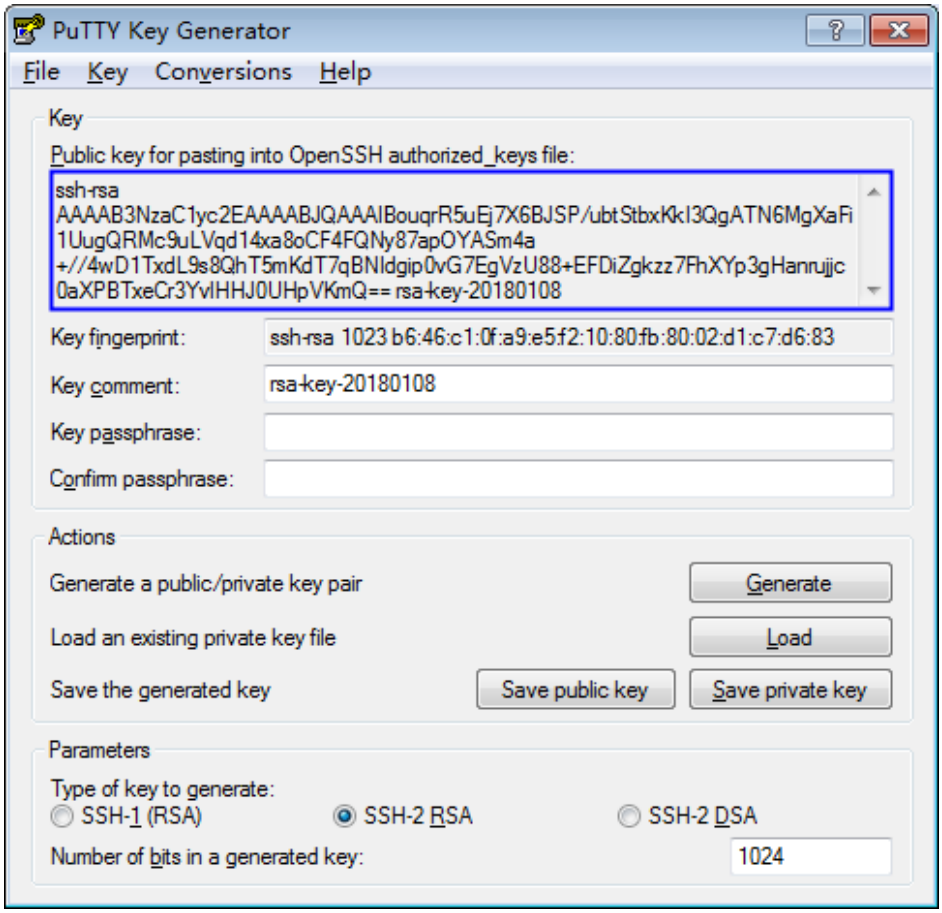
Tabla 3-1 Descripción del parámetro

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

Paso 3 Haga clic en **Generate** para generar una clave pública y una clave privada. Consulte **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. Guárdela en un lugar 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	● 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.	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.	1. Choose **Conversions** > **Export OpenSSH key**. **NOTA** No introduzca la información de **Key passphrase**. De lo contrario, no se puede obtener la contraseña. 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.	1. En la página de **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 utilizar su propio par de claves (por ejemplo, usar 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.

Restricciones

- Los algoritmos de encriptación y desencriptación compatibles de los pares de claves importados son los siguientes:
  - SSH-2 (RSA, 1024)
  - SSH-2 (RSA, 2048)
  - SSH-2 (RSA, 4096)
- 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.

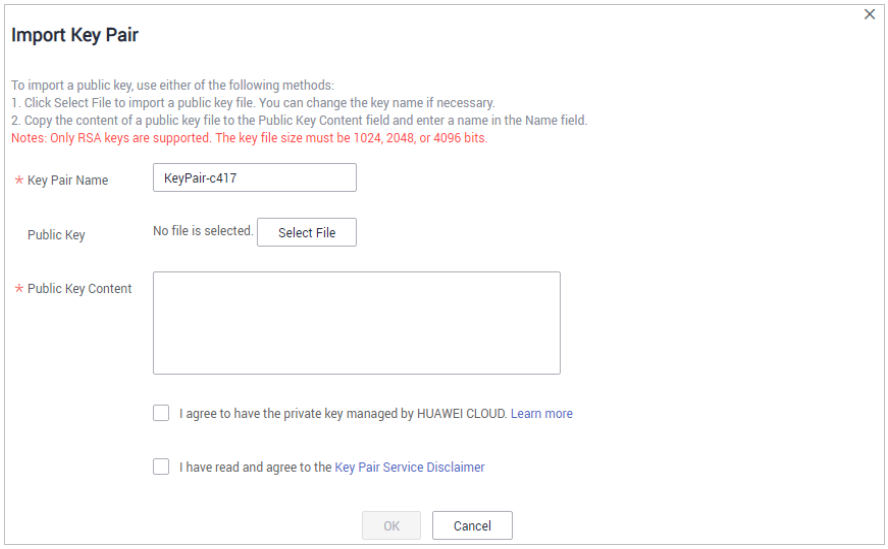
Paso 3 Haga clic en . Elija **Security & Compliance** > **Data Encryption Workshop**.

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**.

Figura 3-5 Importación de un par de claves

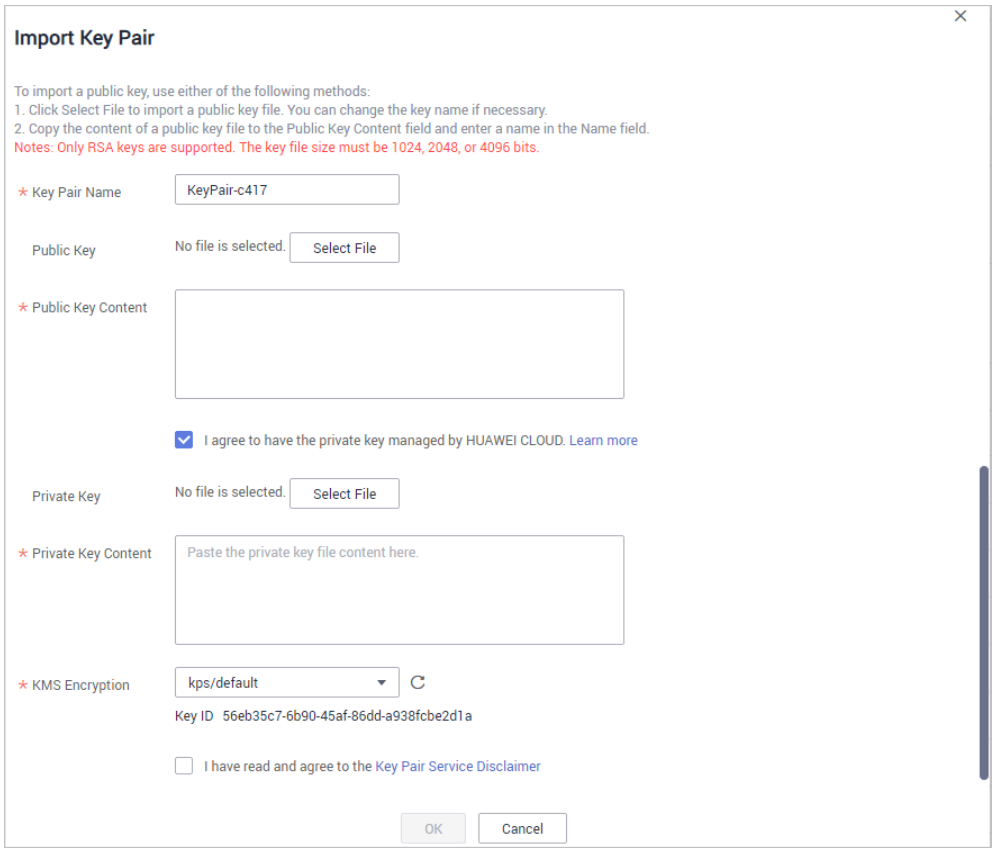


NOTA

Puede personalizar el nombre de un par de claves importadas.

Paso 7 Si desea que su clave privada sea administrada por Huawei Cloud, lea y confirme **I agree to have the private key managed by HUAWEI CLOUD**. Omita este paso si no necesita tener la clave privada gestionada por Huawei Cloud.

Figura 3-6 Alojamiento de la clave privada en Huawei Cloud



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.
- 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.

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.

