Data Encryption Workshop

Visão geral de serviço

Edição 15

Data 29-03-2022

HUAWEI

HUAWEI TECHNOLOGIES CO., LTD.

Marcas registadas e permissões


e outras marcas registadas da Huawei são marcas registadas da Huawei Technologies Co., Ltd. Todos as outras marcas registadas e os nomes registados mencionados neste documento são propriedade dos seus respectivos detentores.

Aviso

Os produtos, serviços e funcionalidades adquiridos são estipulados pelo contrato feito entre a Huawei e o cliente. Todos ou parte dos produtos, serviços e funcionalidades descritos neste documento pode não estar dentro do âmbito de aquisição ou do âmbito de uso. Salvo especificação em contrário no contrato, todas as declarações, informações e recomendações neste documento são fornecidas "TAL COMO ESTÁ" sem garantias, ou representações de qualquer tipo, seja expressa ou implícita.

As informações contidas neste documento estão sujeitas a alterações sem aviso prévio. Foram feitos todos os esforços na preparação deste documento para assegurar a exatidão do conteúdo, mas todas as declarações, informações e recomendações contidas neste documento não constituem uma garantia de qualquer tipo, expressa ou implícita.

Huawei Technologies Co., Ltd.

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

Site: https://www.huawei.com

Email: support@huawei.com

Índice

1 O que é o DEW?

DEW

Os dados são o principal ativo de uma empresa. Cada empresa tem seus principais dados confidenciais, que precisam ser criptografados e protegidos contra violações.

O Data Encryption Workshop (DEW) é um serviço de criptografia de dados na nuvem. Consiste no Key Management Service (KMS), Cloud Secret Management Service (CSMS), Key Pair Service (KPS), e Dedicated Hardware Security Module (Dedicated HSM), ajudando você a proteger seus dados e chaves e simplificando o gerenciamento de chaves. A DEW usa HSMs para proteger a segurança de suas chaves e pode ser integrada a outros serviços da HUAWEI CLOUD para resolver problemas de segurança de dados, segurança de chaves e gerenciamento de chaves. Além disso, o DEW permite que você desenvolva aplicações de criptografia personalizados.

Tabela 1-1 Visão geral de serviço

Serviço	Descrição	Referência
Key Management Service (KMS)	O KMS é um serviço seguro, confiável e fácil de usar para gerenciar suas chaves na nuvem. Ele ajuda você a criar, gerenciar e proteger chaves com facilidade. O KMS usa Módulos de segurança de hardware (HSMs) para proteger chaves, ajudando você a criar e controlar chaves mestras de clientes (CMKs) com facilidade. Todas as CMKs são protegidas por chaves raiz nos HSMs para evitar vazamento de chaves.	**Tipos de chave**

Serviço	Descrição	Referência
Cloud Secret Management Service (CSMS)	O CSMS é um serviço de hospedagem secreta seguro, confiável e fácil de usar. Os usuários ou aplicações podem usar o CSMS para criar, recuperar, atualizar e excluir credenciais de maneira unificada durante todo o ciclo de vida das credenciais. O CSMS pode ajudá-lo a eliminar os riscos incorridos pela codificação rígida, configuração de texto simples e abuso de permissão.	**Criar um segredo**
Key Pair Service (KPS)	O KPS é um serviço de nuvem seguro, confiável e fácil de usar, projetado para gerenciar e proteger seus pares de chaves SSH (abreviação de pares de chaves). O KPS usa HSMs para gerar números aleatórios verdadeiros que são então usados para produzir pares de chaves. Além disso, adota uma solução de gerenciamento de pares de chaves completa e confiável para ajudar os usuários a criar, importar e gerenciar pares de chaves com facilidade. A chave pública de um par de chaves gerado é armazenada no KPS, enquanto a chave privada pode ser baixada e salva separadamente, o que garante a privacidade e a segurança do par de chaves.	**Criar um par de chaves**
Dedicated Hardware Security Module (Dedicated HSM)	O Dedicated HSM permite a criptografia de dados na nuvem, especificamente, criptografando e descriptografando dados, verificando assinaturas, gerando chaves e armazenando chaves. O Dedicated HSM fornece hardware de criptografia, garantindo a segurança e a integridade dos dados em Elastic Cloud Servers (ECSs) e atendendo aos requisitos de conformidade. O Dedicated HSM oferece um gerenciamento seguro e confiável para as chaves geradas por suas instâncias e usa vários algoritmos para criptografia e descriptografia de dados.	**Dedicated HSM**

Conceitos

Esta seção descreve os conceitos básicos do DEW.

Tabela 1-2 Conceitos básicos

Item	Definição	Referência
Módulo de segurança de hardware (HSM)	Um HSM é um tipo de hardware de computador que protege e gerência as chaves usadas por sistemas de autenticação forte e fornece operações criptográficas relacionadas.	-
Chave mestra do cliente (CMK)	Uma CMK é uma chave de criptografia de chave (KEK) criada por um usuário ou serviço de nuvem usando o KMS. Ele é usado para criptografar e proteger as chaves de criptografia de dados (DEKs). Uma CMK pode ser usada para criptografar uma ou mais DEKs. As CMKs são categorizadas em chaves personalizadas e chaves padrão.	**O que é uma Chave mestra do cliente?**
Chave mestra padrão (DMK)	Uma chave mestra padrão é criada automaticamente por outro serviço de nuvem usando o KMS, como o Object Storage Service (OBS). O alias de uma chave mestra padrão termina com **/default**.	**O que é uma Chave mestra padrão?**
Material de chave	Os materiais de chave são uma entrada importante para operações criptográficas. Uma CMK consiste em um ID de chave, metadados e um material de chave.	-
Criptografia do envelope	A criptografia de envelope é a prática de criptografar dados com uma DEK e, em seguida, criptografar a DEK com uma chave raiz que você pode gerenciar totalmente. Nesse caso, as CMKs não são necessárias para criptografia ou descriptografia.	**Quais são os benefícios da criptografia de envelope?**
Chave de criptografia de dados (DEK)	Uma DEK é usada para criptografar dados.	**O que é uma Chave de criptografia de dados?**

Item	Definição	Referência
Criptografia de chave simétrica	A criptografia de chave simétrica também é chamada de criptografia de chave dedicada. O remetente e o receptor usam a mesma chave para criptografar e descriptografar dados. Vantagens: criptografia e descriptografia são rápidas. Desvantagens: cada par de chaves deve ser único. O gerenciamento de chaves é difícil se houver um grande número de usuários. Cenários: criptografar uma grande quantidade de dados.	**Tipos de chave**
Criptografia de chave assimétrica	A criptografia de chave assimétrica também é chamada de criptografia de chave pública. Um par de chaves é usado para criptografia e descriptografia. Uma é uma chave pública e a outra é uma chave privada. Vantagens: chaves diferentes são usadas para criptografia e descriptografia, aumentando a segurança. Desvantagens: criptografia e descriptografia são lentos. Cenários: criptografar informações confidenciais.	**Tipos de chave**
Par de chaves	Um par de chaves é um par de chave pública assimétrica e chave privada. Por padrão, RSA-2048 é usado para criptografia.	**Gerenciamento de pares de chaves**
Par de chaves privadas	Um par de chaves privadas pode ser visto ou usado apenas pela conta atual.	**Criar um par de chaves**
Par de chaves de conta	Um par de chaves de conta pode ser visto ou usado por todos os usuários sob a conta.	**Atualizar um par de chaves**

2 KMS

2.1 Funções

O KMS é um serviço de nuvem seguro, confiável e fácil de usar que ajuda os usuários a criar, gerenciar e proteger chaves de maneira centralizada.

Ele usa módulos de segurança de hardware (HSMs) para proteger as chaves. Todas as CMKs são protegidas por chaves raiz nos HSMs para evitar vazamento de chaves.

Ele também controla o acesso a chaves e registra todas as operações em chaves com logs rastreáveis. Além disso, fornece registros de uso de todas as chaves, atendendo aos requisitos de auditoria e conformidade regulatória.

Funções

- No console do KMS, você pode executar as seguintes operações em CMKs:
  - Criar, consultar, habilitar, desabilitar, agendar a exclusão e cancelar a exclusão de CMKs
  - Modificar o alias e a descrição de CMKs
  - Usar a ferramenta on-line para criptografar e descriptografar pequenos volumes de dados
  - Adicionar, pesquisar, editar e excluir tags
  - Criar, cancelar e consultar concessões
- Você pode usar a API para executar as seguintes operações:
  - Criar, criptografar ou descriptografar chaves de criptografia de dados (DEKs)
  - Concessões de retirada
  - Assinar ou verificar a assinatura de mensagens ou resumos de mensagens

  Para obter detalhes, consulte a *Referência de API do Data Encryption Workshop*.
- Gerar hardware verdadeiro número aleatório.

  Você pode gerar números aleatórios de 512-bit usando a API do KMS. Os números aleatórios verdadeiros de hardware de 512-bit podem ser usados como ou servir como base para materiais de chave e parâmetros de criptografia. Para obter detalhes, consulte a *Referência de API do Data Encryption Workshop*.

