Data Encryption Workshop

Descripción general del servicio

Edición	15
Fecha	2022-03-09

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 ¿Qué es DEW?

DEW

Los datos son el activo principal de una empresa. Cada empresa tiene sus datos confidenciales principales, que deben ser cifrados y protegidos contra violaciones de seguridad.

Data Encryption Workshop (DEW) es un servicio de encriptación de datos en la nube. Se compone de Key Management Service (KMS), Cloud Secret Management Service (CSMS), Key Pair Service (KPS), y Dedicated Hardware Security Module (Dedicated HSM), lo que le ayuda a proteger sus datos y claves, y simplifica la gestión de claves. DEW utiliza HSMs para proteger la seguridad de sus claves, y se puede integrar con otros Servicios de Huawei Cloud para abordar problemas de seguridad de datos, seguridad de claves y gestión de claves. Además, DEW le permite desarrollar aplicaciones de encriptación personalizadas.

Tabla 1-1 Descripción general del servicio

Servicio	Descripción	Referencia
Key Management Service (KMS)	KMS es un servicio seguro, confiable y fácil de usar para administrar sus claves en la nube. Le ayuda a crear, gestionar y proteger claves fácilmente. KMS utiliza módulos de seguridad de hardware (HSM) para proteger las claves, lo que le ayuda a crear y controlar las claves maestras del cliente (CMK) con facilidad. Todas las CMK están protegidas por claves root en HSM para evitar fugas de claves.	**Tipos de clave**

Servicio	Descripción	Referencia
Cloud Secret Management Service (CSMS)	CSMS es un servicio de alojamiento secreto seguro, confiable y fácil de usar. Los usuarios o las aplicaciones pueden usar CSMS para crear, recuperar, actualizar y eliminar credenciales de manera unificada durante todo el ciclo de vida de las credenciales. CSMS puede ayudarlo a eliminar los riesgos incurridos por la codificación de hardware, la configuración de texto sin formato y el abuso de permisos.	**Creación de un secreto**
Key Pair Service (KPS)	KPS es un servicio en la nube seguro, confiable y fácil de usar diseñado para gestionar y proteger sus pares de claves SSH (pares de claves para abreviar). KPS usa HSMs para generar números aleatorios verdaderos que luego se usan para producir pares de claves. Además, adopta una solución de gestión de pares de claves completa y confiable para ayudar a los usuarios a crear, importar y gestionar pares de claves con facilidad. La clave pública de un par de claves generado se almacena en KPS mientras que la clave privada se puede descargar y guardar por separado, lo que garantiza la privacidad y seguridad del par de claves.	**Creación de par de claves**
Dedicated Hardware Security Module (Dedicated HSM)	HSM dedicado permite la encriptación de datos en la nube, específicamente, cifrar y descifrar datos, verificar firmas, generar claves y almacenar claves. HSM dedicado proporciona encriptación de hardware, garantizando la seguridad y la integridad de los datos en Elastic Cloud Servers (ECSs) y cumpliendo con los requisitos de cumplimiento. HSM dedicado le ofrece una gestión segura y confiable de las claves generadas por sus instancias, y utiliza múltiples algoritmos para el encriptación y desencriptación de datos.	HSM dedicado

Conceptos

Esta sección describe los conceptos básicos en DEW.

Tabla 1-2 Conceptos Básicos

Artículo	Definición	Referencia
Hardware Security Module (HSM)	Un HSM es un tipo de hardware informático que protege y administra las claves utilizadas por los sistemas de autenticación fuertes y proporciona operaciones criptográficas relacionadas.	-
Customer Master Key (CMK)	Una CMK es una Key Encryption Key (KEK) creada por un usuario o servicio en la nube que utiliza KMS. Se utiliza para cifrar y proteger Data Encryption Keys (DEKs). Se puede usar un CMK para cifrar uno o más DEK. Los CMK se clasifican en claves personalizadas y claves predeterminadas.	**¿Qué es una clave maestra del cliente?**
Default Master Key (DMK)	Otro servicio en la nube que utiliza KMS crea automáticamente una clave maestra predeterminada, como el Object Storage Service (OBS). El alias de una clave maestra predeterminada termina en **/default**.	**¿Qué es una clave maestra predeterminada?**
Key material	Los materiales clave son entradas importantes para las operaciones criptográficas. Un CMK consiste en un ID de clave, metadatos y un material de clave.	-
Envelope encryption	El encriptación de sobres es la práctica de cifrar datos con un DEK y luego cifrar el DEK con una clave root que puede gestionar completamente. En este caso, los CMK no son necesarios para el encriptación o desencriptación.	**¿Cuáles son los beneficios del Envelope Encryption?**
Data Encryption Key (DEK)	Se utiliza un DEK para cifrar datos.	**¿Qué es una clave de cifrado de datos?**
Symmetric key encryption	La encriptación de clave simétrica también se denomina encriptación de clave dedicada. El remitente y el receptor usan la misma clave para cifrar y descifrar datos. Ventaja: El cifrado y el descifrado son rápidos. Desventaja: Cada par de llaves debe ser único. La gestión de claves es difícil si hay un gran número de usuarios. Escenario: Cifrar una gran cantidad de datos.	Tipos de clave

Artículo	Definición	Referencia
Asymmetric key encryption	La encriptación de clave asimétrica también se denomina encriptación de clave pública. Se utilizan un par de claves para la encriptación y la desencriptación. Una es una clave pública, y la otra es una clave privada. Ventaja: Se utilizan diferentes claves para la encriptación y la desencriptación, mejorando la seguridad. Desventaja: El cifrado y el descifrado son lentos. Escenario: Cifrar información confidencial.	**Tipos de clave**
Key pair	Un par de claves es un par de clave pública asimétrica y clave privada. Por defecto, RSA-2048 se utiliza para criptografía.	**Gestión de pares de claves**
Private key pair	Un par de claves privadas puede ser visto o utilizado solo por la cuenta actual.	**Creación de un par de claves**
Account key pair	Todos los usuarios de la cuenta pueden ver o usar un par de claves de cuenta.	**Actualización de un par de claves**

2 KMS

2.1 Funciones

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

Utiliza Hardware Security Modules (HSMs) para proteger las claves. Todas las CMK están protegidas por claves root en HSM para evitar fugas de claves.

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

Funciones

- En la consola KMS, puede realizar las siguientes operaciones en CMK:
  - Creación, consulta, habilitación, deshabilitación, programación de la eliminación y cancelar la eliminación de CMK
  - Modificación del alias y la descripción de CMK
  - Uso de la herramienta en línea para cifrar y descifrar pequeños volúmenes de datos
  - Adición, búsqueda, edición y eliminación de etiquetas
  - Creación, cancelación y consulta de subvenciones
- Puede utilizar la API para realizar las siguientes operaciones:
  - Creación, encriptación o desencriptación de data encryption keys (DEKs)
  - Subsidios de jubilación
  - Firma o verificación de la firma de mensajes o resúmenes de mensajes

  Para obtener más información, consulta la *Referencia de la API de Data Encryption Workshop*.
- Generar hardware verdadero número aleatorio.

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

Algoritmos criptográficos soportados por KMS

Las claves simétricas creadas en la consola KMS utilizan el algoritmo AES-256. Las claves asimétricas creadas por KMS soportan los algoritmos RSA y ECC.

Tabla 2-1 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 keys	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

Tabla 2-2 describes the encryption and decryption algorithms supported for user-imported keys. Solo se pueden importar claves simétricas de 256 bits.

Tabla 2-2 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**	Seleccione un algoritmo de encriptación basado en sus funciones HSM. Si los HSM soportan el algoritmo **RSAES_OAEP_SHA_256**, utilice **RSAES_OAEP_SHA_256** para cifrar materiales de clave. **AVISO** El algoritmo de encriptación **RSAES_OAEP_SHA_1** ya no es seguro. Tenga cuidado al realizar esta operación.
RSAES_OAEP_SHA_1	Algoritmo de encriptación RSA que utiliza Optimal Asymmetric Encryption Padding (OAEP) y tiene la función hash **SHA-1**	

2.2 Ventajas del producto

- Amplia integración de servicios

  KMS se puede integrar con Object Storage Service (OBS), Elastic Volume Service (EVS) y Image Management Service (IMS), para gestionar las claves de estos servicios

en la consola KMS y cifrar y descifrar los datos locales realizando las llamadas a la API de KMS.

