Data Encryption Workshop

Guia de usuário do

Edição 28

Data 2022-05-30

HUAWEI

HUAWEI CLOUD COMPUTING 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, os serviços e as funcionalidades adquiridos são estipulados pelo contrato estabelecido entre a Huawei Cloud e o cliente. Os produtos, os serviços e as funcionalidades descritos neste documento, no todo ou em parte, podem 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 ESTÃO" sem garantias ou representações de qualquer tipo, sejam expressas ou implícitas.

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 Cloud Computing Technologies Co., Ltd.

Endereço: Huawei Cloud Data Center, Rua Jiaoxinggong
Avenida Qianzhong
Novo Distrito de Gui'an
Guizhou 550029
República Popular da China

Site: https://www.huaweicloud.com/intl/pt-br/

Índice

1 Serviço de gerenciamento de chaves

1.1 Tipos de chaves

As CMKs podem ser categorizadas em chaves simétricas e chaves assimétricas.

Chaves simétricas são comumente usadas para criptografia de dados. Chaves assimétricas são usadas para verificação de assinatura digital ou criptografia de informações confidenciais em sistemas onde a relação de confiança não é mútua. Uma chave assimétrica consiste em uma chave pública e uma chave privada. A chave pública pode ser enviada para qualquer pessoa. A chave privada deve ser armazenada com segurança e acessível apenas a usuários confiáveis.

Uma chave assimétrica pode ser usada para gerar e verificar uma assinatura. Para transferir dados com segurança, um signatário envia a chave pública para um receptor, usa a chave privada para assinar dados e, em seguida, envia os dados e a assinatura para o receptor. O receptor pode usar a chave pública para verificar a assinatura.

Tabela 1-1 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.
Chave assimétrica	RSA	• RSA_2048 • RSA_3072 • RSA_4096	Senha assimétrica de RSA	Criptografa e descriptografa uma pequena quantidade de dados ou cria assinaturas digitais.

Tipo de chave	Tipo de algoritmo	Especificações de chave	Descrição	Utilização
	ECC	• EC_P256 • EC_P384	Curva elíptica recomendada pelo NIST	Assinatura digital

1.2 Criação de uma CMK

Esta seção descreve como criar uma CMK no console do KMS.

As CMKs podem ser categorizadas em chaves simétricas e chaves assimétricas.

Pré-requisitos

Você obteve uma conta e sua senha para fazer logon no console de gerenciamento.

A conta tem permissões KMS CMKFullAccess ou superiores.

Restrições

- Você pode criar até 100 CMKs, excluindo chaves mestras padrão.
- As chaves simétricas são criadas usando o algoritmo de criptografia e descriptografia AES-256. A chave tem 256 bit de comprimento e pode ser usada para criptografar e descriptografar uma pequena quantidade de dados ou chaves de dados.
- Chaves assimétricas são criadas usando algoritmos RSA ou ECC. Chaves RSA podem ser usadas para criptografia, descriptografia, assinatura digital e verificação de assinatura. As chaves ECC podem ser usadas apenas para assinatura digital e verificação de assinatura.
- Os aliases das chaves mestras padrão terminam com **/default**. Portanto, ao escolher aliases para suas CMKs, não use aliases que terminem com **/default**.
- DEW não limita o número de vezes que uma CMK pode ser chamada.

Cenários

- **Criptografar dados no OBS**.
- **Criptografar dados no EVS**.
- **Criptografar dados no IMS**.
- **Criptografar uma instância de banco de dados RDS**.
- Criptografia direta e descriptografia de pequenos volumes de dados
- Criptografia e descriptografia de DEK para aplicações do usuário
- Chaves assimétricas podem ser usadas para assinaturas digitais e verificação de assinatura.

Criar uma CMK

Passo 1 **Faça logon no console de gerenciamento.**

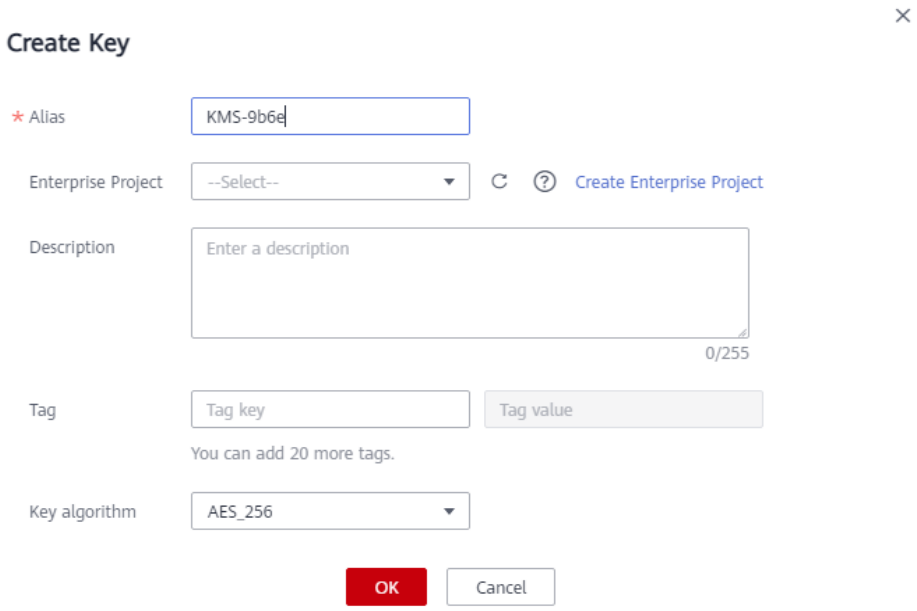
Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou um projeto.

Passo 3 Clicar em . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 Clique em **Create Key** no canto superior direito.

Passo 5 Configurar parâmetros na caixa de diálogo **Create Key**.

Figura 1-1 Criação de uma chave



- **Alias** é o alias da CMK a ser criada.

  NOTA

  - Você pode inserir dígitos, letras, sublinhados (_), hifens (-), dois-pontos (:) e barras (/).
  - Você pode inserir até 255 caracteres.

- **Key Algorithm**: selecione um algoritmo de chave. Para obter mais informações, consulte **Tabela 1-2**.

Tabela 1-2 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.

Tipo de chave	Tipo de algoritmo	Especificações de chave	Descrição	Utilização
Chave assimétrica	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

- **Usage**: selecione **SIGN_VERIFY** ou **ENCRYPT_DECRYPT**.
  - Para uma chave simétrica, o valor padrão é **ENCRYPT_DECRYPT**.
  - Para chaves assimétricas RSA, selecione **ENCRYPT_DECRYPT** ou **SIGN_VERIFY**. O valor padrão é **SIGN_VERIFY**.
  - Para uma chave assimétrica ECC, o valor padrão é **SIGN_VERIFY**.

  NOTA

  O uso da chave só pode ser configurado durante a criação da chave e não pode ser modificado posteriormente.
- (Opcional) **Description** é a descrição da CMK.
- O parâmetro **Enterprise Project** precisa ser definido apenas para usuários corporativos.

  Se você for um usuário corporativo e tiver criado um projeto corporativo, selecione o projeto corporativo necessário na lista suspensa. O projeto padrão é **default**.

  Se não houver opções do **Enterprise Management** exibidas, não será necessário configurá-lo.

  NOTA

  - Você pode usar projetos corporativos para gerenciar recursos de nuvem e membros do projeto. Para obter mais informações sobre projetos corporativos, consulte **Guia de usuário do Enterprise Management**.
  - Para obter detalhes sobre como ativar a função de projeto da empresa, consulte **Ativação da central empresarial**

Passo 6 (Opcional) Adicione tags à CMK conforme necessário e insira a chave da tag e o valor da tag.

NOTA

- Quando uma CMK for criada sem nenhuma tag, você poderá adicionar uma tag à CMK mais tarde, conforme necessário. Clique no alias da CMK, clique na guia **Tags** e clique em **Add Tag**.
- A mesma tag (incluindo chave de tag e valor de tag) pode ser usada para diferentes CMKs. No entanto, na mesma CMK, uma chave de tag pode ter apenas um valor de tag.
- Um máximo de 20 tags podem ser adicionadas para uma CMK.
- Se desejar excluir uma tag da lista de tags ao adicionar várias tags, você pode clicar em **Delete** na linha onde a tag a ser adicionada está localizada para excluir a tag.

Passo 7 Clique em **OK**. Uma mensagem é exibida no canto superior direito da página, indicando que a chave foi criada com sucesso.

Na lista CMK, você pode exibir as CMKs criadas. O status padrão de uma CMK é **Enabled**.

----Fim

Operações relacionadas

- Para obter detalhes sobre como carregar objetos com criptografia do servidor, consulte a seção **Carregamento de um arquivo com criptografia do servidor** no *Guia de operação do console do Object Storage Service*.
- Para obter detalhes sobre como criptografar dados em discos do EVS, consulte a seção **Compra de um disco do EVS** no *Guia de usuário do Elastic Volume Service*.
- Para obter detalhes sobre como criptografar imagens privadas, consulte a seção **Criptografar uma Imagem** no *Guia de usuário do Image Management Service*.
- Para obter detalhes sobre como criptografar discos para uma instância de banco de dados no RDS, consulte a seção "Compra de uma instância" no *Guia de usuário do Relational Database Service*.
- Para obter detalhes sobre como criar uma DEK e uma DEK sem texto simples, consulte as seções "Criação de uma DEK" e "Criação de uma DEK sem texto não criptografado" na *Referência de API do Data Encryption Workshop*.
- Para obter detalhes sobre como criptografar e descriptografar uma DEK para um aplicação de usuário, consulte as seções "Criptografia uma DEK" e "Descriptografia de uma DEK" na *Conferência de API do Data Encryption Workshop*.

1.3 Criação de CMKs usando materiais importados de chave

1.3.1 Visão geral

Uma CMK contém metadados de chave (ID da chave, alias da chave, descrição, status da chave e data de criação) e materiais de chave utilizados para criptografia e descriptografia dados.

- Quando um usuário usa o console do KMS para criar uma CMK, o KMS gera automaticamente um material de chave para a CMK.
- Se quiser usar seu próprio material de chave, você pode usar a função de importação de chave no console do KMS para criar uma CMK cujo material de chave esteja vazio e importar o material de chave para a CMK.

Observações importantes

- Segurança

  Você precisa garantir que as fontes aleatórias atendam aos seus requisitos de segurança ao usá-las para gerar materiais importantes. Ao usar a função de chave de importação, você precisa ser responsável pela segurança de seus principais materiais. Salve o backup original do material da chave para que o material da chave de backup possa ser importado para o KMS no momento em que o material da chave for excluído acidentalmente.

- Disponibilidade e durabilidade

  Antes de importar o material da chave para o KMS, você precisa garantir a disponibilidade e a durabilidade do material da chave.

As diferenças entre o material de chave importado e o material de chave gerado pelo KMS são mostradas em **Tabela 1-3**.

Tabela 1-3 Diferenças entre o material chave importado e o material chave gerado pelo KMS

Fonte de material de chave	Diferença
As CMKs usando materiais de chave importados	● Você pode excluir o material da chave, mas não pode excluir a CMK e seus metadados. ● Tais chaves não podem ser rotacionadas. ● Ao importar o material da chave, você pode definir o tempo de expiração do material da chave. Após a expiração do material da chave, o KMS exclui automaticamente o material da chave dentro de 24 horas, mas não exclui a CMK e seus metadados. É recomendável que você salve uma cópia do material em seu dispositivo local, pois ele pode ser usado para reimportação em casos de materiais de chave inválidos ou exclusão incorreta de materiais de chave. **NOTA** Chaves usando algoritmos RSA_2048, RSA_3072, RSA_4096, EC_P256 e EC_P384 são permanentemente válidas. Seus principais materiais não podem ser excluídos manualmente e seu tempo de expiração não pode ser configurado.
As CMKs usando os principais materiais gerados pelo KMS	● O material da chave não pode ser excluído manualmente. ● As teclas simétricas podem ser giradas. ● Você não pode definir o tempo de expiração para o material de chave.

- Vinculação

  Quando um material de chave é importado para uma CMK, a CMK é permanentemente associada ao material de chave. Outros materiais importantes não podem ser importados para a CMK.

- Singularidade

  Se você usar a CMK criada usando o material de chave importado para criptografar dados, os dados criptografados poderão ser descriptografados somente pela CMK que foi usada para criptografar os dados, porque os metadados e o material de chave da CMK devem ser consistentes.

1.3.2 Importação de materiais de chave

Se você quiser usar seus próprios materiais de chave em vez dos materiais gerados pelo KMS, poderá usar o console para importar seus materiais de chave para o KMS. As CMKs criadas usando materiais importados e materiais gerados pelo KMS são gerenciadas em conjunto pelo KMS.

Esta seção descreve como importar materiais de chave no console do KMS.

Pré-requisitos

- Você obteve uma conta e sua senha para fazer logon no console de gerenciamento.
- Você preparou os materiais de chave a serem importados.

Procedimento

Passo 1 **Faça logon no console de gerenciamento.**

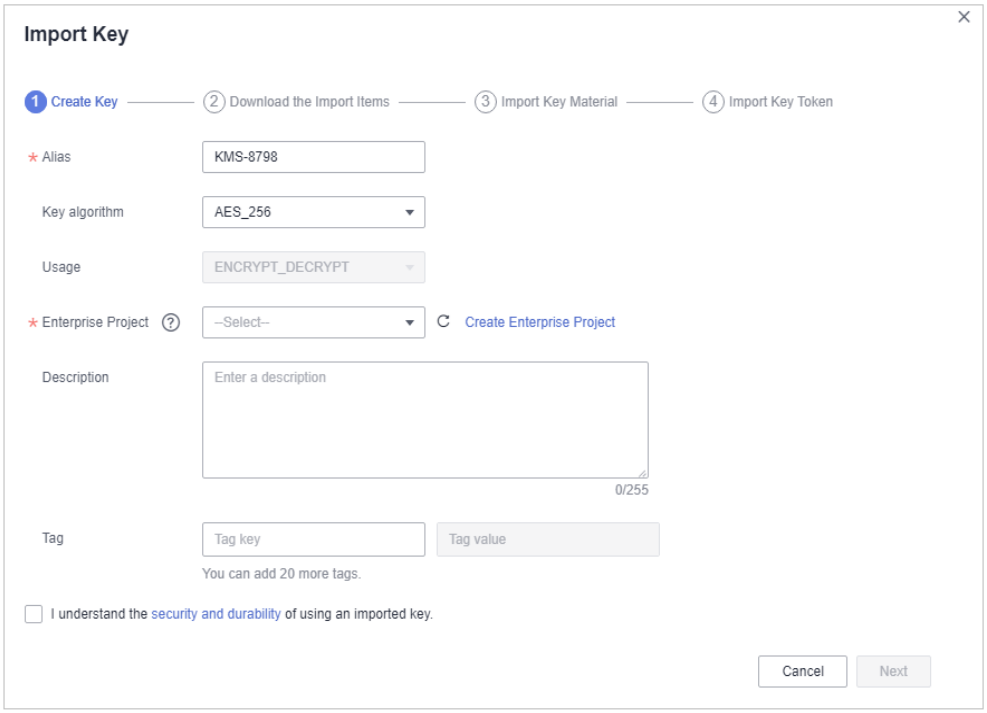
Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou um projeto.

Passo 3 Clicar em . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 Clique em **Import Key**. A caixa de diálogo **Import Key** é exibida.

Passo 5 Configure os parâmetros de chave.

Figura 1-2 Criar uma chave vazia



- **Alias** é o alias da CMK a ser criada.

  NOTA

  - Você pode inserir dígitos, letras, sublinhados (_), hifens (-), dois-pontos (:) e barras (/).
  - Você pode inserir até 255 caracteres.

- **Key Algorithm**: selecione um algoritmo de chave. Para obter mais informações, consulte **Tabela 1-4**.

Tabela 1-4 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.
Chave assimétrica	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

- **Usage**: selecione **SIGN_VERIFY** ou **ENCRYPT_DECRYPT**.
  - Para uma chave simétrica, o valor padrão é **ENCRYPT_DECRYPT**.
  - Para chaves assimétricas RSA, selecione **ENCRYPT_DECRYPT** ou **SIGN_VERIFY**. O valor padrão é **SIGN_VERIFY**.
  - Para uma chave assimétrica ECC, o valor padrão é **SIGN_VERIFY**.

  NOTA

  O uso da chave só pode ser configurado durante a criação da chave e não pode ser modificado posteriormente.
- (Opcional) **Description** é a descrição da CMK.
- O parâmetro **Enterprise Project** precisa ser definido apenas para usuários corporativos.

  Se você for um usuário corporativo e tiver criado um projeto corporativo, selecione o projeto corporativo necessário na lista suspensa. O projeto padrão é **default**.

  Se não houver opções do **Enterprise Management** exibidas, não será necessário configurá-lo.

  NOTA

  - Você pode usar projetos corporativos para gerenciar recursos de nuvem e membros do projeto. Para obter mais informações sobre projetos corporativos, consulte **Guia de usuário do Enterprise Management**.
  - Para obter detalhes sobre como ativar a função de projeto da empresa, consulte **Ativação da central empresarial**

Passo 6 (Opcional) Adicione tags à CMK conforme necessário e insira a chave da tag e o valor da tag.

NOTA

- Se uma CMK foi criada sem nenhuma tag, você pode adicionar uma tag à CMK mais tarde, conforme necessário. Clique no alias da CMK, clique na guia **Tags** e clique em **Add Tag**.
- A mesma tag (incluindo chave de tag e valor de tag) pode ser usada para diferentes CMKs. No entanto, na mesma CMK, uma chave de tag pode ter apenas um valor de tag.
- Um máximo de 20 tags podem ser adicionadas para cada CMK.
- Se desejar excluir uma tag da lista de tags ao adicionar várias tags, você pode clicar em **Delete** na linha onde a tag a ser adicionada está localizada para excluir a tag.

Passo 7 Clique em **security and durability** para entender a segurança e a durabilidade da chave importada.

Passo 8 Selecione **I understand the security and durability of using an imported key** e crie uma CMK cujo material da chave esteja vazio.

Passo 9 Clique em **Next** para ir para a etapa **Download the Import Items**. Selecione um algoritmo de encapsulamento de chave com base em **Tabela 1-5**.

Tabela 1-5 Algoritmos de encapsulamento de chave

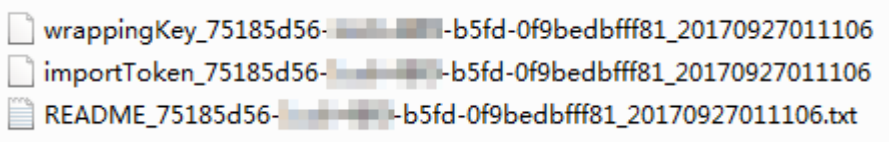
Algoritmo	Descrição	Configuração
RSAES_OAEP_SHA_256	Algoritmo de criptografia de RSA que usa OAEP e tem a função de hash **SHA-256**	Escolha um algoritmo na caixa de listagem suspensa. Se os HSMs oferecerem suporte ao algoritmo **RSAES_OAEP_SHA_256**, use **RSAES_OAEP_SHA_256** para criptografar materiais de chave.

NOTA

Se você interromper um processo de importação de material de chave e quiser tentar novamente, clique em **Import Key Material** na linha da CMK necessária e importe o material de chave na caixa de diálogo exibida.

Passo 10 Clique em **Download**. Os seguintes arquivos são baixados: **wrappingKey**, **importToken** e **README**, como mostrado na **Figura 1-3**.

Figura 1-3 Download de arquivo



- **wrappingKey_*CMKID_DownloadTime*** é uma chave de encapsulamento usada para criptografar materiais de chave.
- **importToken_*CMKID_DownloadTime*** é um token usado para importar materiais de chave para o KMS.

- **README_*CMKID_DownloadTime*** é um arquivo de descrição que registra informações como o número de série de uma CMK, o algoritmo de encapsulamento, o nome da chave de encapsulamento, o nome do arquivo de token e o tempo de expiração do arquivo de token e da chave de encapsulamento.

AVISO

- **wrappingKey_Key ID_***Download_time* é codificado em formato binário.
- A chave de encapsulamento e o token de importação expiram em 24 horas. Se tiverem expirado, baixe-os novamente.

Você também pode obter a chave de encapsulamento e importar o token via API.

1. Chame a API **get-parameters-for-import** para obter a chave de encapsulamento e importar o token.

   O exemplo a seguir descreve como obter a chave de encapsulamento e o token de importação de uma CMK (ID: **43f1ffd7-18fb-4568-9575-602e009b7ee8**; algoritmo de criptografia: **RSAES_OAEP_SHA_256**).

   public_key: conteúdo da chave de encapsulamento (codificação Base-64) retornado após a chamada da API

   import_token: conteúdo do token de importação (codificação Base-64) retornado após a chamada da API

   - Exemplo de solicitação

     ```
     {
         "key_id": "43f1ffd7-18fb-4568-9575-602e009b7ee8",
         "wrapping_algorithm":"RSAES_OAEP_SHA_256"
     }
     ```

   - Exemplo de resposta

     ```
     {
         "key_id": "43f1ffd7-18fb-4568-9575-602e009b7ee8",
         "public_key":"public key base64 encoded data",
         "import_token":"import token base64 encoded data",
         "expiration_time":1501578672
     }
     ```

2. Salve a chave de encapsulamento e converta seu formato. Somente o material da chave criptografado usando a chave de encapsulamento convertida pode ser importado para o console de gerenciamento.

   a. Copie o conteúdo da chave **public_key**, cole-a em um arquivo .txt e salve o arquivo como **PublicKey.b64**.

   b. Use OpenSSL para executar o seguinte comando para executar a codificação Base-64 no conteúdo do arquivo **PublicKey.b64** para gerar dados binários e salvar o arquivo convertido como **PublicKey.bin**:

      openssl enc -d -base64 -A -in PublicKey.b64 -out PublicKey.bin

3. Salve o token de importação, copie o conteúdo do token **import_token**, cole-o em um arquivo .txt e salve o arquivo como **ImportToken.b64**.

Passo 11 Use o arquivo **wrappingKey** para criptografar os materiais de chave a serem importados.

- Método 1: use a chave de encapsulamento baixada para criptografar materiais de chave em seu HSM. Para obter detalhes, consulte o guia de operação do seu HSM.
- Método 2: use o OpenSSL para criptografar os materiais de chave.

> **NOTA**
>
> Se você precisar executar o comando **openssl pkeyutl**, a versão do OpenSSL deve ser 1.0.2 ou posterior.

O exemplo a seguir descreve como usar a chave de encapsulamento baixada para criptografar o material da chave gerada (chave simétrica de 256-bit). O procedimento é o seguinte:

a. Para gerar um material de chave para uma chave simétrica de 256-bit usando o algoritmo AES256, no agente em que o OpenSSL foi instalado, execute o seguinte comando para gerar o material de chave e salve-o como **PlaintextKeyMaterial.bin**:

   openssl rand -out *PlaintextKeyMaterial.bin* 32

   Para gerar um material de chave para uma chave assimétrica RSA ou ECC, execute as seguintes operações:

   i. Gere uma chave hexadecimal AES256.

      openssl rand -out 0xPlaintextKeyMaterial.bin -hex 32

   ii. Converta a chave hexadecimal AES256 para o formato binário.

      cat 0xPlaintextKeyMaterial.bin | xxd -r -ps > PlaintextKeyMaterial.bin

b. Use a chave de encapsulamento baixada para criptografar o material da chave e salve o material da chave criptografada como **EncryptedKeyMaterial.bin**.

   Substitua ***PublicKey.bin*** no comando com o nome da chave de encapsulamento *wrappingKey_key ID_download time* baixado em **Passo 10**.

   Tabela 1-6 Criptografar o material de chave gerado usando a chave de encapsulamento baixada

Algoritmo de chave de encapsulamento	Criptografia de material de chave
RSAES_OAEP_SHA_256	**openssl pkeyutl** **-in *PlaintextKeyMaterial.bin*** **-inkey *PublicKey.bin*** **-out *EncryptedKeyMaterial.bin*** **-keyform der** **-pubin -encrypt** **-pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256**

c. Para importar uma chave assimétrica, gere uma chave privada assimétrica e use um material de chave temporária para criptografar a chave privada.

   - Tome o algoritmo RSA4096 como um exemplo. Realize as operações a seguir:

     1) Gere uma chave privada.

        openssl genrsa -out rsa_private_key.pem 4096

     2) Converta a chave para o formato DER.

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

3) Use um material de chave temporária para criptografar a chave privada.

openssl enc -id-aes256-wrap-pad -K $(cat 0xPlaintextKeyMaterial.bin) -iv A65959A6 -in rsa_private_key.der -out out_rsa_private_key.der

NOTA

Por padrão, o algoritmo -id-aes256-wrap-pad não está habilitado no OpenSSL. Para envolver uma chave, atualize o OpenSSL para a versão mais recente e corrija-a primeiro. Para obter detalhes, consulte Perguntas frequentes.

Passo 12 Clique em **Next** para ir para a etapa **Import Key Material**.

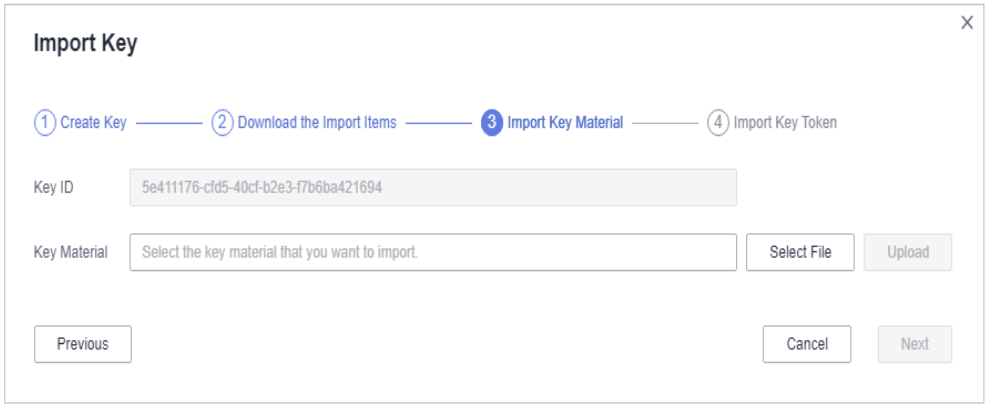
Tabela 1-7 Parâmetros para importar materiais de chave (para chaves simétricas)

Parâmetro	Descrição
Key ID	ID aleatório de uma CMK gerada durante a criação da CMK
Key material	Importar um material de chave.

Tabela 1-8 Parâmetros para importar materiais de chave (para chaves assimétricas)

Parâmetro	Descrição
Key ID	ID aleatório de uma CMK gerada durante a criação da CMK
Material de chave temporária	Importar um material de chave temporária.
Texto cifrado de chave privada	Selecione texto cifrado de chave privada.

Figura 1-4 Importação de materiais de chave



Passo 13 Clique em **Next** para ir para a etapa **Import Key Token**. Configure os parâmetros conforme descrito em **Tabela 1-9**.

Tabela 1-9 Parâmetros para importar um token de chave

Parâmetro	Descrição
Key ID	ID aleatório de uma CMK gerada durante a criação da CMK
Token de importação de chave	Selecione o token baixado em **Passo 10**.
Modo de expiração do material de chave	● **O material de chave nunca expirará**: utilize esta opção para especificar que os materiais de chave não expirarão após a importação. ● **O material de chave expirará**: use essa opção para especificar o tempo de expiração dos materiais de chave. Por padrão, os materiais de chave expiram em 24 horas após a importação. Depois que o material da chave expira, o sistema exclui automaticamente o material da chave dentro de 24 horas. Uma vez que o material da chave é excluído, a chave não pode ser usada e seu status muda para **Pending import**.

Passo 14 Clique em **OK**. Quando a mensagem **Key imported successfully** é exibida no canto superior direito, os materiais são importados.