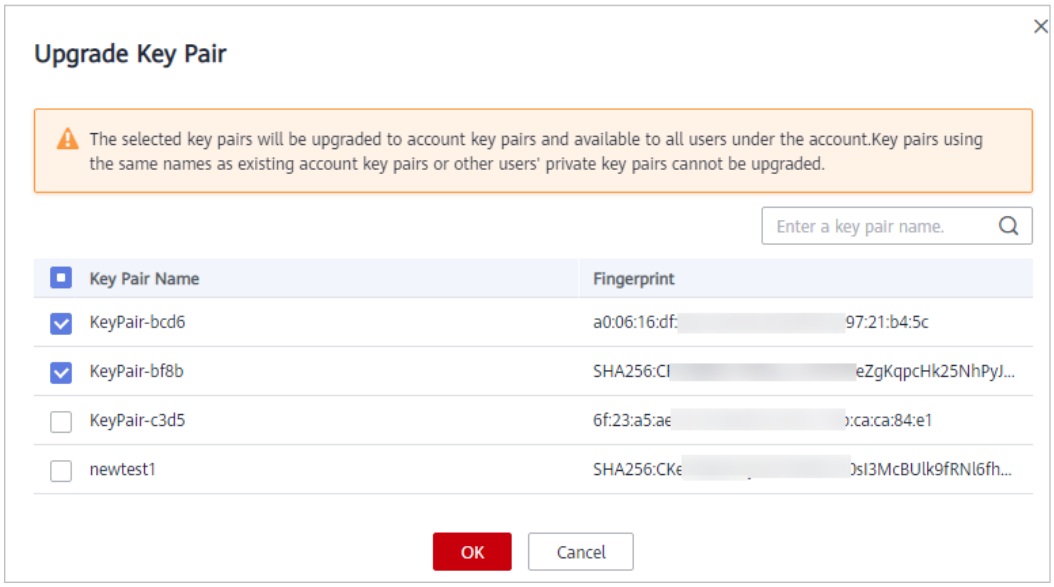
Paso 3 Haga clic en . Elija **Security & Compliance** > **Data Encryption Workshop**.

Paso 4 En 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 aparece, 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 el sistema operativo Linux, puede vincular un par de claves al ECS en la consola KPS. KPS configurará el par de claves para el ECS, y luego el modo de inicio de sesión de ECS se cambiará a **Key Pair**. Después de vincular 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 ECS que ejecutan el sistema operativo 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**.

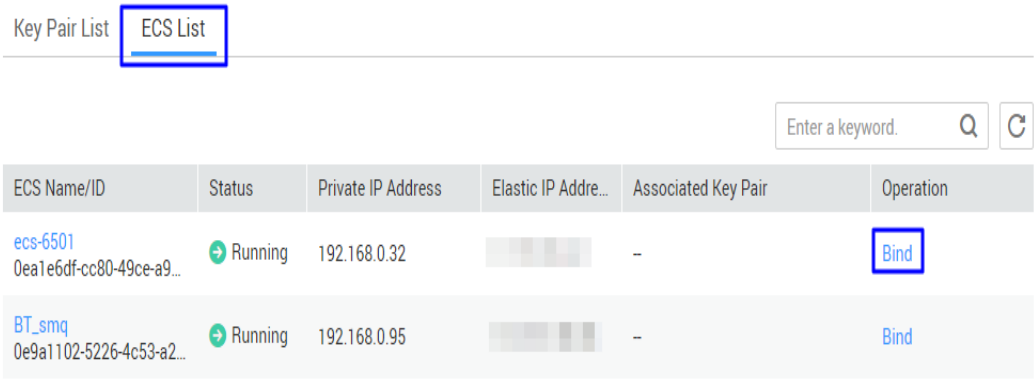
Paso 2 Haga clic en  en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

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

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**.

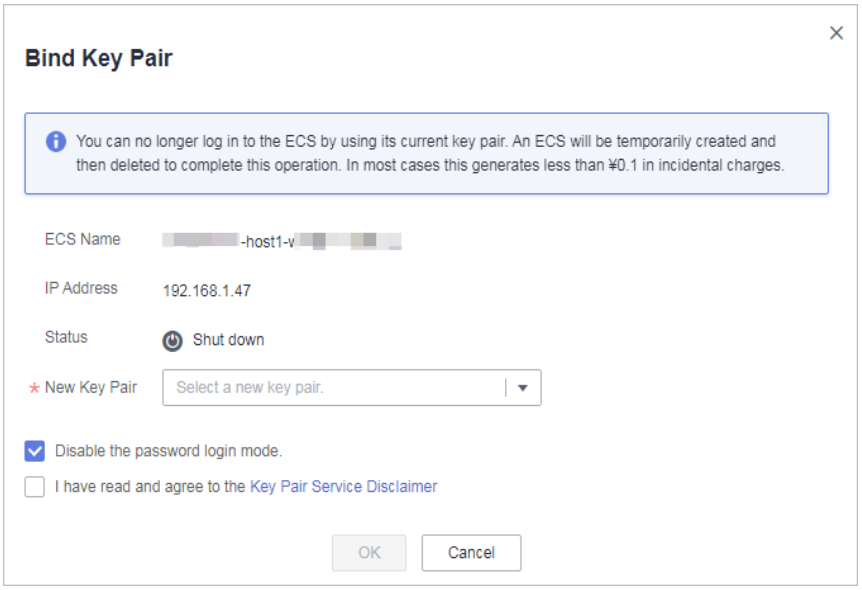
Figura 3-8 Vinculación



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

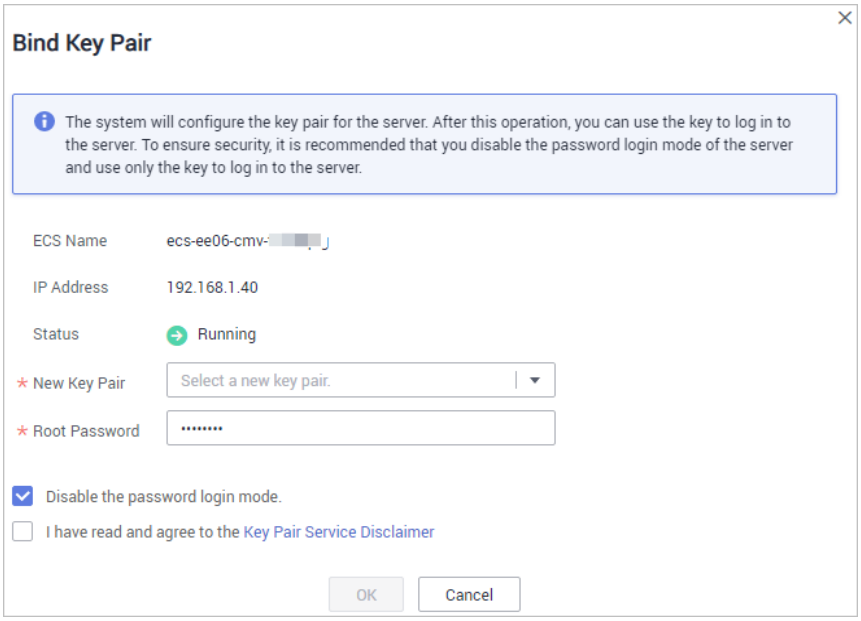
- Si el ECS está apagado, se mostrará un cuadro de diálogo, como se muestra en **Figura 3-9**.

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



- Si el ECS se está ejecutando, debe proporcionar la contraseña de root. Consulte **Figura 3-10**.

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



NOTA

- Si tiene la contraseña de root del ECS, puede ingresar directamente la contraseña para vincular el par de claves al ECS.
- Si no tiene la contraseña de root 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 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 el 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 9 Seleccione **I have read and agree to the Key Pair Service Disclaimer**.

Paso 10 Haga clic en **OK** para completar la operación.

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

----Fin

3.4.2 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.

Prerrequisitos

Ha obtenido una cuenta y su contraseña para iniciar sesión en 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 . Elija **Security & Compliance** > **Data Encryption Workshop**.

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

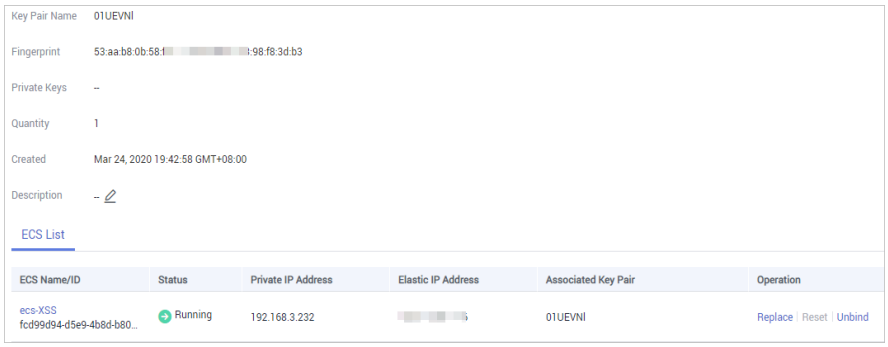
Paso 5 Verifique la información del par de claves en la lista.

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 ECS que usan el par de claves. Consulte **Figura 3-11** para obtener más detalles.

Figura 3-11 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.

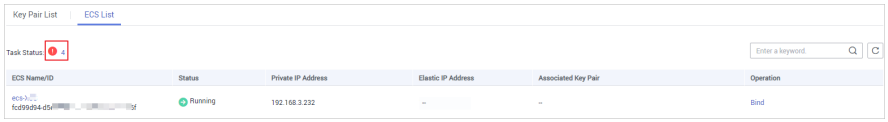
Vincular un par de claves a los ECS. Para obtener más información sobre los parámetros, consulte **Tabla 3-3**.

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: ● Running ● Creating ● Faulty ● Shut down ● DELETE ● HARD_REBOOT ● MIGRATING ● REBOOT ● RESIZE ● REVERT_RESIZE ● SHELVED ● SHELVED_OFF ● LOADED ● UNKNOWN ● VERIFY_RESIZE
Private IP address	Dirección IP privada
EIP	Dirección IP elástica
Bound key pair	Par de claves enlazadas al ECS

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

Figura 3-12 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 3-13**.