Algoritmos criptográficos suportados pelo KMS

As chaves simétricas criadas no console do KMS usam o algoritmo AES-256. As chaves assimétricas criadas pelo KMS oferecem suporte aos algoritmos RSA e ECC.

Tabela 2-1 Algoritmos de chave suportados pelo KMS

Tipo de chave	Tipo de algoritmo	Especificações de chave	Descrição	Utilização
Chave simétrica	AES	AES_256	Chave simétrica de AES	Criptografa e descriptografa uma pequena quantidade de dados ou chaves de dados.
Chaves assimétricas	RSA	• RSA_2048 • RSA_3072 • RSA_4096	Senha assimétrica de RSA	Criptografa e descriptografa uma pequena quantidade de dados ou cria assinaturas digitais.
	ECC	• EC_P256 • EC_P384	Curva elíptica recomendada pelo NIST	Assinatura digital

Tabela 2-2 descreve os algoritmos de criptografia e descriptografia suportados para chaves importadas pelo usuário. Somente chaves simétricas de 256-bit podem ser importadas.

Tabela 2-2 Algoritmos de agrupamento de chaves

Algoritmo	Descrição	Configuração
RSAES_OAEP_SHA_256	Algoritmo de criptografia RSA que usa OAEP e tem a função de hash **SHA-256**	Selecione um algoritmo de criptografia com base nas funções do HSM. Se os HSMs oferecerem suporte ao algoritmo **RSAES_OAEP_SHA_256**, use **RSAES_OAEP_SHA_256** para criptografar materiais de chave. **AVISO** O algoritmo de criptografia **RSAES_OAEP_SHA_1** não é mais seguro. Tenha cuidado ao realizar esta operação.
RSAES_OAEP_SHA_1	Algoritmo de encriptação RSA que utiliza Preenchimento de criptografia assimétrica ideal (OAEP) e tem a função de hash **SHA-1**	

2.2 Vantagens do produto

- Ampla integração de serviços

  O KMS pode ser integrado ao Object Storage Service (OBS), Elastic Volume Service (EVS) e Image Management Service (IMS), para gerenciar chaves desses serviços no console do KMS, além de criptografar e descriptografar seus dados locais fazendo as chamadas da API do KMS.
- Conformidade regulamentar

  As chaves são geradas por HSMs validados por terceiros. O acesso às chaves é controlado e todas as operações envolvendo chaves são rastreáveis por registros, em conformidade com as leis e regulamentos chineses e internacionais.

2.3 Cenários de aplicação

Pré-requisitos

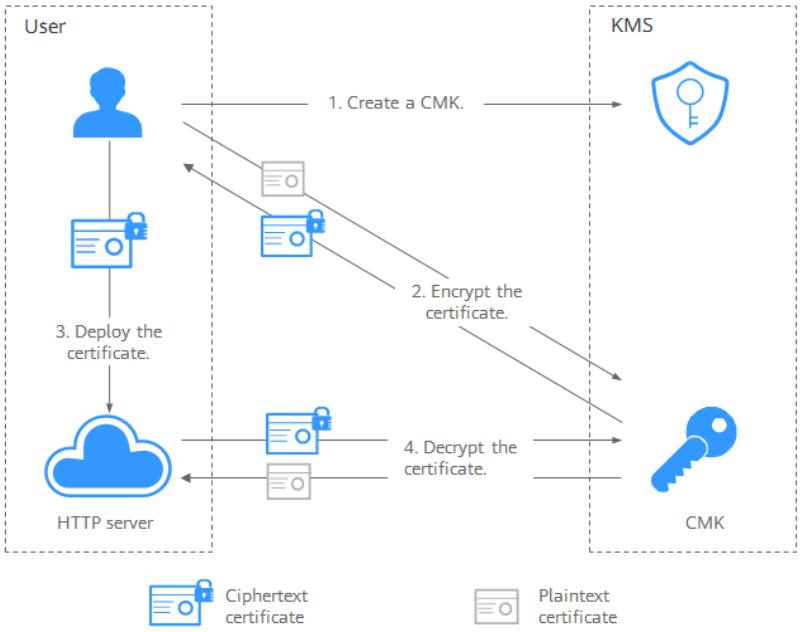
Todas as CMKs mencionadas nesta seção são chaves simétricas. Para obter detalhes sobre chaves simétricas e chaves assimétricas, consulte **Visão geral de chave**.

Criptografia e descriptografia de dados pequenos

Você pode usar a ferramenta on-line no console do KMS ou chamar APIs do KMS para criptografar ou descriptografar diretamente uma pequena quantidade de dados, como senhas, certificados ou números de telefone. Atualmente, um máximo de 4 KB de dados podem ser criptografados ou descriptografados dessa maneira.

Figura 2-1 mostra um exemplo sobre como chamar as APIs para criptografar e descriptografar um certificado HTTPS.

Figura 2-1 Criptografar e descriptografar um certificado HTTPS



O procedimento é o seguinte:

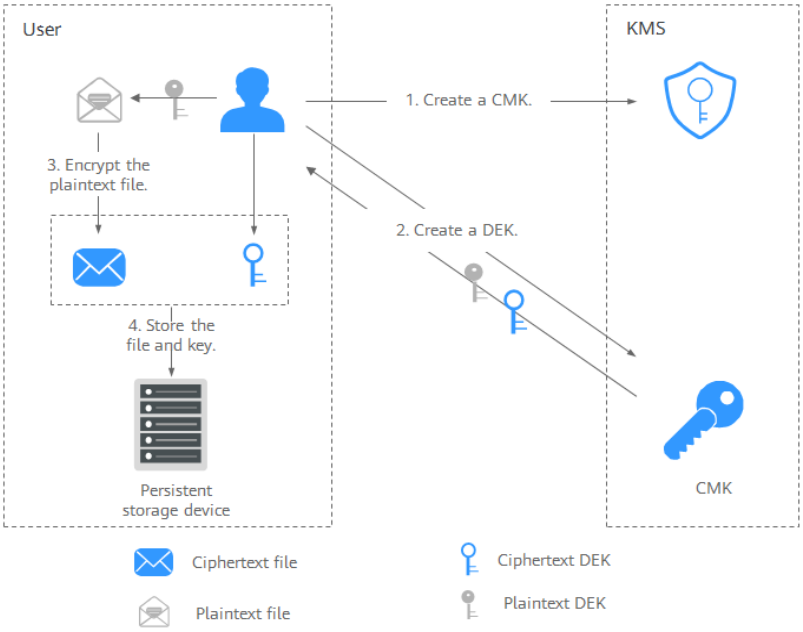
1. Crie uma CMK no KMS.
2. Chame a **encriptação de dados de** API do KMS e use a CMK para criptografar o certificado de texto sem formatação.
3. Implante o certificado em um servidor.
4. O servidor chama o **dados descriptografados de** API do KMS para descriptografar o certificado de texto cifrado.

Criptografia e descriptografia de dados grandes

Se você quiser criptografar ou descriptografar grandes volumes de dados, como imagens, vídeos e arquivos de banco de dados, você pode usar o método de criptografia de envelope, onde os dados não precisam ser transferidos pela rede.

- **Figura 2-2** ilustra o processo para criptografar um arquivo local.

Figura 2-2 Criptografar um arquivo local



O procedimento é o seguinte:

a. Crie uma CMK no KMS.

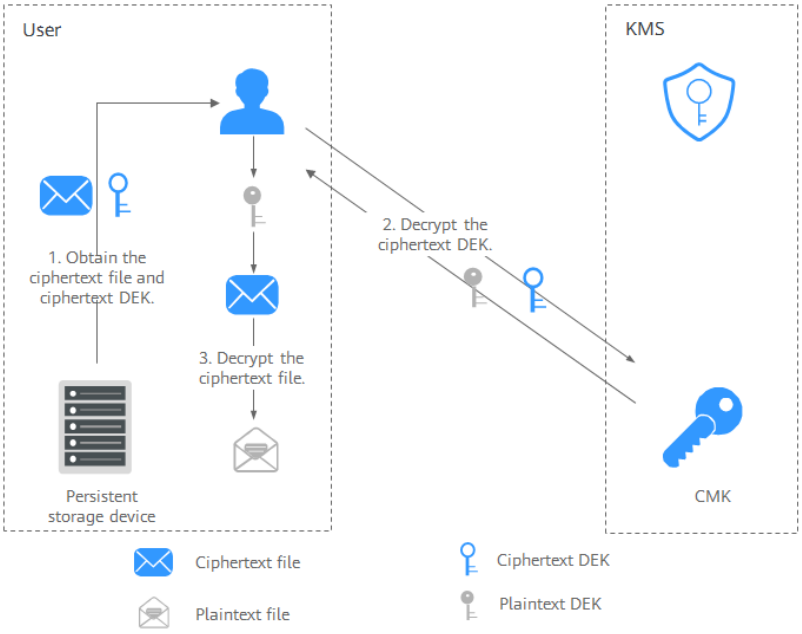
b. Chame a **chave de dados de criação de** API do KMS para criar uma DEK. Então você obtém uma DEK de texto não criptografado e uma DEK de texto cifrado. A DEK de texto cifrado é gerada quando você usa uma CMK para criptografar a DEK de texto não criptografado.

c. Use a DEK de texto não criptografado para criptografar o arquivo. Um arquivo de texto cifrado é gerado.

d. Salve a DEK de texto cifrado e o arquivo de texto cifrado juntos em um dispositivo de armazenamento persistente ou um serviço de armazenamento.