AVISO

Os materiais de chave podem ser importados com sucesso quando correspondem ao ID da CMK e ao token correspondentes.

Os materiais importados são exibidos na lista de CMKs. O status padrão de uma CMK importada é **Enabled**.

----Fim

1.3.3 Exclusão de materiais de chave

Ao importar materiais de chave, você pode especificar seu tempo de expiração. Depois que o material da chave expirar, o KMS o excluirá e o status da CMK será alterado para **Pending import**. Você pode excluir manualmente os materiais de chave conforme necessário. O efeito da expiração do material da chave é o mesmo da exclusão manual do material da chave.

Esta seção descreve como excluir materiais de chave importados no console do KMS.

Pré-requisitos

- Você obteve uma conta e sua senha para fazer logon no console de gerenciamento.
- Você importou materiais de chave para uma CMK.
- A fonte material da CMK é **External**.
- O status da CMK é **Enabled** ou **Disabled**.

Restrições

- Para reimportar um material de chave excluído, verifique se o material importado é o mesmo que o excluído.
- Os dados criptografados usando uma CMK não podem ser descriptografados se o material da chave da CMK tiver sido excluído. Para descriptografar os dados, importe novamente o material da chave.
- Após a exclusão, a CMK ficará indisponível e seu status mudará para **Pending import**.
- Os materiais de chave das chaves assimétricas não podem ser excluídos diretamente. Para excluí-los, execute as instruções em **Agendamento da exclusão de uma ou mais CMKs**.

Procedimento

Passo 1 **Faça logon no console de gerenciamento.**

Passo 2 Clique em  no canto superior esquerdo do console de gerenciamento e selecione uma região ou um projeto.

Passo 3 Clicar em  . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 Na linha que contém a CMK desejada, clique em **Delete Key Material**.

Passo 5 Na caixa de diálogo exibida, clique em **OK**. Quando **Key material deleted successfully** é exibido no canto superior direito, os materiais da chave são excluídos com sucesso.

Após a exclusão, a CMK ficará indisponível e seu status será alterado para **Pending import**.

----Fim

1.4 Gerenciamento de CMKs

1.4.1 Visualização de uma CMK

Esta seção descreve como exibir as informações sobre a chave mestra no console do KMS, incluindo o alias, o status, o ID e o horário de criação da chave. O status de uma CMK pode ser **Enabled**, **Disabled** ou **Pending deletion**.

Procedimento

Passo 1 **Faça logon no console de gerenciamento.**

Passo 2 Clique em  no canto superior esquerdo do console de gerenciamento e selecione uma região ou um projeto.

Passo 3 Clicar em  . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 Verifique a lista de chaves. **Tabela 1-10** descreve os parâmetros.

Figura 1-5 Chaves personalizadas

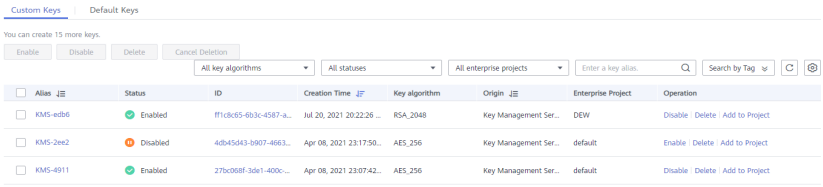


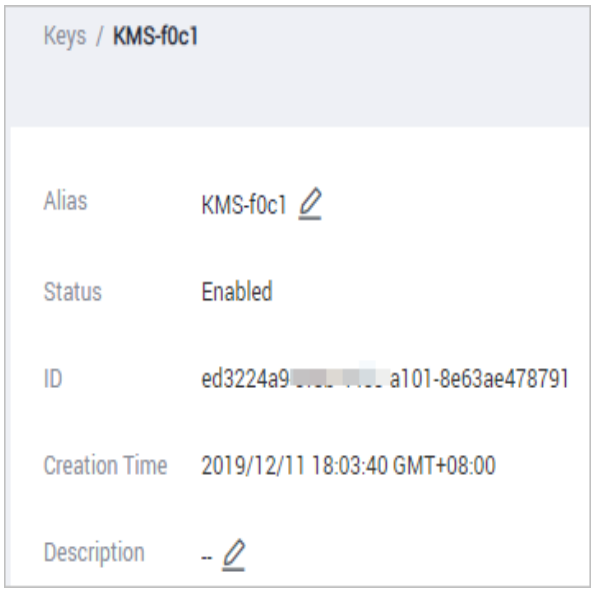
Figura 1-6 Chaves padrão

Tabela 1-10 Parâmetros da lista de chaves

Parâmetro	Descrição
Alias	Alias de uma CMK
Status	Status de uma CMK, que pode ser um dos seguintes: ● **Enabled** A CMK está habilitada. ● **Disabled** A CMK está desativada. ● **Pending deletion** A CMK está programada para exclusão.
ID	ID aleatório de uma CMK gerada durante a criação da CMK **NOTA** Use esse ID como o valor de **Path** se estiver criando uma política personalizada no IAM e tiver selecionado **Specify resource path** para **KeyId**.
Creation Time	Tempo de criação do CMK
Key Algorithm and Usage	Algoritmo de chave selecionado durante a criação da chave e seu uso
Enterprise Project	Projeto empresarial a CMK é usada para

Passo 5 Você pode clicar no alias de uma CMK para exibir seus detalhes, conforme mostrado na **Figura 1-7**.

Figura 1-7 Detalhes da CMK



NOTA

Para alterar o alias ou a descrição da CMK, clique em ao lado do valor de **Alias** ou **Description**.

- Uma chave mestra padrão (cujo sufixo de alias é **/default**) não permite alterações de alias e descrição.
- O alias e a descrição de uma CMK não podem ser alterados se a CMK estiver no status de **Pending deletion**.

----Fim

1.4.2 Ativação de uma ou mais CMKs

Esta seção descreve como usar o console do KMS para ativar uma ou mais CMKs. Somente as CMKs ativadas podem ser usadas para criptografar ou descriptografar dados. Uma nova CMK está no estado **Enabled** por padrão.

Pré-requisitos

- Você obteve uma conta e sua senha para fazer logon no console de gerenciamento.
- A CMK que você deseja habilitar está no status **Disabled**.

Procedimento

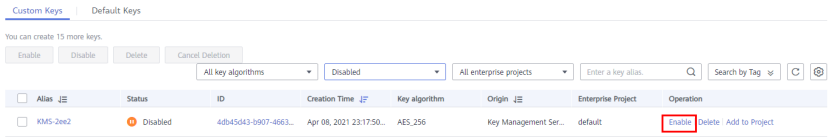
Passo 1 **Faça logon no console de gerenciamento.**

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou um projeto.

Passo 3 Clicar em . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 Na linha que contém a CMK desejada, clique em **Enable**.

Figura 1-8 Ativação de uma CMK



Passo 5 Na caixa de diálogo exibida, clique em **Yes** para habilitar a CMK.

NOTA

Para ativar várias CMKs ao mesmo tempo, selecione-as e clique em **Enable** no canto superior esquerdo da lista.

----Fim

1.4.3 Desativação de uma ou mais CMKs

Esta seção descreve como usar o console do KMS para desativar uma ou mais CMKs, protegendo assim os dados em casos urgentes.

Depois de desabilitada, uma CMK não pode ser usada para criptografar ou descriptografar nenhum dado. Antes de usar uma CMK desativada para criptografar ou descriptografar dados, você deve ativá-la seguindo as instruções em **Ativação de uma ou mais CMKs**.

Pré-requisitos

- Você obteve uma conta e sua senha para fazer logon no console de gerenciamento.
- A CMK que você deseja desativar está no status **Enabled**.

Restrições

- As chaves mestras padrão criadas pelo KMS não podem ser desabilitadas.
- Uma CMK desativada ainda é faturável. Ele deixará de incorrer em cobranças se for excluído.

Procedimento

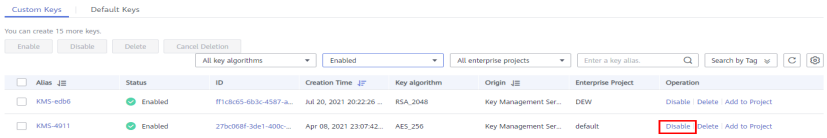
Passo 1 **Faça logon no console de gerenciamento.**

Passo 2 Clique em  no canto superior esquerdo do console de gerenciamento e selecione uma região ou um projeto.

Passo 3 Clicar em  . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 Na linha que contém a CMK desejada, clique em **Disable**.

Figura 1-9 Desativar uma CMK



Passo 5 Na caixa de diálogo exibida, selecione **I understand the impact of disabling keys** e clique em **Yes**.

> **NOTA**
>
> Para desabilitar várias CMKs por vez, selecione-as e clique em **Disable** no canto superior esquerdo da lista.

----Fim

1.4.4 Agendamento da exclusão de uma ou mais CMKs

Antes de excluir a CMK, confirme se ela não está em uso e não será usada. você pode verificar o uso da chave em logs de auditoria.

Pré-requisitos

- Você obteve uma conta e sua senha para fazer logon no console de gerenciamento.
- A CMK para a qual você deseja agendar a exclusão está no status **Enabled** ou **Disabled**.

Restrições

- Uma chave não será excluída até que seu período de exclusão agendado expire. Você pode definir o período para um valor dentro do intervalo de 7 a 1096 dias. Antes da data de exclusão especificada, você pode cancelar a exclusão se quiser usar a CMK. Assim que a exclusão entrar em vigor, a CMK será excluída permanentemente e você não poderá descriptografar os dados criptografados por ela. Portanto, é aconselhável ter cuidado ao realizar esta operação.
- As chaves mestras padrão criadas pelo KMS não podem ser agendadas para exclusão.
- Uma CMK com status de exclusão pendente não incorre em cobranças. Se você cancelar a exclusão, a cobrança será retomada a partir do momento em que a CMK foi programada para ser excluída.

Procedimento

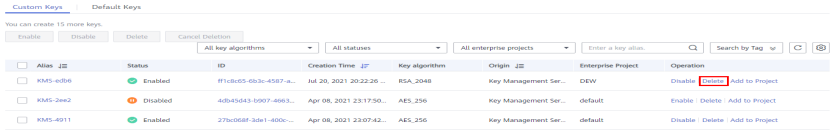
Passo 1 **Faça logon no console de gerenciamento.**

Passo 2 Clique em  no canto superior esquerdo do console de gerenciamento e selecione uma região ou um projeto.

Passo 3 Clicar em  . Escolha **Security & Compliance** > **Data Encryption Workshop**.

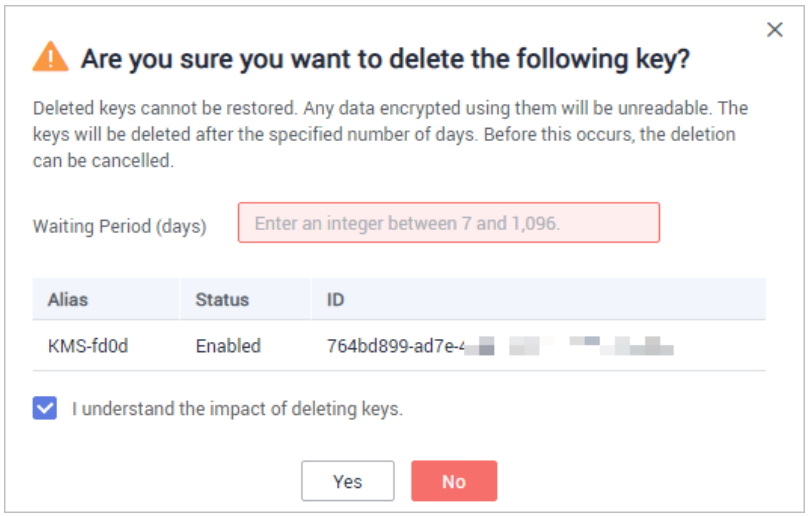
Passo 4 Na linha que contém a CMK desejada, clique em **Delete**.

Figura 1-10 Agendamento da exclusão de uma CMK



Passo 5 Na caixa de diálogo exibida, insira o número de dias após os quais você deseja que a exclusão entre em vigor.

Figura 1-11 Inserir o período após o qual você deseja que a exclusão entre em vigor



Passo 6 Na caixa de diálogo que é exibida, selecione **I understand the impact of deleting keys** e clique em **Yes**.

NOTA

Para agendar a exclusão de várias CMKs por vez, selecione-as e clique em **Delete** no canto superior esquerdo da lista.

----Fim

1.4.5 Cancelamento da exclusão programada de uma ou mais CMKs

Esta seção descreve como usar o console do KMS para cancelar a exclusão programada de uma ou mais CMKs antes da execução da exclusão. Após o cancelamento, a CMK está no status **Disabled**.

Pré-requisitos

- Você obteve uma conta e sua senha para fazer logon no console de gerenciamento.
- A CMK para a qual você deseja cancelar a exclusão programada está no status de **Pending deletion**.

Procedimento

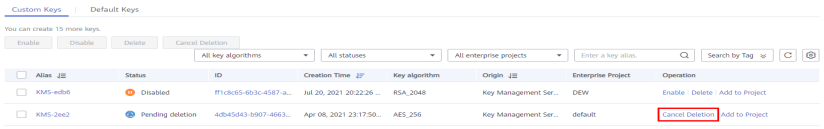
Passo 1 **Faça logon no console de gerenciamento.**

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou um projeto.

Passo 3 Clicar em . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 Na linha que contém a CMK desejada, clique em **Cancel Deletion**.

Figura 1-12 Cancelar a exclusão programada de uma CMK



Passo 5 Na caixa de diálogo exibida, clique em **Yes** para cancelar a exclusão agendada.

NOTA

Para cancelar a exclusão de várias CMKs por vez, selecione-as e clique em **Cancel Deletion** no canto superior esquerdo da lista.

----Fim

1.4.6 Adição de uma chave a um projeto

Você pode alocar chaves para projetos empresariais no console do KMS.

Pré-requisitos

Você obteve uma conta e sua senha para fazer logon no console de gerenciamento.

NOTA

O projeto empresarial de chaves mestras padrão não pode ser alterado.

Procedimento

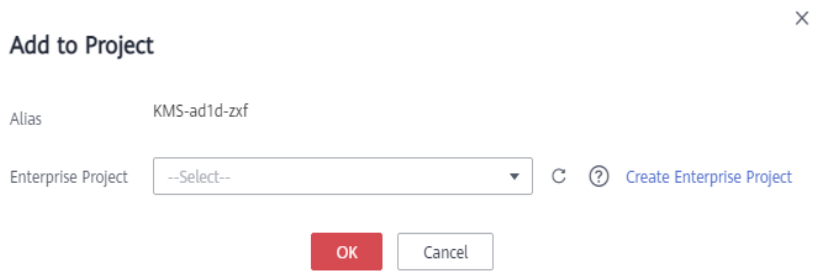
Passo 1 **Faça logon no console de gerenciamento.**

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou um projeto.

Passo 3 Clicar em . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 Na linha que contém a chave de destino, clique em **Add to Project**.

Figura 1-13 Adicionar uma chave a um projeto



Passo 5 Selecionar um projeto.

Passo 6 Clique em **OK**.

----Fim

1.5 Usar a ferramenta on-line para criptografar e descriptografar dados de tamanho pequeno

Esta seção descreve como usar a ferramenta on-line para criptografar ou descriptografar dados de tamanho pequeno (4 KB ou menos) no console do KMS.

Pré-requisitos

- Você obteve uma conta e sua senha para fazer logon no console de gerenciamento.

Restrições

- As chaves mestras padrão não podem ser usadas para criptografar ou descriptografar esses dados com a ferramenta.
- Você pode chamar uma API para usar uma chave mestra padrão para criptografar ou descriptografar pequenos volumes de dados. Para obter detalhes, consulte a *Referência de API do Data Encryption Workshop*.
- Use a CMK atual para criptografar os dados.
- Tenha cuidado ao excluir uma CMK. A ferramenta on-line não pode descriptografar dados se a CMK usada para criptografia tiver sido excluída.

Criptografar dados

Passo 1 **Faça logon no console de gerenciamento.**

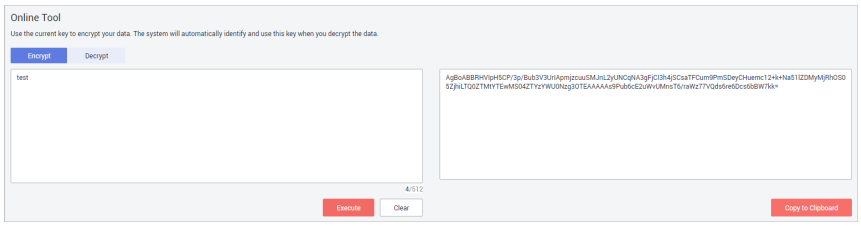
Passo 2 Clique em  no canto superior esquerdo do console de gerenciamento e selecione uma região ou um projeto.

Passo 3 Clicar em  . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 Clique no alias da CMK desejada para visualizar seus detalhes e acesse a ferramenta on-line para criptografia e descriptografia de dados.

Passo 5 Clique em **Encrypt**. Na caixa de texto à esquerda, insira os dados a serem criptografados. Veja **Figura 1-14** para detalhes.

Figura 1-14 Criptografar dados



Passo 6 Clique em **Execute**. Texto cifrado dos dados é exibido na caixa de texto à direita.

NOTA

- Use a CMK atual para criptografar os dados.
- Você pode clicar em **Clear** para limpar os dados inseridos.
- Você pode clicar em **Copy to Clipboard** para copiar o texto cifrado e salvá-lo em um arquivo local.

----Fim

Descriptografar dados

Passo 1 **Faça logon no console de gerenciamento.**

Passo 2 Clicar em ☰. Escolha **Security & Compliance** > **Data Encryption Workshop**.

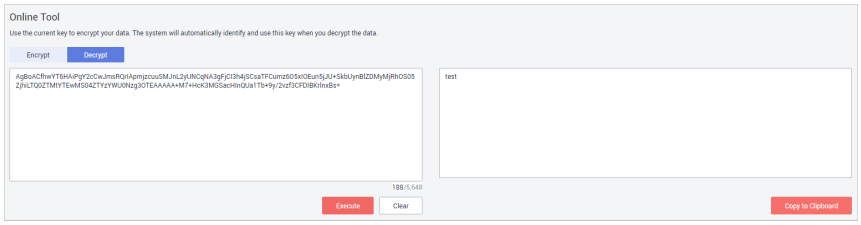
Passo 3 Você pode clicar em qualquer CMK no status **Enabled** para ir para a página de criptografia e descriptografia da ferramenta on-line.

Passo 4 Clique em **Decrypt**. Na caixa de texto à esquerda, insira os dados a serem descriptografados. Veja **Figura 1-15** para detalhes.

NOTA

- A ferramenta irá identificar a criptografia original de CMK e usá-la para descriptografar os dados.
- No entanto, se o CMK tiver sido excluído, a descriptografia falhará.

Figura 1-15 Descriptografar dados



Passo 5 Clique em **Execute**. O texto não criptografado dos dados é exibido na caixa de texto à direita.

NOTA

Você pode clicar em **Copy to Clipboard** para copiar o texto não criptografado e salvá-lo em um arquivo local.

----Fim

1.6 Gerenciamento de tags

1.6.1 Adição de uma tag

As tags são usadas para identificar CMKs. Você pode adicionar tags a CMKs para classificá-las, rastreá-las e coletar seu status de uso de acordo com as tags.

Pré-requisitos

Você obteve uma conta e sua senha para fazer logon no console de gerenciamento.

Restrições

Tags não podem ser adicionadas às chaves mestras padrão.

Procedimento

Passo 1 **Faça logon no console de gerenciamento.**

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou um projeto.

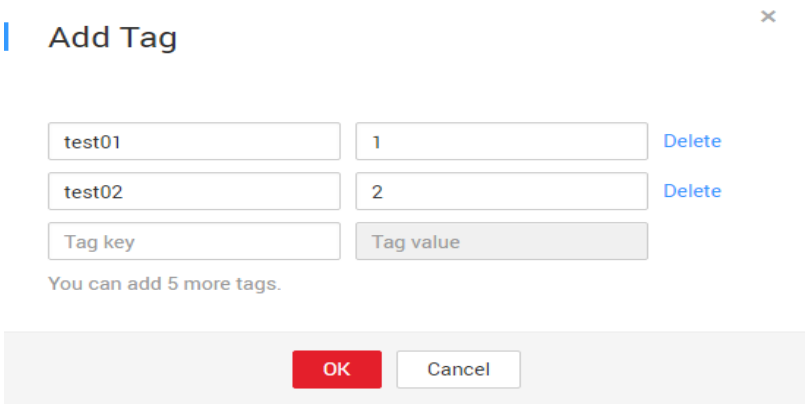
Passo 3 Clicar em . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 Clique no alias da CMK desejada para visualizar seus detalhes.

Passo 5 Clique em **Tags** para ir para a página de gerenciamento de tags.

Passo 6 Clique em **Add Tag**. Na caixa de diálogo **Add Tag**, insira a chave e o valor da tag. **Tabela 1-11** descreve os parâmetros.

Figura 1-16 Adição de uma tag



NOTA

Se quiser excluir uma tag a ser adicionada ao adicionar várias tags, você pode clicar em **Delete** na linha onde a tag a ser adicionada está localizada para excluir a tag.

Tabela 1-11 Parâmetros de tag

Parâmetro	Descrição	Valor	Exemplo de valor
Tag key	Nome de uma tag. A mesma tag (incluindo chave de tag e valor de tag) pode ser usada para diferentes CMKs. No entanto, na mesma CMK, uma chave de tag pode ter apenas um valor de tag. Um máximo de 20 tags podem ser adicionadas para uma CMK.	● Obrigatório. ● Cada chave de tag deve ser exclusiva sob a mesma CMK. ● Limite de 36 caracteres. ● Os seguintes tipos de caracteres são permitidos: – Letras maiúsculas – Letras minúsculas – Dígitos – Caracteres especiais, incluindo hifens (-) e sublinhados (_)	cost
Tag value	Valor da tag	● Este parâmetro pode estar vazio. ● Limite de 43 caracteres. ● Os seguintes tipos de caracteres são permitidos: – Letras maiúsculas – Letras minúsculas – Dígitos – Caracteres especiais, incluindo hifens (-) e sublinhados (_)	100

Passo 7 Clique em **OK** para concluir.

----Fim

1.6.2 Pesquisa de uma CMK por tag

Esta seção descreve como pesquisar uma CMK por tag em um projeto no console do KMS.

Pré-requisitos

- Você obteve uma conta e sua senha para fazer logon no console de gerenciamento.
- As tags foram adicionadas.

Restrições

- Múltiplas tags podem ser adicionadas em uma pesquisa. Um máximo de 20 tags podem ser adicionadas para uma pesquisa. Se várias tags forem pesquisadas ao mesmo tempo, cada CMK no resultado da pesquisa atende aos critérios de pesquisa combinados.

- Se você quiser excluir uma tag adicionada dos critérios de pesquisa, clique em ao lado da tag.
- Você pode clicar em **Reset** para redefinir os critérios de pesquisa.

Procedimento

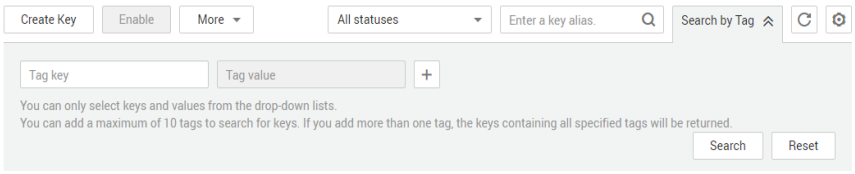
Passo 1 **Faça logon no console de gerenciamento.**

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou um projeto.

Passo 3 Clicar em . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 Clique em **Search by Tag** para mostrar a caixa de pesquisa. **Figura 1-17** descreve os detalhes.

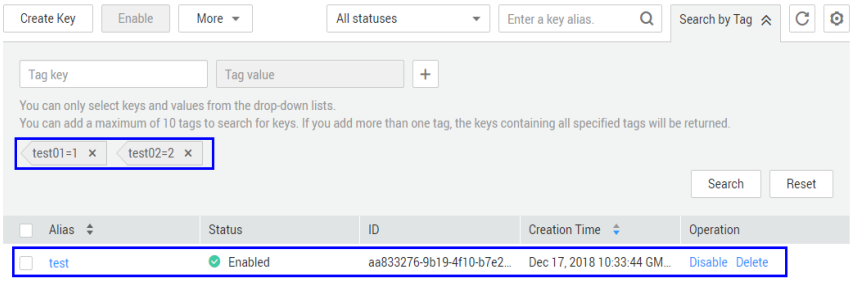
Figura 1-17 Pesquisa de tags



Passo 5 Na caixa de pesquisa, insira ou selecione uma chave de tag e um valor de tag.

Passo 6 Clique em para adicionar a entrada aos critérios de pesquisa e clique em **Search**. A lista exibe as CMKs que atendem aos critérios de pesquisa. Para mais detalhes, consulte **Figura 1-18**.

Figura 1-18 Procurar resultados



NOTA

- Múltiplas tags podem ser adicionadas em uma pesquisa. Um máximo de 20 tags podem ser adicionadas para uma pesquisa. Se várias tags forem pesquisadas ao mesmo tempo, cada CMK no resultado da pesquisa atende aos critérios de pesquisa combinados.
- Se você quiser excluir uma tag adicionada dos critérios de pesquisa, clique em ao lado da tag.
- Você pode clicar em **Reset** para redefinir os critérios de pesquisa.

----Fim

1.6.3 Modificação de valores de tag

Esta seção descreve como modificar valores de tag no console do KMS.

Pré-requisitos

Você obteve uma conta e sua senha para fazer logon no console de gerenciamento.

Procedimento

Passo 1 **Faça logon no console de gerenciamento.**

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou um projeto.

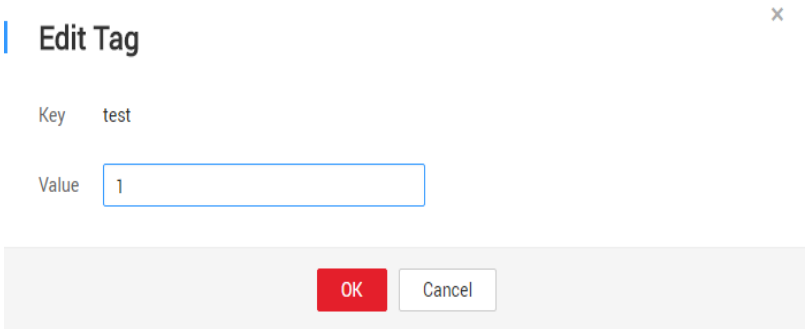
Passo 3 Clicar em . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 Clique no alias da CMK desejada para visualizar seus detalhes.

Passo 5 Clique em **Tags** para ir para a página de gerenciamento de tags.

Passo 6 Clique em **Edit** da tag de destino e a caixa de diálogo **Edit Tag** é exibida.

Figura 1-19 Editar uma tag



Passo 7 Na caixa de diálogo **Edit Tag**, insira um valor de identificador e clique em **OK** para concluir a edição.

----Fim

1.6.4 Exclusão de tags

Esta seção descreve como excluir tags no console do KMS.

Pré-requisitos

Você obteve uma conta e sua senha para fazer logon no console de gerenciamento.

Procedimento

Passo 1 **Faça logon no console de gerenciamento.**

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou um projeto.

Passo 3 Clicar em . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 Clique no alias da CMK desejada para visualizar seus detalhes.

Passo 5 Clique em **Tags** para ir para a página de gerenciamento de tags.

Passo 6 Clique em **Delete** da tag de destino e a caixa de diálogo **Delete Tag** é exibida.

