Data Encryption Workshop

Perguntas frequentes

Edição	27
Data	26-08-2026

HUAWEI TECHNOLOGIES CO., LTD.

Marcas registadas e permissões


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

Aviso

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

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

Huawei Technologies Co., Ltd.

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

Site: https://www.huawei.com

Email: support@huawei.com

Índice

1 Relacionado ao KMS

1.1 O que é o serviço de gerenciamento de chaves?

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

Ele usa Módulos de Segurança de Hardware (HSMs) para proteger as chaves. Todas as chaves são protegidas por chaves raiz em HSMs para evitar vazamento de chaves. O módulo HSM atende aos requisitos de segurança FIPS 140-2 Nível 3.

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

1.2 O que é uma Chave principal do cliente?

Uma Chave principal do cliente (CMK) é uma Chave de criptografia de chave (KEK) criada por um usuário no KMS. Ela é usada para criptografar e proteger DEKs. Uma CMK pode ser usada para criptografar uma ou mais DEKs.

As CMKs são categorizadas em chaves personalizadas e chaves padrão.

- Chaves personalizadas

  Chaves criadas ou importadas por usuários no console do KMS.

- Chaves padrão

  Quando um usuário usa o KMS para criptografia em um serviço de nuvem pela primeira vez, o serviço de nuvem cria automaticamente uma chave com o sufixo de alias **/default**.

  Você pode usar o console de gerenciamento para consultar, mas não pode desativar ou agendar a exclusão de Chaves principais padrão.

Tabela 1-1 Chaves principais padrão

Alias	Serviço em nuvem
obs/default	Object Storage Service (OBS)

Alias	Serviço em nuvem
evs/default	Elastic Volume Service (EVS)
ims/default	Image Management Service (IMS)
kps/default	Key Pair Service (KPS)
csms/default	Cloud Secret Management Service (CSMS)

1.3 O que é uma chave padrão?

Uma chave padrão é criada automaticamente por outro serviço de nuvem usando o KMS, como o Object Storage Service (OBS). O alias de uma chave padrão termina com **/default**.

Você pode usar o console de gerenciamento para consultar, mas não pode desativar ou agendar a exclusão de chaves padrão.

As chaves padrão são hospedadas gratuitamente e são cobradas com base no número de solicitações de API para elas. Se as solicitações da API excederem o limite gratuito, a parte em excesso será cobrada.

Tabela 1-2 Chaves principais padrão

Alias	Serviço de nuvem
obs/default	Object Storage Service (OBS)
evs/default	Elastic Volume Service (EVS)
ims/default	Image Management Service (IMS)
vbs/default	Volume Backup Service (VBS)
sfs/default	Scalable File Service (SFS)
kps/default	Key Pair Service (KPS)
csms/default	Cloud Secret Management Service (CSMS)

NOTA

Uma chave padrão é criada automaticamente quando um usuário emprega a função de criptografia do KMS pela primeira vez em outro serviço de nuvem.

1.4 Quais são as diferenças entre uma chave personalizada e uma chave padrão?

A tabela a seguir descreve as diferenças entre uma chave personalizada e uma chave padrão.

Tabela 1-3 Diferenças entre uma chave personalizada e uma chave padrão

Item	Definição	Diferença
Chave personalizada	Uma Chave de criptografia de chave (KEK) criada usando o KMS. A chave é usada para criptografar e proteger DEKs. Uma chave personalizada pode ser usada para criptografar várias DEKs.	● Ela pode ser desativada e agendada para exclusão. ● É cobrada por uso após ser criada ou importada.
Chave padrão	Gerada automaticamente pelo sistema quando você usa o KMS para criptografar dados em outro serviço de nuvem pela primeira vez. O sufixo da chave é **/default**. Exemplo: **evs/default**	● Ela não pode ser desativada ou agendada para exclusão. ● Você não é cobrado quando usa o serviço de nuvem gerado automaticamente pelo sistema. Se o número de solicitações de API for superior a 20.000, você será cobrado.

1.5 O que é uma chave de criptografia de dados?

Uma chave de criptografia de dados (DEK) é usada para criptografar dados.

1.6 Por que não consigo excluir uma CMK imediatamente?

A decisão de excluir uma CMK deve ser considerada com muita cautela. Antes da exclusão, confirme se todos os dados criptografados da CMK foram migrados. Assim que a CMK for excluída, você não poderá descriptografar dados com ela. Portanto, o KMS oferece um período especificado pelo usuário de 7 a 1096 dias para que a exclusão finalmente entre em vigor. No dia programado da exclusão, a CMK será excluída permanentemente. No entanto, antes do dia programado, você ainda pode cancelar a exclusão pendente. Este é um meio de precaução dentro do KMS.

1.7 Quais serviços de nuvem podem usar o KMS para criptografia?

Object Storage Service (OBS), Elastic Volume Service (EVS), Image Management Service (IMS) e Relational Database Service (RDS) podem usar o KMS para criptografia.

Tabela 1-4 Lista de serviços de nuvem que usam criptografia do KMS

Nome do serviço	Descrição
Object Storage Service (OBS)	Você pode fazer upload e download de objetos do Object Storage Service (OBS) no modo comum ou no modo de criptografia no lado do servidor. Quando você faz upload de objetos no modo de criptografia, os dados são criptografados no lado do servidor e, em seguida, armazenados com segurança no OBS em texto cifrado. Quando você baixa objetos criptografados, os dados em texto cifrado são descriptografados no lado do servidor e, em seguida, fornecidos a você em texto não criptografado. O OBS suporta a criptografia no lado do servidor com o modo de chaves gerenciadas por KMS (SSE-KMS). No modo SSE-KMS, o OBS usa as chaves fornecidas pelo KMS para criptografia do lado do servidor. Para obter detalhes sobre como carregar objetos para o OBS no modo SSE-KMS, consulte o **Guia de operação do console do Object Storage Service**.
Elastic Volume Service (EVS)	Se você ativar a função de criptografia ao criar um disco EVS, o disco será criptografado com a DEK gerada usando sua CMK. Os dados armazenados no disco EVS serão automaticamente criptografados. Para obter detalhes sobre como usar a função de criptografia do EVS, consulte **Guia de usuário do Elastic Volume Service**.
Image Management Service (IMS)	Ao criar uma imagem privada usando um arquivo de imagem externo, você pode ativar a função de criptografia de imagem privada e selecionar uma CMK fornecida pelo KMS para criptografar a imagem. Para obter detalhes sobre como usar a função de criptografia de imagem privada do Image Management Service (IMS), consulte **Guia de usuário do Image Management Service**.
Scalable File Service (SFS)	Ao criar um sistema de arquivos no SFS, a CMK fornecida pelo KMS pode ser selecionada para criptografar o sistema de arquivos, de modo que os arquivos armazenados no sistema de arquivos sejam criptografados automaticamente. Para obter detalhes sobre como usar a função de criptografia do sistema de arquivos do SFS, consulte **Guia de usuário do Scalable File Service**.
Relational Database Service (RDS)	Ao comprar uma instância de banco de dados, você pode ativar a função de criptografia de disco da instância de banco de dados e selecionar uma CMK criada no KMS para criptografar o disco da instância de banco de dados. Ativar a função de criptografia de disco aumentará a segurança dos dados. Para obter detalhes sobre como usar a função de criptografia de disco do RDS, consulte *Relational Database Service User Guide*.
Document Database Service (DDS)	Ao comprar uma instância do DDS, você pode ativar a função de criptografia de disco da instância e selecionar uma CMK criada no KMS para criptografar o disco da instância. Ativar a função de criptografia de disco aumentará a segurança dos dados. Para obter detalhes sobre como usar a função de criptografia de disco do DDS, consulte **Primeiros passos do Document Database Service**.

1.8 Como os serviços da Huawei Cloud usam o KMS para criptografar dados?

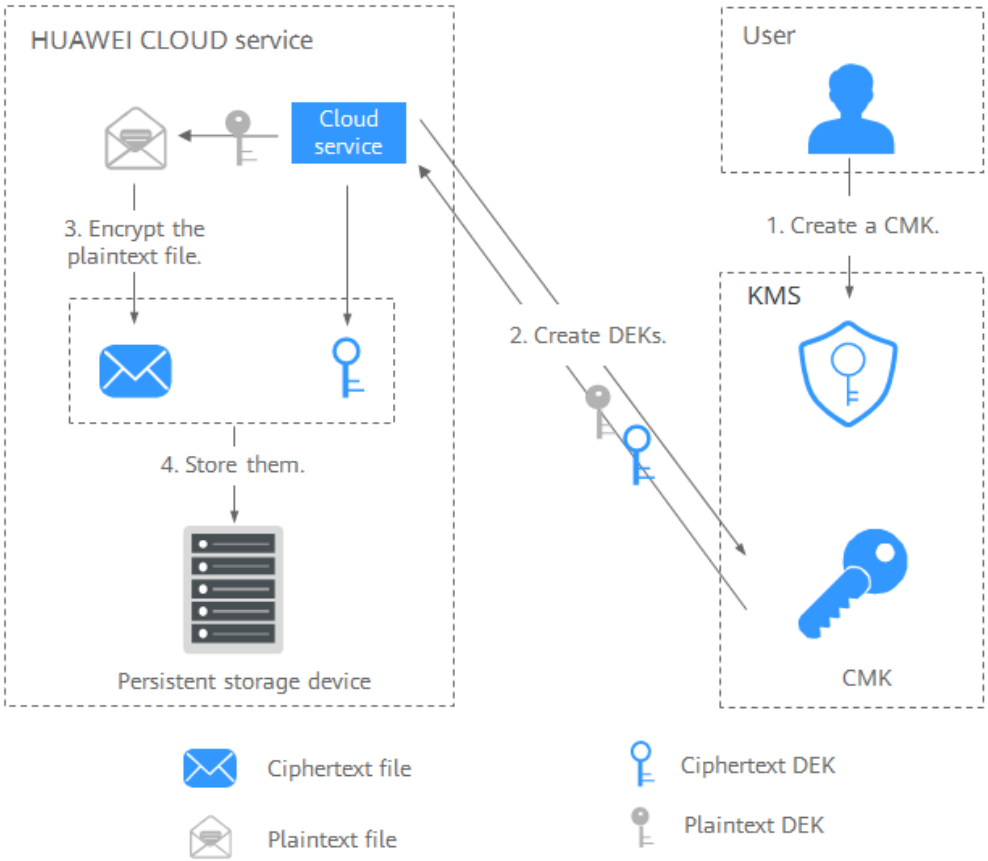
Os serviços da Huawei Cloud (incluindo OBS, IMS, EVS e RDS) usam a criptografia de envelope fornecida pelo **KMS** para proteger os dados.

NOTA

A criptografia de envelope é um método de criptografia que permite que as DEKs sejam armazenadas, transmitidas e usadas em "envelopes" de CMKs. Como resultado, as CMKs não criptografam e descriptografam dados diretamente.

- Quando você usa um serviço da Huawei Cloud para criptografar dados, precisa especificar uma CMK no KMS. O serviço da Huawei Cloud gera uma DEK de texto não criptografado e uma DEK de texto cifrado. A DEK de texto cifrado é gerada criptografando a DEK de texto não criptografado usando a CMK especificada. O serviço da Huawei Cloud usa a DEK de texto não criptografado para criptografar dados e armazena os dados de texto cifrado e a DEK de texto cifrado no serviço da Huawei Cloud. Veja a figura a seguir.