- **Figura 2-3** ilustra o processo para descriptografar um arquivo local.

Figura 2-3 Descriptografar um arquivo local



O procedimento é o seguinte:

a. Obtenha a DEK de texto cifrado e o arquivo do dispositivo de armazenamento persistente ou do serviço de armazenamento.

b. Chame a **chave de dados descriptografia de** API do KMS e use a CMK correspondente (aquele usado para criptografar a DEK) para descriptografar a DEK de texto cifrado. Então você obtém o DEK de texto não criptografado.

   Se a CMK for excluída, a descriptografia falhará. Portanto, mantenha corretamente suas CMKs.

c. Use a DEK de texto não criptografado para descriptografar o arquivo de texto cifrado.

Links úteis

Documento	Ligação
Melhores práticas	• **Criptografia ou descriptografia de pequenos volumes de dados** • "Criptografia ou descriptografia de uma grande quantidade de dados"
Exemplo de API	• **Criptografia ou descriptografia de pequenos volumes de dados** • **Criptografia ou descriptografia de uma grande quantidade de dados**

2.4 Usar o KMS

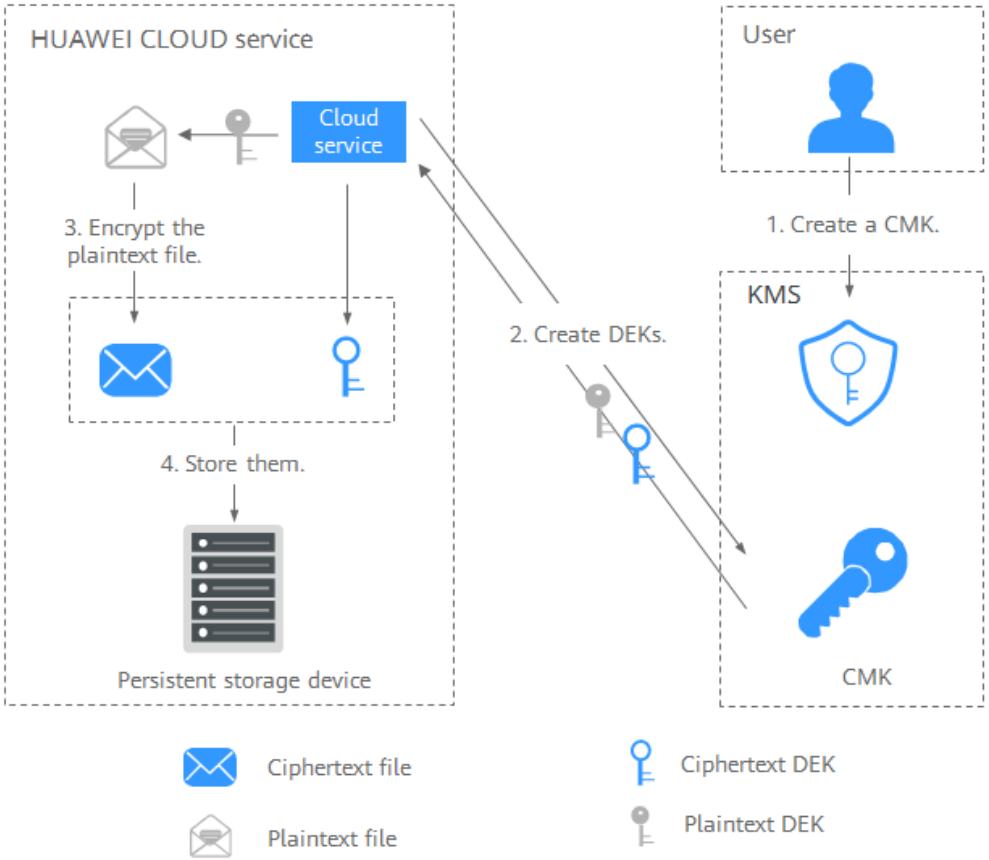
Pré-requisitos

Todas as CMKs mencionadas nesta seção são chaves simétricas. Para obter detalhes sobre chaves simétricas e chaves assimétricas, consulte **Visão geral de chave**.

Interagindo com os serviços da HUAWEI CLOUD

Serviços da HUAWEI CLOUD usa a tecnologia de criptografia de envelope e chamam as APIs de KMS para criptografar os recursos do serviço. Suas CMKs estão sob sua própria gestão. Com sua concessão, serviços da HUAWEI CLOUD usa uma CMK específica sua para criptografar dados.

Figura 2-4 Como a HUAWEI CLOUD usa o KMS para criptografia



O processo de encriptação é o seguinte:

1. Criar uma CMK no KMS.
2. Serviços da HUAWEI CLOUD chama a **criar-datakey** API do KMS para criar uma DEK. Então você obtém uma DEK de texto não criptografado e uma DEK de texto cifrado.

> NOTA
>
> As DEKs de texto cifrado são geradas quando você usa uma CMK para criptografar as DEKs de texto não criptografado.

3. Serviços da HUAWEI CLOUD usa a DEK de texto simples para criptografar um arquivo de texto não criptografado, gerando um arquivo de texto cifrado.
4. Serviços da HUAWEI CLOUD armazenam o DEK de texto cifrado e o arquivo de texto cifrado em um dispositivo de armazenamento persistente ou em um serviço de armazenamento.

> NOTA
>
> Quando os usuários baixam os dados de um serviço da HUAWEI CLOUD, o serviço usa a CMK especificada pelo KMS para descriptografar o texto cifrado DEK, usa a DEK descriptografada para descriptografar dados, e, em seguida, fornece os dados descriptografados para os usuários baixarem.

Tabela 2-3 Lista de serviços em nuvem que usam criptografia KMS

Nome do serviço	Descrição
Object Storage Service (OBS)	Você pode fazer upload de objetos e baixá-los do Object Storage Service (OBS) no modo comum ou no modo de criptografia do lado do servidor. Quando você carrega objetos no modo de criptografia, os dados são criptografados no lado do servidor e, em seguida, armazenados com segurança no OBS em texto cifrado. Quando você baixa objetos criptografados, os dados em texto cifrado são descriptografados no lado do servidor e, em seguida, fornecidos a você em texto sem formatação. O OBS suporta a encriptação do lado do servidor com o modo de chaves geridas por KMS (SSE-KMS). No modo SSE-KMS, o OBS utiliza as chaves fornecidas pelo KMS para a encriptação do lado do servidor. Para obter detalhes sobre como carregar objetos para o OBS no modo SSE-KMS, consulte *Guia de operação do console do Object Storage Service*.
Elastic Volume Service (EVS)	Se você ativar a função de criptografia ao criar um disco EVS, o disco será criptografado com a DEK gerada usando sua CMK. Os dados armazenados no disco EVS serão automaticamente encriptados. Para obter detalhes sobre como usar a função de criptografia do EVS, consulte o *Guia de usuário do Elastic Volume Service*.
Image Management Service (IMS)	Ao criar uma imagem privada usando um arquivo de imagem externo, você pode ativar a função de criptografia de imagem privada e selecionar uma CMK fornecida pelo KMS para criptografar a imagem. Para obter detalhes sobre como usar a função de criptografia de imagem privada do Serviço de Gerenciamento de Imagens (IMS), consulte o *Guia de usuário do Image Management Service* .
Relational Database Service (RDS)	Ao comprar uma instância de banco de dados, você pode ativar a função de criptografia de disco da instância de banco de dados e selecionar uma CMK criada no KMS para criptografar o disco da instância de banco de dados. Ativar a função de criptografia de disco aumentará a segurança dos dados. Para obter detalhes sobre como usar a função de criptografia de disco do RDS, consulte o *Guia de usuário do Relational Database Service*.

Nome do serviço	Descrição
Document Database Service (DDS)	Ao comprar uma instância DDS, você pode ativar a função de criptografia de disco da instância e selecionar uma CMK criada no KMS para criptografar o disco da instância. Ativar a função de criptografia de disco aumentará a segurança dos dados. Para obter detalhes sobre como usar a função de criptografia de disco do DDS, consulte o *Guia de usuário do Document Database Service*.

Trabalhar com aplicações de usuário

Para criptografar dados de texto não criptografado, um aplicação de usuário pode chamar a API KMS necessária para criar uma DEK. A DEK pode então ser usada para criptografar os dados de texto não criptografado. Em seguida, a aplicação pode armazenar os dados criptografados. Além disso, a aplicação do usuário pode chamar a API do KMS para criar CMKs. As DEKs podem ser armazenadas em texto cifrado após serem criptografadas com as CMKs.

A criptografia de envelope é implementada, com CMKs armazenadas em KMS e DEKs de texto cifrado em aplicações de usuário. O KMS é chamado para descriptografar uma DEK de texto cifrado somente quando necessário.

O processo de encriptação é o seguinte:

1. A aplicação chama o **criar-chave** API do KMS para criar uma CMK.
2. A aplicação chama o **criar-datakey** API do KMS para criar uma DEK. Uma DEK de texto simples e uma DEK de texto cifrado são geradas.