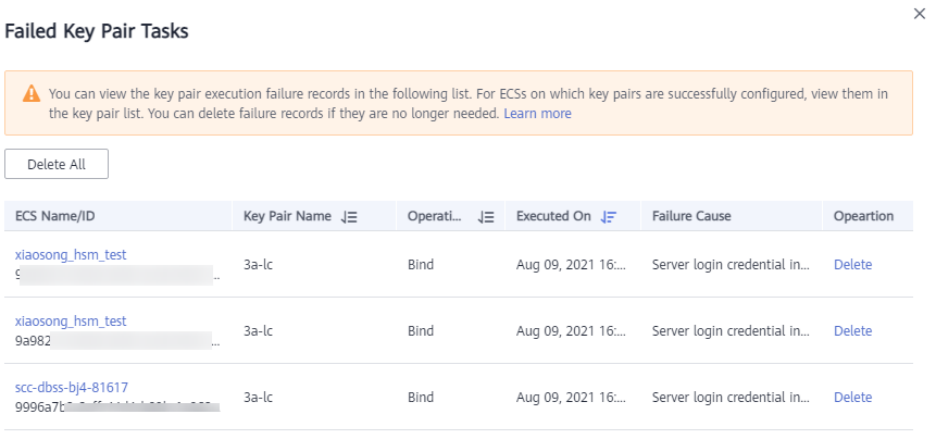
NOTA

Estado de reinicio o sustitución del par de claves:

: En ejecución

: Error en la ejecución

Figura 3-13 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

3.4.3 Restablecimiento de un par de claves

Si se pierde su clave privada, puede utilizar un nuevo par de claves para volver a configurar 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.

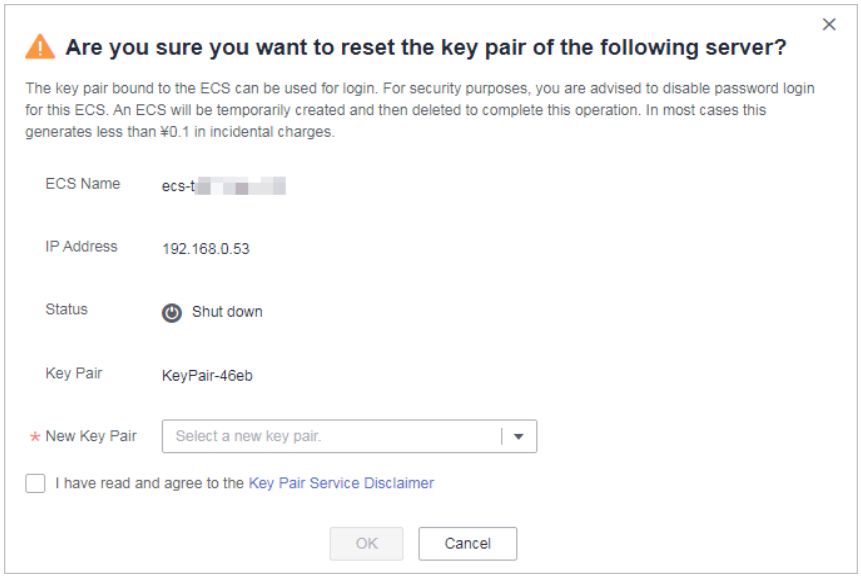
Paso 3 Haga clic en . Elija **Security & Compliance** > **Data Encryption Workshop**.

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.

Figura 3-14 Restablecimiento de un par de claves



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

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

Paso 9 Haga clic en **OK**. El par de claves ECS se restablecerá en unos 10 minutos.

----Fin

3.4.4 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/autorized_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.

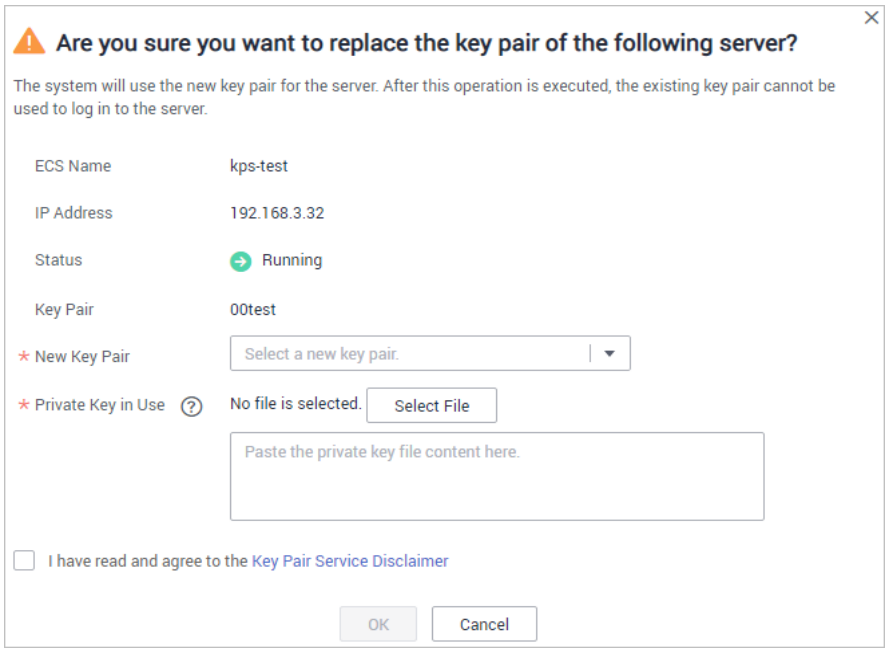
Paso 3 Haga clic en . Elija **Security & Compliance** > **Data Encryption Workshop**.

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.

Figura 3-15 Sustitución de un par de claves



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 in**.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 el formato**.ppk**, conviértelo haciendo referencia a **¿Cómo convierto el formato de un archivo de clave privada?**

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

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

----Fin

3.4.5 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 del ECS a través de la consola de gestión. El KPS desvinculará el par de claves del ECS. Después de que el par de claves esté desvinculado, 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 unido 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 ECS de su par de claves, para enlazar un 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 de 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  . Elija **Security & Compliance** > **Data Encryption Workshop**.

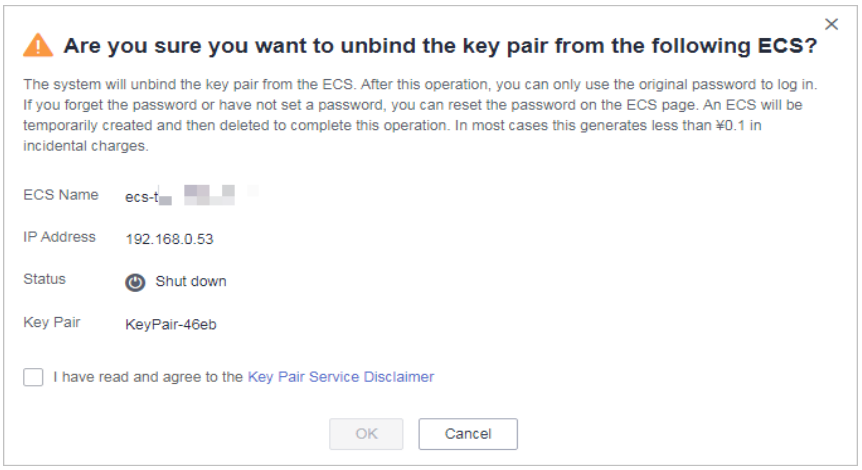
Paso 4 En el panel de navegación de la izquierda, haga clic en **Key Pair Service**.

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

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

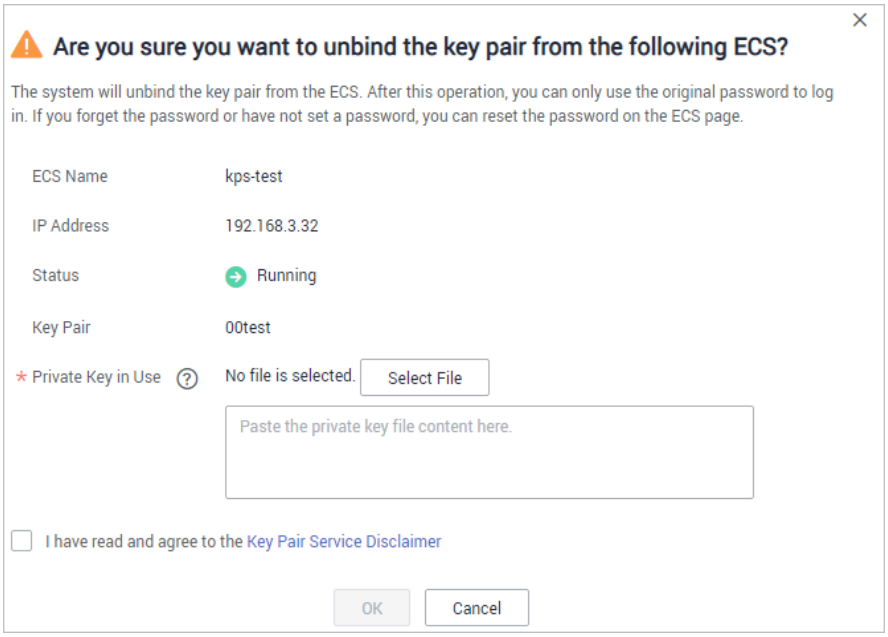
- Si el ECS está apagado, se mostrará un cuadro de diálogo, como se muestra en **Figura 3-16**.