Figura 1-1 Como a Huawei Cloud usa o KMS para criptografia



- Quando os usuários baixam os dados da Huawei Cloud, o serviço usa a CMK especificada pelo KMS para descriptografar a DEK de texto cifrado, usa a DEK descriptografada para descriptografar os dados e, em seguida, fornece os dados descriptografados para os usuários baixarem.

1.9 Quais são os benefícios da criptografia de envelope?

A criptografia de envelope é a prática de criptografar dados com uma DEK e, em seguida, criptografar a DEK com uma chave raiz que você pode gerenciar totalmente. Nesse caso, as CMKs não são necessárias para criptografia ou descriptografia.

Benefícios:

- Vantagens em relação à criptografia de CMK no KMS

  Os usuários podem usar CMKs para criptografar e descriptografar dados no console do KMS ou chamando APIs do KMS.

  Uma CMK não pode criptografar e descriptografar dados com mais de 4 KB. Um envelope pode criptografar e descriptografar volumes maiores de dados.

  Os dados criptografados usando envelopes não precisam ser transferidos. Somente as DEKs precisam ser transferidas para o servidor do KMS.

- Vantagens em relação à criptografia usando serviços em nuvem
  - Segurança

    Os dados transferidos para a nuvem para criptografia estão expostos a riscos como interceptação e phishing.

    Durante a criptografia do envelope, o KMS usa Módulos de segurança de hardware (HSMs) para proteger as chaves. Todas as CMKs são protegidas por chaves raiz nos HSMs para evitar vazamento de chaves.
  - Confiabilidade

    Você vai se preocupar com a segurança dos dados na nuvem. Também é difícil para os serviços em nuvem provar que nunca fazem uso indevido ou divulgam esses dados.

    Se você escolher a criptografia de envelope, o KMS controlará o acesso a chaves e registrará todos os usos e operações de chaves com logs rastreáveis, atendendo aos requisitos de conformidade normativa e de auditoria.
  - Desempenho e custo

    Para criptografar ou descriptografar dados usando um serviço de nuvem, você precisa enviar os dados para o servidor de criptografia e receber os dados processados. Esse processo afeta seriamente o desempenho do seu serviço e incorre em altos custos.

    A criptografia de envelope permite gerar DEKs on-line chamando APIs de algoritmo criptográfico do KMS e criptografar uma grande quantidade de dados locais com as DEKs.

1.10 Existe um limite para o número de chaves personalizadas que posso criar no KMS?

Sim.

Você pode criar um máximo de 20 chaves personalizadas, incluindo as que estão nos estados ativado, desativado e pendente de exclusão. As chaves padrão não estão incluídas.

1.11 Posso exportar uma CMK do KMS?

Não.

Para garantir a segurança da CMK, os usuários só podem criar e usar CMKs no KMS.

1.12 Posso descriptografar meus dados se eu excluir permanentemente minha chave personalizada?

Não.

Se você tiver excluído permanentemente sua chave personalizada, os dados criptografados usando-a não poderão ser descriptografados. Antes da data de exclusão programada da chave personalizada, você pode cancelar a exclusão programada.

1.13 Como usar a ferramenta on-line para criptografar ou descriptografar pequenos volumes de dados?

Você pode usar a ferramenta on-line para criptografar ou descriptografar dados nos seguintes procedimentos:

Criptografia de dados

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

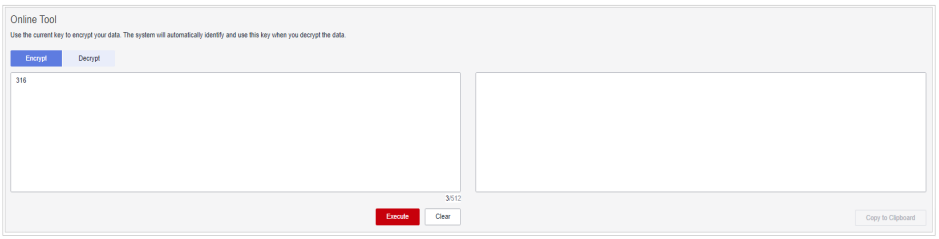
Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou projeto.

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 1-2**.

Figura 1-2 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

NOTA

Digite o texto não criptografado no console, o texto será codificado no formato Base64 antes da criptografia.

O resultado da descriptografia retornado via API estará no formato Base64. Execute a decodificação Base64 para obter o texto não criptografado inserido no console.

Descriptografia de dados

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

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

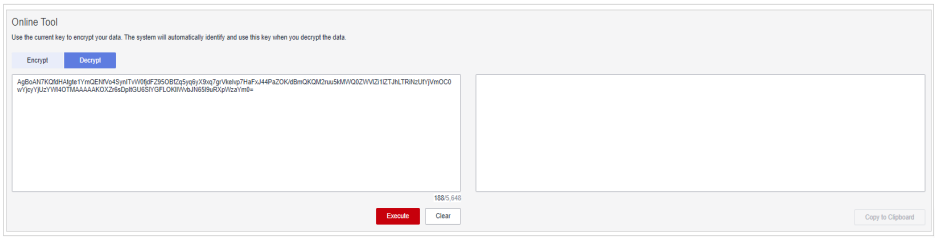
Passo 3 Você pode clicar em qualquer chave não padrão no status **Enabled** para acessar a página de criptografia e descriptografia da ferramenta on-line.

Passo 4 Clique em **Decrypt**. Na caixa de texto à esquerda, insira os dados a serem descriptografados. Para obter detalhes, consulte **Figura 1-3**.

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 1-3 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

1.14 Posso atualizar CMKs criadas por materiais de chave gerados por KMS?

Não.

As chaves criadas usando materiais gerados pelo KMS não podem ser atualizadas. Você só pode usar o KMS para criar novas CMKs para criptografar e descriptografar dados.

1.15 Quando devo usar uma CMK criada com materiais de chaves importados?

- Se você não quiser usar materiais de chave gerados pelo KMS, poderá importar seus próprios materiais de chave para criar uma CMK. Tal CMK permite a exclusão de apenas os materiais de chaves quando você não precisa deles. Além disso, quando você descobrir que os materiais de chaves foram excluídos incorretamente, poderá importar os mesmos materiais para a CMK.
- Você também pode importar materiais de chave fora da nuvem para o KMS quando quiser usar as mesmas chaves dentro e fora da nuvem. Essa prática tem se mostrado útil quando os usuários migram dados criptografados locais para a nuvem.

1.16 O que devo fazer quando excluir acidentalmente materiais de chaves?

Você pode importar os materiais de chaves de backup do seu dispositivo local novamente.

AVISO

Antes de importar materiais de chaves, é aconselhável fazer backup dos materiais. Os materiais a serem reimportados devem ser consistentes com os materiais excluídos por engano.

1.17 Como as chaves padrão são geradas?

As chaves padrão são geradas automaticamente.

Quando um usuário usa o KMS para criptografia em um serviço de nuvem pela primeira vez, o serviço de nuvem cria automaticamente uma chave com o sufixo de alias **/default**.

Você pode usar o console de gerenciamento para consultar, mas não pode desativar ou agendar a exclusão de Chaves principais padrão.

As chaves padrão são hospedadas gratuitamente e são cobradas com base no número de solicitações de API para elas. Se as solicitações da API excederem o limite gratuito, a parte em excesso será cobrada.

Tabela 1-5 Chaves principais padrão

Alias	Serviço em nuvem
obs/default	Object Storage Service (OBS)
evs/default	Elastic Volume Service (EVS)

Alias	Serviço em nuvem
ims/default	Image Management Service (IMS)
kps/default	Key Pair Service (KPS)
csms/default	Cloud Secret Management Service (CSMS)

1.18 O que devo fazer se não tiver as permissões para realizar operações no KMS?

Sintoma

Uma mensagem indicando a falta de permissões é exibida quando você tenta executar operações em chaves, como exibir, criar ou importar chaves.

Possíveis causas

Sua conta não está vinculada às políticas do sistema do KMS necessárias.

Solução

Passo 1 Verifique se sua conta foi vinculada às políticas **KMS Administrator** e **KMS CMKFullAccess**.

Para obter detalhes sobre como verificar seus grupos de usuários e permissões, consulte **Grupos de usuários e autorização**.

Se sua conta tiver sido vinculada às políticas do sistema do KMS necessárias, acesse **Passo 2**.

Passo 2 Vincule sua conta às políticas do sistema necessárias.

- Para obter detalhes sobre como adicionar permissões de administrador, consulte **Grupos de usuários e autorização**.
- Para obter detalhes sobre como adicionar uma política personalizada, consulte **Criação de uma política personalizada do DEW**.

----Fim

1.19 Por que não posso encapsular chaves assimétricas usando -id-aes256-wrap-pad no OpenSSL?

Sintoma

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 aplique o patch primeiro.

Solução

Use os comandos bash para criar uma cópia local do OpenSSL existente. Não é necessário excluir ou modificar as configurações de instalação do cliente do OpenSSL padrão.

Passo 1 Alterne para o usuário **root**.

sudo su -

Passo 2 Execute o seguinte comando e registre a versão do OpenSSL:

openssl version

Passo 3 Execute os seguintes comandos para criar o diretório **/root/build**. Este diretório será usado para armazenar o arquivo binário do OpenSSL mais recente.

mkdir $HOME/build

mkdir -p $HOME/local/ssl

cd $HOME/build

Passo 4 Baixe a versão mais recente do OpenSSL em https://www.openssl.org/source/.

Passo 5 Baixe e descompacte o arquivo binário.

Passo 6 Substitua **openssl-1.1.1d.tar.gz** pela versão mais recente do OpenSSL baixada na **etapa 4**.

curl -O https://www.openssl.org/source/openssl-1.1.1d.tar.gz

tar -zxf openssl-1.1.1d.tar.gz

Passo 7 Use a ferramenta **gcc** para corrigir a versão e compilar o arquivo binário baixado.

yum install patch make gcc -y

NOTA

Se você estiver usando uma versão diferente do OpenSSL-1.1.1d, talvez seja necessário alterar o diretório e os comandos usados, ou esse patch pode não funcionar corretamente.

Passo 8 Execute os seguintes comandos:

```
sed -i "/BIO_get_cipher_ctx(benc, &ctx);/a\ EVP_CIPHER_CTX_set_flags(ctx,
EVP_CIPHER_CTX_FLAG_WRAP_ALLOW);" $HOME/build/openssl-1.1.1d/apps/enc.c
```

Passo 9 Execute os seguintes comandos para compilar o arquivo **enc.c** do OpenSSL:

cd $HOME/build/openssl-1.1.1d/

./config --prefix=$HOME/local --openssldir=$HOME/local/ssl

make -j$(grep -c ^processor /proc/cpuinfo)

make install

Passo 10 Configure a variável de ambiente **LD_LIBRARY_PATH** para garantir que as bibliotecas necessárias estejam disponíveis para OpenSSL. A versão mais recente do OpenSSL foi vinculada dinamicamente ao arquivo binário no diretório **$HOME/local/ssl/lib/** e não pode ser executada diretamente no shell.

