Data Encryption Workshop

Descripción general del servicio

Edición 15

Fecha 2024-09-13

HUAWEI TECHNOLOGIES CO., LTD.

Marcas y permisos


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

Aviso

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

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

Huawei Technologies Co., Ltd.

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

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

Email: support@huawei.com

Índice

1 ¿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. Proporciona services such as Key Management Service (KMS), Cloud Secret Management Service (CSMS), Key Pair Service (KPS), y Dedicated Hardware Security Module (Dedicated HSM). DEW protege sus datos y claves y simplifica la gestión de claves. DEW utiliza módulos de seguridad de hardware (HSM) para proteger la seguridad de sus claves y se puede integrar con varios servicios de Huawei Cloud. Además, DEW le permite desarrollar aplicaciones de encriptación personalizadas.

Figura 1-1 Subservicios de DEW

Tabla 1-1 Descripción 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. HSM cumple con los requisitos de seguridad FIPS 140-2 Nivel 3. Le ayuda a crear y gestionar claves. Todas las claves están protegidas por claves raíz en HSM para evitar fugas de claves.	**Tipos de clave**
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 secreto. 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 los HSM 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 un par de claves**

Servicio	Descripción	Referencia
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 la encriptación y desencriptación de datos.	**HSM dedicado**

2 Basic Concepts

To help you understand and use DEW better, this document describes the related basic terms.

Tabla 2-1 Common encryption terms

Term	Definition	More info
Symmetric key encryption	Symmetric key encryption is also called dedicated key encryption. The sender and receiver use the same key to encrypt and decrypt data. Advantage: Encryption and decryption are fast. Disadvantage: Each pair of keys must be unique. Key management is difficult if there are a large number of users. Scenario: Encrypt a large amount of data.	**Key Types**
Asymmetric key encryption	Asymmetric key encryption is also called public key encryption. A pair of keys are used for encryption and decryption. One is a public key, and the other is a private key. Advantage: Different keys are used for encryption and decryption, enhancing security. Disadvantage: Encryption and decryption are slow. Scenario: Encrypt sensitive information.	**Key Types**
Hash-based Message Authentication Code (HMAC)	HMAC combines information with keys and encrypts the result using a hash function to protect information integrity and verify information.	-

Term	Definition	More info
Digital signature	A digital signature is also known as a public key digital signature, which is used to verify the authenticity and integrity of a message. After a message is encrypted using a private key and is sent, the receiver uses a public key to decrypt the message. The security of electronic files are protected by comparing the signature information.	-

Tabla 2-2 KMS terms

Item	Definition	Reference
Hardware Security Module (HSM)	An HSM is a type of computer hardware that protects and manages the keys used by strong authentication systems and provides related cryptographic operations.	-
Customer Master Key (CMK)	A CMK is a Key Encryption Key (KEK) created by a user or cloud service using KMS. It is used to encrypt and protect Data Encryption Keys (DEKs). One CMK can be used to encrypt one or more DEKs. CMKs are categorized into custom keys and default keys.	**What Is a Customer Master Key?**
Default key	A default key is automatically created by another cloud service using KMS, such as Object Storage Service (OBS). The alias of a default key ends with **/default**.	**What Is a Default Key?**
Key material	Key materials are important input for cryptographic operations. A CMK consists of a key ID, metadata, and a key material.	-
Envelope encryption	Envelope encryption is the practice of encrypting data with a DEK and then encrypting the DEK with a root key that you can fully manage. In this case, CMKs are not required for encryption or decryption.	**What Are the Benefits of Envelope Encryption?**
Data Encryption Key (DEK)	A DEK is used to encrypt data.	**What Is a Data Encryption Key?**

Tabla 2-3 SSH key pair terms

Term	Definition	More info
SSH key pair	An SSH key pair is used for encrypting and verifying SSH network connections. Each SSH key pair consists of a private key and a public key. ● A private key is an encrypted file which can only be accessed by the owner. ● A public key is an unencrypted file which can be shared with anyone. If you are connecting to another user's computer, you can use the public key to encrypt messages and the private key to decrypt. The private key can be accessed only by the owner and the public key can be shared with others. As a result, SSH key pairs are more secure than conventional password verification.	**Key Pair Service**
Private key pair	A private key pair can be viewed or used only by the current account.	**Creating a Key Pair**
Account key pair	An account key pair can be viewed or used by all users under the account.	**Upgrading a Key Pair**

3 KMS

3.1 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 claves están protegidas por claves raíz en HSM para evitar fugas de claves. El módulo HSM cumple con los requisitos de seguridad FIPS 140-2 Nivel 3.

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

Funciones

- En la consola KMS, puede:
  - Crear, consultar, habilitar y deshabilitar CMK, así como programar y cancelar la eliminación de CMK.
  - Modificar el alias y las descripciones de los CMK.
  - Utilizar la herramienta en línea para cifrar y descifrar datos de pequeño tamaño.
  - Agregar, buscar, editar y eliminar etiquetas.
  - Crear, cancelar y consultar concesiones.
- Puedes usar las API para:
  - Crear, cifrar o descifrar DEK.
  - Retirar concesiones.
  - Firmar o verificar la firma de los mensajes o resúmenes de mensajes.
  - Generar y verificar códigos de autenticación de mensajes.

  Para obtener más información, consulta la *Referencia de la API de Data Encryption Workshop*.
- Generar hardware verdaderos números aleatorios.

  Puede generar números aleatorios de 512 bits basados en hardware mediante la API de KMS. Los números aleatorios verdaderos de 512 bits se pueden usar como base para

materiales clave y parámetros de encriptación. Para obtener más información, consulta la *Referencia de la API de Data Encryption Workshop*.

Algoritmos de clave soportados por KMS

Las claves simétricas creadas en la consola KMS utilizan los algoritmos AES y SM4. Las claves asimétricas creadas por KMS soportan RSA, SM2, y los algoritmos ECC.

Tabla 3-1 Algoritmos de clave soportados por KMS

Tipo de clave	Tipo de algoritmo	Especificaciones de clave	Descripción	Escenario de aplicación
Clave simétrica	AES	AES_256	Clave simétrica de AES	● La encriptación y desencriptación de datos ● Cifrado y descifrado de los DEK **NOTA** Puede cifrar y descifrar una pequeña cantidad de datos utilizando la herramienta en línea en la consola. Necesita invocar a las API para cifrar y descifrar una gran cantidad de datos.
Symmetric key	AES	● HMAC_256 ● HMAC_384 ● HMAC_512	Clave simétrica de HMAC	Genera y verifica un código de autenticación de mensaje

Tipo de clave	Tipo de algoritmo	Especificaciones de clave	Descripción	Escenario de aplicación
Asymmetric key	RSA	● RSA_2048 ● RSA_3072 ● RSA_4096	Contraseña asimétrica de RSA	● Firma digital y verificación de firma ● La encriptación y desencriptación de datos **NOTA** Las claves asimétricas son aplicables a escenarios de firma y verificación de firma. Las claves asimétricas no son lo suficientemente eficientes para la encriptación de datos. Las claves simétricas son adecuadas para cifrar y descifrar datos.
	ECC	● EC_P256 ● EC_P384	Curva elíptica recomendada por NIST	Firma digital y verificación de firma

describe los algoritmos de cifrado y descifrado compatibles con las claves importadas por el usuario.

Tabla 3-2 Algoritmos de envoltura de claves

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

3.2 Ventajas

Amplia integración de servicios

- Al integrarse con OBS, EVS e IMS, puede usar KMS para gestionar las claves de los servicios o usar las API de KMS para cifrar y descifrar datos locales.
- Al integrar con Cloud Trace Service (CTS), puede usar CTS para ver los registros de operaciones KMS recientes.

Cumplimiento reglamentario

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

Fácil de usar

Puede usar y gestionar claves fácilmente usando la consola o las API, no es necesario comprar dispositivos de encriptación de hardware.