   NOTA

   As DEKs de texto cifrado são geradas quando você usa uma CMK para criptografar as DEKs de texto não criptografado em **1**.
3. A aplicação usa a DEK de texto sem formatação para criptografar um arquivo de texto sem formatação. Um arquivo de texto cifrado é gerado.
4. A aplicação salva a DEK de texto cifrado e o arquivo de texto cifrado juntos em um dispositivo de armazenamento persistente ou um serviço de armazenamento.

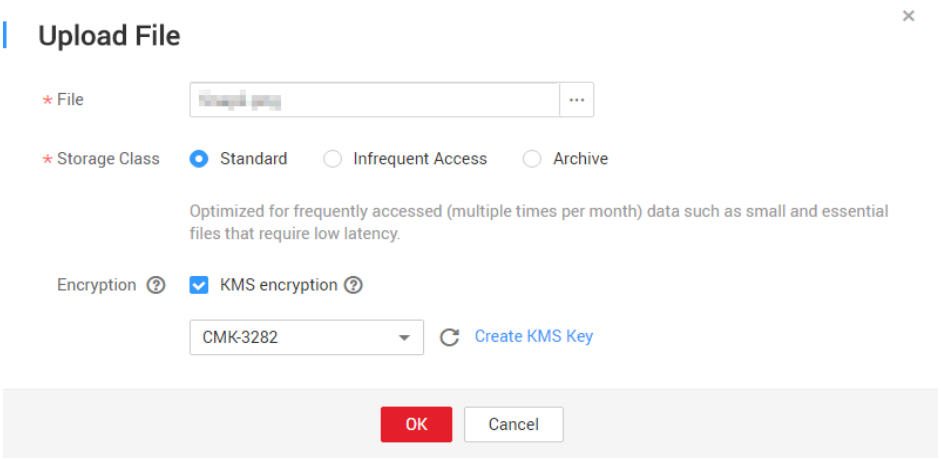
Para obter detalhes, consulte a *Referência de API do Data Encryption Workshop*.

2.5 Serviços em nuvem com KMS integrado

2.5.1 Criptografia de dados no OBS

- Ao usar o Object Storage Service (OBS) para carregar arquivos com criptografia no servidor, você pode selecionar a criptografia de KMS e usar a chave fornecida pelo KMS para criptografar os arquivos a serem carregados. **Figura 2-5** descreve os detalhes. Para obter mais informações sobre o OBS, consulte *Guia de operação do console do Object Storage Service*.

Figura 2-5 Criptografia do lado do servidor de OBS



Existem dois tipos de CMKs que podem ser usados:

- A chave mestra padrão **obs/default** criada pelo KMS
- CMKs criadas no console do KMS usando materiais de chave gerados pelo KMS

- Como alternativa, você pode chamar APIs do OBS para carregar um arquivo com criptografia do lado do servidor usando chaves gerenciadas pelo KMS (SSE-KMS). Para obter detalhes, consulte *Referência de API do Object Storage Service*.

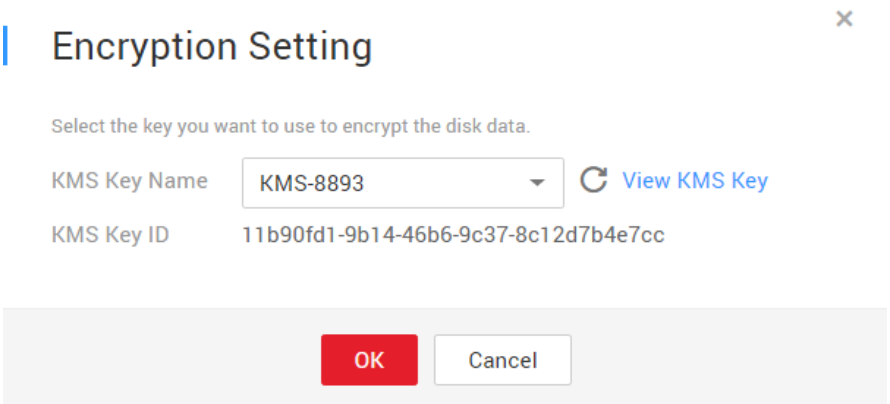
2.5.2 Criptografia de dados no EVS

- Ao comprar um disco, você pode escolher **Advanced Settings** > **Configure** > **Encryption** para criptografar o disco usando a chave fornecida pelo KMS. Para mais detalhes, consulte **Figura 2-6**. Para obter mais informações sobre o EVS, consulte o *Guia de usuário do Elastic Volume Service*.

  NOTA

  Antes de usar a função de criptografia, o EVS deve ter permissão para acessar o KMS. Se você tem o direito de conceder a permissão, você pode conceder a permissão diretamente. Se você não tiver a permissão, entre em contato com um usuário com as permissões de administrador de segurança para adicionar a permissão de administrador de segurança para você. Em seguida, você pode conceder a permissão. Para obter mais informações sobre o EVS, consulte o *Guia de usuário do Elastic Volume Service*.

Figura 2-6 Criptografar dados no EVS



Existem dois tipos de CMKs que podem ser usados:

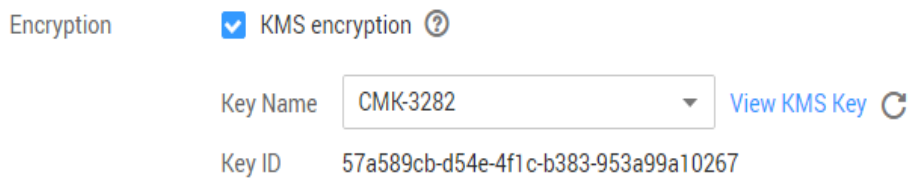
- A chave mestra padrão **evs/default** criada pelo KMS
- CMKs criadas no console do KMS usando materiais de chave gerados pelo KMS

- Você também pode chamar APIs do EVS para criar discos EVS criptografados. Para obter detalhes, consulte a *Referência de API do Elastic Volume Service*.

2.5.3 Criptografia de dados no IMS

- Ao carregar um arquivo de imagem para o Image Management Service (IMS), você pode optar por criptografar o arquivo de imagem usando uma chave fornecida pelo KMS para proteger o arquivo. **Figura 2-7** descreve os detalhes. Para obter detalhes, consulte .

Figura 2-7 Criptografar dados no IMS



Existem dois tipos de CMKs que podem ser usados:

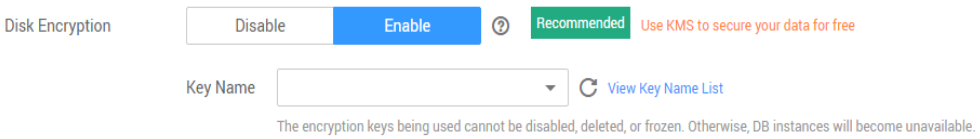
- A chave mestra padrão **ims/default** criada pelo KMS
- CMKs criadas no console do KMS usando materiais de chave gerados pelo KMS

- Você também pode chamar APIs do IMS para criar arquivos de imagem criptografados. Para obter detalhes, consulte a *Referência de API do Image Management Service*.

2.5.4 Criptografia de dados no RDS

- Quando um usuário compra uma instância de banco de dados do Relational Database Service (RDS), ele pode selecionar **Disk encryption** e usar a chave fornecida pelo KMS para criptografar o disco da instância de banco de dados. Para obter mais informações, consulte *Guia de usuário do Relational Database Service*.

Figura 2-8 Criptografar dados no RDS



Existem dois tipos de CMKs que podem ser usados:

- A chave mestra padrão **rds/default** criada pelo KMS
- CMKs criadas no console do KMS usando materiais de chave gerados pelo KMS

- Você também pode chamar as APIs do RDS para comprar instâncias de banco de dados criptografadas. Para obter detalhes, consulte *Guia de usuário do Relational Database Service*.

2.5.5 Encrypting Data in DDS

- When a user purchases a database instance from DDS, the user can select **Disk encryption** and use the key provided by KMS to encrypt the disk of the database instance. For more information, see the *Relational Database Service User Guide*.

  Figura 2-9 Encrypting data in DDS

  There are two types of CMKs that can be used:

  - The default master key **dds/default** created by KMS
  - CMKs that you create on the KMS console using KMS-generated key materials

- You can also call the required API of DDS to purchase encrypted DB instances. For details, see *Document Database Service API Reference*.

3 CSMS

3.1 Funções

O CSMS é um serviço de hospedagem de credenciais seguro, confiável e fácil de usar. Os usuários ou aplicações podem usar o CSMS para criar, recuperar, atualizar e excluir credenciais de maneira unificada durante todo o ciclo de vida das credenciais. O CSMS pode ajudá-lo a eliminar os riscos incorridos pela codificação rígida, configuração de texto simples e abuso de permissão.

Gerenciamento unificado de segredos

Aplicações e sistemas de negócios têm um grande número de segredos e são difíceis de gerenciar.

O CSMS pode armazenar, recuperar e usar segredos de maneira unificada ao longo de seus ciclos de vida.

Execute as seguintes operações para gerenciar segredos usando o CSMS:

1. Coletar segredos.
2. Carregue os segredos no CSMS.
3. Configure permissões de acesso e uso refinados para cada segredo usando o IAM.