Passo 11 Crie um script chamado **openssl.sh** para carregar o caminho **$HOME/local/ssl/lib/** antes de executar o arquivo binário.

cd $HOME/local/bin/

echo -e '#!/bin/bash \nenv LD_LIBRARY_PATH=$HOME/local/lib/ $HOME/local/bin/openssl "$@"' > ./openssl.sh

Passo 12 Execute o seguinte comando para configurar um bit de execução no script:

chmod 755 ./openssl.sh

Passo 13 Execute o seguinte comando para iniciar a versão do OpenSSL corrigida:

$HOME/local/bin/openssl.sh

----Fim

1.20 Algoritmos de chave suportados pelo KMS

Tabela 1-6 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

1.21 O que devo fazer se o KMS não for solicitado e o código de erro 401 for exibido?

Sintoma

Um erro é relatado quando o KMS é solicitado ou a função de criptografia do serviço de nuvem é ativada.

Informações de erro: **httpcode=401,code=APIGW.0301,Msg=Incorrect IAM authentication information: current ip:xx.xx.xx.xx refused**

Possíveis causas

O controle de acesso é configurado no IAM.

Por padrão, o IAM permite o acesso de qualquer endereço IP. Se você configurar a ACL, os endereços IP e os segmentos de rede fora do intervalo especificado não poderão acessar o KMS ou usar o recurso de criptografia na nuvem.

Solução

- Para acessar o KMS por meio do console do serviço de nuvem (por exemplo, para fins de criptografia do OBS), permita o acesso dos segmentos de rede 10.0.0.0/8, 11.0.0.0/8 e 26.0.0.0/8.
- Para chamar o KMS via API, permita o acesso dos endereços IP de origem.

Permissão de acesso a partir de endereços IP específicos

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

Passo 2 Clique em ☰ à esquerda da página e escolha **Management & Governance** > **Identity and Access Management**. A página **Users** é exibida.

Passo 3 Selecione **Security Settings** e clique na guia **ACL**. Verifique se **IP Address Ranges** e **IPv4 CIDR Blocks** estão configurados corretamente.

NOTA

O endereço IP de origem que você usa deve ser especificado nas guias **Console Access** e **API Access**.

----Fim

1.22 Qual é a relação entre o texto cifrado e o texto não criptografado retornado pela API de dados de criptografia?

O comprimento básico do texto cifrado retornado pela API de dados criptografados é de 124 bytes. O texto cifrado consiste em vários campos, incluindo o ID da chave, o algoritmo de criptografia, a versão da chave e o resumo do texto cifrado.

O texto não criptografado tem 16 bytes em cada bloco. Um bloco com menos de 16 bytes será preenchido. Comprimento do texto cifrado = 124 + Ceil(comprimento do texto não criptografado/16) x 16. O resultado da conversão é codificado usando Base64.

Tome entrada de texto não criptografado de 4 bytes como um exemplo. O resultado do cálculo é 124 + Ceil(4/16) x 16 = 140. Os 140 bytes são convertidos em 188 bytes após a codificação Base64.

NOTA

Ceil é uma função de arredondamento. Ceil(a) = 1. O intervalo de valores de **a** é (0,1].

1.23 Como o KMS protege minhas chaves?

O mecanismo do KMS impede que qualquer pessoa acesse suas chaves em texto não criptografado. O KMS depende de módulos de segurança de hardware (HSMs) que protegem a confidencialidade e a integridade de suas chaves. As chaves do KMS de texto não criptografado são sempre criptografadas por HSMs e nunca são armazenadas em nenhum disco. Essas chaves são utilizadas apenas na memória volátil dos HSMs pelo tempo necessário para executar a operação criptográfica que você solicitou.

1.24 Como usar uma chave assimétrica para verificar o resultado da assinatura de um par de chaves públicas?

Em cenários em que os pares de chaves públicas e privadas são usados, a chave privada é usada para assinatura e a chave pública é usada para verificação de assinatura. A chave pública pode ser distribuída para o sujeito do serviço que precisa usar a chave pública. O sujeito do serviço verifica a assinatura dos dados de chave. O KMS fornece a API **get-publickey** para obter chaves públicas.

A CMK **RSA_3072** neste caso é usada para verificar assinaturas. Você pode usar o KMS para assinar APIs. O corpo da solicitação é o seguinte:

```
{
 "key_id": "key_id_value",
 "message": "MTIzNA==",
 "signing_algorithm": "RSASSA_PSS_SHA_256",
 "message_type": "RAW"
}
```

O resultado é o seguinte:

```
{
 "key_id": "key_id_value",
 "signature": "xxx"
}
```

Depois que a chave pública for obtida, certifique-se de que a assinatura seja verificada.

```
public class RawDataVerifyExample {

    /**
     * Basic authentication information:
     * - ACCESS_KEY: access key of the Huawei Cloud account
     * - SECRET_ACCESS_KEY: Huawei Cloud account secret access key, which is
sensitive information. Store this in ciphertext.
     * - IAM_ENDPOINT: endpoint for accessing IAM. For details, see https://
developer.huaweicloud.com/intl/en-us/endpoint?IAM.
```



```
     * - KMS_REGION_ID: regions supported by KMS. For details, see https://
developer.huaweicloud.com/intl/en-us/endpoint?DEW.
     * - KMS_ENDPOINT: endpoint for accessing KMS. For details, see https://
developer.huaweicloud.com/intl/en-us/endpoint?DEW.
     */
    private static final String ACCESS_KEY = System.getenv("HUAWEICLOUD_SDK_AK");
    private static final String SECRET_ACCESS_KEY =
System.getenv("HUAWEICLOUD_SDK_SK");
    private static final String IAM_ENDPOINT = "https://<IamEndpoint>";
    private static final String KMS_REGION_ID = "<RegionId>";
    private static final String KMS_ENDPOINT = "https://<KmsEndpoint>";

    private static final int SALT_LENGTH = 32;
    private static final int TRAILER_FIELD = 1;
    public static final String RSA_PUBLIC_KEY_BEGIN = "-----BEGIN PUBLIC KEY-----
\n";
    public static final String RSA_PUBLIC_KEY_END = "-----END PUBLIC KEY-----";

    // Sample signature data in Base64 encoding format. The original text is 1234.
    private static final String RWA_DATA = "MTIzNA==";

    // Signature value obtained through the sign API of KMS
    private static final String SIGN = "xxx";
    public static void main(String[] args) throws Exception {

        final String keyId = args[0];

        publicKeyVerify(keyId);
    }
   public static void publicKeyVerify(String keyId) throws Exception {

        // 1. Prepare the authentication information for accessing HUAWEI CLOUD.
        final BasicCredentials auth = new BasicCredentials()
                .withIamEndpoint(IAM_ENDPOINT).withAk(ACCESS_KEY).withSk(SECRET_AC
CESS_KEY);

        // 2. Initialize the SDK and transfer the authentication information and
the address for the KMS to access the client.
        final KmsClient kmsClient = KmsClient.newBuilder()
                .withRegion(new Region(KMS_REGION_ID,
KMS_ENDPOINT)).withCredential(auth).build();

        // 3. Obtain the public key information. The returned information is in
PKCS8 format.
        final ShowPublicKeyRequest showPublicKeyRequest = new
ShowPublicKeyRequest()
                .withBody(new OperateKeyRequestBody().withKeyId(keyId));
        final ShowPublicKeyResponse showPublicKeyResponse =
kmsClient.showPublicKey(showPublicKeyRequest);

        // 4. Obtain the public key string.
        final String publicKeyStr =
showPublicKeyResponse.getPublicKey().replace(RSA_PUBLIC_KEY_BEGIN, "")
                .replaceAll("\n", "").replace(RSA_PUBLIC_KEY_END, "");

        // 5. Parse the public key.
        final X509EncodedKeySpec keySpec = new
X509EncodedKeySpec(Base64.getDecoder().decode(publicKeyStr));
        final KeyFactory keyFactory = KeyFactory.getInstance("RSA", new
BouncyCastleProvider());
        final PublicKey publicKey = keyFactory.generatePublic(keySpec);

        // 6. Verify the signature.
        final Signature signature = getSignature();
        signature.initVerify(publicKey);
        signature.update(commonHash(Base64.getDecoder().decode(RWA_DATA)));

        // 7. Obtain the verification result.
        assert signature.verify(Base64.getDecoder().decode(SIGN));
```



```
    }
    private static Signature getSignature() throws Exception {
        Signature signature= Signature.getInstance("NONEwithRSASSA-PSS", new
BouncyCastleProvider());
        MGF1ParameterSpec mgfParam = new MGF1ParameterSpec("SHA256");
        PSSParameterSpec pssParam = new PSSParameterSpec("SHA256", "MGF1",
mgfParam, SALT_LENGTH, TRAILER_FIELD);
        signature.setParameter(pssParam);
        return signature;
    }
    private static byte[] commonHash(byte[] data) {
        byte[] digest;
        try {
            MessageDigest md = MessageDigest.getInstance("SHA256",
BouncyCastleProvider.PROVIDER_NAME);
            md.update(data);
            digest = md.digest();
        } catch (Exception e) {
            throw new RuntimeException("Digest failed.");
        }
        return digest;
    }
}
```

1.25 Uma chave importada suporta rotação?

As chaves importadas não suportam rotação. Depois que os materiais de chaves importados forem excluídos, certifique-se de que os mesmos materiais de chaves sejam importados.

2 Relacionado a credenciais

2.1 Por que não consigo excluir o status da versão de um segredo?

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

3 Relacionado ao KPS

3.1 Como criar um par de chaves?

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.

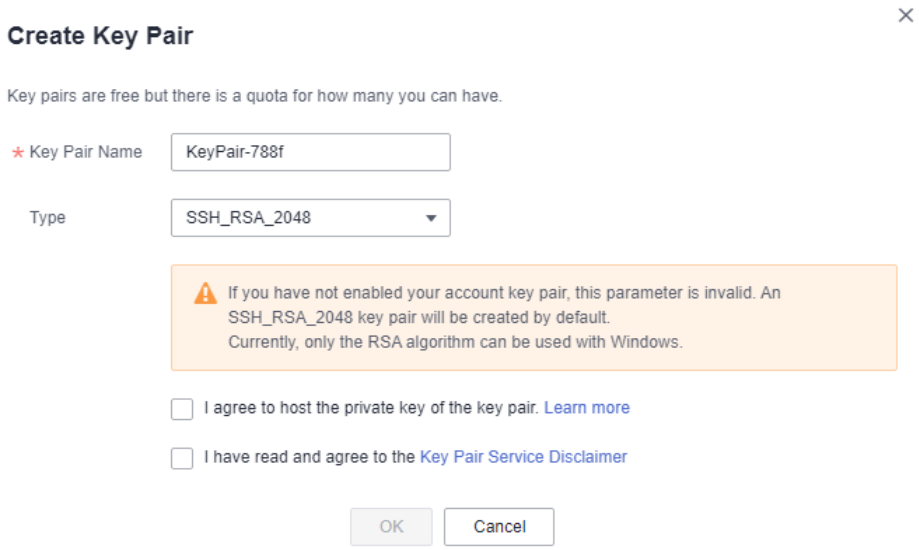
Passo 3 Clique em  à esquerda, escolha **Security & Compliance** > **Data Encryption Workshop**, a página de gerenciamento de chaves é exibida.