3.3 Escenarios de aplicación

Prerrequisitos

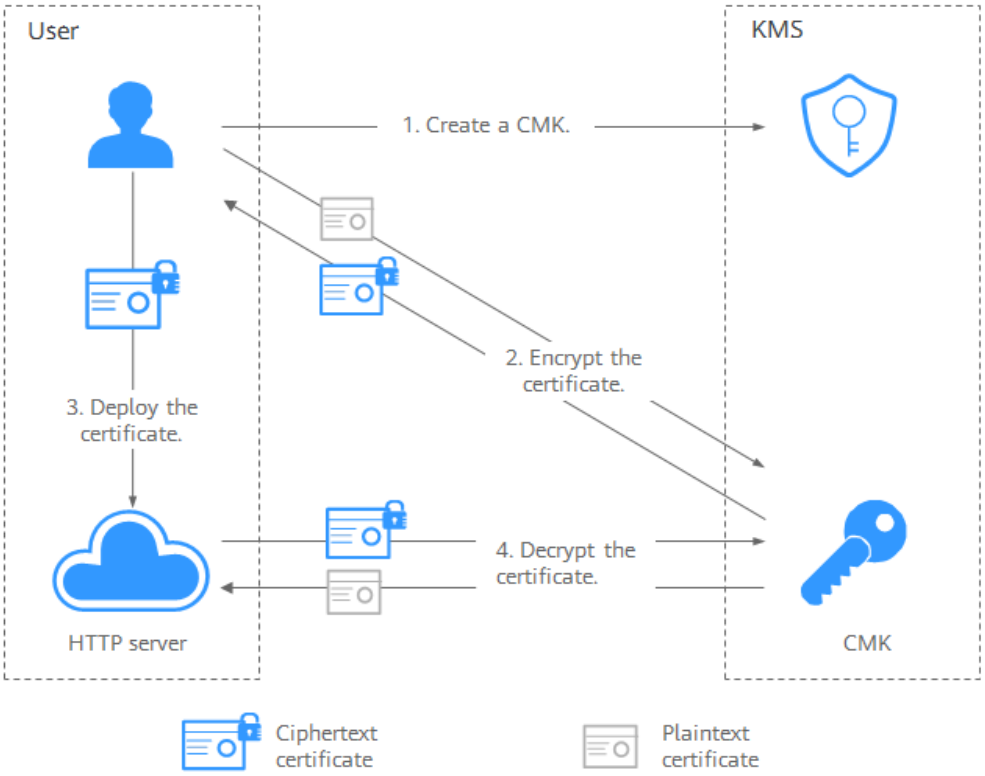
Todas las claves personalizadas mencionadas en esta sección son claves simétricas. Para obtener más información sobre las claves simétricas y las claves asimétricas, consulte **Tipos de claves**.

Cifrado y descifrado de datos pequeños

Puede utilizar la herramienta en línea en la consola de KMS o invocar 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 3-1 muestra un ejemplo sobre cómo invocar a las API para cifrar y descifrar un certificado HTTPS.

Figura 3-1 Cifrado y descifrado de un certificado HTTPS



El procedimiento es el siguiente:

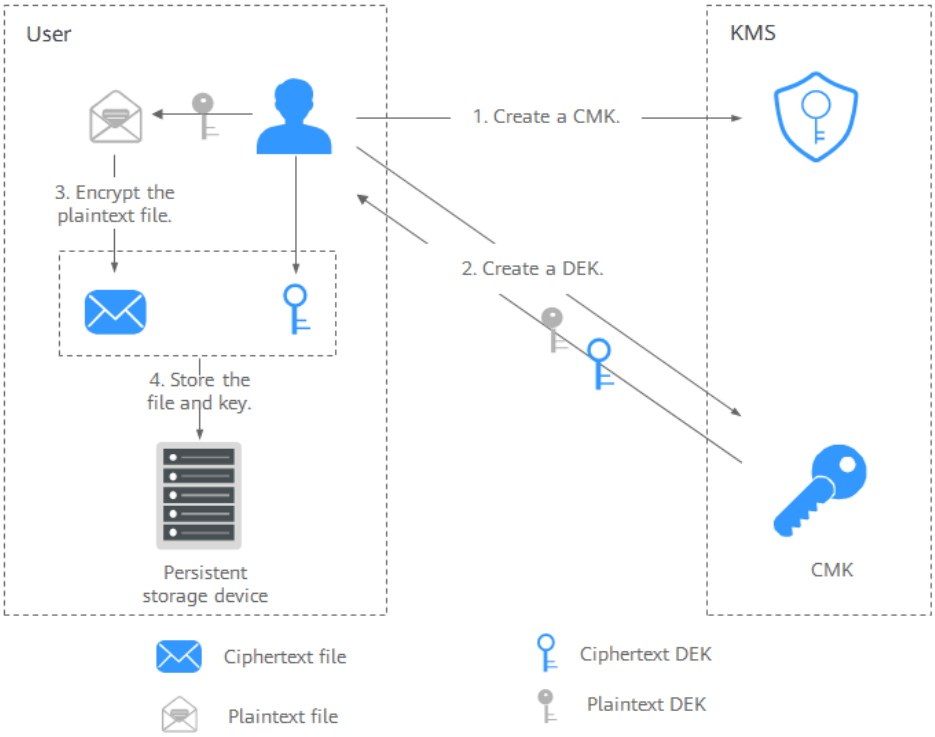
1. Crear un CMK en KMS.
2. Invocar a la API **encrypt-data** de KMS y usar el CMK para cifrar el certificado de texto sin formato.
3. Desplegar el certificado en un servidor.
4. El servidor invoca a la API de **decrypt-data** de KMS para descifrar el certificado de texto cifrado.

Cifrado y descifrado de datos grandes

Si desea cifrar o descifrar grandes volúmenes de datos, como imágenes, vídeos y archivos de bases de datos, puede utilizar el método de cifrado envolvente, en el que no es necesario transferir los datos a través de la red.

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

Figura 3-2 Cifrado de un archivo local



El procedimiento es el siguiente:

a. Crear un CMK en KMS.

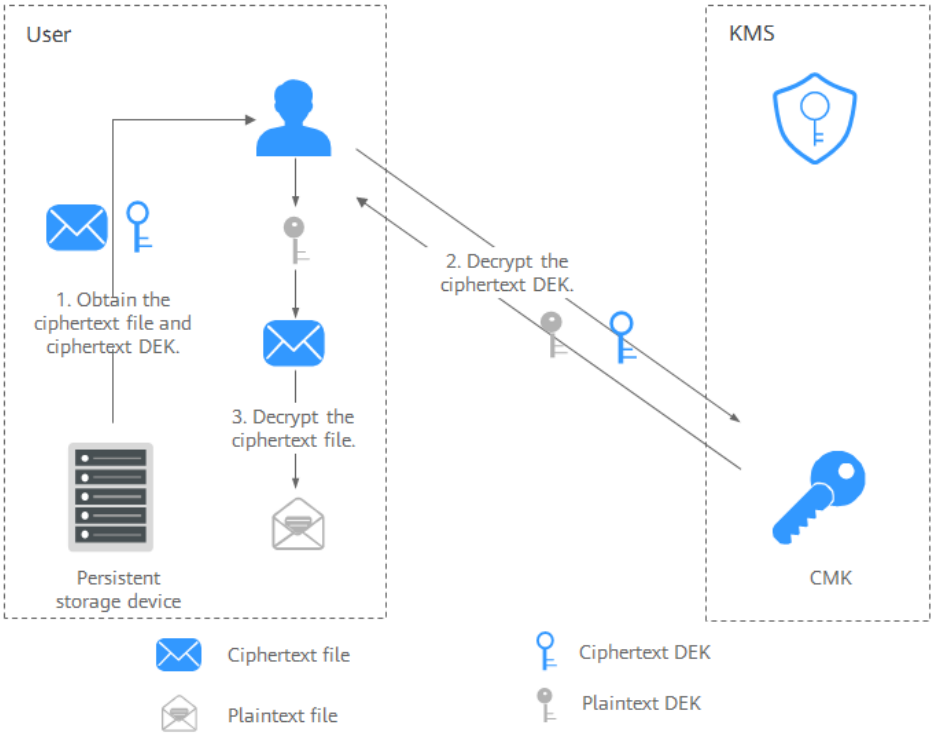
b. Invocar a la API **create-datakey** y de KMS para crear un DEK. Luego obtiene un DEK de texto plano y un DEK de texto cifrado. El DEK de texto cifrado se generó usando una clave personalizada para cifrar el DEK de texto sin formato.

c. Utilizar el DEK de texto sin formato para cifrar el archivo. Se genera un archivo de texto cifrado.

d. Guardar el DEK de texto cifrado y el archivo de texto cifrado juntos en un dispositivo de almacenamiento persistente o un servicio de almacenamiento.