Figura 3-16 Desvinculación de un par de claves (1)



- Si el ECS se está ejecutando, se mostrará un cuadro de diálogo, como se muestra en **Figura 3-17**.

Figura 3-17 Desvinculación de un par de claves (2)



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 el formato**.ppk**, conviértelo haciendo referencia a **¿Cómo convierto el formato de un archivo de clave privada?**

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

Paso 9 Haga clic en **OK**. El par de claves se separará del ECS en aproximadamente un minuto.

NOTA

Después de que el par de claves se desvincule del ECS, restablezca la contraseña para el inicio de sesión en la consola de ECS a tiempo. Para obtener más información, consulte la *Guía del usuario de Elastic Cloud Server*.

----Fin

3.4.6 Eliminación de un par de claves

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

Esta sección describe cómo eliminar un par de claves 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 de KMS y la clave privada se ha guardado localmente, puede usar 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  . Elija **Security & Compliance** > **Data Encryption Workshop**.

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, 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 el formato**.ppk**, conviértelo haciendo referencia a **¿Cómo convierto el formato de un archivo de clave privada?**
- Cuando habilita la función de encriptación KMS para un par de claves, KMS crea automáticamente una clave maestra 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**.

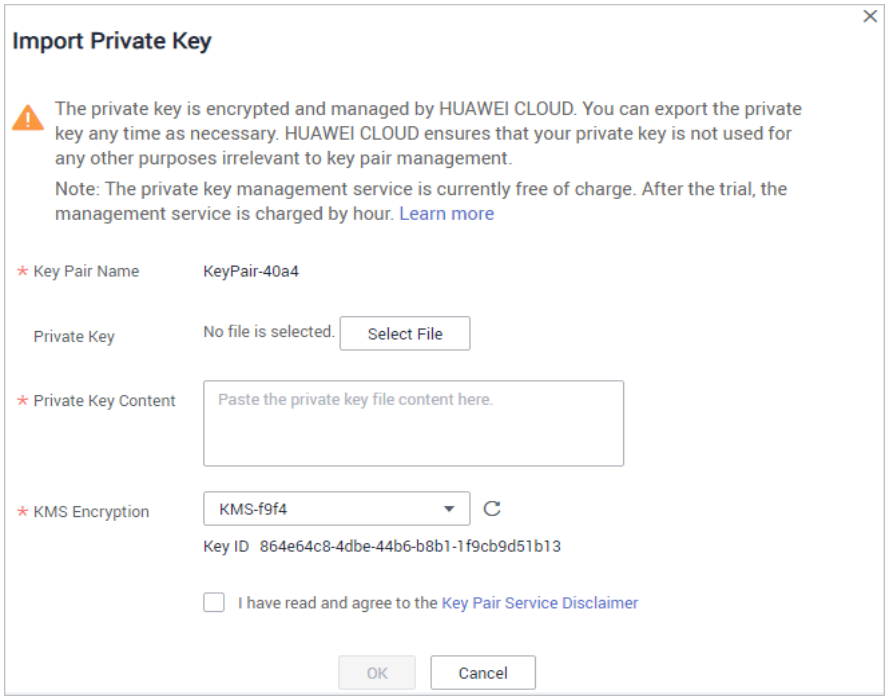
Paso 2 Haga clic en  en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

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

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 los parámetros en el cuadro de diálogo **Import Private Key**.

Figura 3-18 Importación de una clave privada



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

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

NOTA

- Cuando habilita la función de encriptación KMS para un par de claves, KMS crea automáticamente una clave maestra 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 Huawei Cloud, puede descargarlas 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**.

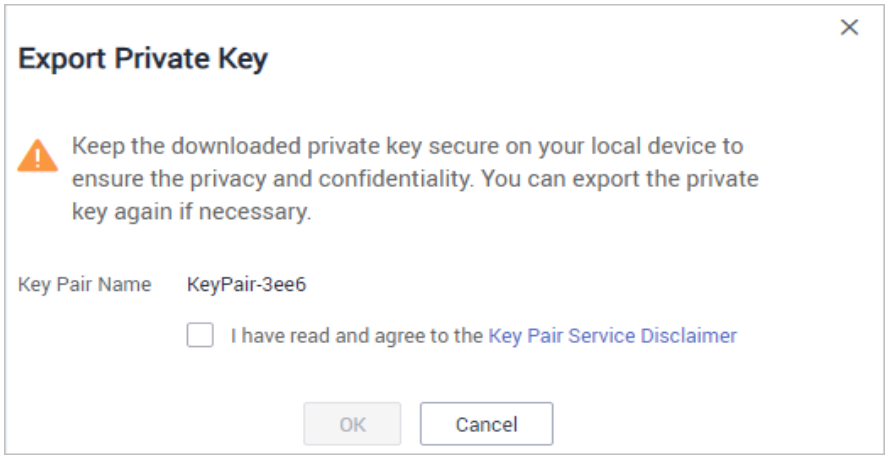
Paso 2 Haga clic en en la esquina superior izquierda de la consola de gestión y seleccione una región o proyecto.

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

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 3-19**.

Figura 3-19 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 en Huawei Cloud ya no son necesarias, puede borrar las claves privadas gestionadas en la consola 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 al realizar esta operación. Si necesita tener la clave privada gestionada en Huawei Cloud de nuevo, puede importar la clave privada 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  . Elija **Security & Compliance** > **Data Encryption Workshop**.

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 al realizar esta operación. Si necesita tener la clave privada gestionada en Huawei Cloud de nuevo, puede importar la clave privada 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 a la 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 Seleccione **Connection** > **Data**. Ingrese el nombre de usuario de la imagen en **Auto-login username**.

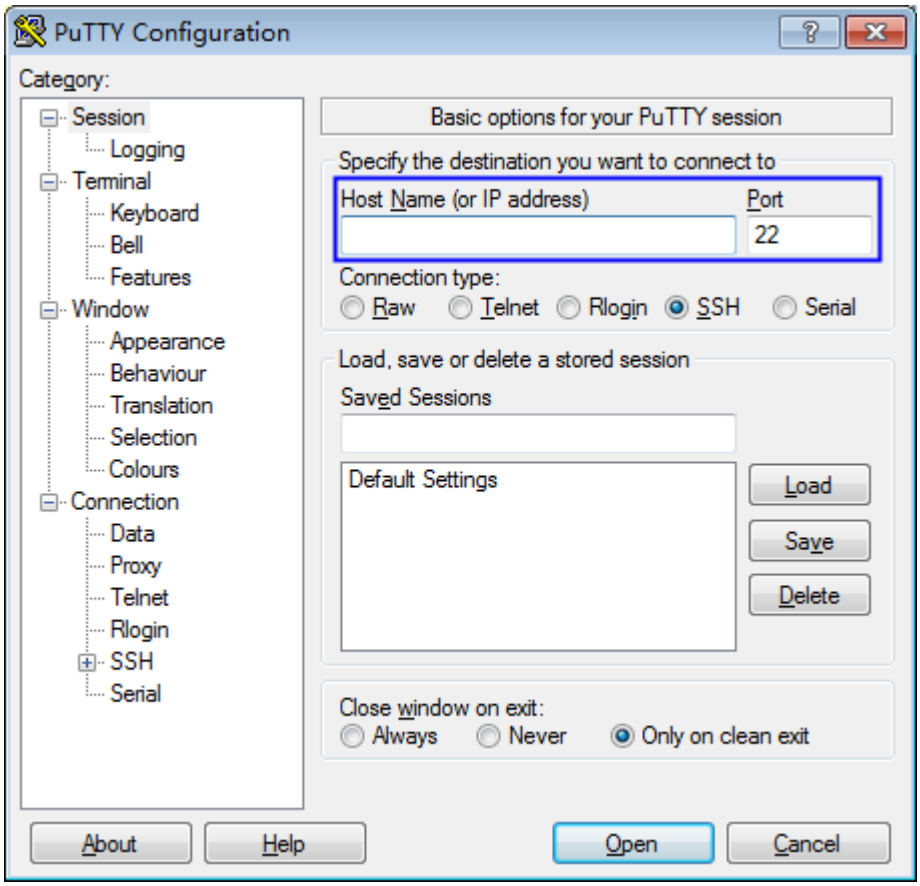
NOTA

- 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 el EIP del ECS en **Host Name (or IP address)**.

Figura 3-20 Configuración del 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 ordenador Linux

Para iniciar sesión en el ECS de Linux desde un equipo Linux, realice las operaciones descritas 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 inicial de la contraseña no afecta al funcionamiento de ECS ni al inicio de sesión. Una vez borrada, la contraseña no se puede restaurar. Antes de eliminar una contraseña, se recomienda registrarla. Para obtener más información, consulte la *Guía del usuario de Elastic Cloud Server*.
- También puede llamar 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 ECS debe estar en formato **.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 **Computing**, haga click en **Elastic Cloud Server**.

Paso 3 En la lista ECS, seleccione el ECS cuya contraseña desea obtener.

Paso 4 En la columna **Operation**, haga clic en **More** y elija **Get Password**.