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

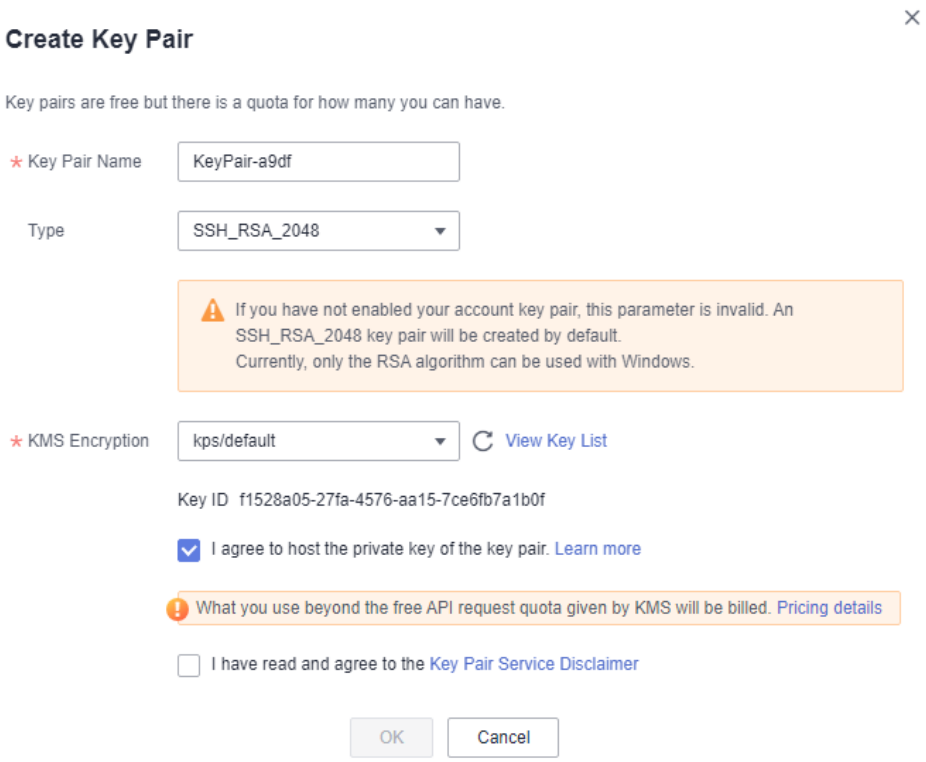
Atualmente, apenas o algoritmo RSA pode ser usado com o Windows.

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.

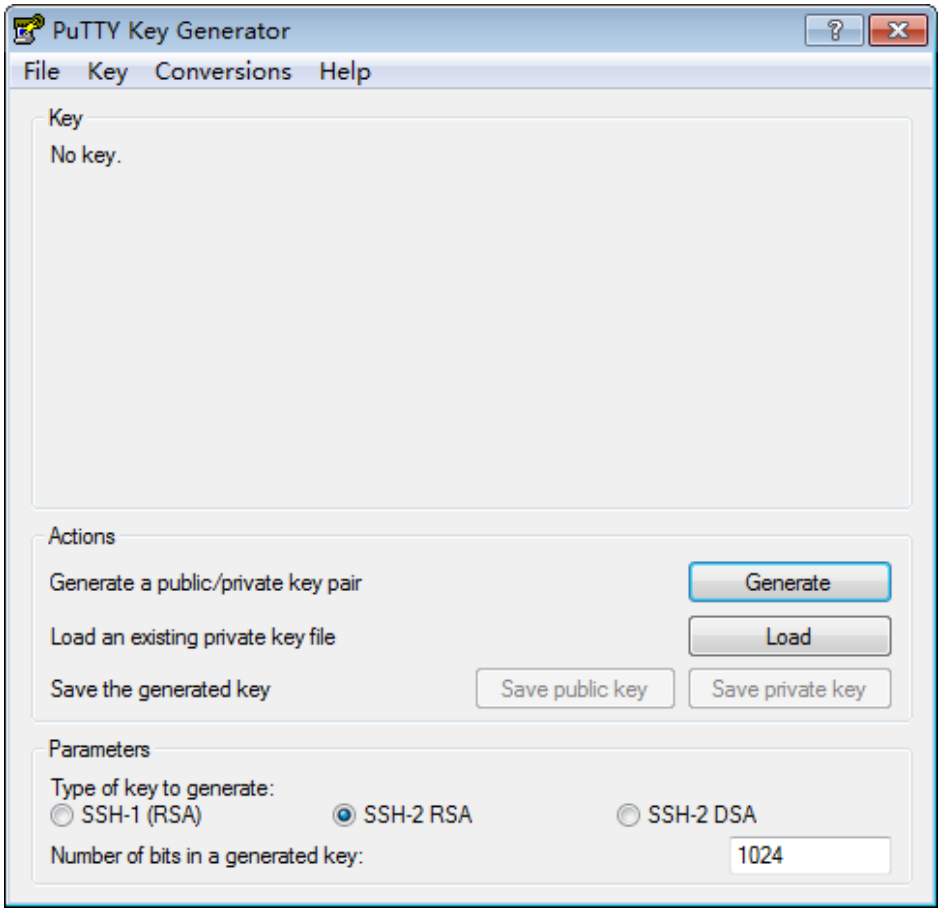
Depois que o par de chaves for criado, você poderá visualizá-lo na lista de pares de chaves. A lista exibe informações como nome do par de chaves, impressão digital, chave privada e quantidade.

----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**.

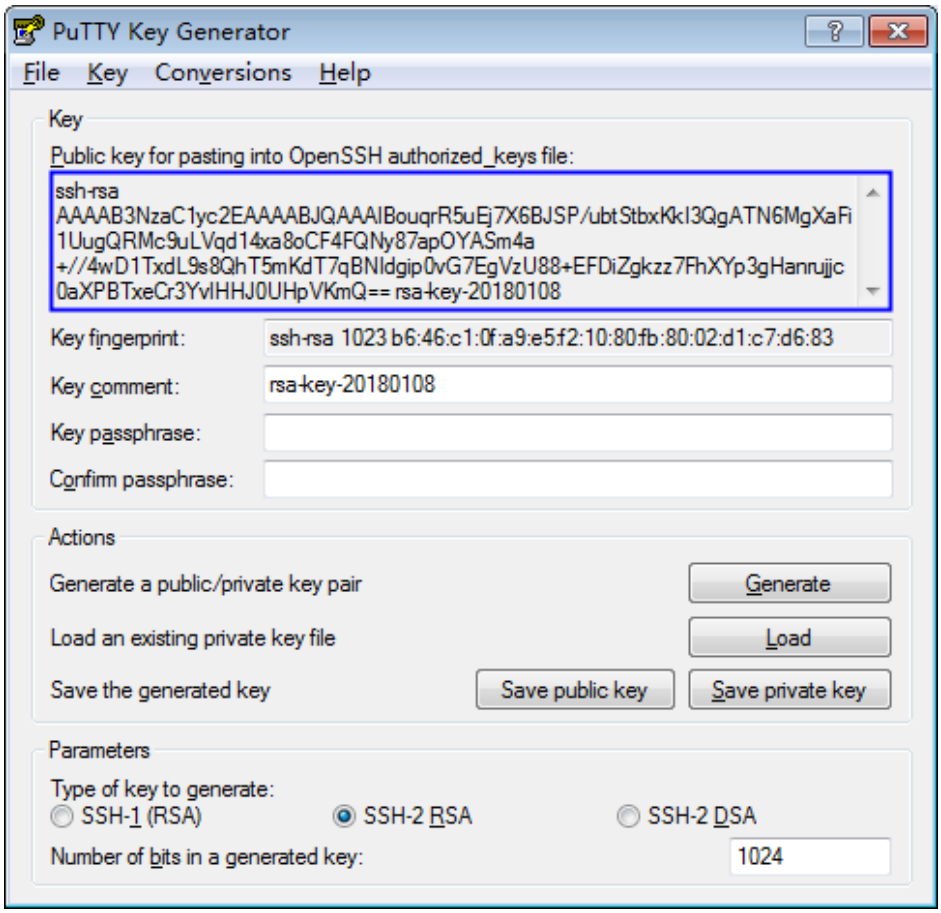
Tabela 3-1 Descrição do parâmetro

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.
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 O que são um par de chaves privadas e um par de chaves de contas?

Um par de chaves privadas pode ser visto ou usado apenas pela conta atual.

Um par de chaves de conta pode ser visto ou usado por todos os usuários sob a conta.

Um par de chaves privadas pode ser atualizado para um par de chaves de conta. Para obter detalhes, consulte **Atualização de um par de chaves**.

3.3 Como lidar com uma falha de importação de um par de chaves criado usando o PuTTYgen?

Sintoma

Quando um par de chaves criado usando o PuTTYgen era importado para o console de gerenciamento, o sistema exibia uma mensagem indicando que a importação da chave pública falhou.

Possíveis causas

O formato do conteúdo da chave pública não atende aos requisitos do sistema.

Armazenar uma chave pública clicando em **Save public key** alterará o formato do conteúdo da chave pública. A importação de tal chave pública falhará porque a chave não passa na verificação de formato pelo sistema.

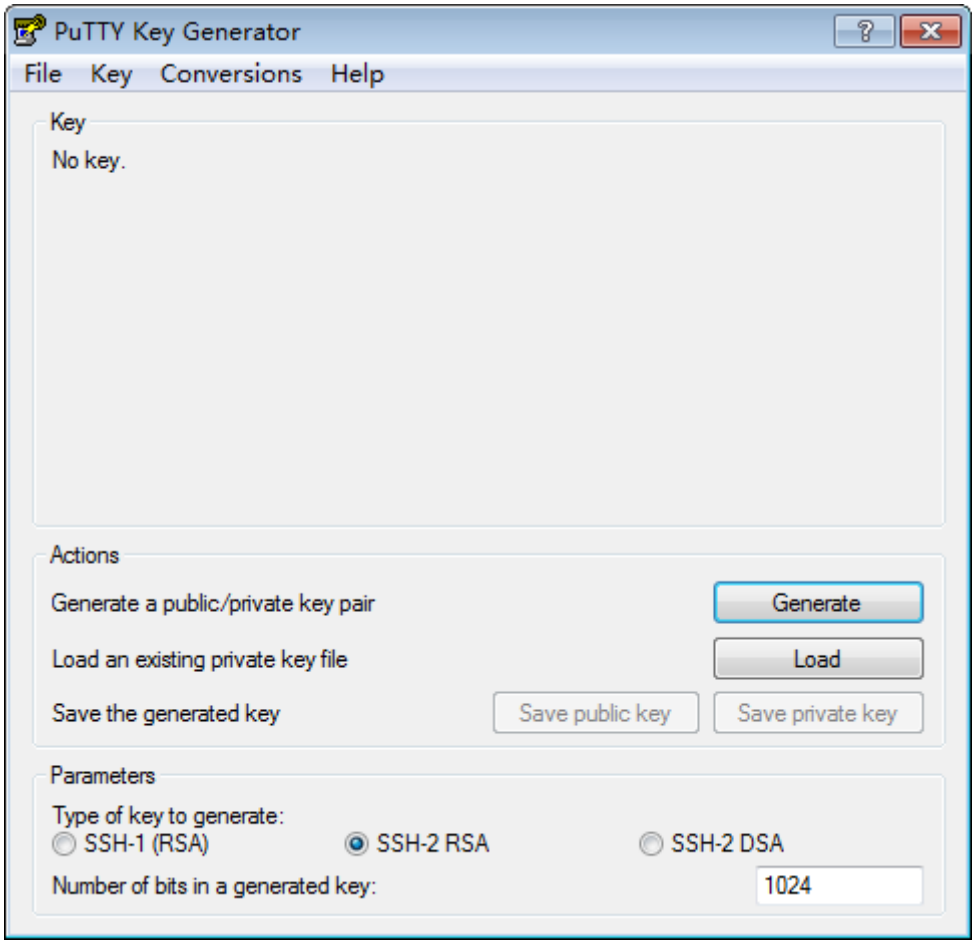
Procedimento

Use a chave privada armazenada localmente e **PuTTY Key Generator** para restaurar o formato do conteúdo da chave pública. Em seguida, importe a chave pública para o console de gerenciamento.