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

Figura 3-3 Descifrar un archivo local



El procedimiento es el siguiente:

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

b. Invoque 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 obtiene 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 recomendadas	● **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**

3.4 Uso de KMS

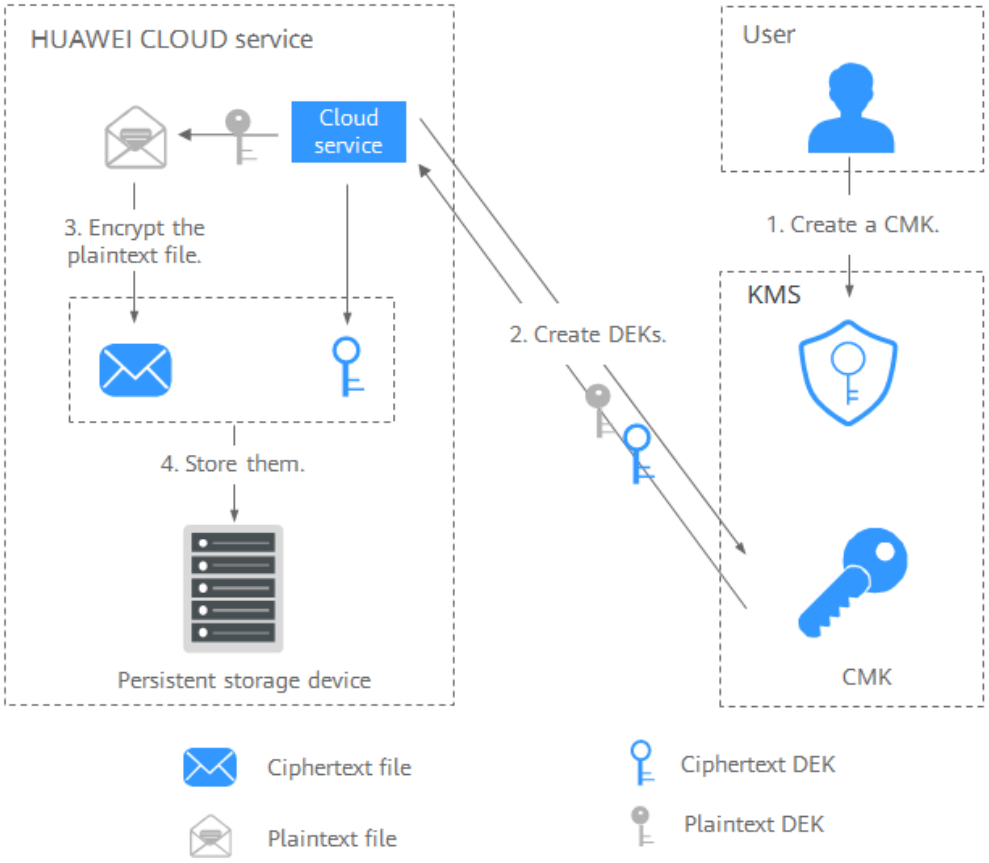
Prerrequisitos

Todas las claves personalizadas mencionadas en esta sección son claves simétricas. Para obtener más información sobre las claves simétricas y las claves asimétricas, consulte **Tipos de claves**.

Interactuar con servicios de Huawei Cloud

Servicios de Huawei Cloud utilizan la tecnología de encriptación de sobres e invocan a las API de KMS para cifrar los recursos de servicio. Sus CMK están bajo su propia gestión. Con su concesión, servicios de Huawei Cloud utilizan una clave personalizada específica para cifrar datos.

Figura 3-4 Cómo Huawei Cloud utiliza KMS para encriptación



El proceso de encriptación es el siguiente:

1. Cree una clave personalizada en KMS.
2. Servicios de Huawei Cloud invocan a la API **create-datakey** del KMS para crear un DEK. Luego obtiene 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. Servicios de Huawei Cloud utilizan el DEK de texto sin formato para cifrar un archivo de texto sin formato, generando un archivo de texto cifrado.
4. Servicios de Huawei Cloud 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 la clave personalizada especificada 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 3-3 Lista de servicios en la nube que utilizan encriptación KMS

Nombre del servicio	Descripción
Object Storage Service (OBS)	Puede cargar objetos y descargarlos desde Object Storage Service (OBS) en modo común o en modo de encriptación del servidor. Cuando carga objetos en modo de encriptación, los datos se cifran en el lado del servidor y luego se almacenan de forma segura en OBS en texto de encriptación. Cuando descarga objetos cifrados, los datos en texto cifrado se descifran en el lado del servidor y luego se le proporcionan en texto sin formato. OBS admite la encriptación del lado del servidor con el modo de claves gestionadas por KMS (SSE-KMS). En el modo SSE-KMS, OBS utiliza las claves proporcionadas por KMS para encriptación del lado del servidor. Para obtener detalles acerca de cómo cargar objetos a OBS en modo SSE-KMS, consulte **Guía de operación de consola de Object Storage Service**.
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 detalles sobre cómo utilizar la función de encriptación de EVS, consulte **Guía de usuario de Elastic Volume Service**.
Image Management 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 Image Management Service (IMS), consulte **Guía de usuario de Image Management Service**.

Nombre del servicio	Descripción
Scalable File Service (SFS)	Al crear un sistema de archivos en SFS, el CMK proporcionado por KMS se puede seleccionar para cifrar el sistema de archivos, de modo que los archivos almacenados en el sistema de archivos se cifran automáticamente. Para obtener más información acerca de cómo utilizar la función de encriptación del sistema de archivos de SFS, consulte **Guía de usuario de Scalable File Service**.
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 detalles acerca de cómo utilizar la función de encriptación de disco de RDS, consulte **Guía de usuario de Relational Database Service**.
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 **Pasos iniciales de Document Database Service**.

Trabajar con aplicaciones de usuario

Para cifrar datos de texto sin formato, una aplicación de usuario puede invocar 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 invocar 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 los CMK almacenados en KMS y los DEK de texto encriptación en aplicaciones de usuario. KMS es invocado para descifrar un texto cifrado DEK solo cuando es necesario.

El proceso de encriptación es el siguiente:

1. La aplicación invoca a la API **create-key** de KMS para crear una clave personalizada.
2. La aplicación invoca 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.

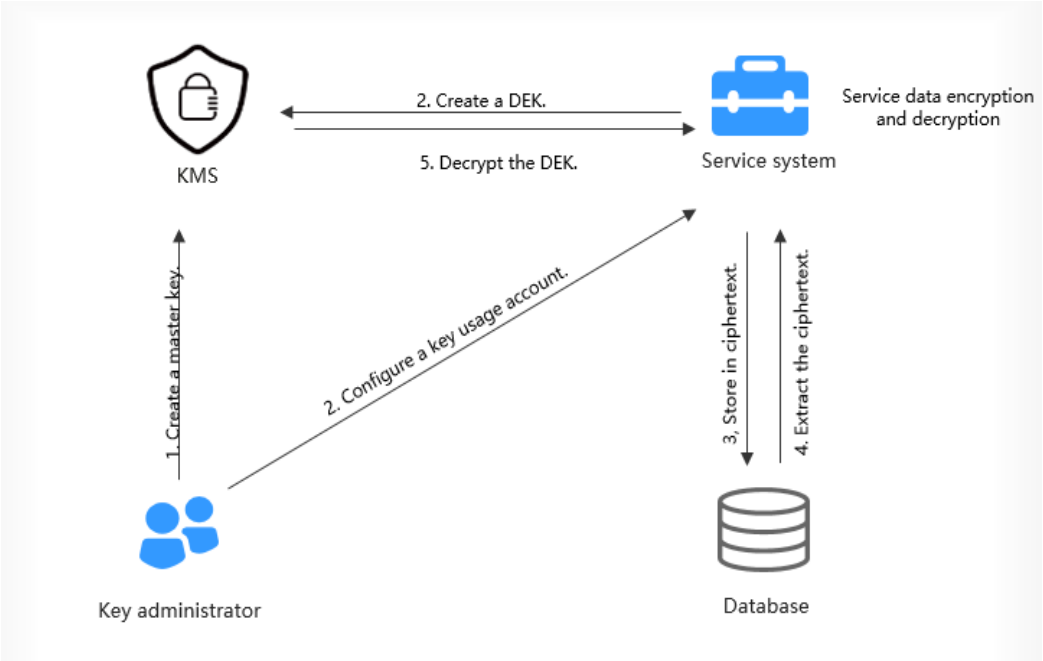
4. La aplicación guarda el DEK de texto cifrado y el archivo de texto cifrado juntos en un dispositivo de almacenamiento persistente o un servicio de almacenamiento.

