## Data Encryption Workshop

# Visão geral de serviço

**Edição** 16

**Data** 14-09-2024

**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. Ele fornece serviços como Key Management Service (KMS), Cloud Secret Management Service (CSMS), Key Pair Service (KPS) e Dedicated Hardware Security Module (Dedicated HSM). O DEW protege seus dados e chaves e simplifica o gerenciamento de chaves. O DEW usa módulos de segurança de hardware (HSMs) para proteger a segurança de suas chaves e pode ser integrado a vários serviços da Huawei Cloud. Além disso, o DEW permite que você desenvolva aplicações de criptografia personalizadas.

**Figura 1-1** Subserviços do DEW

**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.<br>O KMS usa módulos de segurança de hardware (HSMs) para proteger as chaves. O HSM atende aos requisitos de segurança FIPS 140-2 Nível 3. Ele ajuda você a criar e gerenciar chaves. Todas as chaves são protegidas por chaves raiz em HSMs para evitar vazamento de chaves. | **Tipos de chaves** |
| Cloud Secret Management Service (CSMS) | O CSMS é um serviço de hospedagem do segredo seguro, confiável e fácil de usar.<br>Os usuários ou aplicações podem usar o CSMS para criar, recuperar, atualizar e excluir credenciais de maneira unificada durante todo o ciclo de vida do segredo. O CSMS pode ajudá-lo a eliminar os riscos incorridos pela codificação rígida, configuração de texto não criptografado e abuso de permissão. | **Criação de 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 (abreviadamente, pares de chaves).<br>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. | **Criação de um par de chaves** |

| Serviço | Descrição | Referência |
| --- | --- | --- |
| Dedicated Hardware Security Module<br>(Dedicated HSM) | O HSM dedicado permite a criptografia de dados na nuvem, especificamente, criptografando e descriptografando dados, verificando assinaturas, gerando chaves e armazenando chaves.<br>O HSM dedicado fornece hardware de criptografia, garantindo a segurança e a integridade dos dados em Elastic Cloud Servers (ECSs) e atendendo aos requisitos de conformidade. O HSM dedicado oferece um gerenciamento seguro e confiável para as chaves geradas por suas instâncias e usa vários algoritmos para criptografia e descriptografia de dados. | **HSM dedicado** |

# 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 chaves são protegidas por chaves raiz em HSMs para evitar vazamento de chaves. O módulo HSM atende aos requisitos de segurança FIPS 140-2 Nível 3.

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 seus requisitos de auditoria e conformidade regulatória.

### Funções

- No console do KMS, você pode:
  - Criar, consultar, ativar e desativar CMKs, bem como programar e cancelar a exclusão de CMK.
  - Modificar o alias e as descrições de CMKs.
  - Usar a ferramenta on-line para criptografar e descriptografar dados de pequeno porte.
  - Adicionar, pesquisar, editar e excluir tags.
  - Criar, cancelar e consultar concessões.
- Você pode usar as APIs para:
  - Criar, criptografar ou descriptografar DEKs.
  - Retirar concessões.
  - Assinar ou verificar a assinatura de mensagens ou resumos de mensagens.
  - Gerar e verificar códigos de autenticação de mensagens.

  Para obter detalhes, consulte a *Referência de API do Data Encryption Workshop*.
- Gerar números aleatórios verdadeiros de hardware.

  Você pode gerar números aleatórios de 512 bits com base no hardware usando a API do KMS. Os números aleatórios verdadeiros de 512 bits podem ser usados como base para

os materiais de chaves e parâmetros de criptografia. Para obter detalhes, consulte a *Referência de API do Data Encryption Workshop*.

## Algoritmos de chave suportados pelo KMS

As chaves simétricas criadas no console do KMS usam os algoritmos AES e SM4. As chaves assimétricas criadas pelo KMS são compatíveis com os algoritmos RSA, SM2 e ECC.

**Tabela 2-1** Algoritmos de chave suportados pelo KMS

| Tipo de chave | Tipo de algoritmo | Especificações da chave | Descrição | Cenário de aplicação |
| --- | --- | --- | --- | --- |
| Chave simétrica | AES | AES_256 | Chave simétrica de AES | ● Criptografia e descriptografia de dados<br>● Criptografia e descriptografia de DEKs<br>**NOTA**<br>Você pode criptografar e descriptografar uma pequena quantidade de dados usando a ferramenta on-line no console.<br>Você precisa chamar APIs para criptografar e descriptografar uma grande quantidade de dados. |
| Chave simétrica | AES | ● HMAC_256<br>● HMAC_384<br>● HMAC_512 | Chave simétrica de HMAC | Gera e verifica um código de autenticação de mensagem |

| Tipo de chave | Tipo de algoritmo | Especificações da chave | Descrição | Cenário de aplicação |
|---|---|---|---|---|
| Chave assimétrica | RSA | ● RSA_2048<br>● RSA_3072<br>● RSA_4096 | Senha assimétrica de RSA | ● Assinatura digital e verificação de assinatura<br>● Criptografia e descriptografia de dados<br>**NOTA**<br>Chaves assimétricas são aplicáveis a cenários de assinatura e verificação de assinatura. As chaves assimétricas não são suficientemente eficientes para a criptografia de dados. Chaves simétricas são adequadas para criptografar e descriptografar dados. |
| | ECC | ● EC_P256<br>● EC_P384 | Curva elíptica recomendada pelo NIST | Assinatura digital e verificação de assinatura |

descreve os algoritmos de criptografia e descriptografia suportados para chaves importadas pelo usuário.

**Tabela 2-2** Algoritmos de agrupamento de chaves

| Algoritmo | Descrição | Configuração |
| --- | --- | --- |
| RSAES_OAEP_SHA_256 | Algoritmo RSA que usa OAEP e tem a função de hash **SHA-256** | Selecione um algoritmo baseado em suas funções de HSM.<br>Se o seu HSM oferecer suporte ao algoritmo **RSAES_OAEP_SHA_256**, use **RSAES_OAEP_SHA_256** para criptografar materiais de chave. |

# 2.2 Vantagens

## Ampla integração de serviços

- Ao integrar-se ao OBS, EVS e IMS, você pode usar o KMS para gerenciar as chaves dos serviços ou usar as APIs do KMS para criptografar e descriptografar dados locais.
- Com a integração com o Cloud Trace Service (CTS), você pode usar o CTS para visualizar registros recentes de operação do KMS.

## Conformidade regulatória

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

## Fácil de usar

Você pode usar e gerenciar chaves facilmente usando o console ou APIs, sem precisar comprar dispositivos de criptografia de hardware.

# 2.3 Cenários de aplicações

## Pré-requisitos

Todas as chaves personalizadas mencionadas nesta seção são chaves simétricas. Para obter detalhes sobre chaves simétricas e chaves assimétricas, consulte **Tipos de chaves**.

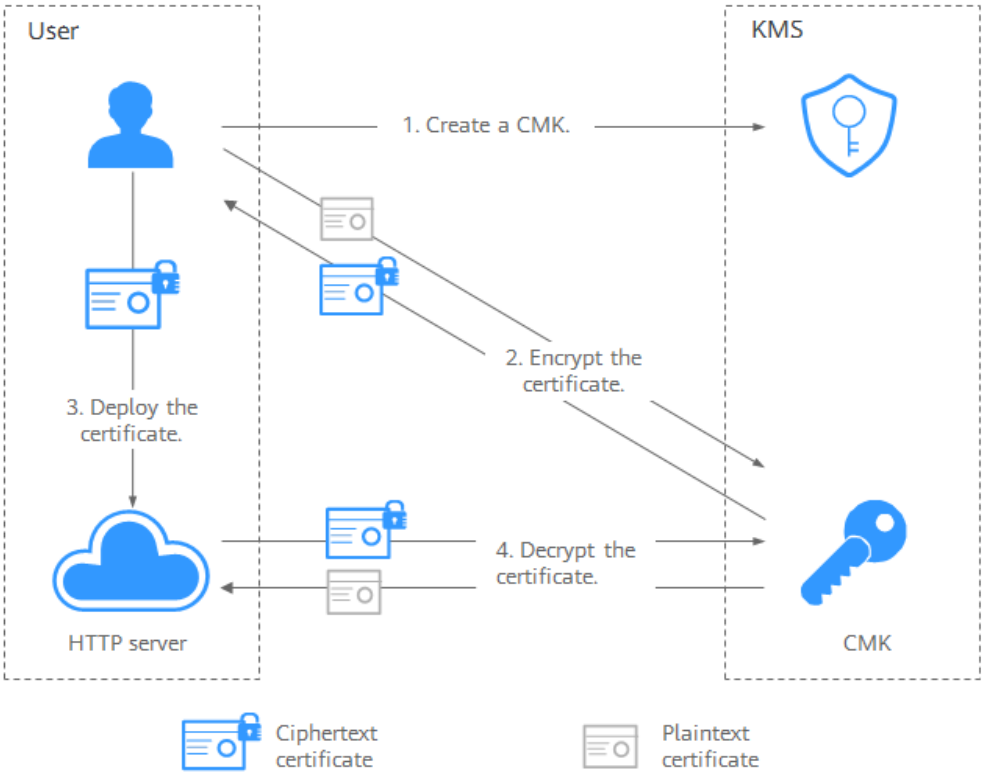
## Criptografia e descriptografia de dados pequenos

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 API de **encrypt-data** do KMS e use a CMK para criptografar o certificado de texto não criptografado.
3. Implemente o certificado em um servidor.
4. O servidor chama a API de **decrypt-data** do KMS para descriptografar o certificado de texto cifrado.