Passo 7 Na caixa de diálogo **Delete Tag**, clique em **Yes** para concluir a exclusão.

----Fim

1.7 Rotação de CMKs

1.7.1 Sobre a rotação de chaves

Finalidade da rotação da chave

As chaves que são amplamente ou repetidamente usadas são inseguras. Para aumentar a segurança das chaves de criptografia, é aconselhável alternar periodicamente as chaves e alterar seus materiais de chave.

Os objetivos da rotação de chaves são:

- Para reduzir a quantidade de dados criptografados por cada chave.

  Uma chave será insegura se for usada para criptografar um grande número de dados. A quantidade de dados criptografados de uma chave refere-se ao número total de bytes ou mensagens criptografadas usando a chave.
- Para melhorar a capacidade de responder a eventos de segurança.

  Em seu projeto inicial de segurança do sistema, você deve projetar a função de rotação de chaves e usá-la para O&M de rotina, para que ela esteja à mão quando ocorrer uma emergência.
- Para melhorar a capacidade de isolamento de dados.

  Os dados de texto cifrado gerados antes e depois da rotação da chave serão isolados. Você pode identificar o escopo de impacto de um evento de segurança com base na chave envolvida e tomar ações de acordo.

Métodos de rotação de chaves

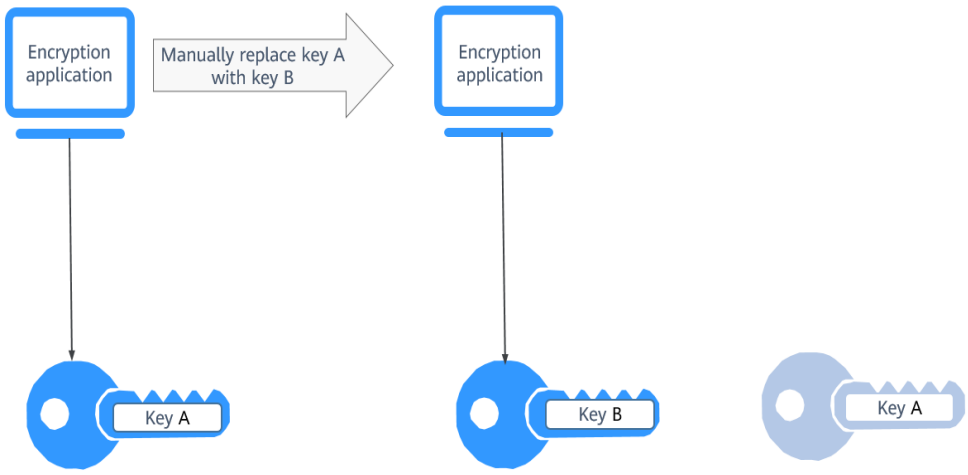
Você pode usar um dos seguintes métodos de rotação de chaves:

- Rotação manual da chave

  Substitua a chave em uso por uma nova chave. Por exemplo, se a chave A estiver em uso, você poderá criar a chave B usando um novo material de criptografia e substituir a chave A pela chave B. Isso alcança o mesmo resultado que alterar o material da chave A.

  Tomemos o OBS como exemplo. Para girar manualmente uma chave, crie uma nova CMK no console do KMS. Substitua a CMK antiga pela nova no console do OBS.

Figura 1-20 Rotação manual da chave



- Rotação automática da chave

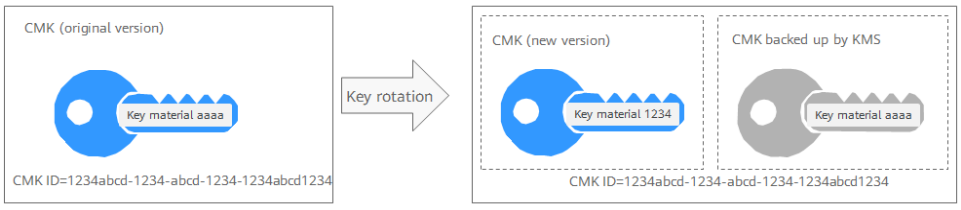
  O KMS gira automaticamente as chaves com base no período de rotação configurado (365 dias por padrão). O sistema gera automaticamente uma nova chave para substituir a chave em uso. A rotação automática da chave altera apenas o material da chave de uma CMK. Os atributos lógicos da CMK não serão alterados, incluindo seu ID de chave, alias, descrição e permissões.

  A rotação automática da chave tem as seguintes características:

  a. Ativar rotação para uma CMK existente. O KMS gerará automaticamente novos materiais de chaves para a CMK.

  b. Os dados não são recriptografados em uma rotação automática de chaves. A DEK gerada usando a CMK não é rotacionada automaticamente, e os dados que foram criptografados usando a CMK não serão criptografados novamente. Se uma DEK tiver vazado, a rotação automática não pode conter o impacto do vazamento.

Figura 1-21 Rotação de chave



NOTA

O KMS mantém todas as versões de uma CMK, para que você possa descriptografar qualquer texto cifrado criptografado usando a CMK.

- O KMS usa a versão mais recente da CMK para criptografar dados.
- Ao descriptografar dados, o KMS usa a versão da CMK usada para criptografar os dados.

Modos de rotação

Tabela 1-12 Modos de rotação de chaves

Tipo de chave	Modo de rotação
Chave mestra padrão	Não pode ser girada.
Chave definida pelo usuário (CMK importada)	Só pode ser girada manualmente. Para obter mais informações sobre chaves definidas pelo usuário, consulte **Visão geral da CMK**.
Chave simétrica	Pode ser girada automaticamente ou manualmente.
Chave assimétrica	Só pode ser girada manualmente.
CMK desabilitada	As CMKs desabilitadas não são rotacionadas. O KMS mantém seu status de rotação inalterado. Depois que uma CMK for ativada, se ela tiver sido usada por mais tempo do que o período de rotação, o KMS girará as chaves imediatamente. Se a CMK tiver sido usada por um período menor que o de rotação, o KMS implementará o plano de rotação original. Para obter mais informações, consulte **Desativação de uma ou mais CMKs**.
As CMKs em estado de exclusão pendente	As CMKs desabilitadas não são rotacionadas. O KMS mantém seu status de rotação inalterado. Depois que uma CMK for ativada, se ela tiver sido usada por mais tempo do que o período de rotação, o KMS girará as chaves imediatamente. Se a CMK tiver sido usada por um período menor que o de rotação, o KMS implementará o plano de rotação original. Para obter mais informações, consulte **Agendamento da exclusão de uma ou mais chaves**.

NOTA

Você pode verificar os detalhes de rotação na página **Rotation Policy**, incluindo o horário da última rotação e o número de rotações.

Preços para rotação de chaves

A ativação da rotação de chaves pode incorrer em taxas adicionais. Para obter detalhes, consulte **Descrição da cobrança**.

1.7.2 Ativação da rotação de chaves

Esta seção descreve como ativar a rotação de uma CMK no console do KMS.

Por padrão, a rotação automática de chaves é desativada para uma CMK. Sempre que você ativa a rotação de chaves, o KMS gira automaticamente as CMKs com base no período de rotação definido.

Pré-requisitos

- Você obteve uma conta e sua senha para fazer logon no console de gerenciamento.
- A CMK está habilitado.
- A **Origin** da CMK é **KMS**.

Restrições

Uma CMK desativada nunca é girada, mesmo que a rotação esteja habilitada para ela.

O KMS retoma a rotação quando esta CMK está ativada. Se você ativar essa CMK após o término de um período de rotação, o KMS irá rodá-la dentro de 24 horas.

Procedimento

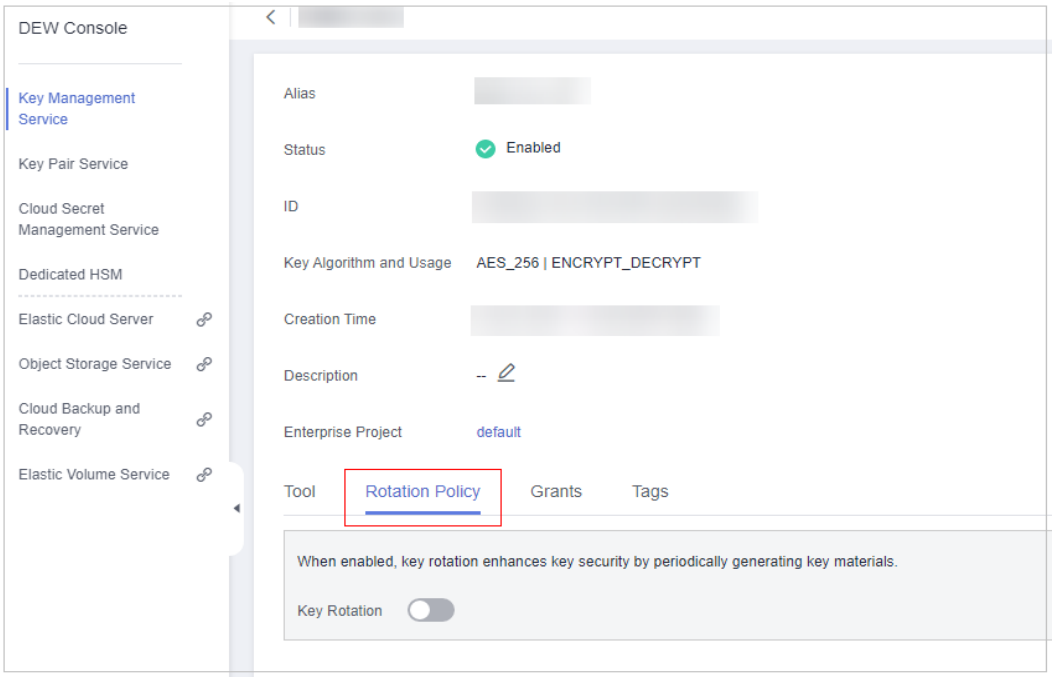
Passo 1 **Faça logon no console de gerenciamento.**

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou um projeto.

Passo 3 Clicar em . Escolha **Security & Compliance** > **Data Encryption Workshop**.

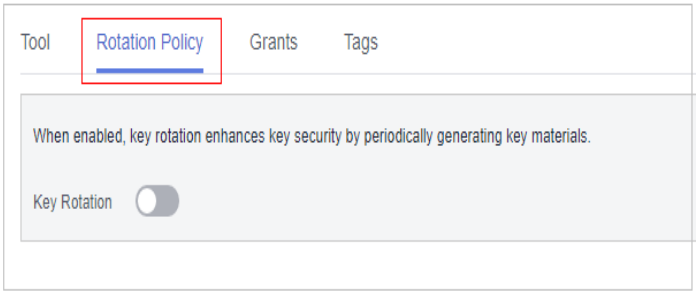
Passo 4 Clique no alias da CMK desejada para visualizar seus detalhes.

Figura 1-22 Detalhes da CMK



Passo 5 Clique na guia **Rotation Policy**. O interruptor de rotação é exibido, como mostrado na **Figura 1-23**.

Figura 1-23 Rotação de CMK



Passo 6 Clique em  para ativar a rotação de chaves.

Passo 7 Configure o período de rotação e clique em **OK**, como mostrado na **Figura 1-24**. Para obter mais informações, consulte **Tabela 1-13**.

Figura 1-24 Ativar a rotação de chaves

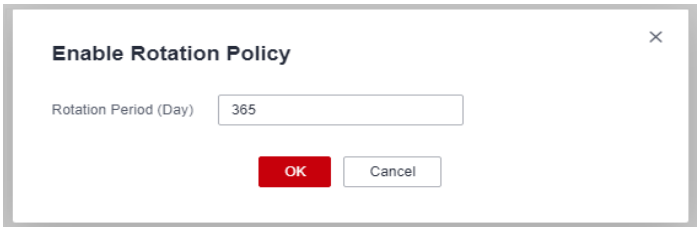
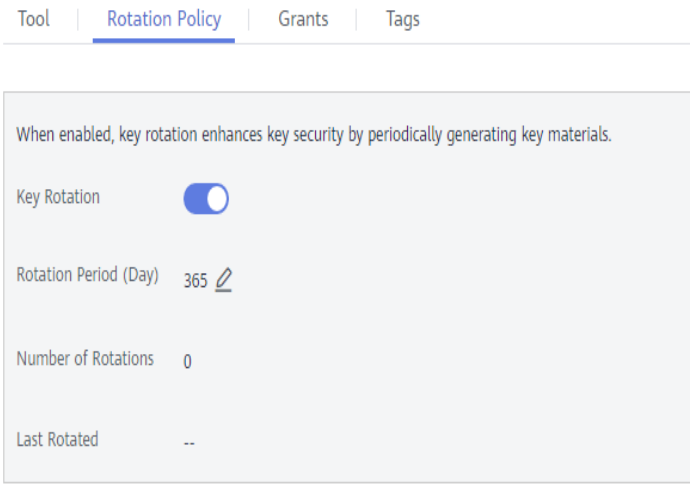


Tabela 1-13 Parâmetros de rotação de chave

Parâmetro	Descrição
Rotação de CMK	Interruptor de rotação. O status padrão é  .  : desativado  : ativado Depois que a rotação estiver ativada, a CMK será girada com base no período definido. **NOTA** Uma CMK desativada nunca é girada, mesmo que a rotação esteja habilitada para ela. O KMS retoma a rotação quando esta CMK está ativada. Se você ativar essa CMK após o término de um período de rotação, o KMS irá rodá-la dentro de 24 horas.
Período de rotação (dia)	Período de rotação (dia). O valor é um número inteiro que varia de 30 a 365. O valor padrão é **365**. Configure o período com base na frequência com que uma CMK é usada. Se for usado com frequência, configure um período curto; caso contrário, defina um longo.

Passo 8 Verifique os detalhes da rotação, como mostrado na figura a seguir.

Figura 1-25 Detalhes da rotação da CMK



NOTA

Você pode clicar em para alterar o período de rotação. Depois que o período é alterado, o KMS gira a CMK pelo novo período.

----Fim

1.7.3 Desativação de rotação de chaves

Esta seção descreve como desativar a rotação de uma chave no console do KMS.

Pré-requisitos

- Você obteve uma conta e sua senha para fazer logon no console de gerenciamento.
- A chave está ativada.
- A **Origin** do CMK é **KMS**.
- A rotação da chave foi ativada.

Procedimento

Passo 1 **Faça logon no console de gerenciamento.**

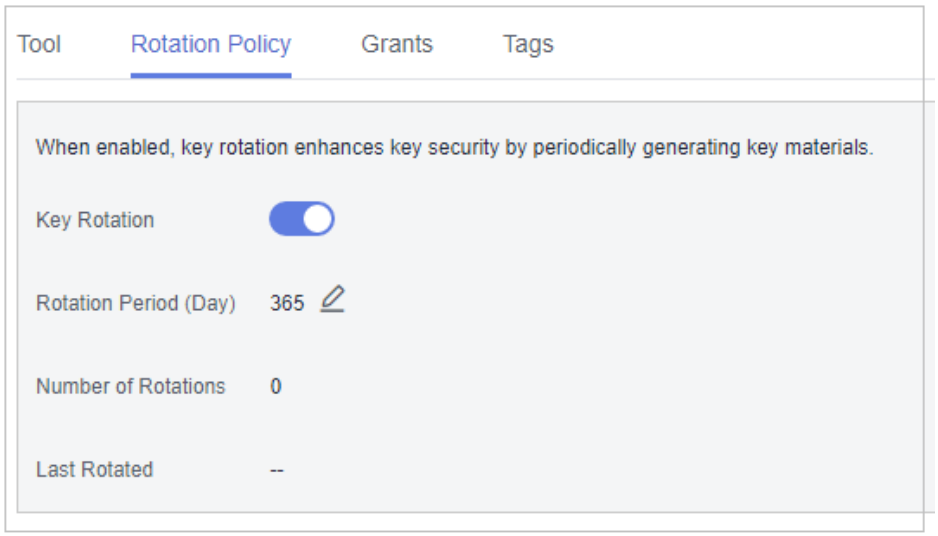
Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou um projeto.

Passo 3 Clicar em . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 Clique no alias de uma chave simétrica.

Passo 5 Clique na guia **Rotation Policy**. O interruptor de rotação é exibido, como mostrado na figura a seguir.

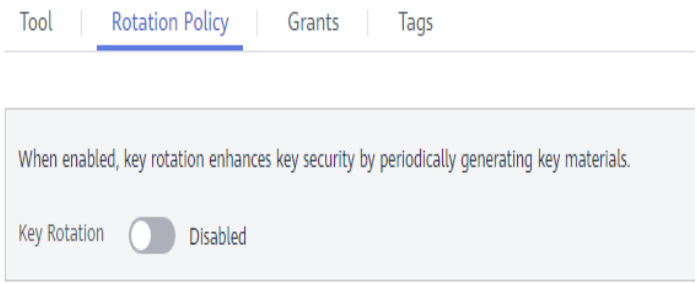
Figura 1-26 Rotação de CMKs



Passo 6 Clique em  para desativar a rotação de chaves.

Passo 7 Verifique o status da rotação, como mostrado em **Figura 1-27**.

Figura 1-27 Desativação de rotação de chaves



----Fim

2 Serviço de gerenciamento de segredo em nuvem

2.1 Criação de um segredo

Esta seção descreve como criar um segredo no console CSMS.

Você pode criar um segredo e armazenar seu valor em sua versão inicial, que é marcada como **SYSCURRENT**.

Pré-requisitos

Você obteve uma conta e sua senha para fazer logon no console de gerenciamento.

Restrições

- Um usuário pode criar no máximo 200 credenciais.
- Por padrão, a chave mestra padrão **csms/default** criada pelo CSMS é usada como a chave mestra de criptografia do segredo atual. Você também pode criar uma chave e usar uma chave de criptografia definida pelo usuário no console do KMS.

Criação de um segredo

Passo 1 **Faça logon no console de gerenciamento.**

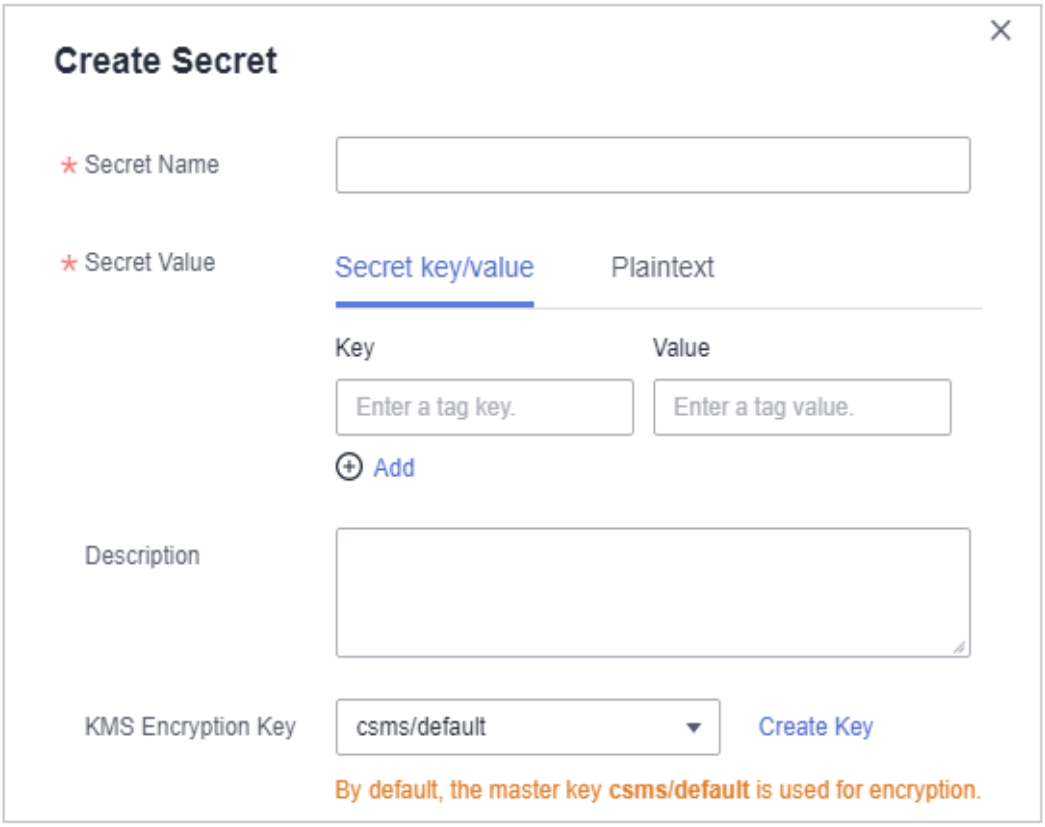
Passo 2 Clique em  no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em  . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 No painel de navegação, escolha **Cloud Secret Management Service**.

Passo 5 Clique em **Create Secret**.

Figura 2-1 Criação de um segredo



Passo 6 Na caixa de diálogo **Create Secret**, insira o nome, o valor, a descrição do segredo e selecione uma chave de criptografia KMS.

- **Secret Name**: insira um nome de segredo.
- **Secret Value**: insira a chave/valor de segredo ou o segredo de texto simples.
- **Description**: digite a descrição de segredo.
- **KMS Encryption Key**: selecione o CMK padrão **csms/default** ou uma chave definida pelo usuário no KMS.

  NOTA

  Por padrão, a chave mestra padrão **csms/default** criada pelo CSMS é usada como a chave mestra de criptografia do segredo atual. Você também pode criar uma chave e usar uma chave de criptografia definida pelo usuário no console do KMS. Para mais detalhes, consulte **Criação de uma CMK**.

Passo 7 Clique em **OK**.

Na lista de segredo, você pode ver os segredos criados. O status padrão de um segredo é **Enabled**.

----Fim

2.2 Gerenciamento de segredos

2.2.1 Visualização de um segredo

Esta seção descreve como verificar nomes de segredos, status e tempo de criação no console do CSMS. O status da credencial pode ser **Enabled** ou **Pending deletion**.

Pré-requisitos

Você obteve uma conta e sua senha para fazer logon no console de gerenciamento.

Procedimento

Passo 1 **Faça logon no console de gerenciamento.**

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 No painel de navegação, escolha **Cloud Secret Management Service**.

Passo 5 Confira a lista de segredo. Para obter mais informações, consulte **Tabela 2-1**.

Figura 2-2 Lista de segredo

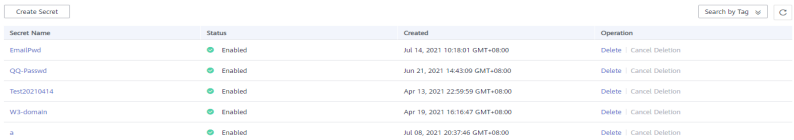
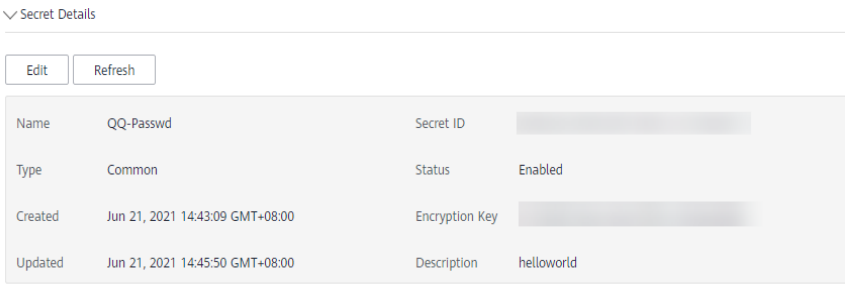


Tabela 2-1 Parâmetros da lista de segredo

Parâmetro	Descrição
Secret Name	Nome de segredo
Status	Estado de segredo. Pode ser: ● **Enabled** O segredo está ativado. ● **Pending deletion** O segredo está à espera de ser excluído.
Created	Momento em que um segredo é criado
Operation	Você pode programar ou cancelar a exclusão de um segredo na coluna **Operation**.

Passo 6 Clique em um segredo para ver seus detalhes. Consulte **Figura 2-3**.

Figura 2-3 Detalhes de segredo



NOTA

- Você pode clicar em **Edit** para modificar a chave de criptografia e a descrição de um segredo.
- Você pode clicar em **Refresh** para atualizar informações de segredo.

----Fim

2.2.2 Exclusão de um segredo

Antes de excluir um segredo, confirme se ele não está em uso e não será usado.

Pré-requisitos

- Você obteve uma conta e sua senha para fazer logon no console de gerenciamento.
- O segredo a ser excluído está no estado **Enabled**.

Restrições

- Um segredo não será excluído até que o período de exclusão agendado expire. Você pode definir o período para um valor dentro do intervalo de 7 a 30 dias. Antes da data de exclusão especificada, você pode cancelar a exclusão se quiser usar o segredo. Se o período de exclusão agendado de um segredo expirar, o segredo será excluído e não poderá ser restaurado.
- Se você optar por excluir um segredo imediatamente, ele não poderá ser restaurado. Tenha cuidado ao realizar esta operação.

Procedimento

Passo 1 **Faça logon no console de gerenciamento.**

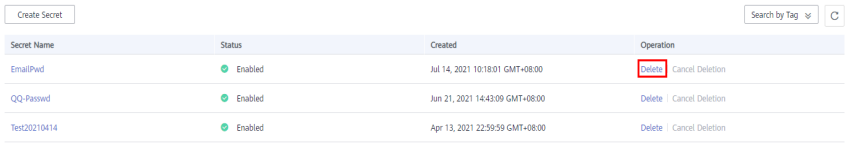
Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 No painel de navegação, escolha **Cloud Secret Management Service**.

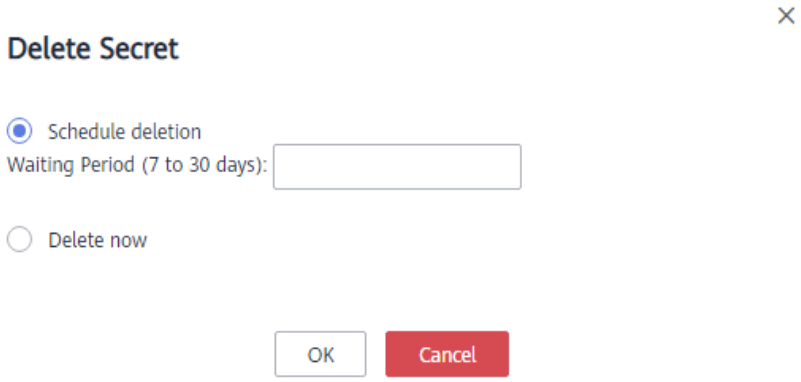
Passo 5 Na linha de um segredo, clique em **Delete**.

Figura 2-4 Excluir um segredo



Passo 6 Na caixa de diálogo exibida, clique em **Schedule deletion** ou **Delete now**.

Figura 2-5 Excluir um segredo



Passo 7 Clique em **OK**.

NOTA

- Um segredo não será excluído até que o período de exclusão agendado expire. Você pode definir o período para um valor dentro do intervalo de 7 a 30 dias. Antes da data de exclusão especificada, você pode cancelar a exclusão se quiser usar o segredo. Se o período de exclusão agendado de um segredo expirar, o segredo será excluído e não poderá ser restaurado.
- Se você optar por excluir um segredo imediatamente, ele não poderá ser restaurado. Tenha cuidado ao realizar esta operação.

----Fim

2.3 Gerenciamento de versões de segredos

2.3.1 Gerenciamento de valores de segredos

Esta seção descreve como salvar e exibir valores secretos no console do CSMS.

Você pode criar uma nova versão de um segredo para criptografar e manter um novo valor secreto. Por padrão, a versão de segredo mais recente no estado **SYSCURRENT**. A versão anterior está no estado **SYSPREVIOUS**.

Pré-requisitos

Você obteve uma conta e sua senha para fazer logon no console de gerenciamento.

Restrições

- Um segredo pode ter até 20 versões.
- As versões secretas são numeradas v1, v2, v3, e assim por diante, com base em seu tempo de criação.