Recuperação de segredo seguro

Muitas aplicações armazenam segredos de texto simples, como senhas, tokens, certificados, chaves SSH e chaves de API, em seus arquivos de configuração para serem usados para autenticação quando acessam bancos de dados ou outros serviços. Segredos de texto não criptografado e codificados são propensos a violações e incorrer em riscos de segurança.

O CSMS permite que os usuários consultem dinamicamente segredos por meio de APIs em vez de codificar os segredos, reduzindo significativamente os riscos de violação.

Execute as seguintes operações para gerenciar segredos usando o CSMS:

quando uma aplicação lê suas configurações, ele chama APIs CSMS para recuperar segredos. Não são necessários segredos codificados nem de texto não criptografado.

Rotação de credenciais e chaves

Os segredos precisam ser atualizados periodicamente para aumentar a segurança. Para girar um segredo, você precisa atualizar o segredo em todas as aplicações e configurações que o usam, o que é demorado, propenso a erros e pode causar interrupção do serviço.

O CSMS permite o conveniente gerenciamento secreto de várias versões. As aplicações podem chamar APIs ou SDKs do CSMS para atualizar segredos com segurança sem cometer erros.

Execute as seguintes operações para gerenciar segredos usando o CSMS:

1. um administrador adiciona uma versão secreta no console do CSMS ou por meio de APIs e atualiza o segredo.
2. As aplicações chamam CSMS APIs ou SDKs para obter a versão mais recente ou especificada do segredo e executar atualização completa ou em escala de cinza.
3. Repita regularmente os passos **1** e **2** para girar segredos.
4. Ative a rotação das chaves de criptografia para melhorar a segurança do armazenamento.

Funcionalidades básicas do CSMS

Tabela 3-1 Funcionalidades básicas do CSMS

Função	Descrição
Gerenciamento secreto do ciclo de vida	● Criar, visualizar e agendar e cancelar a exclusão de segredos. ● Alterar a chave de encriptação secreta e a descrição.
Gerenciamento secreto de versões	● Criar e visualizar versões secretas. ● Ver valores secretos.
Gerenciamento de status de versão secreta	Atualizar, consultar e excluir versões de credenciais.
Gerenciamento de tags secretas	Adicionar, pesquisar, editar e excluir tags.

3.2 Vantagens do produto

Criptografia secreta

Os segredos são criptografados pelo KMS antes do armazenamento. As chaves de criptografia são geradas e protegidas pelo HSM de terceiros autenticados. Quando você recupera segredos, eles são transferidos para servidores locais via TLS.

Recuperação de segredo seguro

O CSMS chama APIs secretas em vez de segredos codificados em aplicações. Os segredos podem ser recuperados e gerenciados dinamicamente. O CSMS gerencia segredos de aplicações de maneira centralizada para reduzir os riscos de violação.

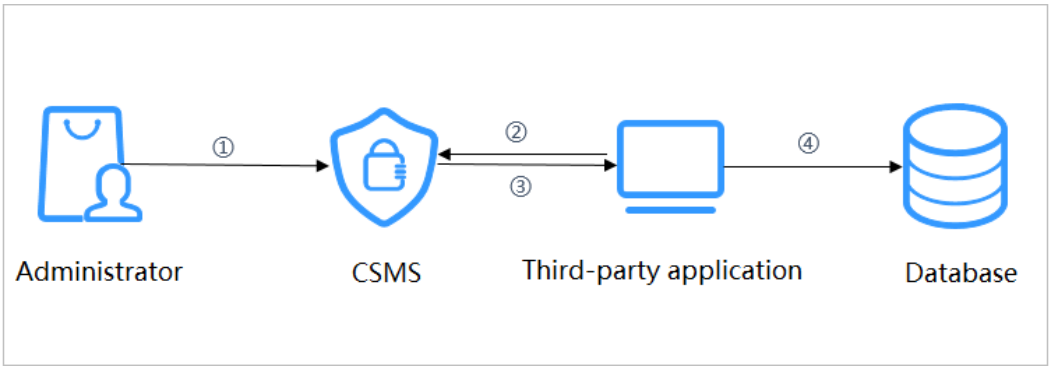
Gerenciamento e controle centralizados de segredos

O gerenciamento de identidade e permissão do IAM garante que apenas usuários autorizados possam recuperar e modificar credenciais. O CTS monitora o acesso às credenciais. Esses serviços impedem o acesso não autorizado e a violação de informações confidenciais.

3.3 Cenários de aplicação

Esta seção usa um nome de usuário básico do banco de dados e sua senha como um exemplo para descrever como o CSMS funciona.

Figura 3-1 Processo de login baseado em segredo



O procedimento é o seguinte:

Passo 1 Crie um segredo no **console** ou por meio de uma API para armazenar informações do banco de dados (como endereço, porta e senha do banco de dados).

Passo 2 Use uma aplicação para acessar o banco de dados. O CSMS consultará o segredo que você criou.

Passo 3 O CSMS recupera e descriptografa o texto cifrado de credenciais e retorna com segurança as informações armazenadas na credencial para a aplicação por meio da API de gerenciamento de credenciais.

Passo 4 A aplicação obtém o segredo de texto simples descriptografado e o usa para acessar o banco de dados.

----Fim

4 KPS

4.1 Funções

Key Pair Service (KPS) é um serviço de nuvem seguro, confiável e fácil de usar projetado para gerenciar e proteger seus pares de chaves SSH (pares de chaves para breve).

Como uma alternativa ao método tradicional de autenticação de nome de usuário+senha, os pares de chaves permitem que você efetue login remotamente em ECSs de Linux.

Um par de chaves, incluindo uma chave pública e uma chave privada, são gerados com base em um algoritmo de criptografia. A chave pública é salva automaticamente no KPS, enquanto a chave privada pode ser salva no host local do usuário. Você também pode salvar suas chaves privadas no KPS e gerenciá-las com o KPS com base em suas necessidades. Se você configurou a chave pública em um ECS de Linux, poderá usar a chave privada para fazer login no ECS sem uma senha. Como você não precisa digitar uma senha, a senha não será interceptada, rachada e vazada, e o servidor se torna mais seguro.

O KPS usa HSMs para gerar números aleatórios verdadeiros que são então usados para produzir pares de chaves. Além disso, adota uma solução de gerenciamento de pares de chaves completa e confiável para ajudar os usuários a criar, importar e gerenciar pares de chaves com facilidade. A chave pública de um par de chaves gerado é armazenada no KPS, enquanto a chave privada pode ser baixada e salva separadamente, o que garante a privacidade e a segurança do par de chaves.

Funções

Usando o console do KPS ou APIs, você pode executar as seguintes operações em pares de chaves:

- Criar, importar, exibir e excluir pares de chaves
- Redefinir, substituir, vincular e desvincular pares de chaves
- Gerir, importar, exportar e limpar chaves privadas

Algoritmos de criptografia suportados pelo KPS

- Os pares de chaves SSH-2 criados no console do KPS suportam apenas os algoritmos de criptografia **RSA-2048**.

- As chaves importadas para o console do KPS suportam os seguintes algoritmos criptográficos:
  - RSA-1024
  - RSA-2048
  - RSA-4096
  - ECDSA-nisty256
  - ECDSA-nisty384
  - ECDSA-nisty521
  - Ed25519
  - DSA

4.2 Vantagens do produto

- Segurança de login reforçada

  Você pode fazer login em um ECS de Linux sem digitar uma senha, evitando efetivamente que a conta seja divulgada devido à interceptação e cracking de senha. Como resultado, a segurança dos ECSs de Linux é bastante melhorada.
- Conformidade regulamentar

  Os números aleatórios são gerados por HSMs validados por terceiros. O acesso a pares de chaves é controlado e todas as operações envolvendo pares de chaves são rastreáveis por registros, em conformidade com as leis e regulamentos chineses e internacionais.

4.3 Cenários de aplicação

Ao adquirir um ECS executando um sistema operacional Linux, você pode optar por autenticar os usuários que tentam fazer login no ECS com o par de chaves SSH fornecido pela KPS. Ao adquirir um ECS executando um sistema operacional Windows, você pode optar por obter a senha usada para fazer login no seu ECS a partir do arquivo de chave fornecido pelo KPS.

Fazer login em um ECS de Linux

Se o Elastic Cloud Server (ECS) executar um sistema operacional Linux, você poderá usar um par de chaves para fazer login no ECS. Para obter detalhes, consulte o **Guia de usuário do Elastic Cloud Server**.

Ao comprar um ECS, você pode escolher um dos seguintes pares de chaves:

- Pares de chaves criados ou importados no console do ECS
- Pares de chaves criados ou importados para o console do KPS

Os dois tipos de pares de chaves só diferem na forma como são importados.

Obter a senha para fazer logon em um ECS do Windows

Se o Elastic Cloud Server (ECS) executar um sistema operacional Windows, você precisará obter a senha de login usando a chave privada de um par de chaves. Para obter detalhes, consulte o **Guia de usuário do Elastic Cloud Server**.