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

3.5 Example Scenario

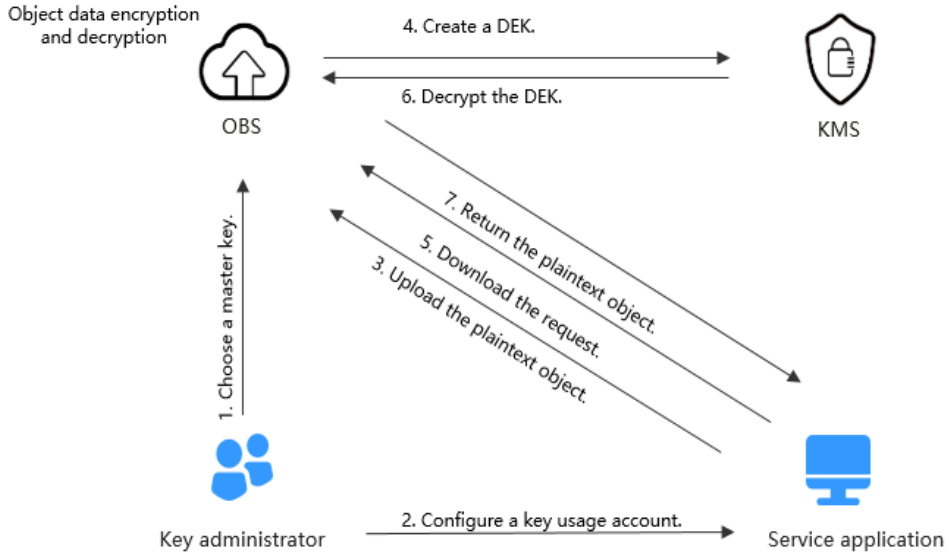
User-Integrated KMS to Applications

Figura 3-5 Principles of user-integrated KMS to applications



Encrypting and Decrypting a Cloud Service Integrated with KMS

Figura 3-6 Principles of a cloud service integrated with KMS



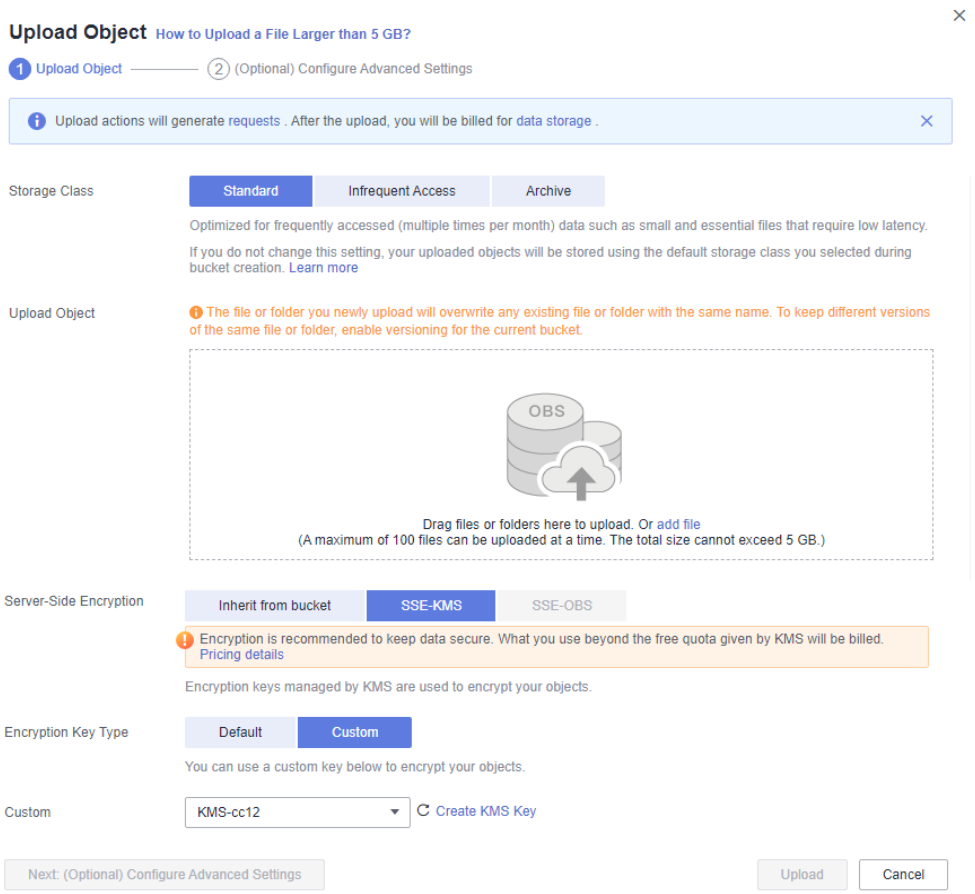
- For details about how to use KMS, see **Using KMS to Encrypt and Decrypt Data for Cloud Services**.
- For details about how to encrypt or decrypt a large amount of data, see **Encrypting or Decrypting a Large Amount of Data**.

3.6 Servicios en la nube con KMS integrado

3.6.1 Encriptación de datos en OBS

- Cuando utilice Object Storage Service (OBS) para cargar datos con encriptación del servidor, puede seleccionar **SEE-KMS encryption** y utilizar la clave proporcionada por KMS para cifrar los archivos que se van a cargar. Para más detalles, consulte **Figura 3-7**. Para obtener más información, consulte *Guía de usuario de Object Storage Service*.

Figura 3-7 Encriptación del lado del servidor OBS



Hay dos tipos de CMK que se pueden utilizar:

– La clave predeterminada **obs/default** creada por KMS

– Claves personalizadas creadas en la consola KMS

- Alternativamente, puede invocar 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*.

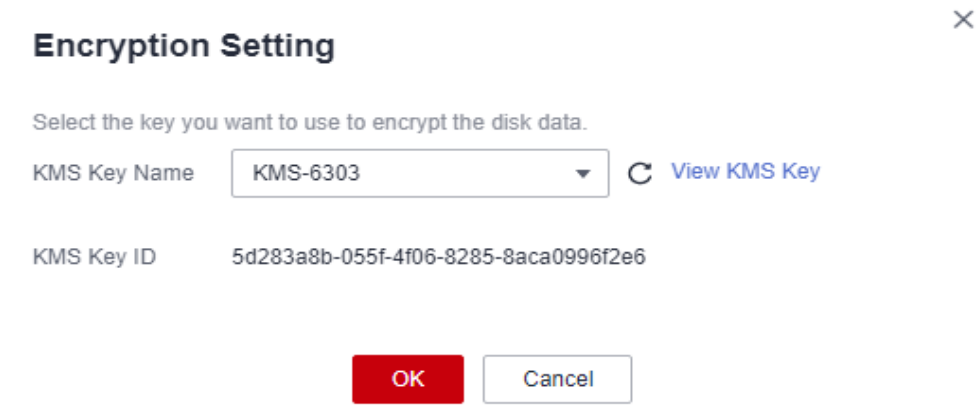
3.6.2 Encriptación de datos en EVS

- Al comprar un disco, puede elegir **Advanced Settings** > **Encryption** para cifrar el disco con la clave proporcionada por KMS. Para más detalles, consulte **Figura 3-8**. Para obtener más información acerca de EVS, consulte la Guía del usuario de *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 del usuario de *Guía del usuario de Elastic Volume Service*.

Figura 3-8 Encriptación de datos en EVS



Hay dos tipos de CMK que se pueden utilizar:

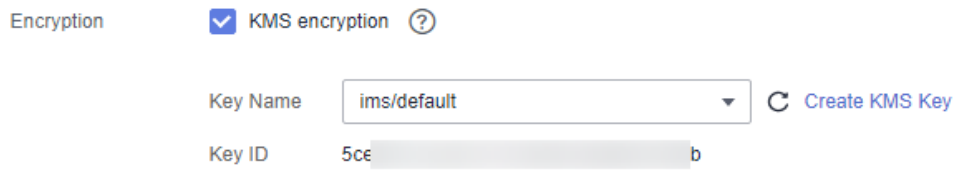
- La clave predeterminada **evs/default** creada por KMS
- Claves personalizadas que cree en la consola de KMS con materiales de clave generados por KMS

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

3.6.3 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. **Figura 3-9** describe detalles. Para obtener más información, consulte *Guía de usuario de Image Management Service*.

Figura 3-9 Encriptación de datos en IMS



Hay dos tipos de CMK que se pueden utilizar:

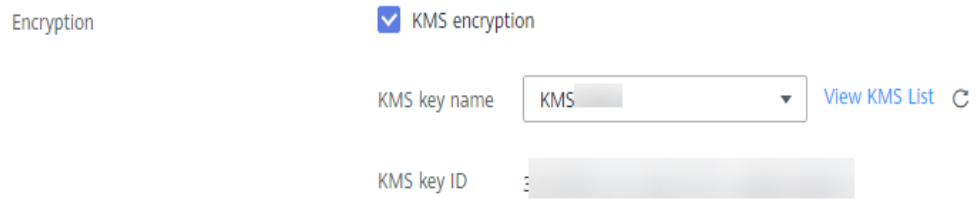
- La clave predeterminada **ims/default** creada por KMS
- Claves personalizadas que cree en la consola de KMS con materiales de clave generados por KMS

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

3.6.4 Cifrado de datos en SFS

- Al crear un sistema de archivos mediante el servicio de archivos escalable (SFS), puede seleccionar **KMS encryption** y utilizar la clave proporcionada por el KMS para cifrar el sistema de archivos. Para más detalles, véase **Figura 3-10**. Para obtener más información, consulte *Guía de usuario de Scalable File Service*.