Procedimento

Passo 1 **Faça logon no console de gerenciamento.**

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

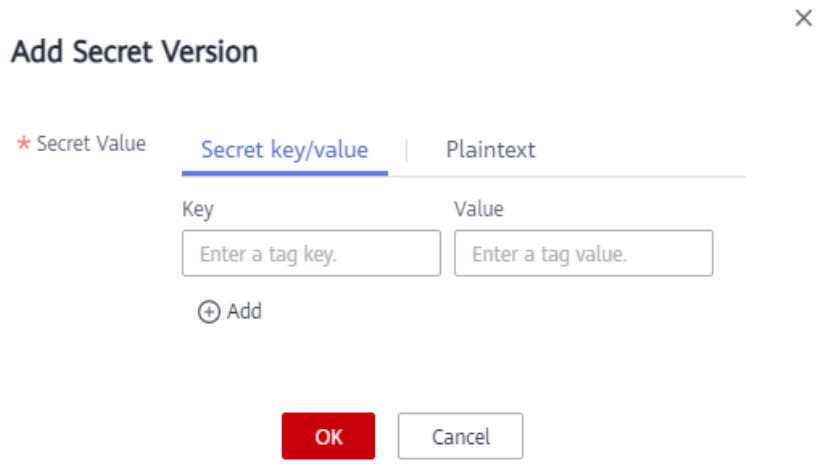
Passo 3 Clique em . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 No painel de navegação, escolha **Cloud Secret Management Service**.

Passo 5 Clique em um nome secreto para ir para a página de detalhes.

Passo 6 Na área **Version List**, clique em **Add Secret Version**. Configure a chave de segredo e o valor na caixa de diálogo exibida.

Figura 2-6 Adicionar um valor de segredo

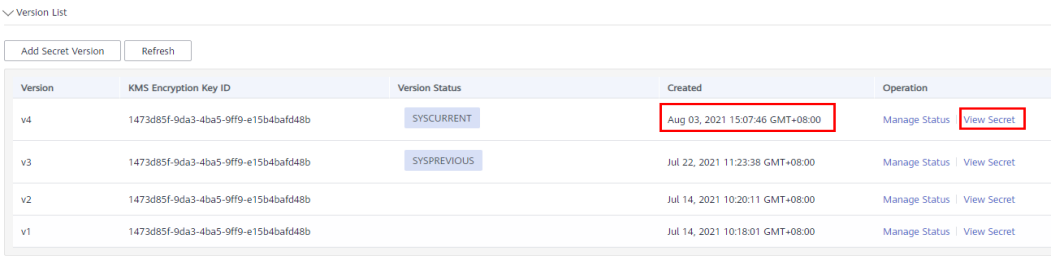


Passo 7 Clique em **OK**. Uma mensagem é exibida no canto superior direito da página, indicando que o valor foi adicionado com sucesso.

Veja o valor de segredo mais recente na lista de versões secretas.

Passo 8 Na área **Version List**, clique em **View Secret** na coluna **Operation** de um segredo.

Figura 2-7 Lista de versões de segredos



Passo 9 Na caixa de diálogo **View Secret**, clique em **Yes**.

NOTA

Os valores secretos geralmente são obtidos por meio de APIs. Verificar os valores no console incorre em riscos de segurança.

Passo 10 Visualize o valor de segredo e clique em **OK**.

----Fim

2.3.2 Gerenciamento de status de versão de segredo

Esta seção descreve como adicionar, alterar e excluir status de versão de segredo.

Valores de segredo são criptografados e armazenados em versões de segredo. Uma versão pode ter vários status. Versões sem nenhum status são consideradas obsoletas e podem ser automaticamente excluídas pelo CSMS.

Pré-requisitos

Você obteve uma conta e sua senha para fazer logon no console de gerenciamento.

Restrições

- A versão inicial é marcada pela tag de status **SYSCURRENT**.
- Você pode marcar uma versão com tags pré-configuradas ou definidas pelo usuário. Uma versão pode ter várias tags de status, mas uma tag de status pode ser usada para apenas uma versão. Por exemplo, se você adicionar a tag de status usada pela versão A à versão B, a tag será movida da versão A para a versão B.
- Um segredo pode ter até 12 status de versão. Um status pode ser usado para apenas uma versão.
- **SYSCURRENT** e **SYSPREVIOUS** são status pré-configurados e não podem ser excluídos.

Procedimento

Passo 1 **Faça logon no console de gerenciamento.**

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

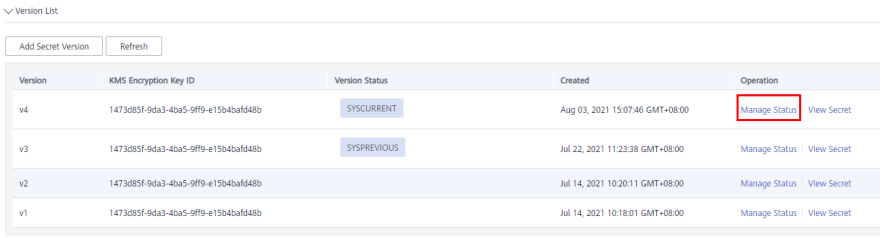
Passo 3 Clique em . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 No painel de navegação, escolha **Cloud Secret Management Service**.

Passo 5 Clique em um nome de segredo para ir para a página de detalhes.

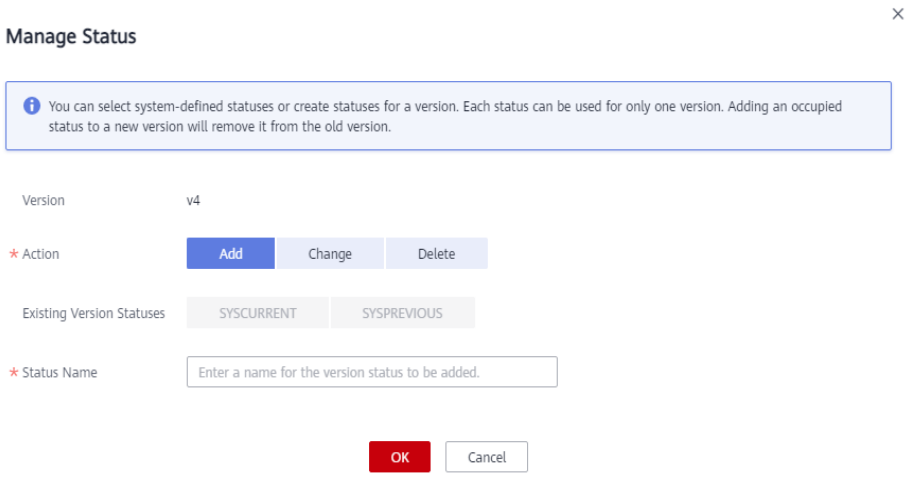
Passo 6 Na área **Version List**, clique em **Manage Status** na coluna **Operation**.

Figura 2-8 Lista de versões de segredo



Passo 7 Na caixa de diálogo **Manage Status**, adicione, altere ou exclua o status de uma versão de segredo.

Figura 2-9 Gerenciamento de status



- Adicionar um status de versão

  Na caixa de diálogo **Manage Status**, clique em **Add** e insira um nome de status. Clique em **OK**.

  NOTA

  Um segredo pode ter até 12 status de versão. Um status pode ser usado para apenas uma versão.

- Atualizar o status da versão de um segredo

  Na caixa de diálogo **Manage Status**, clique em **Change** e selecione um status de versão existente. Clique em **OK**.

- Excluir o status da versão de um segredo

  Na caixa de diálogo **Manage Status**, clique em **Delete** e selecione um status de versão. Clique em **OK**.

  NOTA

  SYSCURRENT e **SYSPREVIOUS** são status pré-configurados e não podem ser excluídos.

----Fim

2.4 Gerenciamento de tags

2.4.1 Adição de uma tag

As tags são usadas para identificar segredos. Você pode facilmente classificar e rastrear segredos usando tags.

Pré-requisitos

Você obteve uma conta e sua senha para fazer logon no console de gerenciamento.

Procedimento

Passo 1 **Faça logon no console de gerenciamento.**

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

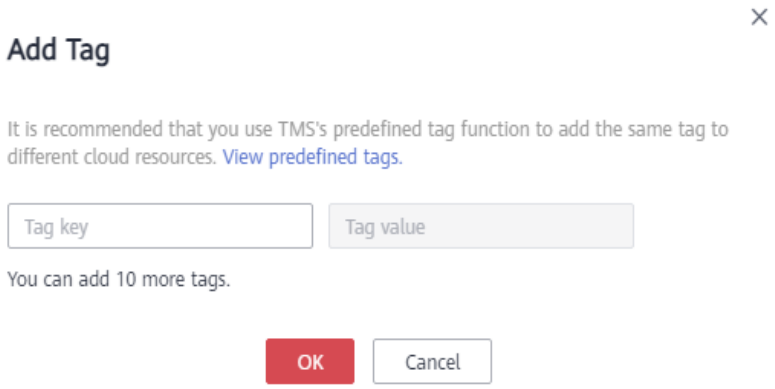
Passo 3 Clique em . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 No painel de navegação, escolha **Cloud Secret Management Service**.

Passo 5 Clique em um nome secreto para ir para a página de detalhes.

Passo 6 Na área **Tags**, clique em **Add Tag**. Na caixa de diálogo **Add Tag**, insira a chave e o valor da tag. **Tabela 2-2** descreve os parâmetros.

Figura 2-10 Adicionar uma tag.



NOTA

- Se quiser usar a mesma tag para identificar vários recursos de nuvem, você pode criar tags predefinidas no TMS. Desta forma, a mesma tag pode ser selecionada para todos os serviços. Para obter mais informações sobre tags predefinidas, consulte o *Guia de usuário do Tag Management Service*.
- Para excluir uma tag, clique em **Delete** ao lado dela.

Tabela 2-2 Parâmetros de tag

Parâmetro	Descrição	Observações
Tag key	Nome da tag. As chaves de tag de um segredo não podem ter valores duplicados. Uma chave de tag pode ser usada para vários segredos. Um segredo pode ter até 10 tags.	● Obrigatório. ● As chaves de tag de um segredo não podem ter valores duplicados. ● Limite de 36 caracteres. ● Os seguintes tipos de caracteres são permitidos: – Letras maiúsculas – Letras minúsculas – Números – Caracteres especiais, incluindo hifens (-) e sublinhados (_) – Caracteres chineses
Tag value	Valor da tag	● Opcional ● Limite de 43 caracteres. ● Os seguintes tipos de caracteres são permitidos: – Letras maiúsculas – Letras minúsculas – Números – Caracteres especiais, incluindo hifens (-) e sublinhados (_) – Caracteres chineses

Passo 7 Clique em **OK**.

----Fim

2.4.2 Procura de um segredo por tag

Esta seção descreve como pesquisar um segredo por tag em um projeto no console do CSMS.

Pré-requisitos

- Você obteve uma conta e sua senha para fazer logon no console de gerenciamento.
- As tags foram adicionadas.

Procedimento

Passo 1 **Faça logon no console de gerenciamento.**

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 No painel de navegação, escolha **Cloud Secret Management Service**.

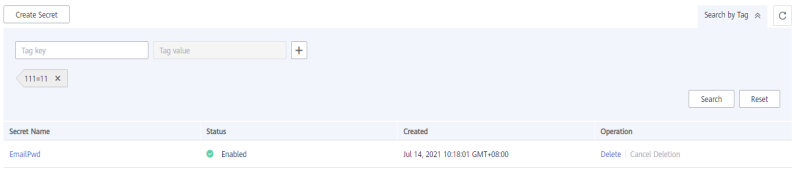
Passo 5 Clique em **Search by Tag** para mostrar a caixa de pesquisa.

Figura 2-11 Caixa de pesquisa

Passo 6 Na caixa de pesquisa, insira ou selecione uma chave de tag e um valor de tag.

Passo 7 Clique em para adicionar a entrada aos critérios de pesquisa e clique em **Search**.

Figura 2-12 Resultado da pesquisa



NOTA

- Várias tags podem ser adicionadas para uma pesquisa. Um máximo de 10 tags podem ser adicionadas para uma pesquisa. Cada resultado de pesquisa atende a todos os critérios de pesquisa.
- Para excluir uma tag dos critérios de pesquisa, clique em ao lado da tag.
- Você pode clicar em **Reset** para redefinir os critérios de pesquisa.

----Fim

2.4.3 Modificação de um valor de tag

Esta seção descreve como modificar valores de tag no console do CSMS.

Pré-requisitos

Você obteve uma conta e sua senha para fazer logon no console de gerenciamento.

Procedimento

Passo 1 **Faça logon no console de gerenciamento.**

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

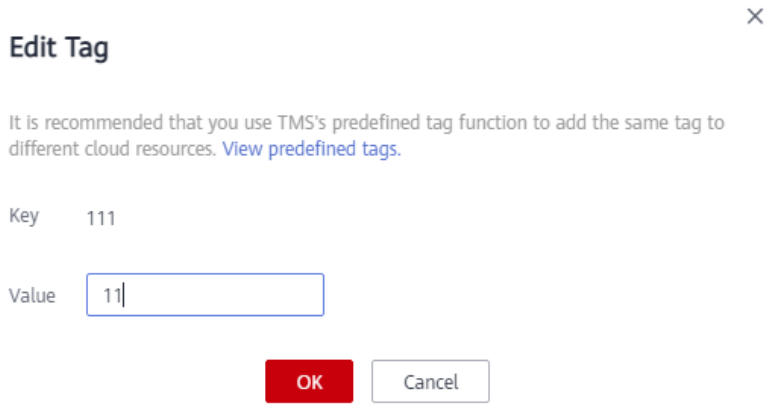
Passo 3 Clique em . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 No painel de navegação, escolha **Cloud Secret Management Service**.

Passo 5 Clique em um nome de segredo para ir para a página de detalhes.

Passo 6 Na área **Tags**, clique em **Edit**.

Figura 2-13 Editar uma tag



Passo 7 Na caixa de diálogo **Edit Tag**, insira um valor de tag e clique em **OK**.

----Fim

2.4.4 Exclusão de uma tag

Esta seção descreve como excluir tags no console do CSMS.

Pré-requisitos

Você obteve uma conta e sua senha para fazer logon no console de gerenciamento.

Procedimento

Passo 1 **Faça logon no console de gerenciamento.**

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

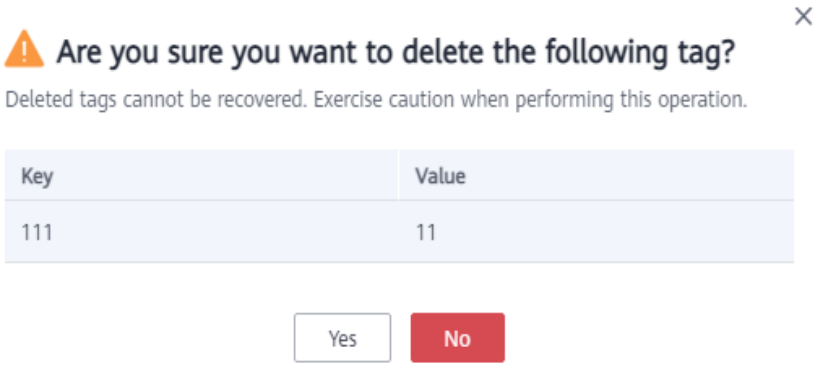
Passo 3 Clique em . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 No painel de navegação, escolha **Cloud Secret Management Service**.

Passo 5 Clique em um nome de segredo para ir para a página de detalhes.

Passo 6 Na área **Tags**, clique em **Delete**.

Figura 2-14 Excluir uma tag



Passo 7 Na caixa de diálogo **Delete Tag**, clique em **Yes**.

----Fim

3 Serviço de par de chaves

3.1 Criação de um par de chaves

Para fins de segurança do sistema, é recomendável usar o modo de autenticação de par de chaves para autenticar o usuário que tenta fazer logon em um ECS.

Você pode criar um par de chaves e usá-lo para autenticação ao fazer logon no ECS.

NOTA

Se você já criou um par de chaves, não precisa criar novamente.

Você pode criar um par de chaves usando um dos seguintes métodos:

- Criação de um par de chaves no console de gerenciamento

  A chave pública é salva automaticamente na HUAWEI CLOUD. A chave privada pode ser baixada e salva em seu host local. Você também pode salvar suas chaves privadas na HUAWEI CLOUD e gerenciá-las com o KPS com base em suas necessidades. A HUAWEI CLOUD usa chaves de criptografia fornecidas pelo KMS para criptografar suas chaves privadas para garantir armazenamento e acesso seguros. Para mais detalhes, consulte **Criação de um par de chaves no console de gerenciamento**.

  NOTA

  - O par de chaves criado no console de gerenciamento usa o algoritmo de criptografia e descriptografia **SSH-2 (RSA, 2048)**.
  - Os pares de chaves criados por um usuário do IAM no console de gerenciamento podem ser usados apenas pelo usuário. Se vários usuários do IAM precisarem usar o mesmo par de chaves, você poderá criar um par de chaves de conta.

- Criação de um par de chaves usando a ferramenta PuTTYgen

  Tanto a chave pública quanto a chave privada podem ser armazenadas no host local. Para mais detalhes, consulte **Criação de um par de chaves usando o PuTTYgen**.

  NOTA

  PuTTYgen é uma ferramenta para gerar chaves públicas e privadas. Você pode obter a ferramenta de **https://www.putty.org/**.

Pré-requisitos

Você obteve o nome de usuário e a senha para fazer logon no console de gerenciamento e um método de pagamento foi vinculado ao usuário.

Criação de um par de chaves no console de gerenciamento

Passo 1 **Efetue logon no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

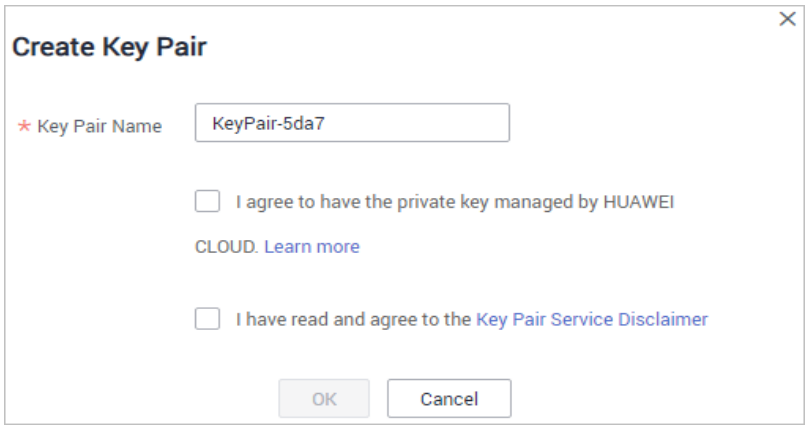
Passo 3 Clique em . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 No painel de navegação à esquerda, clique em **Key Pair Service**.

Passo 5 Clique em **Create Key Pair**.

Passo 6 Na caixa de diálogo **Create Key Pair**, insira um nome para o par de chaves a ser criado.

Figura 3-1 Criação de um par de chaves

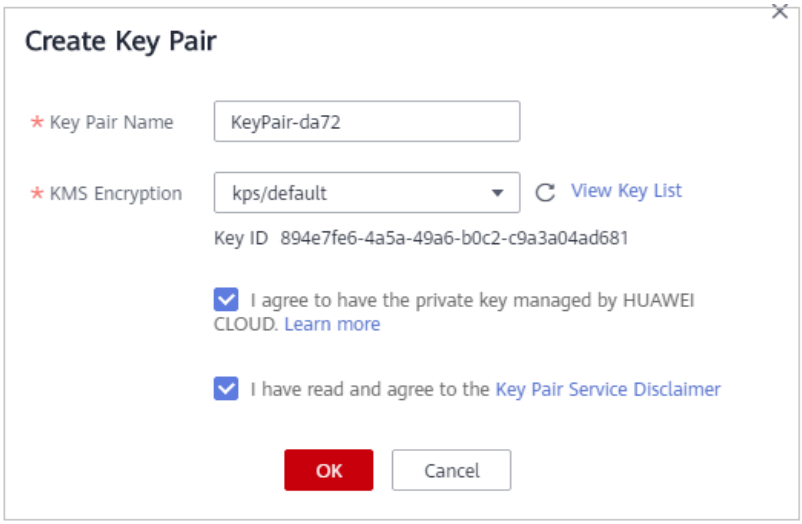


Passo 7 Se você deseja que sua chave privada seja gerenciada pela HUAWEI CLOUD, leia e confirme **I agree to have the private key managed by HUAWEI CLOUD**. Selecione uma chave de criptografia na caixa de listagem suspensa **KMS encryption**. Ignore esta etapa se você não precisar ter a chave privada gerenciada pela HUAWEI CLOUD.

NOTA

- O KPS usa a chave de criptografia fornecida pelo KMS para criptografar chaves privadas. Quando o usuário usa a função de criptografia KMS do par de chaves, o KMS cria automaticamente uma chave mestra padrão **kps/default** para criptografia do par de chaves.
- Ao selecionar uma chave de criptografia, você pode selecionar uma chave de criptografia existente ou clicar em **View Key List** para criar uma chave de criptografia.

Figura 3-2 Gerenciamento de chaves privadas



Passo 8 Leia o *Key Pair Service Disclaimer* e selecione **I have read and agree to the Key Pair Service Disclaimer**.

Passo 9 Clique em **OK**. O navegador baixa automaticamente a chave privada. Quando a chave privada é baixada, uma caixa de diálogo é exibida.

Passo 10 Salve a chave privada conforme solicitado pela caixa de diálogo.

AVISO

- Se a chave privada não for gerenciada pela HUAWEI CLOUD, ela poderá ser baixada apenas uma vez. Mantenha-o corretamente. Se a chave privada for perdida, você poderá vincular um par de chaves ao ECS novamente redefinindo a senha ou o par de chaves. Para obter detalhes, consulte **Como lidar com a falha no logon no ECS após a desvinculação do par de chaves?**
- Se você autorizou a HUAWEI CLOUD a gerenciar a chave privada, poderá exportar a chave privada a qualquer momento, conforme necessário.

Passo 11 Depois que a chave privada for salva, clique em **OK**. O par de chaves foi criado com sucesso.

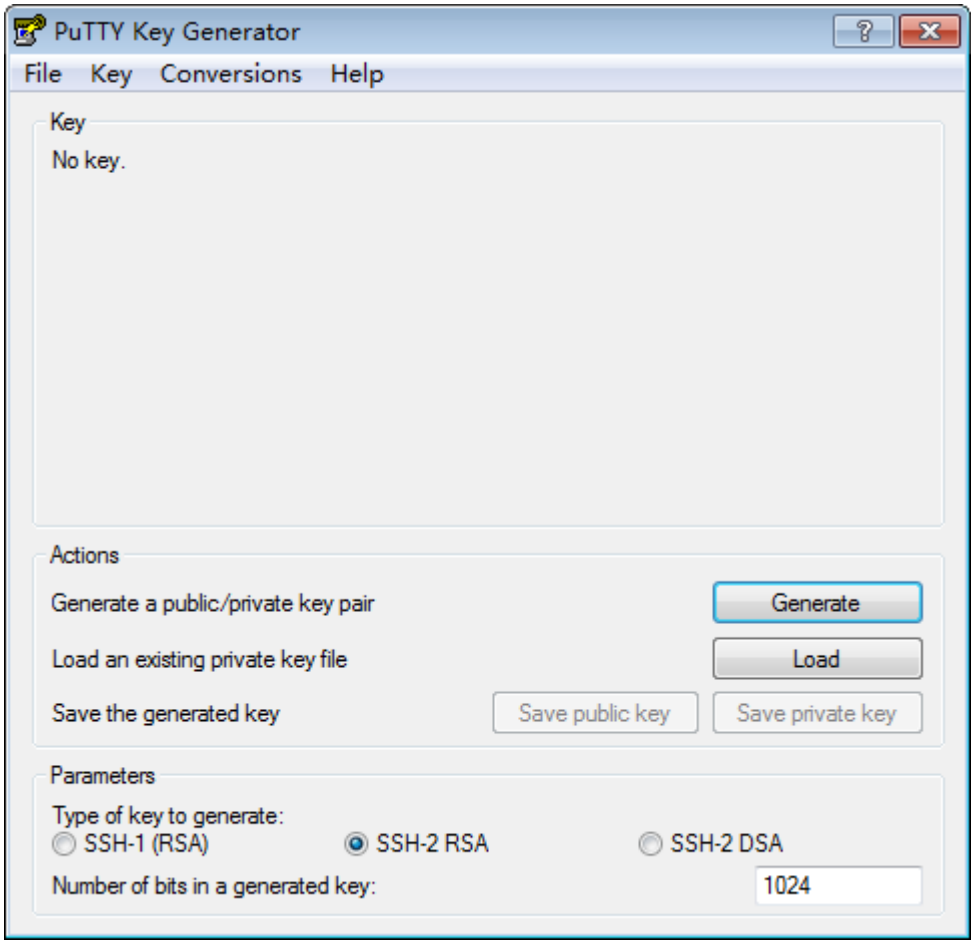
Depois que o par de chaves for criado, você poderá visualizá-lo na lista de pares de chaves. A lista exibe informações como nome do par de chaves, impressão digital, chave privada e quantidade.

----Fim

Criação de um par de chaves usando o PuTTYgen

Passo 1 Gere as chaves pública e privada. Clique duas vezes em **PuTTYgen.exe**. A página **PuTTY Key Generator** é exibida, como mostrado na **Figura 3-3**.

Figura 3-3 Gerador de chaves PuTTY



Passo 2 Configure os parâmetros conforme descrito em **Tabela 3-1**.

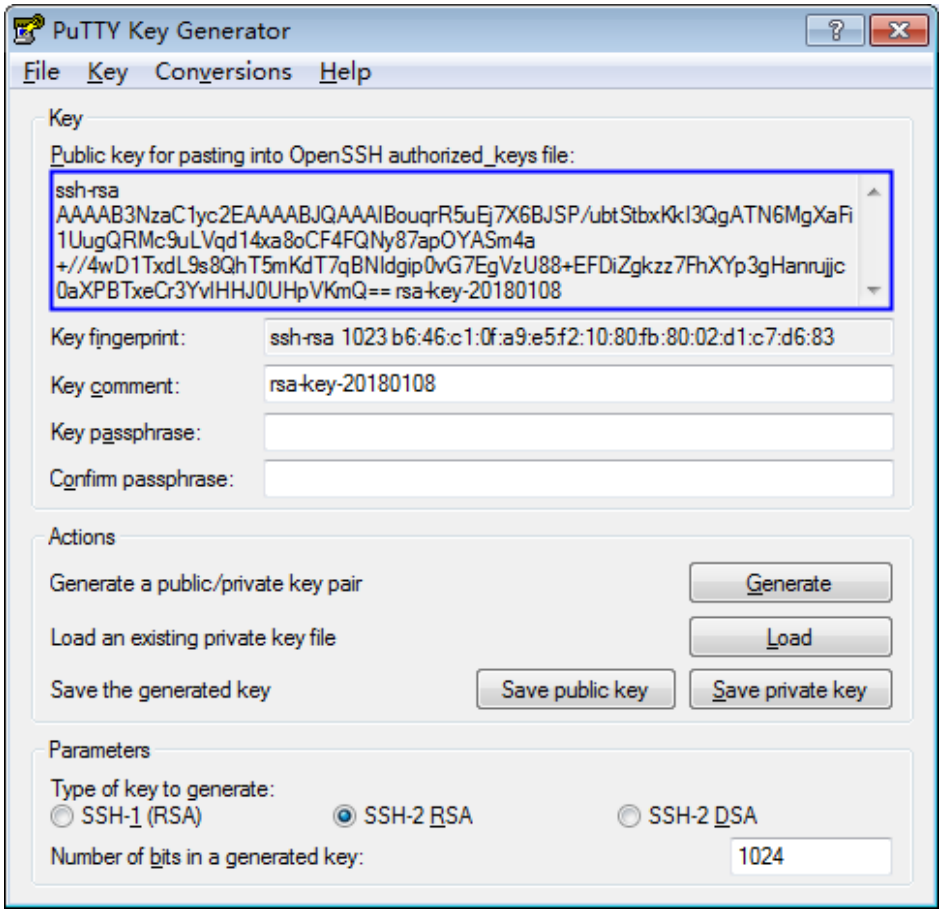
Tabela 3-1 Descrição do parâmetro

Parâmetro	Descrição
Tipo de chave a ser gerada	Algoritmo de criptografia e descriptografia de pares de chaves a importar para o console de gerenciamento. Atualmente, apenas **SSH-2 RSA** é suportado.
Número de bits em uma chave gerada	Comprimento de um par de chaves a ser importado para o console de gerenciamento. Atualmente, os seguintes valores de comprimento são suportados: **1024**, **2048** e **4096**.

