Data Encryption Workshop

Guia de usuário do

Edição 34

Data 2024-09-14

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
1.1 Tipos de chaves....1
1.2 Criação de uma chave....2
1.3 Criação de CMKs usando materiais importados de chave....6
1.3.1 Visão geral....7
1.3.2 Importação de materiais de chave....8
1.3.3 Exclusão de materiais de chave....16
1.4 Gerenciamento de CMKs....17
1.4.1 Visualização de uma CMK....17
1.4.2 Ativação de uma ou mais CMKs....19
1.4.3 Desativação de uma ou mais CMKs....20
1.4.4 Exclusão de uma ou mais CMKs....21
1.4.5 Cancelamento da exclusão programada de uma ou mais CMKs....22
1.4.6 Adição de uma chave a um projeto....23
1.5 Pesquisa de uma chave....24
1.6 Uso da ferramenta on-line para criptografar e descriptografar dados de tamanho pequeno....25
1.7 Gerenciamento de tags....27
1.7.1 Adição de uma tag....27
1.7.2 Modificação de valores de tag....29
1.7.3 Exclusão de tags....29
1.8 Rotação de CMKs....30
1.8.1 Sobre a rotação de chaves....30
1.8.2 Ativação da rotação de chaves....32
1.8.3 Desativação da rotação de chaves....35
1.9 Managing a Grant....36
1.9.1 Criação de uma concessão....36
1.9.2 Consulta de uma concessão....40
1.9.3 Revogação de uma concessão....41
2 Serviço de gerenciamento de segredo em nuvem....43
2.1 Visão geral do segredo....43
2.2 Política de rotação....45
2.3 Criação de um segredo....45
2.3.1 Criação de um segredo compartilhado....45

2.4 Gerenciamento de segredos.....48
2.4.1 Visualização de um segredo.....48
2.4.2 Exclusão de um segredo.....49
2.5 Gerenciamento de versões de segredos.....51
2.5.1 Salvamento e visualização de valores de segredos.....51
2.5.2 Gerenciamento de status de versão de segredo.....52
2.5.3 Definição do tempo de expiração da versão.....53
2.5.4 Versão de segredos de rotação.....54
2.6 Gerenciamento de tags.....56
2.6.1 Adição de uma tag.....56
2.6.2 Pesquisa de um segredo por tag.....58
2.6.3 Modificação de um valor de tag.....59
2.6.4 Exclusão de uma tag.....59
3 Serviço de par de chaves.....61
3.1 Criação de um par de chaves.....61
3.2 Importação de um par de chaves.....66
3.3 Atualização de um par de chaves.....70
3.4 Gerenciamento de pares de chaves.....71
3.4.1 Vinculação de um par de chaves.....71
3.4.2 Vinculação de pares de chaves em lotes.....74
3.4.3 Visualização de um par de chaves.....77
3.4.4 Redefinição de um par de chaves.....79
3.4.5 Substituição de um par de chaves.....80
3.4.6 Desvinculação de um par de chaves.....82
3.4.7 Exclusão de um par de chaves.....85
3.5 Gerenciamento de chaves privadas.....85
3.5.1 Importação de uma chave privada.....85
3.5.2 Exportação de uma chave privada.....87
3.5.3 Limpeza de uma chave privada.....89
3.6 Uso de uma chave privada para fazer logon no ECS do Linux.....89
3.7 Uso de uma chave privada para obter a senha de logon do ECS de Windows.....92
4 HSM dedicado.....94
4.1 Guia de operação.....94
4.2 Compra de uma instância do HSM dedicado.....96
4.2.1 Criação de uma instância do HSM dedicado.....96
4.2.2 Ativação de uma instância do HSM dedicado.....99
4.3 Exibição de instâncias do HSM dedicado.....103
4.4 Gerenciamento de tags.....106
4.4.1 Adição de uma tag.....106
4.4.2 Pesquisa de uma instância do HSM dedicado por tag.....108
4.4.3 Modificação de um valor de tag.....109
4.4.4 Exclusão de uma tag.....110

4.5 Uso de instâncias do HSM dedicado 111

5 Registros de auditoria 114

5.1 Operações suportadas pelo CTS 114

5.2 Uso do CTS para consultar rastreamentos da operação do DEW 117

6 Controle de permissão 118

6.1 Criação de um usuário e autorização ao usuário a permissão para acessar o DEW 118

6.2 Criação de uma política de DEW personalizada 124

1 Serviço de gerenciamento de chaves

1.1 Tipos de chaves

As CMKs incluem chaves personalizadas e chaves padrão. Esta seção descreve como criar, visualizar, ativar, desativar, programar a exclusão e cancelar a exclusão de chaves personalizadas.

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

As chaves simétricas são mais comumente usadas para proteção de 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 da chave	Descrição	Uso
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 da chave	Descrição	Uso
Chave simétrica	AES	• HMAC_256 • HMAC_384 • HMAC_512	Chave simétrica de HMAC	Gera e verifica um código de autenticação de mensagem
Chave simétrica	SM3	HMAC_SM3	Chave simétrica de SM3	Gera e verifica um código de autenticação de mensagem
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

1.2 Criação de uma chave

Esta seção descreve como criar uma chave personalizada no console do KMS.

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

Pré-requisitos

A conta tem permissões KMS CMKFullAccess ou superiores.

Restrições

- Você pode criar até 20 chaves personalizadas, excluindo as chaves padrão. As chaves de réplica ocupam a cota de chave personalizada na região.
- As chaves simétricas são criadas usando a chave AES. A chave AES-256 pode ser usada para criptografar e descriptografar uma pequena quantidade de dados ou chaves de dados. A chave HMAC é usada para gerar e verificar códigos de autenticação de mensagens.
- 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 padrão terminam com **/default**. Ao escolher aliases para suas chaves personalizadas, não use aliases terminados com **/default**.

- As chaves do DEW podem ser chamadas por meio de APIs para 20.000 vezes gratuitamente por mês.

Cenários

- **Criptografar dados no OBS**
- **Criptografar dados no EVS**
- **Criptografar dados no IMS**
- **Criptografar uma instância de banco de dados RDS**
- Use chaves personalizadas para criptografar e descriptografar diretamente pequenos volumes de dados.
- Criptografia e descriptografia de DEK para aplicações do usuário
- Geração e verificação do código de autenticação de mensagens
- Chaves assimétricas podem ser usadas para assinaturas digitais e verificação de assinatura.

Criação de uma chave

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

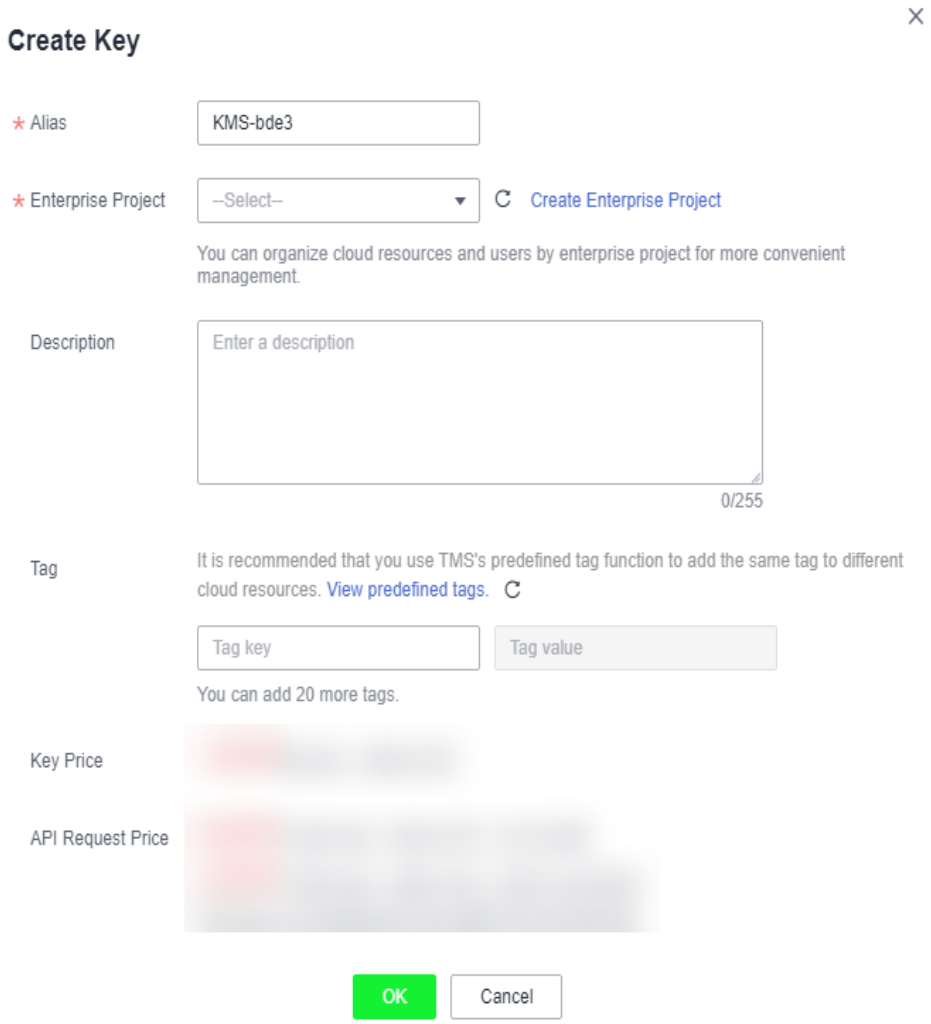
Passo 2 Clique em  no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

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

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

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

Figura 1-1 Criação de uma chave



- **Alias** é o alias da chave 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 da chave	Descrição	Uso
Chave simétrica	AES	AES_256	Chave simétrica de AES	Criptografa e descriptografa uma pequena quantidade de dados ou chaves de dados.
Chave simétrica	AES	– HMAC_256 – HMAC_384 – HMAC_512	Chave simétrica de HMAC	Gera e verifica um código de autenticação de mensagem
Chave simétrica	SM3	HMAC_SM3	Chave simétrica de SM3	Gera e verifica um código de autenticação de mensagem
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**, **ENCRYPT_DECRYPT** ou **GENERATE_VERIFY_MAC**.
  - Para uma chave simétrica AES_256, o valor padrão é **ENCRYPT_DECRYPT**.
  - Para uma chave simétrica HMAC, o valor padrão é **GENERATE_VERIFY_MAC**.
  - 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 chave personalizada.
- O parâmetro **Enterprise Project** precisa ser definido apenas para usuários empresariais.

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

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

NOTA

- Você pode usar projetos empresariais para gerenciar recursos de nuvem e membros do projeto. Para obter mais informações sobre projetos empresariais, consulte **O que é o serviço de gerenciamento de projetos empresariais?**
- Para obter detalhes sobre como ativar a função do projeto empresarial, consulte **Ativação da central empresarial**.

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

NOTA

- Depois de criar uma CMK, você pode clicar no alias da CMK para acessar a página de detalhes da CMK e adicionar uma tag à CMK.
- A mesma tag (incluindo chave de tag e valor de tag) pode ser usada para diferentes chaves personalizadas. No entanto, sob a mesma chave personalizada, uma chave de tag pode ter apenas um valor de tag.
- Um máximo de 20 tags podem ser adicionadas para uma chave personalizada.
- 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 de chaves, você pode exibir a chave criada. O status padrão de uma chave é **Enabled**.

----Fim

Operações relacionadas

- Para obter detalhes sobre como fazer upload de objetos com criptografia no lado do servidor, consulte a seção "Fazer upload de um arquivo com criptografia no lado do servidor" no *Guia de usuário 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 "Criptografia de 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 não criptografado, 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 uma aplicação de usuário, consulte as seções "Criptografia de uma DEK" e "Descriptografia de uma DEK" na *Referência de API do Data Encryption Workshop*.

1.3 Criação de CMKs usando materiais importados de chave

1.3.1 Visão geral

Uma chave personalizada contém metadados de chave (ID da chave, alias da chave, descrição, status da chave e data de criação) e materiais de chaves usados para criptografar e descriptografar dados.

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

Observações importantes

- Segurança

  Você precisa garantir que as fontes aleatórias atendam aos seus requisitos de segurança ao usá-las para gerar materiais de chaves. Ao usar a função de chave de importação, você precisa ser responsável pela segurança de seus materiais de chaves. 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 da chave importado e o material da chave gerado pelo KMS

Fonte de material de chave	Diferença
Chaves importadas	• Você pode excluir o material da chave, mas não pode excluir a chave personalizada e seus metadados. • Tais chaves não podem ser giradas. • 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 em 24 horas, mas não exclui a chave personalizada e seus metadados. Recomenda-se salvar uma cópia do material em seu dispositivo local, pois ela pode ser usada para reimportação em casos de materiais de chaves inválidos ou de exclusão incorreta de materiais de chaves. **NOTA** Chaves usando algoritmos RSA_2048, RSA_3072, RSA_4096, EC_P256 e EC_P384 são permanentemente válidas. Seus materiais de chaves não podem ser excluídos manualmente e seu tempo de expiração não pode ser configurado.

Fonte de material de chave	Diferença
Chaves criadas no KMS	● O material da chave não pode ser excluído manualmente. ● As chaves 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 chave personalizada, a chave personalizada é permanentemente vinculada ao material da chave. Outros materiais de chaves não podem ser importados para a chave personalizada.

- Exclusividade

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

Restrições

- O algoritmo de chave HMAC não suporta a importação de materiais de chave.

Procedimento

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

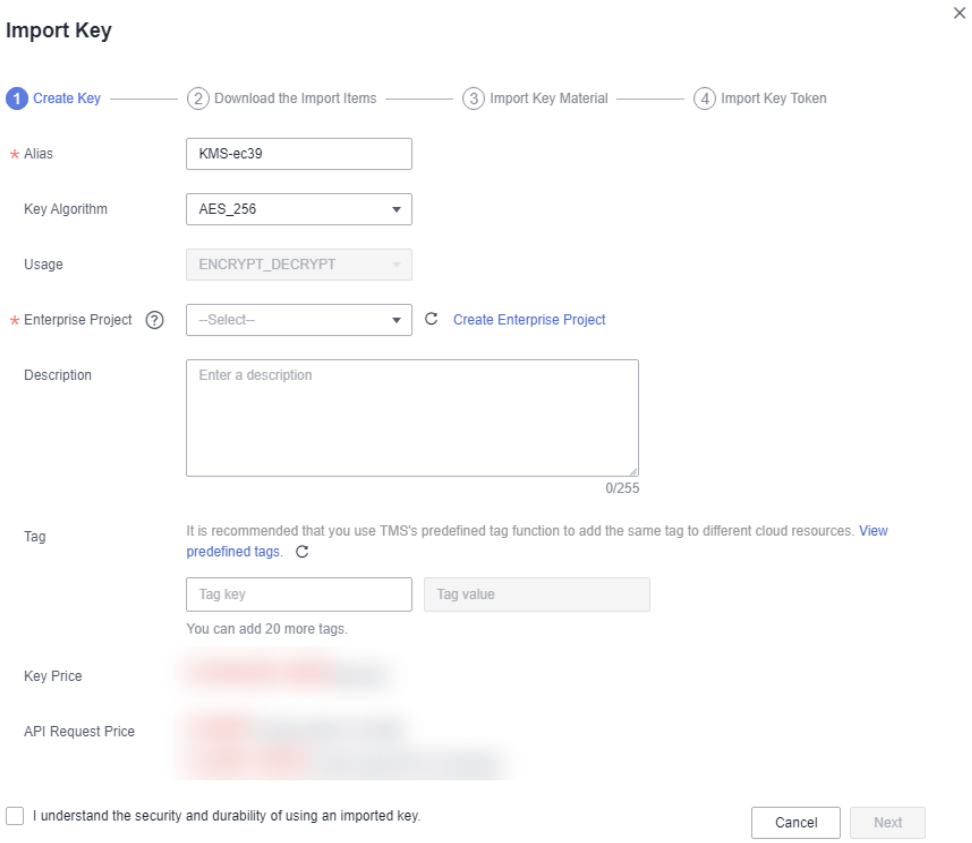
Passo 2 Clique em  no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

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

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

Passo 5 Configure os parâmetros de chaves.

Figura 1-2 Criação de uma chave vazia



- **Alias** é o alias da chave 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 chaves suportados pelo KMS

Tipo de chave	Tipo de algoritmo	Especificações da chave	Descrição	Uso
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 da chave	Descrição	Uso
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**, **ENCRYPT_DECRYPT** ou **GENERATE_VERIFY_MAC**.
  - Para uma chave simétrica AES_256, o valor padrão é **ENCRYPT_DECRYPT**.
  - Para uma chave simétrica HMAC, o valor padrão é **GENERATE_VERIFY_MAC**.
  - 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 chave personalizada.
- O parâmetro **Enterprise Project** precisa ser definido apenas para usuários empresariais.

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

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

  NOTA

  - Você pode usar projetos empresariais para gerenciar recursos de nuvem e membros do projeto. Para obter mais informações sobre projetos empresariais, consulte **O que é o serviço de gerenciamento de projetos empresariais?**
  - Para obter detalhes sobre como ativar a função do projeto empresarial, consulte **Ativação da central empresarial**.

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

NOTA

- Se uma chave personalizada tiver sido criada sem qualquer tag, você poderá adicionar uma tag à chave personalizada mais tarde, conforme necessário. Clique no alias da chave personalizada, 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 chaves personalizadas. No entanto, na mesma chave personalizada, uma chave de tag pode ter apenas um valor de tag.
- Um máximo de 20 tags podem ser adicionadas para uma chave personalizada.
- 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 chave personalizada 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**. Selecione um algoritmo de encapsulamento de chave com base em **Table 4 Key wrapping algorithms**.

Figura 1-3 Obter a chave de encapsulamento e o token de importação

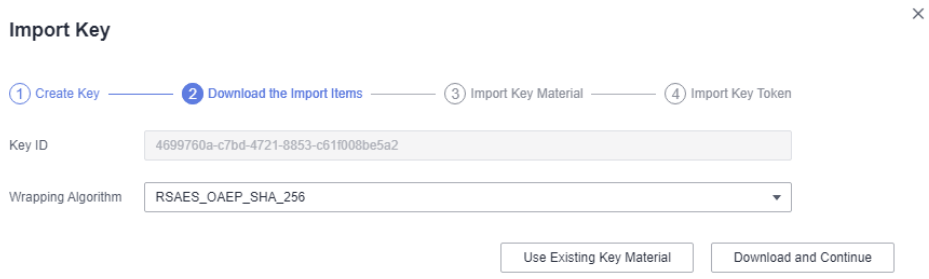


Tabela 1-5 Algoritmos de encapsulamento de chaves

Algoritmo	Descrição	Configuração
RSAES_OAEP_SHA_256	Algoritmo RSA que usa OAEP e tem a função de hash **SHA-256**	Selecione um algoritmo baseado em suas funções de HSM. Se os HSMs oferecerem suporte ao algoritmo **RSAES_OAEP_SHA_256**, use **RSAES_OAEP_SHA_256** para criptografar materiais de chaves.

NOTA

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

Passo 10 Obtenha a chave de encapsulamento e importe o token. Se você já tem um material de chaves, pule esta etapa.

1. Obtenha a chave de encapsulamento e importe o token.
   - Método 1: clique em **Download and Continue**, como mostrado em **Figura 1-4**.

     Figura 1-4 Arquivo baixado

     - **wrappingKey**_*KeyID* é a chave de encapsulamento. É codificada em formato binário e usada para criptografar a chave de encapsulamento do material da chave.
     - Token de importação: você não precisa baixá-lo. O assistente de importação transfere automaticamente o token de importação. Se você fechar o assistente antes de concluir a importação, o token se tornará automaticamente inválido.

     AVISO

     A chave de encapsulamento expira em 24 horas. Se a chave de encapsulamento for inválida, baixe-a novamente.

     O assistente de importação transfere automaticamente o token de importação. Se você fechar o assistente antes de concluir a importação, o token se tornará automaticamente inválido. Para tentar novamente a importação, abra o assistente de importação novamente.

   - Método 2: obtenha a chave de encapsulamento e importe o token chamando APIs.

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

        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: **RSAES_OAEP_SHA_256**).
        - 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
          }
          ```

     ii. 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.

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

2) 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

iii. 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**.

2. Use a chave de encapsulamento para criptografar o material da chave.

NOTA

Depois de executar esta etapa, você obterá um dos seguintes arquivos:

Cenário de chave simétrica: **EncryptedKeyMaterial.bin** (material da chave)

Cenário de chave assimétrica: **EncryptedKeyMaterial.bin** (material de chave temporária) e **out_rsa_private_key.der** (texto cifrado de chave privada)

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

Método 2: use o OpenSSL para gerar um material de chaves e use a chave de encapsulamento baixada para criptografar o material de chaves.

NOTA

Se você precisar executar o comando **openssl pkeyutl**, certifique-se de que sua versão do OpenSSL seja 1.0.2 ou posterior.

a. Gere um material de chaves (chave simétrica de 256 bits) e salve-o como **PlaintextKeyMaterial.bin**.

- Se o algoritmo de chave simétrica AES256 for usado, execute o seguinte comando no cliente onde a ferramenta OpenSSL foi instalada:

  openssl rand -out *PlaintextKeyMaterial.bin* 32

- Se os algoritmos de chave assimétrica RSA e ECC forem usados, execute o seguinte comando no cliente em que a ferramenta OpenSSL foi instalada:

  1) Gere uma chave AES256 hexadecimal.

     openssl rand -out 0xPlaintextKeyMaterial.bin -hex 32

  2) Converta a chave AES256 hexadecimal 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**.

Se a chave de encapsulamento foi baixada do console, substitua ***PublicKey.bin*** no comando a seguir pelo nome da chave de encapsulamento *wrappingKey_keyID*.

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

Algoritmo de chave de encapsulamento	Criptografia de material de chaves
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. (Opcional) Para importar uma chave assimétrica, gere uma chave privada assimétrica, use o material de chave temporária (**EncryptedKeyMaterial.bin**) para criptografar a chave privada e importe o arquivo criptografado como texto cifrado de chave privada.

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

  1) Gere uma chave privada.

     openssl genrsa -out pkcs1_rsa_private_key.pem 4096

  2) Converta o formato para PKCS8.

     openssl pkcs8 -topk8 -inform PEM -in pkcs1_rsa_private_key.pem -outform pem -nocrypt -out rsa_private_key.pem

  3) Converta o formato PKCS8 para o formato DER.

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

  4) 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 ativado no OpenSSL. Para encapsular uma chave, atualize o OpenSSL para a versão mais recente e corrija-o primeiro. Para obter detalhes, consulte Perguntas frequentes.

Passo 11 Se você já tiver o material de chave, clique em **Existing Key Material**. A página **Import Key Material** é exibida.

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

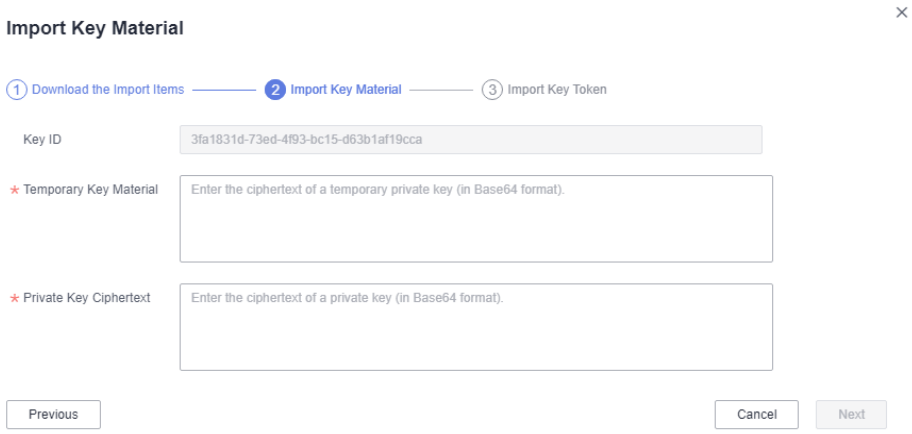
Parâmetro	Descrição
Key ID	ID aleatório de uma CMK gerada durante a criação da CMK

Parâmetro	Descrição
Key material	Importar um material da chave. Por exemplo, use o arquivo **EncryptedKeyMaterial.bin** em **Passo 10.2.b**.