- Cumplimiento de reglamentario

  Las claves son generadas por HSM validados por terceros. El acceso a las llaves está controlado y todas las operaciones que involucran llaves son rastreables por registros, que cumplen con las leyes y regulaciones chinas e internacionales.

2.3 Escenarios de aplicación

Prerrequisitos

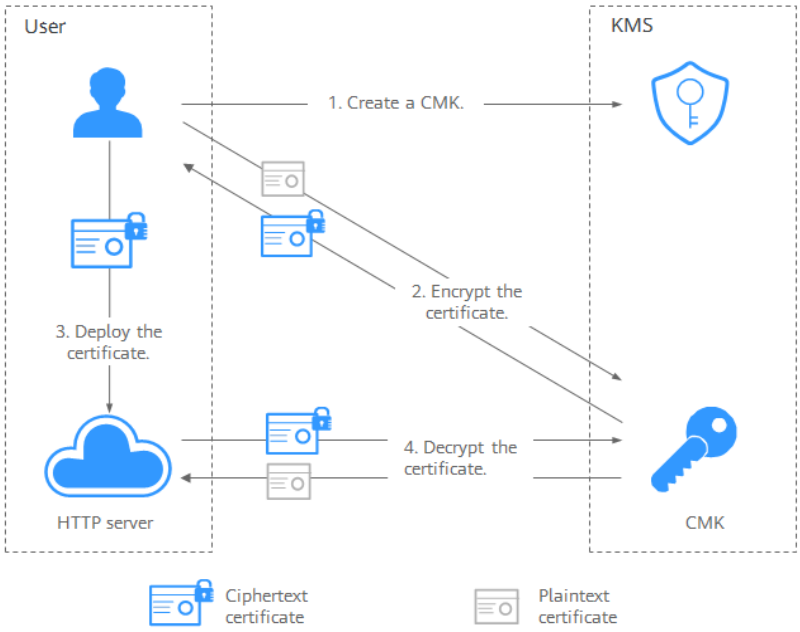
Todas las CMK mencionadas en esta sección son claves simétricas. Para obtener más información sobre las claves simétricas y las claves asimétricas, consulte **Descripción general de clave**.

Cifrado y descifrado de datos pequeños

Puede utilizar la herramienta en línea en la consola de KMS o llamar a las API de KMS para cifrar o descifrar directamente una pequeña cantidad de datos, como contraseñas, certificados o números de teléfono. Actualmente, un máximo de 4 KB de datos pueden ser cifrados o descifrados de esta manera.

Figura 2-1 muestra un ejemplo sobre cómo llamar a las API para cifrar y descifrar un certificado HTTPS.

Figura 2-1 Cifrado y descifrado de un certificado HTTPS



Siga el siguiente procedimiento:

1. Crear un CMK en KMS.
2. Llame a la API **encrypt-data** de KMS y use el CMK para cifrar el certificado de texto sin formato.

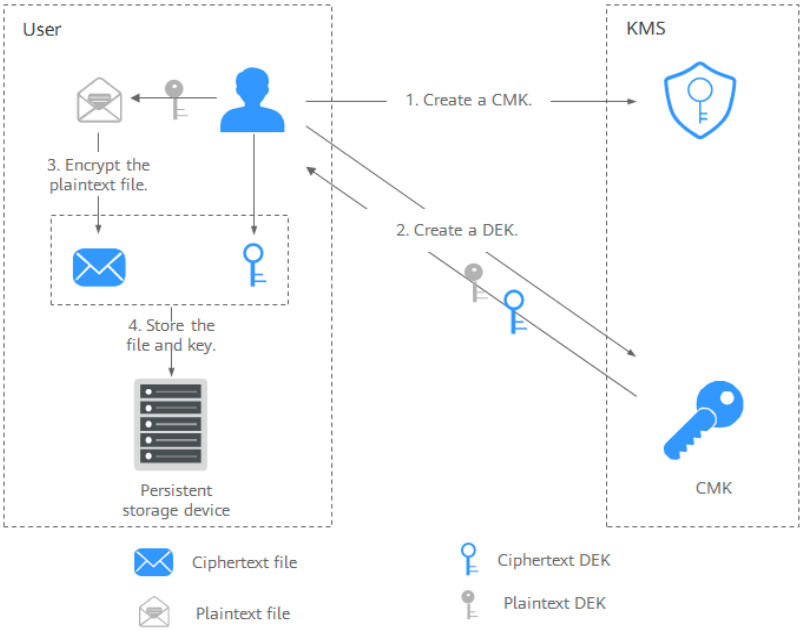
3. Implemente el certificado en un servidor.
4. El servidor llama a la API de **decrypt-data** de KMS para descifrar el certificado de texto cifrado.

Cifrado y descifrado de datos grandes

Si desea cifrar o descifrar grandes volúmenes de datos, como imágenes, vídeos y archivos de base de datos, puede utilizar el método de encriptación de envolvente, donde los datos no es necesario transferirse a través de la red.

- **Figura 2-2** ilustra el proceso para cifrar un archivo local.

Figura 2-2 Cifrado de un archivo local

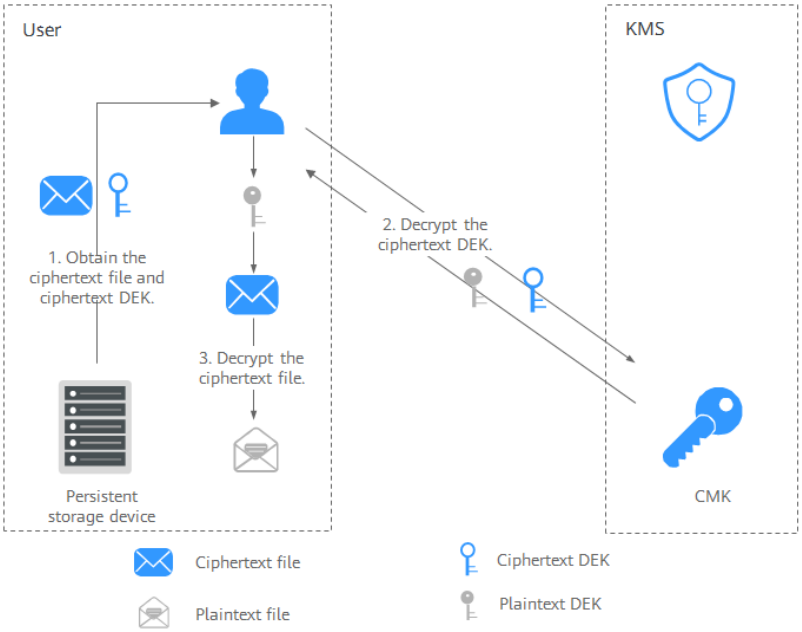


Siga el siguiente procedimiento:

a. Crear un CMK en KMS.
b. Llama a la API **create-datakey** y de KMS para crear un DEK. Luego obtienes un DEK de texto plano y un DEK de texto cifrado. El DEK de texto cifrado se genera cuando se utiliza un CMK para cifrar el DEK de texto sin formato.
c. Utilice el DEK de texto sin formato para cifrar el archivo. Se genera un archivo de texto cifrado.
d. Guarde el DEK de texto cifrado y el archivo de texto cifrado juntos en un dispositivo de almacenamiento persistente o un servicio de almacenamiento.

- **Figura 2-3** ilustra el proceso para descifrar un archivo local.

Figura 2-3 Descifrar un archivo local



Siga el siguiente procedimiento:

a. Obtenga el DEK y el archivo de texto cifrado del dispositivo de almacenamiento persistente o del servicio de almacenamiento.

b. Llame a la API de **decrypt-datakey** de KMS y use el CMK correspondiente (el utilizado para cifrar el DEK) para descifrar el DEK de texto cifrado. Luego obtienes el DEK de texto sin formato.