Figura 3-10 Cifrado de datos en SFS



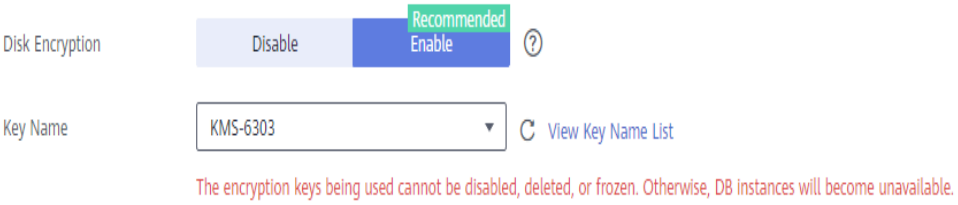
Puede utilizar una clave personalizada creada en la consola KMS para la encriptación.

- Puede utilizar la API de SFS para crear un sistema de archivos cifrado. Para obtener más información, consulte el *Referencia de API de Scalable File Service*.

3.6.5 Encriptación de datos en RDS

- Cuando un usuario compra una instancia de base de datos desde el Relational Database Service (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 3-11 Encriptación de datos en RDS



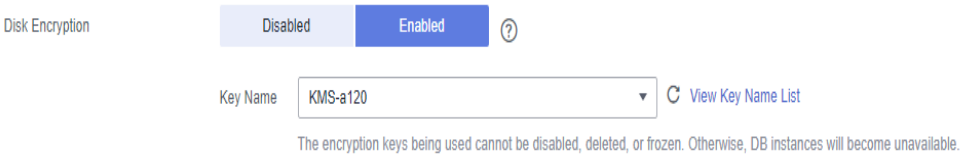
Puede utilizar una clave personalizada creada en la consola KMS para la encriptación.

- También puede invocar 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*.

3.6.6 Encriptación de datos en DDS

- Cuando un usuario compra una instancia de base de datos desde 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 *Guía de usuario de Document Database Service*.

Figura 3-12 Encriptación de datos en DDS



Puede utilizar una clave personalizada creada en la consola KMS para la encriptación.

- También puede invocar 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*.

4 CSMS

4.1 Funciones

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 secreto. 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. Coleccione secretos.
2. Suba 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, invoca a las API de CSMS para recuperar secretos. No se requieren secretos codificados ni de texto sin formato.

Rotación de credenciales y claves

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 invocar 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 de secreto en la consola CSMS o a través de API y actualiza el secreto.
2. Las aplicaciones invocan 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. Repita regularmente los pasos **1** y **2** para rotar secretos.
4. Habilite la rotación de las claves de encriptación para mejorar la seguridad del almacenamiento.

Notificación de Evento Secreto

Después de suscribirse a un evento asociado para un objeto secreto, si el evento está habilitado y se desencadena un evento básico en el objeto secreto, se envía una notificación de evento al tema de notificación especificado por el evento a través de Notificación de mensaje simple (SMN). Los tipos de eventos básicos incluyen la creación de nueva versión secreta, la expiración de la versión secreta, la eliminación secreta y la rotación secreta. Después de configurar la notificación de eventos, puede utilizar las funciones gestionadas basadas en eventos de FunctionGraph para rotar automáticamente los secretos.

Realice las siguientes operaciones para gestionar secretos mediante CSMS:

1. El administrador agrega un evento en la consola de notificación de eventos CSMS o invocando a la API.

2. Al crear o actualizar un secreto, debe asociar el objeto de evento necesario para la suscripción.

3. Recibirá una notificación de evento cuando cambie el estado de secreto. Puede configurar funciones de FunctionGraph para actualizar o rotar secretos automáticamente.

Características básicas de CSMS

Tabla 4-1 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 de secreto y la descripción.

Función	Descripción
Gestión de versión de secreto	● Crear y ver versiones secretas. ● Ver valores secretos. ● Establecer configuraciones de caducidad de versión de secreto.
Gestión de estado de versión de secreto	Actualizar, consultar y eliminar versiones de secreto.
Gestión de etiquetas de secreto	Agregar, buscar, editar y eliminar etiquetas.
Gestión de evento de secreto	● Crear, ver y eliminar eventos ● Cambio de tipos de evento de secreto
Gestión de notificaciones de secreto	Vea el tipo de evento de cambio, el nombre del evento y el nombre de secreto.

4.2 Ventajas

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 invoca 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 e identidades de IAM garantiza que solo los usuarios autorizados puedan recuperar y modificar las credenciales. El CTS supervisa el acceso a las credenciales. Estos servicios evitan el acceso no autorizado y la violación de información confidencial.

Notificación de cambio secreto

SMN notifica a los usuarios de los cambios de eventos secretos básicos de manera oportuna. FunctionGraph se utiliza para configurar funciones para actualizar o rotar secretos automáticamente.

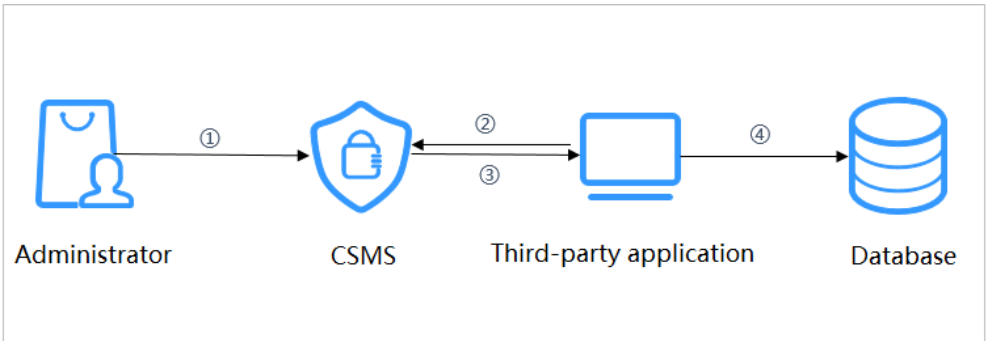
Invocaciones secretas seguras

CCE permite a los usuarios montar secretos en los pods. De esta manera, la información sensible puede desacoplarse del entorno de agrupamiento, lo que evita la fuga de información causada por la codificación dura del programa o la configuración de texto plano.

4.3 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 4-1 Proceso de inicio de sesión basado en secreto



El procedimiento es el siguiente:

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 secreto, y devuelve de forma segura la información almacenada en el secreto a la aplicación a través de la API de gestión de secretos.

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

----Fin

5 KPS

5.1 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, incluidas una clave pública y una clave privada, se generan en base a un algoritmo criptográfico. 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. Por lo tanto, no tendrá que preocuparse por la interceptación, el cracking o la filtración de contraseñas.

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, vinculación y desvinculación de pares de claves
- Gestión, importación, exportación y borrado de claves privadas

Algoritmos criptográficos soportados por KPS

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

  - SSH-DSS
  - SSH-ED25519
  - ECDSA-SHA2-NISTP256
  - ECDSA-SHA2-NISTP384
  - ECDSA-SHA2-NISTP521
  - SSH_RSA: La longitud puede ser de 2048, 3072, 4096 bits.

5.2 Ventajas

- Seguridad de inicio de sesión reforzado

  Puede iniciar sesión en un ECS de Linux sin introducir una contraseña, evitando efectivamente la interceptación de contraseñas, grietas o fugas y mejorando la seguridad de ECS de Linux.
- Cumplimiento 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.

5.3 Escenarios de aplicación

Al comprar un ECS que ejecuta 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 que ejecute 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 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 uno 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 la contraseña para iniciar sesión en un ECS de Windows

Si su ECS ejecuta 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 uno de los siguientes pares de claves:

- Pares de claves creados o importados a 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.