Passo 3 Clique em **Generate** para gerar uma chave pública e uma chave privada. Consulte **Figura 3-4**.

O conteúdo destacado pela caixa de linha azul mostra uma chave pública gerada.

Figura 3-4 Obtenção das chaves públicas e privadas



Passo 4 Copie as informações no quadrado azul e salve-as em um arquivo local .txt.

AVISO

Não salve a chave pública clicando em **Save public key**. Salvar uma chave pública clicando em **Save public key** de PuTTYgen alterará o formato do conteúdo da chave pública. Essa chave não pode ser importada para o console de gerenciamento.

Passo 5 Salve a chave privada no formato PPK ou PEM.

AVISO

Por motivos de segurança, a chave privada só pode ser baixada uma vez. Guarde-a em um local seguro.

Tabela 3-2 Formato de um arquivo de chave privada

Formato de arquivo de chave privada	Cenário de utilização de chave privada	Método de salvamento
PEM	● Use a ferramenta Xshell para efetuar logon no servidor de nuvem que executa o sistema operacional de Linux. ● Gerencie a chave privada no console de gerenciamento.	1. Escolha **Conversions** > **Export OpenSSH key**. 2. Salve a chave privada, por exemplo, **kp-123.pem**, em um diretório local.
	Obter a senha de um servidor de nuvem executando o sistema operacional de Windows.	1. Escolha **Conversions** > **Export OpenSSH key**. **NOTA** Não insira as informações da **Key passphrase**. Caso contrário, a senha não será obtida. 2. Salve a chave privada, por exemplo, **kp-123.pem**, em um diretório local.
PPK	Use a ferramenta PuTTY para fazer logon no servidor em nuvem que executa o sistema operacional de Linux.	1. Na página **PuTTY Key Generator**, escolha **File** > **Save private key**. 2. Salve a chave privada, por exemplo, **kp-123.ppk**, em um diretório local.

Depois que a chave pública e a chave privada forem salvas corretamente, você poderá importar o par de chaves para o console de gerenciamento.

----Fim

3.2 Importação de um par de chaves

Se você precisar usar seu próprio par de chaves (por exemplo, usando o par de chaves criado pela ferramenta PuTTYgen) você pode importar a chave pública para o console de gerenciamento e usar sua chave privada para efetuar logon remotamente em um ECS. Você também pode gerenciar a chave privada no console de gerenciamento da HUAWEI CLOUD, conforme necessário.

Se vários usuários do IAM precisarem usar o mesmo par de chaves, use outra ferramenta (como o PuTTYgen) para criar um par de chaves e importá-lo para cada um dos usuários do IAM separadamente.

Pré-requisitos

Os arquivos de chave pública e privada do par de chaves a ser importado estão prontos.

Restrições

- Os algoritmos de criptografia e descriptografia suportados de pares de chaves importados são os seguintes:
  - SSH-2 (RSA, 1024)
  - SSH-2 (RSA, 2048)
  - SSH-2 (RSA, 4096)
- O formato do arquivo de chave privada que pode ser importado é PEM.

  Se o arquivo estiver no formato **.ppk**, converta-o em um arquivo **.pem**. Para obter detalhes, consulte **Como converter o formato de um arquivo de chave privada?**

Procedimento

Passo 1 **Efetue logon no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

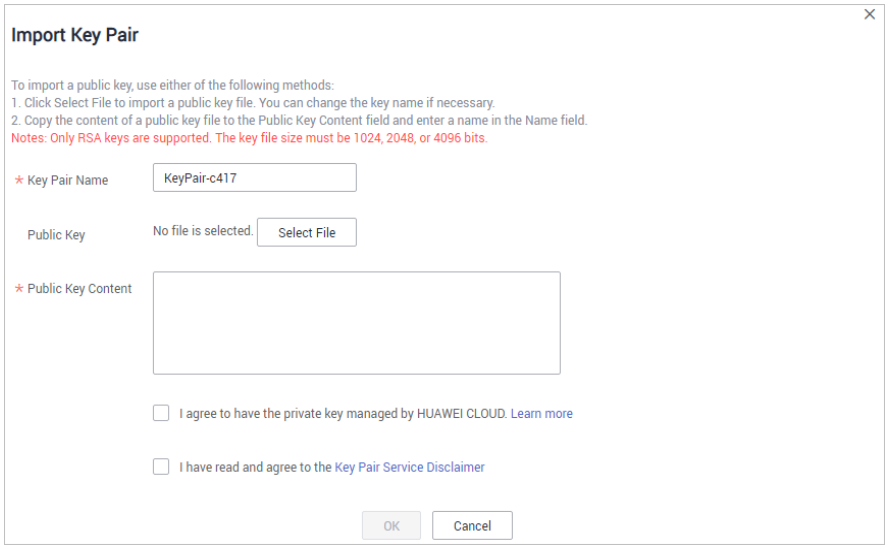
Passo 3 Clique em . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 No painel de navegação à esquerda, clique em **Key Pair Service**.

Passo 5 Clique em **Import Key Pair**.

Passo 6 Na caixa de diálogo **Import Key Pair**, clique em **Select File** e importe um arquivo de chave pública ou copie e cole chaves públicas na caixa de texto **Public Key Content**.

Figura 3-5 Importação de um par de chaves

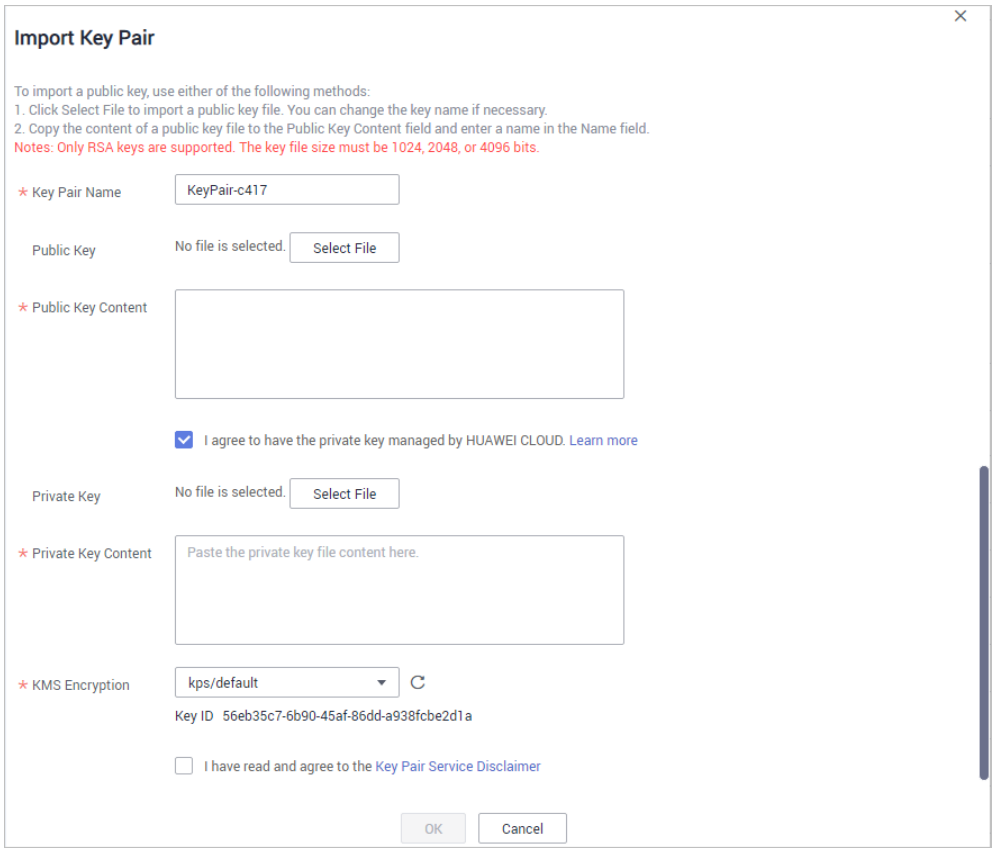


NOTA

Você pode personalizar o nome de um par de chaves importado.

Passo 7 Se você deseja que sua chave privada seja gerenciada pela HUAWEI CLOUD, leia e confirme **I agree to have the private key managed by HUAWEI CLOUD**. Ignore esta etapa se você não precisar ter a chave privada gerenciada pela HUAWEI CLOUD.

Figura 3-6 Hospedagem da chave privada na HUAWEI CLOUD



1. Clique em **Select File**, selecione o arquivo de chave privada **.pem** a ser importado. Como alternativa, você pode copiar e colar o conteúdo da chave privada na caixa de texto **Private Key Content**.
2. Selecione uma chave de criptografia na caixa de listagem suspensa **KMS Encryption**.

   NOTA

   - O KPS usa a chave de criptografia fornecida pelo KMS para criptografar chaves privadas. Quando o usuário usa a função de criptografia KMS do par de chaves, o KMS cria automaticamente uma chave mestra padrão **kps/default** para criptografia do par de chaves.
   - Você pode selecionar uma chave de criptografia existente ou clicar em **View Key List** para criar uma.

Passo 8 Leia o *Key Pair Service Disclaimer* e selecione **I have read and agree to the Key Pair Service Disclaimer**.

Passo 9 Clique em **OK** para importar o par de chaves.

----Fim

3.3 Atualização de um par de chaves

Para permitir que todos os usuários sob sua conta usem seus pares de chaves, você pode atualizar os pares de chaves para pares de chaves de conta.

Pré-requisitos

- Um par de chaves foi criado ou importado.
- O tíquete de serviço para atualização de chave foi tratado.

Restrições

- Os pares de chaves que usam os mesmos nomes que os pares de chaves de conta existentes ou os pares de chaves privadas de outros usuários não podem ser atualizados.

Procedimento

Passo 1 **Faça logon no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

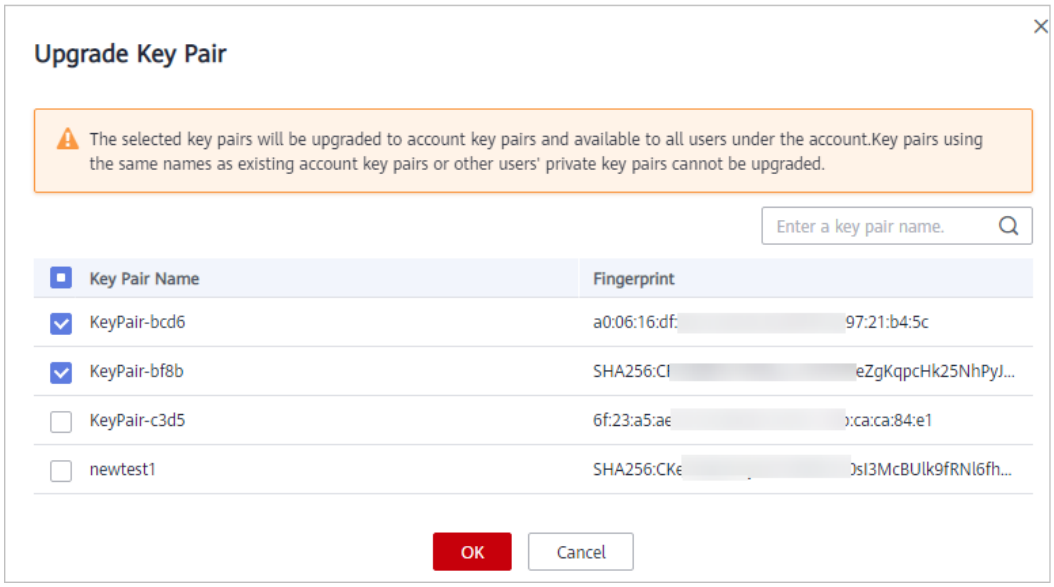
Passo 3 Clique em . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 No painel de navegação à esquerda, clique em **Key Pair Service**.

Passo 5 Clique em **Upgrade Key Pair**.

Passo 6 Na caixa de diálogo exibida, selecione o par de chaves a ser atualizado e clique em **OK**, como mostrado na **Figura 3-7**.

Figura 3-7 Atualização de um par de chaves



NOTA

Os pares de chaves atualizados são exibidos na lista de pares de chaves da conta.

----Fim

3.4 Gerenciamento de pares de chaves

3.4.1 Vinculação de um par de chaves

Se você definir o modo de logon como **Password** ao comprar um ECS que execute o sistema operacional de Linux, poderá vincular um par de chaves ao ECS no console do KPS. O KPS configurará o par de chaves para o ECS e, em seguida, o modo de logon do ECS será alterado para **Key Pair**. Depois que o par de chaves for vinculado, você poderá usar a chave privada para efetuar logon no ECS.

Esta seção descreve como vincular um par de chaves a um ECS no console do KPS.

Pré-requisitos

- O ECS deve estar no estado **Running** ou **Shut down**.
- O ECS não foi vinculado a um par de chaves.
- O ECS cujo par de chaves deve ser redefinido usa a imagem pública fornecida pela HUAWEI CLOUD.
- Para vincular a um par de chaves, você pode escrever a chave pública do usuário no arquivo **/root/.ssh/authorized_keys** no servidor. Certifique-se de que o arquivo não seja modificado antes de vincular ao par de chaves. Caso contrário, a vinculação falhará.

Restrições

- No console de gerenciamento, os pares de chaves não podem ser vinculados a ECSs que executam o sistema operacional de Windows.
- Pares de chaves não podem ser vinculados a imagens públicas executando CoreOS, OpenEuler, FreeBSD (Other), Kylin V10 64-bit, ou UnionTech OS Server 20 Euler 64-bit.

Vinculação de um par de chaves

Passo 1 **Efetue logon no console de gerenciamento**.

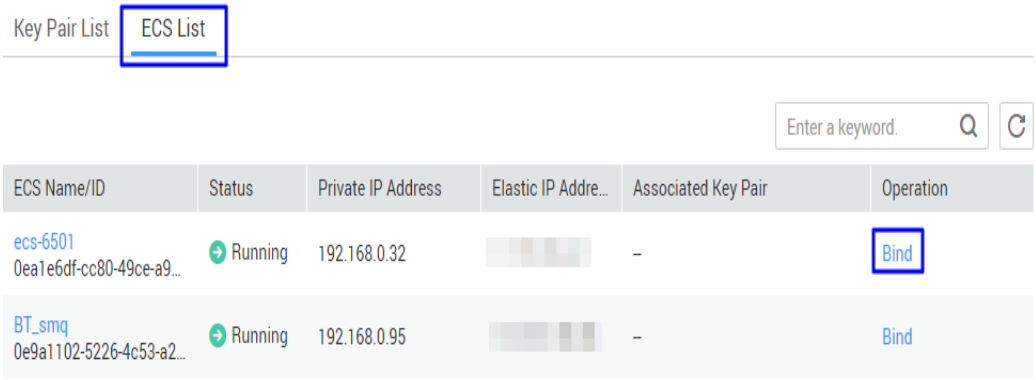
Passo 2 Clique em  no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em  . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 No painel de navegação à esquerda, clique em **Key Pair Service**.

Passo 5 Clique na guia **ECS List**.

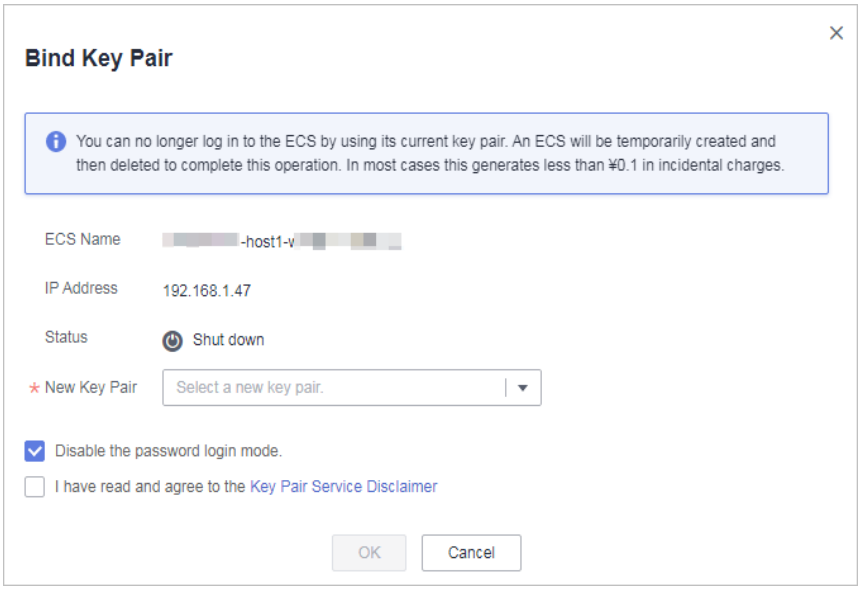
Figura 3-8 Vinculação



Passo 6 Clique em **Bind** na linha de um ECS para abrir a caixa de diálogo **Bind Key Pair**.

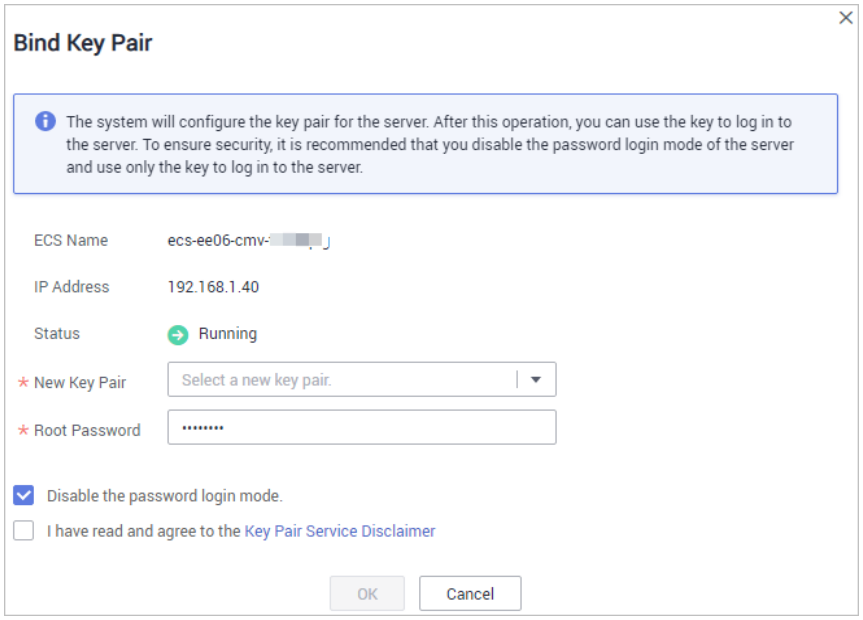
- Se o ECS for desligado, uma caixa de diálogo será exibida, conforme mostrado na **Figura 3-9**.

Figura 3-9 Vinculação de um par de chaves (1)



- Se o ECS estiver em execução, será necessário fornecer a senha raiz. Consulte **Figura 3-10**.

Figura 3-10 Vinculação de um par de chaves (2)



NOTA

- Se você tiver a senha raiz do ECS, poderá inserir diretamente a senha para vincular o par de chaves ao ECS.
- Se você não tiver a senha raiz do ECS, poderá desligar o ECS e vincular o par de chaves quando o ECS estiver no estado de desligamento.

Passo 7 Selecione um novo par de chaves na caixa de listagem suspensa de **New Key Pair**.

Passo 8 Você pode escolher se deseja desativar o modo de logon de senha conforme necessário. Por padrão, o modo de logon de senha está desativado.

NOTA

- Se você não desativar o modo de logon de senha, poderá usar a senha ou o par de chaves para efetuar logon no ECS.
- Se o modo de logon de senha estiver desativado, você poderá usar apenas o par de chaves para efetuar logon no ECS. Se você precisar usar o modo de logon de senha mais tarde, poderá ativar o modo de logon de senha novamente. Para obter detalhes, consulte **Como ativar o modo de logon por senha para um ECS?**

Passo 9 Selecione **I have read and agree to the Key Pair Service Disclaimer**.

Passo 10 Clique em **OK** para concluir a operação.

- Se o ECS não for encerrado, use a senha raiz para vincular o par de chaves. Demora cerca de 30 segundos para ser concluído.
- Se o ECS for encerrado, a operação de vinculação poderá demorar cerca de cinco minutos.

----Fim

3.4.2 Visualização de um par de chaves

Esta seção descreve como exibir as informações do par de chaves, incluindo os nomes, impressões digitais, chaves privadas e chaves usadas na página do KPS do console do DEW.

Pré-requisitos

Você obteve uma conta e sua senha para fazer logon no console de gerenciamento.

Procedimento

Passo 1 **Efetue logon no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 No painel de navegação à esquerda, clique em **Key Pair Service**.

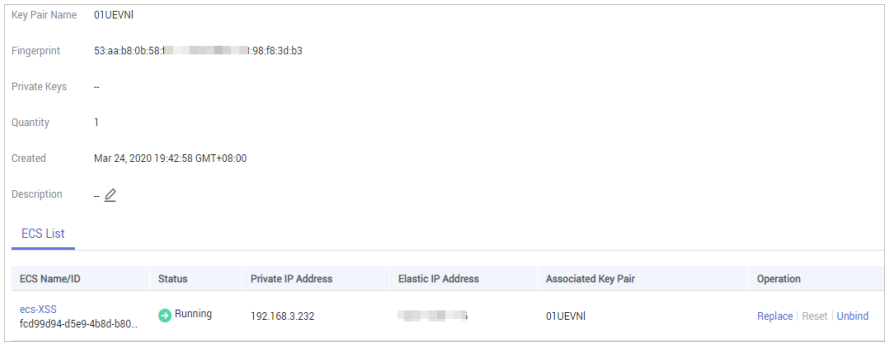
Passo 5 Verifique as informações do par de chaves na lista.

NOTA

A lista descreve os nomes, impressões digitais, chaves privadas e status de pares de chaves.

Passo 6 Clique no nome do par de chaves de destino. As informações detalhadas sobre o par de chaves e a lista de ECSs que usam o par de chaves são exibidas. Veja **Figura 3-11** para detalhes.

Figura 3-11 Detalhes do par de chaves



NOTA

Ao adquirir um ECS, escolha o método de logon usando um par de chaves. Em seguida, o par de chaves será vinculado ao ECS após a compra do ECS.

Vincular um par de chaves a ECSs. Para obter detalhes sobre os parâmetros, consulte **Tabela 3-3**.

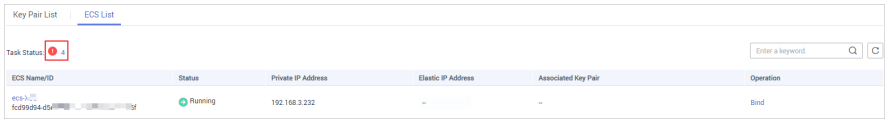
Tabela 3-3 Descrição do parâmetro

Parâmetro	Descrição
ECS Name/ID	Nome e ID de um ECS

Parâmetro	Descrição
Status	Os status de um ECS são os seguintes: ● Running ● Creating ● Faulty ● Shut down ● DELETE ● HARD_REBOOT ● MIGRATING ● REBOOT ● RESIZE ● REVERT_RESIZE ● SHELVED ● SHELVED_OFF ● LOADED ● UNKNOWN ● VERIFY_RESIZE
Private IP address	Endereço IP privado
EIP	Endereço IP elástico
Bound key pair	Par de chaves vinculado ao ECS

Passo 7 Clique em **ECS List** para exibir os ECSs.

Figura 3-12 Lista do ECS



Passo 8 Clique no número ao lado de do ícone de status da tarefa para exibir as tarefas que falharam, conforme mostrado em **Figura 3-13**.

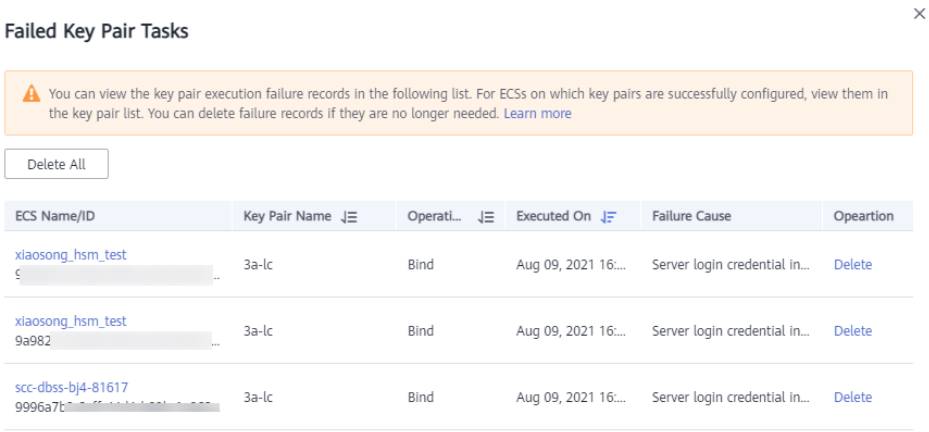
NOTA

Estado da reposição ou substituição do par de chaves:

: em execução

: falha na execução

Figura 3-13 Tarefas de par de chaves com falha



NOTA

- Você pode clicar em **Delete** na linha em que o par de chaves de destino é exibido para excluir a tarefa de par de chaves que falhou. Você também pode clicar em **Delete All** na parte superior da lista para excluir todas as tarefas que falharam.
- Clique em **Learn more** para visualizar documentos relacionados.

----Fim

3.4.3 Redefinição de um par de chaves

Se sua chave privada for perdida, você poderá usar um novo par de chaves para reconfigurar o ECS por meio do console de gerenciamento. Depois de redefinir o par de chaves, você precisa usar a chave privada do novo par de chaves para fazer logon no ECS, e a chave privada original não pode ser usada para fazer logon no ECS.

Esta seção descreve como redefinir um par de chaves no console do KPS.

Pré-requisitos

- O ECS cujo par de chaves deve ser redefinido usa a imagem pública fornecida pela HUAWEI CLOUD.
- Para redefinir o par de chaves, você pode substituir a chave pública do usuário modificando o arquivo **/root/.ssh/authorized_keys** no servidor. Certifique-se de que o arquivo não seja modificado antes de redefinir o par de chaves. Caso contrário, a redefinição falhará.
- O ECS deve estar no estado **Shut down**.