   Si se elimina el CMK, el descifrado falla. Por lo tanto, mantenga correctamente sus CMK.

c. Utilice el DEK de texto sin formato para descifrar el archivo de texto cifrado.

Enlaces útiles

Documento	Enlace
Prácticas mejores	● **Cifrado o descifrado de pequeños volúmenes de datos** ● "Cifrado o descifrado de una gran cantidad de datos"
Ejemplo de API	● **Cifrado o descifrado de pequeños volúmenes de datos** ● **Cifrado o descifrado de una gran cantidad de datos**

2.4 Uso de KMS

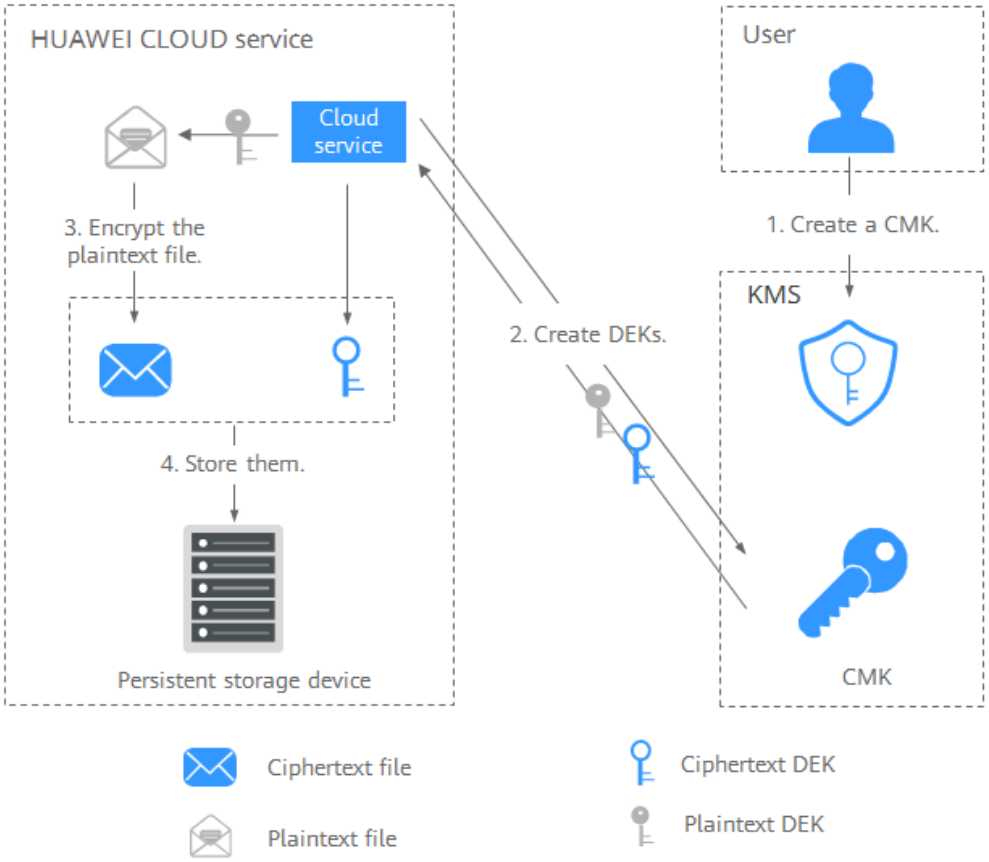
Prerrequisitos

Todas las CMK mencionadas en esta sección son claves simétricas. Para obtener más información sobre las claves simétricas y las claves asimétricas, consulte **Descripción general de clave**.

Interactuación con HUAWEI CLOUD Services

HUAWEI CLOUD services utilizan la tecnología de encriptación de sobres y llaman a las API de KMS para cifrar los recursos de servicio. Sus CMK están bajo su propia gestión. Con su concesión,HUAWEI CLOUD services utilizan un CMK específico suyo para cifrar datos.

Figura 2-4 Cómo Huawei Cloud utiliza KMS para encriptación



El proceso de encriptación es el siguiente:

1. Crear un CMK en KMS.
2. Servicios de Huawei Cloud llaman a la API de creación de datos del KMS para crear un DEK. Luego obtienes un DEK de texto plano y un DEK de texto cifrado.

   NOTA

   Los DEK de texto cifrado se generan cuando se utiliza un CMK para cifrar los DEK de texto sin formato.

3. HUAWEI CLOUD services utilizan el DEK de texto sin formato para cifrar un archivo de texto sin formato, generando un archivo de texto cifrado.
4. HUAWEI CLOUD services almacenan el DEK de texto cifrado y el archivo de texto cifrado en un dispositivo de almacenamiento persistente o un servicio de almacenamiento.

NOTA

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

Tabla 2-3 Lista de servicios en la nube que utilizan encriptación KMS

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

Nombre del servicio	Descripción
Document Database Service (DDS)	Al comprar una instancia DDS, puede habilitar la función de encriptación de disco de la instancia y seleccionar un CMK creado en KMS para cifrar el disco de la instancia. Habilitación de la función de encriptación de disco mejorará la seguridad de los datos. Para obtener más información acerca de cómo utilizar la función de encriptación de disco de DDS, consulte *Guía de usuario de Document Database Service*.

Trabajar con aplicaciones de usuario

Para cifrar datos de texto sin formato, una aplicación de usuario puede llamar a la API de KMS necesaria para crear un DEK. El DEK puede usarse entonces para cifrar los datos de texto sin formato. A continuación, la aplicación puede almacenar los datos cifrados. Además, la aplicación de usuario puede llamar a la API de KMS para crear los CMK. Los DEK se pueden almacenar en texto cifrado después de ser cifrados con los CMK.

Se implementa la encriptación de sobres, con CMKs almacenados en KMS y DEKs de texto encriptación en aplicaciones de usuario. KMS es llamado para descifrar un texto cifrado DEK solo cuando es necesario.

El proceso de encriptación es el siguiente:

1. La aplicación llama a la API **create-key** de KMS para crear un CMK.
2. La aplicación llama a la API **create-datakey** de KMS para crear un DEK. Se generan un DEK de texto sin formato y un DEK de texto cifrado.

   NOTA

   Los DEK de texto cifrado se generan cuando se utiliza un CMK para cifrar los DEK de texto sin formato en **1**.
3. La aplicación utiliza el DEK de texto sin formato para cifrar un archivo de texto sin formato. Se genera un archivo de texto cifrado.
4. La aplicación guarda el DEK de texto cifrado y el archivo de texto cifrado juntos en un dispositivo de almacenamiento persistente o un servicio de almacenamiento.

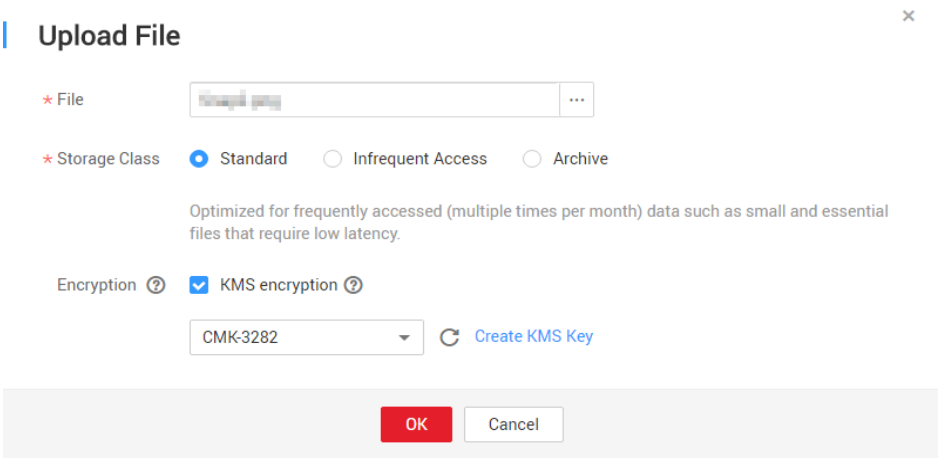
Para obtener más información, consulta la *Referencia de API de Data Encryption Workshop*.