Paso 5 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 6 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 comprar 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 comprar instancias HSM dedicadas a través de la consola de gestión. Después de comprar 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

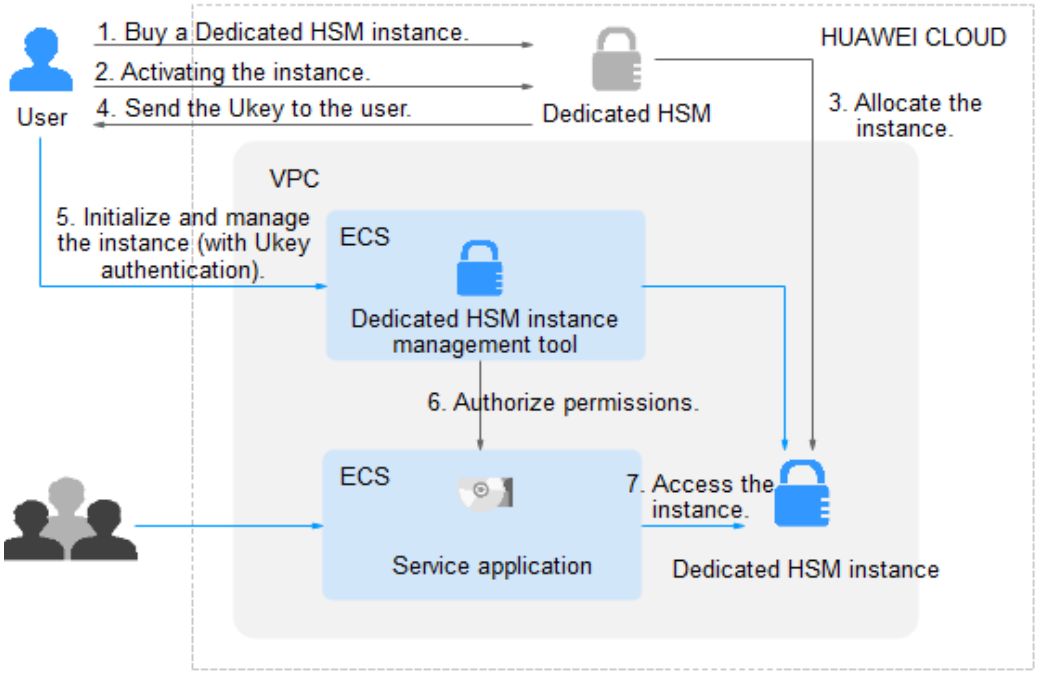


Tabla 4-1 describe la guía de operación.

Tabla 4-1 Descripciones de la guía de operación

No.	Procedimiento	Descripción	Gestionado por
1	Cree 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	Active 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 más detalles, consulte **Activación de una instancia HSM dedicada**.	Usuario

No.	Procedimiento	Descripción	Gestionado por
3	Asigne una instancia HSM dedicada.	Una instancia comprada se asignará al usuario. 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 en seguridad HSM
4	Proporcione el UKey, la guía de inicialización y el software.	● 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. Mantener en buen estado. ● 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.	Experto dedicado en seguridad HSM
5	Inicializar y gestionar instancias (involucrado la autenticación UKey).	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. Para más detalles, consulte **Inicialización de una instancia HSM dedicada**.	Usuario
6	Instale el agente de seguridad y la concesión de permisos de acceso.	Instale e inicialice el agente de seguridad en los nodos de aplicaciones de servicio. Para más detalles, consulte **Instalación del agente de seguridad y concesión de permisos de acceso**.	Usuario
7	Acceda 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 HSM dedicada

4.2.1 Ediciones

HSM dedicado proporciona instancias de la edición platino. Para más detalles, consulte **Tabla 4-2**.

Tabla 4-2 HSM dedicado

Edición	Modo de facturación	Alcance del servicio
Platino	Anual/ Mensual	● Chip exclusivo para encriptación Le proporciona chips exclusivos para la encriptación de datos en la nube, lo que garantiza el aislamiento del hardware mientras mantiene el rendimiento de su servicio. ● Soporte total del servicio Admite la seguridad de las aplicaciones, como el pago financiero, la autenticación de identidad y la firma digital, que cumple con los estrictos requisitos de seguridad de los datos y del sistema. ● Escalable Le permite agregar y reducir de forma fácil y flexible recursos informáticos de contraseñas en función de sus necesidades de servicio. ● Altamente confiable Las instancias de dispositivos de hardware se virtualizan en clústeres para lograr un equilibrio de carga y una alta confiabilidad. ● Compatibilidad Proporciona las mismas funciones y API que los dispositivos criptográficos físicos, lo que facilita la migración a la nube con soporte para PKCS#11 y CSP APIs. ● Algoritmos comunes – Algoritmo simétrico: DES y AES – Algoritmo de resumen: SHA1, SHA256 y SHA384 – Algoritmo asimétrico: RSA, DSA, ECDSA, DH y ECDH. ● Subrack exclusivo y fuente de alimentación Le proporciona un subrack HSM exclusivo y una fuente de alimentación. ● Red dedicada Proporciona ancho de banda de red dedicado y recursos de API. ● Certificación FIPS 140-2 Utiliza FIPS 140-2 nivel 3 certificado HSM para generar claves de encriptación.

4.2.2 Creación de una instancia HSM dedicada

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

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

- Tarifa de instalación inicial, cobrada al crear una instancia dedicada de HSM.
- Cuota anual/mensual, cobrada cuando **Activación de una instancia HSM dedicada**.

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

- When purchasing a Dedicated HSM instance, you need to submit a service ticket to set the UKey recipient information. Only the accounts with the **Ticket Administrator** permission can submit service tickets.
- Después de crear una instancia, un UKey será enviado 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 Click . Choose **Security & Compliance** > **Data Encryption Workshop**.

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 the current region.

Figura 4-3 Selecting a region

Paso 8 Seleccione la edición de servicio para la instancia. **Tabla 4-3** enumera los parámetros relacionados.

Tabla 4-3 Parámetros de edición

Parámetro	Descripción
Service Edition	Edición platino
Encryption Algorithm	Algoritmo de cifrado soportado por la instancia de HSM. ● Algoritmo simétrico: AES ● Algoritmo asimétrico: RSA, DSA, ECDSA, DE y ECDH ● Algoritmo de resumen: SHA1, SHA256, SHA384
Certification	Certificación FIPS 140-2 Nivel 3

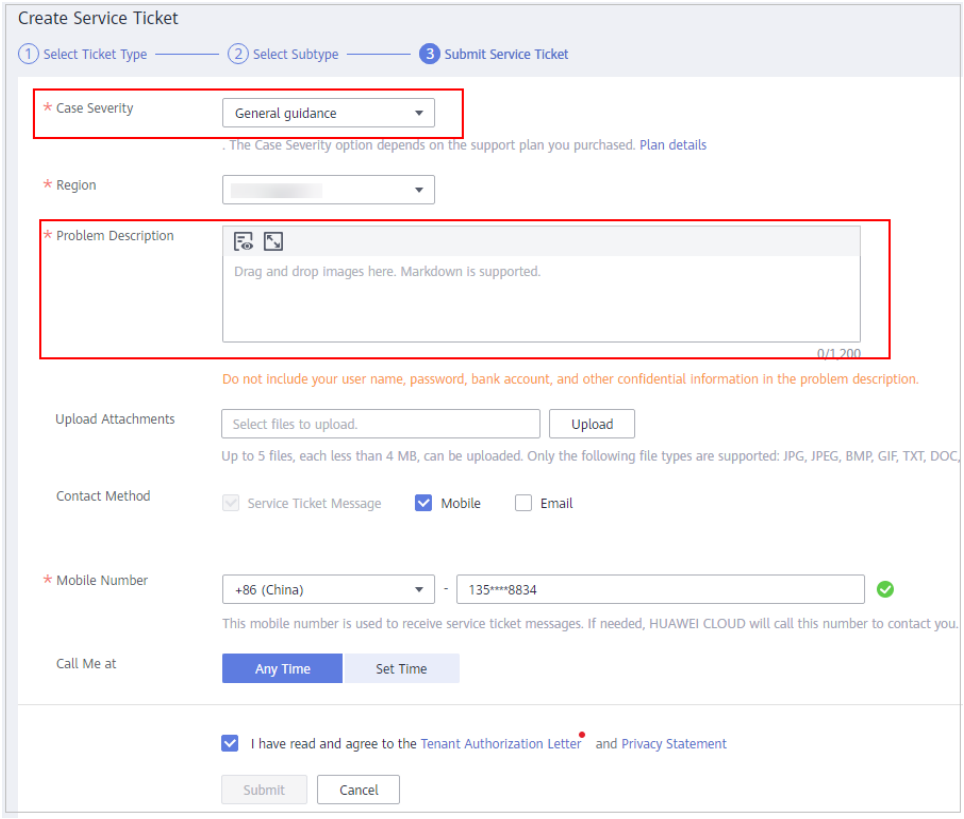
Paso 9 Seleccione **Service Tickets** > **Create Service Ticket**. Nuestros expertos en Huawei Cloud se pondrán en contacto con usted y le proporcionarán un plan de compra personalizado y su presupuesto.

- En la lista desplegable **Case Severity**, seleccione **General guidance**.
- En el cuadro de texto **Problem Description**, escriba **Dedicated HSM Contact Information**.