Procedimento

Passo 1 **Efetue logon no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

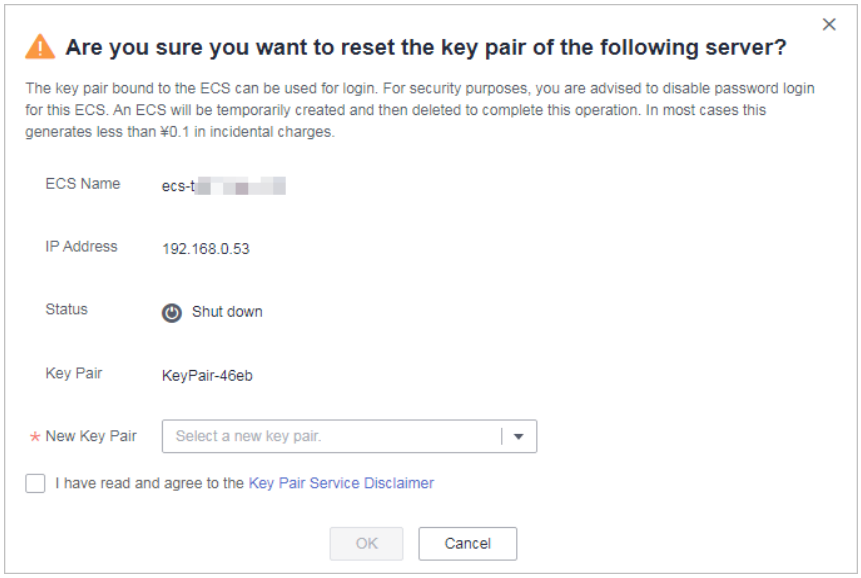
Passo 3 Clique em . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 No painel de navegação à esquerda, clique em **Key Pair Service**.

Passo 5 Clique na guia **ECS List**.

Passo 6 Clique em **Reset** na linha de um ECS.

Figura 3-14 Redefinir um par de chaves



Passo 7 Selecione um novo par de chaves na caixa de listagem suspensa de **New Key Pair**.

Passo 8 Selecione **I have read and agree to the Key Pair Service Disclaimer**.

Passo 9 Clique em **OK**. O par de chaves do ECS será redefinido em cerca de 10 minutos.

----Fim

3.4.4 Substituição de um par de chaves

Se sua chave privada for vazada, você poderá usar um novo par de chaves para substituir a chave pública do ECS por meio do console de gerenciamento. Depois de substituir o par de chaves, você precisa usar a chave privada do novo par de chaves para efetuar logon no ECS, e a chave privada original não pode ser usada para efetuar logon no ECS.

Esta seção descreve como substituir um par de chaves no console do KPS.

Pré-requisitos

- O ECS cujo par de chaves será substituído usa a imagem pública fornecida pela HUAWEI CLOUD.
- Para substituir o par de chaves, você pode substituir a chave pública do usuário modificando o arquivo **/root/.ssh/authorized_keys** no servidor. Certifique-se de que o arquivo não seja modificado antes de substituir o par de chaves. Caso contrário, a substituição da chave pública falhará.
- O ECS deve estar no estado **Running**.

Procedimento

Passo 1 **Efetue logon no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

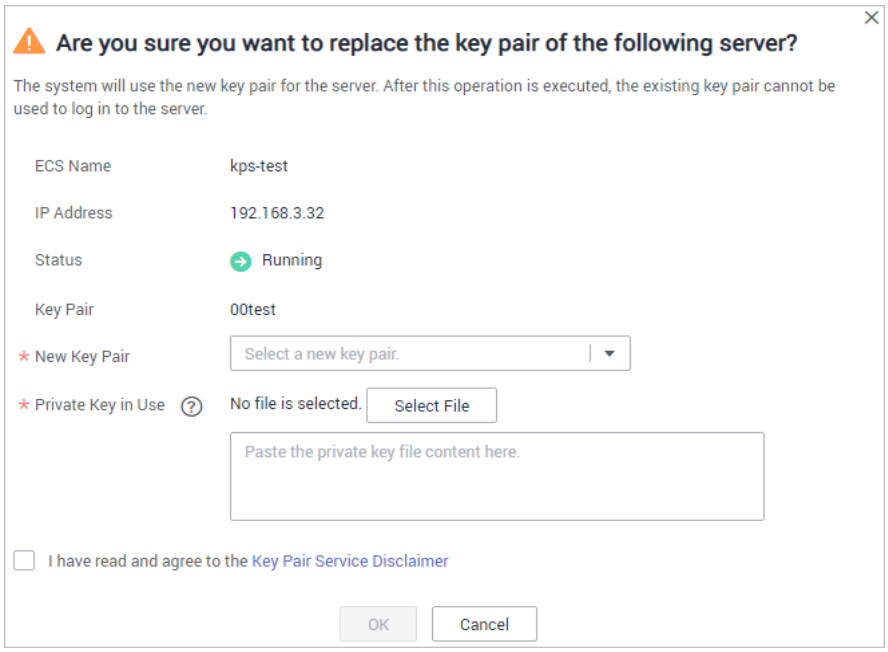
Passo 3 Clique em . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 No painel de navegação à esquerda, clique em **Key Pair Service**.

Passo 5 Clique na guia **ECS List**.

Passo 6 Clique em **Replace** na linha de um ECS. Defina os parâmetros na caixa de diálogo que é exibida.

Figura 3-15 Substituir um par de chaves



Passo 7 Selecione um novo par de chaves na caixa de listagem suspensa de **New Key Pair**.

Passo 8 Clique em **Select File** para carregar a chave privada (em formato **.pem**) do par de chaves original ou copie o conteúdo da chave privada para a caixa de texto.

NOTA

A chave privada a ser carregada ou copiada para a caixa de texto deve estar no formato **.pem**. Se estiver no formato **.ppk**, convertê-lo consultando **Como fazer para converter o formato de um arquivo de chave privada?**

Passo 9 Selecione **I have read and agree to the Key Pair Service Disclaimer**.

Passo 10 Clique em **OK**. O par de chaves do ECS será substituído em cerca de um minuto.

----Fim

3.4.5 Desvinculação de um par de chaves

Quando você usa um par de chaves para fazer logon em um ECS, se quiser alterar o modo de par de chaves para senha, poderá desvincular o par de chaves do ECS por meio do console de gerenciamento. O KPS desvinculará o par de chaves do ECS. Depois que o par de chaves for desvinculado, você poderá usar a senha para efetuar logon no ECS.

Pré-requisitos

- O ECS deve estar no estado **Running** ou **Shut down**.
- O ECS foi vinculado a um par de chaves.
- O ECS a ser desvinculado de seu par de chaves usa a imagem pública fornecida pela HUAWEI CLOUD.
- Para desvincular de um par de chaves, você pode excluir a chave pública do usuário do arquivo **/root/.ssh/authorized_keys** no servidor. Certifique-se de que o arquivo não seja modificado antes de desvincular do par de chaves. Caso contrário, a desvinculação falhará.

Restrições

- Se você não tiver definido a senha para fazer logon no ECS ou se esquecer da senha de logon, poderá redefinir a senha de logon do ECS no console do ECS. Para obter mais informações, consulte o *Guia de usuário do Elastic Cloud Server*.
- Se você ativou o logon de par de chaves para um ECS durante sua criação, mas desvinculou o ECS de seu par de chaves, para vincular um par de chaves novamente, encerre o ECS primeiro.
- Depois de desvincular um ECS de seu par de chaves, redefina a senha no console do ECS em tempo hábil. Para obter mais informações, consulte o *Guia de usuário do Elastic Cloud Server*.

Procedimento

Passo 1 **Efetue logon no console de gerenciamento**.

Passo 2 Clique em  no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em  . Escolha **Security & Compliance** > **Data Encryption Workshop**.

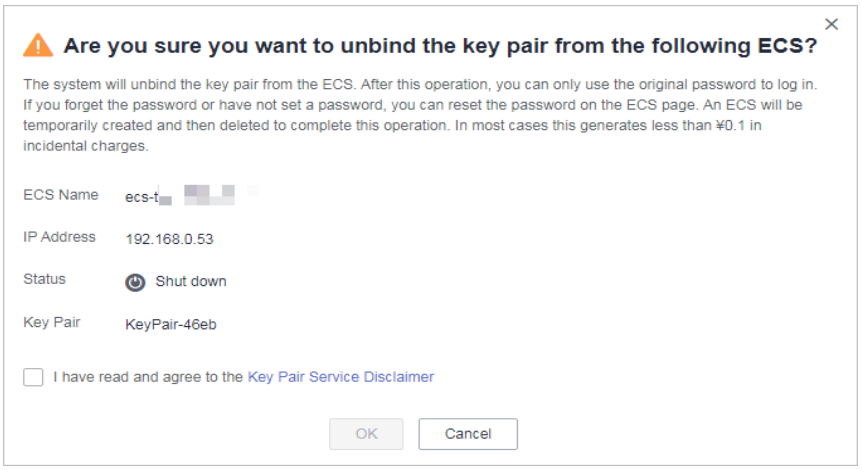
Passo 4 No painel de navegação à esquerda, clique em **Key Pair Service**.

Passo 5 Clique na guia **ECS List**.

Passo 6 Clique em **Unbind** na linha de um ECS.

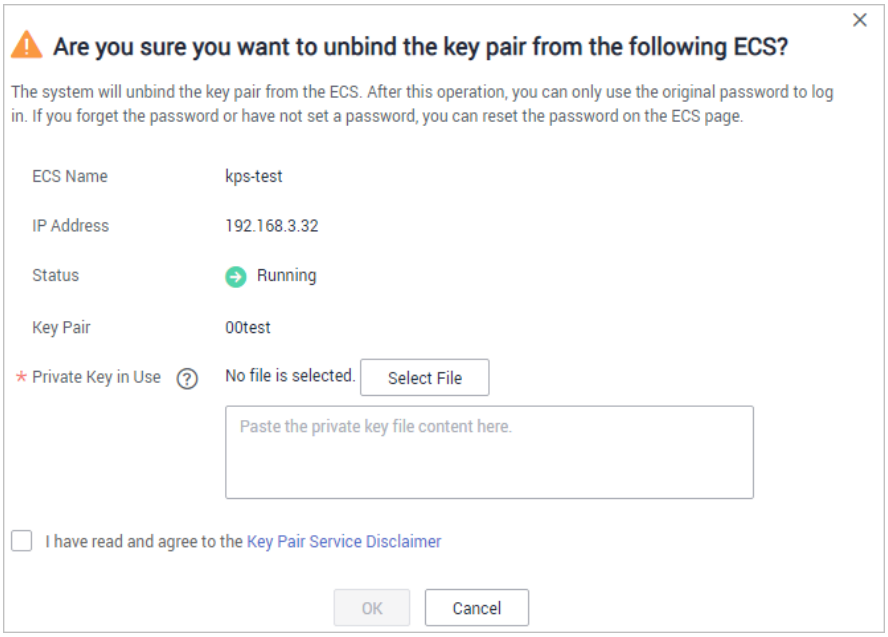
- Se o ECS for desligado, uma caixa de diálogo será exibida, conforme mostrado na **Figura 3-16**.

Figura 3-16 Desvinculação de um par de chaves (1)



- Se o ECS estiver em execução, uma caixa de diálogo será exibida, conforme mostrado na **Figura 3-17**.

Figura 3-17 Desvinculação de um par de chaves (2)



Passo 7 Se você desvincular o par de chaves quando o ECS estiver no estado de execução, será necessário fazer carregamento da chave privada. Clique em **Select file** para carregar a chave privada (no formato **.pem**) do par de chaves existente ou copie a chave privada para a caixa de texto. Se o ECS estiver desligado, ignore esta etapa.

NOTA

A chave privada a ser carregada ou copiada para a caixa de texto deve estar no formato **.pem**. Se estiver no formato **.ppk**, convertê-lo consultando **Como fazer para converter o formato de um arquivo de chave privada?**

Passo 8 Selecione **I have read and agree to the Key Pair Service Disclaimer**.

Passo 9 Clique em **OK**. O par de chaves será desvinculado do ECS em cerca de um minuto.

NOTA

Depois que o par de chaves for desvinculado do ECS, redefina a senha para logon no console do ECS a tempo. Para obter detalhes, consulte o *Guia de usuário do Elastic Cloud Server*.

----Fim

3.4.6 Exclusão de um par de chaves

Você pode excluir um par de chaves se ele não for mais usado.

Esta seção descreve como excluir um par de chaves no console do KPS

Restrições

- Uma chave excluída não pode ser recuperada. Portanto, tenha cuidado ao realizar esta operação.
- A chave privada importada para um par de chaves será excluída com ela.
- Se você excluir a chave pública vinculada a um ECS no console do KMS e a chave privada tiver sido salva localmente, poderá usar a chave privada para efetuar logon no ECS. A operação de exclusão não afeta o logon do ECS.

Procedimento

Passo 1 **Efetue logon no console de gerenciamento**.

Passo 2 Clique em  no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em  . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 No painel de navegação à esquerda, clique em **Key Pair Service**.

Passo 5 Na linha que contém o par de chaves desejado, clique em **Delete**.

NOTA

Se você atualizou o par de chaves para um par de chaves de conta, execute a próxima etapa na lista de pares de chaves de conta.

Passo 6 Na caixa de diálogo **Delete Key Pair** exibida, clique em **OK**. Quando **Key pair deleted successfully** é exibido no canto superior direito, o par de chaves é excluído.

----Fim

3.5 Gerenciamento de chaves privadas

3.5.1 Importação de uma chave privada

Para facilitar o gerenciamento de chaves privadas locais, você pode importar a chave privada para o console do KPS para o gerenciamento centralizado de suas chaves privadas. As chaves privadas gerenciadas são criptografadas pelas chaves fornecidas pelo KMS, garantindo segurança para armazenamento, importação e exportação das chaves privadas. Você pode

baixar as chaves privadas do console de gerenciamento sempre que precisar. Para garantir a segurança das chaves privadas, mantenha as chaves privadas baixadas corretamente.

Esta seção descreve como importar um par de chaves no console do KPS.

Pré-requisitos

O arquivo de chave privada correspondente à chave pública foi obtido.

Restrições

- Somente a chave privada que corresponde a uma chave pública pode ser importada para a chave pública.
- A chave privada a ser carregada ou copiada para a caixa de texto deve estar no formato **.pem**. Se estiver no formato **.ppk**, convertê-lo consultando **Como fazer para converter o formato de um arquivo de chave privada?**
- Quando você ativa a função de criptografia KMS para um par de chaves, o KMS cria automaticamente uma chave mestra padrão **kps/default** para o par de chaves.
- Ao selecionar uma chave de criptografia, você pode selecionar uma chave de criptografia existente ou clicar em **View Key List** para criar uma chave de criptografia.

Procedimento

Passo 1 **Efetue logon no console de gerenciamento**.

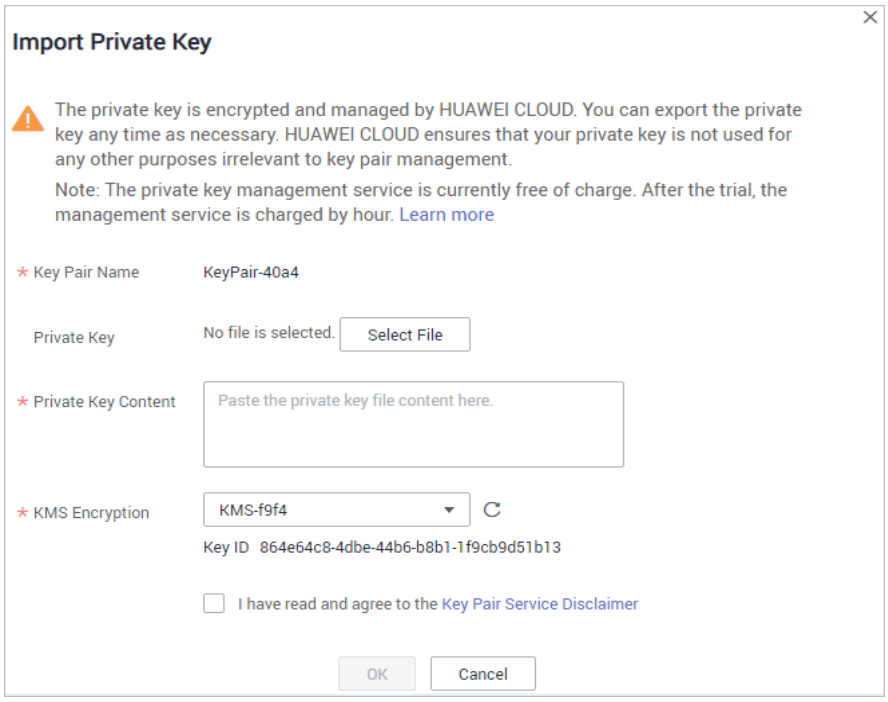
Passo 2 Clique em  no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em  . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 No painel de navegação à esquerda, clique em **Key Pair Service**.

Passo 5 Clique em **Import Private Key** na linha em que a chave pública de destino está localizada. Defina os parâmetros na caixa de diálogo **Import Private Key**.

Figura 3-18 Importar uma chave privada



Passo 6 Clique em **Select File**, selecione um arquivo de chave privada **.pem** local. Como alternativa, você pode copiar e colar o conteúdo da chave privada na caixa de texto **Private Key Content**.

NOTA

- Somente a chave privada que corresponde a uma chave pública pode ser importada para a chave pública.
- A chave privada a ser carregada ou copiada para a caixa de texto deve estar no formato **.pem**. Se estiver no formato **.ppk**, convertê-lo consultando **Como fazer para converter o formato de um arquivo de chave privada?**

Passo 7 Selecione uma chave de criptografia na caixa de listagem suspensa **KMS encryption**.

NOTA

- Quando você ativa a função de criptografia KMS para um par de chaves, o KMS cria automaticamente uma chave mestra padrão **kps/default** para o par de chaves.
- Ao selecionar uma chave de criptografia, você pode selecionar uma chave de criptografia existente ou clicar em **View Key List** para criar uma chave de criptografia.

Passo 8 Selecione **I have read and agree to the Key Pair Service Disclaimer**.

Passo 9 Clique em **OK** para concluir a importação.

----Fim

3.5.2 Exportação de uma chave privada

Se você tiver as chaves privadas gerenciadas pela HUAWEI CLOUD, poderá baixá-las sempre que precisar. Para garantir a segurança da chave privada, mantenha a chave privada baixada corretamente.

Pré-requisitos

A chave privada foi gerenciada no console de gerenciamento.

Restrições

Uma chave privada é criptografada e descriptografada usando a mesma chave de criptografia. Se a chave de criptografia for excluída, a chave privada não será exportada.

Procedimento

Passo 1 **Efetue logon no console de gerenciamento**.

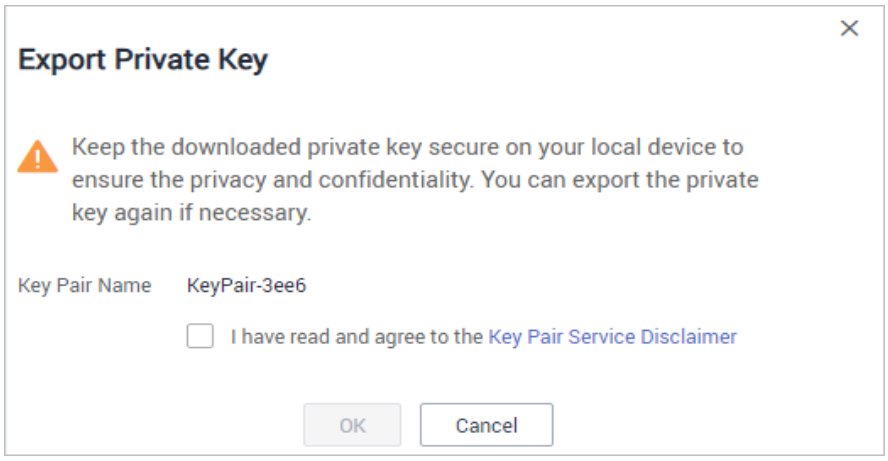
Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 No painel de navegação à esquerda, clique em **Key Pair Service**.

Passo 5 Clique em **Export Private Key** na linha onde reside o par de chaves de destino. A caixa de diálogo **Export Private Key** é exibida, como mostrado na **Figura 3-19**.

Figura 3-19 Exportar uma chave privada



Passo 6 Selecione **I have read and agree to the Key Pair Service Disclaimer**.

Passo 7 Clique em **OK**. O navegador baixa automaticamente a chave privada.

AVISO

Ao exportar uma chave privada, você precisa usar a chave de criptografia que criptografa a chave privada para descriptografar a chave privada. Se a chave de criptografia tiver sido completamente excluída, a exportação da chave privada falhará.

----Fim

3.5.3 Limpeza de uma chave privada

Se as chaves privadas gerenciadas pelo KPS na HUAWEI CLOUD não forem mais necessárias, você poderá limpar as chaves privadas gerenciadas no console do KPS.

Pré-requisitos

A chave privada foi gerenciada no console de gerenciamento.

Restrições

Depois que a chave privada for limpa, você não poderá obter a chave privada da HUAWEI CLOUD. Tenha cuidado ao realizar esta operação. Se você precisar ter a chave privada gerenciada na HUAWEI CLOUD novamente, poderá importar a chave privada para o console de gerenciamento.

Procedimento

Passo 1 **Efetue logon no console de gerenciamento**.

Passo 2 Clique em  no canto superior esquerdo do console de gerenciamento e selecione uma região e um projeto.

Passo 3 Clique em  . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 No painel de navegação à esquerda, clique em **Key Pair Service**.

Passo 5 Clique em **Clear Private Key** na linha em que a chave pública de destino está localizada para limpar a chave privada.

NOTA

Se tiver atualizado o par de chaves para um par de chaves de conta, execute os seguintes passos na lista de pares de chaves de conta.

Passo 6 Na caixa de diálogo **Clear Private Key** exibida, clique em **OK**.

NOTA

Depois que a chave privada for limpa, você não poderá obter a chave privada da HUAWEI CLOUD. Tenha cuidado ao realizar esta operação. Se você precisar ter a chave privada gerenciada na HUAWEI CLOUD novamente, poderá importar a chave privada para o console de gerenciamento.

----Fim

3.6 Usar uma chave privada para fazer logon no ECS do Linux

Depois de criar ou importar um par de chaves no console do KMS, selecione o par de chaves como o modo de logon ao comprar um ECS e selecione o par de chaves criado ou importado.

Depois de adquirir um ECS, você pode usar a chave privada do par de chaves para efetuar logon no ECS.

Pré-requisitos

- A conexão de rede entre a ferramenta de logon (como PuTTY e XShell) e o ECS de destino é normal.
- Você vinculou um EIP ao ECS.
- Você obteve o arquivo de chave privada do ECS.

Restrições

Os formatos dos arquivos de chave privada do ECS devem atender aos seguintes requisitos.

Tabela 3-4 Formatos de arquivo de chave privada

SO local	Ferramenta de logon do ECS de Linux	Formato de arquivo de chave privada
SO de Windows	**Xshell**	**.pem**
	PuTTY	**.ppk**
SO de Linux	-	**.pem** ou **.ppk**

Se o seu arquivo de chave privada não estiver no formato necessário, converta-o consultando **Como converter o formato de um arquivo de chave privada?**

Efetuar logon a partir de um computador de Windows

Para efetuar logon no ECS de Linux a partir de um computador de Windows, execute as operações descritas nesta seção.

Método 1: use o PuTTY para efetuar logon no ECS.

Passo 1 Clique duas vezes em **PUTTY.EXE**. A página **PuTTY Configuration** é exibida.

Passo 2 Escolha **Connection** > **Data**. Digite o nome de usuário da imagem em **Auto-login username**.

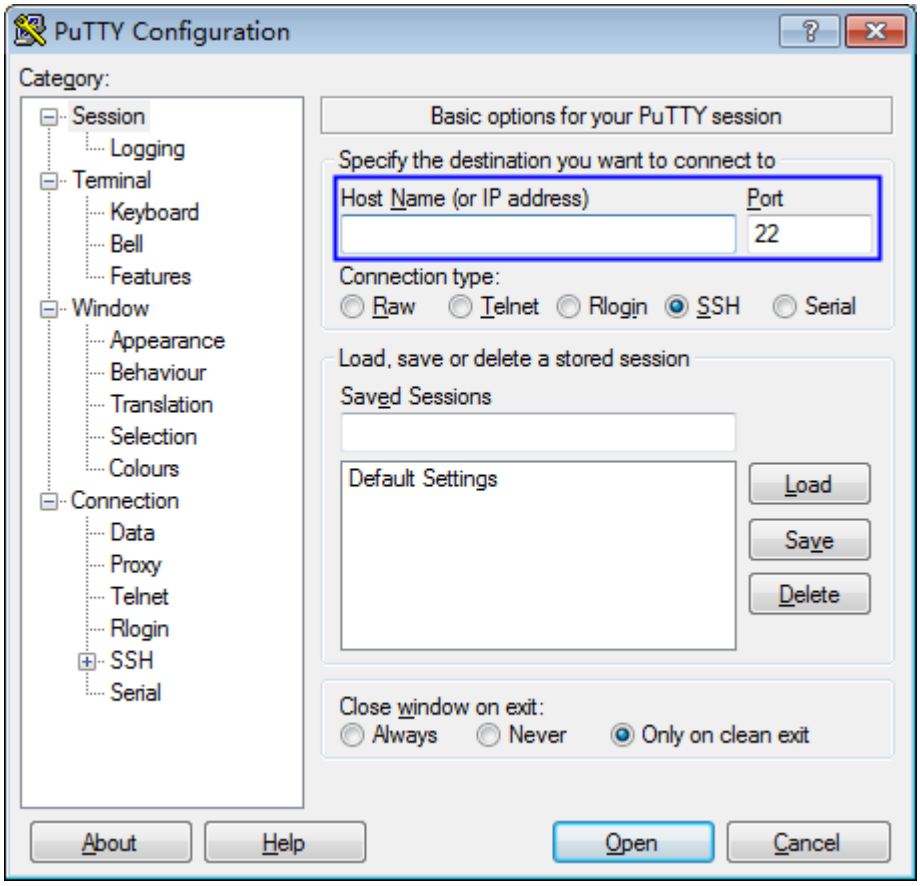
NOTA

- Se a imagem pública do **CoreOS** for usada, o nome de usuário da imagem é **core**.
- Para uma imagem pública **non-CoreOS**, o nome de usuário da imagem é **root**.

Passo 3 Escolha **Conexão** > **SSH** > **Auth**. Em **Private key file for authentication**, clique em **Browse** e selecione um arquivo de chave privada (no formato **.ppk**).

Passo 4 Clique em **Session** e insira o EIP do ECS em **Host Name (or IP address)**.

Figura 3-20 Configurar o EIP



Passo 5 Clique em **Open** para efetuar logon no ECS.

----Fim

Método 2: use o Xshell para efetuar logon no ECS.

Passo 1 Inicie a ferramenta Xshell.

Passo 2 Execute o seguinte comando para efetuar logon remotamente no ECS por meio do SSH:

ssh *Username@EIP*

Um exemplo de comando é fornecido da seguinte forma:

ssh *root@192.168.1.1*

Passo 3 (Opcional) Se o sistema exibir a caixa de diálogo **SSH Security Warning**, clique em **Accept & Save**.

Passo 4 Selecione **Public Key** e clique em **Browse** ao lado da caixa de texto de CMK.

Passo 5 Na caixa de diálogo exibida, clique em **Import**.

Passo 6 Selecione o arquivo de chave armazenado localmente (no formato **.pem**) e clique em **Open**.

Passo 7 Clique em **OK** para efetuar logon no ECS.

----Fim

Fazer logon a partir de um computador de Linux

Para efetuar logon no ECS de Linux a partir de um computador de Linux, execute as operações descritas a seguir: as operações a seguir usam o arquivo de chave privada **kp-123.pem** como um exemplo para fazer logon no ECS. O nome do seu arquivo de chave privada pode ser diferente.

Passo 1 Na CLI do Linux, execute o seguinte comando para alterar as permissões de operação:

chmod 600 ***/path/kp-123.ppk***

NOTA

No comando anterior, **path** é o caminho onde o arquivo de chave é salvo.

Passo 2 Execute o seguinte comando para fazer logon no ECS:

ssh -i ***/path/kp-123*** **root@*EIP***

NOTA

- No comando anterior, **path** é o caminho onde o arquivo de chave é salvo.
- *EIP* é o EIP vinculado ao ECS.