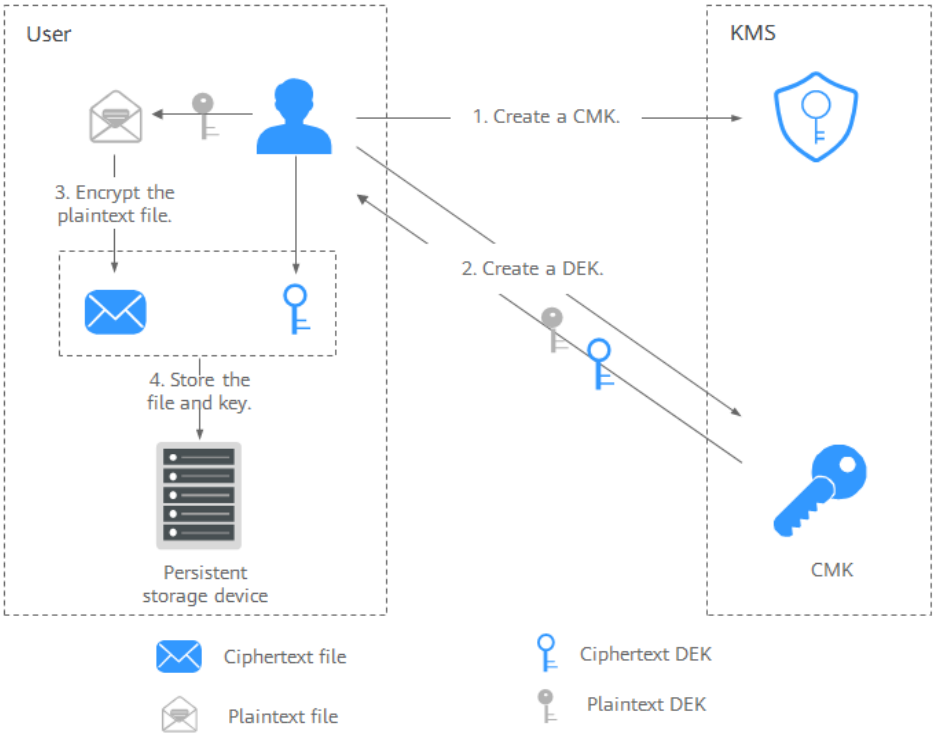
## Criptografia e descriptografia de dados grandes

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 API de **create-datakey** 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 foi gerada usando uma chave personalizada para criptografar a DEK de texto não criptografado.

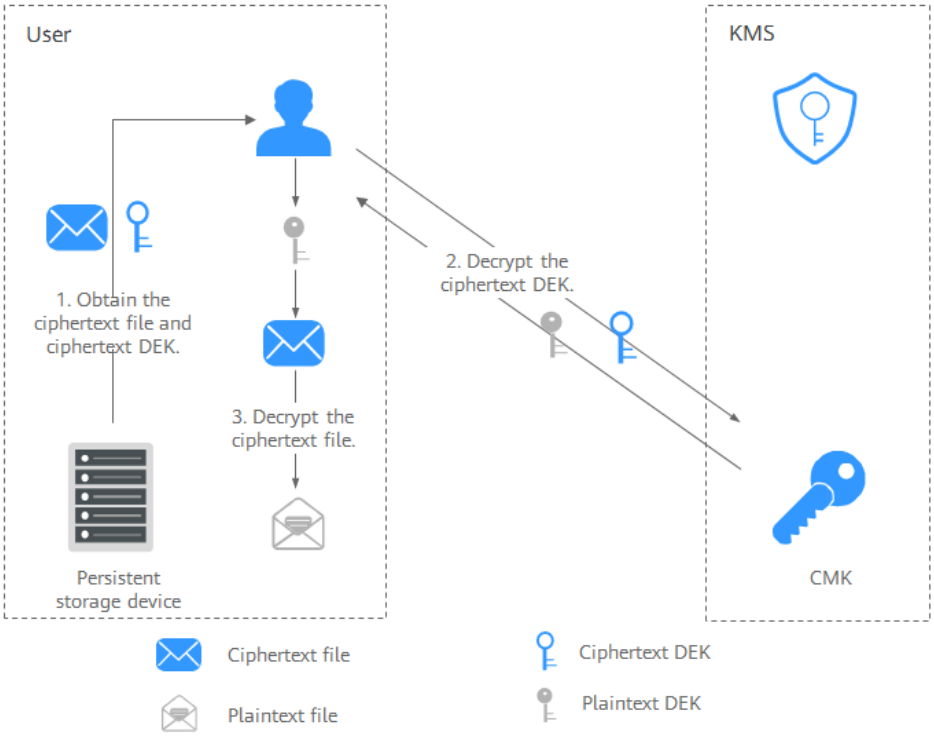
c. Use a DEK de texto não criptografado para criptografar o arquivo. Um arquivo de texto cifrado é gerado.

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 API de **decrypt-datakey** do KMS e use a CMK correspondente (aquela usada para criptografar a DEK) para descriptografar a DEK de texto cifrado. Então você obtém a 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

| Documentação | Link |
| --- | --- |
| Melhores práticas | • **Criptografia ou descriptografia de pequenos volumes de dados**<br>• **Criptografia ou descriptografia de uma grande quantidade de dados** |
| Exemplo de API | • **Criptografia ou descriptografia de pequenos volumes de dados**<br>• **Criptografia ou descriptografia de uma grande quantidade de dados** |

# 2.4 Uso do KMS

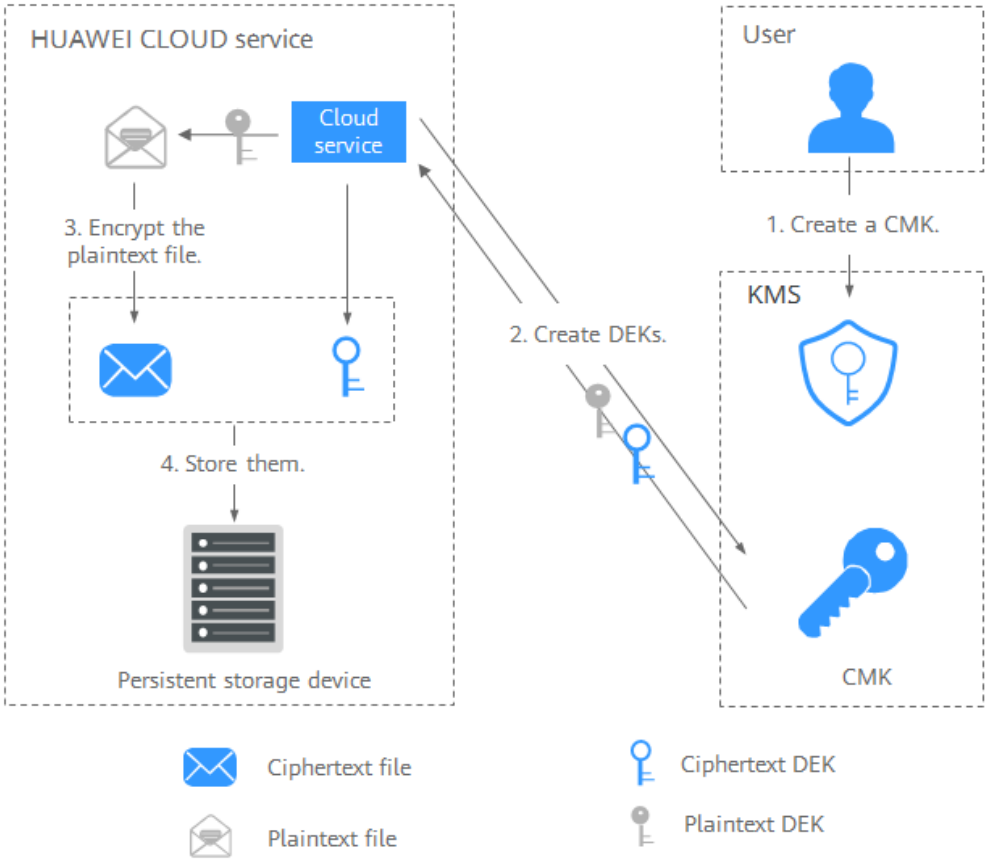
## Pré-requisitos

Todas as chaves personalizadas mencionadas nesta seção são chaves simétricas. Para obter detalhes sobre chaves simétricas e chaves assimétricas, consulte **Tipos de chaves**.