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 4-4 Creación de un ticket de servicio



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

4.2.3 Activación de una instancia HSM dedicada

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

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

Prerrequisitos

- Ha obtenido una cuenta y su contraseña para iniciar sesión en la consola de gestión.
- 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 dedicada. 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 HSM dedicada, no se puede cambiar a otro tipo ni se puede reembolsar. Para utilizar una instancia 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 Click  . Choose **Security & Compliance** > **Data Encryption Workshop**.

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 4-5 Selección de una AZ

Paso 7 Introduzca la información de activación, como se muestra en **Figura 4-6**. **Tabla 4-4** describe los parámetros.

Figura 4-6 Configuración de una instancia HSM dedicada

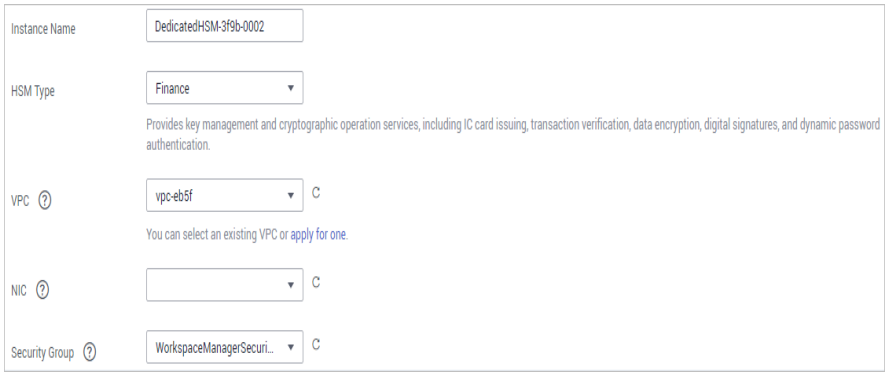


Tabla 4-4 Parámetros de activación

Parámetro	Descripción	Valor de ejemplo
Instance Name	Nombre de una instancia HSM dedicada **NOTA** El nombre de instancia solo puede contener letras, dígitos, guiones bajos (_), y guiones (-).	DedicatedHSM-3c98-0002
HSM Type	Los tipos de HSM disponibles incluyen **Finance**, **Server**, y **Signature server**. ● **Finance**: Proporciona gestión de claves y servicios informáticos de encriptación, incluyendo 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/desencriptación 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 resúmenes 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 *Guía del usuario de Virtual Private Cloud*.	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 dedicada. 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 *Guía del usuario de Virtual Private Cloud*.	**subnet-test-dhsm (192.168.0.0/24)**

Parámetro	Descripción	Valor de ejemplo
Security Group	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. Para obtener más información acerca de los grupos de seguridad, consulte la *Guía del usuario de Virtual Private Cloud*.	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 dedicadas. 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 HSM dedicada en edición platinum:

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

----Fin

4.3 Consulta de instancias de HSM dedicadas

Esta sección describe cómo ver la información de la instancia 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.

Prerrequisitos

Ha obtenido una cuenta y su contraseña para iniciar sesión en 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 . Elija **Security & Compliance** > **Data Encryption Workshop**. Se mostrará la página **Key Management Service**.

Paso 4 En el panel de navegación, elija **Dedicated HSM**.

Paso 5 En la lista, puede ver la información sobre las instancias de HSM.

Tabla 4-5 describe los parámetros de la lista de instancias de HSM.

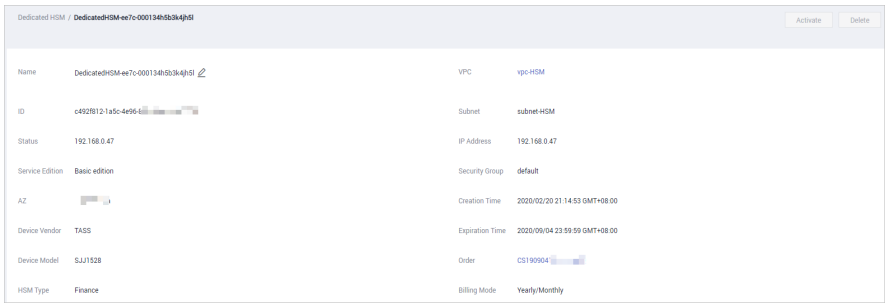
Tabla 4-5 Parámetros de instancia HSM dedicados

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

Parámetro	Descripción
Status	Estado de una instancia HSM dedicada: ● Instalación 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 Platina: Puede utilizar exclusivamente el subrack HSM, la fuente de alimentación, el ancho de banda de la red y los recursos API del HSM.
AZ	Zona de disponibilidad de un dispositivo
Device Vendor	Nombre de un proveedor de dispositivos.
Device Model	Modelo del dispositivo
IP Address	Dirección IP flotante de la instancia HSM dedicada
Fecha y hora de expiración	Tiempo de expiración de la instancia de HSM adquirida.

Paso 6 Puede hacer clic en el nombre de una instancia HSM dedicada para ver detalles sobre la instancia, como se muestra en **Figura 4-7**.

Figura 4-7 Detalles acerca de instancias de HSM dedicadas



Para obtener más información, consulte **Tabla 4-6**.

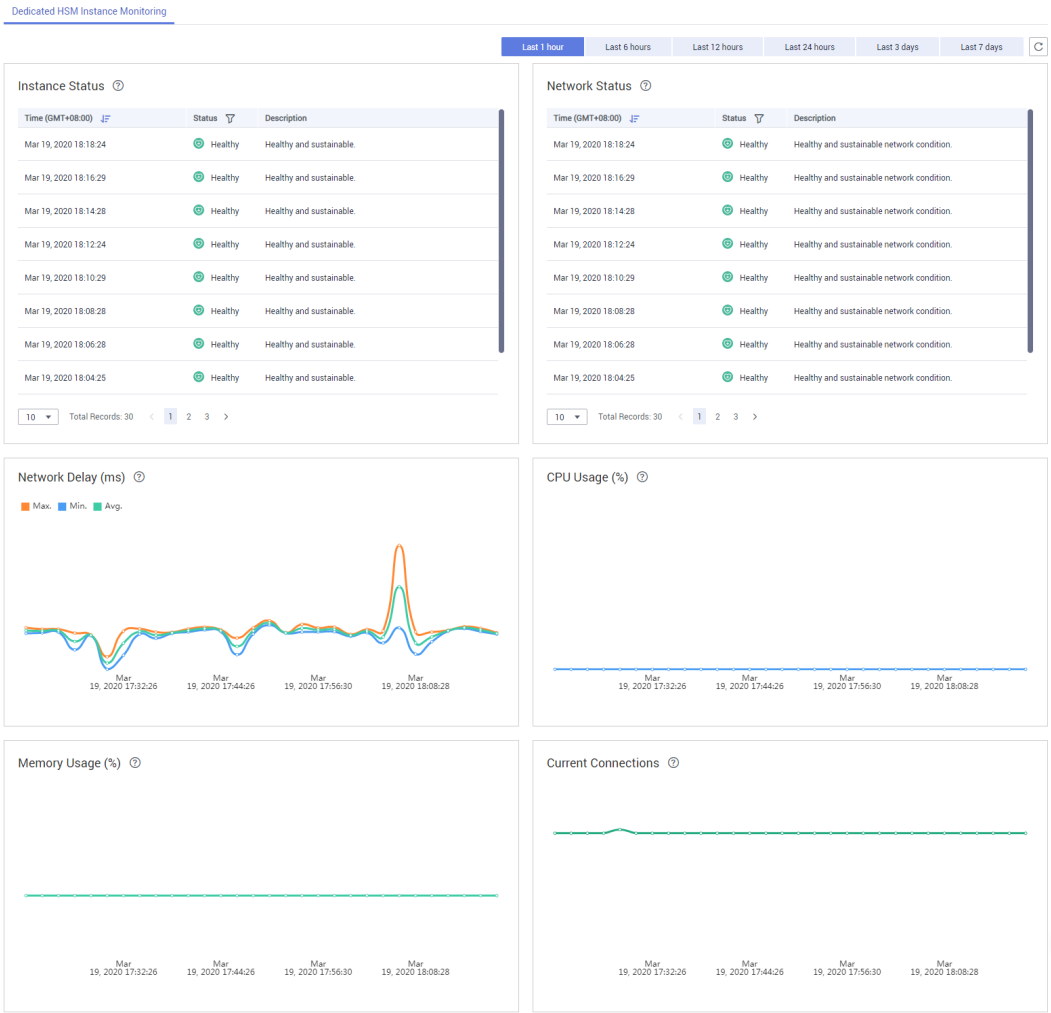
Tabla 4-6 Descripción del parámetro

Parámetro	Descripción
Name	Nombre de una instancia HSM dedicada
ID	ID de una instancia
Status	Estado de una instancia HSM dedicada: ● Instalación 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 Platina: Puede utilizar exclusivamente el subrack HSM, la fuente de alimentación, el ancho de banda de la red y los recursos API del HSM.
Device Vendor	Nombre de un proveedor de dispositivos.
Device Model	Modelo del dispositivo

Parámetro	Descripción
HSM Type	Tipos de función de una instancia, incluidos **Finance**, **Server**, y **Signature Server**.
VPC	VPC a la que pertenece la instancia Para obtener más información acerca de VPC, consulte *Guía del usuario de Virtual Private Cloud*.
Subnet	Subred donde se encuentra la instancia. Para obtener más información acerca de las subredes, consulte *Guía del usuario de Virtual Private Cloud*.
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 *Guía del usuario de Virtual Private Cloud*.
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 prepagado anual/mensual

Paso 7 Vea la información de monitoreo sobre la instancia HSM dedicada, incluido el estado de la instancia, el estado de la red, la latencia de la red, el uso de la CPU, el uso de la memoria y el número de conexiones actuales.