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

Parâmetro	Descrição
Key ID	ID aleatório de uma CMK gerada durante a criação da CMK
Temporary key material	Importar um material de chave temporária. Por exemplo, selecione o arquivo **EncryptedKeyMaterial.bin** em **Passo 10.2.b**.
Private key ciphertext	Selecionar texto cifrado de chave privada. Por exemplo, selecione o arquivo **out_rsa_private_key.der** em **Passo 10.2.c**.

Figura 1-5 Importação de materiais de chave



Passo 12 Clique em **Next** para ir para a etapa **Import Key Token**. Configure os parâmetros conforme descrito em **Tabela 1-9**.

Figura 1-6 Importação de um token de chave

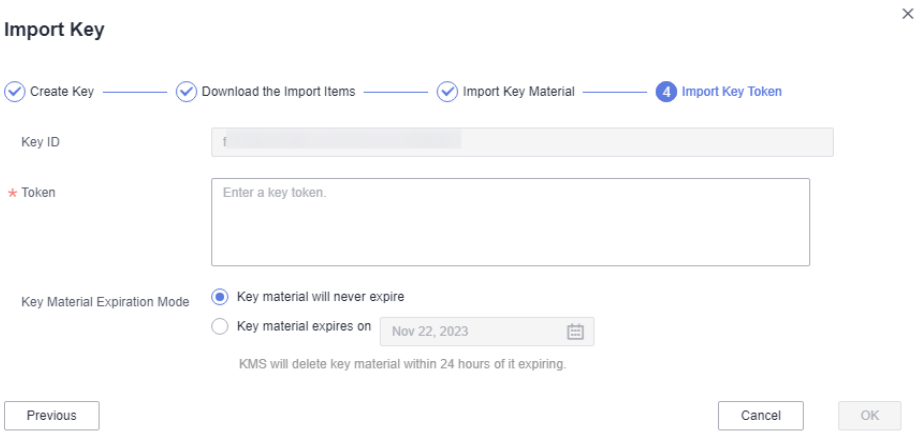


Tabela 1-9 Parâmetros para importar um token de chave

Parâmetro	Descrição
Key ID	ID aleatório de uma CMK gerada durante a criação da CMK
Key import token	Selecione o token de importação obtido via API em **12.b**.
Key material expiration mode	● **Key material will never expire**: use esta opção para especificar que os materiais de chave não expirarão após a importação. ● **Key material will expire**: use essa opção para especificar o tempo de expiração dos materiais de chaves. Por padrão, os materiais de chaves 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 13 Clique em **OK**. Quando a mensagem **Key imported successfully** é exibida no canto superior direito, os materiais são importados.

AVISO

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

Seus 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 chave personalizada 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 importou materiais de chave para uma CMK.
- A fonte de 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 personalizada 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 **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 projeto.

Passo 3 Clique 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 personalizada no console do KMS, incluindo o alias, o status, o ID e o horário de criação da chave. O status de uma chave pode ser **Enabled**, **Disabled**, **Scheduled deletion** ou **Pending import**.

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**.

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

Figura 1-7 Chaves personalizadas

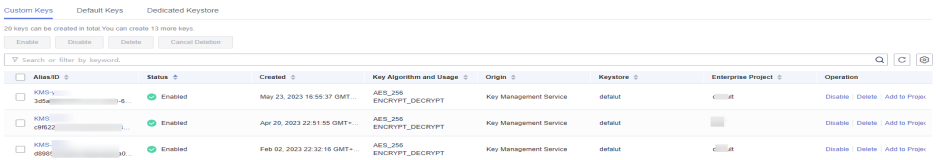


Figura 1-8 Chaves padrão

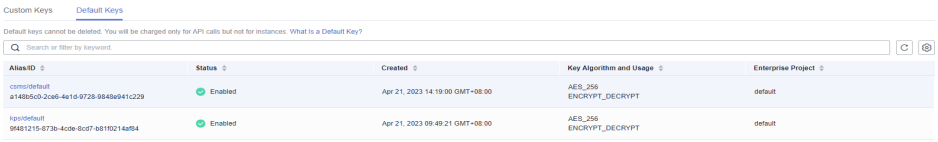


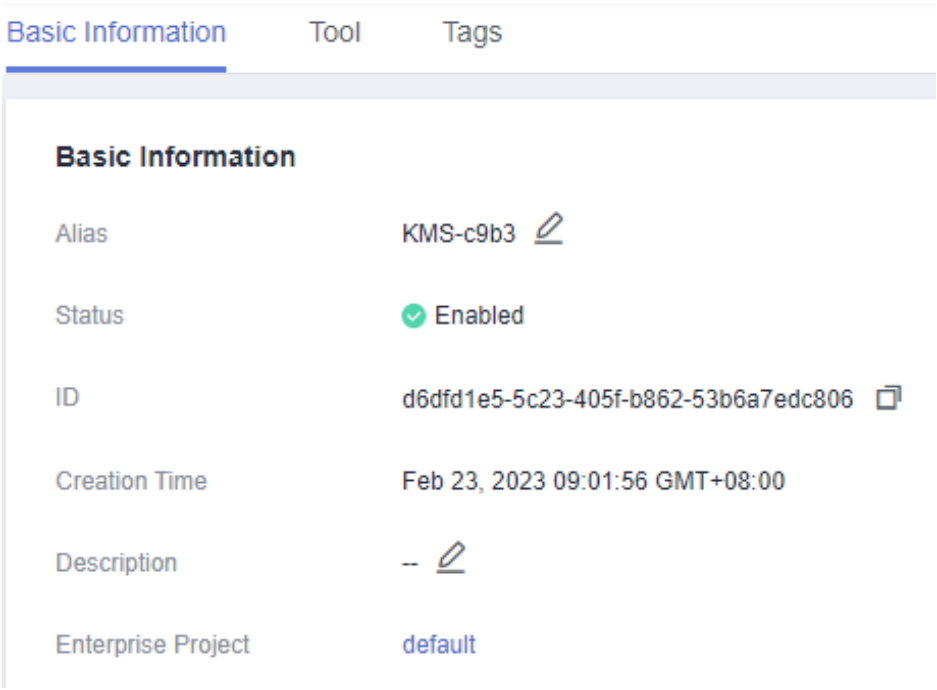
Tabela 1-10 Parâmetros da lista de chaves

Parâmetro	Descrição
Alias/ID	Alias de uma chave e o ID aleatório de uma chave gerada durante sua criação. **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**.
Status	Status de uma CMK, que pode ser um dos seguintes: ● **Enabled** A CMK está ativada. ● **Disabled** A CMK está desativada. ● **Pending deletion** A CMK está programada para exclusão. ● **Pending import** Se sua CMK não tiver materiais, seu status será **Pending import**.
Creation Time	Tempo de criação da CMK
Key Algorithm and Usage	Algoritmo de chave selecionado durante a criação da chave e seu uso

Parâmetro	Descrição
Origin	Fonte do material de chave, que pode ser um dos seguintes: ● **External** A chave é importada para o KMS a partir de um sistema externo. ● **Key Management Service** A chave é uma chave padrão ou criada no KMS.
Enterprise Project	Projeto empresarial para o qual a CMK é usada

Passo 5 Você pode clicar no alias de uma chave para exibir seus detalhes, conforme mostrado na **Figura 1-9**.

Figura 1-9 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 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 chaves personalizadas. Somente chaves personalizadas ativadas podem ser usadas para criptografar ou descriptografar dados. Uma nova chave personalizada está no estado **Enabled** por padrão.

Pré-requisitos

A chave personalizada que você deseja ativar está no status **Disabled**.

Procedimento

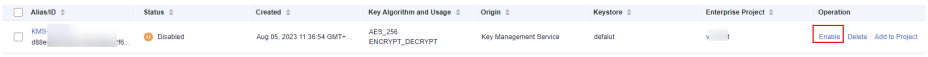
Passo 1 **Faça logon no console de gerenciamento**.

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

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

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

Figura 1-10 Ativação de uma chave



Passo 5 Na caixa de diálogo exibida, clique em **OK** para ativar a chave.

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 chaves personalizadas, protegendo assim os dados em casos urgentes.

Depois de ser desativada, uma chave personalizada não pode ser usada para criptografar ou descriptografar dados. 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

A CMK que você deseja desativar está no status **Enabled**.

Restrições

- As chaves padrão criadas pelo KMS não podem ser desativadas.
- Uma CMK desativada ainda pode ser cobrada. Ela deixará de incorrer em cobranças se for excluída.

Procedimento

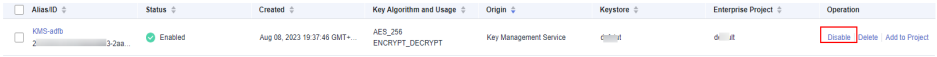
Passo 1 **Faça logon no console de gerenciamento**.

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

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

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

Figura 1-11 Desativação de uma CMK



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

NOTA

Para desativar várias CMKs de uma só vez, selecione-as e clique em **Disable** no canto superior esquerdo da lista.

----Fim

1.4.4 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 de uma das seguintes maneiras:

- Verifique a permissão da CMK para determinar seu escopo de uso possível. Para mais detalhes, consulte **Consulta de uma concessão**.
- Verifique os logs de auditoria para determinar o uso real.

Pré-requisitos

- A chave a ser excluída está no status **Enabled**, **Disabled** ou **Pending import**.

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. Quando a exclusão programada entrar em vigor, a CMK será excluída permanentemente e você não poderá descriptografar dados criptografados pela CMK. Tenha cuidado ao realizar esta operação.
- Para obter detalhes sobre as informações de cobrança sobre uma CMK programada para exclusão, consulte **Uma CMK será cobrada depois de ter sido programada para ser excluída?**
- As chaves padrão criadas pelo KMS não podem ser programadas para exclusão.

Procedimento

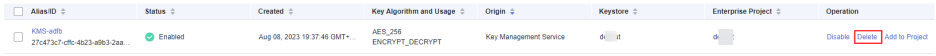
Passo 1 **Faça logon no console de gerenciamento**.

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**.

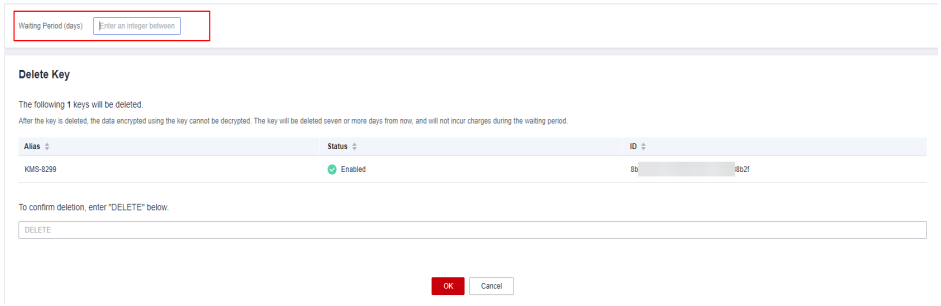
Passo 4 Na linha que contém a CMK desejada, clique em **Delete** na coluna **Operation**.

Figura 1-12 Programação da exclusão de uma CMK



Passo 5 Na caixa de diálogo de exclusão de chave, insira o tempo de atraso de exclusão.

Figura 1-13 Inserir o período após o qual você deseja que a exclusão entre em vigor



NOTA

- 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.
- Para obter detalhes sobre as informações de cobrança sobre uma CMK programada para exclusão, consulte **Uma CMK será cobrada depois de ter sido programada para ser excluída?**

Passo 6 Na caixa de diálogo de confirmação, insira **DELETE** e clique em **OK**. Uma mensagem é exibida, indicando que a tarefa de exclusão de chave foi entregue com sucesso.

Passo 7 Se uma chave for usada para criptografar DDS, RDS ou NoSQL, depois que você clicar em **OK**, uma mensagem "Key *XXX* is being used by *XXX*. Are you sure you want to delete it." é exibida, como mostrado em **Confirmação da exclusão**. Você precisa clicar em **Yes**.

Figura 1-14 Confirmação da exclusão

----Fim

NOTA

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

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 chaves personalizadas antes da execução da exclusão. Após o cancelamento, a chave está no status **Disabled**.

Pré-requisitos

A CMK para a qual você deseja cancelar a exclusão programada está no status **Pending deletion**.

Procedimento

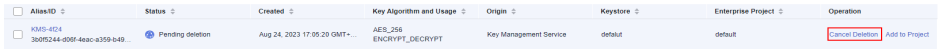
Passo 1 **Faça logon no console de gerenciamento**.

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

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

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

Figura 1-15 Cancelar a exclusão programada de uma CMK



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

- Se uma chave for criada no console do KMS, o status da chave será alterado para **Disabled** após a exclusão programada ser cancelada. Para obter detalhes sobre como ativar a chave, consulte **Ativação de uma ou mais CMKs**.
- Se a CMK for criada usando materiais importados, seu status se tornará **Disabled** após o cancelamento. Para ativar a CMK, consulte **Ativação de uma ou mais CMKs**.
- Se a CMK for criada usando materiais importados e nenhum material de chave tiver sido importado para ela, seu status se tornará **Pending import** após o cancelamento. Para usar a CMK, execute **Criação de CMKs usando materiais importados de chave**.

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

O Enterprise Project é uma plataforma de governança em nuvem que combina com a estrutura organizacional e o modelo de gerenciamento de serviços da sua empresa. Ele ajuda você a gerenciar projetos empresariais, recursos, pessoal, finanças e aplicações na nuvem com base na estrutura organizacional hierárquica (empresas, departamentos e projetos) e na estrutura de serviço do projeto.

Se você tiver ativado o gerenciamento de projetos empresariais, poderá adicionar chaves personalizadas especificadas aos projetos empresariais no console do KMS.

Restrições

- A função de gerenciamento de projetos empresariais foi ativada.

  Se você não ativou a função de gerenciamento de projetos empresariais, a opção **Enterprise Project** não será exibida no console por padrão e você não poderá adicionar

chaves a um projeto. Para obter detalhes sobre como ativar a função de projeto empresarial, consulte **Ativação da central empresarial**.

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

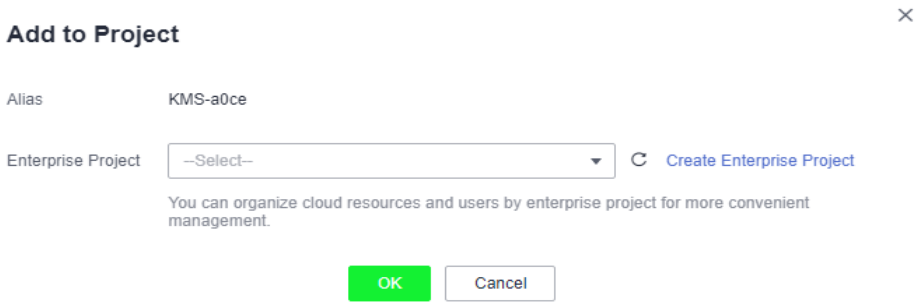
Procedimento

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 projeto.

Passo 3 Na linha que contém a chave de destino, clique em **Add to Project**.

Figura 1-16 Adição de uma chave a um projeto



NOTA

Se você for um usuário não empresarial, a opção **Add to Project** não será exibida na coluna de operação.

Para obter detalhes sobre como ativar a função do projeto empresarial, consulte **Ativação da central empresarial**.

Passo 4 Selecione um projeto.

Passo 5 Clique em **OK**.

----Fim

1.5 Pesquisa de uma chave

Esta seção descreve como pesquisar uma chave personalizada especificando atributos na página do KMS.

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**.

Passo 4 Clique na barra de pesquisa e selecione os critérios para as chaves de filtragem, conforme mostrado na **Figura 1-17**. Pesquise uma chave especificando atributos.

Figura 1-17 Barra de pesquisa

NOTA

- Você pode pesquisar chaves por alias de chave, ID, status, tempo de criação, algoritmo, uso, tempo de expiração do material, origem do material e projeto empresarial.
- Você pode pesquisar chaves por combinação de atributos. Por exemplo, se **Status** estiver definido como **Enabled** e **Key Algorithm** estiver definido como **AES_256**, todas as chaves personalizadas que atendam aos critérios serão exibidas.

----Fim

1.6 Uso da 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

A chave personalizada está no status **Enabled**.

Restrições

- As chaves padrão não podem ser usadas para criptografar ou descriptografar esses dados com a ferramenta.
- Chaves assimétricas não podem ser usadas para criptografar ou descriptografar esses dados com a ferramenta.
- Você pode chamar uma API para usar uma chave 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.

Criptografia de dados

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

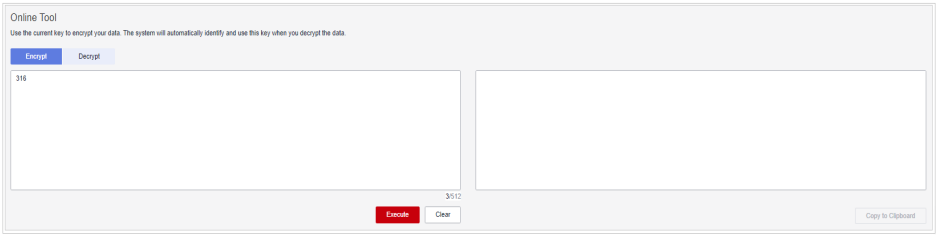
Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

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

Passo 4 Clique no alias de uma chave personalizada para exibir seus detalhes e vá para 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. Para obter detalhes, consulte **Figura 1-18**.

Figura 1-18 Criptografia de 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

Descriptografia de dados

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

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

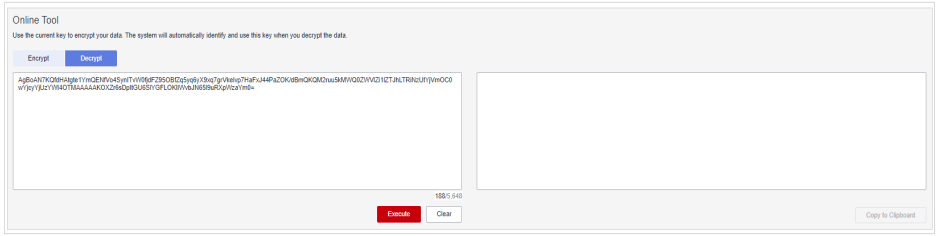
Passo 3 Você pode clicar em qualquer chave não padrão no status **Enabled** para acessar a página de criptografia e descriptografia da ferramenta on-line.

Passo 4 Clique em **Decrypt**. Na caixa de texto à esquerda, insira os dados a serem descriptografados. Para obter detalhes, consulte **Figura 1-19**.

NOTA

- A ferramenta identificará a CMK de criptografia original e a usará para descriptografar os dados.
- No entanto, se a CMK tiver sido excluída, a descriptografia falhará.

Figura 1-19 Descriptografia de 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

1.7 Gerenciamento de tags

1.7.1 Adição de uma tag

As tags são usadas para identificar chaves. Você pode adicionar tags a chaves personalizadas para que possa classificar chaves personalizadas, rastreá-las e coletar seu status de uso de acordo com as tags.

Restrições

Tags não podem ser adicionadas às chaves 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 projeto.

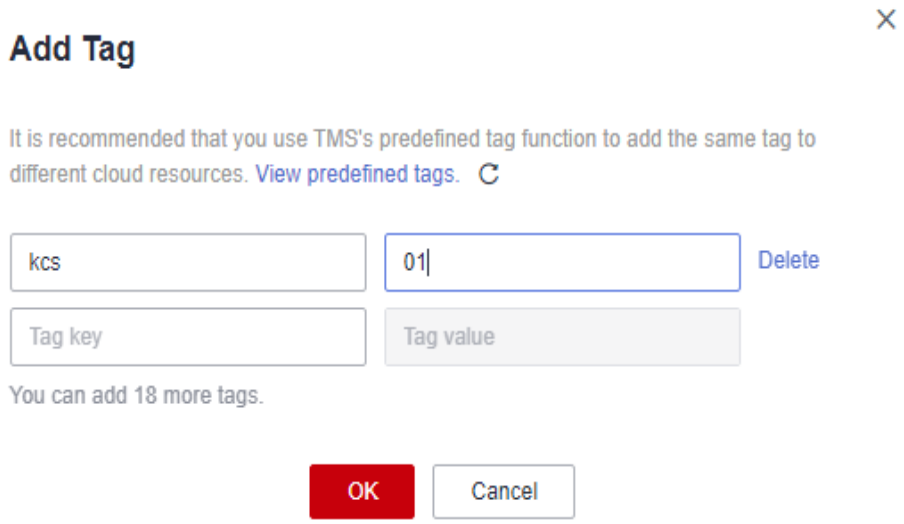
Passo 3 Clique em . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 Clique no alias da chave personalizada desejada para exibir seus detalhes.

Passo 5 Clique em **Tags** para acessar 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 1-20 Adição de 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*.
- 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 chaves personalizadas. No entanto, sob a mesma chave personalizada, uma chave de tag pode ter apenas um valor de tag. Um máximo de 20 tags podem ser adicionadas para uma chave personalizada.	● Obrigatório. ● A chave da tag deve ser exclusiva para a mesma chave personalizada. ● Limite de 128 caracteres. ● O valor não pode começar nem terminar com um espaço. ● Não é possível iniciar com **_sys_**. ● Os seguintes tipos de caracteres são permitidos: – Chinês – Inglês – Números – Espaço – Caracteres especiais: _.:/=+-@	cost
Tag value	Valor da tag	● Este parâmetro pode estar vazio. ● Limite de 255 caracteres. ● Os seguintes tipos de caracteres são permitidos: – Chinês – Inglês – Números – Espaço – Caracteres especiais: _.:/=+-@	100

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

----Fim

1.7.2 Modificação de valores de tag

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

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.

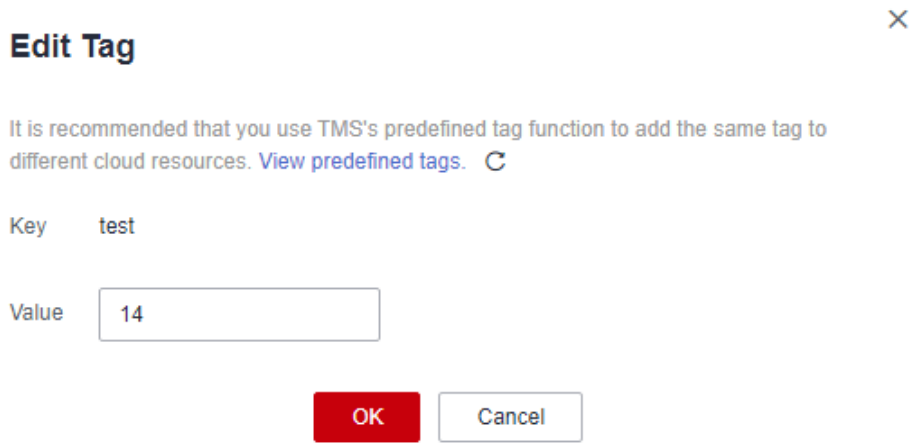
Passo 3 Clique em . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 Clique no alias da chave personalizada desejada para exibir seus detalhes.

Passo 5 Clique em **Tags** para acessar 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 1-21 Edição de uma tag



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

----Fim

1.7.3 Exclusão de tags

Esta seção descreve como excluir tags no console do KMS.

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**.

Passo 4 Clique no alias da chave personalizada desejada para exibir seus detalhes.

Passo 5 Clique em **Tags** para acessar 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 **Confirm**.

----Fim

1.8 Rotação de CMKs

1.8.1 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.

As finalidades 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 disponível 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:

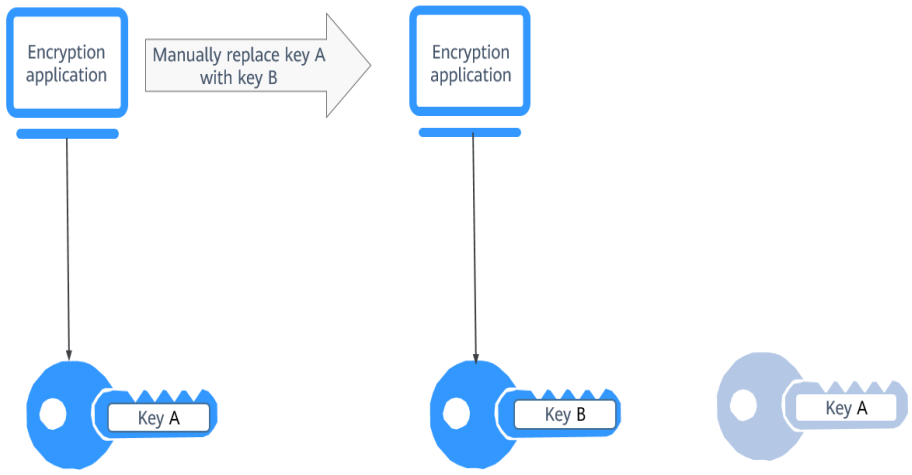
- Rotação manual da chave

  Método 1: crie uma chave B para substituir a chave A atualmente usada.