2.5 Servicios en la nube con KMS integrado

2.5.1 Encriptación de datos en OBS

- Cuando utilice Object Storage Service (OBS) para cargar archivos con encriptación del servidor, puede seleccionar encriptación KMS y utilizar la clave proporcionada por KMS para cifrar los archivos que se van a cargar. **Figura 2-5** describe detalles. Para obtener más información acerca de OBS, consulte la *Object Storage Service Console Operation Guide*

Figura 2-5 Encriptación del lado del servidor OBS



Hay dos tipos de CMK que se pueden utilizar:

- La clave maestra predeterminada **obs/default** creada por KMS
- CMK que cree en la consola de KMS con materiales clave generados por KMS

- Alternativamente, puede llamar a las API de OBS para cargar un archivo con encriptación del lado del servidor mediante claves administradas por KMS (SSE-KMS). Para obtener más información, consulta la *Referencia de API de Object Storage Service*.

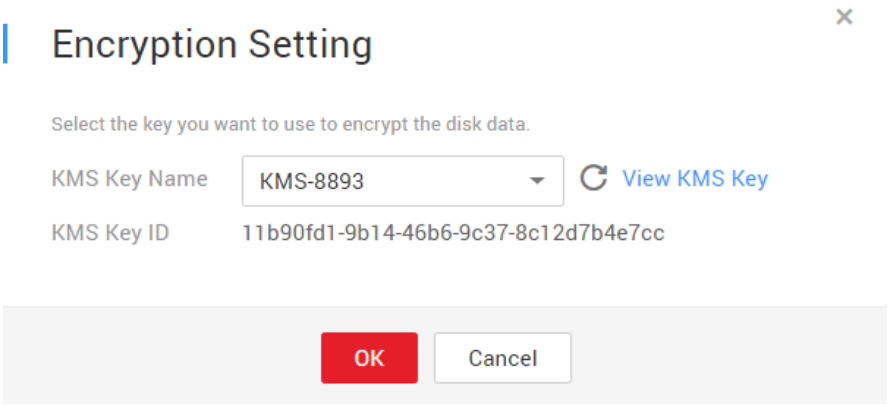
2.5.2 Encriptación de datos en EVS

- Al comprar un disco, puede elegir **Advanced Settings** > **Configure** > **Encryption** para cifrar el disco con la clave proporcionada por KMS. Para más detalles, consulte **Figura 2-6**. Para obtener más información acerca de EVS, consulte la *Guía del usuario de Elastic Volume Service* .

NOTA

Antes de utilizar la función de encriptación, se debe conceder a EVS el permiso para acceder a KMS. Si usted tiene el derecho de conceder el permiso, puede conceder el permiso directamente. Si no tiene el permiso, póngase en contacto con un usuario con los permisos de administrador de seguridad para agregar el permiso de administrador de seguridad por usted. A continuación, puede conceder el permiso. Para obtener más información acerca de EVS, consulte la *Guía de usuario de Elastic Volume Service*.

Figura 2-6 Encriptación de datos en EVS



Hay dos tipos de CMK que se pueden utilizar:

- La clave maestra predeterminada **evs/default** creada por KMS
- CMK que cree en la consola de KMS con materiales clave generados por KMS

- También puede llamar a las API de EVS para crear discos EVS cifrados. Para obtener más información, consulte la *Referencia de API de Elastic Volume Service*.

2.5.3 Encriptación de datos en IMS

- Al cargar un archivo de imagen en Image Management Service (IMS), puede elegir cifrar el archivo de imagen utilizando una clave proporcionada por KMS para proteger el archivo. **Figure Encriptación de datos en IMS** describe detalles. For details, see the .

Figura 2-7 Encriptación de datos en IMS

Hay dos tipos de CMK que se pueden utilizar:

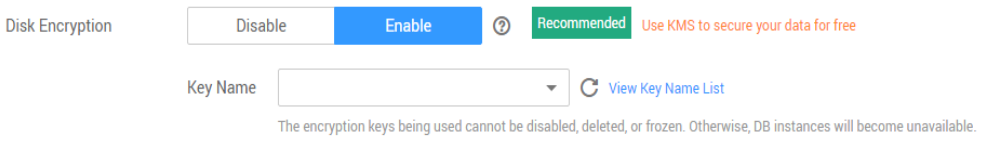
- La clave maestra predeterminada **ims/default** creada por KMS
- CMK que cree en la consola de KMS con materiales clave generados por KMS

- También puede llamar a las API de IMS para crear archivos de imagen cifrados. Para obtener más información, consulte la *Referencia de API de Image Management Service*.

2.5.4 Encriptación de datos en RDS

- Cuando un usuario compra una instancia de base de datos del Servicio de base de datos relacional (RDS), el usuario puede seleccionar **Disk encryption** y utilizar la clave proporcionada por KMS para cifrar el disco de la instancia de base de datos. Para obtener más información, consulte la *Guía del usuario de Relational Database Service*.

Figura 2-8 Encriptación de datos en RDS



Hay dos tipos de CMK que se pueden utilizar:

- La clave maestra predeterminada **rds/default** creada por KMS
- CMK que cree en la consola de KMS con materiales clave generados por KMS

- También puede llamar a las API de RDS para comprar instancias de base de datos cifradas. Para obtener más información, consulte la *Guía del usuario de Relational Database Service*.

2.5.5 Encriptación de datos en DDS

- Cuando un usuario compra una instancia de base de datos de DDS, el usuario puede seleccionar **Disk encryption** y utilizar la clave proporcionada por KMS para cifrar el disco de la instancia de base de datos. Para obtener más información, consulte la *Guía del usuario de Relational Database Service*.

  Figura 2-9 Encriptación de datos en DDS

  Hay dos tipos de CMK que se pueden utilizar:
  - La clave maestra predeterminada **dds/default** creada por KMS
  - CMK que cree en la consola de KMS con materiales clave generados por KMS
- También puede llamar a la API requerida de DDS para comprar instancias de base de datos cifradas. Para obtener más información, consulta *Referencia de API de Document Database Service*.

3 CSMS

3.1 Funciones

CSMS es un servicio de alojamiento de credenciales seguro, confiable y fácil de usar. Los usuarios o las aplicaciones pueden usar CSMS para crear, recuperar, actualizar y eliminar credenciales de manera unificada durante todo el ciclo de vida de las credenciales. CSMS puede ayudarlo a eliminar los riesgos incurridos por la codificación de hardware, la configuración de texto sin formato y el abuso de permisos.

Gestión de Secretos Unificados

Las aplicaciones y los sistemas empresariales tienen un gran número de secretos y son difíciles de gestionar.

CSMS puede almacenar, recuperar y usar secretos de manera unificada a lo largo de sus ciclos de vida.

Realice las siguientes operaciones para gestionar secretos mediante CSMS:

1. Recoge secretos.
2. Sube los secretos a CSMS.
3. Configure los permisos de acceso y uso detallados para cada secreto mediante IAM.

Recuperación segura de secretos

Muchas aplicaciones almacenan secretos de texto sin formato, como contraseñas, tokens, certificados, claves SSH y claves API, en sus archivos de configuración para ser utilizados para la autenticación cuando acceden a bases de datos u otros servicios. Los secretos de texto sin formato y codificados son propensos a la violación e incurren en riesgos de seguridad.

CSMS permite a los usuarios consultar de forma dinámica secretos a través de API en lugar de codificar los secretos, lo que reduce en gran medida los riesgos de violación.

Realice las siguientes operaciones para gestionar secretos mediante CSMS:

Cuando una aplicación lee sus configuraciones, llama a las API de CSMS para recuperar secretos. No se requieren secretos codificados ni de texto sin formato.

Credenciales y Claves Rotativas

Los secretos deben actualizarse periódicamente para mejorar la seguridad. Para rotar un secreto, es necesario actualizar el secreto en todas las aplicaciones y configuraciones que lo utilizan, lo que requiere mucho tiempo, es propenso a errores y puede causar una interrupción del servicio.