Ao comprar um ECS, você pode escolher um dos seguintes pares de chaves:

- Pares de chaves criados ou importados para o console do ECS
- Pares de chaves criados ou importados para o console do KPS

Os dois tipos de pares de chaves só diferem na forma como são importados.

5 Dedicated HSM

5.1 Ilustração do Dedicated Encryption Workshop

5.2 Funções

O Dedicated HSM é um serviço de nuvem usado para criptografia, descriptografia, assinatura, verificação de assinatura, geração de chaves e armazenamento seguro de chaves.

O Dedicated HSM fornece hardware de criptografia, garantindo segurança e integridade de dados em Elastic Cloud Servers (ECSs) e atendendo aos requisitos FIPS 140-2. O Dedicated HSM oferece um gerenciamento seguro e confiável para as chaves geradas por suas instâncias e usa vários algoritmos para criptografia e descriptografia de dados.

Funções

O Dedicated HSM fornece os seguintes recursos:

- Geração, armazenamento, importação, exportação e gerenciamento de chaves de criptografia (chaves simétricas e assimétricas)
- Criptografia e descriptografia de dados usando algoritmos simétricos e assimétricos
- Usar funções de hash criptográficas para calcular resumos de mensagens e código de autenticação de mensagens baseado em hash
- Assinar dados e código em modo criptografado e verificando assinatura
- Geração aleatória de dados em modo criptografado

Algoritmos de criptografia suportados

Tabela 5-1 Algoritmos de criptografia suportados

Categoria	Algoritmo criptográfico comum
Algoritmo de criptografia simétrica	AES
Algoritmo de criptografia assimétrica	RSA, DSA, ECDSA, DH e ECDH
Algoritmo digest	SHA1, SHA256 e SHA384

5.3 Vantagens do produto

- Nuvem aplicável

  O Dedicated HSM é a escolha adequada para transferir recursos de criptografia off-line para a nuvem, reduzindo seus custos de O&M.
- Dimensionamento elástico

  Você pode aumentar ou diminuir de forma flexível o número de instâncias do HSM de acordo com suas necessidades de serviço.
- Gerenciamento da segurança

  O Dedicated HSM separa o gerenciamento de dispositivos do gerenciamento de conteúdo (informações confidenciais). Como usuário do dispositivo, você pode controlar

a geração, o armazenamento e o acesso das chaves. O Dedicated HSM é responsável apenas por monitorar e gerenciar dispositivos e instalações de rede relacionadas. Mesmo o pessoal de O&M não tem acesso às chaves do cliente.

- Autenticação de permissão
  - Instruções sensíveis são classificadas para autorização hierárquica, o que efetivamente impede o acesso não autorizado.
  - Vários tipos de autenticação são suportados, como nome de usuário/senha e certificado digital.
- Confiável
  - O Dedicated HSM fornece validados pela FIPS 140-2 para proteção de suas chaves, garantindo serviços de criptografia de alto desempenho para atender aos seus rigorosos requisitos de segurança.
  - Cada Dedicated HSM tem seus próprios chips. O serviço não é afetado mesmo que alguns chips estejam danificados.
- Segurança certificada

  As instâncias do Dedicated HSM podem ajudá-lo a proteger seus dados em ECSs e atender aos requisitos de conformidade.
- Aplicações amplas

  O Dedicated HSM oferece instâncias de HSM financeiro, HSM de servidor e HSM de servidor de assinatura para uso em vários cenários de serviço.

5.4 Cenários de aplicação

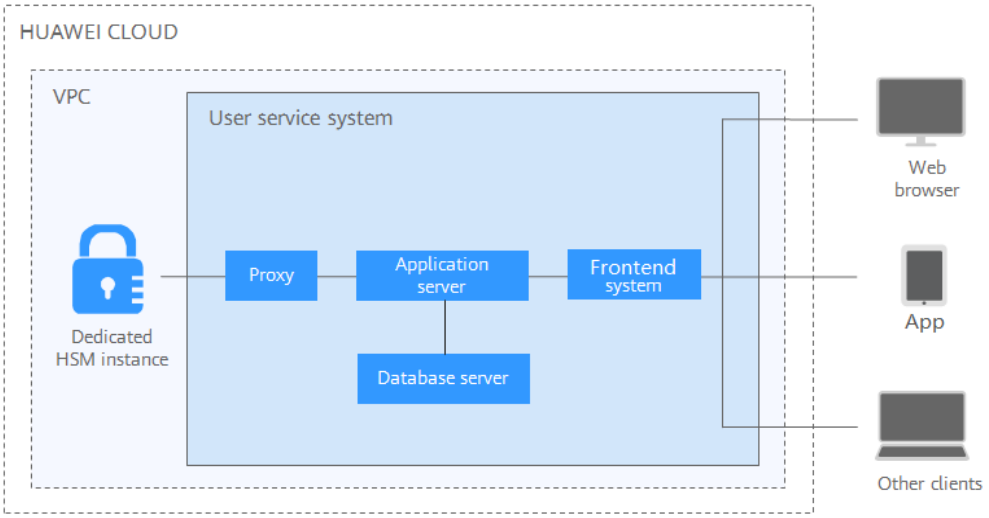
Após a compra de uma instância de Dedicated HSM, você pode usar o UKey fornecido pelo Dedicated HSM para inicializar e gerenciar a instância. Você pode controlar totalmente a geração de chaves, o armazenamento e a autenticação de acesso.

Você pode usar o Dedicated HSM para criptografar seus sistemas de serviço (incluindo criptografia de dados confidenciais, pagamento e tíquetes eletrônicos). O Dedicated HSM ajuda a criptografar dados confidenciais da empresa (como contratos, transações e SNs) e dados confidenciais do usuário (como números de ID do usuário e números de celular), para evitar que hackers invadam a rede e arrastem o banco de dados, o que pode causar vazamento de dados, e impedir o acesso ilegal ou adulteração de dados por usuários internos.

NOTA

Você precisa implantar a instância e o sistema de serviço do Dedicated HSM na mesma VPC e selecionar as regras de grupo de segurança adequadas. Se você tiver alguma dúvida, entre em contato com administradores.

Figura 5-1 Arquitetura



Criptografia de dados sensíveis

Serviços públicos governamentais, empresas de Internet e aplicativos de sistema que contêm imensas informações confidenciais

Os dados são o principal ativo de uma empresa. Cada empresa tem seus principais dados confidenciais. O Dedicated HSM fornece verificação de integridade e armazenamento criptografado para dados confidenciais, o que impede efetivamente que dados confidenciais sejam roubados ou adulterados e impede o acesso não autorizado.

Finanças

Aplicações do sistema para pagamento e pré-pagamento com cartão de transporte, em plataformas de e-commerce, e por outros meios

O Dedicated HSM pode garantir a integridade e a confidencialidade dos dados de pagamento durante a transmissão e o armazenamento, além de garantir a autenticação da identidade de pagamento e o não repúdio do processo de pagamento.

Verificação

Transporte, manufatura e saúde

O Dedicated HSM pode garantir a confidencialidade e a integridade de contratos eletrônicos, faturas, apólices de seguro e registros médicos durante a transmissão e o armazenamento.

6 Descrição do faturamento

Item cobrado

O DEW cobra com base no seu uso e na edição comprada.

Tabela 6-1 Itens cobrados

Nome do serviço	Modo de cobrança	Item cobrado	Descrição
Key Management Service (KMS)	Pagamento por uso	Número de chaves	As instâncias de chave que foram criadas ou importadas com êxito são faturadas com base em pagamento por uso. Os preços são calculados por hora, e nenhuma taxa mínima é necessária.
	Pagamento por uso	Solicitações de API	As primeiras solicitações da API do 20.000 são gratuitas. Chamadas adicionais de API são cobradas. A unidade é chamada 10.000.
KPS	Pagamento por uso	Número de pares de chaves	Gratuito
	Pagamento por uso	Solicitações de API	Gratuito

Nome do serviço	Modo de cobrança	Item cobrado	Descrição
Dedicated HSM	Anual/ Mensal	Edição	Edição Platinum Para detalhes, veja **Edições**.
	Pagamento por uso	Solicitações de API	Gratuito
Cloud Secret Management Service (CSMS)	Pagamento por uso	Número de credenciais	As instâncias CSMS que foram criadas ou importadas com êxito são cobradas em uma base de pagamento por uso. Os preços são calculados por dia, e nenhuma taxa mínima é necessária.
	Pagamento por uso	Solicitações de API	Faturado pelo número de solicitações. A unidade é 10.000 solicitações.

Cobrança

- KMS

  As instâncias de chave criadas ou importadas durante o período da promoção de 1º de outubro de 2021 a 31 de março de 2022 são permanentemente gratuitas. As instâncias de chave criadas ou importadas após 31 de março de 2022 serão cobradas.

  O KMS é cobrado por uso. Nenhuma taxa mínima é necessária. Quando uma chave for criada, ela será cobrada por hora. Você paga pelas chaves que criou e pelas solicitações de API que estão além da faixa gratuita.
- KPS
  - Se você optar por não permitir que a HUAWEI CLOUD gerencie suas chaves privadas ao criá-las ou importá-las, nenhum custo será incorrido.
  - Se você optar por deixar a HUAWEI CLOUD gerenciar suas chaves privadas após importá-las, o KPS será cobrado por hora. Na versão atual, é gratuito.
- Dedicated HSM

  O HSM dedicado oferece pacotes mensais e anuais com base nos modelos de edição e dispositivo das instâncias que você comprou.
- Gerenciamento secreto

  Você é cobrado com base no número de segredos, na duração do uso e no número de solicitações de API.