----Fim

3.7 Usar uma chave privada para obter a senha de logon do ECS de Windows

Uma senha é necessária quando você faz logon em um ECS do Windows. Primeiro de tudo, você deve obter a senha de administrador (senha do **Administrator** da conta ou outra conta definida no Cloudbase-Init) gerado durante a instalação inicial do ECS a partir do arquivo de chave privada baixado quando você cria o ECS. Essa senha é gerada aleatoriamente, com alta segurança.

Você pode obter a senha para efetuar logon em um ECS do Windows por meio do console de gerenciamento

Pré-requisitos

Você obteve o arquivo de chave privada (no formato **.pem**) para fazer logon no ECS.

Restrições

- Depois de obter a senha inicial, é aconselhável limpar as informações de senha registradas no sistema para aumentar a segurança do sistema.

  Limpar as informações iniciais da senha não afeta a operação ou o logon do ECS. Uma vez limpa, a senha não pode ser restaurada. Antes de excluir uma senha, é aconselhável registrá-la. Para obter detalhes, consulte o *Guia de usuário do Elastic Cloud Server*.
- Você também pode chamar a API para obter a senha inicial do ECS do Windows. Para obter detalhes, consulte a *Referência de API do Elastic Cloud Server*.
- O arquivo de chave privada do ECS deve estar no formato **.pem**.

  Se o arquivo estiver no formato **.ppk**, converta-o em um arquivo **.pem**. Para obter detalhes, consulte **Como converter o formato de um arquivo de chave privada?**

Procedimento

Passo 1 **Faça logon no console de gerenciamento**.

Passo 2 Clique em  . Sob **Computing**, clique em **Elastic Cloud Server**.

Passo 3 Na lista ECS, selecione o ECS cuja senha você deseja obter.

Passo 4 Na coluna **Operation**, clique em **More** e escolha **Get Password**.

Passo 5 Use um dos seguintes métodos para obter a senha:

- Clique em **Select File** e carregue o arquivo de chave de um diretório local.
- Copie o conteúdo do arquivo de chave para o campo de texto.

Passo 6 Clique em **Get Password** para obter uma nova senha aleatória.

----Fim

4 HSM dedicado

4.1 Guia de operação

Restrições

- As instâncias do HSM dedicado devem ser usadas em conjunto com a VPC. Depois que uma instância do HSM dedicado é comprada, você precisa configurar sua VPC, grupo de segurança e NIC no console de gerenciamento antes de usá-la.
- Para fins de segurança, as instâncias do HSM dedicado não fornecem serviços para a rede pública. Para gerenciar as instâncias, implemente a ferramenta de gerenciamento na VPC.

Guia de operação

Para usar o HSM dedicado na nuvem, você pode comprar instâncias do HSM dedicado por meio do console de gerenciamento. Depois que uma instância do HSM dedicado for comprada, receberá o UKey enviado pelo HSM dedicado. Você precisa usar o UKey para inicializar e controlar a instância. Você pode usar a ferramenta de gerenciamento para autorizar aos aplicações de serviço a permissão para acessar instâncias do HSM dedicado. **Figura 4-1** ilustra o fluxo da operação.

Figura 4-1 Guia de operação

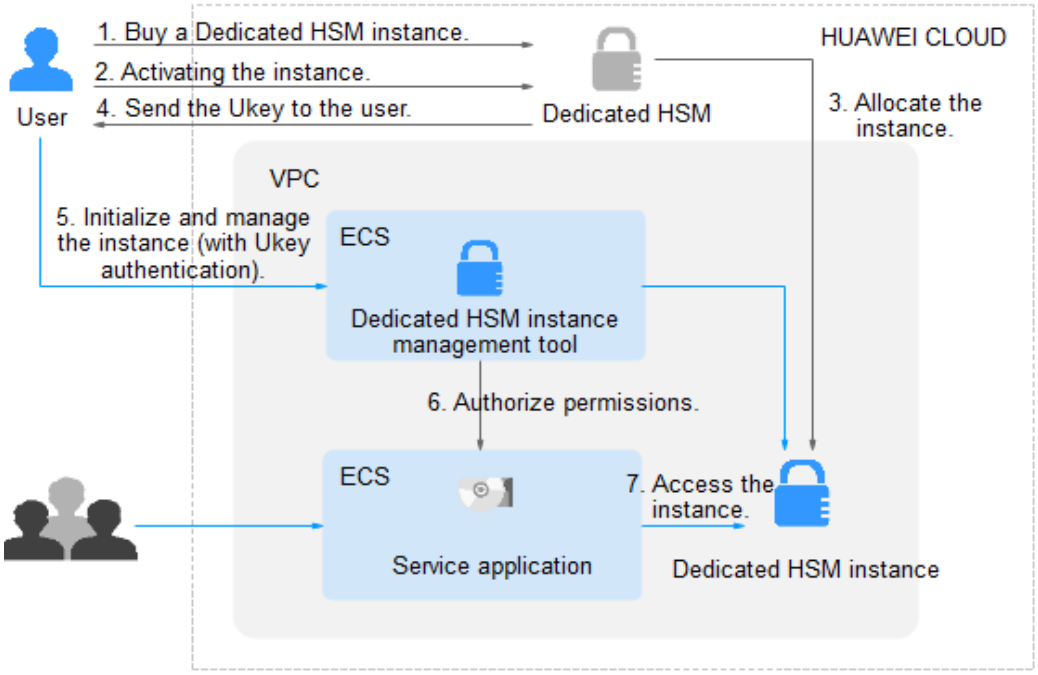


Tabela 4-1 descreve o guia de operação.

Tabela 4-1 Descrições do guia de operação

Nº	Procedimento	Descrição	Operado por
1	Crie uma instância do HSM dedicado.	Crie uma instância no console de gerenciamento do HSM dedicado. A equipe de segurança da HUAWEI CLOUD avaliará seus cenários de uso para garantir que a instância atenda aos seus requisitos de serviço. Então você pode pagar pela instância encomendada.	Usuário
2	Ative uma instância do HSM dedicado.	Depois que uma instância é comprada, você precisa configurar a instância no console de gerenciamento. Você precisa selecionar a VPC à qual a instância pertence e o tipo de função da instância. Para mais detalhes, consulte **Ativação de uma instância do HSM dedicado**.	Usuário
3	Alocar uma instância do HSM dedicado.	Uma instância comprada será alocada ao usuário. Um especialista em segurança entrará em contato com você por meio das informações de contato fornecidas e determinará se a instância solicitada atende aos seus requisitos de serviço. A instância será alocada após as análises de especialistas e confirma seu pedido.	Especialista em segurança do HSM dedicado

Nº	Procedimento	Descrição	Operado por
4	Forneça o UKey, o guia de inicialização e o software.	• Um especialista em segurança envia o Ukey para o endereço de e-mail fornecido. Um UKey é o único identificador de um usuário do HSM dedicado. Mantenha-o corretamente. • Um especialista em segurança fornecerá o software e o guia para inicializar instâncias do HSM dedicado. Se você tiver alguma dúvida, entre em contato com o especialista.	Especialista em segurança do HSM dedicado
5	Inicializar e gerenciar instâncias (envolvendo autenticação de UKey).	1. Instale a ferramenta para gerenciar instâncias do HSM dedicado no nó de gerenciamento de instâncias. 2. Use o UKey e a ferramenta de gerenciamento para inicializar a instância do HSM dedicado e registre um administrador para gerenciar a instância do HSM dedicado e a chave. Para mais detalhes, consulte **Inicializar uma instância do HSM dedicado**.	Usuário
6	Instalar o agente de segurança e conceder permissões de acesso.	Instale e inicialize o agente de segurança em nós de aplicação de serviço. Para mais detalhes, consulte **Instalar o agente de segurança e conceder permissões de acesso**.	Usuário
7	Acesse a instância.	As aplicações de serviço acessam as instâncias do HSM dedicado por meio de APIs ou SDK.	Usuário

4.2 Compra de uma instância do HSM dedicado

4.2.1 Edições

O HSM dedicado fornece instâncias da edição platinum. Para mais detalhes, consulte **Tabela 4-2**.

Tabela 4-2 HSM dedicado

Edição	Modo de cobrança	Escopo do serviço
Platinum	Anual/ Mensal	● Chip exclusivo para criptografia Fornece chips exclusivos para criptografia de dados na nuvem, garantindo o isolamento do hardware enquanto mantém o desempenho do seu serviço. ● Suporte de serviço completo Suporta segurança de aplicações, como pagamento financeiro, autenticação de identidade e assinatura digital, atendendo aos seus requisitos rigorosos de segurança de dados e sistema. ● Escalonável Permite adicionar e reduzir de forma fácil e flexível recursos de computação de senhas com base em suas necessidades de serviço. ● Altamente confiável Instâncias de dispositivos de hardware são virtualizadas em clusters para obter balanceamento de carga e alta confiabilidade. ● Compatibilidade Fornece as mesmas funções e API que os dispositivos criptográficos físicos, facilitando a migração para a nuvem com suporte para APIs de PKCS#11 e de CSP. ● Algoritmos comuns – Algoritmo simétrico: DES e AES – Algoritmo de resumo: SHA1, SHA256 e SHA384 – Algoritmo assimétrico: RSA, DSA, ECDSA, DH e ECDH. ● Subrack e fonte de alimentação exclusivos Fornece subrack e fonte de alimentação do HSM exclusivos. ● Rede dedicada Fornece largura de banda de rede dedicada e recursos de API. ● Certificação FIPS 140-2 Usa o HSM certificado FIPS 140-2 nível 3 para gerar chaves de criptografia.

4.2.2 Creating a Dedicated HSM Instance

When creating a Dedicated HSM instance, you need to specify the region and fill in your contact information.

The fee for a Dedicated HSM instance in platinum edition consists of the following two parts:

- Initial installation fee, charged when you create a Dedicated HSM instance.

- Yearly/Monthly fee, charged when **Ativação de uma instância do HSM dedicado**.

Prerequisites

You have obtained the login account (with the **Ticket Administrator** and **KMS Administrator** permissions) and password for logging in to the management console.

Constraints

- When purchasing a Dedicated HSM instance, you need to submit a service ticket to set the UKey recipient information. Only the accounts with the **Ticket Administrator** permission can submit service tickets.
- After you created an instance, a UKey will be sent to the address in your contact information. Then you can use the UKey to initialize and authorize your service applications to access the instance.

  You need to activate the instance before using it.

Procedure

Passo 1 **Faça logon no console de gerenciamento.**

Passo 2 Click in the upper left corner of the management console and select a region or project.

Passo 3 Click . Choose **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 In the navigation pane, choose **Dedicated HSM**.

Passo 5 Click **Create Dedicated HSM** in the upper right corner of the page.

Passo 6 **Billing Mode** can only be set to **Yearly/Monthly**.

Figura 4-2 Billing Mode

Passo 7 Select the current region.

Figura 4-3 Selecting a region

Passo 8 Select the service edition for the instance. **Tabela 4-3** lists related parameters.

Tabela 4-3 Edition parameters

Parameter	Description
Service Edition	Platinum edition

Parameter	Description
Encryption Algorithm	Encryption algorithm supported by the HSM instance. ● Symmetric algorithm: AES ● Asymmetric algorithm: RSA, DSA, ECDSA, DE, and ECDH ● Digest algorithm: SHA1, SHA256, SHA384
Certification	FIPS 140-2 Level 3 certified

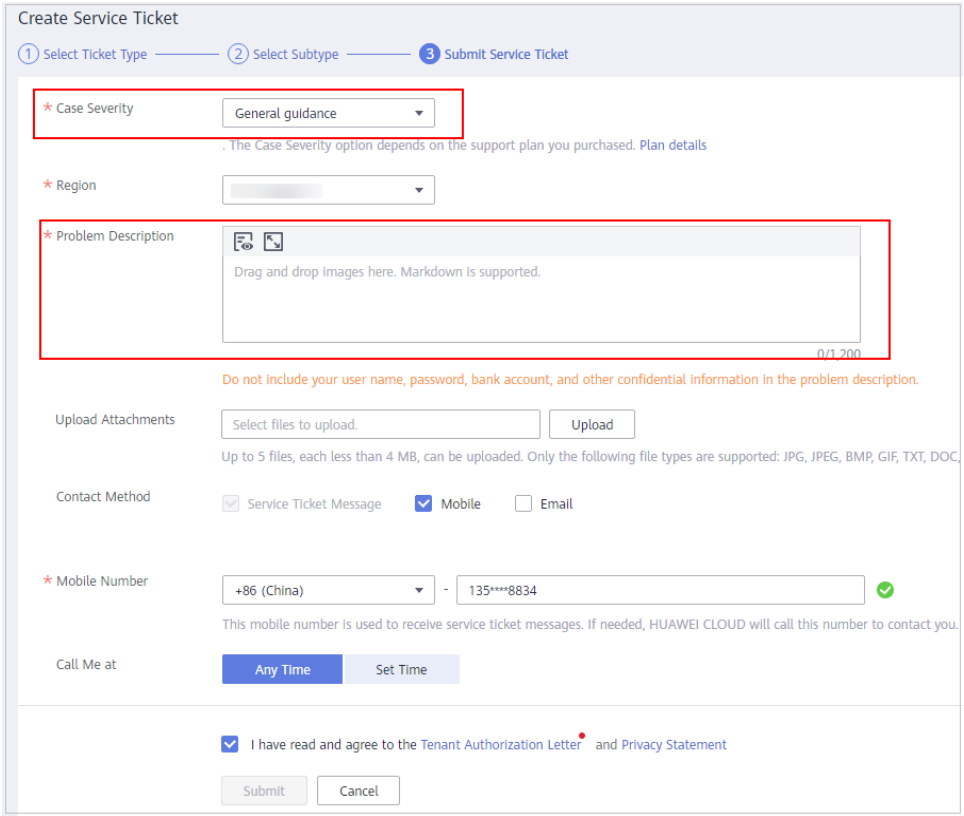
Passo 9 Choose **Service Tickets** > **Create Service Ticket**. Our HUAWEI CLOUD experts will contact you and provide a customized purchase plan and its quote.

- In the **Case Severity** drop-down list, select **General guidance**.
- In the **Problem Description** text box, enter **Dedicated HSM Contact Information**.

AVISO

Ensure that the contact information provided in the **Confidential Information** text box is valid so that our security experts can contact you in a timely manner.

Figura 4-4 Creating a service ticket



Passo 10 Click **Submit**. The service ticket is displayed on the **My Service Tickets** page.

NOTA

After the service ticket is created successfully, you can click **View Details** in the **Operation** column to view details. You can remind the support team of a service ticket, leave your messages, cancel a service ticket, or closed a service ticket based on service ticket statuses.

----Fim

4.2.3 Ativação de uma instância do HSM dedicado

Você precisa ativar uma instância do HSM dedicado antes de usá-la. O pacote anual ou mensal será cobrado durante a ativação.

Esta seção descreve como ativar uma instância do HSM dedicado por meio do console de gerenciamento.

Pré-requisitos

- Você obteve uma conta e sua senha para fazer logon no console de gerenciamento.
- O status da instância do HSM dedicado é **Para ser ativado**.

Restrições

- O nome da instância pode conter apenas letras, dígitos, sublinhados (_) e hifens (-).
- Dois nós são criados como o pool de recursos em segundo plano para uma instância do HSM dedicado. Para garantir a alta disponibilidade dos nós, um endereço IP flutuante é atribuído à instância.
- Se a instância não for criada, você pode clicar em **Delete** na linha em que a instância está localizada para excluí-la. Em seguida, solicite um reembolso enviando um tíquete de serviço.
- Depois que uma instância do HSM dedicado é criada com sucesso, ela não pode ser alterada para outro tipo nem reembolsada. Para usar uma instância do HSM dedicado de outro tipo, você precisa comprar outra.

Procedimento

Passo 1 **Faça logon no console de gerenciamento.**

Passo 2 Click in the upper left corner of the management console and select a region or project.

Passo 3 Click . Choose **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 In the navigation pane, choose **Dedicated HSM**.

Passo 5 Clique em **Activate** na linha em que a instância de destino está localizada.

Passo 6 Selecione uma AZ.

Figura 4-5 Selecionar uma AZ

Passo 7 Insira as informações de ativação, conforme mostrado na **Figura 4-6**. **Tabela 4-4** descreve os parâmetros.

Figura 4-6 Configuração de uma instância do HSM dedicado

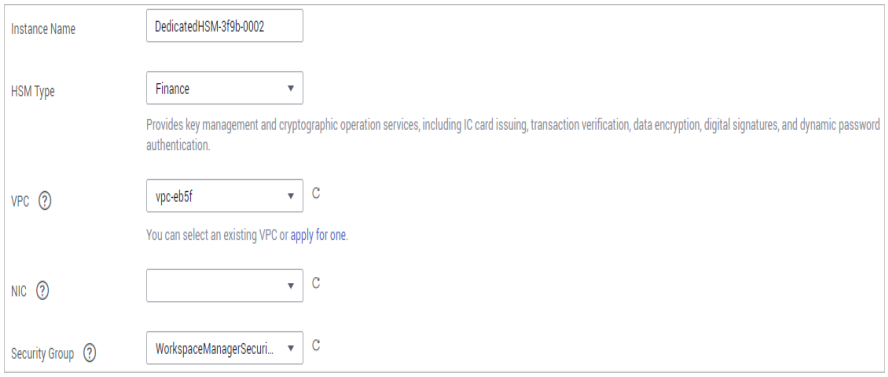


Tabela 4-4 Parâmetros de ativação

Parâmetro	Descrição	Valor de exemplo
Instance Name	Nome de uma instância do HSM dedicado **NOTA** O nome da instância pode conter apenas letras, dígitos, sublinhados (_) e hifens (-).	DedicatedHSM-3c98-0002
HSM Type	Os tipos de HSM disponíveis incluem **Finance**, **Server** e **Signature server**. ● **Finance**: fornece gerenciamento de chaves e serviços de computação de criptografia, incluindo emissão de cartões IC, verificação de transações, criptografia de dados, assinaturas digitais e autenticação de senha dinâmica. ● **Server**: fornece serviços de gerenciamento de chaves completos e seguros e operações criptográficas simultâneas de alto desempenho, como assinaturas de dados, verificação de assinaturas e criptografia/descriptografia de dados. ● **Signature server**: garante a integridade, confidencialidade, anti-repúdio e rastreabilidade pós-evento dos dados do usuário usando assinaturas digitais, envelopes digitais e resumos digitais.	**Finance**
VPC	Você pode selecionar uma Virtual Private Cloud (VPC) existente ou clicar em **Apply for VPC** para criar uma. Para obter mais informações sobre VPC, consulte o *Guia de usuário da Virtual Private Cloud*.	vpc-test-dhsm

Parâmetro	Descrição	Valor de exemplo
NIC	Todas as sub-redes disponíveis são exibidas na página. O sistema atribui automaticamente três endereços IP à instância. **NOTA** Dois nós são criados como o pool de recursos em segundo plano para uma instância do HSM dedicado. Para garantir a alta disponibilidade dos nós, um endereço IP flutuante é atribuído à instância. Para obter mais informações sobre sub-redes, consulte o *Guia de usuário da Virtual Private Cloud*.	**subnet-test-dhsm (192.168.0.0/24)**
Security Group	O grupo de segurança configurado para a instância é exibido na página. Depois que um grupo de segurança é selecionado para uma instância, a instância é protegida pelas regras de acesso do grupo de segurança. Para obter mais informações sobre grupos de segurança, consulte o *Guia de usuário da Virtual Private Cloud*.	WorkspaceUserSecurityGroup

Passo 8 Se você comprou uma instância do HSM dedicado na edição padrão:

Clique em **Create Now** para retornar à lista de instâncias do HSM dedicado. Você pode exibir informações sobre a instância ativada.

Se o status da instância do HSM dedicado for **Creating**, a instância será ativada com sucesso.

Passo 9 Se você comprou uma instância do HSM dedicado na edição platinum:

1. Defina a duração necessária.

   A duração exigida varia de um mês a um ano.

   NOTA

   A opção **Auto-renew** permite que o sistema renove seu serviço até o período comprado, quando o serviço está prestes a expirar.

2. Confirme a configuração e clique em **Next**.

   Para qualquer dúvida sobre o preço, clique em **Pricing details**.

3. Na página **Order Details**, confirme os detalhes do pedido, leia e selecione **I have read and agree to the Privacy Policy Statement**.
4. Clique em **Pay Now** para pagar pelo pacote anual ou mensal.
5. Na página **Pay**, selecione um método de pagamento para pagar seu pedido.

   Após o pagamento bem-sucedido, você pode exibir as informações sobre a instância do HSM na página de lista de instâncias do HSM.

   Se o **Status** da instância for **Creating**, a instância foi ativada e está sendo alocada para você. Estará disponível em 5 a 10 minutos.

   Creating: o sistema está alocando uma instância para você. Esse processo geralmente dura de 5 a 10 minutos.

   Após a atribuição, o status da instância pode mudar para um dos seguintes:

- **Creation failed**: uma instância falha ao ser criada devido a recursos insuficientes ou falhas de rede.

  NOTA

  Se a instância não for criada, você pode clicar em **Delete** na linha em que a instância está localizada para excluí-la. Em seguida, solicite um reembolso enviando um tíquete de serviço.

- **Running**: uma instância foi atribuída com sucesso a você e está sendo executada corretamente.

  NOTA

  Depois que uma instância do HSM dedicado é criada com sucesso, ela não pode ser alterada para outro tipo nem reembolsada. Para usar uma instância do HSM dedicado de outro tipo, você precisa comprar outra.

----Fim

4.3 Exibição de instâncias do HSM dedicado

Esta seção descreve como exibir as informações da instância do HSM dedicado, incluindo nome/ID, status, versão do serviço, fornecedor do dispositivo, modelo do dispositivo, endereço IP e hora de criação.

Pré-requisitos

Você obteve uma conta e sua senha para fazer logon no console de gerenciamento.

Procedimento

Passo 1 **Faça logon no console de gerenciamento.**

Passo 2 Clique em  no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

Passo 3 Clique em  . Escolha **Security & Compliance** > **Data Encryption Workshop**. A página **Key Management Service** será exibida.

Passo 4 No painel de navegação, escolha **Dedicated HSM**.

Passo 5 Na lista, você pode exibir as informações sobre as instâncias do HSM.

Tabela 4-5 descreve os parâmetros na lista de instâncias do HSM.

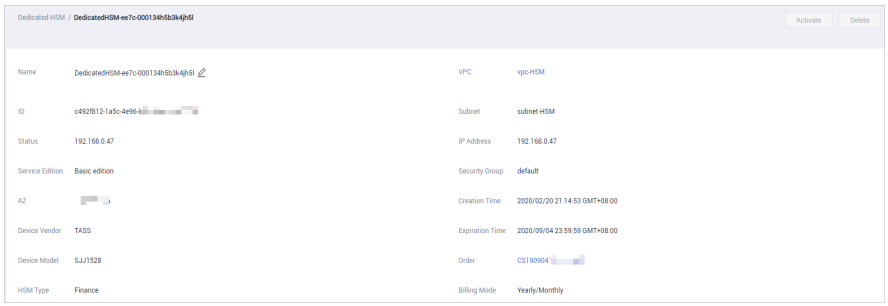
Tabela 4-5 Parâmetros de instância do HSM dedicado

Parâmetro	Descrição
Name/ID	Nome e ID de uma instância do HSM dedicado

Parâmetro	Descrição
Status	Status de uma instância do HSM dedicado: ● Installing Depois de pagar a taxa de instalação inicial, a instância comprada será instalada. O status da instância do HSM dedicado será **Installing**. ● To be activated O status de uma instância que foi instalada, mas não ativada é **To be activated**. ● Creating Depois de ativar uma instância, o sistema alocará a instância para você de acordo com sua configuração. A instância está no status de **Creating** durante este processo. ● Creation failed Devido a recursos insuficientes ou falhas de rede, uma instância pode falhar ao ser criada. Neste caso, a instância estará no status de **Creation failed**. ● Running Depois que uma instância for configurada e alocada, ela estará no status de **Running**. ● Frozen Se uma instância não for renovada após sua expiração, seu status será alterado para **Frozen**.
Service Edition	Edição Platinum: você pode usar exclusivamente o subrack do HSM, a fonte de energia, a largura de banda da rede e os recursos da API do HSM.
AZ	AZ de um dispositivo
Device Vendor	Nome do fornecedor do dispositivo.
Device Model	Modelo do dispositivo
IP Address	Endereço IP flutuante da instância do HSM dedicado
Expiration Time	Tempo de expiração da instância de HSM comprada.

Passo 6 Você pode clicar no nome de uma instância do HSM dedicado para exibir detalhes sobre a instância, conforme mostrado na **Figura 4-7**.

Figura 4-7 Detalhes sobre instâncias do HSM dedicado



Para obter mais informações, consulte **Tabela 4-6**.

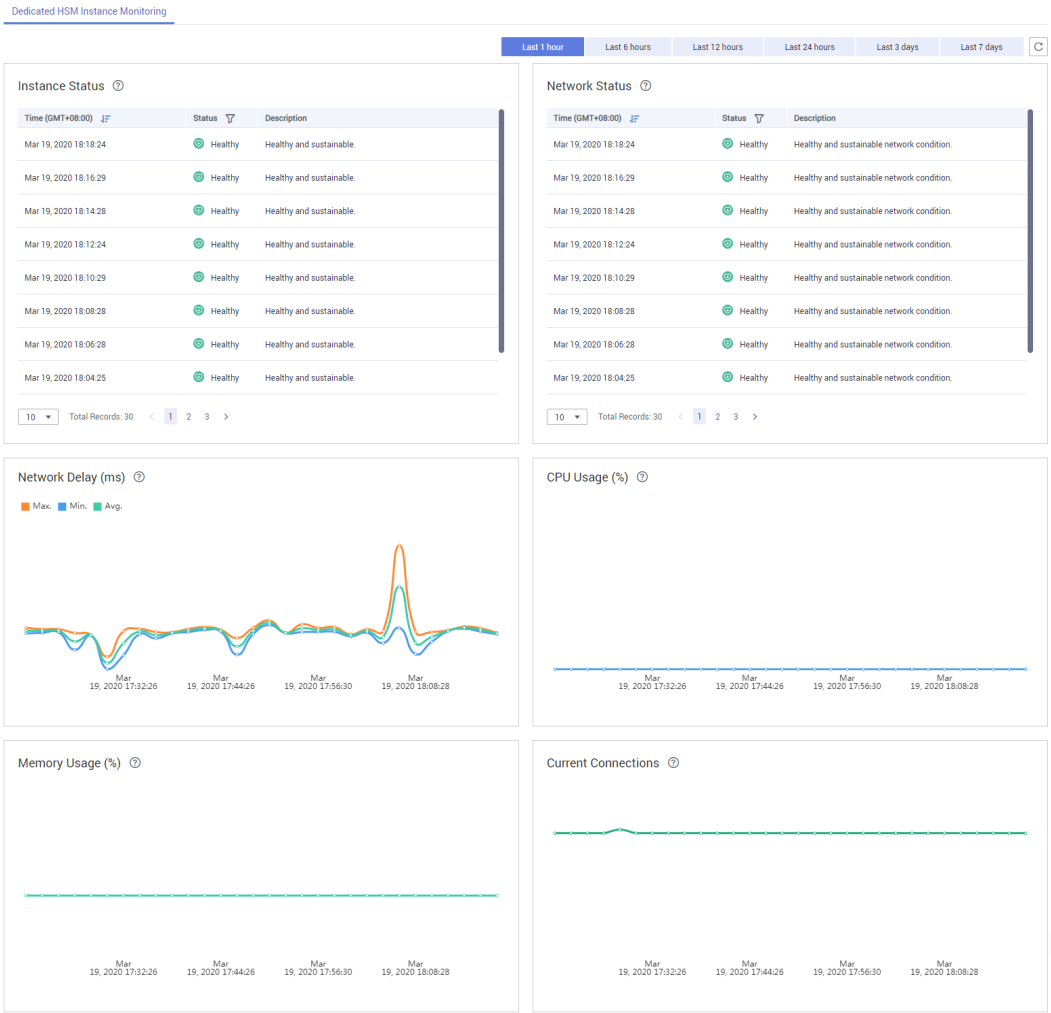
Tabela 4-6 Descrição do parâmetro

Parâmetro	Descrição
Name	Nome de uma instância do HSM dedicado
ID	ID de uma instância
Status	Status de uma instância do HSM dedicado: ● Installing Depois de pagar a taxa de instalação inicial, a instância comprada será instalada. O status da instância do HSM dedicado será **Installing**. ● To be activated O status de uma instância que foi instalada, mas não ativada é **To be activated**. ● Creating Depois de ativar uma instância, o sistema alocará a instância para você de acordo com sua configuração. A instância está no status de **Creating** durante este processo. ● Creation failed Devido a recursos insuficientes ou falhas de rede, uma instância pode falhar ao ser criada. Neste caso, a instância estará no status de **Creation failed**. ● Running Depois que uma instância for configurada e alocada, ela estará no status de **Running**. ● Frozen Se uma instância não for renovada após sua expiração, seu status será alterado para **Frozen**.
Service Edition	Edição Platinum: você pode usar exclusivamente o subrack do HSM, a fonte de energia, a largura de banda da rede e os recursos da API do HSM.
Device Vendor	Nome do fornecedor do dispositivo.
Device Model	Modelo do dispositivo

Parâmetro	Descrição
HSM Type	Tipos de função de uma instância, incluindo **Finance**, **Server** e **Signature Server**.
VPC	VPC à qual a instância pertence Para obter mais informações sobre a VPC, consulte *Guia de usuário do Virtual Private Cloud*.
Subnet	Sub-rede onde a instância está localizada. Para obter mais informações sobre sub-redes, consulte *Guia de usuário do Virtual Private Cloud*.
IP Address	Endereço IP flutuante da instância do HSM dedicado
Security Group (SG)	Grupo de segurança ao qual a instância pertence Para obter mais informações sobre grupos de segurança, consulte *Guia de usuário do Virtual Private Cloud*.
Creation Time	Hora em que a instância é comprada
Expiration Time	Hora em que a instância expira
Order	ID do pedido da instância. Você pode clicar no número do pedido para consultar os detalhes do pedido.
Billing Mode	Pacote pré-pago anual/mensal

Passo 7 Visualize as informações de monitoramento sobre a instância do HSM dedicado, incluindo a integridade da instância, a integridade da rede, a latência da rede, o uso da CPU, o uso da memória e o número de conexões atuais.