CSMS permite una conveniente gestión de secretos multi-versión. Las aplicaciones pueden llamar a las API o SDK de CSMS para actualizar de forma segura los secretos sin cometer errores.

Realice las siguientes operaciones para gestionar secretos mediante CSMS:

1. Un administrador agrega una versión secreta en la consola CSMS o a través de API y actualiza el secreto.
2. Las aplicaciones llaman a las API o SDK de CSMS para obtener la versión más reciente o especificada del secreto y realizar una actualización completa o en escala de grises.
3. Repetir regularmente los pasos **1** y **2** para rotar secretos.
4. Habilite la rotación de las claves de encriptación para mejorar la seguridad del almacenamiento.

Características básicas de CSMS

Tabla 3-1 Características básicas de CSMS

Función	Descripción
Gestión secreta del ciclo de vida	● Crear, ver y programar y cancelar la eliminación de secretos. ● Cambiar la clave de encriptación secreta y la descripción.
Gestión de versiones secreta	● Crear y ver versiones secretas. ● Ver valores secretos.
Gestión secreta del estado de la versión	Actualizar, consultar y eliminar versiones de credenciales.
Gestión de etiquetas secretas	Agregar, buscar, editar y eliminar etiquetas.

3.2 Ventajas del producto

Encriptación de secreto

Los secretos son cifrados por KMS antes del almacenamiento. Las claves de cifrado se generan y protegen mediante HSM autenticado de terceros. Cuando recupera secretos, se transfieren a servidores locales a través de TLS.

Recuperación segura de secretos

CSMS llama a las API secretas en lugar de a los secretos codificados en las aplicaciones. Los secretos se pueden recuperar y gestionar dinámicamente. CSMS gestiona los secretos de las aplicaciones de manera centralizada para reducir los riesgos de violación.

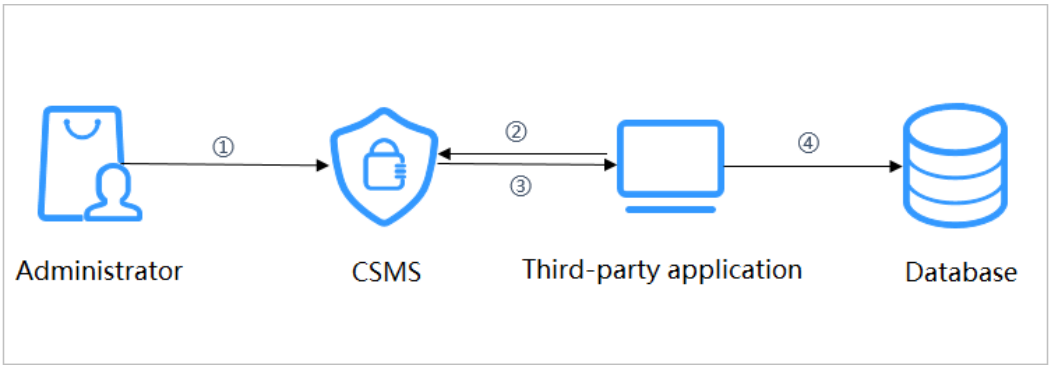
Gestión y control de secretos centralizados

La gestión de permisos y identidades de IAM garantiza que solo los usuarios autorizados puedan recuperar y modificar las credenciales. CTS monitorea el acceso a las credenciales. Estos servicios evitan el acceso no autorizado y la violación de información confidencial.

3.3 Escenarios de aplicación

Esta sección utiliza un nombre de usuario básico de la base de datos y su contraseña como ejemplo para describir cómo funciona el CSMS.

Figura 3-1 Proceso de inicio de sesión basado en secreto



Siga el siguiente procedimiento:

Paso 1 Cree un secreto en la **consola** o a través de una API para almacenar información de la base de datos (como la dirección de la base de datos, el puerto y la contraseña).

Paso 2 Utilice una aplicación para acceder a la base de datos. CSMS consultará el secreto que creó.

Paso 3 CSMS recupera y descifra el texto cifrado de credenciales y devuelve de forma segura la información almacenada en la credencial a la aplicación a través de la API de gestión de credenciales.

Paso 4 La aplicación obtiene el secreto de texto plano descifrado y lo utiliza para acceder a la base de datos.

----Fin

4 KPS

4.1 Funciones

Key Pair Service (KPS) es un servicio en la nube seguro, confiable y fácil de usar diseñado para gestionar y proteger sus pares de claves SSH (pares de claves para abreviar).

Como alternativa al método tradicional de autenticación de nombre de usuario y contraseña, los pares de claves le permiten iniciar sesión remotamente en los ECS de Linux.

Un par de claves, incluyendo una clave pública y una clave privada, se generan en base a un algoritmo de encriptación. La clave pública se guarda automáticamente en KPS, mientras que la clave privada se puede guardar en el host local del usuario. También puede guardar sus claves privadas en KPS y gestionarlas con KPS según sus necesidades. Si ha configurado la clave pública en un ECS de Linux, puede usar la clave privada para iniciar sesión en el ECS sin una contraseña. Como no es necesario introducir una contraseña, la contraseña no será interceptada, descifrada y filtrada, y el servidor se vuelve más seguro.

KPS usa HSMs para generar números aleatorios verdaderos que luego se usan para producir pares de claves. Además, adopta una solución de gestión de pares de claves completa y confiable para ayudar a los usuarios a crear, importar y gestionar pares de claves con facilidad. La clave pública de un par de claves generado se almacena en KPS mientras que la clave privada se puede descargar y guardar por separado, lo que garantiza la privacidad y seguridad del par de claves.

Funciones

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

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

Algoritmos de criptografía compatibles con KPS

- Los pares de claves SSH-2 creados en la consola KPS solo admiten los algoritmos de criptografía **RSA-2048**.
- Las claves importadas a la consola de KPS admiten los siguientes algoritmos criptográficos:

- RSA-1024
- RSA-2048
- RSA-4096
- ECDSA-nisty256
- ECDSA-nisty384
- ECDSA-nisty521
- Ed25519
- DSA

4.2 Ventajas del producto

- Seguridad de inicio de sesión reforzado

  Puede iniciar sesión en un ECS de Linux sin ingresar una contraseña, evitando efectivamente que se divulgue la cuenta debido a la interceptación de contraseñas y el craqueo. Como resultado, la seguridad de los ECS de Linux mejora considerablemente.
- Cumplimiento de reglamentario

  Los números aleatorios son generados por HSM validados por terceros. El acceso a los pares de claves está controlado y todas las operaciones que involucran pares de claves son rastreables por registros, que cumplen con las leyes y regulaciones chinas e internacionales.

4.3 Escenarios de aplicación

Al comprar un ECS que ejecuta un sistema operativo Linux, puede elegir autenticar a los usuarios que intentan iniciar sesión en su ECS con el par de claves SSH proporcionado por KPS. Al comprar un ECS con un sistema operativo Windows, puede elegir obtener la contraseña utilizada para iniciar sesión en su ECS desde el archivo de clave proporcionado por KPS.

Inicio de sesión en un ECS de Linux

Si su Elastic Cloud Server (ECS) ejecuta un sistema operativo Linux, puede usar un par de claves para iniciar sesión en el ECS. Para obtener más información, consulte la **Guía de usuario de Elastic Cloud Server**.

Al comprar un ECS, puede elegir cualquiera de los siguientes pares de claves:

- Pares de claves creados o importados en la consola de ECS
- Pares de claves creados o importados a la consola KPS

Los dos tipos de pares de claves solo difieren en la forma en que se importan.

Obtención de contraseña para iniciar sesión en un ECS de Windows

Si su Elastic Cloud Server (ECS) ejecuta un sistema operativo Windows, debe obtener la contraseña de inicio de sesión utilizando la clave privada de un par de claves. Para obtener más información, consulte la **Guía de usuario de Elastic Cloud Server**.