Passo 1 Restaure o arquivo de chave pública no formato correto.

1. Clique duas vezes em **PuTTYgen.exe**. A página **PuTTY Key Generator** é exibida, como mostrado em **Figura 3-5**.

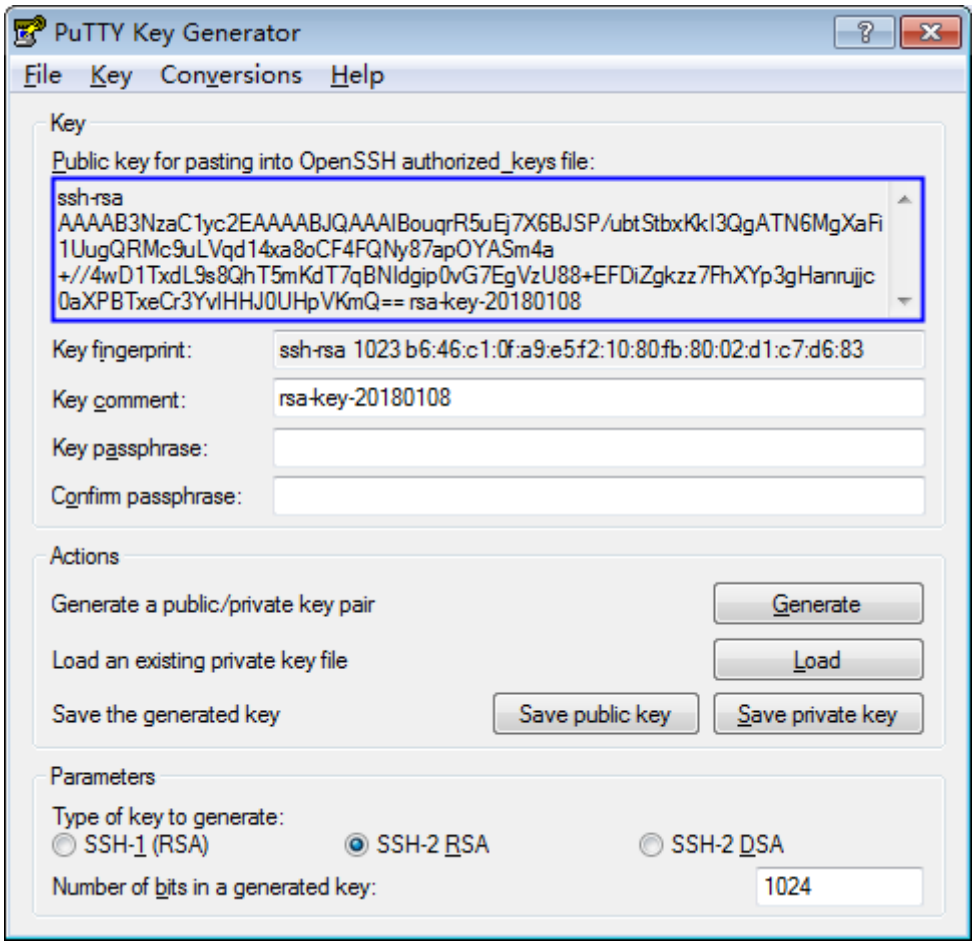
Figura 3-5 Interface principal do PuTTY Key Generator



2. Clique em **Load** e selecione a chave privada.

   O sistema carrega automaticamente a chave privada e restaura o formato do conteúdo da chave pública no **PuTTY Key Generator**. O conteúdo na caixa vermelha em **Figura 3-6** é a chave pública com o formato atendendo aos requisitos do sistema.

Figura 3-6 Restaurar o formato do conteúdo da chave pública



3. Copie as informações no quadrado azul e salve-as em um arquivo **.txt** local.

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 2 Importe o arquivo de chave pública no formato correto para o console do KPS.

1. Faça logon no console de gerenciamento.
2. Clique em ☰ à esquerda, escolha **Security & Compliance** > **Data Encryption Workshop**, a página de gerenciamento de chaves é exibida.
3. No painel de navegação, clique em **Key Pair Service**.
4. Na página **Key Pair Service**, clique em **Import Key Pair**.
5. Clique em **Select File**, selecione o arquivo .txt de chave pública ou copie e cole o conteúdo da chave pública na caixa de texto do conteúdo da chave pública.
6. Clique em **OK** para importar o arquivo de chave pública.

----Fim

3.4 O que devo fazer quando não consigo importar um par de chaves usando o Internet Explorer 9?

Sintoma

A importação de um par de chaves pode falhar se o Internet Explorer 9 for usado.

Procedimento

Passo 1 Clique em  no canto superior direito do navegador.

Passo 2 Selecione **Internet Options**.

Passo 3 Clique na guia **Security** na caixa de diálogo exibida.

Passo 4 Clique em **Internet**.

Passo 5 Se o nível de segurança indicar **Custom**, clique em **Default Level** para restaurar as configurações padrão.

Passo 6 Mova a barra de rolagem para definir o nível de segurança como **Medium** e clique em **Apply**.

Passo 7 Clique em **Custom Level**.

Passo 8 Defina **Initialize and script ActiveX controls not marked as safe for scripting** como **Prompt**.

Passo 9 Clique em **Yes**.

----Fim

3.5 Como fazer logon em um ECS de Linux com uma chave privada?

Cenário

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.

Efetuar logon a partir de um computador de Windows

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

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

As operações a seguir usam o PuTTY para fazer logon no ECS. Antes de efetuar logon, você deve obter o formato de chave privada no formato .ppk.

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**.

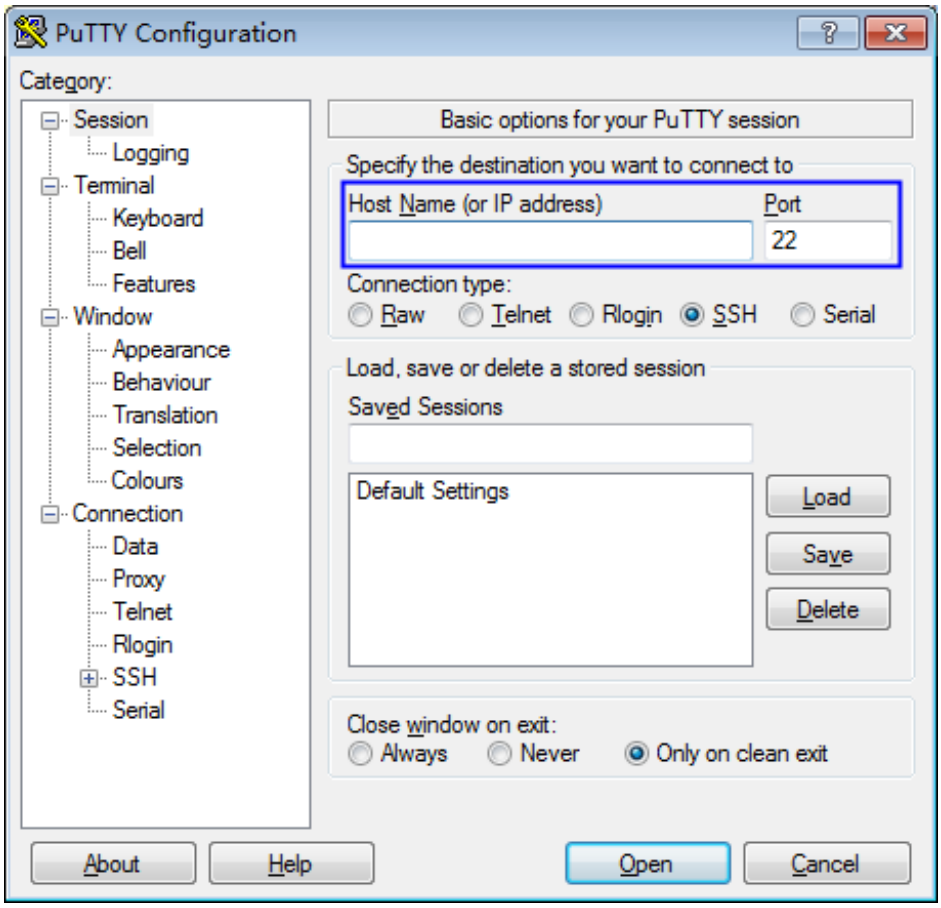
NOTA

- 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 3-7 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

3.6 Como usar uma chave privada para obter a senha para fazer logon em um ECS do Windows?

Cenário

Uma senha é necessária quando você faz logon em um ECS do Windows. Primeiro, você deve obter a senha de administrador (senha da conta **Administrator** ou outra conta definida no

Cloudbase-Init) gerada durante a instalação inicial do ECS a partir do arquivo de chave privada baixado quando você cria o ECS. Essa senha é gerada aleatoriamente, oferecendo alta segurança.

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

NOTA

- 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. Depois de limpa, a senha não poderá ser recuperada. 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 a *Referência de API do Elastic Cloud Server*.

Pré-requisitos

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

Obtenção de uma senha

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

3.7 Como lidar com a falha na vinculação de um par de chaves?

Sintoma

Falha ao vincular o par de chaves ao ECS.

NOTA

- A caixa de diálogo **Failed Key Pair Task** apenas registra e exibe operações de par de chaves com falha em ECSs, que não afetam o status do ECS e as operações subsequentes. É possível clicar em **Delete** na linha do registro de falha para excluí-lo ou clicar em **Delete All** para excluir todos os registros de falha.
- Clique em **Learn more** para visualizar documentos relacionados.

Possíveis causas

- Uma senha incorreta ou inválida foi fornecida.
- A permissão ou grupo de proprietários do arquivo de chave pública foi alterado.
- A configuração SSH do ECS foi modificada.
- A direção de entrada da porta 22 do grupo de segurança ECS não está aberta para 100.125.0.0/16.
- O ECS foi desligado, iniciado ou um disco foi desanexado durante o processo de vinculação do par de chaves ao ECS.
- A conexão de rede está com defeito.
- As regras de firewall foram configuradas para o ECS.

Procedimento de manuseio

Passo 1 Verifique o status do ECS.

- Se estiver em execução, vá para **Passo 2**.
- Se estiver desligado, vá para **Passo 5**.