  Método 2: modifique a chave A e use-a.

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

Figura 1-22 Rotação manual da chave



- Rotação automática da chave

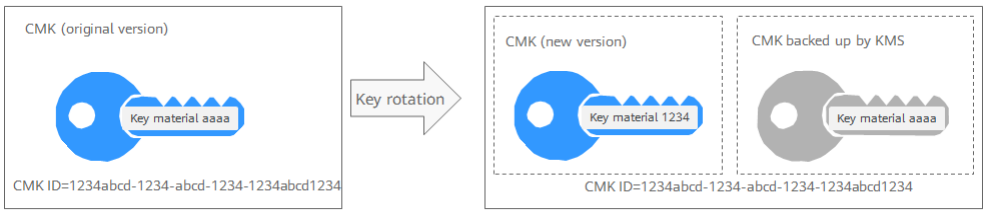
  O KMS faz a rotação automática das chaves com base no período de rotação configurado (365 dias por padrão). O sistema gera automaticamente uma nova chave para substituir a chave em uso. A rotação automática da chave altera apenas o material da chave de uma CMK. Os atributos lógicos da chave não serão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

  A rotação automática da chave tem as seguintes características:

  a. Ativar a rotação de uma chave personalizada existente. O KMS gerará automaticamente novos materiais de chave para a chave personalizada.

  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 vazada, a rotação automática não pode conter o impacto do vazamento.

Figura 1-23 Rotação de chave



NOTA

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

- O KMS usa a versão mais recente da chave personalizada para criptografar dados.
- Ao descriptografar dados, o KMS usa a versão da chave personalizada que foi usada para criptografar os dados.

Modos de rotação

Tabela 1-12 Modos de rotação de chaves

Tipo de chave	Modo de rotação
Chave padrão	Não pode ser girada.
Chave personalizada	As chaves podem ser giradas automaticamente ou manualmente, dependendo do tipo de algoritmo de chave. ● Chave simétrica: pode ser girada automaticamente ou manualmente. ● Chave assimétrica: só pode ser girada manualmente.
CMK desativada	As CMKs desativadas não são giradas. O KMS mantém seu status de rotação inalterado. Depois que uma chave personalizada for ativada, se ela tiver sido usada por mais tempo do que o período de rotação, o KMS girará as chaves imediatamente. Se a chave personalizada 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	O KMS não rotaciona CMKs com status de exclusão pendente. Depois de cancelar a exclusão de uma CMK, o status de rotação de chave anterior será restaurado. Se a chave personalizada 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**.

1.8.2 Ativação da rotação de chaves

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

Por padrão, a rotação automática de chaves está desativada para uma chave personalizada. Toda vez que você ativa a rotação de chaves, o KMS gira automaticamente as chaves personalizadas com base no período de rotação definido.

Pré-requisitos

- A chave está ativada.
- A **Origin** da chave é **KMS**.
- Somente as chaves simétricas podem ser giradas.

Restrições

- Uma chave personalizada desativada nunca é girada, mesmo que a rotação esteja ativada para ela.

  O KMS retoma a rotação quando essa chave personalizada está ativada. Se você ativar essa chave personalizada após o término de um período de rotação, o KMS irá girá-la dentro de 24 horas.
- Somente CMKs podem ser giradas.

Procedimento

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

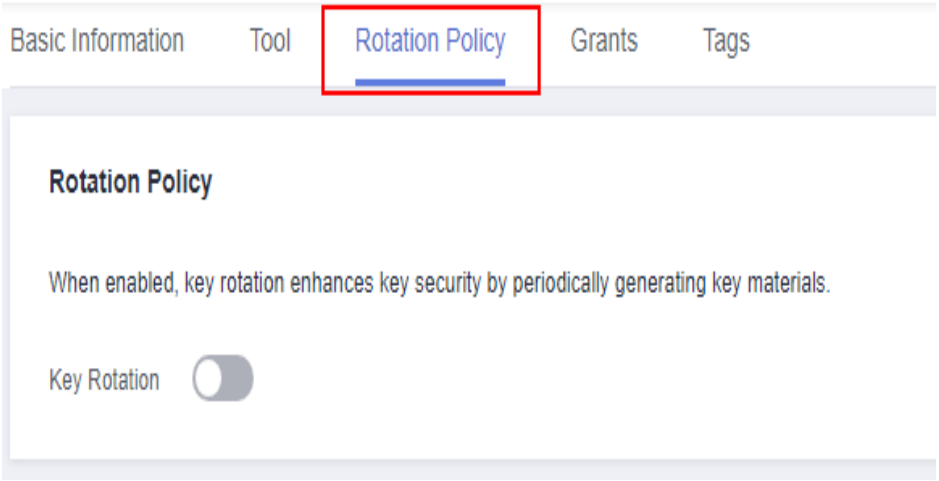
Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

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

Passo 4 Clique no alias da chave personalizada desejada para exibir seus detalhes.

Passo 5 Clique na guia **Rotation Policy**. A chave de rotação é exibida, conforme mostrado em **Figura 1-24**.

Figura 1-24 Rotação de chave



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 1-25**. Para obter mais informações, consulte **Tabela 1-13**.

Figura 1-25 Ativação de rotação de chaves

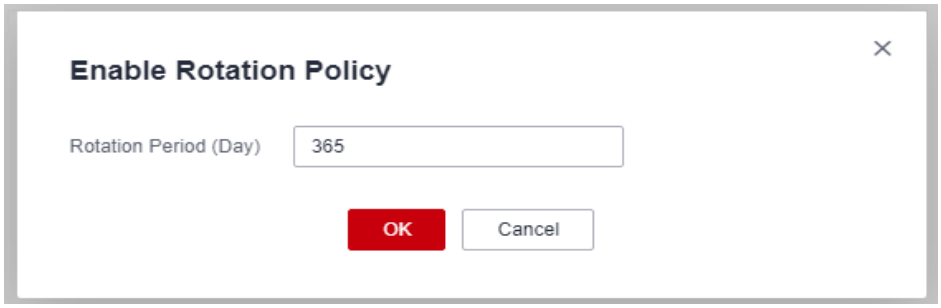
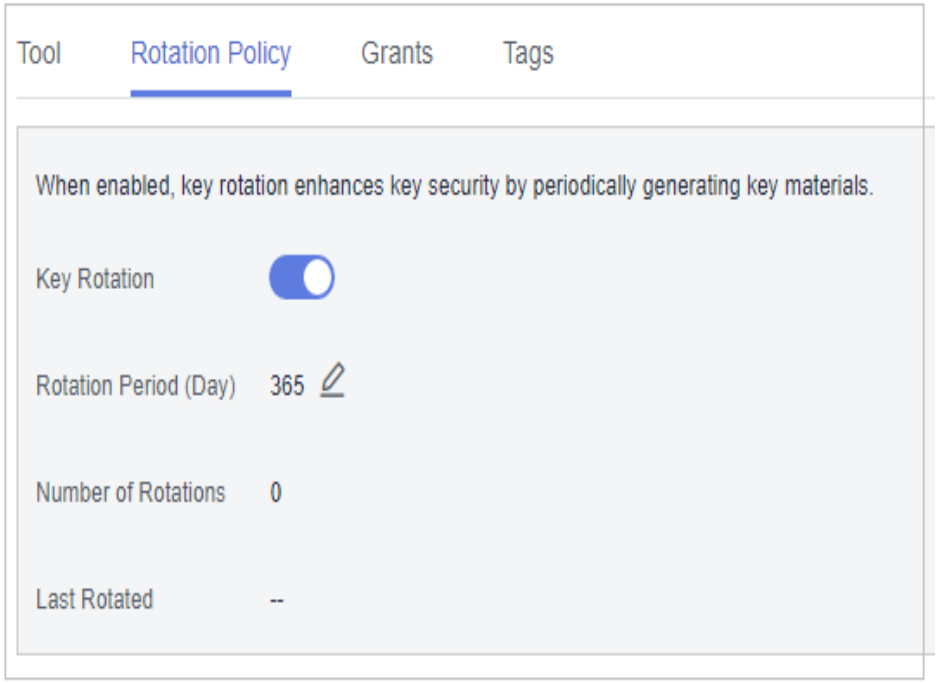


Tabela 1-13 Parâmetros de rotação de chave

Parâmetro	Descrição
Key rotation	Chave de rotação. O status padrão é  .  : desativada  : ativada Depois que a rotação estiver ativada, a chave será girada com base no período definido. **NOTA** Uma chave personalizada desativada nunca é girada, mesmo que a rotação esteja ativada para ela. O KMS retoma a rotação quando essa chave personalizada está ativada. Se você ativar essa chave personalizada após o término de um período de rotação, o KMS irá girá-la dentro de 24 horas.
Rotation Period (day)	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 chave personalizada é usada. Se for usado com frequência, configure um período curto; caso contrário, defina um período longo.

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

Figura 1-26 Detalhes da rotação da chave



NOTA

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

----Fim

1.8.3 Desativação da rotação de chaves

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

Pré-requisitos

- A chave está ativada.
- A **Origin** da chave 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 projeto.

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

Passo 4 Clique no alias de uma chave simétrica.

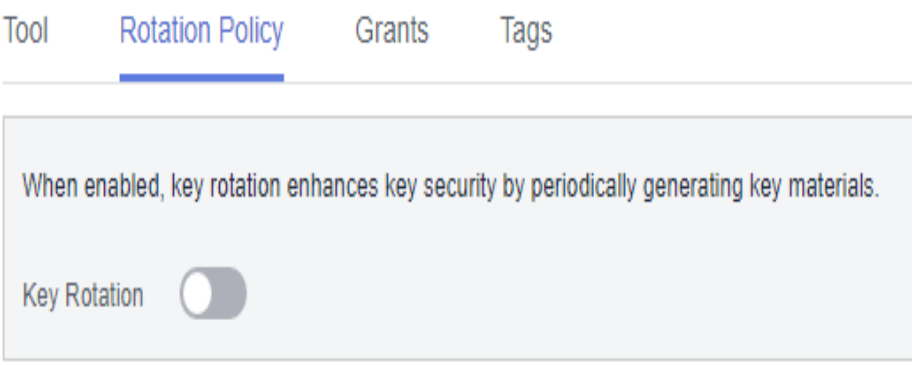
Passo 5 Clique em **Rotation Policy** e a caixa de diálogo será exibida.

Passo 6 Clique em  para desativar a rotação de chaves.

Passo 7 Na caixa de diálogo de confirmação exibida, clique em **OK**.

Passo 8 Verifique o status da rotação, conforme mostrado em **Figura 1-27**.

Figura 1-27 Desativação de rotação de chaves



----Fim

1.9 Managing a Grant

1.9.1 Criação de uma concessão

Você pode criar concessões para que outros usuários ou contas do IAM usem a chave personalizada. Você pode criar um máximo de 100 concessões em uma chave personalizada.

Pré-requisitos

- Você obteve o ID do beneficiário (usuário para quem as permissões devem ser autorizadas).
- A chave personalizada desejada está no status **Enabled**.

Restrições

- O proprietário de uma chave personalizada pode criar uma concessão para a chave personalizada no console do KMS ou chamando APIs. Os usuários ou contas do IAM que têm a permissão de criação de concessão atribuída pelo proprietário da chave personalizada podem criar concessões para a chave personalizada somente chamando APIs.
- Um máximo de 100 concessões podem ser criadas para uma chave personalizada.

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**.

Passo 4 Clique no alias da chave personalizada desejada para acessar sua página de detalhes e criar uma concessão nela.

Passo 5 Clique na guia **Grants**.

Passo 6 Clique em **Create Grant**. A caixa de diálogo **Create Grant** é exibida.

Figura 1-28 Criação de uma concessão (para um usuário)

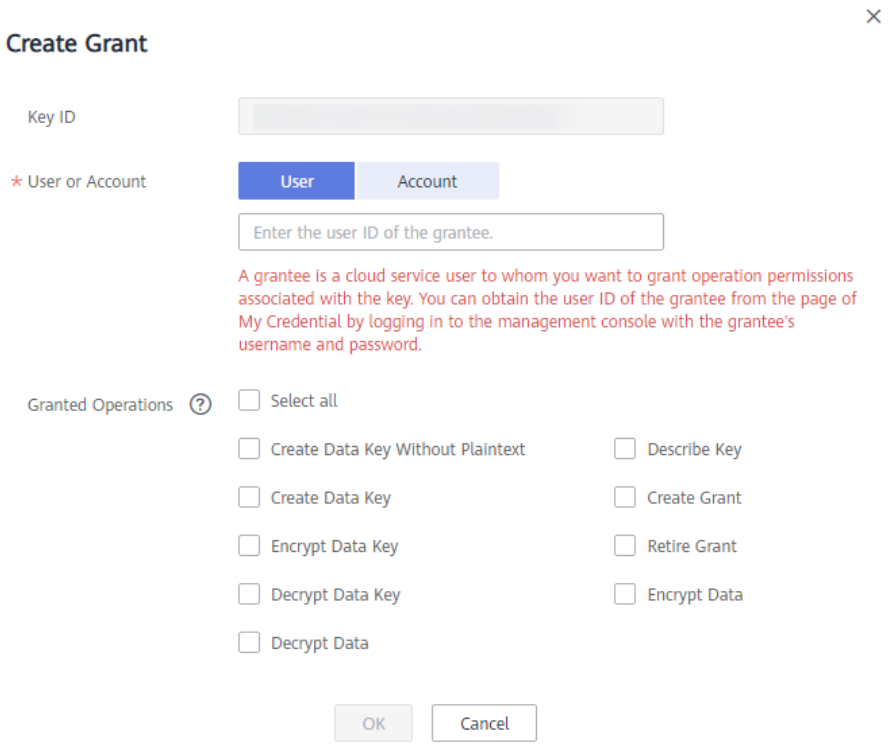
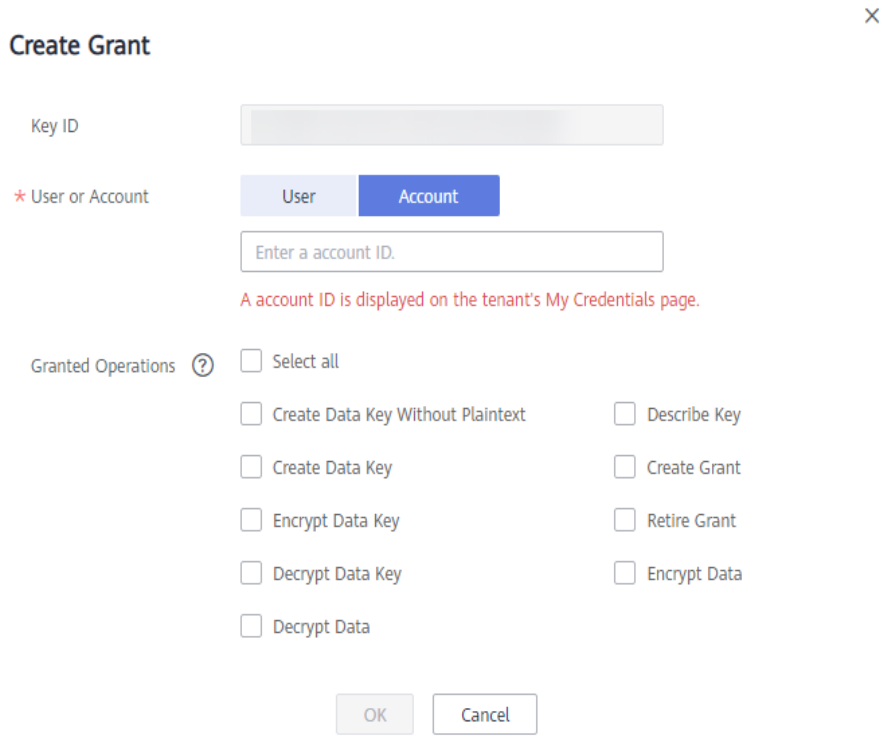


Figura 1-29 Criação de uma concessão (para uma conta)



Passo 7 Na caixa de diálogo exibida, insira o ID do usuário a ser autorizado e selecione as permissões a serem concedidas. Para obter mais informações, consulte **Tabela 1-14**.

AVISO

Um beneficiário pode realizar as operações autorizadas apenas chamando as APIs necessárias. Para obter detalhes, consulte a *Referência de API do Key Management Service*.

Tabela 1-14 Descrição do parâmetro

Parâmetro	Descrição	Exemplo de valor
Key ID	ID de uma chave personalizada (lida automaticamente pelo sistema)	-

Parâmetro	Descrição	Exemplo de valor
User or Tenant	Se um usuário ou uma conta está autorizado. ● User ID do usuário: insira o ID de usuário do IAM. Para obter o ID, clique no nome de usuário no canto superior direito da página, escolha **My Credentials**. Escolha **API Credentials** no painel de navegação e copie o valor de **IAM User ID**. Após a conclusão da autorização, o usuário do IAM pode usar as chaves especificadas. ● Account ID da conta: insira o ID de usuário do IAM. Para obter o ID, clique no nome de usuário no canto superior direito da página, escolha **My Credentials**. Escolha **API Credentials** no painel de navegação e copie o valor de **Account ID**. Após a conclusão da autorização, todos os usuários do IAM sob a conta podem usar chaves especificadas.	d9a6b2bdaedd4ba586cabe6372d1b312
Grant Name	Você pode nomear a concessão.	test

Parâmetro	Descrição	Exemplo de valor
Operations	As seguintes permissões podem ser autorizadas: **NOTA** ● Você pode criar várias concessões em uma chave personalizada para fornecer permissões diferentes para o mesmo usuário. As permissões do usuário na chave personalizada são a combinação de todas as concessões. ● Este parâmetro não pode ser deixado em branco. ● Não é permitido selecionar apenas **Create Grant**. ● **Create Data Key Without Plaintext** ● **Create Data Key** ● **Encrypt Data Key** ● **Decrypt Data Key** ● **Query Key Information** ● **Create Grant** ● **Retire Grant** – Um beneficiário pode retirar uma concessão se o beneficiário não precisa dessa permissão. – Se, antes de retirar uma concessão, o beneficiário tiver concedido a permissão a outro usuário, a permissão desse usuário não será afetada pela retirada da concessão. ● **Encrypt Data** ● **Decrypt Data**	-

Passo 8 Clique em **OK**. Quando a mensagem **Grant created successfully** é exibida no canto superior direito, a concessão foi criada.

Na lista de concessões, você pode exibir o nome da concessão, o ID da concessão, o tipo de concessão, o ID do beneficiário, a operação concedida e a hora de criação da concessão.

----Fim

1.9.2 Consulta de uma concessão

Esta seção descreve como exibir os detalhes sobre uma concessão de chave personalizada no console do KMS, como o ID de concessão, o ID do usuário beneficiário, a operação concedida e o tempo de criação.

Pré-requisitos

Você criou uma concessão.

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**.

Passo 4 Clique no alias da chave personalizada desejada para exibir seus detalhes.

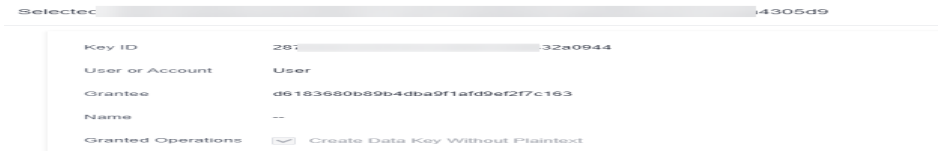
Passo 5 Clique em **Grant** para exibir as informações de concessão da chave personalizada atual. A **Tabela 1-15** descreve os parâmetros.

Tabela 1-15 Descrição do parâmetro

Parâmetro	Descrição
Grant Name	Nome da concessão quando criada
Grant ID	Identificação exclusiva gerada aleatoriamente de uma concessão
Granted To	Se as permissões são concedidas a um usuário ou conta.
Grantee ID	ID do usuário ou da conta autorizados.
Granted Operations	Operações autorizadas (como **Create Data Key**) na chave personalizada
Created	Tempo de criação da concessão
Operation	Operações que podem ser realizadas em uma concessão. Por exemplo, você pode revogar uma concessão.

Passo 6 Selecione a concessão de destino e clique em no canto inferior direito para exibir os detalhes da concessão, conforme mostrado na **Figura 1-30**.

Figura 1-30 Visualização dos detalhes da concessão



----Fim

1.9.3 Revogação de uma concessão

Você pode revogar uma concessão no console do KMS em um dos seguintes cenários:

- Um beneficiário não precisa da concessão de chave personalizada. (O beneficiário pode dizer ao usuário que criou a concessão para revogar a concessão ou chamar a API necessária para revogar a concessão diretamente.)

- Você não quer que o beneficiário tenha a concessão.

Quando uma concessão é revogada, o beneficiário não tem mais a permissão correspondente. No entanto, se o beneficiário tiver criado a mesma concessão para outro usuário, a permissão desse usuário não será afetada.

Esta seção descreve como revogar uma concessão no console do KMS.

Pré-requisitos

Você criou uma concessão.

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**.

Passo 4 Clique no alias da chave personalizada desejada para exibir seus detalhes.

Passo 5 Na linha de um beneficiário, clique em **Revoke Grant**.

Passo 6 Na caixa de diálogo exibida, clique em **OK**. Se **Grant *grant ID* revoked successfully** for exibido no canto superior direito, a concessão foi revogada.

----Fim

2 Serviço de gerenciamento de segredo em nuvem

2.1 Visão geral do segredo

Segredos compartilhados

O gerenciamento do ciclo de vida completo é suportado para segredos personalizados em diferentes cenários. Você pode usar o CSMS para gerenciar, recuperar e armazenar de forma centralizada e segura vários tipos de segredos, como senhas de contas de bancos de dados, senhas de servidores, chaves SSH e chaves de acesso. Várias versões podem ser gerenciadas, para que você possa alternar segredos.

Segredos do RDS

O vazamento de segredos de banco de dados é a principal causa de vazamento de dados. O CSMS suporta o host de segredo do RDS e a rotação automática e manual, atendendo a vários cenários de gerenciamento de segredos de banco de dados e reduzindo os riscos de segurança enfrentados pelos dados de serviço.