Al comprar un ECS, puede elegir cualquiera de los siguientes pares de claves:

- Pares de claves creados en la consola ECS o importados a ella
- Pares de claves creados o importados a la consola KPS

Los dos tipos de pares de claves solo difieren en la forma en que se importan.

5 HSM dedicado

5.1 Funciones

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

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

Funciones

HSM dedicado ofrece las siguientes capacidades:

- Generación, almacenamiento, importación, exportación y gestión de claves de encriptación (tanto simétricas como asimétricas)
- Encriptación y desencriptación de datos mediante algoritmos simétricos y asimétricos
- Uso de funciones hash criptográficas para calcular resúmenes de mensajes y código de autenticación de mensajes basado en hash
- Firmar datos y código en modo cifrado y verificar la firma
- Generación de datos aleatorios en modo cifrado

Algoritmos de criptografía compatibles

Tabla 5-1 Algoritmos de criptografía compatibles

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

5.2 Ventajas del producto

- Aplicable en la nube

  HSM dedicado es la opción óptima para transferir capacidades de encriptación fuera de línea a la nube, reduciendo sus costos de operación.

- Escalamiento elástico

  Puede aumentar o disminuir de forma flexible el número de instancias de HSM según sus necesidades de servicio.

- Gestión de la seguridad

  HSM dedicado separa la gestión de dispositivos de la gestión de contenido (información confidencial). Como usuario del dispositivo, puede controlar la generación, el almacenamiento y el acceso de claves. HSM dedicado solo es responsable de supervisar y administrar los dispositivos y las instalaciones de red relacionadas. Incluso el personal de O&M no tiene acceso a las claves del cliente.

- Autenticación del permiso
  - Las instrucciones confidenciales se clasifican para la autorización jerárquica, lo que impide efectivamente el acceso no autorizado.
  - Se admiten varios tipos de autenticación, como nombre de usuario/contraseña y certificado digital.

- Confiable
  - El HSM dedicado proporciona HSM de nivel 3 validados por FIPS 140-2 para la protección de sus claves, lo que garantiza servicios de cifrado de alto rendimiento para cumplir con sus estrictos requisitos de seguridad.
  - Cada HSM dedicado tiene sus propios chips. El servicio no se ve afectado incluso si algunos chips están dañados.

- Cumplimiento de seguridad

  Las instancias HSM dedicadas pueden ayudarlo a proteger sus datos en ECS y cumplir con los requisitos de cumplimiento.

- Amplia aplicación

  HSM dedicado ofrece instancias de HSM financiera, HSM de servidor y HSM de servidor de firmas para su uso en diversos escenarios de servicio.

5.3 Escenarios de aplicación

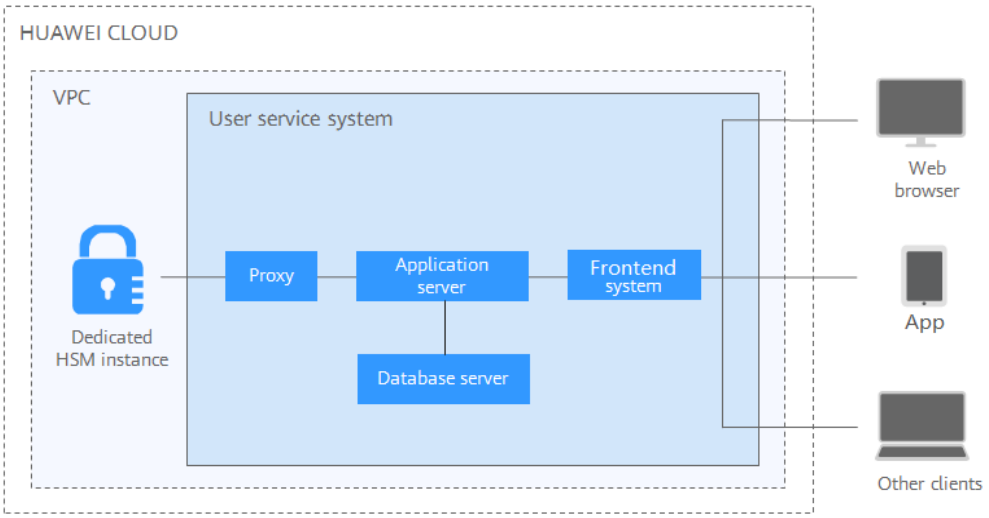
Después de comprar una instancia HSM dedicada, puede usar el UKey proporcionado por HSM dedicado para inicializar y gestionar la instancia. Puede controlar completamente la generación de claves, el almacenamiento y la autenticación de acceso.

Puede utilizar HSM dedicado para cifrar sus sistemas de servicio (incluido la encriptación de datos confidenciales, pagos y tickets electrónicos). HSM dedicado le ayuda a cifrar datos confidenciales de la empresa (como contratos, transacciones y SN) y datos confidenciales del usuario (como números de identificación de usuario y números de móviles), para evitar que los piratas informáticos descifran la red y arrastren la base de datos, lo que puede causar fugas de datos. y evitar el acceso ilegal o la manipulación de los datos por parte de los usuarios internos.

NOTA

Debe implementar el sistema de servicio y instancia de HSM dedicado en la misma VPC y seleccionar las reglas de grupo de seguridad adecuadas. Si tiene alguna pregunta, póngase en contacto con los administradores.

Figura 5-1 Arquitectura



Encriptación de datos confidenciales

Servicios públicos gubernamentales, empresas de Internet y aplicaciones de sistemas que contienen una inmensa información confidencial

Los datos son el activo principal de una empresa. Cada empresa tiene sus datos confidenciales principales. HSM dedicado proporciona comprobación de integridad y almacenamiento cifrado de datos confidenciales, lo que evita eficazmente que los datos confidenciales sean robados o manipulados, y evita el acceso no autorizado.

Finanzas

Aplicaciones de sistema de pago y prepago con tarjeta de transporte, en plataformas de comercio electrónico y por otros medios

HSM dedicado puede garantizar la integridad y confidencialidad de los datos de pago durante la transmisión y el almacenamiento, y garantizar la autenticación de la identidad de pago y el no repudio del proceso de pago.

Verificación

Transporte, fabricación y cuidado de la salud

HSM dedicado puede garantizar la confidencialidad e integridad de los contratos electrónicos, facturas, pólizas de seguro y registros médicos durante la transmisión y el almacenamiento.

6 Descripción de facturación

Artículos de facturación

Los cargos de DEW se basan en su uso y la edición comprada.

Tabla 6-1 Artículos de facturación

Nombre del servicio	Modo de facturación	Artículos de facturación	Descripción
Key Management Service (KMS)	Pago por uso	Cantidad de claves	Las instancias clave que se han creado o importado correctamente se facturan según el pago por uso. Los precios se calculan por hora y no se requiere una tarifa mínima.
	Pago por uso	Solicitudes API	Las primeras solicitudes de API de 20,000 son gratuitas. Se cobran llamadas API adicionales. La unidad es 10,000 llamadas.
KPS	Pago por uso	Número de pares de claves	Gratis
	Pago por uso	Solicitudes API	Gratis
Dedicated HSM	Anual/ Mensual	Edición	Edición platina Para obtener más información, consulte **Ediciones**.
	Pago por uso	Solicitudes API	Gratis

Nombre del servicio	Modo de facturación	Artículos de facturación	Descripción
Cloud Secret Management Service (CSMS)	Pago por uso	Número de credenciales	Las instancias de CSMS que se han creado o importado correctamente se facturan de forma de pago por uso. Los precios se calculan por día, y no se requiere una tarifa mínima.
	Pago por uso	Solicitudes API	Facturado por el número de solicitudes. La unidad es 10,000 solicitudes.

Facturación

- KMS

  Las instancias clave creadas o importadas durante el período de promoción desde el 1 de octubre de 2021 hasta el 31 de marzo de 2022 son permanentemente gratuitas. Las instancias clave creadas o importadas después del 31 de marzo de 2022 se cobrarán.