## Interação com os serviços da Huawei Cloud

Serviços da Huawei Cloud usam a tecnologia de criptografia de envelope e chamam as APIs do KMS para criptografar os recursos do serviço. Suas CMKs estão sob seu próprio gerenciamento. Com sua concessão, os serviços da Huawei Cloud usam uma chave personalizada específica sua para criptografar dados.

**Figura 2-4** Como a Huawei Cloud usa o KMS para criptografia




O processo de criptografia é o seguinte:

1. Crie uma chave personalizada no KMS.
2. Serviços da Huawei Cloud chamam a API **create-datakey** 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 usam a DEK de texto não criptografado para criptografar um arquivo de texto não criptografado, gerando um arquivo de texto cifrado.
4. Serviços da Huawei Cloud armazenam a 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 chave personalizada especificada pelo KMS para descriptografar a DEK de texto cifrado, usa a DEK descriptografada para descriptografar dados e fornece os dados descriptografados para os usuários baixarem.

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

| Nome do serviço | Descrição |
| --- | --- |
| Object Storage Service (OBS) | Você pode fazer upload e download de objetos do Object Storage Service (OBS) no modo comum ou no modo de criptografia no lado do servidor. Quando você faz upload de 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 não criptografado. O OBS suporta a criptografia no lado do servidor com o modo de chaves gerenciadas por KMS (SSE-KMS). No modo SSE-KMS, o OBS usa as chaves fornecidas pelo KMS para criptografia do lado do servidor.<br>Para obter detalhes sobre como carregar objetos para o OBS no modo SSE-KMS, consulte o **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 criptografados.<br>Para obter detalhes sobre como usar a função de criptografia do EVS, consulte **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.<br>Para obter detalhes sobre como usar a função de criptografia de imagem privada do Image Management Service (IMS), consulte **Guia de usuário do Image Management Service**. |
| Scalable File Service (SFS) | Ao criar um sistema de arquivos no SFS, a CMK fornecida pelo KMS pode ser selecionada para criptografar o sistema de arquivos, de modo que os arquivos armazenados no sistema de arquivos sejam criptografados automaticamente.<br>Para obter detalhes sobre como usar a função de criptografia do sistema de arquivos do SFS, consulte **Guia de usuário do Scalable File Service**. |

| Nome do serviço | Descrição |
| --- | --- |
| 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.<br>Para obter detalhes sobre como usar a função de criptografia de disco do RDS, consulte **Guia de usuário do Relational Database Service**. |
| Document Database Service (DDS) | Ao comprar uma instância do 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.<br>Para obter detalhes sobre como usar a função de criptografia de disco do DDS, consulte **Primeiros passos do Document Database Service**. |

### Trabalho com aplicações de usuário

Para criptografar dados de texto não criptografado, uma aplicação de usuário pode chamar a API do 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 criptografia é o seguinte:

1. A aplicação chama a API **create-key** do KMS para criar uma chave personalizada.
2. A aplicação chama a API **create-datakey** do KMS para criar uma DEK. Uma DEK de texto não criptografado 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 não criptografado para criptografar um arquivo de texto não criptografado. Um arquivo de texto cifrado é gerado.
4. A aplicação salva o 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*.

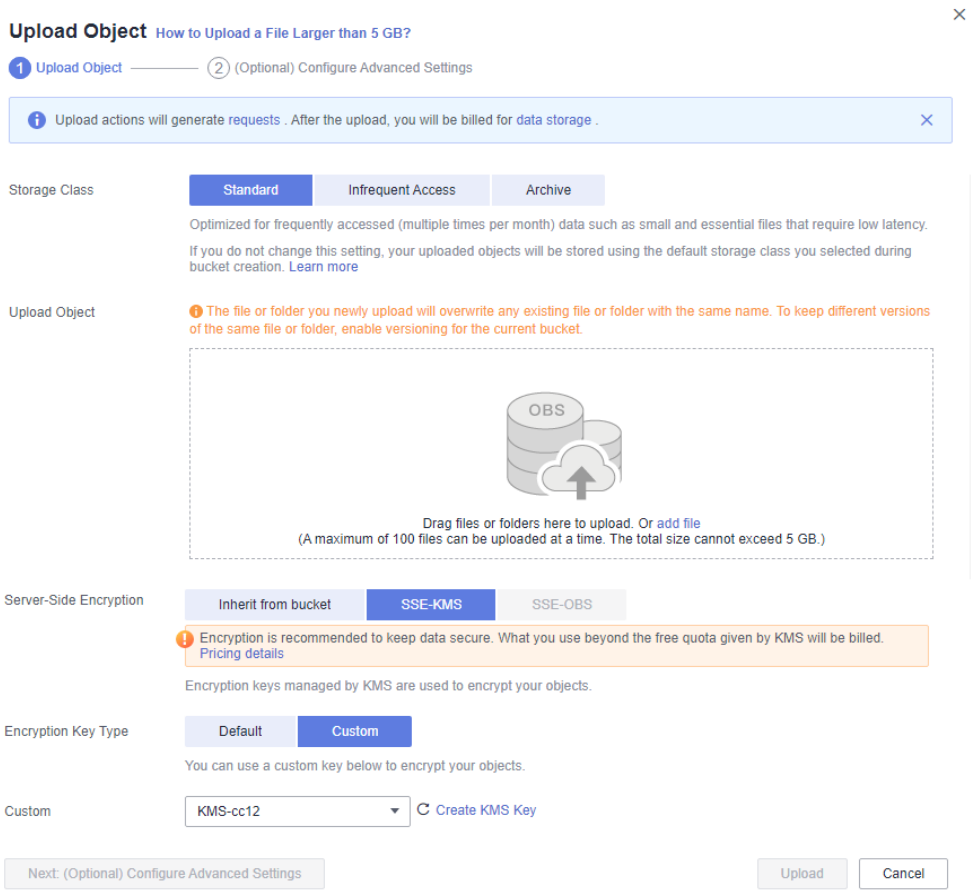
## 2.5 Serviços em nuvem com KMS integrado

## 2.5.1 Criptografia de dados no OBS

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

  **Figura 2-5** Criptografia no lado do servidor do OBS




  Existem dois tipos de CMKs que podem ser usados:

  – A chave padrão **obs/default** criada pelo KMS

  – Chaves personalizadas que você criou no console do KMS

- Como alternativa, você pode chamar APIs do OBS para carregar um arquivo com criptografia no lado do servidor usando chaves gerenciadas pelo KMS (SSE-KMS). Para obter detalhes, consulte *Referência de API do Object Storage Service*.

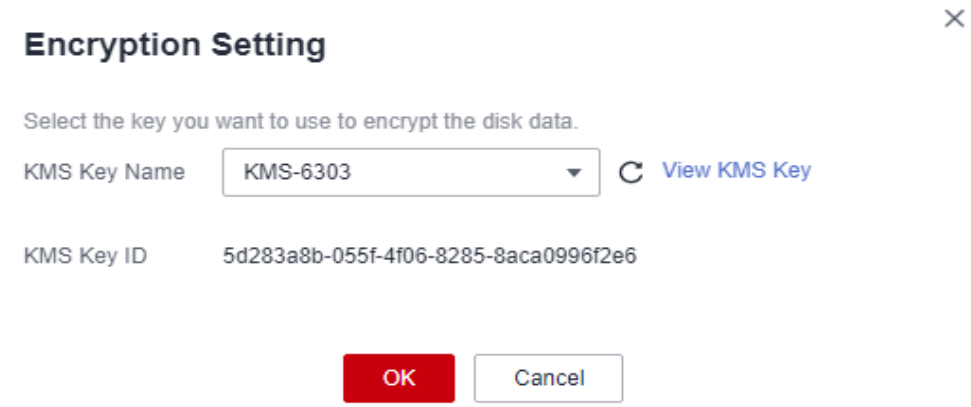
## 2.5.2 Criptografia de dados no EVS

- Ao comprar um disco, você pode escolher **Advanced Settings** > **Encryption** para criptografar o disco usando a chave fornecida pelo KMS. Para obter 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** Criptografia de dados no EVS




Existem dois tipos de CMKs que podem ser usados:

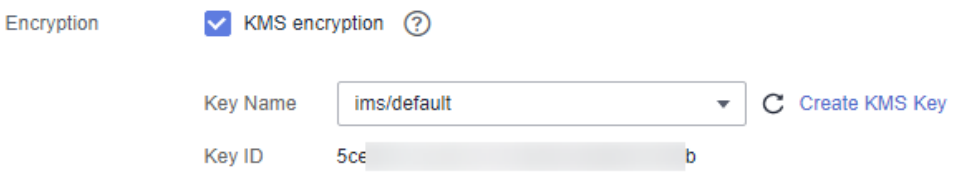
- A chave padrão **evs/default** criada pelo KMS
- Chaves personalizadas que você cria no console do KMS usando materiais de chave gerados pelo KMS

- Você também pode chamar APIs do EVS para criar discos do 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 o *Guia de usuário do Image Management Service*.