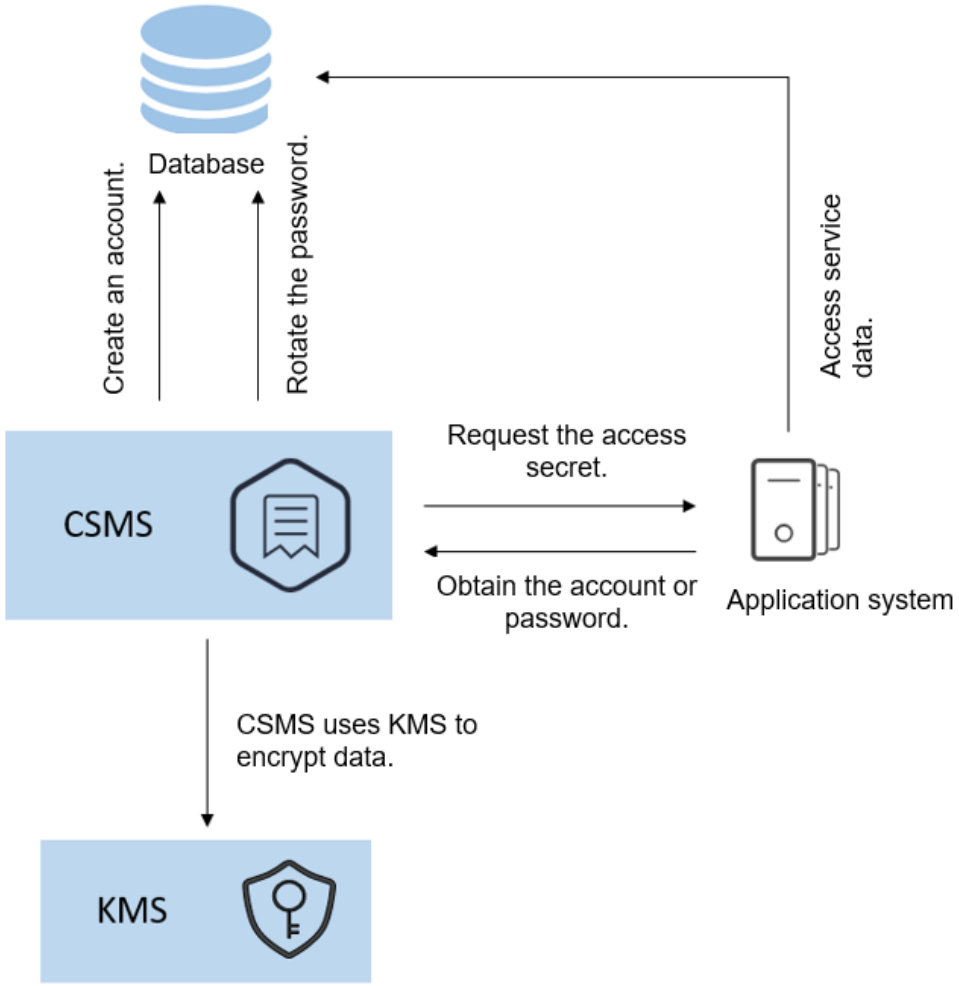
Diferenças entre segredos compartilhados e segredos do RDS

Tabela 2-1 Diferença entre credenciais

	Segredo compartilhado	Segredo do RDS
Cenário de aplicação	Suporta o gerenciamento do ciclo de vida completo de segredos personalizados em diferentes cenários.	Hospeda automaticamente os segredos do banco de dados do RDS da Huawei Cloud.
Rotação automática	Não suportado. Os usuários precisam acionar a rotação.	Suportado. Modelos de rotação de usuário único e usuário duplo são suportados.

Uso de segredos do RDS

Figura 2-1 Arquitetura



Descrição do processo:

1. Crie um segredo do RDS.

- Defina o nome e a tag de segredos.
- Configure uma política de rotação automática.

2. Um sistema de aplicação pode solicitar um segredo de acesso do CSMS e obter o valor de segredo para acessar o banco de dados correspondente. Para obter detalhes sobre como chamar APIs, consulte **Consulta da versão e do valor do segredo**.
3. O sistema de aplicação usa o valor de segredo retornado para analisar os dados de texto não criptografado. Depois de obter a conta e a senha, o sistema da aplicação pode acessar o banco de dados de destino correspondente ao usuário.

⚠ CUIDADO

- Depois que a rotação automática estiver ativada, as senhas hospedadas pela instância do banco de dados serão atualizadas periodicamente. Certifique-se de que a aplicação que usa a instância de banco de dados tenha concluído a adaptação do código para que os segredos mais recentes possam ser obtidos dinamicamente quando a conexão de banco de dados for estabelecida.
- Não armazene em cache nenhuma informação em segredos. Caso contrário, a conta e a senha podem se tornar inválidas após a rotação, causando falhas de conexão de banco de dados.

2.2 Política de rotação

Rotação de usuário único

A política de rotação de usuário único aplica-se a cenários de usuário único. É usada principalmente para contas com rotação de baixa frequência e requisitos de baixa confiabilidade. Esta é uma política de rotação simples adequada para a maioria dos casos. O segredo atual pode estar temporariamente indisponível no momento em que a senha é redefinida.

Você pode usar a rotação de usuário único para:

- Selecione ou crie uma conta de banco de dados como o valor do segredo ao criar uma conta de banco de dados.
- Para o acesso ao banco de dados, uma conexão de banco de dados não é excluída durante a rotação de segredos. Após a rotação, novas conexões usam os novos segredos.

Rotação de usuário duplo

A rotação de usuário duplo é usada principalmente para contas com alta frequência de rotação e requisitos de alta confiabilidade de rotação. Duas contas com a mesma permissão são hospedadas. O segredo do status **SYSPREVIOUS** é girado a cada vez. O acesso ao programa não será interrompido quando uma senha for redefinida e trocada. Durante a rotação, o status do novo segredo é alterado para **SYSPENDING** e a API do RDS é chamada para redefinir a senha. Depois que a senha for redefinida, o status do novo segredo será alterado de **SYSPENDING** para **SYSCURRENT**, e o status do segredo no estado **SYSCURRENT** será alterado para **SYSPREVIOUS**.

- Você precisa selecionar ou criar duas contas de banco de dados como valores de segredos.
- Os dois valores de segredos são girados alternadamente. Você precisa obter o valor de segredo de **SYSCURRENT** cada vez.

2.3 Criação de um segredo

2.3.1 Criação de um segredo compartilhado

Esta seção descreve como criar um segredo no console do CSMS.

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

Restrições

- Um usuário pode criar um máximo de 200 segredos.
- Por padrão, a chave padrão **csms/default** criada pelo CSMS é usada como a chave de criptografia do segredo atual. Você também pode criar uma chave simétrica definida pelo usuário 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 ou um projeto.

Passo 3 Clique em  à esquerda, escolha **Security & Compliance** > **Data Encryption Workshop**, a página de gerenciamento de chaves é exibida.

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

Passo 5 Clique em **Create Secret**. Configure os parâmetros na caixa de diálogo **Create Secret**, conforme mostrado em **Figura 2-2**. Para obter mais informações, consulte **Tabela 2-2**.

Figura 2-2 Criação de um segredo

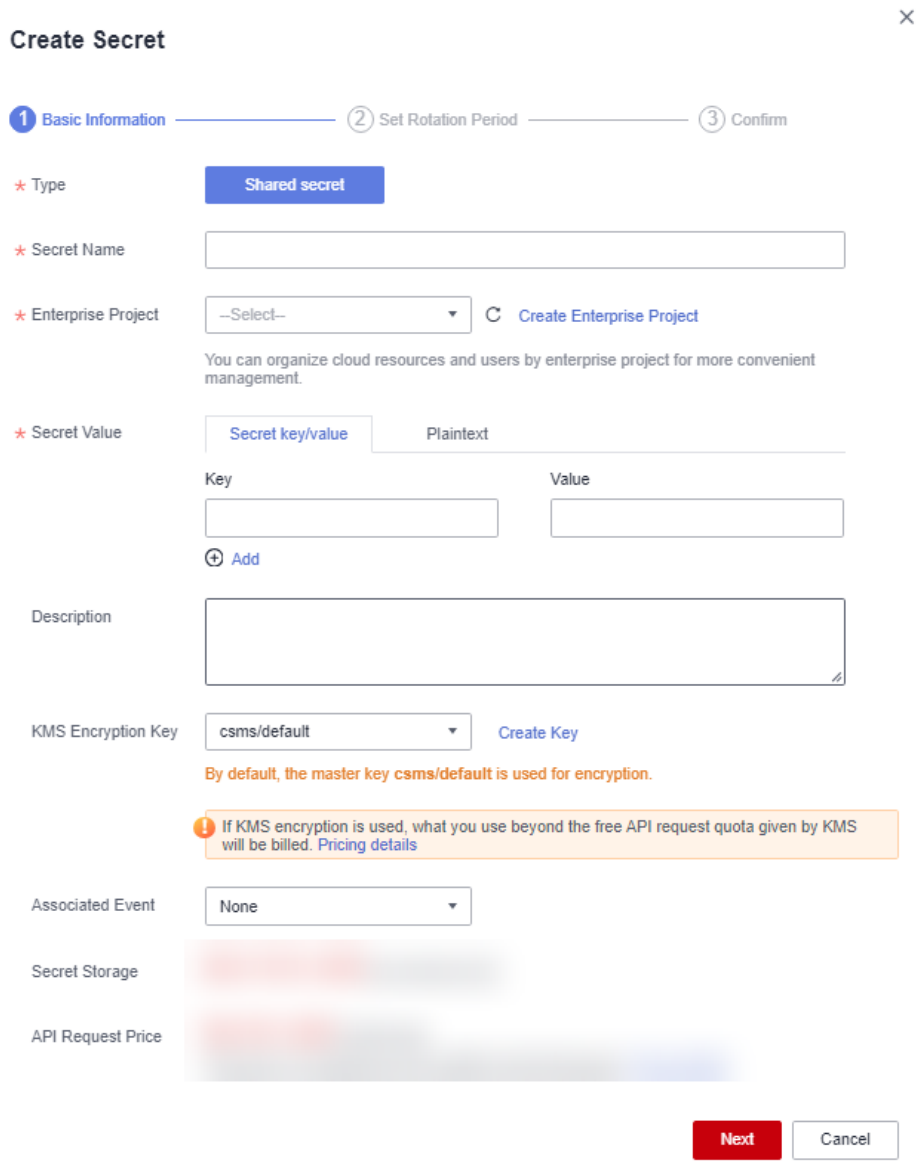


Tabela 2-2 Parâmetros de segredo

Parâmetro	Descrição
Type	Tipo de segredo. O valor padrão é **Shared secret**.
Secret Name	Nome de segredo
Enterprise Project	Projeto empresarial ao qual o segredo deve ser vinculado
Secret Value	Par de chave/valor de segredos e o segredo de texto não criptografado a ser criptografado
Description	Descrição de um segredo

Parâmetro	Descrição
KMS Encryption Key	Selecione a chave padrão **csms/default** ou uma chave personalizada criada no KMS. **NOTA** Por padrão, a chave padrão **csms/default** criada pelo CSMS é usada como a chave principal de criptografia do segredo atual. Você também pode criar uma chave ou usar uma chave personalizada no console do KMS. Para obter detalhes, consulte **Criação de uma chave**.
Associated Event	Ao criar um segredo, você pode vinculá-lo a um evento de segredo. Você pode adicionar, excluir, modificar e consultar versões de segredos na página de notificação de eventos.

Passo 6 Clique em **Next** e defina o período de rotação.

Passo 7 Clique em **Next** e confirme as informações de criação.

Passo 8 Clique em **OK**.

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

----Fim

2.4 Gerenciamento de segredos

2.4.1 Visualização de um segredo

Esta seção descreve como verificar nomes, status e tempo de criação de segredos no console do CSMS. O status de segredos pode ser **Enabled** 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 Clique em  à esquerda, escolha **Security & Compliance** > **Data Encryption Workshop**, a página de gerenciamento de chaves é exibida.

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

Passo 5 Verifique a lista de segredos. Para obter mais informações, consulte **Tabela 2-3**.

Figura 2-3 Lista de segredos

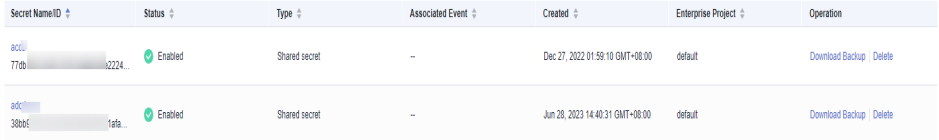


Tabela 2-3 Parâmetros da lista de segredos

Parâmetro	Descrição
Secret Name/ID	Nome de segredo
Status	Status de um segredo. O valor pode ser **Enabled** ou **Pending deletion**.
Type	Tipo de segredos, incluindo segredos compartilhados e segredos de instância de banco de dados RDS.
Created	Momento em que um segredo é criado
Enterprise Project	Projeto empresarial ao qual o segredo deve ser vinculado
Operation	Você pode gerenciar segredos na coluna **Operation**, por exemplo, baixar backup de segredos, excluir segredos e cancelar a exclusão de segredos.

Passo 6 Clique em um segredo para ver seus detalhes. Consulte **Figura 2-4**.

Figura 2-4 Detalhes de segredos

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

2.4.2 Exclusão de um segredo

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

Pré-requisitos

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.
- Para obter detalhes sobre as informações de cobrança sobre um segredo a ser excluído, consulte **As credenciais programadas para serem excluídas são cobradas?**

- Se você excluir um segredo imediatamente, poderá restaurá-lo usando o backup de segredo que você baixou com antecedência. Tenha cuidado ao realizar esta operação.

Exclusão de um segredo

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

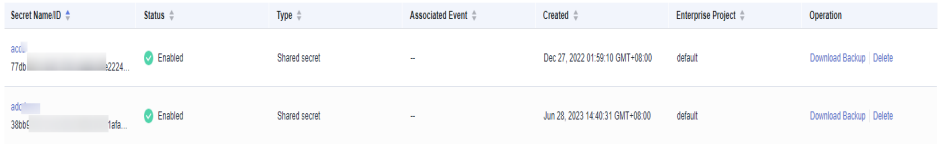
Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou um projeto.

Passo 3 Clique em à esquerda, escolha **Security & Compliance** > **Data Encryption Workshop**, a página de gerenciamento de chaves é exibida.

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

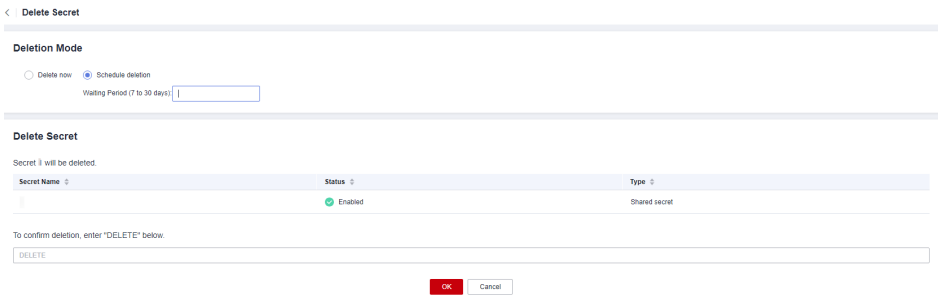
Passo 5 Na linha de um segredo, clique em **Delete**.

Figura 2-5 Exclusão de um segredo



Passo 6 Na página exibida, selecione um modo de exclusão. Se você quiser excluir o segredo em um horário específico, defina **Schedule deletion**.

Figura 2-6 Configuração da exclusão de programação



Passo 7 Na caixa de diálogo de confirmação, insira **DELETE** e 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.
- Para obter detalhes sobre as informações de cobrança sobre um segredo a ser excluído, consulte **As credenciais programadas para serem excluídas são cobradas?**
- Se você excluir um segredo imediatamente, poderá restaurá-lo usando o backup de segredo que você baixou com antecedência. Tenha cuidado ao realizar esta operação.

----Fim

2.5 Gerenciamento de versões de segredos

2.5.1 Salvamento e visualização de valores de segredos

Esta seção descreve como salvar e visualizar valores de segredos no console do CSMS.

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

Restrições

- Um segredo pode ter até 20 versões.
- As versões de segredos são numeradas como 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 ou um projeto.

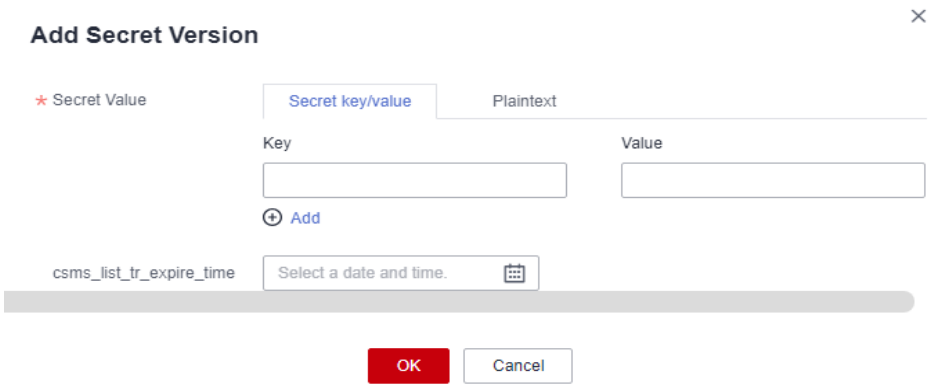
Passo 3 Clique em à esquerda, escolha **Security & Compliance** > **Data Encryption Workshop**, a página de gerenciamento de chaves é exibida.

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

Passo 5 Clique em um nome de segredo para acessar 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 2-7 Adição de um valor de segredo



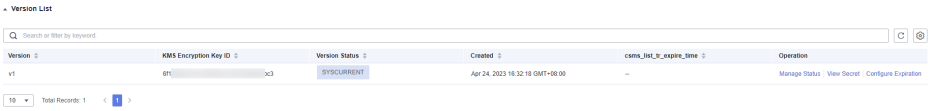
Passo 7 Você pode selecionar um tempo de expiração para o valor de segredo armazenado. O tempo pode ser específico para segundos. Depois que a configuração for concluída, você poderá exibir o tempo de expiração na lista de versões de segredos. Por exemplo, 30 de junho de 2023 19:52:59.

Passo 8 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 de segredos.

Passo 9 Na área **Version List**, clique em **View Secret** na coluna **Operation** de um segredo.

Figura 2-8 Lista de versões de segredos



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

----Fim

2.5.2 Gerenciamento de status de versão de segredo

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

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

Restrições

- A versão inicial é marcada pela tag de status **SYSCURRENT**.
- Você pode marcar uma versão com uma tag criada no serviço ou com uma tag personalizada. 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 ou um projeto.

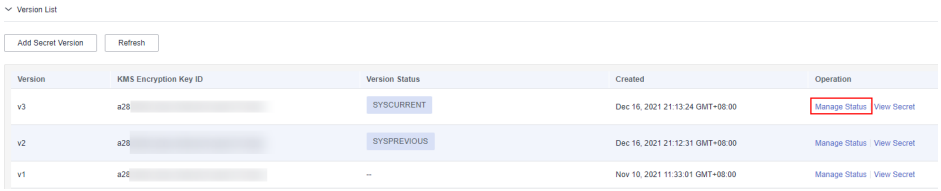
Passo 3 Clique em à esquerda, escolha **Security & Compliance** > **Data Encryption Workshop**, a página de gerenciamento de chaves é exibida.

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

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

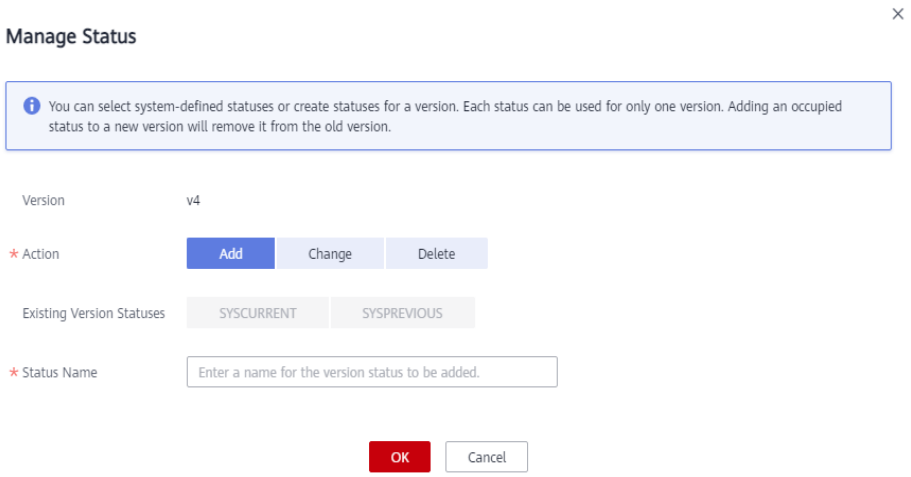
Passo 6 Na área **Version List**, clique em **Manage Status** na coluna **Operation**.

Figura 2-9 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 2-10 Gerenciamento de status



- Adição de 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.

- Atualização do 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**.

- Exclusão do 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

2.5.3 Definição do tempo de expiração da versão

Esta seção descreve como definir o tempo de expiração da versão na página de detalhes de segredos.

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 Clique em à esquerda, escolha **Security & Compliance** > **Data Encryption Workshop**, a página de gerenciamento de chaves é exibida.

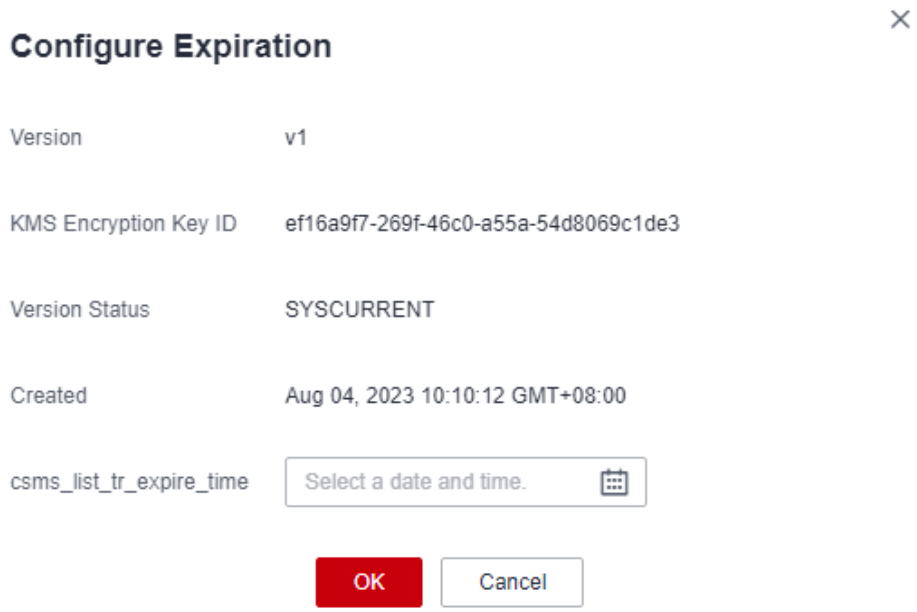
Passo 4 No painel de navegação, escolha **Cloud Secret Management Service**.

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

Passo 6 Na área **Current Version**, clique em **Configure Expiration** da versão de segredos de destino.

Passo 7 Na página exibida, defina uma hora de expiração e clique em **OK**.

Figura 2-11 Definição de um tempo de expiração



----Fim

2.5.4 Versão de segredos de rotação

Esta seção descreve como girar versões de segredos na página de detalhes de segredos.

Restrições

- O tipo do segredo é o segredo da instância de banco de dados RDS.
- Você precisa usar uma agência do IAM para autorizar a conta **op_svc_kms**, as permissões **KMS CMKFullAccess** e **RDS FullAccess** (necessário somente quando a rotação automática estiver ativada).
- A conta de segredo deve ser uma conta de banco de dados RDS existente.

Rotação manual

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.

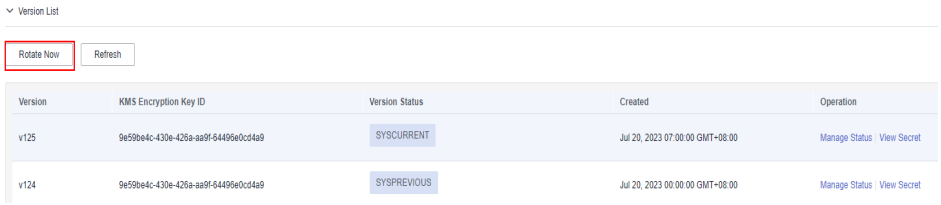
Passo 3 Clique em à esquerda, escolha **Security & Compliance** > **Data Encryption Workshop**, a página de gerenciamento de chaves é exibida.

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

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

Passo 6 Na área **Version List**, clique em **Rotate Now**.

Figura 2-12 Lista de versões



Passo 7 Na página **Rotate Now**, clique em **OK**. Se uma mensagem indicando o sucesso da rotação for exibida no canto superior direito, a alternância de versão será concluída.

Passo 8 Após a conclusão da rotação da versão, a versão cujo status é **SYSCURRENT** é a versão do segredo mais recente.

----Fim

Rotação automática

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.

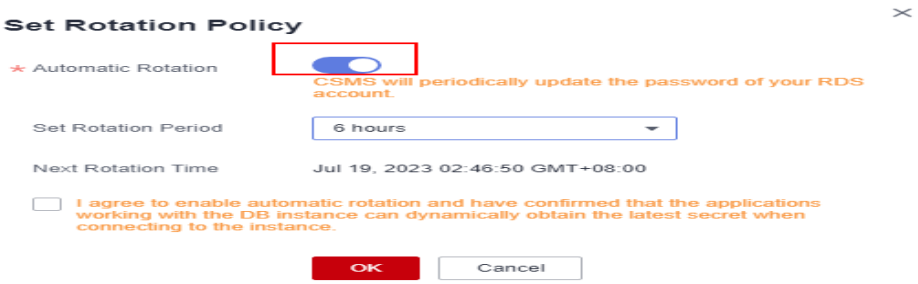
Passo 3 Clique em à esquerda, escolha **Security & Compliance** > **Data Encryption Workshop**, a página de gerenciamento de chaves é exibida.