6 HSM dedicado

6.1 Infografías de HSM dedicado

6.2 Funciones

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

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

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

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

Tabla 6-1 Algoritmos de criptografía compatibles

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

Tipos de HSM dedicados

Tabla 6-2 Tipos de HSM dedicados

Tipo de HSM	Función	Escenario de aplicación
Módulo de seguridad de hardware (HSM)	● Cifrado y descifrado de datos ● Firma de datos y verificación. ● Resumen de datos ● Generación y verificación de direcciones MAC	Cálculos básicos de contraseñas en aplicaciones de una amplia gama de industrias, como autenticación de identidad, protección de datos, claves SSL y descarga de computación.
Finanzas	● Generación, encriptación, conversión y verificación del número de identificación personal (PIN) ● Generación y verificación de control de acceso a medios (MAC) ● Generación y verificación del valor de verificación de la tarjeta (CVV) ● Generación y verificación del tipo de código de asignación (TAC) ● Conjunto de instrucciones Racal típico ● Conjunto de instrucciones comunes del Banco Popular de China (PBOC) 3.0	Cálculo criptográfico en sistemas financieros, tales como sistemas de emisión de tarjetas y sistemas de punto de venta (POS)
Servidor de verificación de firmas	● Firma y verificación de firma ● Codificación y decodificación de envolventes digitales ● Codificación y decodificación de envolventes digitales firmadas ● Verificación de certificados	Uso de firmas en sistemas de Autoridad de Certificación (CA), verificación de certificados, transmisión cifrada de una gran cantidad de datos y autenticación de identidad

6.3 Ventajas

- 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 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 gestionar 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.
  - HSM dedicado proporciona soluciones confiables de respaldo y alojamiento para datos HSM.
- Certificación 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.

6.4 Escenarios de aplicación

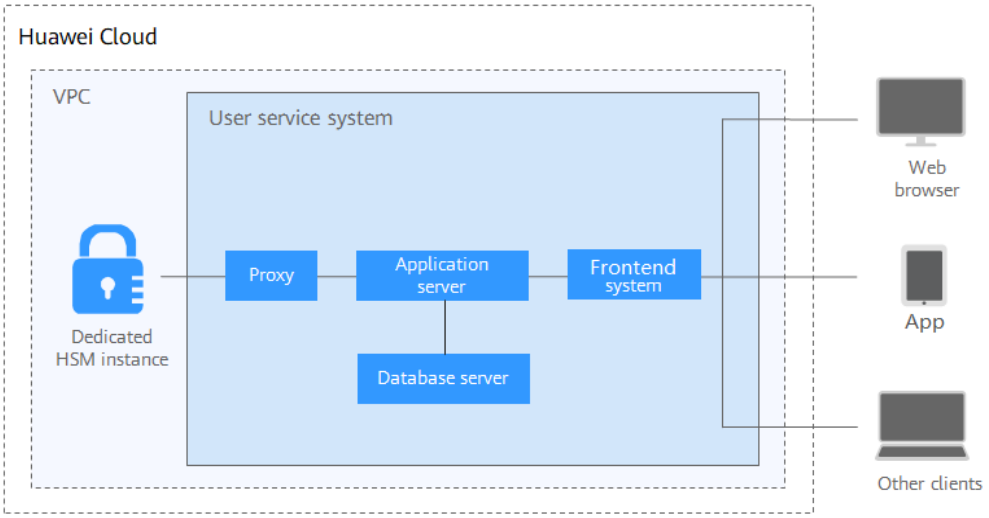
Después de comprar una instancia HSM dedicada, puede usar el UKey proporcionado por HSM dedicado para inicializar y gestionar la instancia. Puede controlar completamente la generación de claves, el almacenamiento y la autenticación de acceso.

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 desplegar el sistema de servicio e 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 personal de soporte técnico.

Figura 6-1 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.

6.5 Ediciones

HSM dedicado proporciona instancias de la edición platino (fuera de China continental). Para obtener más información, véase **Tabla 6-3**.

Tabla 6-3 HSM dedicado

Edición	Modo de facturación	Alcance del servicio
Edición platino (fuera de China continental)	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. • Escalabilidad 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 balanceo 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 las PKCS#11 y CSP. • 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 HSM certificado por FIPS 140-2 nivel 3 para generar claves de cifrado.

7 Seguridad

7.1 Responsabilidades compartidas

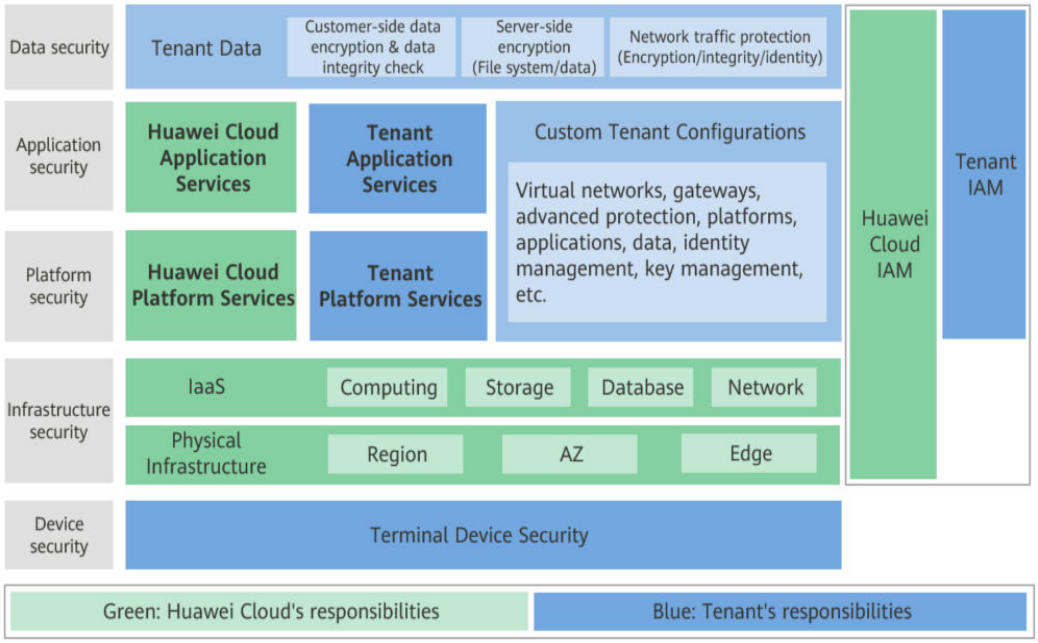
Huawei garantiza que su compromiso con la seguridad cibernética nunca se verá compensado por la consideración de intereses comerciales. Para hacer frente a los desafíos emergentes de seguridad en la nube y a las amenazas y ataques generalizados de seguridad en la nube, Huawei Cloud crea un sistema integral de garantía de seguridad de servicios en la nube para diferentes regiones e industrias basado en las ventajas únicas de software y hardware, las leyes, las regulaciones, los estándares de la industria y el ecosistema de seguridad de Huawei.

Figura 7-1 ilustra las responsabilidades compartidas por Huawei Cloud y los usuarios.

- **Huawei Cloud**: Garantizar la seguridad de los servicios en la nube y proporcionar nubes seguras. Las responsabilidades de seguridad de Huawei Cloud incluyen garantizar la seguridad de nuestros servicios IaaS, PaaS y SaaS, así como los entornos físicos de los centros de datos de Huawei Cloud donde nuestros IaaS, PaaS, y los servicios SaaS operan. Huawei Cloud es responsable no solo de las funciones de seguridad y el rendimiento de nuestra infraestructura, servicios en la nube y tecnologías, sino también de la seguridad general de la nube y, en el sentido más amplio, del cumplimiento de seguridad de nuestra infraestructura y servicios.
- **Tenant**: Utilizar la nube de forma segura. Los inquilinos de Huawei Cloud son responsables de la gestión segura y efectiva de las configuraciones personalizadas por el inquilino de los servicios en la nube, incluidos IaaS, PaaS y SaaS. Esto incluye, entre otros, redes virtuales, el sistema operativo de los hosts e invitados de máquinas virtuales, firewalls virtuales, API Gateway, servicios de seguridad avanzados, todo tipo de servicios en la nube, datos del inquilino, cuentas de identidad, y gestión de claves.

Libro blanco de seguridad de Huawei Cloud elabora las ideas y medidas para construir la seguridad en Huawei Cloud, incluidas las estrategias de seguridad en la nube, el modelo de responsabilidad compartida, el cumplimiento y la privacidad, las organizaciones y el personal de seguridad, la seguridad de la infraestructura, el servicio y la seguridad del inquilino, la seguridad de ingeniería, seguridad de O&M y seguridad del ecosistema.

Figura 7-1 Modelo de responsabilidad de seguridad compartida de Huawei Cloud



7.2 Identificación y gestión de activos

En la siguiente tabla se enumeran los principales activos gestionados mediante DEW y cómo se gestionan.

Subservicio	Activo	Cómo gestionar
KMS	Clave	Las claves están protegidas por HSM.
CSMS	Secreto	Los secretos están protegidos por HSM.
KPS	Par de claves	Los pares de claves están protegidos por HSM.
Dedicated HSM	Instancia de HSM dedicado	Los usuarios controlan los permisos de las instancias de HSM dedicado. Los HSM se gestionan en las salas de equipos del centro de datos de Huawei Cloud de manera unificada.

7.3 Autenticación de identidad y control de acceso

Autenticación de identidad

Puede acceder a DEW a través de la consola DEW, las API o SDK. Independientemente del método de acceso, las solicitudes se envían a través de las API de REST proporcionadas por DEW.