  KMS se cobra por uso. No se requiere una tarifa mínima. Una vez que se crea una clave, se cargará por hora. Usted paga por las claves que creó y las solicitudes de API que están más allá del rango gratuito.
- KPS
  - Si no decide dejar que Huawei Cloud administre sus claves privadas al crearlas o importarlas, no se incurrirá en ningún costo.
  - Si decides dejar que Huawei Cloud gestione tus claves privadas después de importarlas, KPS se cobra por hora. En la versión actual, es gratuito.
- HSM dedicado

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

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

Para obtener detalles de precios, consulte **Detalles de precios del producto**.

Cambio del modo de facturación

DEW no admite la cancelación de la suscripción actualmente.

Renovación

Si no renueva el servicio DEW facturado anualmente/mensualmente al expirar, un período de retención está disponible para usted.

Para obtener más información sobre el período de retención, consulte **Período de retención**.

Para evitar pérdidas innecesarias causadas por problemas de seguridad, renueve su suscripción antes de que expire el período de retención.

Puede renovar sus recursos en la consola de gestión. Para obtener más información, consulte **Renovación manual de un recurso**.

Vencimiento y pago atrasado

- Vencimeinto

  Si no renueva su suscripción al expirar, hay un período de retención disponible para usted. Para obtener más información, consulte **Período de retención**.

- Pago atrasado

  Si su cuenta tiene una cantidad pendiente, puede ver sus detalles en el Centro de facturación. Para evitar que los recursos relacionados se detengan o liberen, recargue su cuenta a tiempo. Para obtener más información, consulte **Pago de la cantidad pendiente**.

Preguntas frecuentes

Para obtener más preguntas frecuentes sobre facturación, consulte **Preguntas frecuentes sobre DEW**.

7 Gestión de permisos

Si desea asignar diferentes permisos de acceso a los empleados de una empresa para los recursos DEW adquiridos en Huawei Cloud, puede usar Identity and Access Management (IAM) para realizar una gestión de permisos perfeccionada. IAM proporciona autenticación de identidad, gestión de permisos y control de acceso, lo que le ayuda a proteger el acceso a sus recursos en la nube.

Con IAM, puede usar su cuenta de Huawei Cloud para crear usuarios de IAM para sus empleados y asignar permisos a los usuarios para controlar su acceso a tipos de recursos específicos. Por ejemplo, si tiene desarrolladores de software y desea asignarles el permiso para acceder a DEW pero no para eliminar DEW o sus recursos, puede crear una política de IAM para asignar a los desarrolladores el permiso para acceder a DEW pero evitar que eliminen datos relacionados con DEW.

Si la cuenta de Huawei Cloud cumple con sus requisitos y no necesita crear un usuario de IAM independiente para el control de permisos, puede omitir esta sección. Esto no afectará a otras funciones de DEW.

IAM se ofrece de forma gratuita, y usted paga solo por los recursos facturables en su cuenta. Para obtener más información, consulte **Descripción general del servicio IAM**.

Permisos de DEW

De forma predeterminada, los nuevos usuarios de IAM no tienen permisos asignados. Debe agregar un usuario a uno o más grupos y adjuntar directivas o roles de permisos a estos grupos. Los usuarios heredan permisos de sus grupos y pueden realizar operaciones específicas en servicios en la nube según los permisos.

DEW es un servicio a nivel de proyecto implementado y accedido en regiones físicas específicas. Para asignar permisos a un grupo de usuarios, especifique el ámbito como proyectos específicos de la región y seleccione proyectos para que los permisos surtan efecto. Si se selecciona **All projects**, los permisos surtirán efecto para el grupo de usuarios en todos los proyectos específicos de la región. Los usuarios deben cambiar a la región autorizada al acceder a DEW.

Puede conceder permisos a los usuarios mediante roles y políticas.

- Roles: Un tipo de mecanismo de autorización de grano grueso que define permisos relacionados con las responsabilidades del usuario. Este mecanismo proporciona solo un número limitado de roles de nivel de servicio para la autorización. Algunos roles dependen de otros roles para que surtan efecto. Cuando asigne dichos roles a los

usuarios, recuerde asignar los roles de los que dependen. Sin embargo, los roles no son una opción ideal para la autorización detallada y el control de acceso seguro.

- Políticas: Un tipo de mecanismo de autorización detallado que define los permisos necesarios para realizar operaciones en recursos de nube específicos bajo ciertas condiciones. Este mecanismo permite una autorización más flexible basada en políticas, cumpliendo los requisitos para un control de acceso seguro. Por ejemplo, puede conceder a los usuarios de DEW solo los permisos para administrar un determinado tipo de servidores en la nube. La mayoría de las políticas contienen permisos para API específicas y los permisos se definen mediante acciones de API. Para ver las acciones de API admitidas por DEW, consulte **Políticas de permisos y acciones admitidas**.

Tabla 7-1 enumera todas las directivas del sistema de DEW.

Tabla 7-1 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
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 KeypairReadOnlyAc-cess	Permisos de sólo lectura para KPS. Los usuarios con este permiso sólo pueden ver los datos de KPS.	Política del sistema	Ninguno

Tabla 7-2 enumera las operaciones comunes soportadas por cada permiso definido por el sistema de DEW. Seleccione los permisos necesarios.

Tabla 7-2 Operaciones comunes respaldadas por cada política o función definida por el sistema

Operación	Administrador de KMS	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
Crear una clave	√	√	x	x
Habilitar una clave	√	√	x	x

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

Operación	Administrador de KMS	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
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
Enviar mensajes de firma	√	√	x	x
Autenticación de firma	√	√	x	x
Habilitar la rotación de clave	√	√	x	x
Modificar intervalo de rotación de clave	√	√	x	x
Deshabilitar 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

Operación	Administrador de KMS	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
Agregar o eliminar etiquetas de clave por lotes	√	√	x	x
Agregar etiquetas a una clave	√	√	x	x
Eliminar etiquetas de clave	√	√	x	x
Consultar la lista de clave	√	√	x	x
Consultar detalles de clave	√	√	x	x
Consultar clave pública	√	√	x	x
Cantidad de instancia de consulta	√	√	x	x
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

Operación	Administrador de KMS	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
Consultar una tarea de vinculación	x	x	√	√
Consultar tareas fallidas	x	x	√	√
Eliminar todas las tareas con error	x	x	√	x
Eliminar una tarea fallida	x	x	√	x
Consultar tareas en ejecución	x	x	√	√

Enlaces útiles

- **¿Qué es IAM?**
- **Creación de un usuario y autorizar al usuario el permiso de acceso a DEW**
- **Políticas de permisos y acciones admitidas**

8 ¿Cómo acceder?

Huawei Cloud proporciona una plataforma de gestión de servicios basada en web. Puede acceder a DEW mediante la API a través de HTTPS o en la consola de gestión.

- Consola de gestión

  Si se ha registrado en la nube pública, puede iniciar sesión en la consola de gestión directamente. En la esquina superior izquierda de la consola, haga clic en  . Elija **Security & Compliance** > **Data Encryption Workshop**.

- API

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

9 Servicios relacionados

OBS

Object Storage Service (OBS) es un servicio de almacenamiento en la nube optimizado para almacenar las cantidades masivas de datos. Proporciona capacidades de almacenamiento ilimitadas, seguras y altamente confiables con un costo relativamente bajo. KMS proporciona capacidades de gestión y control centrales de CMK para OBS. Se utiliza para la encriptación del lado del servidor con claves gestionadas por KMS (SSE-KMS) en OBS.

EVS

Elastic Volume Service (EVS) ofrece almacenamiento en bloque escalable para servidores en la nube. Con alta confiabilidad, alto rendimiento y especificaciones ricas, los discos EVS se pueden utilizar para sistemas de archivos distribuidos, entornos de desarrollo y pruebas, aplicaciones de almacén de datos y escenarios de computación de alto rendimiento (HPC) para satisfacer diversos requisitos de servicio. KMS proporciona capacidades de gestión y control centrales de CMK para EVS. Se utiliza para encriptación en EVS.