**Figura 2-7** Criptografia de dados no IMS




Existem dois tipos de CMKs que podem ser usados:

- A chave padrão **ims/default** criada pelo KMS
- Chaves personalizadas que você cria no console do KMS usando materiais de chave gerados pelo KMS

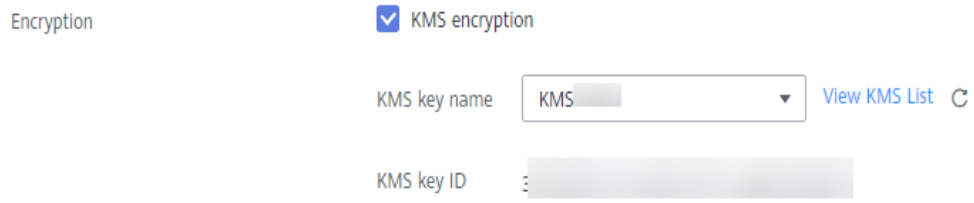
  

- Você também pode chamar APIs do IMS para criar arquivos de imagem criptografados. Para obter detalhes, consulte *Referência de API do Image Management Service*.

## 2.5.4 Criptografia de dados no SFS

- Ao criar um sistema de arquivos usando o Scalable File Service (SFS), você pode selecionar **KMS encryption** e usar a chave fornecida pelo KMS para criptografar o sistema de arquivos. Para obter detalhes, consulte **Figura 2-8**. Para obter mais informações, consulte o *Guia de usuário do Scalable File Service*.

  **Figura 2-8** Criptografia de dados no SFS

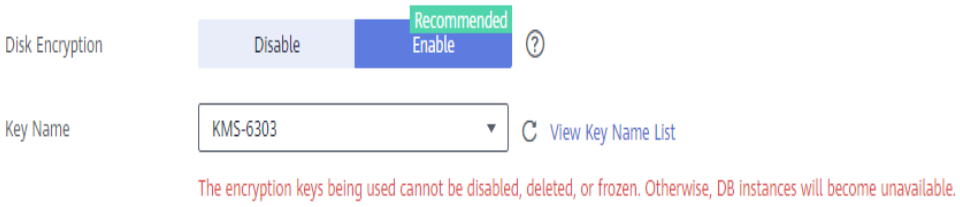
  
  

  Você pode usar uma chave personalizada criada no console do KMS para criptografia.
- Você pode usar a API do SFS para criar um sistema de arquivos criptografado. Para obter detalhes, consulte a *Referência de API do Scalable File Service*.

## 2.5.5 Criptografia de dados no RDS

- Quando um usuário compra uma instância de banco de dados do Relational Database Service (RDS), o usuário 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 2-9** Criptografia de dados no RDS

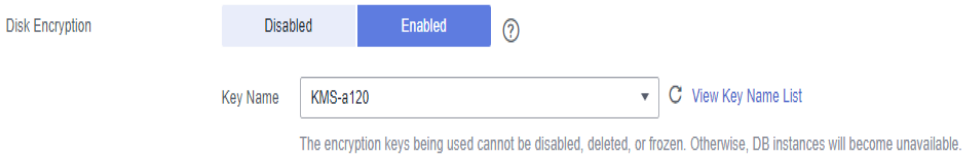
  Você pode usar uma chave personalizada criada no console do KMS para criptografia.
- Você também pode chamar as APIs do RDS para comprar instâncias de banco de dados criptografadas. Para obter detalhes, consulte *Guia de usuário do Relational Database Service*.

## 2.5.6 Criptografia de dados no DDS

- Quando um usuário compra uma instância de banco de dados do DDS, o usuário 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 o *Guia de usuário do Document Database Service*.

**Figura 2-10** Criptografia de dados no DDS




Você pode usar uma chave personalizada criada no console do KMS para criptografia.

- Você também pode chamar a API necessária do DDS para comprar instâncias de banco de dados criptografadas. Para obter detalhes, consulte *Referência de API do Document Database Service*.

# 3 CSMS

## 3.1 Funções

O CSMS é um serviço de hospedagem do segredo 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 do segredo. O CSMS pode ajudá-lo a eliminar os riscos incorridos pela codificação rígida, configuração de texto não criptografado 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 durante todo o seu ciclo de vida.

Execute as seguintes operações para gerenciar segredos usando o CSMS:

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

### Recuperação segura de segredos

Muitas aplicações armazenam segredos de texto não criptografado, 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 em texto não criptografado e codificados são propensos a violações e incorrem em riscos de segurança.

O CSMS permite que os usuários consultem dinamicamente os segredos por meio de APIs, em vez de codificá-los, o que reduz bastante os riscos de violação.

Execute as seguintes operações para gerenciar segredos usando o CSMS:

Quando uma aplicação lê suas configurações, ela chama APIs de CSMS para recuperar segredos. Não são necessários segredos codificados ou em texto não criptografado.

## Rotação de credenciais e chaves

Os segredos precisam ser atualizados periodicamente para aumentar a segurança. Para rotacionar um segredo, você precisa atualizá-lo em todas as aplicações e configurações que o utilizam, o que é demorado, sujeito a erros e pode causar interrupção do serviço.

O CSMS permite o conveniente gerenciamento de segredos 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 de segredo no console do CSMS ou por meio de APIs e atualiza o segredo.
2. As aplicações chamam as APIs ou SDKs do CSMS para obter a versão mais recente ou uma versão especificada do segredo e realizar a 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.

## Notificação do evento de segredo

Depois que você se inscrever em um evento associado a um objeto de segredo, se o evento estiver ativado e um evento básico for acionado no objeto de segredo, uma notificação de evento será enviada ao tópico de notificação especificado pelo evento por meio do Simple Message Notification (SMN). Os tipos de evento básicos incluem criação de nova versão de segredos, expiração de versão de segredos, exclusão de segredos e rotação de segredos. Depois de configurar a notificação de eventos, você pode usar funções gerenciadas por eventos no FunctionGraph para girar segredos automaticamente.

Execute as seguintes operações para gerenciar segredos usando o CSMS:

1. O administrador adiciona um evento no console de notificação de eventos do CSMS ou chamando a API.

2. Ao criar ou atualizar um segredo, você precisa vincular o objeto de evento necessário para a assinatura.

3. Você receberá uma notificação de evento quando o status de segredo mudar. Você pode configurar funções no FunctionGraph para atualizar ou girar automaticamente segredos.

## Funcionalidades básicas do CSMS

**Tabela 3-1** Funcionalidades básicas do CSMS

| Função | Descrição |
| --- | --- |
| Gerenciamento do ciclo de vida do segredo | ● Criar, visualizar, agendar e cancelar a exclusão de segredos.<br>● Alterar a chave de criptografia de segredos e a descrição. |

| Função | Descrição |
| --- | --- |
| Gerenciamento da versão de segredos | ● Criar e visualizar versões de segredos.<br>● Visualizar os valores de segredos.<br>● Definir configurações de expiração de versão do segredo. |
| Gerenciamento do status da versão de segredos | Atualizar, consultar e excluir versões de segredos. |
| Gerenciamento de tags de segredos | Adicionar, pesquisar, editar e excluir tags. |
| Gerenciamento de eventos de segredos | ● Criar, exibir e excluir eventos<br>● Tipos de eventos de alteração de segredos |
| Gerenciamento de notificações de segredos | Exibir o tipo de evento de alteração, o nome do evento e o nome do segredo. |

# 3.2 Vantagens

## Criptografia do segredo

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

## Recuperação de segredos segura

O CSMS chama APIs de segredos 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.

## Notificação de alteração de segredo

O SMN notifica os usuários sobre alterações de eventos de segredos básicos em tempo hábil. O FunctionGraph é usado para configurar funções para atualizar ou girar automaticamente segredos.

## Chamada de segredos segura

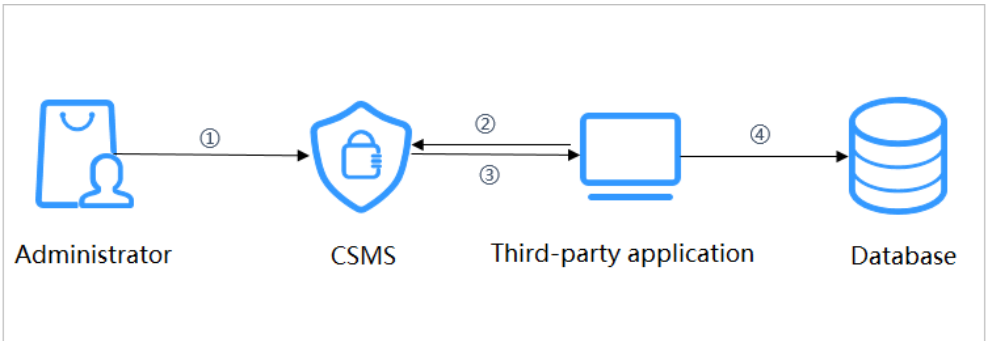
O CCE permite que os usuários montem segredos em pods. Desta forma, as informações confidenciais podem ser desacopladas do ambiente de cluster, o que impede o vazamento de informações causado pela codificação rígida do programa ou pela configuração de texto não criptografado.

# 3.3 Cenários de aplicações

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 logon 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 o endereço, a porta e a 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 do segredo e retorna com segurança as informações armazenadas no segredo para a aplicação por meio da API de gerenciamento de segredo.