Las API de DEW admiten múltiples tipos de solicitudes de autenticación. Tome AK/SK como ejemplo. Una solicitud autenticada debe contener un valor de firma. El valor de firma se calcula basándose en la clave de acceso del solicitante como el factor de encriptación y la

información específica transportada en el cuerpo de solicitud. OBS admite la autenticación mediante un par AK/SK. Utiliza encriptación basada en AK/SK para autenticar solicitudes. Para obtener más información, véase **Autenticación**.

Control de acceso

- DEW utiliza Identity and Access Management (IAM) para implementar un control de acceso refinado. De forma predeterminada, los nuevos usuarios de IAM no tienen permisos asignados. Debe agregar un usuario a uno o más grupos y asignar políticas de permisos a estos grupos. Después de la autorización, el usuario puede realizar operaciones específicas en los servicios en la nube en función de los permisos. Para obtener más información, consulte **Control de permiso**.
- Para los subservicios KMS, puede configurar sus permisos en la consola de KMS. Puede crear subvenciones para que otros usuarios o cuentas de IAM utilicen sus CMK. Puede crear hasta 100 subvenciones en un CMK. Para obtener más información, consulte **Gestión de una concesión**.

7.4 Tecnologías de protección de datos

DEW toma diferentes medidas para mantener los datos almacenados en DEW seguros y confiables.

Medida	Descripción	Referencia
Cifrado de transmisión (HTTPS)	DEW utiliza HTTPS para mejorar la seguridad de la transmisión de datos.	**Hacer una solicitud de API**
Gestión de claves	Los HSM se utilizan para gestionar y almacenar materiales clave para evitar fugas de claves.	**Funciones**
Encriptación de sobre	En escenarios en los que se necesita cifrar o descifrar una gran cantidad de datos, DEW proporciona encriptación de sobre para proteger los datos confidenciales en los sistemas de aplicación. Las claves de datos utilizadas para la encriptación se almacenan, transfieren y se utilizan con sobres.	**Cifrado o descifrado de una gran cantidad de datos**
Mecanismo de rotación de clave	Las claves que se usan ampliamente o repetidamente son inseguras. DEW le permite rotar periódicamente las claves y cambiar los materiales clave para cumplir con las mejores prácticas de encriptación.	**Acerca de rotación de clave**

Medida	Descripción	Referencia
Gestión de secreto	DEW proporciona gestión del ciclo de vida de los secretos y admite un acceso seguro y cómodo a las aplicaciones, ayudándole a reducir los riesgos de fuga de secretos causados por la codificación dura y a mejorar la seguridad de los datos y los activos.	**Gestión de secreto**
Importación de secreto	Los materiales clave importados a KMS se pueden cifrar mediante los algoritmos RSAES_OAEP_SHA_256 o SM2_ENCRYPT.	**Importación de materiales de clave**

7.5 Auditoría y registro

Cloud Trace Service (CTS) registra las operaciones en los recursos de la nube de su cuenta. Puede utilizar los logs generados por CTS para realizar análisis de seguridad, realizar un seguimiento de los cambios de recursos, auditar el cumplimiento y localizar fallos.

Para obtener más información, consulte **¿Qué es Cloud Trace Service?**

CTS puede realizar un seguimiento de las operaciones de DEW. Para obtener más información, consulte **Auditoría de registros**.

7.6 Resiliencia del servicio

DEW implementa aislamiento de fallos, copia de respaldo de datos y control de tráfico para mejorar la resistencia del servicio y mejorar la seguridad de los datos del usuario.

Aislamiento de fallas

- El diseño de aislamiento entre regiones de DEW garantiza que los fallos en una región no afecten a los servicios de DEW en otras regiones.
- Los servidores DEW y los HSM adoptan el diseño de DR de nivel zona de disponibilidad, de modo que los fallos en una zona de disponibilidad no afectan la disponibilidad de DEW. En caso de fallo, DEW protege automáticamente la zona de disponibilidad defectuosa y conmuta el tráfico a otra zona de disponibilidad, planificando sin problemas las cargas de trabajo.
- Los servidores de DEW y los HSM se despliegan en modo de clúster. Si cualquier fallo de un solo servidor o de un solo HSM no afecta la disponibilidad de DEW.

Copia de respaldo de datos

Las claves de DEW se replican entre múltiples HSM para evitar la pérdida permanente de claves en el caso de un fallo de HSM. Los datos de DEW (datos no confidenciales) se replican entre múltiples servidores e instancias de base de datos, y se realizan copias de respaldo en tiempo real para evitar la pérdida de datos.

Control de Flujo

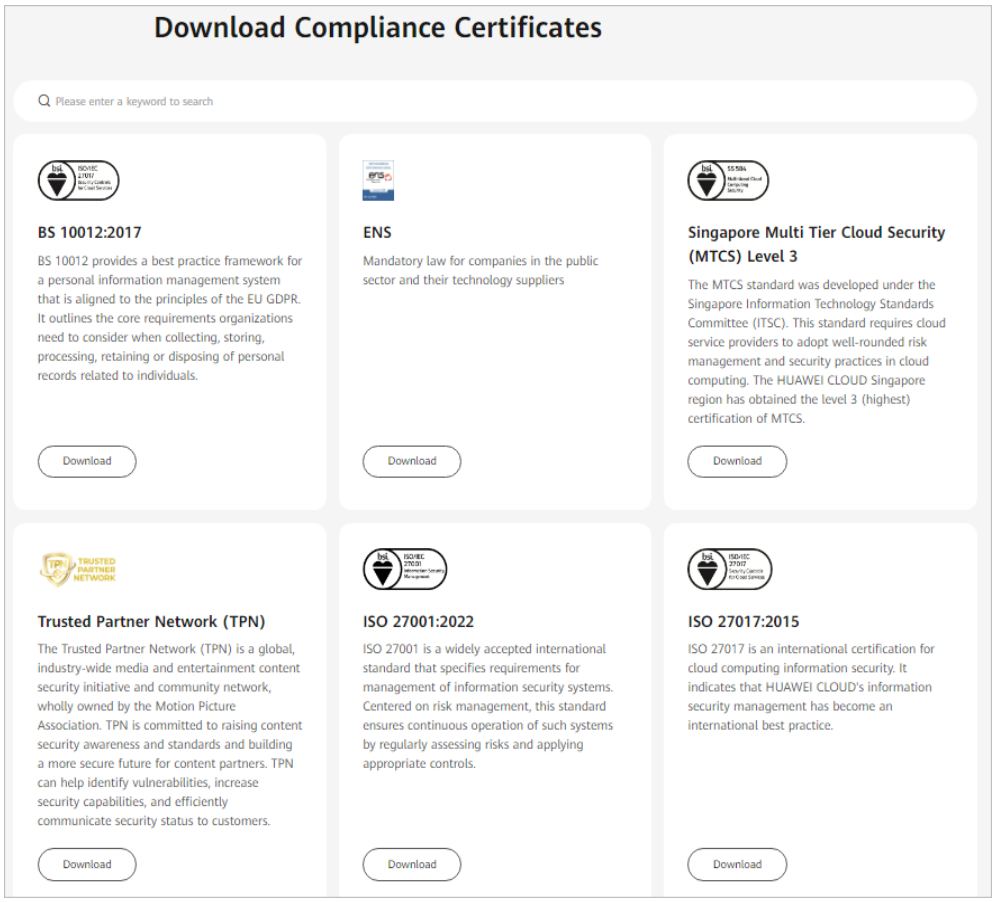
DEW puede cumplir con el objetivo de SLA de 99.95% de disponibilidad y proporcionar una gran cuota de invocaciones de API para cada usuario. Si un usuario ha agotado su cuota de invocaciones de API, DEW restringirá sus invocaciones de API posteriores para garantizar la disponibilidad del servicio.

7.7 Certificados

Certificados de Cumplimiento

Los servicios y plataformas de Huawei Cloud han obtenido diversas certificaciones de seguridad y cumplimiento de organizaciones autorizadas, como la Organización Internacional de Normalización (ISO). Puede **descargarlos** desde la consola.