IMS

Image Management Service (IMS) admite la gestión del ciclo de vida de las imágenes. KMS proporciona capacidades de gestión y control centrales de CMK para Image Management Service (IMS). Se utiliza para encriptación de imágenes privadas en IMS.

ECS

Elastic Cloud Server (ECS) es un componente informático básico que consta de CPU, memoria, sistema operativo y EVS. Después de crear un ECS, puede usarlo como su equipo local o servidor físico.

KPS gestiona pares de claves de ECS. Los pares de claves se utilizan para autenticar a los usuarios que inician sesión en los ECS.

HSM dedicado puede cifrar datos confidenciales en los sistemas de servicio de su ECS. Puede controlar la generación, el almacenamiento y la autorización de acceso de las claves para garantizar la integridad y confidencialidad de los datos durante la transmisión y el almacenamiento.

DDS

Document Database Service (DDS) es un servicio de base de datos compatible con MongoDB que es seguro, altamente disponible, confiable, escalable y fácil de usar. Proporciona funciones de creación de instancias de base de datos, escalamiento, redundancia, respaldo, restauración, monitoreo y reporte de alarmas con solo unos pocos clics en la consola DDS. KMS proporciona capacidades de gestión y control centrales de CMK para DDS. Se utiliza para la encriptación de disco en DDS.

CTS

Cloud Trace Service (CTS) le proporciona un historial de operaciones de KMS. Una vez habilitado el servicio CTS, puede ver todas las rastros generados para revisar y auditar las operaciones de KMS realizadas. Para obtener más información, consulte la *Guía de usuario de Cloud Trace Service*.

Tabla 9-1 Operaciones DEW soportadas por CTS

Operación	Tipo de recurso	Nombre del rastro
Creación de un CMK	cmk	createKey
Creación de un DEK	cmk	createDataKey
Creación de un DEK sin texto plano	cmk	createDataKeyWithoutPlaintext
Habilitación de un CMK	cmk	enableKey
Deshabilitación de un CMK	cmk	disableKey
Encriptación de un DEK	cmk	encryptDatakey
Desencriptación de un DEK	cmk	decryptDatakey
Programación de la eliminación de una CMK	cmk	scheduleKeyDeletion
Cancelación de la eliminación programada de un CMK	cmk	cancelKeyDeletion
Generación de números aleatorios	rng	genRandom
Cambio del alias de un CMK	cmk	updateKeyAlias
Cambio de la descripción de un CMK	cmk	updateKeyDescription
Riesgos que provocan la eliminación de CMK	cmk	deleteKeyRiskTips
Importación de material de clave	cmk	importKeyMaterial
Eliminación de material de clave	cmk	deleteImportedKeyMaterial

Operación	Tipo de recurso	Nombre del rastro
Creación de una subvención	cmk	createGrant
Retiro de una subvención	cmk	retireGrant
Revocación de una subvención	cmk	revokeGrant
Encriptación de datos	cmk	encryptData
Desencriptación de datos	cmk	decryptData
Adición de una etiqueta	cmk	dealUnifiedTags
Eliminación de una etiqueta	cmk	dealUnifiedTags
Adición o eliminación de etiquetas en lotes	cmk	dealUnifiedTags
Eliminación de etiquetas por lotes	cmk	batchDeleteKeyTags
Creación o importación de un par de claves SSH	keypair	createOrImportKeypair
Eliminación de un par de claves SSH	keypair	deleteKeypair
Importación de una clave privada	keypair	importPrivateKey
Exportación de una 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

IAM

La gestión de identidades y accesos (IAM) proporciona la función de gestión de permisos para DEW.

Solo los usuarios que tienen permisos de administrador de KMS pueden usar DEW.

Solo los usuarios que tienen los permisos Administrador de KMS y Administrador del servidor pueden usar la función de par de claves.

Para solicitar permisos, póngase en contacto con un usuario con permisos de administrador de seguridad. Para obtener más información, consulte la *Guía de usuario de Identity and Access Management*.

10 Mecanismo de protección de datos personales

Para garantizar que sus datos personales, como el nombre de usuario, la contraseña y el número de teléfono móvil, no sean filtrados u obtenidos por entidades o personas no autorizadas o no autenticadas, DEW controla el acceso a los registros de datos y registros para las operaciones realizadas con los datos.

Datos personales que se recopilarán

Tabla 10-1 enumera los datos personales generados o recopilados por DEW.

Tabla 10-1 Datos personales

Tipo	Origen	Puede ser modificado	Obligatorio
Tenant ID	● ID de inquilino en el token cuando se realiza una operación en la consola. ● ID de inquilino en el token cuando se invoca una API.	No	Sí

Modo de almacenamiento

Los ID de inquilinos no son datos confidenciales y se almacenan en texto plano.

Control de permisos de acceso

Los usuarios solo pueden ver los registros relacionados con sus propios servicios.

Registros de logs

DEW registra los logs de todas las operaciones, como la edición, consulta y eliminación, realizadas sobre datos personales. Los registros se cargan en Cloud Trace Service (CTS). Solo puede ver los registros generados para las operaciones realizadas.

A Historial de cambios

Publicado en	Descripción
2022-03-29	Este es el decimoquinto lanzamiento oficial. Se optimizó la descripción de facturación en **Descripción de facturación**.
2021-12-27	Este es el decimocuarto lanzamiento oficial. Se optimizaron funciones en la sección **Funciones**. Se optimizó la descripción en **Escenarios de aplicación**.
2021-10-26	Este es el trece lanzamiento oficial. Se agregó descripción acerca de la gestión secreta en **CSMS**.
2021-09-30	Este es el duodécimo lanzamiento oficial. ● Se agregaron enlaces a documentos relacionados en la sección **Escenarios de aplicación**. ● Se ha mejorado la descripción de facturación en **Descripción de facturación**.
2021-07-20	Este es el undécimo lanzamiento oficial. Se optimizaron funciones y características optimizadas en **Funciones**.
2021-06-10	Este es el décimo lanzamiento oficial. Se agregó la tabla "Operaciones comunes admitidas por cada política o rol definido por el sistema" en **Gestión de permisos**.
2020-12-14	Este es el noveno lanzamiento oficial. Agregó **Mecanismo de protección de datos personales**.
2020-05-27	Este es el octavo lanzamiento oficial. Agregó **Descripción de facturación**.

Publicado en	Descripción
2020-02-10	Este es el séptimo lanzamiento oficial. Se modificaron nombres de política de sistema DEW en la sección "Gestión de permisos" en el capítulo "Descripción general del servicio" basado en cambios de IAM GUI: cambió **DEW Keypair Admin** a **DEW KeypairFullAccess**, **DEW Keypair Viewer** a **DEW KeypairReadOnlyAccess**, y **KMS CMK Admin** a **KMS CMKFullAccess**.
2019-12-03	Este es el sexto lanzamiento oficial. Se agregó la sección "Encriptación del servidor RDS".
2019-07-04	Este es el quinto lanzamiento oficial. ● Se agregó el proceso de uso en **Uso de KMS**. ● Optimizó **Gestión de permisos**.
2019-03-30	Este es el cuarto lanzamiento oficial. Se optimizó la estructura del documento para proporcionar a los usuarios una mejor referencia.
2018-05-30	Este es el tercer lanzamiento oficial. ● Se modificó la sección "Funciones": agregó descripción sobre la vinculación, desvinculación, restablecimiento y sustitución de un par de claves. ● Se agregó una descripción sobre la importación y exportación de claves privadas en **Servicios relacionados**.
2018-01-30	Esta edición es el segundo lanzamiento oficial. ● Agregó la sección "Par de claves SSH". ● Modificó la sección "Escenarios de aplicación": se agregó la parte "Autentificación de usuarios que inician sesión en ECS." ● Modificó la sección "Funciones": agregó descripciones sobre la creación, importación y eliminación de pares de claves. ● Modificó sección **Uso de KMS**: agregó una descripción sobre ECS. ● Modificó sección **Servicios relacionados**: agregó la descripción acerca de la relación con ECS
2017-12-31	Este es el primer lanzamiento oficial.