**Passo 4** A aplicação obtém o segredo de texto não criptografado 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 (abreviadamente, pares de chaves).

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

Um par de chaves, incluindo uma chave pública e uma chave privada, é gerado com base em um algoritmo criptográfico. 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, você pode usar a chave privada para fazer logon no ECS sem uma senha. Portanto, você não precisa se preocupar com interceptação, quebra ou vazamento de senhas.

### Funções

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

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

### Algoritmos criptográficos suportados pelo KPS

- Os pares de chaves SSH criados no console de gerenciamento suportam os seguintes algoritmos criptográficos:
  - SSH-ED25519
  - ECDSA-SHA2-NISTP256
  - ECDSA-SHA2-NISTP384
  - ECDSA-SHA2-NISTP521
  - SSH_RSA: o comprimento pode ser 2048, 3072 e 4096 bits.

- As chaves SSH importadas para o console do KPS suportam os seguintes algoritmos criptográficos:
  - SSH-DSS
  - SSH-ED25519
  - ECDSA-SHA2-NISTP256
  - ECDSA-SHA2-NISTP384
  - ECDSA-SHA2-NISTP521
  - SSH_RSA: o comprimento pode ser 2048, 3072 e 4096 bits.

# 4.2 Vantagens

- Segurança de logon reforçada

  Você pode fazer logon em um ECS do Linux sem digitar uma senha, evitando efetivamente a interceptação, a quebra ou o vazamento de senhas e melhorando a segurança do ECS do Linux.
- Conformidade regulatória

  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 logs, em conformidade com as leis e regulamentos chineses e internacionais.

# 4.3 Cenários de aplicações

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

## Fazer logon em um ECS de Linux

Se o seu Elastic Cloud Server (ECS) executar o Linux, você poderá usar um par de chaves para fazer logon 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.

## Obtenção da senha para fazer logon em um ECS de Windows

Se o seu ECS executa o Windows, você precisa obter a senha de logon 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 HSM dedicado

# 5.1 Infográficos do HSM dedicado

# 5.2 Funções

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

O HSM dedicado fornece hardware de criptografia, garantindo segurança e integridade de dados em Elastic Cloud Servers (ECSs) e atendendo aos requisitos de FIPS 140-2. O HSM dedicado 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 HSM dedicado 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
- Assinatura de dados e códigos em modo criptografado e verificação da assinatura
- Geração aleatória de dados em modo criptografado

## Algoritmos de criptografia suportados

Você pode usar algoritmos criptográficos chineses e certos algoritmos criptográficos comuns internacionais para atender a vários requisitos do usuário.

**Tabela 5-1** Algoritmos de criptografia suportados

| Categoria | Algoritmo criptográfico comum |
| --- | --- |
| Algoritmo criptográfico simétrico | AES |
| Algoritmo criptográfico assimétrico | RSA, DSA, ECDSA, DH e ECDH |
| Algoritmo de resumo | SHA1, SHA256 e SHA384 |

## Tipos do HSM dedicado

**Tabela 5-2** Tipos do HSM dedicado

| Tipo de HSM | Função | Cenário de aplicação |
| --- | --- | --- |
| Módulo de segurança de hardware (HSM) | ● Criptografia e descriptografia de dados<br>● Assinatura e verificação de dados<br>● Resumo dos dados<br>● Geração e verificação de endereços MAC | Cálculos básicos de senha em aplicações de uma ampla gama de setores, como autenticação de identidade, proteção de dados, chaves SSL e descarregamento de computação. |
| Finanças | ● Geração, criptografia, conversão e verificação do número de identificação pessoal (PIN)<br>● Geração e verificação do MAC (Controle de Acesso ao Meio)<br>● Geração e verificação do CVV (Valor de Verificação de Cartão)<br>● Geração e verificação do TAC (Código de Atribuição do Tipo)<br>● Conjunto de instruções típico de Racal<br>● Conjunto de instruções comuns do PBOC (Banco Popular da China) 3.0 | Cálculo criptográfico em sistemas financeiros, como sistemas de emissão de cartões e sistemas de ponto de venda (POS) |
| Servidor de verificação de assinatura | ● Verificação de assinatura e assinatura<br>● Codificação e decodificação de envelopes digitais<br>● Codificação e decodificação de envelopes digitais assinados<br>● Verificação de certificado | Uso de assinatura em sistemas de AC (Autoridade de certificação), verificação de certificados, transmissão criptografada de uma grande quantidade de dados e autenticação de identidade |

# 5.3 Vantagens

- Nuvem aplicável

  O HSM dedicado é a escolha ideal 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 HSM dedicado 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 às chaves. O HSM dedicado é responsável apenas pelo monitoramento e gerenciamento de 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 HSM dedicado 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 HSM dedicado tem seus próprios chips. O serviço não é afetado mesmo que alguns chips estejam danificados.
  - O HSM dedicado fornece soluções confiáveis de backup e hospedagem para dados do HSM.
- Certificação de segurança

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

  O HSM dedicado 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 aplicações

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

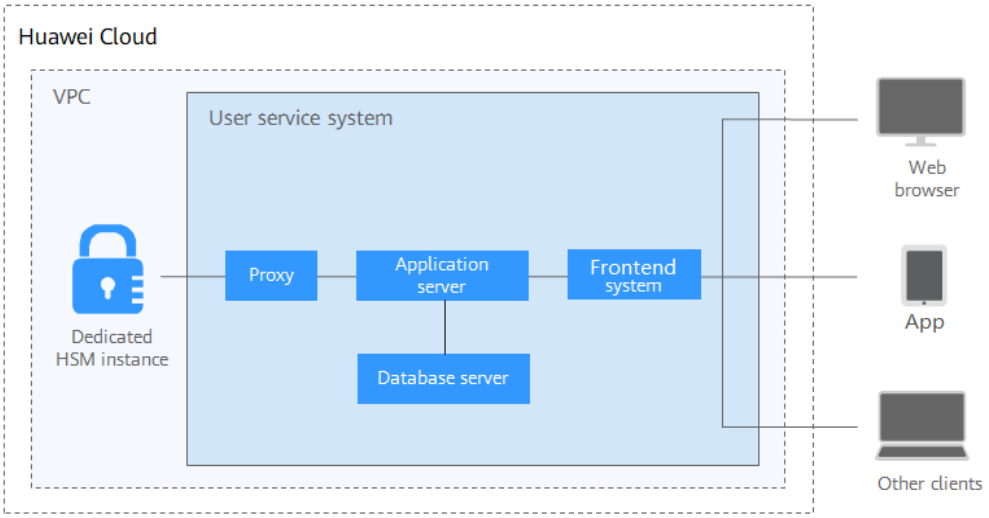
Você pode usar o HSM dedicado para criptografar seus sistemas de serviço (incluindo criptografia de dados confidenciais, pagamento e tíquetes eletrônicos). O HSM dedicado ajuda a criptografar dados confidenciais da empresa (como contratos, transações e SNs) e dados confidenciais do usuário (como números 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 evitar o acesso ilegal ou adulteração de dados por usuários internos.

**NOTA**

Você precisa implementar a instância e o sistema de serviço do HSM dedicado na mesma VPC e selecionar as regras de grupo de segurança adequadas. Se você tiver alguma dúvida, entre em contato com pessoal de suporte técnico.

**Figura 5-1** Arquitetura




## Criptografia de dados confidenciais

Serviços públicos governamentais, empresas de Internet e aplicações de sistema que contêm muitas informações confidenciais

Os dados são o principal ativo de uma empresa. Cada empresa tem seus principais dados confidenciais. O HSM dedicado 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 comércio eletrônico e por outros meios

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

# 6 Segurança

## 6.1 Responsabilidades compartilhadas

Huawei garante que seu compromisso com a segurança cibernética nunca será superado pela consideração de interesses comerciais. Para lidar com os desafios emergentes de segurança na nuvem e ameaças e ataques à segurança na nuvem, a Huawei Cloud constrói um sistema abrangente de garantia de segurança de serviços em nuvem para diferentes regiões e indústrias com base nas vantagens exclusivas de software e hardware da Huawei, leis, regulamentos, padrões da indústria e ecossistema de segurança.