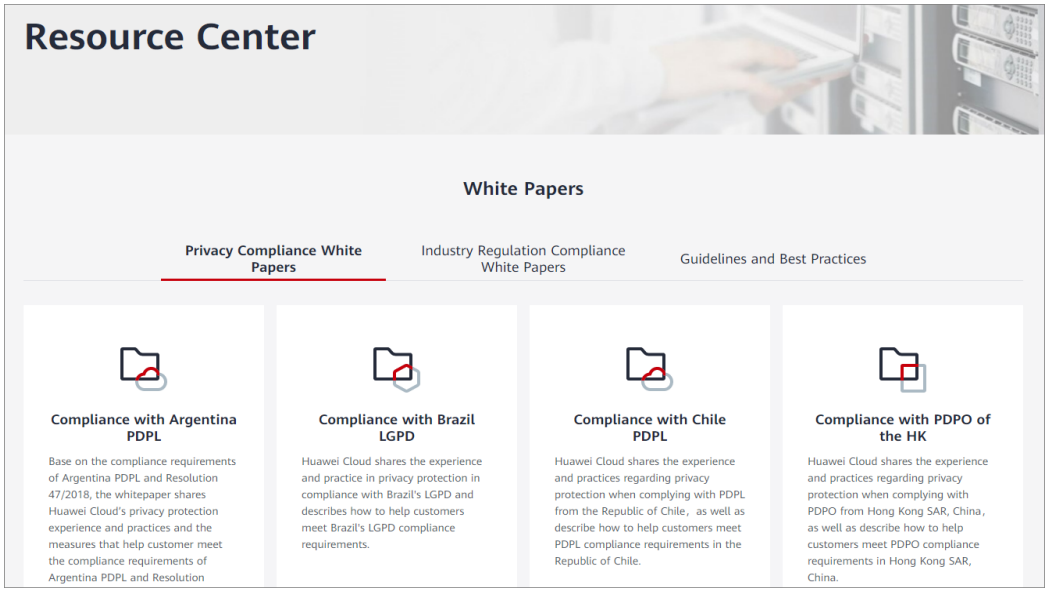
Figura 7-2 Descarga de certificados de cumplimiento



Centro de recursos

Huawei Cloud también proporciona los siguientes recursos para ayudar a los usuarios a cumplir con los requisitos de cumplimiento. Para obtener más información, consulte **Centro de recursos**.

Figura 7-3 Centro de recursos



8 Gestión de permisos de DEW

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 de Huawei Cloud.

Con IAM, puede usar su cuenta de Huawei para crear usuarios de IAM para sus empleados y conceder 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 cumple con sus requisitos y no necesita crear un usuario 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 detalles, consulte **Descripción de servicio**.

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 políticas 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: 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 gestionar 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 compatibles con DEW, consulte **Políticas de permiso y acciones admitidas**.

En las tablas siguientes se enumeran todos los permisos del sistema DEW.

Tabla 8-1 Políticas del sistema KMS

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

Tabla 8-2 Políticas del sistema KPS

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

Tabla 8-3 Políticas del sistema CSMS

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

NOTA

Las políticas de DEW KeypairFullAccess y DEW KeypairReadOnlyAccess utilizadas para la autorización de proyectos de empresa no tienen efecto para usuarios individuales.

Si es un usuario individual y necesita utilizar la autorización de proyecto de empresa, asegúrese de que se ha agregado a un grupo de usuarios y autorice el grupo de usuarios.

Tabla 8-4 enumera las operaciones comunes soportadas por cada permiso definido por el sistema de DEW. Seleccione los permisos necesarios.

Tabla 8-4 Operaciones comunes para cada política definida por el sistema o función de KMS

Operación	KMS Administrator	KMS CMKFullAccess
Crear una clave	√	√
Habilitar una clave	√	√
Deshabilitar una clave	√	√
Programar eliminación de clave	√	√
Cancelar la eliminación de clave programada	√	√
Modificar un alias de clave	√	√
Modificar descripción de clave	√	√
Generar un número aleatorio	√	√
Crear un DEK	√	√
Crear un DEK sin texto sin formato	√	√

Operación	KMS Administrator	KMS CMKFullAccess
Cifrar un DEK	√	√
Descifrar un DEK	√	√
Obtener parámetros para importar una clave	√	√
Importar materiales de clave	√	√
Eliminar materiales de clave	√	√
Crear una concesión	√	√
Revocar una concesión	√	√
Retirar una concesión	√	√
Consultar la lista de concesiones	√	√
Consultar concesiones retirables	√	√
Cifrar datos	√	√
Descifrar datos	√	√
Enviar mensajes de firma	√	√
Autenticar firma	√	√
Habilitar la rotación de clave	√	√
Modificar intervalo de rotación de clave	√	√
Deshabilitar la rotación de clave	√	√
Consultar estado de rotación de clave	√	√
Consultar instancias de CMK	√	√
Consultar etiquetas de clave	√	√
Consultar etiquetas de proyecto	√	√
Agregar o eliminar etiquetas de clave por lotes	√	√
Agregar etiquetas a una clave	√	√

Operación	KMS Administrator	KMS CMKFullAccess
Eliminar etiquetas de clave	√	√
Consultar la lista de clave	√	√
Consultar detalles de clave	√	√
Consultar clave pública	√	√
Cantidad de instancia de consulta	√	√
Cuotas de consulta	√	√
Consultar la lista de pares de claves	x	x
Crear o importar un par de claves	x	x
Consultar pares de claves	x	x
Eliminar un par de claves	x	x
Actualizar descripción del par de claves	x	x
Vincular un par de claves	x	x
Desvincular un par de claves	x	x
Consultar una tarea de vinculación	x	x
Consultar tareas fallidas	x	x
Eliminar todas las tareas con error	x	x
Eliminar una tarea fallida	x	x
Consultar tareas en ejecución	x	x

Enlaces útiles

- **Qué es IAM**
- **Crear un usuario y autorizarle el permiso de acceso a DEW**
- **Políticas de permisos y acciones admitidas**

9 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, consulte la *Referencia de la API de Data Encryption Workshop*.

10 Servicios relacionados

OBS

Object Storage Service (OBS) es un servicio escalable que proporciona almacenamiento en la nube seguro, confiable y rentable para grandes cantidades de datos. 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) le permite gestionar todo el ciclo de vida de sus 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.

SFS

Scalable File Service (SFS) proporciona almacenamiento de archivos (NAS) de alto performance que se puede ampliar a petición. KMS proporciona capacidades de gestión y control centrales de CMK para SFS. Se utiliza para la encriptación del sistema de archivos en SFS.

Relational Database Service (RDS) es una base de datos en la nube que es confiable, escalable, fácil de gestionar e inmediatamente lista para su uso. KMS proporciona capacidades de gestión y control centrales de CMK para RDS. Se utiliza para la encriptación de disco en bases de datos en la nube.

ECS

Un ECS es un componente informático básico que consiste en CPU, memoria, sistema operativo y elastic volume service (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 DEW. Una vez habilitado el servicio CTS, puede ver todos los rastros generados para revisar y auditar las operaciones de KMS realizadas. Para obtener más información, consulte *Guía de usuario de Cloud Trace Service*.

Tabla 10-1 Operaciones KMS registradas por CTS

Operación	Tipo de recurso	Nombre del rastro
Crear una clave	cmk	createKey
Crear un DEK	cmk	createDataKey
Crear un DEK sin texto sin formato	cmk	createDataKeyWithoutPlain-text
Habilitar una clave	cmk	enableKey
Deshabilitar una clave	cmk	disableKey
Cifrar un DEK	cmk	encryptDatakey
Descifrar un DEK	cmk	decryptDatakey
Programar eliminación de clave	cmk	scheduleKeyDeletion
Cancelar la eliminación de clave programada	cmk	cancelKeyDeletion
Generar números aleatorios	rng	genRandom

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

Tabla 10-2 Operaciones KMS registradas por CSMS

Operación	Tipo de recurso	Nombre del rastro
Crear un secreto	csms	createSecret
Actualizar un secreto	csms	updateSecret
Eliminar un secreto	csms	forceDeleteSecret
Programar la eliminación de un secreto	csms	scheduleDelSecret
Cancelar la eliminación secreta programada	csms	restoreSecretFromDeleted-Status
Crear un estado secreto	csms	createSecretStage
Actualizar un estado secreto	csms	updateSecretStage

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

Tabla 10-3 Operaciones de KMS registradas por KPS

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

Tabla 10-4 Operaciones KMS grabadas por HSM dedicado

Operación	Tipo de recurso	Nombre del rastro
Comprar una instancia de HSM	hsm	purchaseHsm
Configurar una instancia de HSM	hsm	createHsm
Eliminar 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 del usuario de *Guía de usuario de Identity and Access Management*.

11 Mecanismo de protección de datos personales

Para garantizar que sus datos personales, como el nombre de usuario, la contraseña y el número de celular, 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 11-1 enumera los datos personales generados o recopilados por DEW.

Tabla 11-1 Datos personales

Tipo	Origen	Puede ser modificado	Obligatorio
ID del tenant	• ID de tenant en el token cuando se realiza una operación en la consola. • ID de tenant en el token cuando se invoca una API.	No	Sí

Modo de almacenamiento

Los ID de tenant 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.