Passo 2 Use a senha para fazer logon no ECS para verificar se a senha está correta.

- Se estiver correta, vá para **Passo 4**.
- Se estiver incorreta, use a senha correta para vincular o par de chaves novamente.

Passo 3 Verifique se o caminho de permissão e o grupo de proprietários do arquivo **/root/.ssh/authorized_keys** no ECS foram modificados.

- Se sim, restaure a permissão para o seguinte:
  - O grupo proprietário de cada nível tem a permissão **root:root**.
  - A permissão para o arquivo .ssh é 700.
  - A permissão para **authorized_keys** é 600.
- Se não, vá para **Passo 4**.

Passo 4 Verifique se o arquivo **/root/.ssh/authorized_keys** do ECS foi modificado.

- Se sim, restaure o conteúdo original do arquivo **/root/.ssh/authorized_keys** com base nos requisitos do site.
- Se não, vá para **Passo 5**.

Passo 5 Verifique se a direção de entrada da porta 22 do grupo de segurança do ECS está aberta para 100.125.0.0/16. Ou seja, 100.125.0.0/16 pode se conectar remotamente a ECSs do Linux por meio de SSH.

- Se sim, vá para **Passo 6**.
- Se não, adicione a seguinte regra de grupo de segurança e vincule o par de chaves novamente. Para obter detalhes sobre como adicionar um grupo de segurança, consulte **Adição de uma regra de grupo de segurança**.

Direção	Protocolo/ aplicação	Porta	Fonte
Entrada	SSH (22)	22	0.0.0.0/0

Passo 6 Verifique se o ECS pode ser ligado, desligado e conectado.

- Se sim, vincule o par de chaves novamente.
- Se não, vá para **Passo 7**.

Passo 7 Verifique se a rede está com defeito.

- Se sim, entre em contato com o suporte técnico para verificar e localizar a falha.
- Se não, vincule o par de chaves novamente.

----Fim

3.8 Como lidar com a falha na substituição de um par de chaves?

Sintoma

Falha ao substituir o par de chaves no ECS.

NOTA

A caixa de diálogo **Failed Key Pair Task** apenas registra e exibe operações de par de chaves com falha em ECSs, que não afetam o status do ECS e as operações subsequentes. É possível clicar em **Delete** na linha do registro de falha para excluí-lo ou clicar em **Delete All** para excluir todos os registros de falha.

Possíveis causas

- Uma chave privada incorreta ou inválida foi fornecida.
- A direção de entrada da porta 22 do grupo de segurança do ECS não está aberta para 100.125.0.0/16.
- A configuração SSH do ECS foi modificada.
- O ECS foi desligado, iniciado ou um disco foi desanexado durante o processo de substituição do par de chaves para o ECS.
- A conexão de rede está com defeito.
- As regras de firewall foram configuradas para o ECS.

Procedimento de manuseio

Passo 1 Use o par de chaves SSH para fazer logon no ECS e verifique se a chave privada está correta.

- Se estiver correta, vá para **Passo 2**.
- Se estiver incorreta, use a chave privada correta para substituir o par de chaves novamente.

Passo 2 Verifique se o arquivo **/root/.ssh/authorized_keys** do ECS foi modificado.

- Se sim, restaure o conteúdo original do arquivo **/root/.ssh/authorized_keys** com base nos requisitos do site.
- Se não, vá para **Passo 3**.

Passo 3 Verifique se a direção de entrada da porta 22 do grupo de segurança do ECS está aberta para 100.125.0.0/16. Ou seja, 100.125.0.0/16 pode se conectar remotamente a ECSs do Linux por meio de SSH.

- Se sim, vá para **Passo 4**.
- Se não, adicione a seguinte regra de grupo de segurança e substitua o par de chaves novamente.

Direção	Protocolo/ aplicação	Porta	Fonte
Entrada	SSH (22)	22	0.0.0.0/0

Passo 4 Verifique se o ECS pode ser ligado, desligado e conectado.

- Se sim, substitua o par de chaves novamente.
- Se não, vá para **Passo 5**.

Passo 5 Verifique se a rede está com defeito.

- Se sim, entre em contato com o suporte técnico para verificar e localizar a falha.
- Se não, substitua o par de chaves novamente.

----Fim

3.9 Como lidar com a falha na redefinição de um par de chaves?

Sintoma

Falha ao redefinir o par de chaves no ECS.

NOTA

A caixa de diálogo **Failed Key Pair Task** apenas registra e exibe operações de par de chaves com falha em ECSs, que não afetam o status do ECS e as operações subsequentes. É possível clicar em **Delete** na linha do registro de falha para excluí-lo ou clicar em **Delete All** para excluir todos os registros de falha.

Possíveis causas

- A direção de entrada da porta 22 do grupo de segurança do ECS não está aberta para 100.125.0.0/16.
- O ECS foi desligado, iniciado ou um disco foi desanexado durante o processo de redefinição do par de chaves para o ECS.
- A conexão de rede está com defeito.
- As regras de firewall foram configuradas para o ECS.

Procedimento de manuseio

Passo 1 Verifique se a direção de entrada da porta 22 do grupo de segurança do ECS está aberta para 100.125.0.0/16. Ou seja, 100.125.0.0/16 pode se conectar remotamente a ECSs do Linux por meio de SSH.

- Se sim, vá para **Passo 2**.
- Se não, adicione a regra de grupo de segurança a seguir e redefina o par de chaves novamente.

Direção	Protocolo/ aplicação	Porta	Fonte
Entrada	SSH (22)	22	0.0.0.0/0

Passo 2 Verifique se o ECS pode ser ligado, desligado e conectado.

- Se sim, redefina o par de chaves novamente.
- Se não, vá para **Passo 3**.

Passo 3 Verifique se a rede está com defeito.

- Se sim, entre em contato com o suporte técnico para verificar e localizar a falha.
- Se não, redefina o par de chaves novamente.

----Fim

3.10 Como lidar com a falha na desvinculação de um par de chaves?

Sintoma

Falha ao desvincular o par de chaves do ECS.

NOTA

A caixa de diálogo **Failed Key Pair Task** apenas registra e exibe operações de par de chaves com falha em ECSs, que não afetam o status do ECS e as operações subsequentes. É possível clicar em **Delete** na linha do registro de falha para excluí-lo ou clicar em **Delete All** para excluir todos os registros de falha.

Possíveis causas

- Uma chave privada incorreta ou inválida foi fornecida.
- A direção de entrada da porta 22 do grupo de segurança do ECS não está aberta para 100.125.0.0/16.
- A configuração SSH do ECS foi modificada.
- O ECS foi desligado, iniciado ou um disco foi desanexado durante o processo de desvinculação do par de chaves do ECS.
- A conexão de rede está com defeito.
- As regras de firewall foram configuradas para o ECS.

Procedimento de manuseio

Passo 1 Verifique o status do ECS.

- Se estiver em execução, vá para **Passo 2**.
- Se estiver desligado, vá para **Passo 4**.

Passo 2 Use o par de chaves SSH para fazer logon no ECS e verifique se a chave privada está correta.

- Se estiver correta, vá para **Passo 4**.
- Se estiver incorreta, use a chave privada correta para desvincular o par de chaves novamente.

Passo 3 Verifique se o arquivo **/root/.ssh/authorized_keys** do ECS foi modificado.

- Se sim, restaure o conteúdo original do arquivo **/root/.ssh/authorized_keys**.
- Se não, vá para **Passo 4**.

Passo 4 Verifique se a direção de entrada da porta 22 do grupo de segurança do ECS está aberta para 100.125.0.0/16. Ou seja, 100.125.0.0/16 pode se conectar remotamente a ECSs do Linux por meio de SSH.

- Se sim, vá para **Passo 5**.
- Se não, adicione a seguinte regra de grupo de segurança e desvincule o par de chaves novamente.

Direção	Protocolo/ aplicação	Porta	Fonte
Entrada	SSH (22)	22	0.0.0.0/0

Passo 5 Verifique se o ECS pode ser ligado, desligado e conectado.

- Se sim, desvincule o par de chaves novamente.
- Se não, vá para **Passo 6**.

Passo 6 Verifique se a rede está com defeito.

- Se sim, entre em contato com o suporte técnico para verificar e localizar a falha.
- Se não, desvincule o par de chaves novamente.

----Fim

3.11 Preciso reiniciar os servidores depois de substituir seu par de chaves?

Não. A substituição do par de chaves não afeta os serviços.

3.12 Como ativar o modo de logon com senha para um ECS?

Se você desativar o modo de logon com senha ao vincular um par de chaves a um ECS, poderá ativar o modo de logon com senha novamente mais tarde quando precisar.

Procedimento

O exemplo a seguir descreve como fazer logon no ECS usando PuTTY e ativar o modo de logon com senha.

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**.

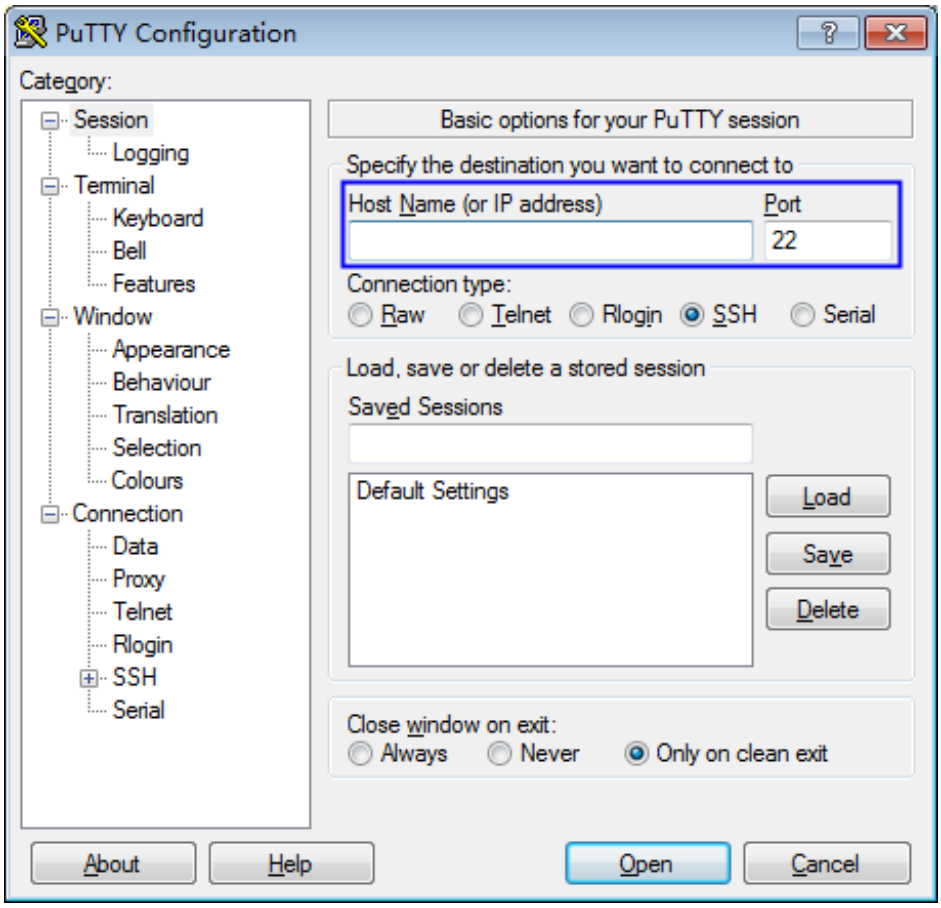
Passo 3 Escolha **Connection** > **SSH** > **Auth**. Em **Private key file for authentication**, clique em **Browse** e selecione um arquivo de chave privada (no formato **.ppk**).