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

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

Passo 6 Clique em **Set Rotation Policy** no canto superior direito. Na página **Set Rotation Policy**, ative o botão **Automatic Rotation**, conforme mostrado na **Figura 2-13**.

Figura 2-13 Rotação automática



Passo 7 Defina o período de rotação e clique em **OK**. Uma mensagem indicando que a política de rotação foi definida com sucesso é exibida no canto superior direito.

----Fim

2.6 Gerenciamento de tags

2.6.1 Adição de uma tag

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

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.

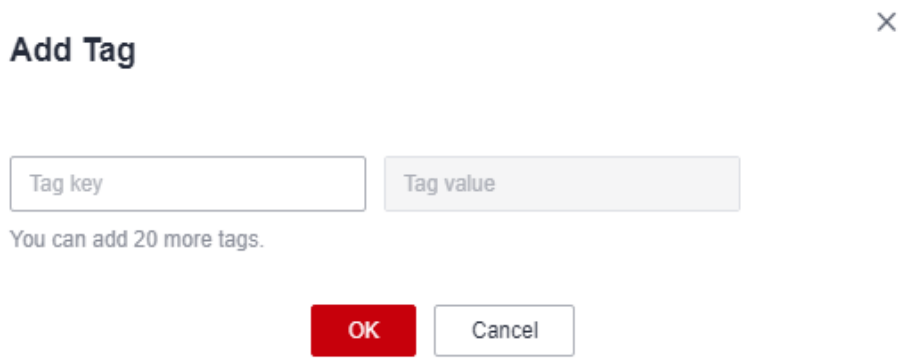
Passo 3 Clique em à esquerda, escolha **Security & Compliance** > **Data Encryption Workshop**, a página de gerenciamento de chaves é exibida.

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

Passo 5 Clique em um nome de segredo para acessar 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. A **Tabela 2-4** descreve os parâmetros.

Figura 2-14 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 2-4 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 20 tags.	● Obrigatório. ● A chave da tag deve ser exclusiva para a mesma chave personalizada. ● Limite de 128 caracteres. ● O valor não pode começar nem terminar com um espaço. ● Não é possível iniciar com **_sys_**. ● Os seguintes tipos de caracteres são permitidos: – Chinês – Inglês – Números – Espaço – Caracteres especiais: _.:/=+-@
Tag value	Valor da tag	● Opcional ● Limite de 255 caracteres. ● Os seguintes tipos de caracteres são permitidos: – Chinês – Inglês – Números – Espaço – Caracteres especiais: _.:/=+-@

Passo 7 Clique em **OK**.

----Fim

2.6.2 Pesquisa de um segredo por tag

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

Pré-requisitos

As tags foram adicionadas.

Procedimento

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

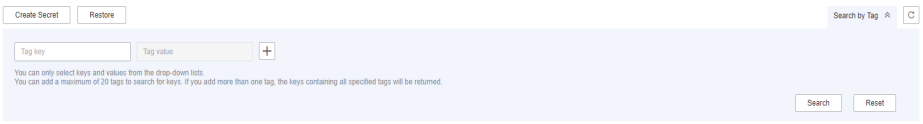
Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou um projeto.

Passo 3 Clique em à esquerda, escolha **Security & Compliance** > **Data Encryption Workshop**, a página de gerenciamento de chaves é exibida.

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

Passo 5 Clique em **Search by Tag** para mostrar a caixa de pesquisa, conforme mostrado na **Figura 2-15**.

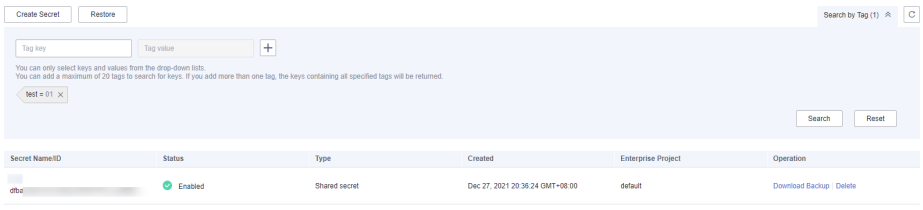
Figura 2-15 Caixa de pesquisa



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**. Conforme mostrado em **Figura 2-16**.

Figura 2-16 Resultado da pesquisa



NOTA

- Várias tags podem ser adicionadas para uma pesquisa. Um máximo de 20 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

2.6.3 Modificação de um valor de tag

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

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.

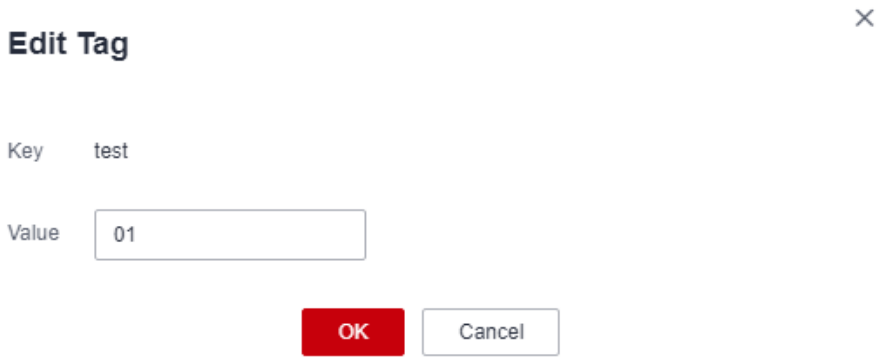
Passo 3 Clique em à esquerda, escolha **Security & Compliance** > **Data Encryption Workshop**, a página de gerenciamento de chaves é exibida.

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

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

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

Figura 2-17 Edição de uma tag



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

----Fim

2.6.4 Exclusão de uma tag

Esta seção descreve como excluir tags no console do CSMS.

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 Clique em à esquerda, escolha **Security & Compliance** > **Data Encryption Workshop**, a página de gerenciamento de chaves é exibida.

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

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

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

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 que você use 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 efetuar logon no seu 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. Huawei Cloud usa chaves de criptografia fornecidas pelo KMS para criptografar suas chaves privadas e garantir armazenamento e acesso seguros. Para mais detalhes, consulte **Criação de um par de chaves usando o 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

Ao criar um par de chaves de conta pela primeira vez, você precisa obter um usuário com a função de sistema Tenant Administrator.

Criação de um par de chaves usando o console de gerenciamento

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.

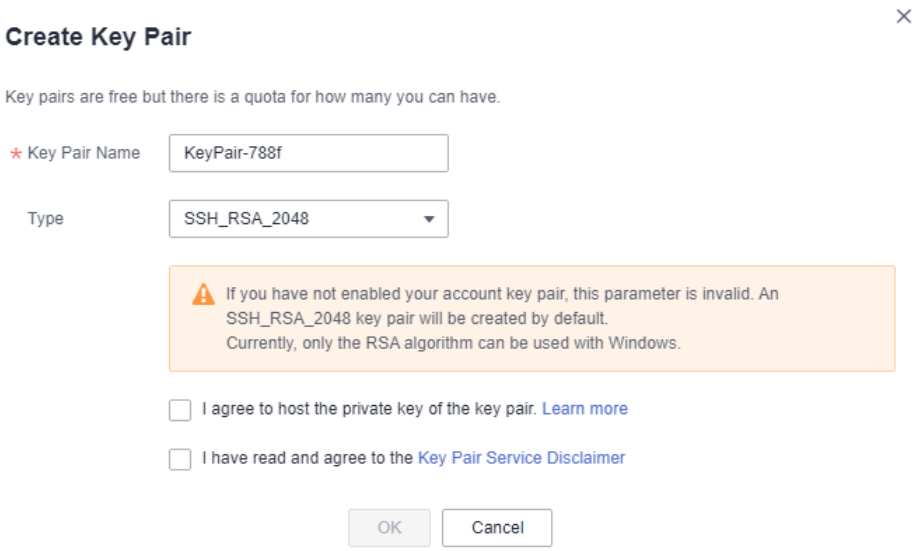
Passo 3 Clique em à esquerda, escolha **Security & Compliance** > **Data Encryption Workshop**, a página de gerenciamento de chaves é exibida.

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, como mostrado em **Figura 3-1**.

Figura 3-1 Criação de um par de chaves



Passo 7 (Opcional) Selecione um tipo de par de chaves. Se nenhum par de chaves estiver ativado para sua conta, um par de chaves SSH_RSA_2048 será criado por padrão.

NOTA

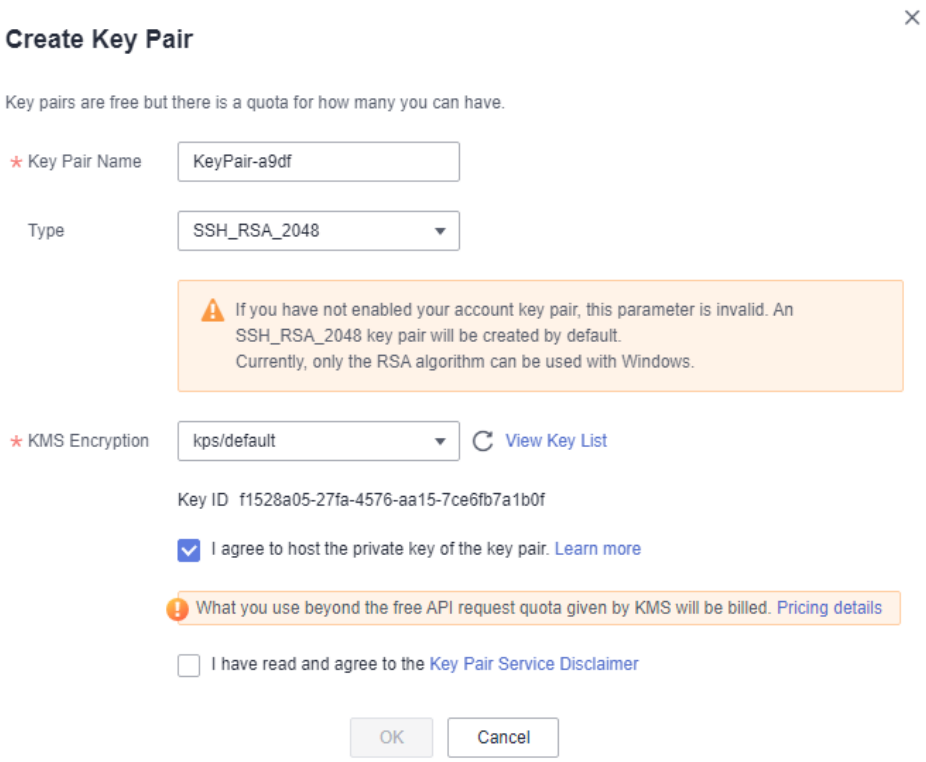
Atualmente, apenas o algoritmo RSA pode ser usado com o Windows.

Passo 8 Se você quiser ter sua chave privada gerenciada, leia e confirme **I agree to host the private key of the key pair.** Selecione uma chave de criptografia na caixa de listagem suspensa **KMS encryption**. Ignore esta etapa se você não precisa ter a chave privada gerenciada.

NOTA

- O KPS usa a chave de criptografia fornecida pelo KMS para criptografar chaves privadas. Quando o usuário usa a função de criptografia do KMS do par de chaves, o KMS cria automaticamente uma chave 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 9 Leia o *Aviso de isenção de responsabilidade do serviço de par de chaves* e selecione **I have read and agree to the Key Pair Service Disclaimer**.

Passo 10 Clique em **OK**. O navegador baixa automaticamente a chave privada. Quando a chave privada é baixada, uma caixa de diálogo é exibida.

Passo 11 Salve a chave privada conforme solicitado pela caixa de diálogo.

AVISO

- Se a chave privada não for gerenciada, ela poderá ser baixada apenas uma vez. Guarde-a adequadamente. 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, você pode exportar a chave privada a qualquer momento, conforme necessário.

Passo 12 Depois que a chave privada for salva, clique em **OK**. O par de chaves foi criado com sucesso.

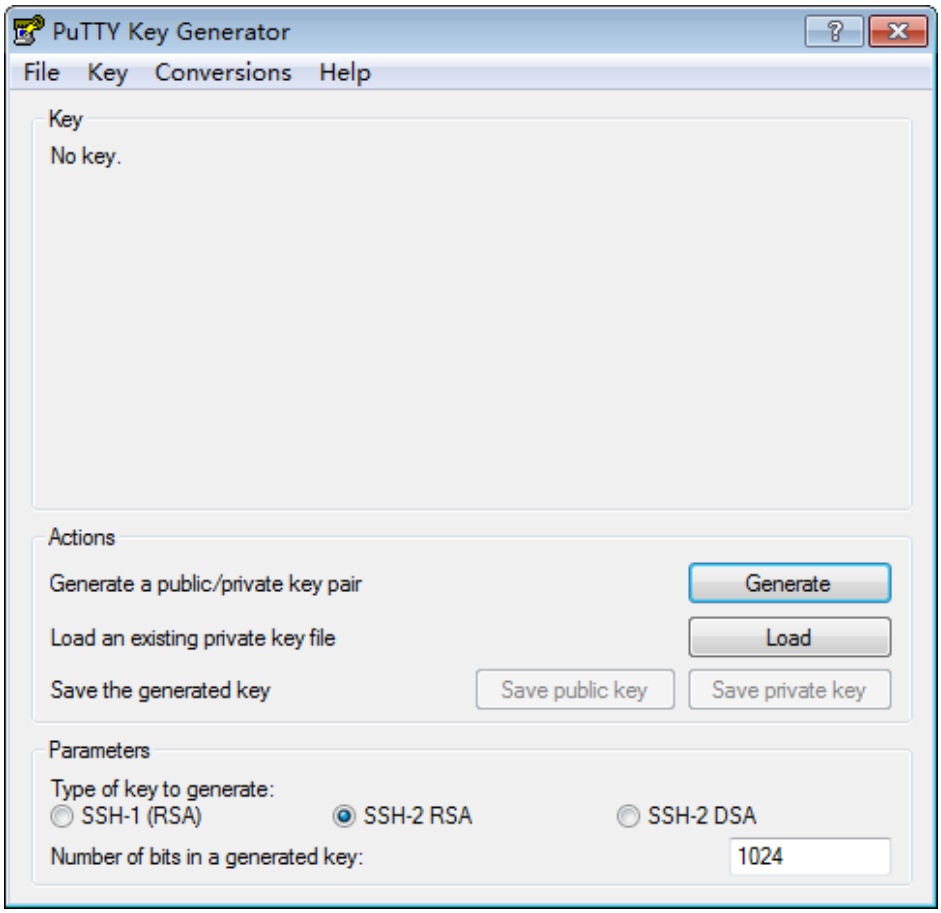
Depois que o par de chaves for criado, você poderá visualizá-lo na lista de pares de chaves. A lista exibe informações como nome do par de chaves, impressão digital, chave privada e quantidade.

----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 em **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

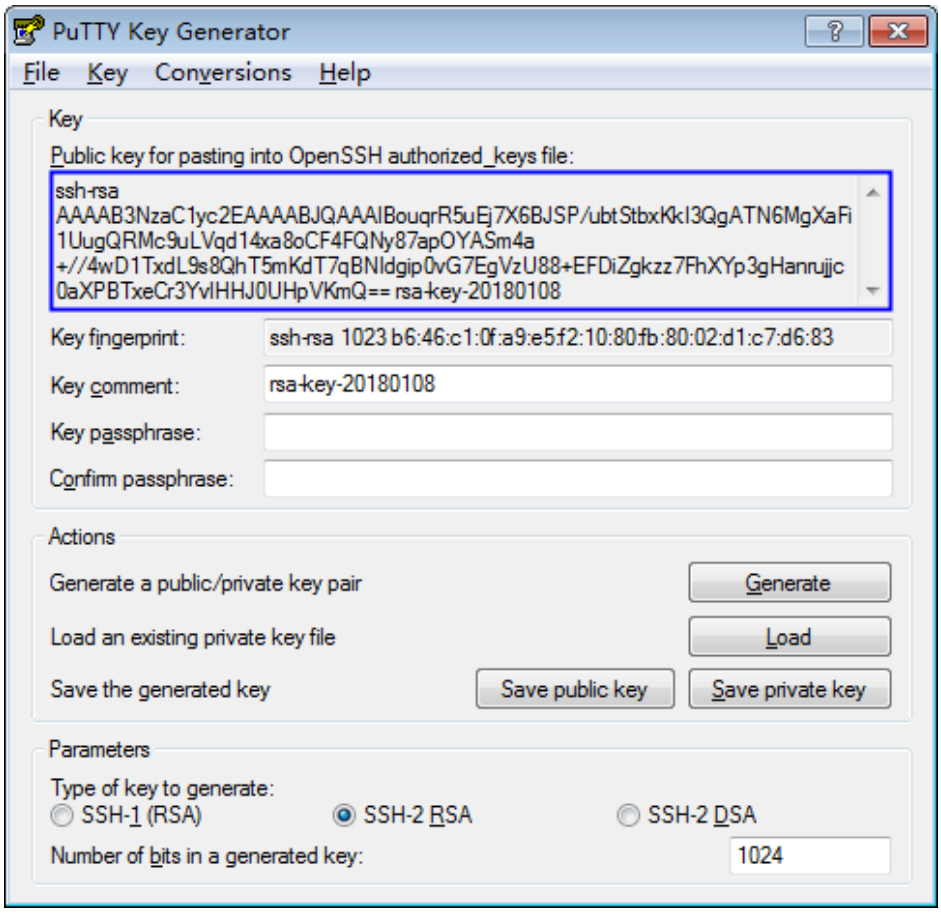
Parâmetro	Descrição
Type of key to generate	Algoritmo de criptografia e descriptografia de pares de chaves a importar para o console de gerenciamento. Atualmente, apenas **SSH-2 RSA** é suportado.

Parâmetro	Descrição
Number of bits in a generated key	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. Mantenha-a segura.

Tabela 3-2 Formato de um arquivo de chave privada

Formato de arquivo de chave privada	Cenário de uso da chave privada	Método de salvamento
PEM	• Usar a ferramenta Xshell para efetuar logon no servidor de nuvem que executa o sistema operacional de Linux. • Gerenciar 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	Usar 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.
- O par de chaves importado é um par de chaves de conta. Se um par de chaves privadas com o mesmo nome tiver sido criado, o sistema exibirá uma mensagem indicando que o nome do par de chaves já existe quando você importar o par de chaves da conta.
- Cada usuário do IAM não tem um par de chaves privadas com o mesmo nome.

Restrições

- As chaves SSH importadas para o console do KPS suportam os seguintes algoritmos criptográficos:
  - SSH-DSS
  - SSH-ED25519
  - ECDSA-SHA2-NISTP256
  - ECDSA-SHA2-NISTP384
  - ECDSA-SHA2-NISTP521
  - SSH_RSA: o comprimento pode ser 2048, 3072 e 4096 bits.
- 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 **Faça logon no console de gerenciamento**.

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

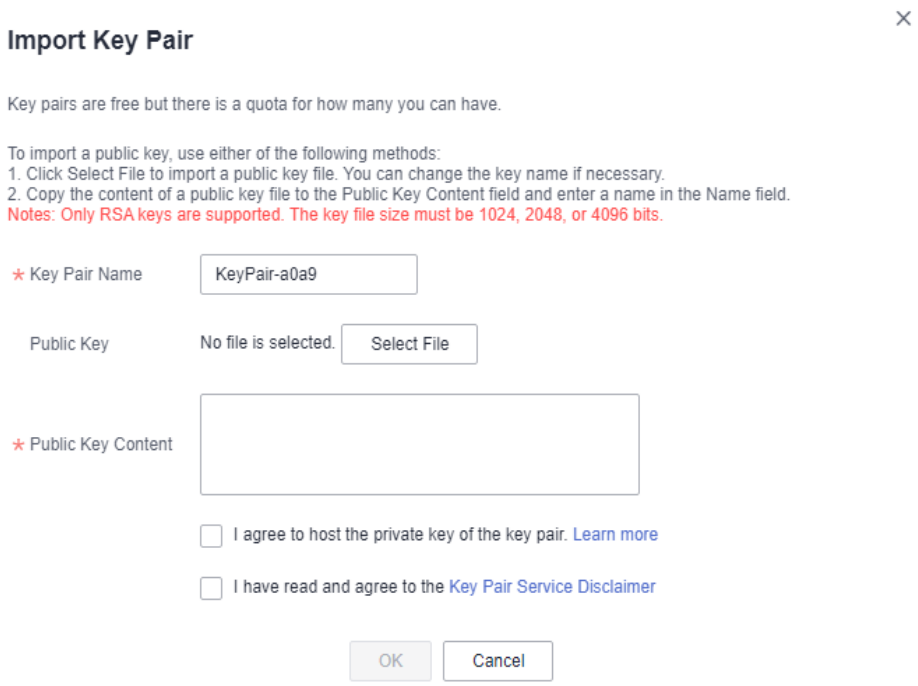
Passo 3 Clique em  à esquerda, escolha **Security & Compliance** > **Data Encryption Workshop**, a página de gerenciamento de chaves é exibida.

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**, como mostrado em **Figura 3-5**.

Figura 3-5 Importação de um par de chaves

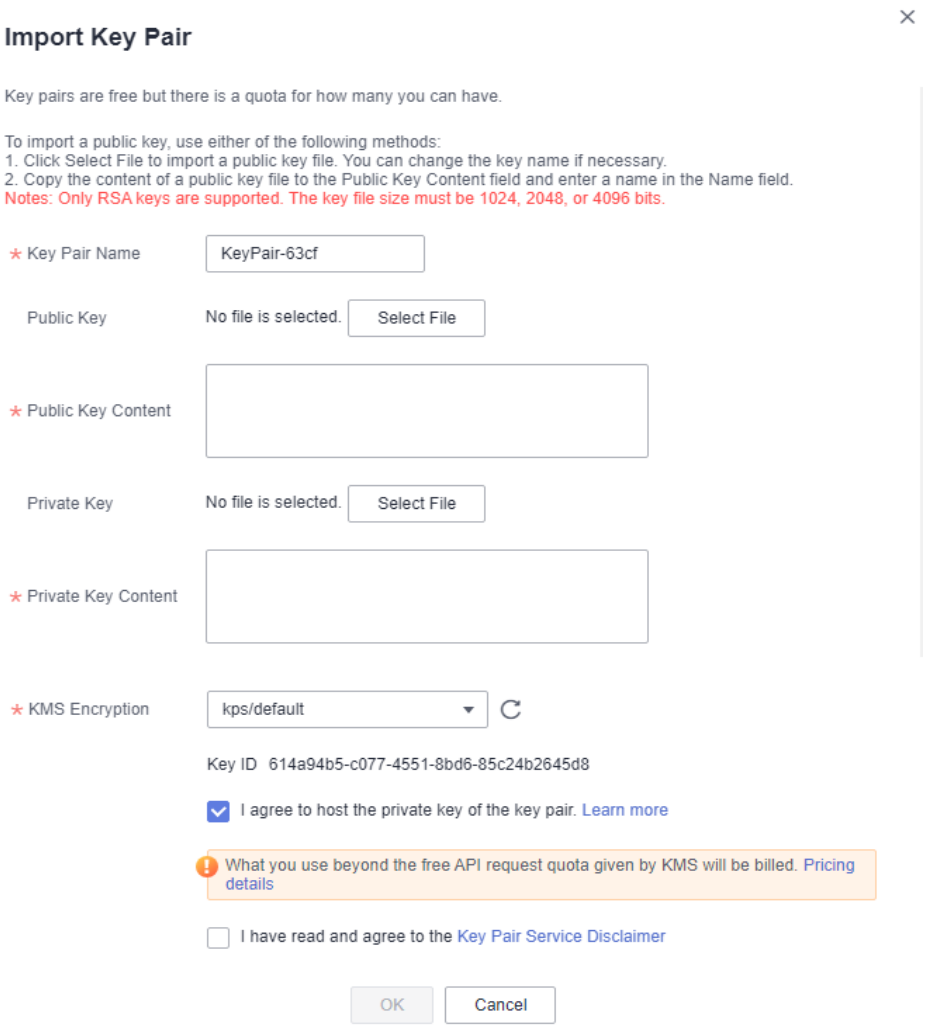


NOTA

- Você pode personalizar o nome de um par de chaves importado.
- Se o sistema exibir uma mensagem indicando que o nome já existe, será necessário alterar o nome do par de chaves porque o nome foi criado por outro usuário do IAM.