Figura 4-8 Monitorización de instancias de HSM dedicadas



----Fin

4.4 Uso de instancias de HSM dedicadas

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

Artículo	Descripción	Cómo obtener
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	*Manual del usuario de la instancia HSM dedicada* y *Guía de instalación de la instancia HSM dedicada*	
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.	Compre ECS según sea necesario. Para obtener más información, consulte **Compra de un ECS**.
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 implementa la instancia 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.
   - Configurar **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 desvincualción 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 APIs.

NOTA

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

----Fin

5 Registros de auditoría

5.1 Operaciones apoyadas por CTS

Tabla 5-1 enumera las operaciones DEW grabadas por CTS.

Tabla 5-1 Operaciones de DEW soportadas por CTS

Operación	Tipo de recurso	Nombre del rastro
Creación de claves	cmk	createKey
Creación de claves de datos	cmk	createDatakey
Creación de claves de datos sin texto plano	cmk	createDatakeyWithoutPlaintext
Habilitación de claves	cmk	enableKey
Deshabilitación de clave	cmk	disableKey
Encriptación de clave de datos	cmk	encryptDatakey
Desencriptación de claves de datos	cmk	decryptDatakey
Eliminación de clave programada	cmk	scheduleKeyDeletion
Cancelación de la eliminación de clave programada	cmk	cancelKeyDeletion
Generación de números aleatorios	rng	genRandom
Actualización de alias de clave	cmk	updateKeyAlias
Actualización de la descripción clave	cmk	updateKeyDescription

Operación	Tipo de recurso	Nombre del rastro
Indicación de riesgo de eliminación de clave	cmk	deleteKeyRiskTips
Importación de material de clave	cmk	importKeyMaterial
Eliminación de material de clave	cmk	deleteImportedKeyMaterial
Creación de autenticación	cmk	createGrant
Retirada de autorización	cmk	retireGrant
Revocación de autorización	cmk	revokeGrant
Encriptación de datos	cmk	encryptData
Desencriptación de datos	cmk	decryptData
Adición de etiquetas	cmk	dealUnifiedTags
Eliminación de etiquetas	cmk	dealUnifiedTags
Adición de etiquetas por lotes	cmk	dealUnifiedTags
Eliminación de etiquetas por lotes	cmk	batchDeleteKeyTags
Creación e importación de pares de claves SSH	keypair	createOrImportKeypair
Eliminación de pares de claves SSH	keypair	deleteKeypair
Importación de clave privada	keypair	importPrivateKey
Exportación de clave privada	keypair	exportPrivateKey
Compra de una instancia de HSM	hsm	purchaseHsm
Configuración de una instancia de HSM	hsm	createHsm
Eliminación de una instancia de HSM	hsm	deleteHsm

5.2 Uso de CTS para consultar rastros de operación 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.

Consulta de registros de auditoría de DEW

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en ☰. En **Management & Governance**, haga clic en **Cloud Trace Service**.

Paso 3 En la página mostrada, puede consultar rastros definiendo los criterios de filtrado. Los cuatro filtros siguientes están disponibles:

- **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**

  Seleccione el filtro de la lista desplegable.

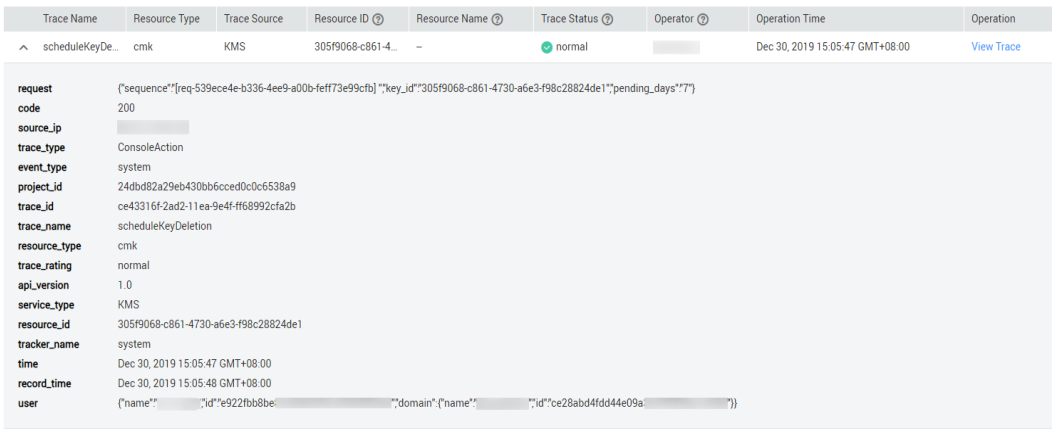
  - Establezca **Trace Type** en **Management**.
  - Establezca **Trace Source** en **KMS**.
  - Cuando selecciona **Trace name** para **Search By** también debe seleccionar un nombre de seguimiento específico. Cuando selecciona **Resource ID** para **Search By** también debe seleccionar o ingresar un ID de recurso específico. Cuando selecciona **Resource name** para **Search By**, también debe seleccionar o ingresar un nombre de recurso específico.

- **Operador**: Seleccione un operador específico (un usuario en lugar de un inquilino).
- **Trace Rating**: las opciones disponibles incluyen **all trace status**, **normal**, **warning**, y **incident**. Solo se puede habilitar una de ellas.
- **Time Range**: En la esquina superior derecha de la página, puede consultar rastros en la última hora, un día, una semana o dentro de un período personalizado.

Paso 4 Haga clic en **Search** para ver el evento de operación correspondiente.

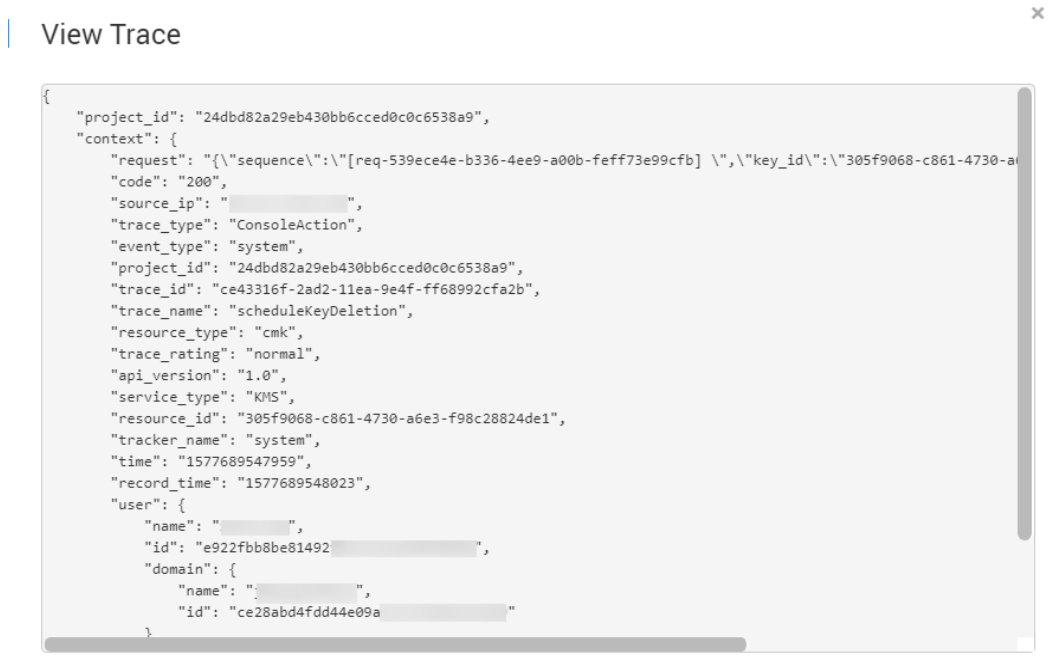
Paso 5 Haga clic en ⌄ a la izquierda de un rastro para ver sus detalles. Consulte **Figura 5-1**.

Figura 5-1 Ampliación de los detalles de rastro



Paso 6 Haga clic en **View Trace** en la columna **Operation**. En el cuadro de diálogo **View Trace** que se muestra en **Figura 5-2**, se muestran los detalles de la estructura de rastro.

Figura 5-2 Visualización de rastros



----Fin

6 Control de permisos

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

En este capítulo se describe cómo utilizar **IAM** para implementar un control de permisos detallado para los recursos 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.
- Otorgue a los usuarios sólo los permisos necesarios para realizar una tarea.
- Delegue una cuenta de Huawei Cloud de confianza o un servicio en la nube para realizar operaciones profesionales y eficientes en sus recursos DEW.

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

En esta sección se describe el procedimiento para conceder permisos (consultar **Figura 6-1**).

Prerrequisitos

Antes de autorizar permisos para un grupo de usuarios, debe saber qué permisos DEW se pueden agregar al grupo de usuarios. **Tabla 6-1** enumera las directivas del sistema DEW.