NOTA

Se o arquivo estiver no formato **.pem**, converta-o referindo-se a **Conversão do arquivo de chave privada no formato .pem para o formato .ppk**.

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

Figura 3-8 Configuração do EIP



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

Passo 6 Execute o seguinte comando para abrir o arquivo **/etc/ssh/sshd_config**:

vi /etc/ssh/sshd_config

Passo 7 Pressione **i** para entrar no modo de edição e ativar o modo de logon com senha.

- Para um sistema operacional não SUSE, altere o valor de **PasswordAuthentication** para **yes**.
  ```
  PasswordAuthentication yes
  ```
- Para um sistema operacional SUSE, altere os valores de **PasswordAuthentication** e **UsePAM** para **yes**.
  ```
  PasswordAuthentication yes
  UsePAM yes
  ```

  NOTA

  - Sistema operacional não SUSE

    Para desativar o logon com senha, altere o valor de **PasswordAuthentication** para **no**. Se o parâmetro **PasswordAuthentication** não estiver contido no arquivo **/etc/ssh/sshd_config**, adicione-o e defina-o como **no**.
  - Sistema operacional SUSE

    Para desativar o logon com senha, altere os valores de **PasswordAuthentication** e **UsePAM** para **no**. Se o arquivo não contiver os parâmetros **PasswordAuthentication** e **UsePAM**, adicione os parâmetros e defina os valores como **no**.

Passo 8 Pressione **Esc** para sair do modo de edição.

Passo 9 Digite **:wq** e pressione **Enter** para salvar e sair.

Passo 10 Execute o seguinte comando para reiniciar o serviço SSH para que a configuração entre em vigor:

- Sistema operacional não Ubuntu14.xx

  service sshd restart
- Sistema operacional Ubuntu14.xx

  service ssh restart

----Fim

3.13 Como lidar com a falha no logon no ECS após desvincular o par de chaves?

Sintoma

- Quando o modo de logon de um ECS é o par de chaves, mas o par de chaves inicial foi desvinculado, não há senha ou par de chaves disponível para fazer logon no ECS. Como resolver esse problema?
- Ao vincular um par de chaves a um ECS no console do KPS, desativei o modo de logon com senha. Depois que o par de chaves é desvinculado, não tenho senha e par de chaves para fazer logon no ECS. Como resolver esse problema?

Procedimento

Método 1: redefinir a senha

Redefina a senha no console do ECS e use a senha para fazer logon no ECS. Para obter detalhes, consulte *Guia de usuário do Elastic Cloud Server*.

Método 2: redefinir o par de chaves

Desligue o ECS, vincule o par de chaves ao ECS no console do KPS e use o par de chaves para efetuar logon no ECS. O procedimento é o seguinte:

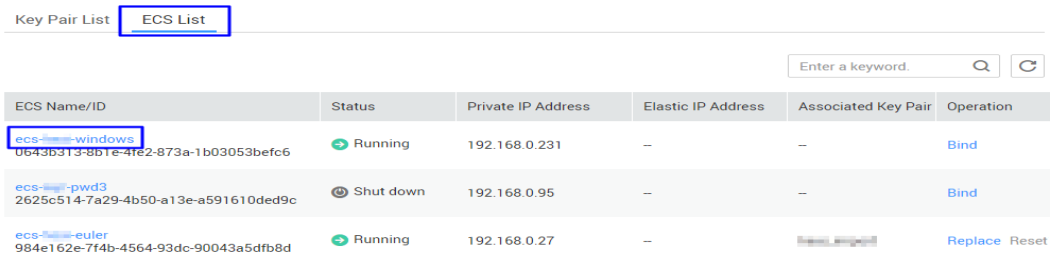
Passo 1 **Faça logon no console de gerenciamento**.

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 Clique em **ECS List** para exibir os ECSs. Para mais detalhes, consulte **Figura 3-9**.

Figura 3-9 Lista do ECS



Passo 5 Clique no nome do ECS de destino. A página de detalhes do ECS é exibida.

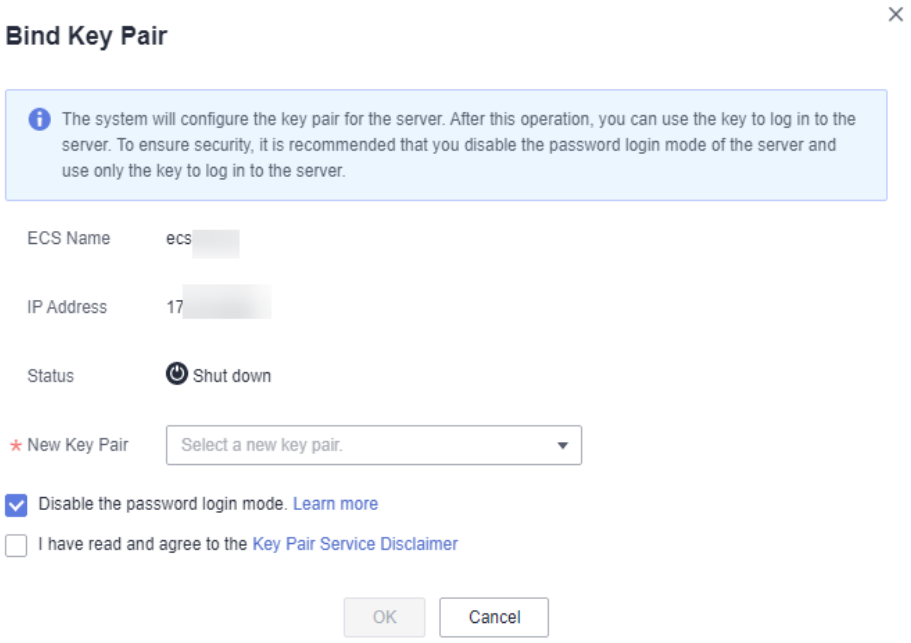
Passo 6 Clique em **Shut Down** no canto superior direito da página para desligar o ECS.

Passo 7 Retorne à página de lista do ECS consultando a etapa **Passo 5**.

Passo 8 Clique em **Bind** na linha do ECS de destino. A caixa de diálogo **Bind Key Pair** é exibida.

Passo 9 Selecione um novo par de chaves na caixa de listagem suspensa de **New Key Pair**.

Figura 3-10 Vinculação de um par de chaves



Passo 10 Você pode escolher se deseja desativar o modo de logon com senha conforme necessário. Por padrão, o modo de logon com senha está desativado.

NOTA

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

Passo 11 Selecione **I have read and agree to the Key Pair Service Disclaimer**.

Passo 12 Clique em **OK**. O par de chaves é vinculado. Depois que a vinculação for concluída, você poderá usar o par de chaves para fazer logon no ECS.

----Fim

3.14 O que devo fazer se minha chave privada for perdida?

Para chave privada gerenciada no KPS

Você pode exportar a chave privada do KPS novamente.

Para chave privada não gerenciada no KPS

A chave privada não pode ser recuperada.

Você pode redefinir a senha ou o par de chaves vinculado ao ECS. Para mais detalhes, consulte **Como lidar com a falha no logon no ECS após desvincular o par de chaves?**

3.15 Como converter o formato de um arquivo de chave privada?

Conversão do arquivo de chave privada no formato .ppk para o formato .pem

A chave privada a ser carregada ou copiada para a caixa de texto deve estar no formato .pem. Se o arquivo estiver no formato .ppk, execute as seguintes etapas:

Passo 1 Visite o seguinte site e baixe o PuTTY e o PuTTYgen:

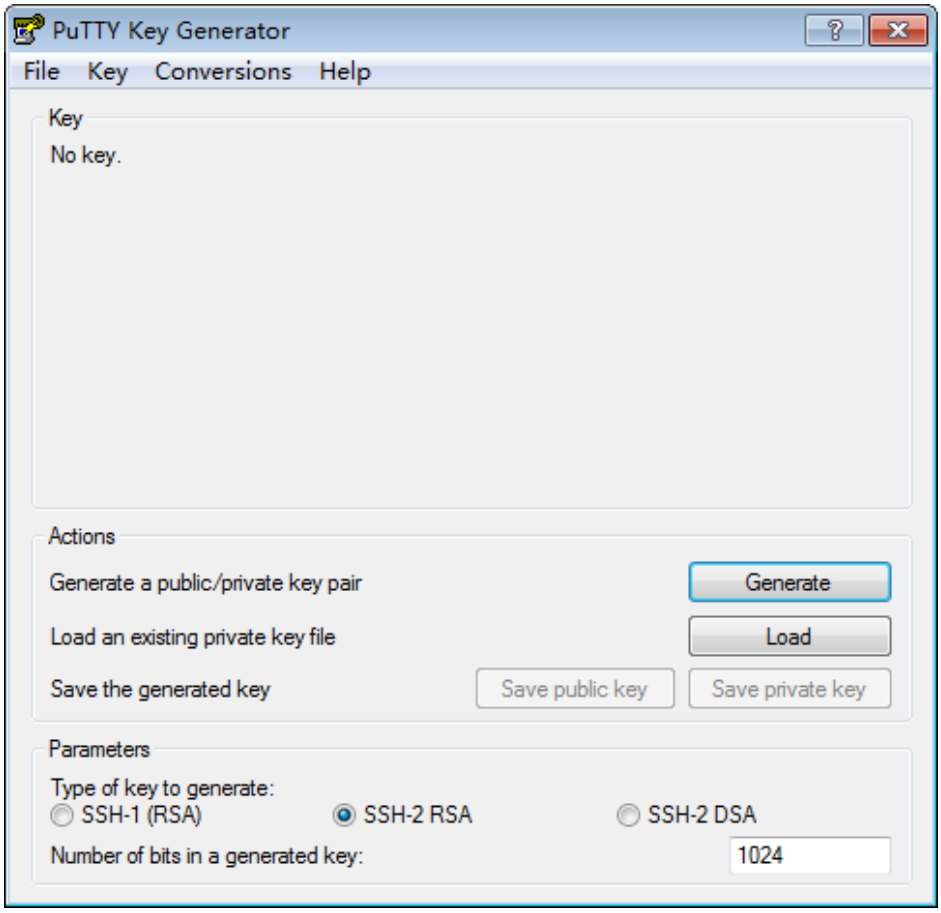
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

NOTA

PuTTYgen é um gerador de chave privada, que é usado para criar um par de chaves que consiste em uma chave pública e uma chave privada para o PuTTY.

Passo 2 Clique duas vezes em **PuTTYGEN.exe**. A página **PuTTY Key Generator** é exibida, como mostrado em **Figura 3-11**.

Figura 3-11 Gerador de chaves PuTTY



Passo 3 Escolha **Conversions** > **Import Key** para importar o arquivo de chave privada no formato **.ppk**.

Passo 4 Escolha **Conversions** > **Export OpenSSH Key**, a caixa de diálogo **PuTTYgen Warning** é exibida.