Passo 7 Se você quiser que sua chave privada seja gerenciada, leia e confirme **I agree to host the private key of the key pair.**, conforme mostrado em **Figura 3-6**. Ignore esta etapa se você não precisar gerenciar a chave privada.

Figura 3-6 Gerenciamento de chaves privadas



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 do KMS do par de chaves, o KMS cria automaticamente uma chave principal 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 *Aviso de isenção de responsabilidade do serviço de par de chaves* 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.
- Os usuários com a função de sistema Administrador do locatário devem realizar a atualização pelo menos uma vez. O número de pares de chaves a serem atualizados não é limitado.
- 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.
- Se um par de chaves privadas for atualizado para um par de chaves de conta, a cota de par de chaves de conta não será ocupada.

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.

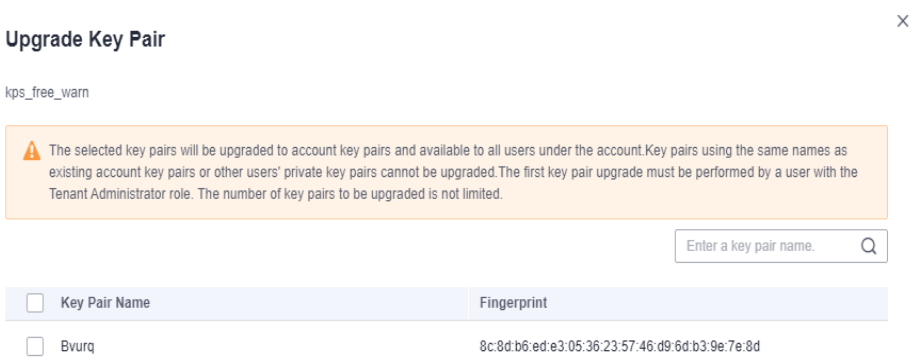
Passo 3 Clique em à esquerda, escolha **Security & Compliance** > **Data Encryption Workshop**, a página de gerenciamento de chaves é exibida.

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 executa o Linux, poderá vincular um par de chaves ao ECS no console do KPS. O KPS configurará o par de chaves e, em seguida, o modo de logon do ECS será alterado para **Key Pair**. Depois que o par de chaves é vinculado, você pode usar a chave privada para fazer 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-se a um par de chaves, você pode gravar 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 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 **Faça logon no console de gerenciamento**.

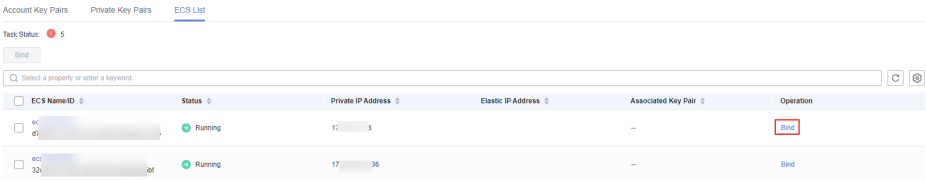
Passo 2 Clique em  no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

Passo 3 Clique em  à esquerda, escolha **Security & Compliance** > **Data Encryption Workshop**, a página de gerenciamento de chaves é exibida.

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

Passo 5 Clique em **ECS List** para exibir os ECSs, conforme mostrado em **Figura 3-8**.

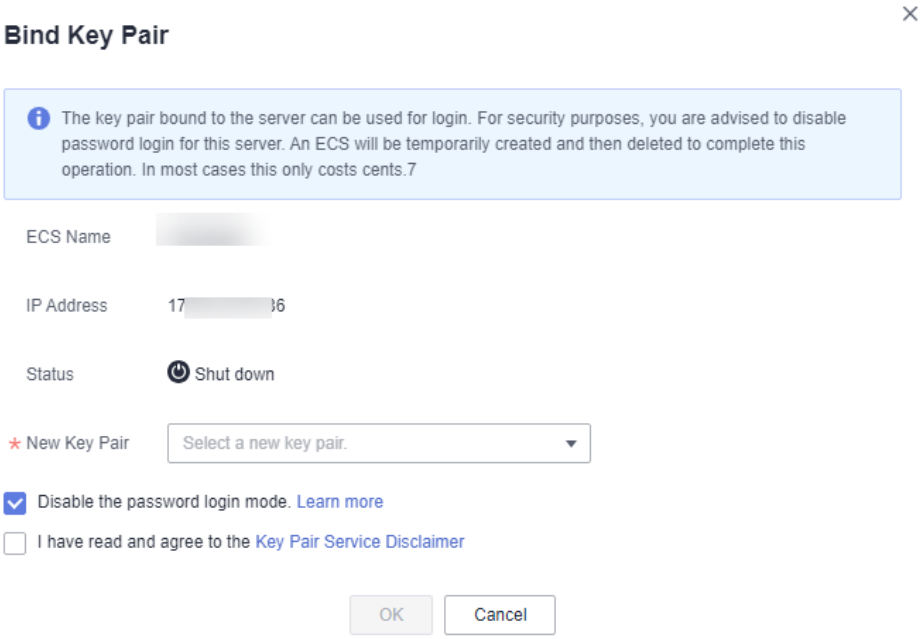
Figura 3-8 Vinculação



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

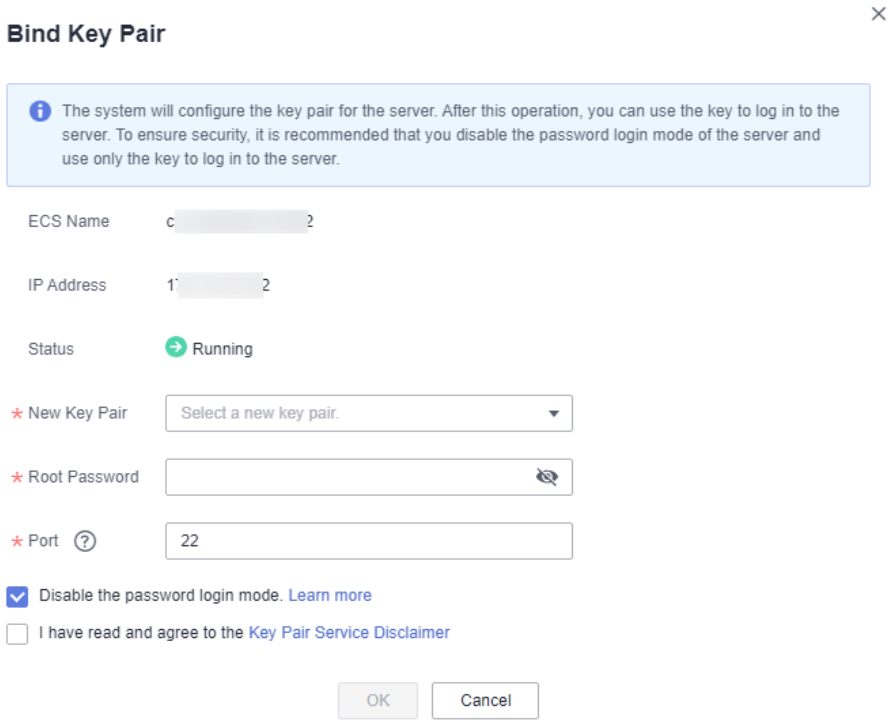
- Se o ECS for desligado, uma caixa de diálogo será exibida, conforme mostrado em **Figura 3-9**.

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



- Se o ECS estiver em execução, você precisará fornecer a senha de raiz. Para mais detalhes, consulte **Figura 3-10**.

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



NOTA

- Se você tiver a senha de raiz do ECS, poderá inserir diretamente a senha para vincular o par de chaves ao ECS.
- Se você não tiver a senha de 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 O número de porta padrão é 22 e pode ser modificado.

NOTA

Antes de usar a porta definida pelo usuário, certifique-se de que:

- O par de chaves pode ser conectado ao ECS usando a porta. Para obter detalhes sobre como modificar a configuração de grupo de segurança de um ECS, consulte **Configuração de regras de grupos de segurança**.
- Modifique a porta padrão do ECS e certifique-se de que a porta esteja ativada. Para obter detalhes, consulte **Aprimoramento da segurança para logons SSH em ECSs de Linux**.

Passo 9 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 fazer 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 10 Selecione **I have read and agree to the Key Pair Service Disclaimer**.

Passo 11 Clique em **OK** para concluir a operação.

- Se o ECS não for encerrado, use a senha de 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 Vinculação de pares de chaves em lotes

Quando o ECS está no estado **Running**, você pode vincular pares de chaves em lotes no console.

Esta seção descreve como vincular pares de chaves em lotes no console do KMS.

Cenário de aplicação

- Se vários ECSs a serem vinculados tiverem a mesma senha, você poderá inserir a senha e selecionar o par de chaves com apenas alguns cliques.
- Se as senhas dos ECSs a serem vinculados forem diferentes, você poderá inserir suas senhas e selecionar o mesmo par de chaves para a vinculação.

Pré-requisitos

- O ECS deve estar no estado **Running**.
- O ECS não foi vinculado a um par de chaves.

Restrições

- No console de gerenciamento, os pares de chaves não podem ser vinculados a ECSs que executam o 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.
- Você pode vincular pares de chaves a um máximo de 10 ECSs por vez.

Procedimento

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

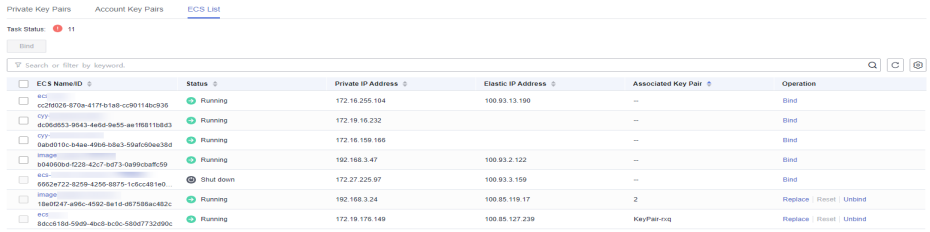
Passo 2 Clique em  no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

Passo 3 Clique em  à esquerda, escolha **Security & Compliance** > **Data Encryption Workshop**, a página de gerenciamento de chaves é exibida.

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

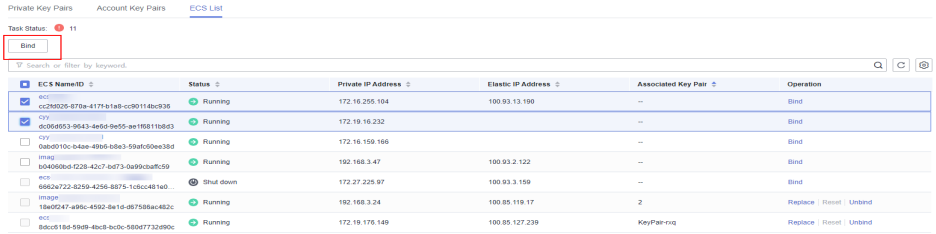
Passo 5 Clique em **ECS List**. A página da lista do ECS é exibida, conforme mostrado em **Figura 3-11**.

Figura 3-11 Lista do ECS



Passo 6 Selecione os servidores a serem vinculados em lotes e clique em **Bind** acima da caixa de pesquisa, conforme mostrado em **Vinculação de pares de chaves em lotes**. Para obter detalhes, consulte **Figura 3-12**.

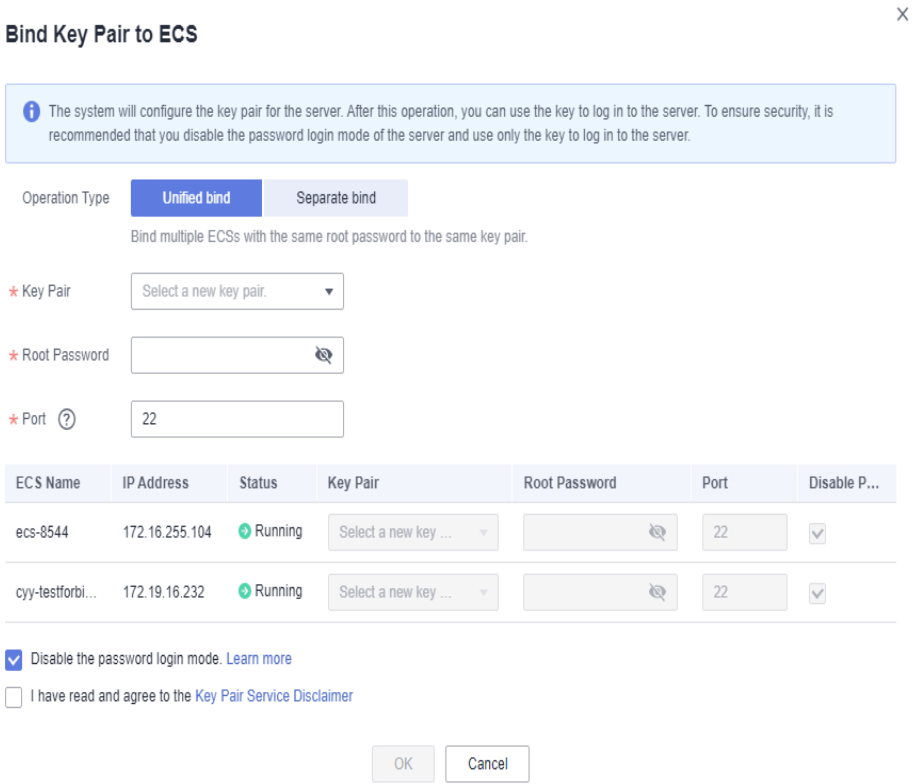
Figura 3-12 Vinculação de pares de chaves em lotes



Passo 7 Clique em **Bind**. A caixa de diálogo **Bind Key Pair to ECS** é exibida.

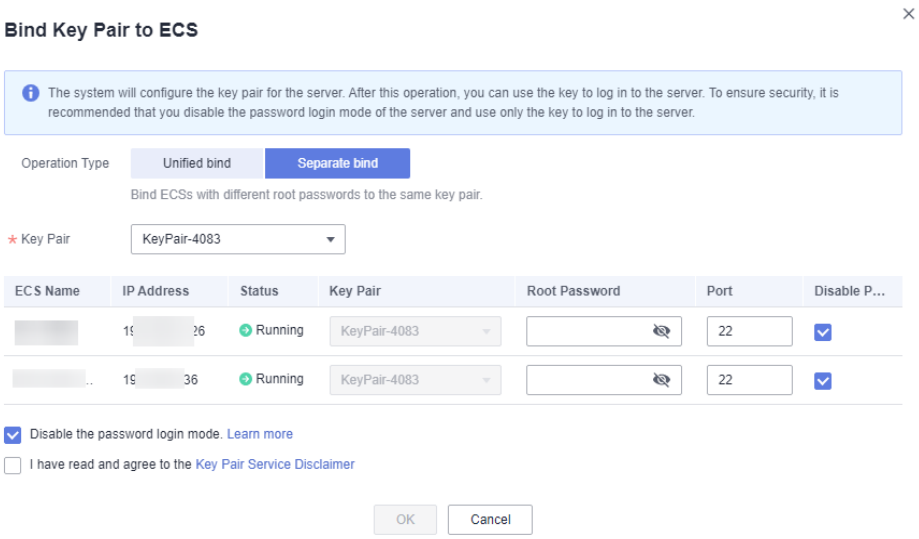
- Se as senhas dos ECSs a serem vinculados forem as mesmas, você poderá selecionar um par de chaves com um clique e digitar a senha para vincular o par de chaves. Para obter detalhes, consulte **Figura 3-13**.

Figura 3-13 Vinculação unificada



- Se as senhas dos ECSs a serem vinculados forem diferentes, você poderá vinculá-las separadamente. Para obter detalhes, consulte **Figura 3-14**.

Figura 3-14 Vinculação separada



NOTA

Se você selecionar **Unified bind**, somente o mesmo par de chaves poderá ser usado para vinculação.

Passo 8 O número de porta padrão é 22 e pode ser modificado.

NOTA

Antes de usar a porta definida pelo usuário, certifique-se de que:

- O par de chaves pode ser conectado ao ECS usando a porta. Para obter detalhes sobre como modificar a configuração de grupo de segurança de um ECS, consulte **Configuração de regras de grupos de segurança**.
- Modifique a porta padrão do ECS e certifique-se de que a porta esteja ativada. Para obter detalhes, consulte **Aprimoramento da segurança para logons SSH em ECSs de Linux**.

Passo 9 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 fazer 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 10 Selecione **I have read and agree to the Key Pair Service Disclaimer**.

Passo 11 Clique em **OK**. Os pares de chaves são vinculados em lotes. A vinculação leva cerca de 3 a 5 minutos.

----Fim

3.4.3 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.

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 à esquerda, escolha **Security & Compliance** > **Data Encryption Workshop**, a página de gerenciamento de chaves é exibida.

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

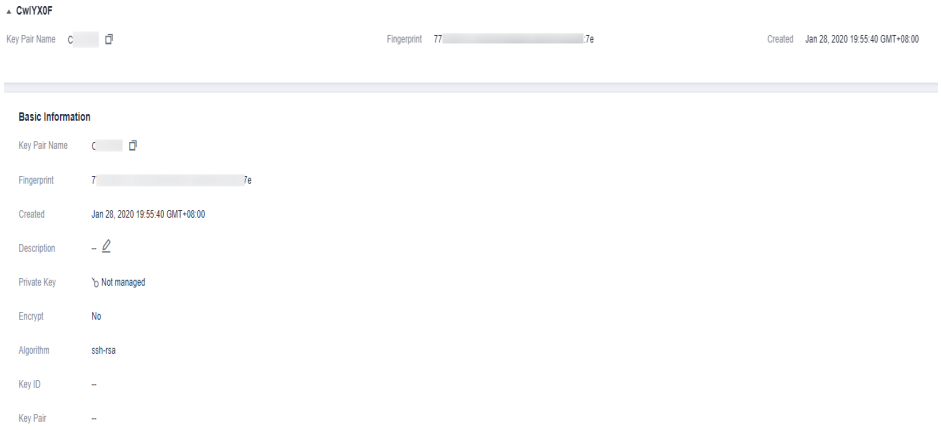
Passo 5 Clique na guia **Private Key Pairs** e visualize as informações sobre o par de chaves na lista de pares de chaves.

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 usando o par de chaves são exibidas.

Figura 3-15 Detalhes do par de chaves



NOTA

Ao comprar 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.

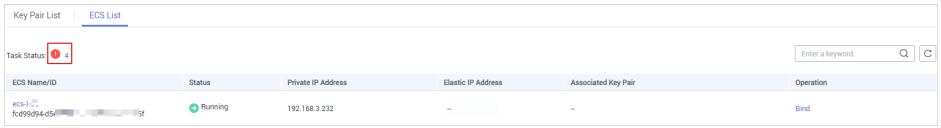
Vincule um par de chaves a ECSs. Para obter detalhes sobre parâmetros, consulte **Tabela 3-3**.

Tabela 3-3 Descrição do parâmetro

Parâmetro	Descrição
ECS Name/ID	Nome e ID de um ECS
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 3-16 Lista do ECS



Passo 8 Clique no número ao lado do ícone de status da tarefa para visualizar as tarefas com falha, conforme mostrado em **Figura 3-17**

NOTA

Status da redefinição ou substituição do par de chaves:

: em execução

: falha na execução

Figura 3-17 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

3.4.4 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. Após 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 **Faça logon no console de gerenciamento**.

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

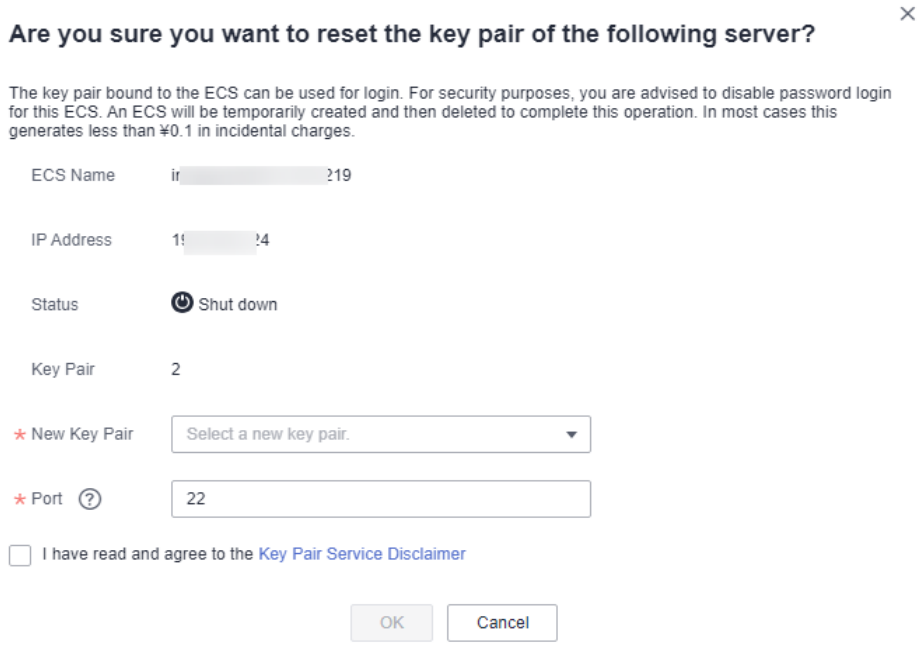
Passo 3 Clique em à esquerda, escolha **Security & Compliance** > **Data Encryption Workshop**, a página de gerenciamento de chaves é exibida.

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, conforme mostrado na **Figura 3-18**.

Figura 3-18 Redefinição de um par de chaves



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

Passo 8 O número de porta padrão é 22 e pode ser modificado.

NOTA

Antes de usar a porta definida pelo usuário, certifique-se de que:

- O par de chaves pode ser conectado ao ECS usando a porta. Para obter detalhes sobre como modificar a configuração de grupo de segurança de um ECS, consulte **Configuração de regras de grupos de segurança**.
- Modifique a porta padrão do ECS e certifique-se de que a porta esteja ativada. Para obter detalhes, consulte **Aprimoramento da segurança para logons SSH em ECSs de Linux**.

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 reiniciado em cerca de 10 minutos.

----Fim

3.4.5 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 fazer logon no ECS, e a chave privada original não pode ser usada para fazer logon no ECS.

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

Pré-requisitos

- O ECS cujo par de chaves deve ser 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 **Faça logon no console de gerenciamento**.

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

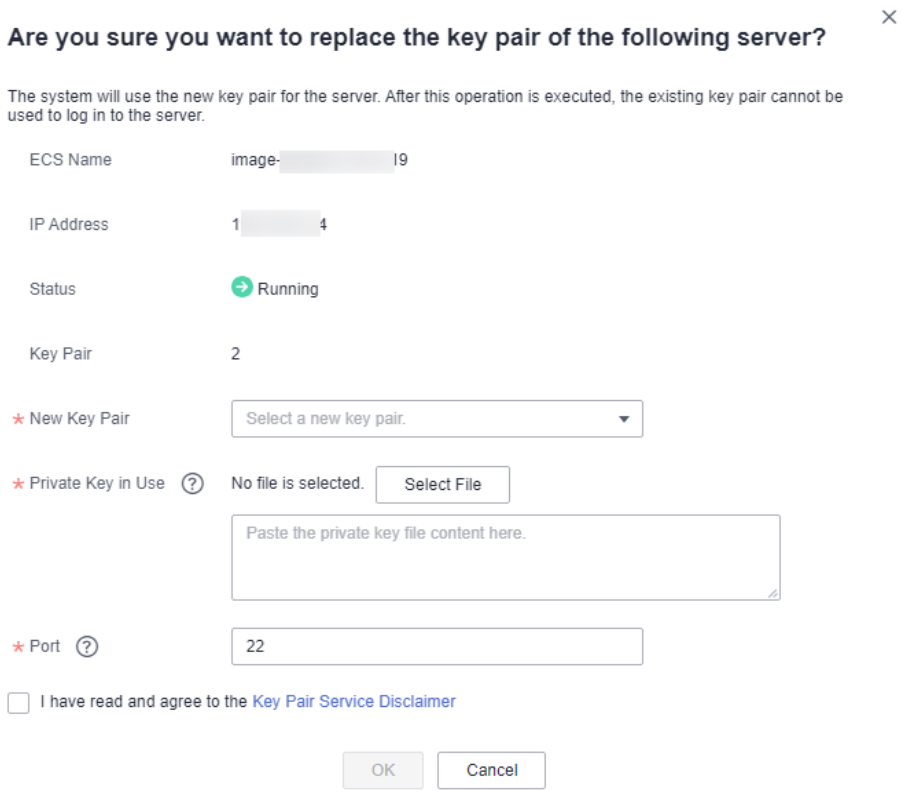
Passo 3 Clique em à esquerda, escolha **Security & Compliance** > **Data Encryption Workshop**, a página de gerenciamento de chaves é exibida.