Para obter detalhes de preços, consulte **Detalhes de preços do produto**.

Alteração do modo de cobrança

O DEW não suporta o cancelamento de inscrição atualmente.

Renovação

Se você não renovar o serviço DEW faturado anualmente/mensal após sua expiração, um período de retenção estará disponível para você.

Para obter detalhes sobre o período de retenção, consulte **Período de retenção**.

Para evitar perdas desnecessárias causadas por problemas de segurança, renove sua assinatura antes que o período de retenção expire.

Você pode renovar seus recursos no console de gerenciamento. Para obter detalhes, consulte **Renovação manual de um recurso**.

Expiração e pagamento em atraso

- Vencimento

  Se você não renovar sua assinatura após a expiração, um período de retenção estará disponível para você. Para obter detalhes, consulte **Período de retenção**.

- Pagamento em atraso

  Se a sua conta tiver um montante pendente, pode ver os respetivos detalhes no Centro de Faturamento. Para evitar que os recursos relacionados sejam interrompidos ou liberados, recarregue sua conta a tempo. Para obter detalhes, consulte **Reembolso do valor pendente**.

Perguntas frequentes

Para mais perguntas frequentes sobre faturamento, consulte **Perguntas frequentes sobre DEW**.

7 Gerenciamento de permissões

Se você quiser atribuir permissões de acesso diferentes a funcionários em uma empresa para os recursos de DEW comprados na HUAWEI CLOUD, você pode usar o Identity and Access Management (IAM) para executar o gerenciamento de permissões refinado. O IAM fornece autenticação de identidade, gerenciamento de permissões e controle de acesso, ajudando você a proteger o acesso aos seus recursos de nuvem.

Com o IAM, você pode usar sua conta da HUAWEI CLOUD para criar usuários do IAM para seus funcionários e atribuir permissões aos usuários para controlar seu acesso a tipos de recursos específicos. Por exemplo, se você tiver desenvolvedores de software e quiser atribuir a eles a permissão para acessar o DEW, mas não para excluir o DEW ou seus recursos, em seguida, você pode criar uma política do IAM para atribuir aos desenvolvedores a permissão para acessar o DEW, mas impedi-los de excluir dados relacionados ao DEW.

Se a conta da HUAWEI CLOUD atendeu aos seus requisitos e você não precisa criar um usuário IAM independente para controle de permissão, pode pular esta seção. Isso não afetará outras funções do DEW.

O IAM é oferecido gratuitamente e você paga apenas pelos recursos faturáveis em sua conta. Para obter mais detalhes, consulte **Visão geral de serviço do IAM**.

Permissões do DEW

Por padrão, os novos usuários do IAM não têm permissões atribuídas. Você precisa adicionar um usuário a um ou mais grupos e anexar políticas de permissões ou funções a esses grupos. Os usuários herdam permissões de seus grupos e podem executar operações especificadas em serviços de nuvem com base nas permissões.

DEW é um serviço de nível de projeto implantado e acessado em regiões físicas específicas. Para atribuir permissões a um grupo de usuários, especifique o escopo como projetos específicos da região e selecione projetos para que as permissões entrem em vigor. Se **All projects** estiver selecionado, as permissões entrarão em vigor para o grupo de usuários em todos os projetos específicos da região. Os usuários precisam alternar para a região autorizada ao acessar o DEW.

Você pode conceder permissões aos usuários usando funções e políticas.

- Funções: um tipo de mecanismo de autorização de granulação grosseira que define permissões relacionadas às responsabilidades do usuário. Esse mecanismo fornece apenas um número limitado de funções de nível de serviço para autorização. Alguns papéis dependem de outros papéis para ter efeito. Ao atribuir tais funções aos usuários,

lembre-se de atribuir as funções das quais eles dependem. No entanto, as funções não são uma escolha adequada para autorização refinada e controle de acesso seguro.

- Políticas: um tipo de mecanismo de autorização refinado que define as permissões necessárias para realizar operações em recursos de nuvem específicos sob determinadas condições. Esse mecanismo permite uma autorização baseada em políticas mais flexível, atendendo aos requisitos de controle de acesso seguro. Por exemplo, você pode conceder aos usuários do DEW apenas as permissões para gerenciar um determinado tipo de servidores em nuvem. A maioria das políticas contém permissões para APIs específicas, e as permissões são definidas usando ações da API. Para as ações de API suportadas pela DEW, consulte **Políticas de permissões e ações suportadas**.

Tabela 7-1 lista todas as políticas do sistema do DEW.

Tabela 7-1 Funções e políticas definidas pelo sistema suportadas pelo DEW

Nome da função/ política	Descrição	Tipo	Dependência
KMS Administrator	Permissões de administrador para o KMS	Função do sistema	Nenhum
KMS CMKFullAccess	Permissões completas para KMS. Os usuários com essas permissões podem executar todas as operações permitidas pelas políticas.	Política do sistema	Nenhum
DEW KeypairFullAccess	Permissões completas para o KPS. Os usuários com essas permissões podem executar todas as operações permitidas pelas políticas.	Política do sistema	Nenhum
DEW KeypairReadOnlyAccess	Permissões somente leitura para o KPS. Os utilizadores com esta permissão só podem ver os dados do KPS.	Política do sistema	Nenhum

Tabela 7-2 lista as operações comuns suportadas por cada permissão definida pelo sistema de DEW. Selecione as permissões conforme necessário.

Tabela 7-2 Operações comuns suportadas por cada política ou função definida pelo sistema

Operação	KMS Administrator	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
Criar uma chave	√	√	x	x
Ativar uma chave	√	√	x	x

Operação	KMS Administrator	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
Desativar uma chave	√	√	x	x
Programar a exclusão da chave	√	√	x	x
Cancelar exclusão de chave agendada	√	√	x	x
Modificar um alias de chave	√	√	x	x
Modificar descrição da chave	√	√	x	x
Gerar um número aleatório	√	√	x	x
Criar uma DEK	√	√	x	x
Criar uma DEK sem texto não criptografado	√	√	x	x
Criptografar uma DEK	√	√	x	x
Descriptografar uma DEK	√	√	x	x
Obter parâmetros para importar uma chave	√	√	x	x
Importar os materiais de chave	√	√	x	x
Eliminar os materiais de chave	√	√	x	x
Criar uma concessão	√	√	x	x
Revogar uma concessão	√	√	x	x

Operação	KMS Administrator	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
Retirar uma concessão	√	√	x	x
Consultar a lista de concessões	√	√	x	x
Consultar concessões removíveis	√	√	x	x
Criptografar dados	√	√	x	x
Descriptografar dados	√	√	x	x
Enviar mensagens de assinatura	√	√	x	x
Autenticar assinatura	√	√	x	x
Ativar rotação de chaves	√	√	x	x
Modificar o intervalo de rotação da chave	√	√	x	x
Desativar rotação de chaves	√	√	x	x
Consultar status da rotação da chave	√	√	x	x
Consultar instâncias de CMK	√	√	x	x
Consultar tags de chave	√	√	x	x
Consultar tags de projeto	√	√	x	x
Adicionar ou excluir tags de chave em lote	√	√	x	x

Operação	KMS Administrator	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
Adicionar tags a uma chave	√	√	x	x
Excluir tags de chave	√	√	x	x
Consultar a lista de chaves	√	√	x	x
Consultar detalhes da chave	√	√	x	x
Consultar chave pública	√	√	x	x
Consultar quantidade da instância	√	√	x	x
Consultar cotas	√	√	x	x
Consultar a lista de pares de chaves	x	x	√	√
Criar ou importar um par de chaves	x	x	√	X
Consultar pares de chaves	x	x	√	√
Excluir um par de chaves	x	x	√	x
Atualizar descrição do par de chaves	x	x	√	x
Vincular um par de chaves	x	x	√	x
Desvincular um par de chaves	x	x	√	x
Consultar uma tarefa de vinculação	x	x	√	√
Consultar tarefas com falha	x	x	√	√

Operação	KMS Administrator	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
Excluir todas as tarefas que falharam	x	x	√	x
Excluir tarefa com falha	x	x	√	x
Consultar tarefas de execução	x	x	√	√

Links úteis

- **O que é IAM?**
- **Criação de um usuário e autorização do usuário a permissão para acessar o DEW**
- **Políticas de permissões e ações suportadas**

8 Como acessar

A HUAWEI CLOUD fornece uma plataforma de gerenciamento de serviços baseada na web. Você pode acessar o DEW usando a API via HTTPS ou no console de gerenciamento.

- Console de gerenciamento

  Se você se registrou na nuvem pública, pode fazer login no console de gerenciamento diretamente. No canto superior esquerdo do console, clique em  . Escolha **Security & Compliance** > **Data Encryption Workshop**.

- API

  Você pode acessar o DEW usando a API. Para obter detalhes, consulte a *Referência de API do Data Encryption Workshop*.