Para ver las políticas del sistema de otros servicios, consulte **Permisos de sistema**.

Tabla 6-1 Roles y políticas definidas por el sistema compatibles con DEW

Nombre de rol/ política	Descripción	Tipo	Dependencia
KMS Administrator	Permisos de administrador para KMS	Rol del sistema	Ninguno

Nombre de rol/ política	Descripción	Tipo	Dependencia
KMS CMKFullAccess	Permisos completos para KMS. Los usuarios con estos permisos pueden realizar todas las operaciones permitidas por las políticas.	Política del sistema	Ninguno
DEW KeypairFullAccess	Permisos completos para KPS. Los usuarios con estos permisos pueden realizar todas las operaciones permitidas por las políticas.	Política del sistema	Ninguno
DEW KeypairReadOnlyAccess	Permisos de sólo lectura para KPS. Los usuarios con este permiso sólo pueden ver los datos de KPS.	Política del sistema	Ninguno

Tabla 6-2 describe las operaciones comunes soportadas por cada permiso definido por el sistema de DEW. Seleccione los permisos necesarios.

Tabla 6-2 Operaciones comunes respaldadas por cada política o función definida por el sistema

Operación	Administrador de KMS	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

Operación	Administrador de KMS	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
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
Eliminar materiales de clave	√	√	x	x
Crear una autorización	√	√	x	x
Revocar una autorización	√	√	x	x
Retirar una autorización	√	√	x	x
Consultar la lista de concesiones	√	√	x	x
Consultar autorización retirable	√	√	x	x
Cifrar datos	√	√	x	x
Descifrar datos	√	√	x	x

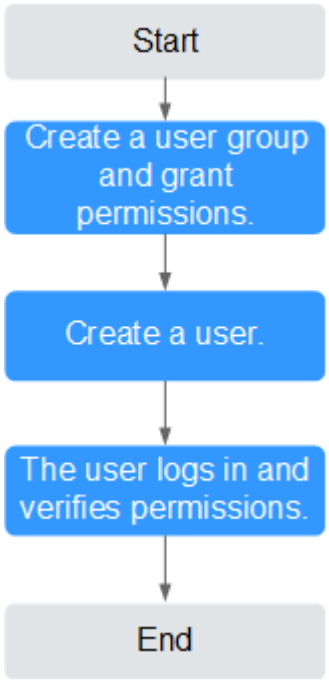
Operación	Administrador de KMS	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
Enviar mensajes de firma	√	√	x	x
Autenticación de firma	√	√	x	x
Habilitación de la rotación de clave	√	√	x	x
Modificar intervalo de rotación de clave	√	√	x	x
Deshabilitación de la rotación de clave	√	√	x	x
Consultar estado de rotación de clave	√	√	x	x
Consultar instancias CMK	√	√	x	x
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

Operación	Administrador de KMS	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
Consultar detalles de clave	√	√	x	x
Consultar clave pública	√	√	x	x
Cantidad de instancia de consulta	√	√	x	x
Consultar cuotas	√	√	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
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

Operación	Administrador de KMS	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
Consultar tareas en ejecución	x	x	√	√

Proceso de Autorización

Figura 6-1 Autorización del permiso de acceso DEW a un usuario



1. **Cree un grupo de usuarios 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 los permisos completos para las claves).

2. **Cree un usuario y agréguelo a un grupo de usuarios.**

   Cree un usuario en la consola de IAM y agregue el usuario al grupo de usuarios creado en **1**.

6.2 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 directivas personalizadas, consulte **Políticas de permisos y acciones admitidas**.

Puede crear 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: Editar las políticas JSON desde cero o basándose en una política existente. Para obtener más información sobre cómo crear directivas 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: negar 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 Permitir y Denegar, las acciones Denegar tienen prioridad sobre las acciones Permitir.

  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"
            ]
        }
    ]
}
```


A Historial de cambios

Publicado en	Descripción
2021-12-17	Este es el vigésimo séptimo lanzamiento oficial. Modified the following sections: ● In **Creación de CMK mediante materiales de clave importados**, asymmetric keys can be imported. ● In **Eliminación de materiales de clave**, the key materials of asymmetric keys cannot be directly deleted.
2021-10-26	This is the twenty-sixth official release. Added **Cloud Secret Management Service**.
2021-09-30	This is the twenty-fifth official release. ● Added description about Chinese cryptographic algorithms in **Creación de un CMK**. ● Added description about Chinese cryptographic algorithms in **Creación de CMK mediante materiales de clave importados**. ● Updated screenshots in **Gestión de pares de claves**.
2021-08-30	Este es el vigésimo cuarto lanzamiento oficial. Se cambió la edición profesional a la edición platino.

Publicado en	Descripción
2021-07-20	Este es el vigésimo tercer lanzamiento oficial. ● Changed the entry of DEW from **Security** to **Security and Compliance**. ● Modified the key creation procedure and screenshots in **Creación de un CMK**. ● Optimized content and updated screenshots in **Gestión de CMK**. ● Optimized the description of key pairs in **Gestión de pares de claves**. ● Added description about key types in **Tipos de claves**. ● Optimized operations in **Gestión de claves privadas**. ● Optimized operations in **HSM dedicado**.
2021-06-30	This is the twenty-second official release. ● Added **Adición de una clave a un proyecto**. ● Added constraints in **Vinculación de un par de claves**. ● Updated screenshots in **Gestión de CMK**.
2021-02-22	This is the twenty-first official release. Modified **Creación de una instancia HSM dedicada**.
2020-12-21	Este es el vigésimo lanzamiento oficial. Se optimizaron secciones en este documento.
2020-12-14	This is the nineteenth official release. Modified **Creación de un CMK**.
2020-09-25	This is the eighteenth official release. Modified **Creación de una instancia HSM dedicada**.
2020-08-24	This is the seventeenth official release. Added the description about how to obtain KeyId in **Creación de una política de DEW personalizada**.

Publicado en	Descripción
2020-08-12	This is the sixteenth official release. ● Added **Actualización de un par de claves**. ● Updated screenshots in **Creación de un par de claves**. ● Updated screenshots in **Importación de un par de claves**. ● Updated screenshots in **Consulta de un par de claves**. ● Updated screenshots and added descriptions in **Eliminación de un par de claves**. ● Updated screenshots and added descriptions in **Importación de una clave privada**. ● Updated screenshots and added descriptions in **Exportación de una clave privada**. ● Updated screenshots and added descriptions in **Borrar una clave privada**.
2020-07-14	This is the fifteenth official release. ● Added **Creación de CMK mediante materiales de clave importados**. ● Added the description about enterprise project functions in **Creación de un CMK**, **Creación de CMK mediante materiales de clave importados**, and **Consulta de un CMK**.
2020-04-07	Este es el decimocuarto lanzamiento oficial. Se actualizaron las capturas de pantalla.
2020-02-10	This is the thirteen official release. Modified **Control de permisos**.
2019-08-09	This is the twelfth official release. Modified section **Key Management Service**: updated screenshots.
2019-07-19	This is the eleventh official release. ● Added **Activación de una instancia HSM dedicada**. ● Added **Consulta de instancias de HSM dedicadas**.
2019-07-12	This is the tenth official release. Added **Compra de una instancia HSM dedicada**.

Publicado en	Descripción
2019-07-04	This is the ninth official release. ● Added the method of viewing key usage records in **Programación de la eliminación de uno o más CMK**. ● Modified section **Key Pair Service**: updated screenshots. ● Added **Uso de instancias de HSM dedicadas**. ● Added the resource types and event names of purchasing, configuring, and deleting an HMS instance to the table "DEW operations supported by CTS".
2019-04-22	Este es el octavo lanzamiento oficial. Se optimizó el diagrama de flujo y los gráficos de arquitectura.
2018-10-25	This is the seventh official release. Modified section **Consulta de un par de claves**: added the description about the page that displays details of key pairs.
2018-08-30	This is the sixth official release. ● Added **HSM dedicado**. ● Se agregó la sección "Encriptación de su sistema de servicio con HSM dedicado". ● Added **Uso de instancias de HSM dedicadas**.
2018-07-05	This is the fifth official release. ● Modified section **Creación de un CMK**: added the procedure for adding a tag. ● Updated screenshots.
2018-05-30	This is the fourth official release. ● Added **Vinculación de un par de claves**. ● Added **Desvinculación de un par de claves**. ● Added **Restablecimiento de un par de claves**. ● Added **Sustitución de un par de claves**. ● Added the description about deleting failure records in **Consulta de un par de claves**. ● Modified section **Consulta de un par de claves**: added the description about the list of ECSs bound to key pairs.

Publicado en	Descripción
2018-04-30	This is the third official release. ● Added **Adición de una etiqueta**. ● Added section "Searching for Tags". ● Added **Modificación de valores de etiqueta**. ● Added **Eliminación de etiquetas**. ● Updated screenshots.
2018-01-30	Esta edición es el segundo lanzamiento oficial. ● Se agregó la sección "Par de claves SSH". ● Added **Creación de un par de claves**. ● Added **Importación de un par de claves**. ● Added **Consulta de un par de claves**. ● Added **Eliminación de un par de claves**.
2017-12-31	Este es el primer lanzamiento oficial.