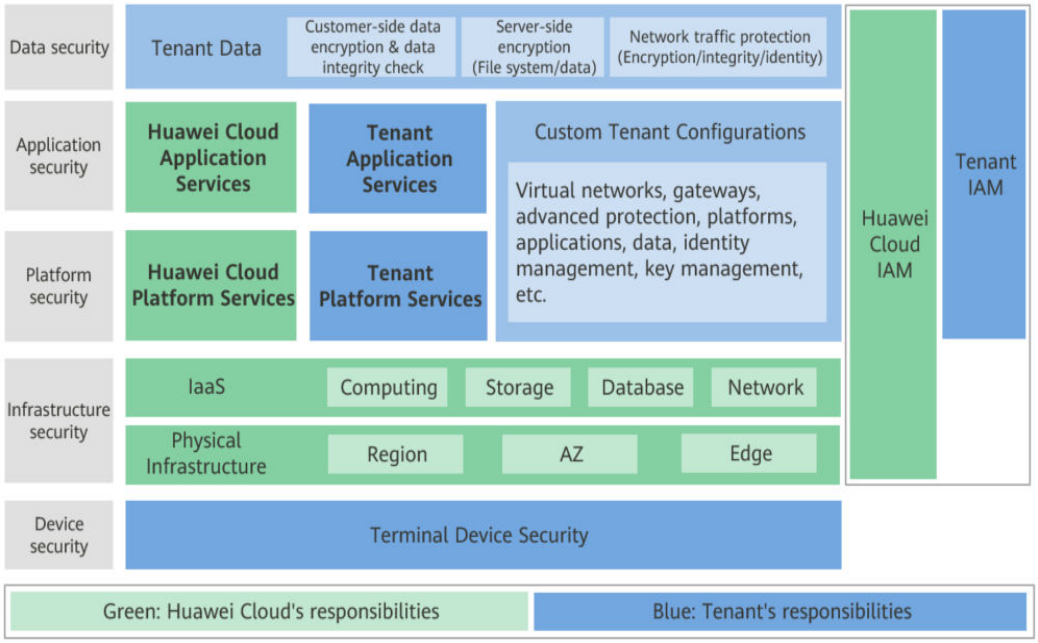
**Figura 6-1** ilustra as responsabilidades partilhadas pela Huawei Cloud e pelos usuários.

- **Huawei Cloud**: garante a segurança dos serviços de nuvem e fornece nuvens seguras. As responsabilidades de segurança da Huawei Cloud incluem garantir a segurança de nossos serviços de IaaS, PaaS e SaaS, bem como os ambientes físicos dos data centers da Huawei Cloud onde nossos serviços de IaaS, PaaS e SaaS operam. A Huawei Cloud é responsável não apenas pelas funções de segurança e pelo desempenho de nossa infraestrutura, serviços de nuvem e tecnologias, mas também pela segurança geral de O&M na nuvem e, no sentido mais amplo, pela certificação de segurança de nossa infraestrutura e serviços.
- **Locatário**: usa a nuvem com segurança. Os locatários da Huawei Cloud são responsáveis pelo gerenciamento seguro e eficaz das configurações personalizadas dos serviços em nuvem, incluindo IaaS, PaaS e SaaS. Isso inclui, mas não se limita a, redes virtuais, o SO de hosts e convidados de máquinas virtuais, firewalls virtuais, API Gateway, serviços avançados de segurança, todos os tipos de serviços em nuvem, dados de locatários, contas de identidade e gerenciamento de chaves.

**O livro branco de segurança da Huawei Cloud** elabora as ideias e medidas para a construção da segurança da Huawei Cloud, incluindo estratégias de segurança na nuvem, o modelo de responsabilidade compartilhada, conformidade e privacidade, organizações e pessoal de segurança, segurança de infraestrutura, serviço e segurança de locatários, segurança de engenharia, segurança de O&M e segurança do ecossistema.

**Figura 6-1** Modelo de responsabilidade de segurança compartilhada da Huawei Cloud




# 6.2 Identificação e gerenciamento de ativos

A tabela a seguir lista os principais ativos gerenciados usando o DEW e como eles são gerenciados.

| Subserviço | Ativo | Como gerenciar |
|---|---|---|
| KMS | Chave | As chaves são protegidas por HSMs. |
| CSMS | Segredo | Os segredos são protegidos por HSMs. |
| KPS | Par de chaves | Os pares de chaves são protegidos por HSMs. |
| HSM dedicado | Instância de HSM dedicado | As permissões das instâncias de HSM dedicado são controladas pelos usuários. Os HSMs são gerenciados nas salas de equipamentos do data center da Huawei Cloud de maneira unificada. |

# 6.3 Autenticação de identidade e controle de acesso

## Autenticação de identidade

Você pode acessar o DEW por meio do console, das APIs ou do SDK do DEW. Independentemente do método de acesso, as solicitações são enviadas por meio das APIs REST fornecidas pelo DEW.

As APIs do DEW suportam vários tipos de solicitações de autenticação. Tomemos como exemplo a AK/SK. Uma solicitação autenticada deve conter um valor de assinatura. O valor da assinatura é calculado com base na chave de acesso do solicitante como o fator de

criptografia e as informações específicas transportadas no corpo da solicitação. O OBS suporta autenticação usando um par de AK/SK. Ele usa criptografia baseada em AK/SK para autenticar solicitações. Para mais detalhes, consulte **Autenticação**.

### Controle de acesso

- O DEW usa o Identity and Access Management (IAM) para implementar o controle de acesso refinado. Por padrão, os novos usuários do IAM não têm permissões atribuídas. Você precisa adicionar um usuário a um ou mais grupos e atribuir políticas de permissões a esses grupos. Após a autorização, o usuário pode executar operações especificadas em serviços de nuvem com base nas permissões. Para obter detalhes, consulte **Controle de permissões**.
- Para os subserviços do KMS, é possível configurar suas permissões no console do KMS. Você pode criar concessões para que outros usuários ou contas do IAM usem suas CMKs. Você pode criar até 100 concessões em uma CMK. Para obter detalhes, consulte **Gerenciamento de uma concessão**.

## 6.4 Tecnologias de proteção de dados

O DEW toma medidas diferentes para manter os dados armazenados no DEW seguros e confiáveis.

| Medida | Descrição | Referência |
| --- | --- | --- |
| Criptografia de transmissão (HTTPS) | O DEW usa HTTPS para melhorar a segurança da transmissão de dados. | **Fazer uma solicitação de API** |
| Gerenciamento de chaves | Os HSMs são usados para gerenciar e armazenar materiais de chaves para evitar vazamentos de chaves. | **Funções** |
| Criptografia do envelope | Em cenários em que uma grande quantidade de dados precisa ser criptografada ou descriptografada, o DEW fornece criptografia de envelope para proteger dados confidenciais em sistemas de aplicações. As chaves de dados usadas para criptografia são armazenadas, transferidas e usadas com envelopes. | **Criptografia ou descriptografia de uma grande quantidade de dados** |
| Mecanismo de rotação da chave | As chaves que são amplamente ou repetidamente usadas são inseguras. O DEW permite que você gire chaves periodicamente e altere os materiais da chave para estar em conformidade com as melhores práticas de criptografia. | **Sobre a rotação de chaves** |

| Medida | Descrição | Referência |
| --- | --- | --- |
| Gerenciamento de segredos | O DEW fornece gerenciamento do ciclo de vida de segredos e oferece suporte ao acesso seguro e conveniente a aplicações, ajudando a reduzir os riscos de vazamento de segredos causados por codificação rígida e a melhorar a segurança de dados e ativos. | **Gerenciamento de segredos** |
| Importação de segredos | Os materiais de chaves importados para o KMS podem ser criptografados usando os algoritmos RSAES_OAEP_SHA_256 ou SM2_ENCRYPT. | **Importação de materiais de chave** |

# 6.5 Auditoria e registro

Cloud Trace Service (CTS) registra as operações nos recursos em nuvem em sua conta. Você pode usar os logs gerados pelo CTS para realizar análises de segurança, rastrear alterações de recursos, auditar conformidade e localizar falhas.

Para obter detalhes, consulte **O que é o Cloud Trace Service?**

O CTS pode rastrear as operações do DEW. Para obter detalhes, consulte **Registros de auditoria**.

# 6.6 Resiliência de serviço

O DEW implementa isolamento de falhas, backup de dados e controle de tráfego para melhorar a resiliência do serviço e aumentar a segurança dos dados do usuário.

## Isolamento de falha

- O design de isolamento entre regiões do DEW garante que as falhas em uma região não afetem os serviços do DEW em outras regiões.
- Os servidores e HSMs do DEW adotam o design de DR em nível de AZ, de modo que as falhas em uma AZ não afetam a disponibilidade do DEW. No caso de uma falha, o DEW protege automaticamente a AZ defeituosa e transfere o tráfego para outra AZ, programando as cargas de trabalho sem problemas.
- Os servidores e HSMs do DEW são implementados no modo de cluster. Se qualquer falha de servidor único ou HSM único não afeta a disponibilidade do DEW.

## Backup de dados

As chaves do DEW são replicadas entre vários HSMs para evitar perda de chave permanente no caso de uma falha de HSM. Os dados do DEW (dados não confidenciais) são replicados entre vários servidores e instâncias de banco de dados e têm backup em tempo real para evitar perda de dados.