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. Para obter detalhes, consulte **Figura 3-19**.

Figura 3-19 Substituição de 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 (no formato .pem) do par de chaves original ou copiar 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, converta-a consultando **Como converter o formato de um arquivo de chave privada?**

Passo 9 O número de porta padrão é 22 e pode ser modificado.

NOTA

Antes de usar a porta definida pelo usuário, certifique-se de que:

- O par de chaves pode ser conectado ao ECS usando a porta. Para obter detalhes sobre como modificar a configuração de grupo de segurança de um ECS, consulte **Configuração de regras de grupos de segurança**.
- Modifique a porta padrão do ECS e certifique-se de que a porta esteja ativada. Para obter detalhes, consulte **Aprimoramento da segurança para logons SSH em ECSs de Linux**.

Passo 10 Selecione **I have read and agree to the Key Pair Service Disclaimer**.

Passo 11 Clique em **OK**. O par de chaves será substituído do ECS em cerca de um minuto.

----Fim

3.4.6 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 no console de gerenciamento. O KPS irá desvincular o par de chaves do ECS. Depois que o par de chaves for desvinculado, você poderá usar a senha para fazer 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 efetuar 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 *Guia de usuário do Elastic Cloud Server*.
- Se você ativou o logon do par de chaves para um ECS durante sua criação, mas desvinculou o par de chaves usado para logon, para vincular o par de chaves novamente, desligue o ECS primeiro.

- Depois de desvincular um ECS do seu par de chaves, redefina a senha no console do ECS em tempo hábil. Para obter mais informações, consulte *Guia de usuário do Elastic Cloud Server*.

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 à esquerda, escolha **Security & Compliance** > **Data Encryption Workshop**, a página de gerenciamento de chaves é exibida.

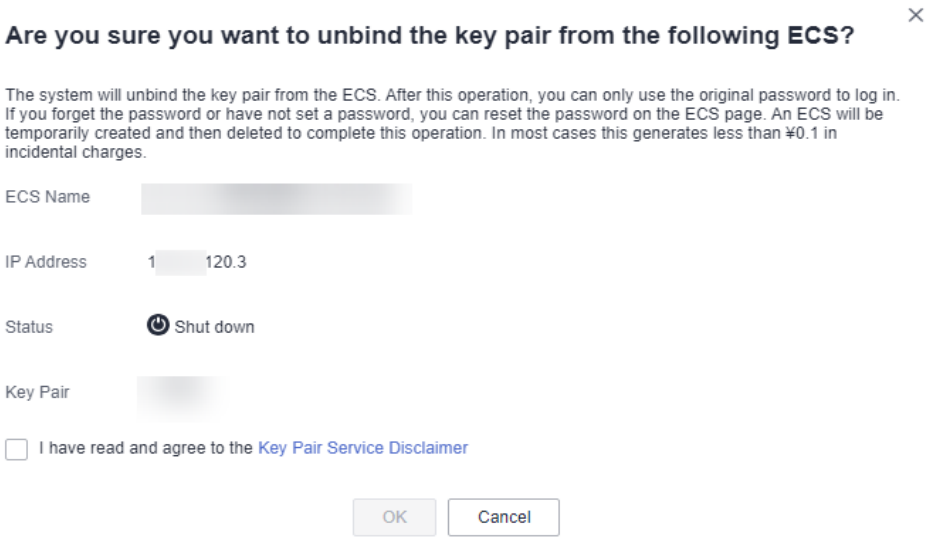
Passo 4 No painel de navegação à esquerda, clique em **Key Pair Service**.

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

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

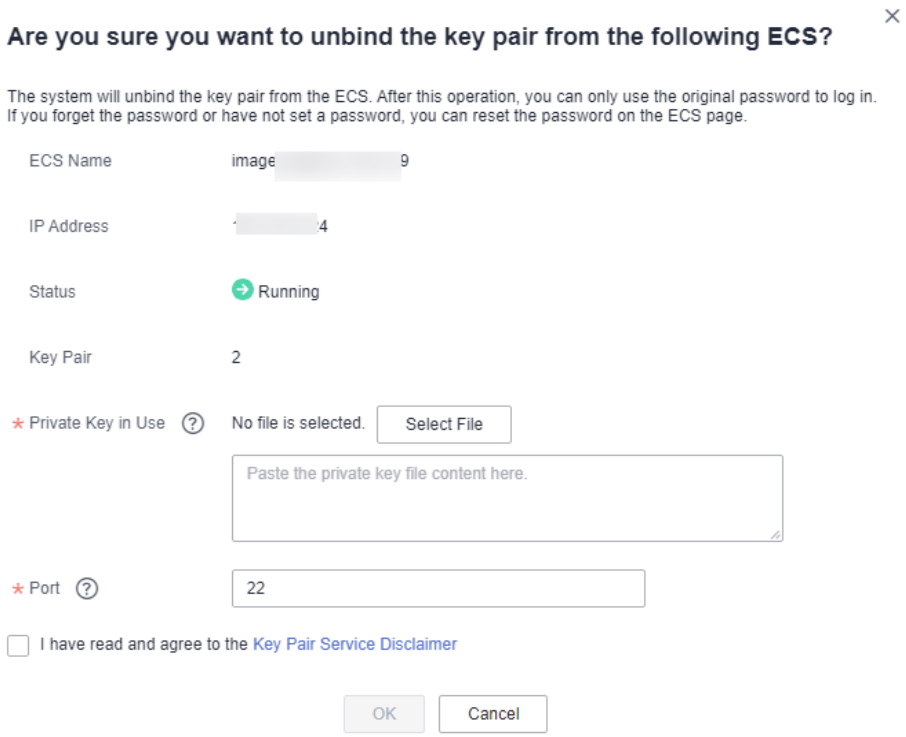
- Se o ECS for desligado, será exibida uma caixa de diálogo, conforme mostrado em **Figura 3-20**.

Figura 3-20 Desvinculação de um par de chaves (1)



- Se o ECS estiver em execução, uma caixa de diálogo será exibida.

Figura 3-21 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 upload 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, pule 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, converta-a consultando **Como converter o formato de um arquivo de chave privada?**

Passo 8 O número de porta padrão é 22 e pode ser modificado.

NOTA

Antes de usar a porta definida pelo usuário, certifique-se de que:

- O par de chaves pode ser conectado ao ECS usando a porta. Para obter detalhes sobre como modificar a configuração de grupo de segurança de um ECS, consulte **Configuração de regras de grupos de segurança**.
- Modifique a porta padrão do ECS e certifique-se de que a porta esteja ativada. Para obter detalhes, consulte **Aprimoramento da segurança para logons SSH em ECSs de Linux**.

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

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

NOTA

Depois de desvincular um ECS do seu par de chaves, redefina a senha no console do ECS em tempo hábil. Para obter mais informações, consulte *Guia de usuário do Elastic Cloud Server*.

----Fim

3.4.7 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 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 **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 à esquerda, escolha **Security & Compliance** > **Data Encryption Workshop**, a página de gerenciamento de chaves é exibida.

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, insira **DELETE** e 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, converta-a consultando **Como converter o formato de um arquivo de chave privada?**
- Quando você ativa a função de criptografia para um par de chaves, o KMS cria automaticamente uma chave 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 **Faça logon no console de gerenciamento**.

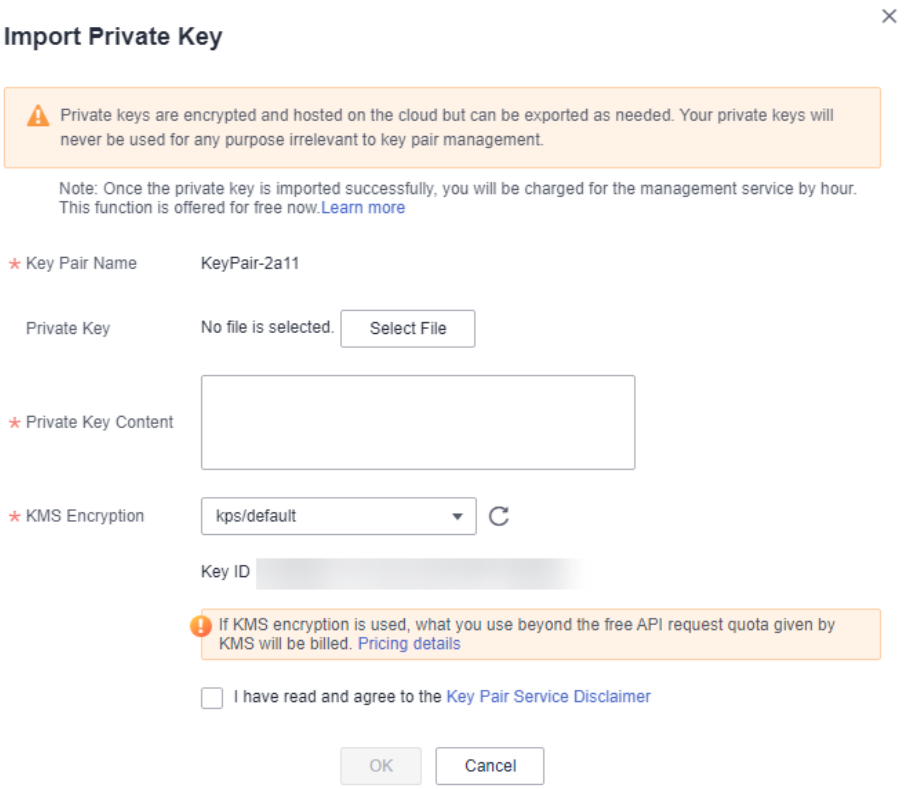
Passo 2 Clique em  no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

Passo 3 Clique em  à esquerda, escolha **Security & Compliance** > **Data Encryption Workshop**, a página de gerenciamento de chaves é exibida.

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**. Para mais detalhes, consulte **Figura 3-22**.

Figura 3-22 Importação de 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.

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

NOTA

- Quando você ativa a função de criptografia para um par de chaves, o KMS cria automaticamente uma chave 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 pelo console de gerenciamento, poderá fazer o download das chaves privadas 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 **Faça logon no console de gerenciamento**.

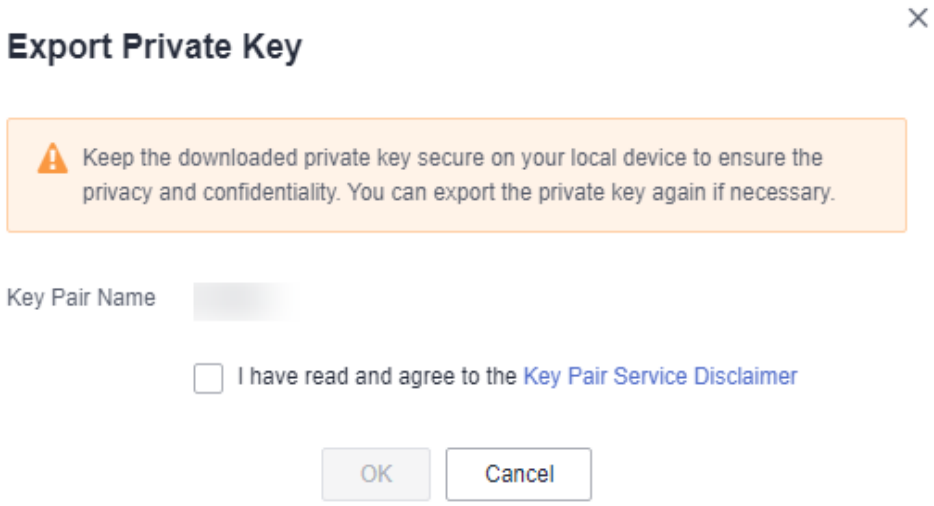
Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

Passo 3 Clique em à esquerda, escolha **Security & Compliance** > **Data Encryption Workshop**, a página de gerenciamento de chaves é exibida.

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 em **Figura 3-23**.

Figura 3-23 Exportação de 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 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 é limpa, você não pode obter a chave privada da Huawei Cloud. Tenha cuidado ao realizar esta operação. Se precisar que a chave privada seja gerenciada novamente, você poderá importar a chave privada para o 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  à esquerda, escolha **Security & Compliance** > **Data Encryption Workshop**, a página de gerenciamento de chaves é exibida.

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 é limpa, você não pode obter a chave privada da Huawei Cloud. Tenha cuidado ao realizar esta operação. Se precisar que a chave privada seja gerenciada novamente, você poderá importar a chave privada para o console de gerenciamento.

----Fim

3.6 Uso de 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 comprar 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 chaves privadas do ECS devem atender aos seguintes requisitos.

Tabela 3-4 Formatos de arquivo de chave privada

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

Fazer logon em um computador do Windows

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

Método 1: usar 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**.

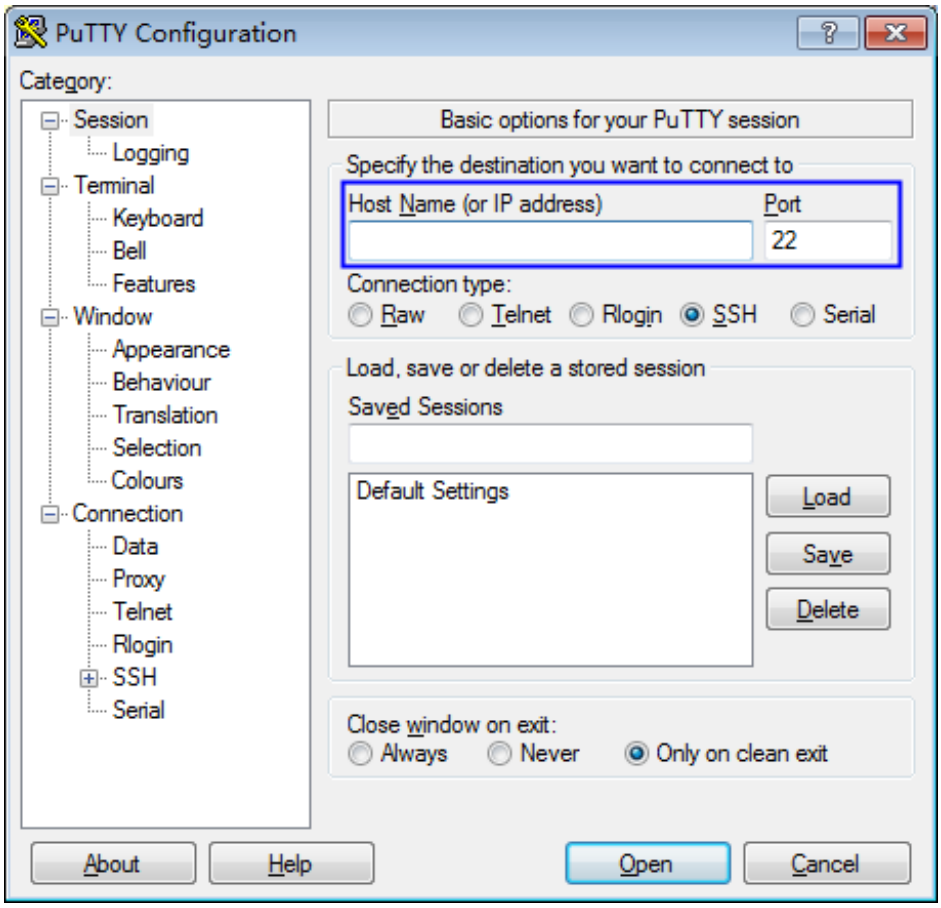
NOTA

- 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 **Connection** > **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 3-24 Configuração do EIP



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

----Fim

Método 2: usar 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 do Linux

Para efetuar logon no ECS do Linux a partir de um computador do Linux, execute as operações descritas a seguir: o procedimento a seguir usa o arquivo de chave privada **kp-123.ppk** como 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 efetuar 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 Uso de 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. Em primeiro lugar, você deve obter a senha de administrador (senha da conta **Administrator** ou outra conta definida em Cloudbase-Init) gerada durante a instalação inicial do ECS a partir do arquivo de chave privada baixado quando você criou o ECS. Essa senha é gerada aleatoriamente, com alta segurança.

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

Pré-requisitos

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 de senha inicial 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 *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 *Referência de API do Elastic Cloud Server*.
- O arquivo de chave privada 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  no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

Passo 3 Clique em  e escolha **Compute** > **Elastic Cloud Server**.

Passo 4 Na lista do ECS, selecione o ECS cuja senha você deseja obter.

Passo 5 Na coluna **Operation**, clique em **More** e escolha **Get Password**.

Passo 6 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 7 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 criada, 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 criar instâncias do HSM dedicado por meio do console de gerenciamento. Depois que uma instância do HSM dedicado for criada, 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 as aplicações de serviço a acessar as instâncias do HSM dedicado. **Figura 4-1** ilustra o fluxo da operação.

Figura 4-1 Guia de operação

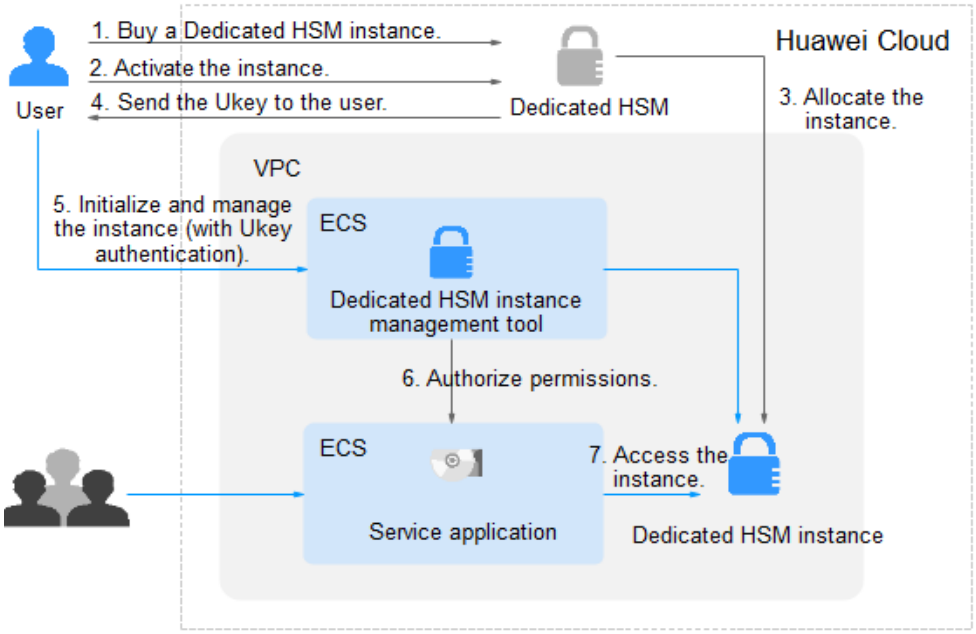


Tabela 4-1 descreve o guia de operação.

Tabela 4-1 Descrições do guia de operação

N.º	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. Em seguida, você pode pagar pela instância solicitada.	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	Aloque uma instância do HSM dedicado.	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 depois que o especialista analisar e confirmar seu pedido.	Especialista em segurança do HSM dedicado

N.º	Procedimento	Descrição	Operado por
4	Obtenha o UKey, os documentos de inicialização e o software.	• Um especialista em segurança envia o Ukey para o endereço de e-mail que você forneceu. Um UKey é o único identificador de um usuário do HSM dedicado. Guarde-o adequadamente. • Um especialista em segurança fornecerá a você o software e o guia para inicializar as instâncias do HSM dedicado. Se você tiver alguma dúvida, entre em contato com o especialista. **NOTA** Você pode enviar um **Tíquete de serviço** para fornecer o endereço do destinatário do UKey e entrar em contato com especialistas em segurança para obter orientação.	Especialista em segurança do HSM dedicado
5	Inicialize e gerencie 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 **Inicialização de uma instância de HSM dedicado**.	Usuário
6	Instale o agente de segurança e conceda permissões de acesso.	Instale e inicialize o agente de segurança nos nós de aplicações de serviço. Para mais detalhes, consulte **Instalação do agente de segurança e concessão de 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 Criação de uma instância do HSM dedicado

Ao criar uma instância de HSM dedicado, você precisa especificar a região e preencher suas informações de contato.

A taxa para uma instância de HSM dedicado na edição platinum consiste nas duas partes a seguir:

- Taxa de instalação inicial, cobrada quando você cria uma instância de HSM dedicado.
- Taxa anual/mensal, cobrada na **Ativação de uma instância do HSM dedicado**.

Pré-requisitos

Você obteve a conta de logon (com as permissões **Ticket Administrator** e **KMS Administrator**) e a senha para efetuar logon no console de gerenciamento.

Restrições

- Ao comprar uma instância de HSM dedicado, você precisa enviar um tíquete de serviço para definir as informações do destinatário do UKey. Somente as contas com a permissão **Ticket Administrator** podem enviar tíquetes de serviço.
- Depois de criar uma instância, um UKey será enviado para o endereço em suas informações de contato. Em seguida, você pode usar o UKey para inicializar e autorizar suas aplicações de serviço a acessar a instância.

  Você precisa ativar a instância antes de usá-la.

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 Clique em à esquerda, escolha **Security & Compliance** > **Data Encryption Workshop**, a página de gerenciamento de chaves é exibida.

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

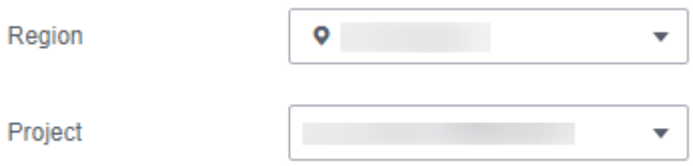
Passo 5 Clique em **Create Dedicated HSM** no canto superior direito da página.

Passo 6 **Billing Mode** só pode ser definido como **Yearly/Monthly**.

Figura 4-2 Modo de cobrança

Passo 7 Selecione uma região e um projeto.

Figura 4-3 Selecionar uma região



NOTA

- Selecione a região atual e o projeto padrão.
- Somente o projeto padrão é suportado. Projetos definidos pelo usuário não podem ser criados.

Passo 8 Selecione a edição de serviço para a instância. Consulte a **Figura 4-4** para obter detalhes. **Tabela 4-2** lista os parâmetros relacionados.