9 Serviços relacionados

OBS

O Object Storage Service (OBS) é um serviço de armazenamento em nuvem otimizado para armazenar grandes quantidades de dados. Ele fornece recursos de armazenamento ilimitados, seguros e altamente confiáveis a um custo relativamente baixo. O KMS fornece recursos centrais de gerenciamento e controle de CMKs para o OBS. Ele é usado para criptografia do lado do servidor com chaves gerenciadas pelo KMS (SSE-KMS) no OBS.

EVS

O Elastic Volume Service (EVS) oferece armazenamento em bloco escalável para servidores em nuvem. Com alta confiabilidade, alto desempenho e especificações elaboradas, os discos do EVS podem ser usados para sistemas de arquivos distribuídos, ambientes de desenvolvimento e teste, aplicativos de data warehouse e cenários de computação de alto desempenho (HPC) para atender a diversos requisitos de serviços. O KMS fornece recursos centrais de gerenciamento e controle de CMKs para EVS. É usado para criptografia no EVS.

IMS

O Image Management Service (IMS) oferece suporte ao gerenciamento do ciclo de vida de imagens. O KMS fornece recursos centrais de gerenciamento e controle de CMKs para o serviço de gerenciamento de imagens (IMS). Ele é usado para criptografia de imagem privada no IMS.

ECS

O Elastic Cloud Server (ECS) é um componente básico de computação que consiste em CPUs, memória, sistema operacional e EVS. Depois de criar um ECS, você pode usá-lo como seu computador local ou servidor físico.

O KPS gerencia pares de chaves dos ECSs. Os pares de chaves são usados para autenticar usuários que fazem login nos ECSs.

O HSM dedicado pode criptografar dados confidenciais nos sistemas de serviço em seu ECS. Você pode controlar a geração, armazenamento e autorização de acesso de chaves para garantir a integridade e a confidencialidade dos dados durante a transmissão e o armazenamento.

DDS

O Document Database Service (DDS) é um serviço de banco de dados compatível com MongoDB que é seguro, altamente disponível, confiável, escalável e fácil de usar. Possibilita a criação de instâncias de BD, dimensionamento, redundância, backup, restauração, monitoramento e funções de relatórios de alarmes em poucos cliques no console do DDS. O KMS fornece recursos centrais de gerenciamento e controle de CMKs para DDS. Ele é usado para criptografia de disco em DDS.

CTS

O Cloud Trace Service (CTS) fornece um histórico das operações do KMS. Depois que o serviço de CTS estiver habilitado, você poderá exibir todos os rastreamentos gerados para revisar e auditar as operações de KMS executadas. Para obter detalhes, consulte *Guia de usuário do Cloud Trace Service*.

Tabela 9-1 Operações de DEW suportadas pelo CTS

Operação	Tipo de recurso	Nome do rastreamento
Criar uma CMK	cmk	createKey
Criar uma DEK	cmk	createDataKey
Criar uma DEK sem texto não criptografado	cmk	createDataKeyWithoutPlaintext
Ativar uma CMK	cmk	enableKey
Desativar uma CMK	cmk	disableKey
Criptografar uma DEK	cmk	encryptDatakey
Descriptografar uma DEK	cmk	decryptDatakey
Programar a exclusão de uma CMK	cmk	scheduleKeyDeletion
Cancelar a exclusão programada de uma CMK	cmk	cancelKeyDeletion
Gerar de números aleatórios	rng	genRandom
Alterar o alias de uma CMK	cmk	updateKeyAlias
Alterar a descrição de uma CMK	cmk	updateKeyDescription
Alertar riscos sobre a exclusão de CMK	cmk	deleteKeyRiskTips
Importar material de chave	cmk	importKeyMaterial
Excluir material de chave	cmk	deleteImportedKeyMaterial
Criar uma concessão	cmk	createGrant
Aposentar um subsídio	cmk	retireGrant

Operação	Tipo de recurso	Nome do rastreamento
Revogar uma concessão	cmk	revokeGrant
Criptografar dados	cmk	encryptData
Descriptografar dados	cmk	decryptData
Adicionar uma tag	cmk	dealUnifiedTags
Excluir uma tag	cmk	dealUnifiedTags
Adicionar ou excluir tags em lotes	cmk	dealUnifiedTags
Excluir tags em lote	cmk	batchDeleteKeyTags
Criar ou importar um par de chaves SSH	par de chaves	createOrImportKeypair
Excluir um par de chaves SSH	par de chaves	deleteKeypair
Importar uma chave privada	par de chaves	importPrivateKey
Exportar uma chave privada	par de chaves	exportPrivateKey
Comprar uma instância de DDM	hsm	purchaseHsm
Configurar uma instância do HSM	hsm	createHsm
Excluir de uma instância de DDM	hsm	deleteHsm

IAM

O Identity and Access Management (IAM) fornece a função de gerenciamento de permissões para DEW.

Somente os usuários que têm permissões de Administrador KMS podem usar DEW.

Somente os usuários que têm as permissões de administrador do KMS e administrador do servidor podem usar a função de par de chaves.

Para solicitar permissões, entre em contato com um usuário com permissões de administrador de segurança. Para obter detalhes, consulte a *Guia de usuário do Identity and Access Management*.

10 Mecanismo de proteção de dados pessoais

Para garantir que seus dados pessoais, como nome de usuário, senha e número de telefone celular, não serão vazados ou obtidos por entidades ou pessoas não autorizadas ou não autenticadas, o DEW controla o acesso aos dados e registra logs para operações realizadas nos dados.

Dados pessoais a recolher

Tabela 10-1 lista os dados pessoais gerados ou coletados pelo DEW.

Tabela 10-1 Dados pessoais

Tipo	Origem	Pode ser modificado	Obrigatório
ID do locatário	● ID de locatário no token quando uma operação é executada no console. ● ID do locatário no token quando uma API é invocada.	Não	Sim

Modo de armazenamento

Os IDs de locatário não são dados confidenciais e são armazenadas em texto simples.

Controle de permissão de acesso

Os usuários podem visualizar apenas logs relacionados aos seus próprios serviços.

Registros de log

O DEW registra logs para todas as operações, como edição, consulta e exclusão, realizadas em dados pessoais. Os logs são carregados no Cloud Trace Service (CTS). Você pode exibir somente os logs gerados para as operações que você executou.

A Histórico de alterações

Lançado em	Descrição
29/03/2022	Este é o décimo quinto lançamento oficial. Otimização da descrição de faturamento em **Descrição de faturamento**.
27/12/2021	Este é o décimo quarto lançamento oficial. Otimização de funções na seção **Funções**. Otimização da descrição em **Cenários de aplicação**.
26/10/2021	Este é o treze lançamento oficial. Adição de descrição sobre o gerenciamento secreto em **CSMS**.
30/09/2021	Este é o décimo segundo lançamento oficial. ● Adição de links para documentos relacionados na seção **Cenários de aplicação**. ● Melhoria da descrição de faturamento em **Descrição do faturamento**.
20/07/2021	Este é o décimo primeiro lançamento oficial. Otimização de funções e recursos em **Funções**.
10/06/2021	Este é o décimo lançamento oficial. Adição da tabela "Operações comuns suportadas por cada política ou função definida pelo sistema" em **Gerenciamento de permissões**.
14/12/2020	Este é o nono lançamento oficial. Adição de **Mecanismo de proteção de dados pessoais**.
27/05/2020	Este é o oitavo lançamento oficial. Adição de **Descrição do faturamento**.

Lançado em	Descrição
10/02/2020	Este é o sétimo lançamento oficial. Modificação de nomes de políticas de sistema de DEW na seção "Gerenciamento de permissões" no capítulo "Visão geral de serviço" com base nas alterações da GUI do IAM: alteração de **DEW Keypair Admin** para **DEW KeypairFullAccess**, **DEW Keypair Viewer** para **DEW KeypairReadOnlyAccess** e **KMS CMK Admin** para **KMS CMKFullAccess**.
03/12/2019	Este é o sexto lançamento oficial. Adição da seção "Criptografia do servidor do RDS".
04/07/2019	Este é o quinto lançamento oficial. ● Adição do processo de uso em **Usar o KMS**. ● Otimização de **Gerenciamento de permissões**.
30/03/2019	Este é o quarto lançamento oficial. Otimização da estrutura do documento para fornecer aos usuários uma melhor referência.
30/05/2018	Este é o terceiro lançamento oficial. ● Modificação de seção "Funções": adição de descrição sobre vinculação, desvinculação, reinicialização e substituição de um par de chaves. ● Adição de descrição sobre a importação e exportação de chaves privadas em **Serviços relacionados**.
30/01/2018	Este é o segundo lançamento oficial. ● Adição da seção "Par de chaves de SSH". ● Modificação de seção "Cenários de aplicações": adição de parte "Autenticação de usuários fazendo login em ECSs". ● Modificação de seção "Funções": adição de descrições sobre a criação, importação e exclusão de pares de chaves. ● Modificação de seção **Usar o KMS**: adição de descrição sobre o ECS. ● Modificação de seção **Serviços relacionados**: adição de descrição sobre o relacionamento com o ECS
31/12/2017	Este é o primeiro lançamento oficial.