## Controle de fluxo

O DEW pode cumprir a meta de SLA de 99,95% de disponibilidade e fornecer uma grande cota de chamadas de API para cada usuário. Se um usuário tiver usado sua cota de chamadas

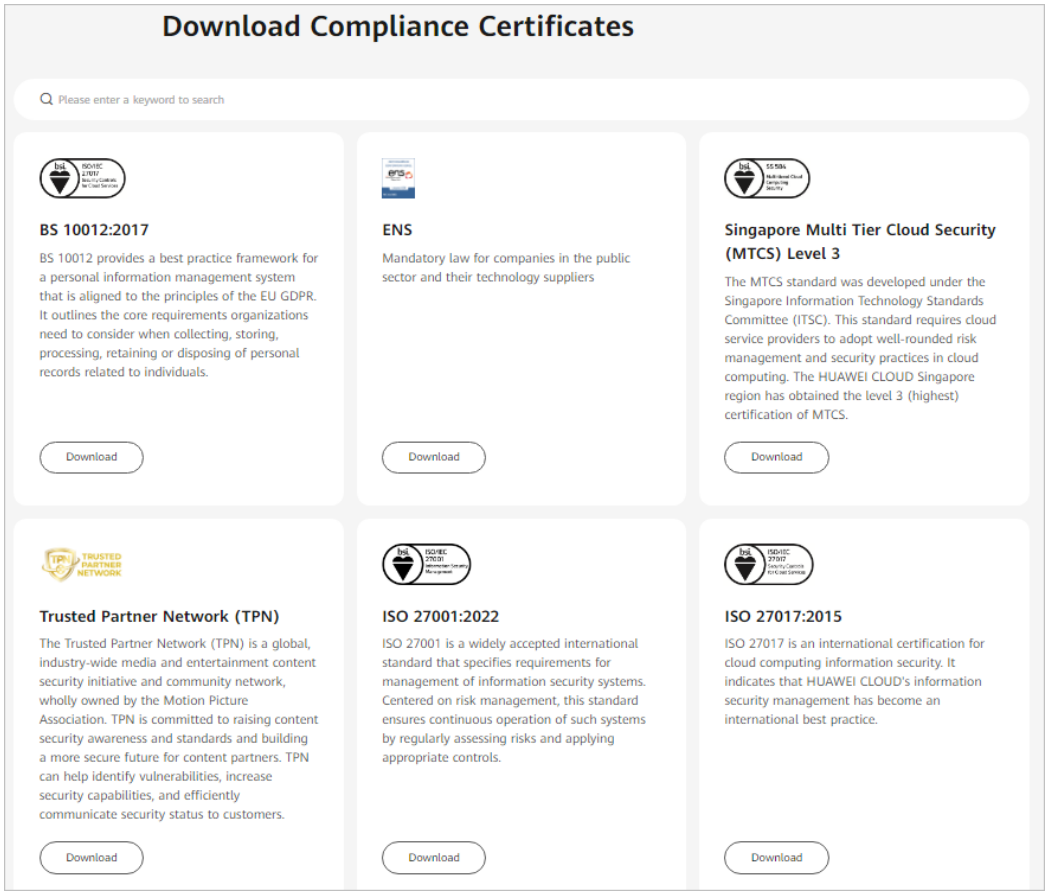
de API, o DEW restringirá suas chamadas de API subsequentes para garantir a disponibilidade do serviço.

# 6.7 Certificados

## Certificados de conformidade

Os serviços e plataformas da Huawei Cloud obtiveram várias certificações de segurança e de conformidade das organizações autorizadas, como a Organização Internacional de Normalização (ISO). Você pode **baixá-los** do console.

**Figura 6-2** Download de certificados de conformidade

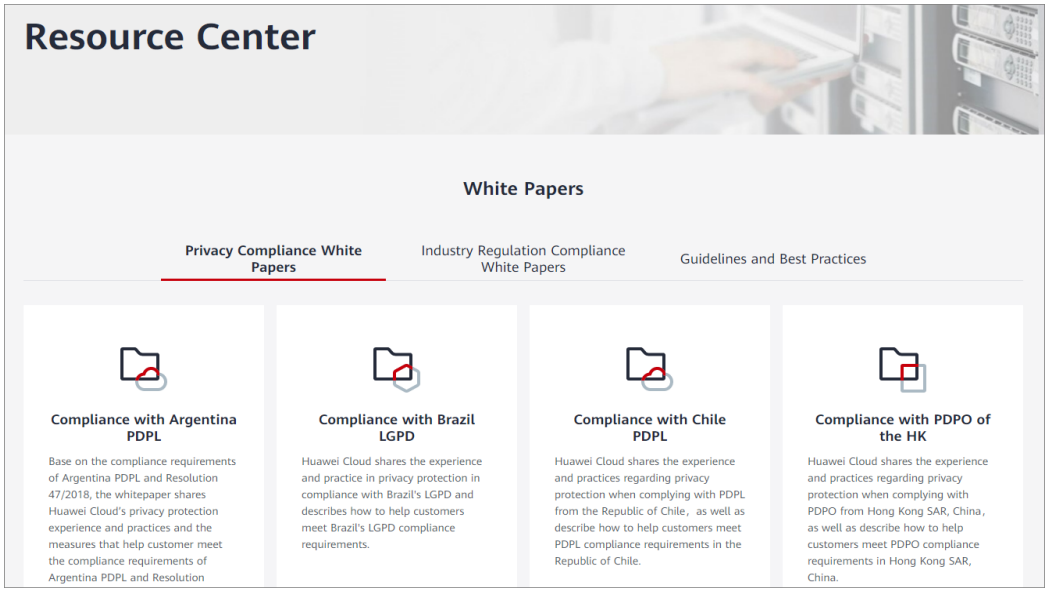



## Central de recursos

A Huawei Cloud também fornece os seguintes recursos para ajudar os usuários a atender aos requisitos de conformidade. Para obter detalhes, consulte **Central de recursos**.

**Figura 6-3** Central de recursos



# 7 Gerenciamento de permissões do DEW

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 refinadas. O IAM fornece autenticação de identidade, gerenciamento de permissões e controle de acesso, ajudando você a proteger o acesso aos seus recursos na Huawei Cloud.

Com o IAM, você pode usar sua conta da Huawei para criar usuários do IAM para seus funcionários e conceder 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 atendeu aos seus requisitos e você não precisa criar um usuário do 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.

O DEW é um serviço de nível de projeto implementado 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 alta granularidade que define permissões relacionadas às responsabilidades do usuário. Esse mecanismo fornece apenas um número limitado de funções de nível de serviço para autorização. Algumas funções dependem de outras funções para entrar em vigor. Ao atribuir essas 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 refinada que define as permissões necessárias para realizar operações em recursos em 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 pelo DEW, consulte **Políticas de permissões e ações suportadas**.

As tabelas a seguir listam todas as permissões do sistema do DEW.

**Tabela 7-1** Políticas do sistema do KMS

| Função/ política | Descrição | Tipo | Dependência |
| --- | --- | --- | --- |
| KMS Administrator | Todas as permissões do KMS | Função | Nenhuma |
| KMS CMKFullAccess | Todas as permissões para chaves do KMS. Os usuários com essas permissões podem executar todas as operações permitidas pelas políticas. | Política | Nenhuma |
| KMS CMKReadOnlyAccess | Permissões somente leitura para chaves do KMS. Os usuários com essas permissões podem executar todas as operações permitidas pelas políticas. | Política | Nenhuma |

**Tabela 7-2** Políticas do sistema do KPS

| Função/ política | Descrição | Tipo | Dependência |
| --- | --- | --- | --- |
| DEW KeypairFullAccess | Todas as permissões para o KPS. Os usuários com essas permissões podem executar todas as operações permitidas pelas políticas. | Política do sistema | Nenhuma |
| DEW KeypairReadOnlyAccess | Permissões somente leitura para o Key Pair Service (KPS) no DEW. Os usuários com essa permissão só podem visualizar os dados do KPS. | Política do sistema | Nenhuma |

**Tabela 7-3** Políticas do sistema do CSMS

| Função/ política | Descrição | Tipo | Dependência |
| --- | --- | --- | --- |
| CSMS FullAccess | Todas as permissões para o Cloud Secret Management Service (CSMS) no DEW. Os usuários com essas permissões podem executar todas as operações permitidas pelas políticas. | Política do sistema | Nenhuma |
| CSMS ReadOnlyAccess | Permissões somente leitura para o Cloud Secret Management Service (CSMS) no DEW. Os usuários com essas permissões podem executar todas as operações permitidas pelas políticas. | Política do sistema | Nenhuma |

NOTA

As políticas DEW KeypairFullAccess e DEW KeypairReadOnlyAccess usadas para autorização de projetos empresariais não entram em vigor para usuários individuais.

Se você for um usuário individual e precisar usar a autorização do projeto empresarial, certifique-se de que você foi adicionado a um grupo de usuários e autorize o grupo de usuários.

Tabela 7-4 lista as operações comuns suportadas por cada permissão definida pelo sistema de DEW. Selecione as permissões conforme necessário.