Figura 4-4 Edição platinum (fora da China continental)

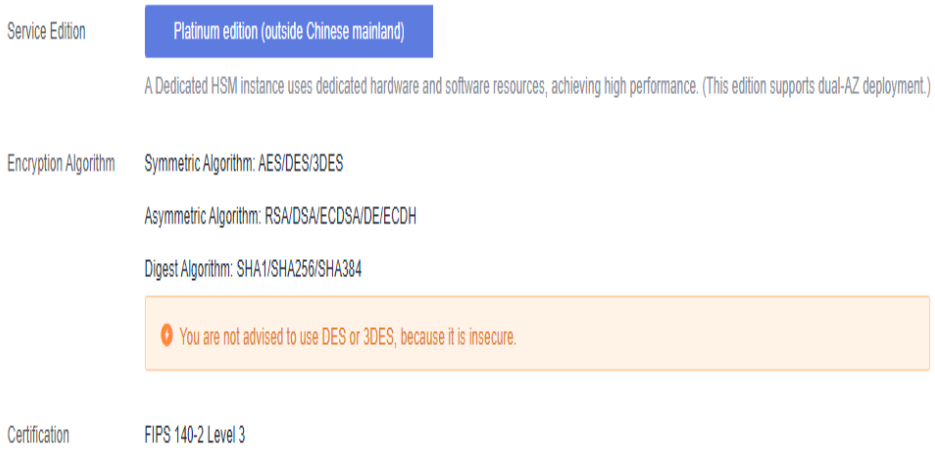


Tabela 4-2 Parâmetros de edição

Parâmetro	Descrição
Service Edition	Edição platinum (fora da China continental)
Encryption Algorithm	Algoritmo suportado pela instância do HSM. ● Algoritmo simétrico: AES ● Algoritmo assimétrico: RSA, DSA, ECDSA, DE e ECDH ● Algoritmo de resumo: SHA1, SHA256, SHA384
Certification	Certificada pela FIPS 140-2 Nível 3

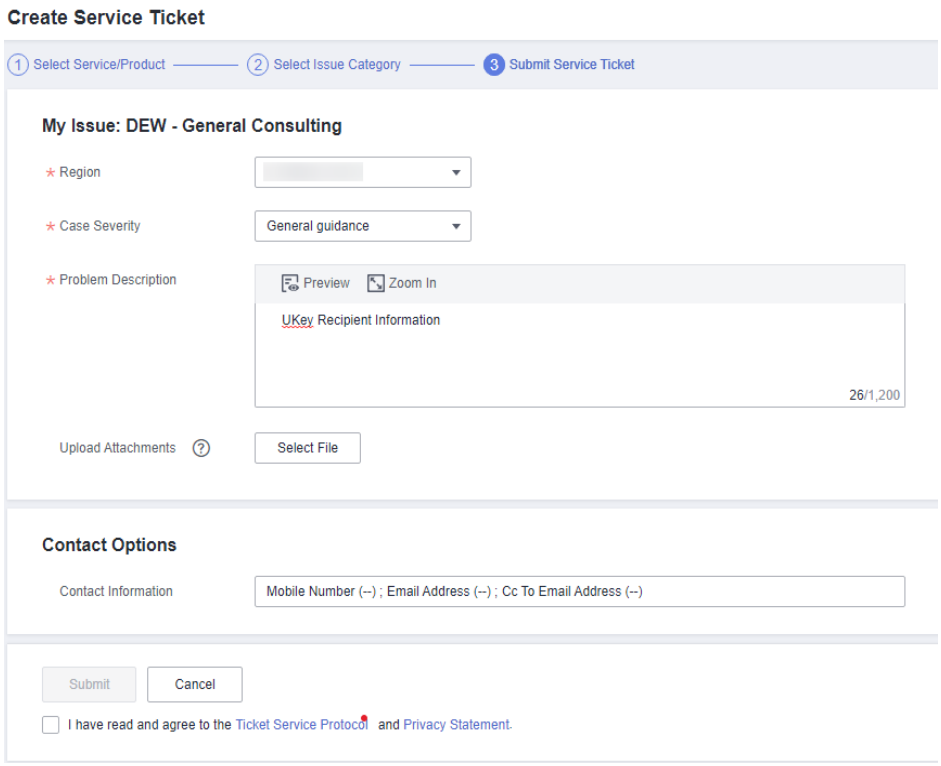
Passo 9 Escolha **Service Tickets** > **Create Service Ticket**. Nossos especialistas da Huawei Cloud entrarão em contato com você e fornecerão um plano de compra personalizado e sua cotação.

- Na lista suspensa **Case Severity**, selecione **General guidance**.
- Na caixa de texto **Problem Description**, insira **Dedicated HSM Contact Information**.
- **Contact Information**: insira o número de telefone e o endereço de e-mail para receber as informações de andamento do tíquete de serviço.

AVISO

Certifique-se de que as informações de contato fornecidas na caixa de texto **Confidential Information** sejam válidas para que nossos especialistas em segurança possam entrar em contato com você em tempo hábil.

Figura 4-5 Criar um tíquete de serviço



Passo 10 Clique em **Submit**. O tíquete de serviço é exibido na página **My Service Tickets**.

NOTA

Depois que o tíquete de serviço for criado com sucesso, você poderá clicar em **View Details** na coluna **Operation** para exibir os detalhes. Você pode lembrar a equipe de suporte de um tíquete de serviço, deixar suas mensagens, cancelar um tíquete de serviço ou fechar um tíquete de serviço com base nos status do tíquete de serviço.

----Fim

4.2.2 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

O status da instância do HSM dedicado é **To be activated**.

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 de HSM dedicado é criada com sucesso, ela não pode ser alterada para outro tipo. 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 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou um projeto.

Passo 3 Clique em à esquerda, escolha **Security & Compliance** > **Data Encryption Workshop**, a página de gerenciamento de chaves é exibida.

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

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

Passo 6 Selecione uma AZ.

Figura 4-6 Selecionar uma AZ

Passo 7 Insira as informações de ativação, conforme mostrado na **Figura 4-7**. A **Tabela 4-3** descreve os parâmetros.

Figura 4-7 Configuração de uma instância do HSM dedicado

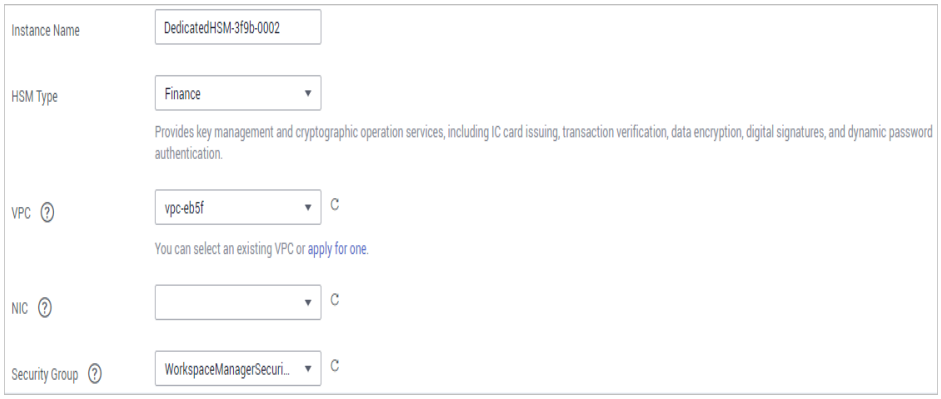


Tabela 4-3 Parâmetros de ativação

Parâmetro	Descrição	Exemplo de valor
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
Enterprise Project	Projeto empresarial ao qual o HSM dedicado será vinculado	default
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
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)**

Parâmetro	Descrição	Exemplo de valor
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.

Procedimento

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

Passo 2 Clique em . Escolha **Security & Compliance** > **Data Encryption Workshop**. A página **Key Management Service** será exibida.

Passo 3 No painel de navegação, escolha **Dedicated HSM**.

Passo 4 Na lista, você pode exibir as informações sobre as instâncias do HSM.

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

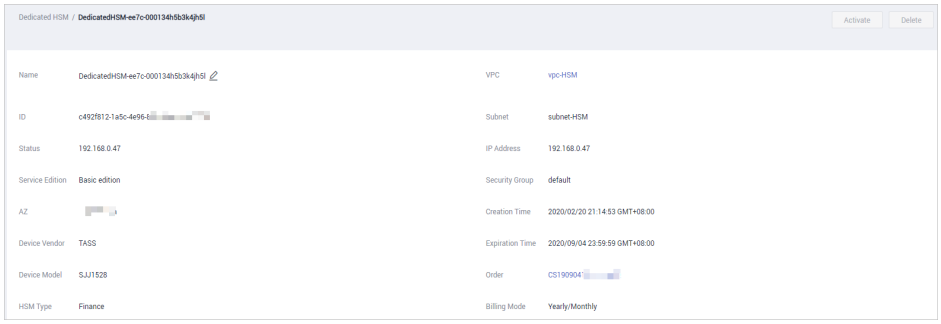
Tabela 4-4 Parâmetros de instância do HSM dedicado

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 (fora da China continental)** ● Edição platinum (fora da China continental): você pode usar exclusivamente o sub-rack do HSM, a fonte de alimentação, a largura de banda da rede e os recursos de API do HSM. Edição platinum: você pode usar exclusivamente o sub-rack do HSM, a fonte de alimentação, a largura de banda da rede e os recursos de API do HSM.
AZ	AZ de um dispositivo
Expiration Time	Tempo de expiração da instância de HSM comprada.

Passo 5 Você pode clicar no nome de uma instância para ver detalhes sobre ela, conforme mostrado em **Figura 4-8**.

Figura 4-8 Detalhes sobre instâncias do HSM dedicado



Para obter mais informações, consulte **Tabela 4-5**.

Tabela 4-5 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 sub-rack do HSM, a fonte de alimentação, a largura de banda da rede e os recursos de API do HSM.
HSM Type	Tipos do HSM de uma instância, incluindo **Finance**, **Server** e **Signature verification server**.

Parâmetro	Descrição
VPC	VPC à qual a instância pertence Para obter mais informações sobre a VPC, consulte *Guia de usuário da Virtual Private Cloud*.
Subnet	Sub-rede onde a instância está localizada. Para obter mais informações sobre sub-redes, consulte *Guia de usuário da 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 da 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

----Fim

4.4 Gerenciamento de tags

4.4.1 Adição de uma tag

Você pode usar tags para identificar instâncias de HSM dedicado. As tags podem ser adicionadas a instâncias de HSM dedicado para facilitar a classificação e a consulta de instâncias.

Procedimento

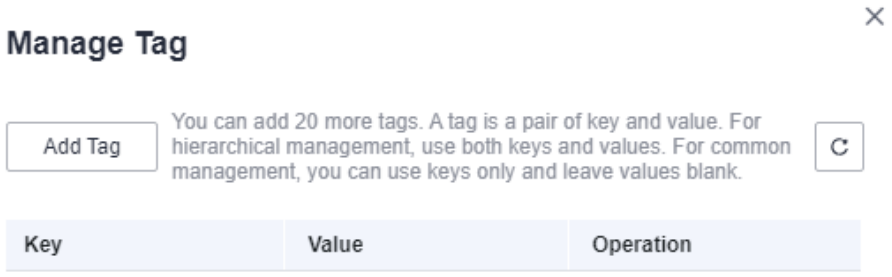
Passo 1 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou um projeto.

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

Passo 3 No painel de navegação, escolha **Dedicated HSM**.

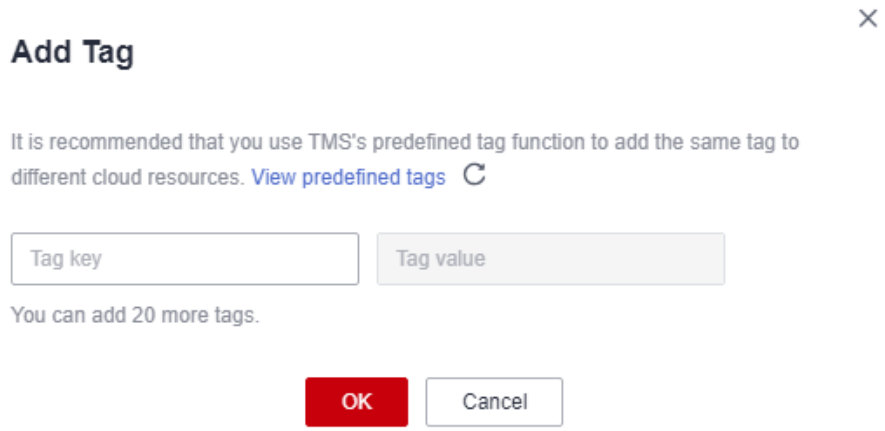
Passo 4 Na coluna **Operation** de uma instância, clique em **Manage Tag**. A página **Manage Tag** é exibida, conforme mostrado em **Figura 4-9**.

Figura 4-9 Gerenciar tag



Passo 5 Clique em **Add Tag**. Na caixa de diálogo que é exibida, insira a chave de tag e o valor da tag. Para obter detalhes sobre os parâmetros, consulte **Tabela 4-6**.

Figura 4-10 Adição de 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 4-6 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 20 tags.	● Obrigatório. ● A chave da tag deve ser exclusiva para a mesma chave personalizada. ● Limite de 128 caracteres. ● O valor não pode começar nem terminar com um espaço. ● Não é possível começar com **_sys_**. ● Os seguintes tipos de caracteres são permitidos: – Chinês – Inglês – Números – Espaço – Caracteres especiais: _.:/=+-@
Tag value	Valor da tag	● Opcional ● Limite de 255 caracteres. ● Os seguintes tipos de caracteres são permitidos: – Chinês – Inglês – Números – Espaço – Caracteres especiais: _.:/=+-@

Passo 6 Clique em **OK**.

----Fim

4.4.2 Pesquisa de uma instância do HSM dedicado por tag

Esta seção descreve como pesquisar instâncias do HSM por tag no projeto atual na página **Instances (New)**.

Pré-requisitos

As tags foram adicionadas.

Procedimento

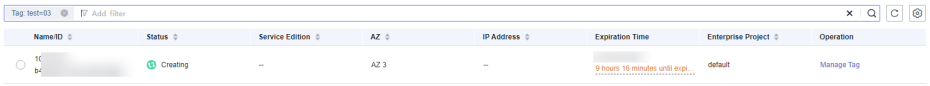
Passo 1 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou um projeto.

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

Passo 3 No painel de navegação, escolha **Dedicated HSM**.

Passo 4 Clique na caixa de pesquisa e selecione uma tag como atributo de filtro para pesquisar instâncias de HSM dedicado, conforme mostrado na **Figura 4-11**.

Figura 4-11 Pesquisa de uma instância do HSM dedicado



----Fim

4.4.3 Modificação de um valor de tag

Esta seção descreve como modificar valores de tag na página do HSM dedicado.

Procedimento

Passo 1 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou um projeto.

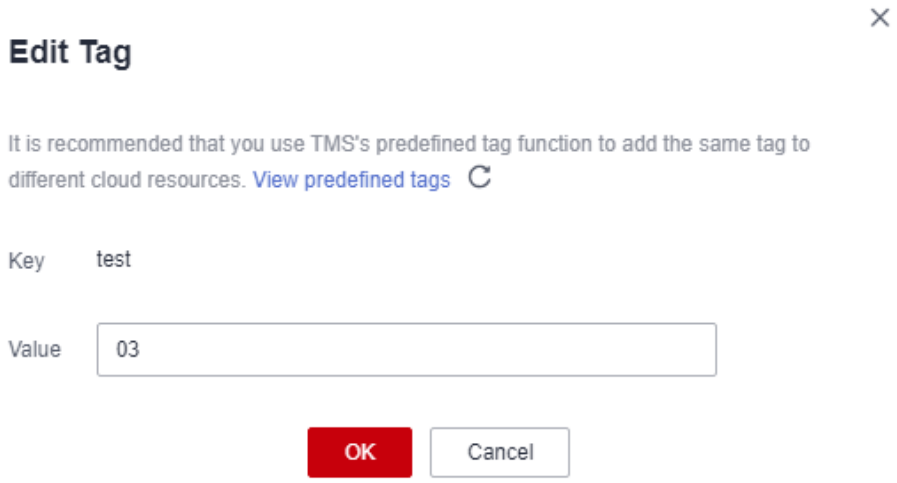
Passo 2 Clique em . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 3 No painel de navegação, escolha **Dedicated HSM**.

Passo 4 Clique em **Manage Tag** na linha em que a instância de destino está localizada. A caixa de diálogo **Manage Tag** é exibida.

Passo 5 Clique em **Edit**. A caixa de diálogo **Edit Tag** é exibida. Depois de alterar o valor da tag, clique em **OK**.

Figura 4-12 Edição de uma tag



----Fim

4.4.4 Exclusão de uma tag

Esta seção descreve como excluir tags na página do HSM dedicado.

Procedimento

Passo 1 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou um projeto.

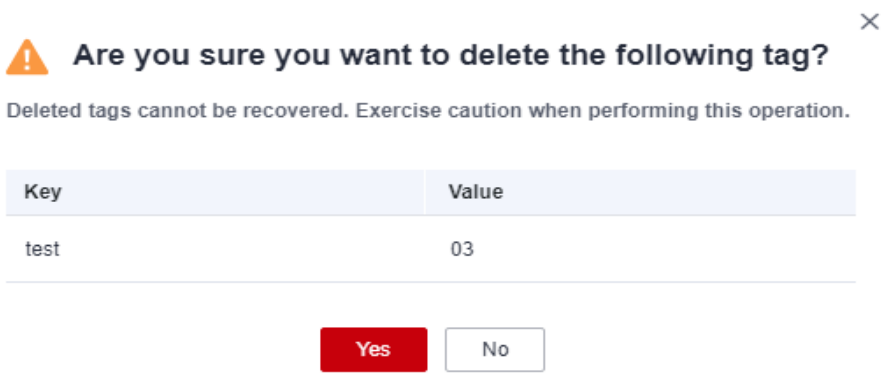
Passo 2 Clique em . Escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 3 No painel de navegação, escolha **Dedicated HSM**.

Passo 4 Clique em **Manage Tag** na linha em que a instância de destino está localizada. A caixa de diálogo **Manage Tag** é exibida.

Passo 5 Na coluna **Operation** de uma tag, clique em **Delete**.

Figura 4-13 Exclusão de uma tag



Passo 6 Na caixa de diálogo **Delete Tag**, clique em **Yes**.

----Fim

4.5 Uso de instâncias do HSM dedicado

Após a conclusão do pagamento, aguarde o envio do Ukey usado 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 softwares 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 permissões 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 instâncias 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**.

Item	Descrição	Como obter
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.	

Inicialização de uma instância de 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 vinculação 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

Instalação do agente de segurança e concessão de 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 balancear cargas.

----Fim

5 Registros de auditoria

5.1 Operações suportadas pelo CTS

As tabelas desta seção descrevem as operações do DEW suportadas pelo CTS.

Tabela 5-1 Operações do KMS registadas pelo CTS

Operação	Tipo de recurso	Nome do rastreamento
Criar uma chave	cmk	createKey
Criar uma DEK	cmk	createDataKey
Criar uma DEK sem texto não criptografado	cmk	createDataKeyWithoutPlain-text
Ativar uma chave	cmk	enableKey
Desativar uma chave	cmk	disableKey
Criptografar uma DEK	cmk	encryptDatakey
Descriptografar uma DEK	cmk	decryptDatakey
Programar a exclusão de chaves	cmk	scheduleKeyDeletion
Cancelar a exclusão da chave programada	cmk	cancelKeyDeletion
Gerar números aleatórios	rng	genRandom
Modificar um alias de chave	cmk	updateKeyAlias
Modificar descrição da chave	cmk	updateKeyDescription
Alertar riscos sobre a exclusão de CMK	cmk	deleteKeyRiskTips

Operação	Tipo de recurso	Nome do rastreamento
Importar materiais de chave	cmk	importKeyMaterial
Excluir materiais de chave	cmk	deleteImportedKeyMaterial
Criar uma concessão	cmk	createGrant
Retirar uma concessão	cmk	retireGrant
Revogar uma concessão	cmk	revokeGrant
Criptografar dados	cmk	encryptData
Descriptografar dados	cmk	decryptData
Adicionar uma tag	cmk	createKeyTag
Excluir uma tag	cmk	deleteKeyTag
Adicionar tags em lotes	cmk	batchCreateKeyTags
Excluir tags em lotes	cmk	batchDeleteKeyTags
Ativar rotação de chaves	cmk	enableKeyRotation
Modificar intervalo de rotação da chave	cmk	updateKeyRotationInterval

Tabela 5-2 Operações do KMS registadas pelo CSMS

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

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

Tabela 5-3 Operações do KMS registadas pelo KPS

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

Tabela 5-4 Operações do KMS registradas pelo HSM dedicado

Operação	Tipo de recurso	Nome do rastreamento
Comprar uma instância do HSM	hsm	purchaseHsm

Operação	Tipo de recurso	Nome do rastreamento
Configurar uma instância do HSM	hsm	createHsm
Excluir uma instância do HSM	hsm	deleteHsm

5.2 Uso do CTS para consultar rastreamentos da operação do DEW

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

Para obter detalhes sobre como exibir logs de auditoria, consulte **Consulta de rastreamentos em tempo real**.

6 Controle de permissão

6.1 Criação de um usuário e autorização ao usuário a permissão para acessar o DEW

Esta seção descreve como usar o **IAM** para implementar o controle de permissões refinadas para seus recursos do 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 da Huawei ou um serviço de nuvem confiáveis para realizar uma O&M profissional e eficiente em seus recursos do DEW.

Se sua conta da Huawei 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 conceder permissões a um grupo de usuários, você precisa entender as permissões do DEW disponíveis e conceder permissões com base no cenário da vida real. As tabelas a seguir descrevem as permissões suportadas no DEW.

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

Tabela 6-1 Políticas do sistema do KMS

Função/ política	Descrição	Tipo	Dependência
KMS Administrator	Todas as permissões do KMS	Função	Nenhuma

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

Tabela 6-2 Políticas do sistema do KPS

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

Tabela 6-3 Políticas do sistema do CSMS

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

Tabela 6-4 descreve as operações comuns suportadas por cada permissão definida pelo sistema de DEW. Selecione as permissões conforme necessário.

Tabela 6-4 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 chaves	√	√	x	x
Cancelar a exclusão da chave agendada	√	√	x	x
Modificar um alias de chave	√	√	x	x
Modificar descrição da chave	√	√	x	x
Gerar um número aleatório	√	√	x	x
Criar uma DEK	√	√	x	x
Criar uma DEK sem texto não criptografado	√	√	x	x
Criptografar uma DEK	√	√	x	x
Descriptografar uma DEK	√	√	x	x
Obter parâmetros para importar uma chave	√	√	x	x
Importar materiais de chave	√	√	x	x

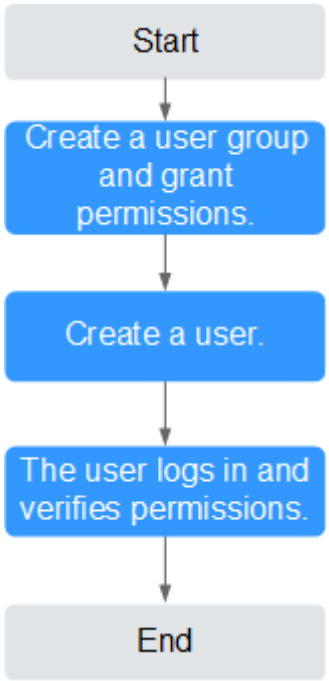
Operação	KMS Administrator	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
Excluir materiais de chave	√	√	x	x
Criar uma concessão	√	√	x	x
Revogar uma concessão	√	√	x	x
Retirar uma concessão	√	√	x	x
Consultar a lista de concessões	√	√	x	x
Consultar concessões recuperáveis	√	√	x	x
Criptografar dados	√	√	x	x
Descriptografar dados	√	√	x	x
Enviar mensagens de assinatura	√	√	x	x
Autenticar assinatura	√	√	x	x
Ativar rotação de chaves	√	√	x	x
Modificar 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

Operação	KMS Administrator	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
Consultar tags de chave	√	√	x	x
Consultar tags do 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
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

Operação	KMS Administrator	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
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 com falha	x	x	√	x
Excluir uma tarefa com falha	x	x	√	x
Consultar tarefas em execução	x	x	√	√

Processo de autorização

Figura 6-1 Autorização da permissão de acesso ao DEW para um usuário



1. **Criação de um grupo de usuários e atribuição de permissões**

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

2. **Criação de um usuário do IAM**

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

3. **Fazer logon** e verificar as permissões.

   Fazer logon no console como usuário recém-criado e verificar se o usuário só tem permissões de leitura para DEW.

   – Escolha **Service List** > **Data Encryption Workshop**. No painel de navegação, escolha **Key Pair Service**. Se aparecer uma mensagem indicando falta de permissões, a política **KMS CMKFullAccess** entrou em vigor.

   – Clique em **Service List** e selecione um serviço diferente do DEW. Se uma mensagem for exibida indicando que você não tem permissão para acessar o serviço, a política **KMS CMKFullAccess** entrou em vigor.

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 pelas 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**: defina-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 o ID, consulte "Visualização de uma CMK".

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

Exemplos 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 **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 a política **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 ações múltiplas

  Uma política personalizada pode conter as ações de vários serviços que todos são do tipo global ou de nível de projeto. A seguir está uma política com várias instruções:

  ```
  {
      "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"
              ]
          }
  ```



```
    ]
}
```