Figura 4-8 Monitoramento de instâncias do HSM dedicado



----Fim

4.4 Usar instâncias do HSM dedicado

Após a conclusão do pagamento, aguarde o envio de Ukey usada para inicializar a instância do HSM dedicado para o seu endereço de e-mail. Um especialista em serviços do HSM dedicado também entrará em contato com você e enviará documentos e software relacionados, incluindo a ferramenta usada para gerenciar instâncias do HSM dedicado e o agente de segurança e o SDK usados para chamadas de serviço.

Pré-requisitos

Depois de configurar uma instância do HSM dedicado, você precisa inicializá-la, instalar o agente de segurança e conceder permissões de acesso. As seguintes informações são necessárias.

Tabela 4-7 Informação necessária

Item	Descrição	Como obter
Ukey	Armazena as informações de gerenciamento de permissão sobre a instância.	Depois que o pedido for pago e a instância do HSM dedicado for configurada, o Ukey será enviada para o endereço de e-mail do destinatário fornecido.
Ferramenta de gerenciamento de instância do HSM dedicado	Funciona com o UKey para gerenciar instâncias remotamente.	Um especialista em serviços também entrará em contato com você e enviará documentos e softwares relacionados.
Documentos de instância do HSM dedicado	*Manual de usuário da instância do HSM dedicado* e *Guia de instalação da instância do HSM dedicado*	
Software de agente de segurança	Estabelece uma conexão segura com a instância.	
SDK	Fornece APIs para o HSM dedicado. Você pode usar o SDK para estabelecer conexões seguras com instâncias.	
Nó de gerenciamento de instâncias do HSM dedicado (por exemplo, um ECS)	Execute a ferramenta de gerenciamento de instâncias do HSM dedicado, que está na mesma VPC em que a instância do HSM dedicado reside, e aloque endereços IP elásticos para conexões remotas.	Compre ECSs conforme necessário. Para obter detalhes, consulte **Compra de um ECS**.
Nós da aplicação de serviço (por exemplo, ECSs)	Execute o software do agente de segurança e as aplicações de serviço dos usuários, que devem estar na VPC onde a instância do HSM dedicado está implementada.	

Inicializar uma instância do HSM dedicado

NOTA

No momento, não é possível efetuar logon em instâncias do HSM dedicado via SSH. Você precisa usar a ferramenta de gerenciamento de instâncias do HSM dedicado para gerenciar as instâncias.

Suponha que você deseja usar um ECS do Windows como o nó de gerenciamento de instâncias do HSM dedicado. Execute as seguintes etapas para inicializar a instância do HSM dedicado:

Passo 1 Adquira um ECS do Windows como o nó de gerenciamento de instâncias do HSM dedicado.

1. Faça logon no console de gerenciamento.
2. Clique em . Escolha **Computing** > **Elastic Cloud Server**.
3. Clique em **Buy ECS**.
   - Defina **Region** e **AZ** como os mesmos da instância do HSM dedicado que você comprou.
   - Defina **Image** como uma imagem pública do Windows.
   - Defina a **VPC** como a VPC à qual pertence a instância do HSM dedicado.
   - Configure o **EIP**. Ele permite que você configure localmente instâncias de HSM convenientemente.

     NOTA

     Depois que a instância do HSM dedicado for inicializada, você poderá desvincular o endereço IP elástico. As operações de encadernação e desvinculação podem ser realizadas sempre que necessário.
   - Defina outros parâmetros com base nos requisitos do site.

Passo 2 Inicialize a instância do HSM dedicado usando a ferramenta de gerenciamento recebida e os documentos relacionados.

Passo 3 Após a conclusão da inicialização, você pode usar a ferramenta de gerenciamento para gerar, destruir, fazer backup e restaurar chaves.

NOTA

Se você tiver alguma dúvida durante a inicialização e o gerenciamento, consulte o especialista em serviço do HSM dedicado.

Para obter mais informações, consulte os documentos sobre instância do HSM dedicado: *manual de usuário da instância do HSM dedicado* e *Guia de instalação da instância do HSM dedicado*.

----Fim

Instalar o agente de segurança e conceder permissões de acesso

Você precisa instalar o agente de segurança em um nó de aplicação de serviço para estabelecer um canal seguro para a instância do HSM dedicado.

Passo 1 Faça download do certificado para acessar a instância do HSM dedicado a partir da ferramenta de gerenciamento.

Passo 2 Instale o agente de segurança no nó da aplicação de serviço.

Passo 3 Importe o certificado para o agente de segurança. Conceda à aplicação de serviço a permissão para acessar a instância do HSM dedicado.

Passo 4 A aplicação de serviço pode acessar a instância do HSM dedicado por meio de SDK ou APIs.

NOTA

Você pode configurar várias instâncias do HSM dedicado no agente de segurança para equilibrar cargas.

----Fim

5 Registros de auditoria

5.1 Operações suportadas pelo CTS

Tabela 5-1 lista as operações do DEW que são registradas pelo CTS.

Tabela 5-1 Operações do DEW suportadas pelo CTS

Operação	Tipo de recurso	Nome do rastreamento
Criação de chave	cmk	createKey
Criação da chave de dados	cmk	createDatakey
Criação de chave de dados sem texto não criptografado	cmk	createDatakeyWithoutPlaintext
Ativação da chave	cmk	enableKey
Desativação da chave	cmk	disableKey
Criptografia de chave de dados	cmk	encryptDatakey
Descriptografia da chave de dados	cmk	decryptDatakey
Exclusão de chave agendada	cmk	scheduleKeyDeletion
Cancelamento da exclusão de chave agendada	cmk	cancelKeyDeletion
Geração de números aleatórios	rng	genRandom
Atualização do alias de chave	cmk	updateKeyAlias
Atualização da descrição da chave	cmk	updateKeyDescription
Alerta de risco de exclusão de chave	cmk	deleteKeyRiskTips

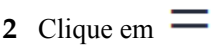
Operação	Tipo de recurso	Nome do rastreamento
Importação de material de chave	cmk	importKeyMaterial
Exclusão de material de chave	cmk	deleteImportedKeyMaterial
Criação de autenticação	cmk	createGrant
Conceder desativação	cmk	retireGrant
Conceder revogação	cmk	revokeGrant
Criptografia de dados	cmk	encryptData
Descriptografia de dados	cmk	decryptData
Adição de tags	cmk	dealUnifiedTags
Exclusão de tags	cmk	dealUnifiedTags
Adição de tags em lote	cmk	dealUnifiedTags
Exclusão de tags em lote	cmk	batchDeleteKeyTags
Criação e importação de par de chaves SSH	par de chaves	createOrImportKeypair
Exclusão de par de chaves SSH	keypair	deleteKeypair
Importação de chave privada	keypair	importPrivateKey
Exportação de chave privada	keypair	exportPrivateKey
Compra de uma instância de DDM	hsm	purchaseHsm
Configuração de uma instância do HSM	hsm	createHsm
Exclusão de uma instância do HSM	hsm	deleteHsm

5.2 Usar o CTS para consultar rastreamentos da operação de DEW

Quando o CTS estiver habilitado, o sistema começará a gravar as operações no KMS. Os registros da operação para os últimos 7 dias são armazenados no console do CTS.

Exibir logs de auditoria do DEW

Passo 1 Faça logon no console de gerenciamento.

Passo 2 Clique em  . Em **Management & Governance**, clique em **Cloud Trace Service**.

Passo 3 Na página exibida, você pode consultar rastreamentos definindo os critérios de filtragem. Os seguintes quatro filtros estão disponíveis:

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

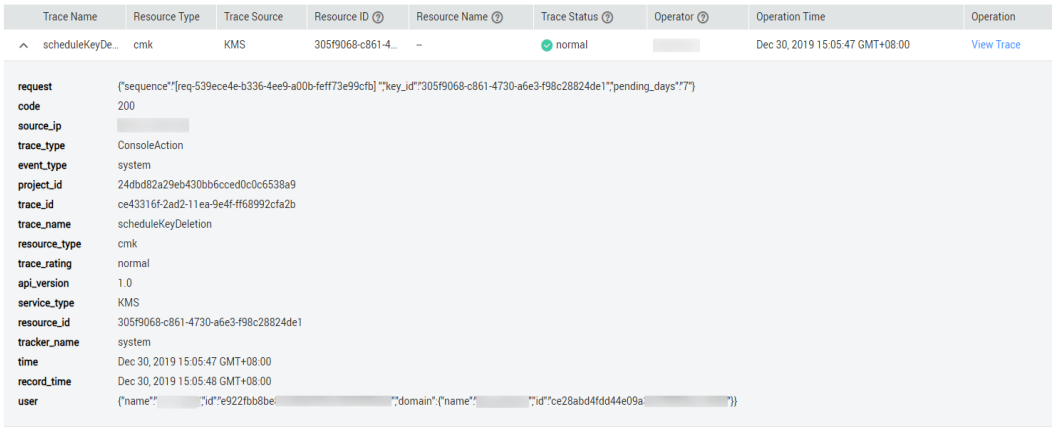
  Selecione o filtro na lista suspensa.

  - Defina **Trace Type** como **Management**.
  - Defina **Trace Source** como **KMS**.
  - Ao selecionar **Trace name** para **Search By**, você também precisa selecionar um nome de rastreamento específico. Quando você seleciona **Resource ID** para **Search By**, também precisa selecionar ou inserir um ID de recurso específico. Ao selecionar **Resource name** para **Search By**, você também precisa selecionar ou inserir um nome de recurso específico.
- **Operator**: selecione um operador específico (um usuário em vez de locatário).
- **Trace Rating**: os valores disponíveis são **All trace statuses**, **normal**, **warning**, e **incident**. Você só pode selecionar um deles.
- **Time Range**: no canto superior direito da página, você pode consultar rastreamentos na última hora, no último dia, na última semana ou dentro de um período personalizado.

Passo 4 Clique em **Search** para exibir o evento de operação correspondente.

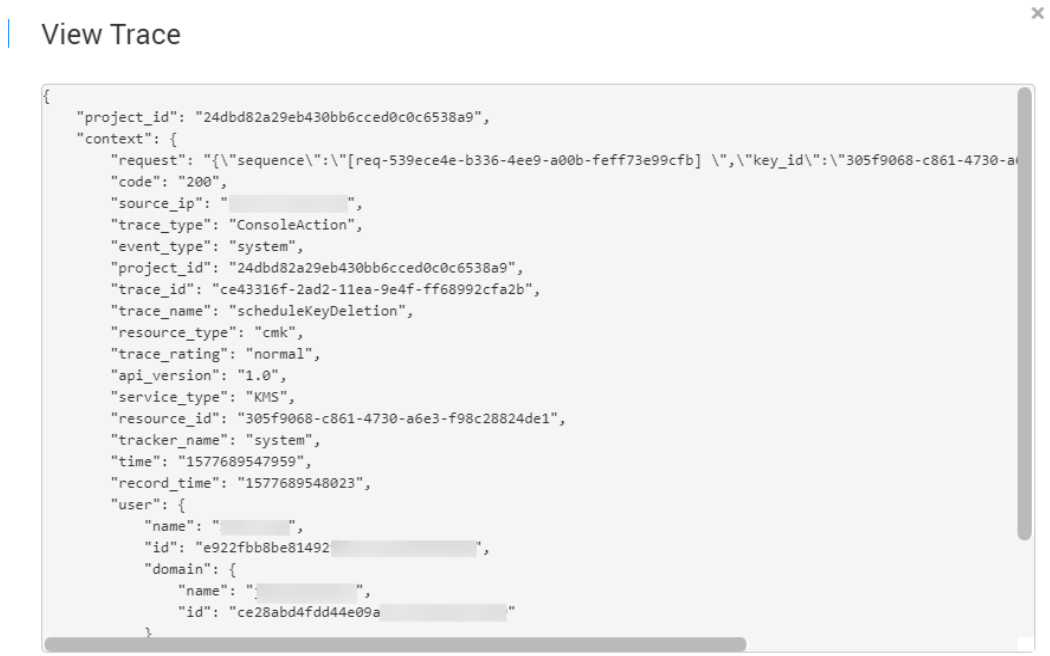
Passo 5 Clique em ⌄ no lado esquerdo de um rastreamento para ver seus detalhes. Consulte **Figura 5-1**.

Figura 5-1 Expansão de detalhes do rastreamento



Passo 6 Clique em **View Trace** na coluna **Operation**. Na caixa de diálogo **View Trace** exibida em **Figura 5-2**, os detalhes da estrutura de rastreamento são exibidos.

Figura 5-2 Exibição de rastreamentos



----Fim

6 Controle de permissão

6.1 Criar um usuário e autorizar o usuário a acessar o DEW

Este capítulo descreve como usar o **IAM** para implementar o controle de permissões refinado para seus recursos DEW. Com o IAM, você pode:

- Criar usuários do IAM para funcionários com base na estrutura organizacional da sua empresa. Cada usuário do IAM tem suas próprias credenciais de segurança para acessar os recursos do DEW.
- Conceder aos usuários somente as permissões necessárias para executar uma tarefa.
- Delegar uma conta confiável da HUAWEI CLOUD ou um serviço em nuvem para realizar O&M profissional e eficiente em seus recursos do DEW.

Se sua conta da HUAWEI CLOUD não exigir usuários individuais do IAM, pule este capítulo.

Esta seção descreve o procedimento para conceder permissões (consulte **Figura 6-1**).

Pré-requisitos

Antes de autorizar permissões para um grupo de usuários, você precisa saber quais permissões do DEW podem ser adicionadas ao grupo de usuários. **Tabela 6-1** lista as políticas do sistema do DEW.

Para as políticas de sistema de outros serviços, consulte **Permissões do sistema**.

Tabela 6-1 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

Nome da função/ política	Descrição	Tipo	Dependência
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 6-2 descreve as operações comuns suportadas por cada permissão definida pelo sistema de DEW. Selecione as permissões conforme necessário.

Tabela 6-2 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
Desativar uma chave	√	√	x	x
Agendar exclusão de chave	√	√	x	x
Cancelar a exclusão da chave agendada	√	√	x	x
Modificar um alias de chave	√	√	x	x
Modificar descrição da chave	√	√	x	x

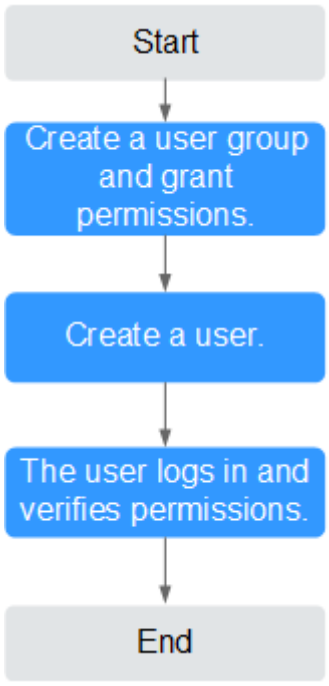
Operação	KMS Administrator	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
Gerar um número aleatório	√	√	x	x
Criar uma DEK	√	√	x	x
Criar uma DEK sem texto não criptografado	√	√	x	x
Criptografar uma DEK	√	√	x	x
Descriptografar uma DEK	√	√	x	x
Obter parâmetros para importar uma chave	√	√	x	x
Importar materiais de chave	√	√	x	x
Excluir materiais de chave	√	√	x	x
Criar uma concessão	√	√	x	x
Revogar uma concessão	√	√	x	x
Retirar uma concessão	√	√	x	x
Consultar a lista de concessões	√	√	x	x
Consultar concessões removível	√	√	x	x
Criptografar dados	√	√	x	x
Descriptografar dados	√	√	x	x

Operação	KMS Administrator	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
Enviar mensagens de assinatura	√	√	x	x
Autenticar assinatura	√	√	x	x
Ativar a rotação de chaves	√	√	x	x
Modificar 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
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

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

Processo de autorização

Figura 6-1 Autorizar a permissão de acesso do DEW a um usuário



1. **Criar um grupo de usuários e atribuir permissões.**

   Crie um grupo de usuários no console do IAM e conceda ao grupo de usuários a permissão **KMS CMKFullAccess** (indicando permissões completas para chaves).

2. **Crie um usuário e adicione-o a um grupo de usuários.**

   Crie um usuário no console do IAM e adicione o usuário ao grupo de usuários criado em **1**.

6.2 Criação de uma política de DEW personalizada

Políticas personalizadas podem ser criadas como um complemento às políticas do sistema do DEW. Para obter detalhes sobre as ações suportadas por políticas personalizadas, consulte **Políticas de permissões e ações suportadas**

Você pode criar políticas personalizadas de uma das seguintes maneiras:

- Editor visual: você pode selecionar configurações de política sem a necessidade de conhecer a sintaxe da política.

  Parâmetros de política do KMS personalizados:

  - **Select service**: selecione **Key Management Service**.
  - **Select action**: configure-o conforme necessário.
  - **(Optional) Select resource**: defina **Resources** como **Specific** e **KeyId** como **Specify resource path**. Na caixa de diálogo exibida, defina **Path** como o ID gerado quando a chave foi criada. Para obter detalhes sobre como obter a ID, consulte "Visualização de uma CMK".

- JSON: edite políticas de JSON do zero ou com base em uma política existente. Para obter detalhes sobre como criar políticas personalizadas, consulte **Criação de uma política personalizada**.

Exemplo de políticas personalizadas

- Exemplo: autorizar usuários a criar e importar chaves

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:cmk:create",
                "kms:cmk:getMaterial",
                "kms:cmkTag:create",
                "kms:cmkTag:batch",
                "kms:cmk:importMaterial"
            ]
        }
    ]
}
```

- Exemplo: negar a exclusão de tags de chave

  Uma política de negação deve ser usada em conjunto com outras políticas para ter efeito. Se as permissões atribuídas a um usuário contiverem ações Allow e Deny, as ações Deny terão precedência sobre as ações Allow.

  O método a seguir pode ser usado se você precisar atribuir permissões da política de **KMS Administrator** a um usuário, mas também proibir que o usuário exclua tags de chave (**kms:cmkTag:delete**). Crie uma política personalizada com a ação de excluir tags de chave, defina seu **Effect** como **Deny** e atribua essa política e as políticas do **KMS Administrator** ao grupo ao qual o usuário pertence. Em seguida, o usuário pode executar todas as operações, exceto a exclusão de tags de chave. O seguinte é uma política para negar tags de par de chaves.

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "kms:cmkTag:delete"
            ]
        }
    ]
}
```

- Exemplo: autorizar usuários a usar chaves

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:dek:crypto",
                "kms:cmk:get",
                "kms:cmk:crypto",
                "kms:cmk:generate",
                "kms:cmk:list"
            ]
        }
    ]
}
```

- Exemplo: política de multi-ação

Uma política personalizada pode conter as ações de vários serviços que todos são do tipo global ou de nível de projeto. O que se segue é uma política com várias declarações:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "rds:task:list"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:dek:crypto",
                "kms:cmk:get",
                "kms:cmk:crypto",
                "kms:cmk:generate",
                "kms:cmk:list"
            ]
        }
    ]
}
```


A História de mudanças

Lançado em	Descrição
17/12/2021	Este é o vigésimo sétimo lançamento oficial. Modificação das seguintes seções: ● Em **Criação de CMKs usando materiais importados de chave**, chaves assimétricas podem ser importadas. ● Em **Exclusão de materiais de chave**, os materiais de chave de chaves assimétricas não podem ser excluídos diretamente.
26/10/2021	Este é o vigésimo sexto lançamento oficial. Adição de **Serviço de gerenciamento de segredo em nuvem**.
30/09/2021	Este é o vigésimo quinto lançamento oficial. ● Adição de descrição sobre algoritmos criptográficos chineses em **Criação de uma CMK**. ● Adição de descrição sobre algoritmos criptográficos chineses em **Criação de CMKs usando materiais importados de chave**. ● Atualização das capturas de tela em **Gerenciamento de pares de chaves**.
30/08/2021	Este é o vigésimo quarto lançamento oficial. Mudança da edição profissional para a edição de platina.

Lançado em	Descrição
20/07/2021	Este é o vigésimo terceiro lançamento oficial. ● Mudança da entrada do DEW de **Security** para **Security and Compliance**. ● Modificação do procedimento de criação de chave e capturas de tela em **Criação de uma CMK**. ● Otimização de conteúdo e atualização de capturas de tela em **Gerenciamento de CMKs**. ● Otimização da descrição de pares de chaves em **Gerenciamento de pares de chaves**. ● Adição de descrição sobre tipos de chave em **Tipos de chaves**. ● Otimização de operações em **Gerenciamento de chaves privadas**. ● Otimização de operações em **HSM dedicado**.
30/06/2021	Este é o vigésimo segundo lançamento oficial. ● Adição de **Adição de uma chave a um projeto**. ● Adição de restrições em **Vinculação de um par de chaves**. ● Atualização das capturas de tela em **Gerenciamento de CMKs**.
22/02/2021	Este é o vigésimo primeiro lançamento oficial. Modificação de **Creating a Dedicated HSM Instance**.
21/12/2020	Este é o vigésimo lançamento oficial. Otimização de seções neste documento.
14/12/2020	Este é o décimo nono lançamento oficial. Modificação de **Criação de uma CMK**.
25/09/2020	Este é o décimo oitavo lançamento oficial. Modificação de **Creating a Dedicated HSM Instance**.
24/08/2020	Este é o décimo sétimo lançamento oficial. Adição da descrição sobre como obter o KeyId em **Criação de uma política de DEW personalizada**.

Lançado em	Descrição
12/08/2020	Este é o décimo sexto lançamento oficial. ● Adição de **Atualização de um par de chaves**. ● Atualização das capturas de tela em **Criação de um par de chaves**. ● Atualização das capturas de tela em **Importação de um par de chaves**. ● Atualização das capturas de tela em **Visualização de um par de chaves**. ● Atualização de capturas de tela e adição de descrições em **Exclusão de um par de chaves**. ● Atualização de capturas de tela e adição de descrições em **Importação de uma chave privada**. ● Atualização de capturas de tela e adição de descrições em **Exportação de uma chave privada**. ● Atualização de capturas de tela e adição de descrições em **Limpeza de uma chave privada**.
14/07/2020	Este é o décimo quinto lançamento oficial. ● Adição de **Criação de CMKs usando materiais importados de chave**. ● Adição da descrição sobre as funções do projeto empresarial em **Criação de uma CMK**, **Criação de CMKs usando materiais importados de chave** e **Visualização de uma CMK**.
07/04/2020	Este é o décimo quarto lançamento oficial. Atualização das capturas de tela.
10/02/2020	Este é o treze lançamento oficial. Modificação de **Controle de permissão**.
09/08/2019	Este é o décimo segundo lançamento oficial. Modificação de seção **Serviço de gerenciamento de chaves**: atualização de capturas de tela.
19/07/2019	Este é o décimo primeiro lançamento oficial. ● Adição de **Ativação de uma instância do HSM dedicado**. ● Adição de **Exibição de instâncias do HSM dedicado**.
12/07/2019	Este é o décimo lançamento oficial. Adição de **Compra de uma instância do HSM dedicado**.

Lançado em	Descrição
04/07/2019	Este é o nono lançamento oficial. ● Adição do método de visualização de registros de uso de chave em **Agendamento da exclusão de uma ou mais CMKs**. ● Modificação de seção **Serviço de par de chaves**: atualização de capturas de tela. ● Adição de **Usar instâncias do HSM dedicado**. ● Adição dos tipos de recursos e nomes de eventos de compra, configuração e exclusão de uma instância do HMS à tabela "Operações do DEW suportadas pelo CTS".
22/04/2019	Este é o oitavo lançamento oficial. Otimização do fluxograma e os gráficos de arquitetura.
25/10/2018	Este é o sétimo lançamento oficial. Modificação de seção **Visualização de um par de chaves**: adição da descrição sobre a página que exibe detalhes de pares de chaves.
30/08/2018	Este é o sexto lançamento oficial. ● Adição de **HSM dedicado**. ● Adição da seção "Criptografia do seu sistema de serviço usando HSM dedicado". ● Adição de **Usar instâncias do HSM dedicado**.
05/07/2018	Este é o quinto lançamento oficial. ● Modificação de seção **Criação de uma CMK**: adição do procedimento para adicionar uma tag. ● Atualização de capturas de tela.
30/05/2018	Este é o quarto lançamento oficial. ● Adição de **Vinculação de um par de chaves**. ● Adição de **Desvinculação de um par de chaves**. ● Adição de **Redefinição de um par de chaves**. ● Adição de **Substituição de um par de chaves**. ● Adição da descrição sobre a exclusão de registros de falha em **Visualização de um par de chaves**. ● Modificação de seção **Visualização de um par de chaves**: adição da descrição sobre a lista de ECSs vinculados a pares de chaves.

Lançado em	Descrição
30/04/2018	Este é o terceiro lançamento oficial. ● Adição de **Adição de uma tag**. ● Adição da seção "Procura por tags". ● Adição de **Modificação de valores de tag**. ● Adição de **Exclusão de tags**. ● Atualização de capturas de tela.
30/01/2018	Este é o segundo lançamento oficial. ● Adição da seção "Par de chaves SSH". ● Adição de **Criação de um par de chaves**. ● Adição de **Importação de um par de chaves**. ● Adição de **Visualização de um par de chaves**. ● Adição de **Exclusão de um par de chaves**.
31/12/2017	Este é o primeiro lançamento oficial.