**Tabela 7-4** Operações comuns para cada política definida pelo sistema ou função do KMS

| Operação | KMS Administrator | KMS CMKFullAccess |
| --- | --- | --- |
| Criar uma chave | √ | √ |
| Ativar uma chave | √ | √ |
| Desativar uma chave | √ | √ |
| Programar a exclusão de chaves | √ | √ |
| Cancelar a exclusão da chave programada | √ | √ |
| Modificar um alias de chave | √ | √ |
| Modificar descrição da chave | √ | √ |
| Gerar um número aleatório | √ | √ |
| Criar uma DEK | √ | √ |
| Criar uma DEK sem texto não criptografado | √ | √ |

| Operação | KMS Administrator | KMS CMKFullAccess |
|---|---|---|
| Criptografar uma DEK | √ | √ |
| Descriptografar uma DEK | √ | √ |
| Obter parâmetros para importar uma chave | √ | √ |
| Importar materiais de chave | √ | √ |
| Excluir materiais de chave | √ | √ |
| Criar uma concessão | √ | √ |
| Revogar uma concessão | √ | √ |
| Retirar uma concessão | √ | √ |
| Consultar a lista de concessões | √ | √ |
| Consultar concessões recuperáveis | √ | √ |
| Criptografar dados | √ | √ |
| Descriptografar dados | √ | √ |
| Enviar mensagens de assinatura | √ | √ |
| Autenticar assinatura | √ | √ |
| Ativar rotação de chaves | √ | √ |
| Modificar intervalo de rotação da chave | √ | √ |
| Desativar rotação de chaves | √ | √ |
| Consultar status da rotação da chave | √ | √ |
| Consultar instâncias de CMK | √ | √ |
| Consultar tags de chave | √ | √ |
| Consultar tags do projeto | √ | √ |
| Adicionar ou excluir tags de chave em lote | √ | √ |
| Adicionar tags a uma chave | √ | √ |
| Excluir tags de chave | √ | √ |
| Consultar a lista de chaves | √ | √ |

| Operação | KMS Administrator | KMS CMKFullAccess |
|---|---|---|
| Consultar detalhes da chave | √ | √ |
| Consultar chave pública | √ | √ |
| Consultar quantidade da instância | √ | √ |
| Consultar cotas | √ | √ |
| Consultar a lista de pares de chaves | x | x |
| Criar ou importar um par de chaves | x | x |
| Consultar pares de chaves | x | x |
| Excluir um par de chaves | x | x |
| Atualizar descrição do par de chaves | x | x |
| Vincular um par de chaves | x | x |
| Desvincular um par de chaves | x | x |
| Consultar uma tarefa de vinculação | x | x |
| Consultar tarefas com falha | x | x |
| Excluir todas as tarefas com falha | x | x |
| Excluir uma tarefa com falha | x | x |
| Consultar tarefas em execução | x | x |

## Links úteis

- **O que é o IAM**
- **Criação de um usuário e autorização ao 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 logon 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 escalável que fornece armazenamento em nuvem seguro, confiável e econômico para grandes quantidades de dados. 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 avançadas, os discos do EVS podem ser usados em sistemas de arquivos distribuídos, ambientes de desenvolvimento e teste, aplicações 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 o EVS. É usado para criptografia no EVS.

## IMS

O Image Management Service (IMS) permite que você gerencie todo o ciclo de vida de suas imagens. O KMS fornece recursos centrais de gerenciamento e controle de CMKs para o Image Management Service (IMS). Ele é usado para criptografia de imagem privada no IMS.

## SFS

O Scalable File Service (SFS) fornece armazenamento de arquivos de alto desempenho (NAS) que pode ser expandido sob demanda. O KMS fornece recursos centrais de gerenciamento e controle de CMKs para o SFS. Ele é usado para criptografia de sistema de arquivos no SFS.

Relational Database Service (RDS) é um banco de dados em nuvem que é confiável, escalável, fácil de gerenciar e imediatamente pronto para uso. O KMS fornece recursos centrais de gerenciamento e controle de CMKs para o RDS. É usado para criptografia de disco em bancos de dados na nuvem.

## ECS

Um ECS é um componente básico de computação que consiste em CPUs, memória, sistema operacional e elastic volume service (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 logon nos ECSs.

O HSM dedicado pode criptografar dados confidenciais nos sistemas de serviço em seu ECS. Você pode controlar a geração, o armazenamento e a autorização de acesso às 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. Ele fornece funções de criação de instância de BD, dimensionamento, redundância, backup, restauração, monitoramento e relatórios de alarmes com apenas alguns cliques no console do DDS. O KMS fornece recursos centrais de gerenciamento e controle de CMKs para o DDS. Ele é usado para criptografia de disco em DDS.

## CTS

O Cloud Trace Service (CTS) fornece a você um histórico das operações do DEW. Depois que o serviço de CTS estiver ativado, 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 do KMS registadas pelo CTS

| Operação | Tipo de recurso | Nome do rastreamento |
|---|---|---|
| Criar uma chave | cmk | createKey |
| Criar uma DEK | cmk | createDataKey |
| Criar uma DEK sem texto não criptografado | cmk | createDataKeyWithoutPlain-text |
| Ativar uma chave | cmk | enableKey |
| Desativar uma chave | cmk | disableKey |
| Criptografar uma DEK | cmk | encryptDatakey |
| Descriptografar uma DEK | cmk | decryptDatakey |
| Programar a exclusão de chaves | cmk | scheduleKeyDeletion |
| Cancelar a exclusão da chave programada | cmk | cancelKeyDeletion |
| Gerar números aleatórios | rng | genRandom |

| Operação | Tipo de recurso | Nome do rastreamento |
|---|---|---|
| Modificar um alias de chave | cmk | updateKeyAlias |
| Modificar descrição da chave | cmk | updateKeyDescription |
| Alertar riscos sobre a exclusão de CMK | cmk | deleteKeyRiskTips |
| Importar materiais de chave | cmk | importKeyMaterial |
| Excluir materiais de chave | cmk | deleteImportedKeyMaterial |
| Criar uma concessão | cmk | createGrant |
| Retirar uma concessão | cmk | retireGrant |
| Revogar uma concessão | cmk | revokeGrant |
| Criptografar dados | cmk | encryptData |
| Descriptografar dados | cmk | decryptData |
| Adicionar uma tag | cmk | createKeyTag |
| Excluir uma tag | cmk | deleteKeyTag |
| Adicionar tags em lotes | cmk | batchCreateKeyTags |
| Excluir tags em lotes | cmk | batchDeleteKeyTags |
| Ativar rotação de chaves | cmk | enableKeyRotation |
| Modificar intervalo de rotação da chave | cmk | updateKeyRotationInterval |

**Tabela 9-2** Operações do KMS registadas pelo CSMS

| Operação | Tipo de recurso | Nome do rastreamento |
|---|---|---|
| Criar um segredo | csms | createSecret |
| Atualizar um segredo | csms | updateSecret |
| Excluir um segredo | csms | forceDeleteSecret |
| Programar a exclusão de um segredo | csms | scheduleDelSecret |
| Cancelar a exclusão programada de segredos | csms | restoreSecretFromDeleted-Status |
| Criar um status de segredos | csms | createSecretStage |
| Atualizar um status de segredos | csms | updateSecretStage |

| Operação | Tipo de recurso | Nome do rastreamento |
|---|---|---|
| Excluir um status de segredos | csms | deleteSecretStage |
| Criar uma versão de segredos | csms | createSecretVersion |
| Baixar um backup de segredos | csms | backupSecret |
| Restaurar um backup de segredos | csms | restoreSecretFromBackup-Blob |
| Atualizar a versão de segredos | csms | putSecretVersion |
| Iniciar a rotação de segredos | csms | rotateSecret |
| Criar um evento de segredos | csms | createSecretEvent |
| Atualizar um evento de segredos | csms | updateSecretEvent |
| Excluir um evento de segredos | csms | deleteSecretEvent |
| Criar uma tag de recurso | csms | createResourceTag |
| Excluir uma tag de recurso | csms | deleteResourceTag |

**Tabela 9-3** Operações do KMS registadas pelo KPS

| Operação | Tipo de recurso | Nome do rastreamento |
|---|---|---|
| Criar ou importar um par de chaves SSH | keypair | createOrImportKeypair |
| Excluir um par de chaves SSH | keypair | deleteKeypair |
| Importar uma chave privada | keypair | importPrivateKey |
| Exportar uma chave privada | keypair | exportPrivateKey |
| Vincular um par de chaves SSH | keypair | bindKeypair |
| Desvincular um par de chaves SSH | keypair | unbindKeypair |
| Limpar chaves privadas | keypair | clearPrivateKey |

**Tabela 9-4** Operações do KMS registradas pelo HSM dedicado

| Operação | Tipo de recurso | Nome do rastreamento |
| --- | --- | --- |
| Comprar uma instância do HSM | hsm | purchaseHsm |
| Configurar uma instância do HSM | hsm | createHsm |
| Excluir uma instância do HSM | hsm | deleteHsm |

## IAM

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

Somente os usuários que têm permissões KMS Administrator podem usar DEW.

Somente os usuários que têm as permissões KMS Administrator e Server Administrator podem usar a função de par de chaves.

Para solicitar permissões, entre em contato com um usuário com permissões Security Administrator. Para obter detalhes, consulte o *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 serem coletados

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

**Tabela 10-1** Dados pessoais

| Tipo | Fonte | Pode ser modificado | Obrigatório |
| --- | --- | --- | --- |
| ID do locatário | • ID de locatário no token quando uma operação é executada no console.<br>• 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 armazenados em texto não criptografado.

## 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.