Passo 5 Clique em **Yes** para salvar o arquivo no formato **.pem**.

----Fim

Conversão do arquivo de chave privada no formato .pem para o formato .ppk

Quando você usa o PuTTY para efetuar logon em um ECS do Linux, a chave privada deve estar no formato .ppk. Se o arquivo estiver no formato .pem, execute as seguintes etapas para converter seu formato:

Passo 1 Visite o seguinte site e baixe o PuTTY e o PuTTYgen:

http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

NOTA

PuTTYgen é um gerador de chave privada, que é usado para criar um par de chaves que consiste em uma chave pública e uma chave privada para o PuTTY.

Passo 2 Clique duas vezes em **PuTTYgen.exe**. A janela **PuTTY Key Generator** é exibida.

Passo 3 Na área **Actions**, clique em **Load** e importe o arquivo de chave privada que você armazenou ao comprar o ECS.

Verifique se o formato de arquivo de chave privada está incluído em **All files (*.*)**.

Passo 4 Clique em **Save private key**.

Passo 5 Salve a chave privada convertida, por exemplo, **kp-123.ppk**, em um diretório local.

----Fim

3.16 Posso alterar o par de chaves de um servidor?

Sim.

Você pode desvincular, redefinir ou substituir um par de chaves conforme necessário. Para obter detalhes, consulte **Gerenciamento de pares de chaves**.

3.17 Um par de chaves pode ser compartilhado por vários usuários?

Os pares de chaves não podem ser compartilhados entre contas, mas podem ser compartilhados pelos usuários do IAM na mesma conta de uma das seguintes maneiras:

- Importar um par de chaves. Para permitir que vários usuários do IAM usem o mesmo par de chaves, você pode criar um par de chaves (usando o PuTTYgen ou outras ferramentas) e importá-lo como um recurso de usuário do IAM. Para obter detalhes, consulte **Importação de um par de chaves**.
- Atualizar um par de chaves de usuário para um par de chaves de conta. É possível **atualizar** um par de chaves **criado no console de gerenciamento** ou importado para o console.

3.18 Como obter o arquivo de chave pública ou privada de um par de chaves?

Obtenção de um arquivo de chave privada

Quando você **cria um par de chaves**, seu arquivo de chave privada será baixado automaticamente.

- Se a chave privada não for gerenciada, ela não poderá ser baixada posteriormente. Guarde-a adequadamente.
- Se você autorizou a Huawei Cloud a gerenciar chaves privadas, poderá exportar as chaves privadas gerenciadas. Para obter detalhes, consulte **Exportação de uma chave privada**.

Obtenção de um arquivo de chave pública

- Se um par de chaves for criado no console de gerenciamento, sua chave pública será armazenada automaticamente na Huawei Cloud. Você pode pressionar **F12** para atualizar a lista de pares de chaves e anotar o campo **public_key** na lista.

- Se um par de chaves foi criado usando o PuTTYgen, você pode encontrar sua chave pública no caminho de armazenamento em seu PC local.

3.19 O que posso fazer se um erro for relatado quando uma chave de conta for criada ou atualizada pela primeira vez?

Criação de um par de chaves de conta pela primeira vez

Ao criar um par de chaves de conta pela primeira vez, você precisa usar um usuário com a função de sistema Administrador do locatário.

Atualização de um par de chaves de conta pela primeira vez

Depois de atualizar um par de chaves para um par de chaves de conta, todos os usuários na sua conta poderão visualizar e usar o par de chaves. Se o nome de um par de chaves for igual ao nome do par de chaves privado de outro subusuário, a atualização não poderá ser realizada. Para atualizar os pares de chaves, 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.

3.20 A cota de par de chaves de conta será ocupada depois que um par de chaves privadas for atualizado para um par de chaves de conta?

Não.

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.

4 Relacionado ao HSM dedicado

4.1 O que é o HSM dedicado?

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

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

4.2 Como o HSM dedicado garante a segurança para a geração de chaves?

- Uma chave é criada remotamente pelo usuário. Durante a criação, apenas o UKey de propriedade do usuário está envolvido na autenticação.
- A configuração do HSM e a preparação das chaves internas podem ser realizadas somente após a autenticação usando o UKey como credencial.

O usuário tem controle total sobre a geração, armazenamento e acesso de chaves. O HSM dedicado é responsável apenas por monitorar e gerenciar HSMs e instalações de rede relacionadas.

4.3 O pessoal da sala de equipamentos tem a função de superadministrador para roubar informações usando um UKey privilegiado?

Os UKeys são de propriedade apenas de usuários que compraram instâncias de HSM dedicado. O pessoal da sala de equipamentos não tem a função de superadministrador.

Os dados confidenciais (chaves) são armazenados em chips. Mesmo o fornecedor de HSM não pode acessar as informações de chave interna.

4.4 Quais HSMs são usados para HSM dedicado?

O HSM dedicado usa HSMs que obtiveram certificação de China State Cryptography Administration (CSCA) e certificação de FIPS 140-2 nível 3, alcançando alta segurança.

4.5 Quais APIs o HSM dedicado suporta?

O HSM dedicado fornece as mesmas funções e interfaces que os dispositivos criptográficos físicos, ajudando você a migrar facilmente os serviços para a nuvem. As APIs suportadas incluem PKCS#11 e CSP.

Para detalhes, consulte **Edições**.

4.6 Como ativar o acesso público a uma instância do HSM dedicado?

Você pode vincular EIPs para acessar instâncias de HSM dedicado a partir da rede pública.

Pré-requisitos

Você tem um EIP que pode ser vinculado à instância do HSM dedicado.

Restrições

- Depois que um EIP é vinculado a uma instância de HSM dedicado, podem ocorrer ataques à rede pública. Tenha cuidado ao vincular um EIP a uma instância de HSM dedicado.
- EIPs são recursos cobrados. Você precisa configurar EIPs conforme necessário. Se você não precisa de EIPs, desvincule-os em tempo hábil. Para obter detalhes sobre como desvincular EIPs, consulte . Se o EIP não for liberado após a desvinculação, a Huawei Cloud cobrará a taxa de retenção de endereço IP. Se um EIP de pagamento por uso cobrado por largura de banda for desvinculado de uma instância, a largura de banda continuará a ser cobrada.

Procedimento

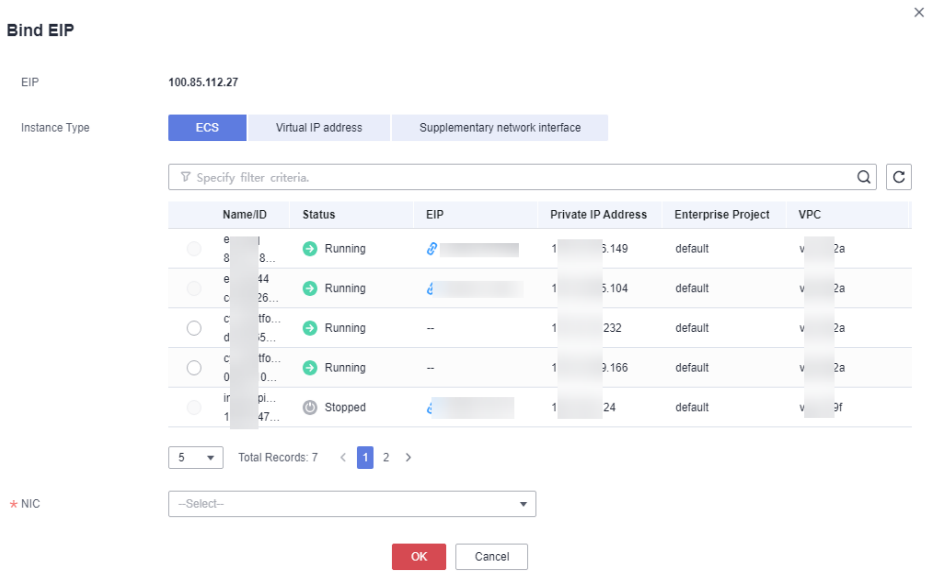
Passo 1 **Faça logon no console de gerenciamento**.

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

Passo 3 Clique em  no lado esquerdo da página. Selecione **Network** > **EIP**. A página de EIP é exibida por padrão.

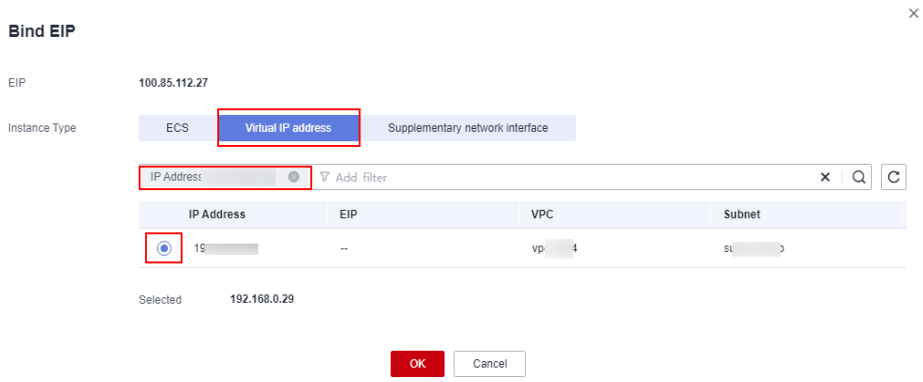
Passo 4 Clique em **Bind** na coluna **Operation** do EIP de destino. A página Bind é exibida, como mostrado na **Figura 4-1**.

Figura 4-1 Vinculação de um EIP



Passo 5 Clique em **Virtual IP Address**, insira o endereço IPv4 da instância a ser vinculada na caixa de pesquisa e selecione o resultado da pesquisa, conforme mostrado em **Vinculação de um endereço IP virtual**.

Figura 4-2 Vinculação de um endereço IP virtual



Passo 6 Selecione o endereço IP correspondente e clique em **OK**.

----Fim

5 Preços

5.1 Como o DEW é cobrado?

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

KMS

O KMS é cobrado por uso. Não é necessário pagar uma taxa mínima. Depois que uma CMK for criada, ela será cobrada por hora. Você paga pelas CMKs que criou e pelas solicitações de API que estão além da faixa gratuita.

KPS

- Se você não optar por permitir que a Huawei Cloud gerencie suas chaves privadas ao criá-las ou importá-las, nenhum custo será incorrido.
- Se você tiver suas chaves gerenciadas pela Huawei Cloud, o KPS será cobrado por hora. Na versão atual, é gratuito.

HSM dedicado

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

CSMS

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

5.2 Como renovar o DEW?

Esta seção descreve como renovar o KMS ou uma instância de HSM dedicado. Após a renovação, você poderá continuar a usar a instância do KMS e do HSM dedicado.

- Renovação automática

Se você selecionou e concordou com a renovação automática do KMS ou do HSM dedicado, o sistema gera automaticamente um pedido de renovação e renova a assinatura com base no período de assinatura original antes que o serviço expire.

- Renovação manual

  Antes que o serviço expire, o sistema enviará uma mensagem SMS ou e-mail para lembrá-lo de renová-lo.

  Se você não renovar o serviço antes que ele expire, ele entrará no período de retenção.

  NOTA

  Se você não renovar sua assinatura antes que ela expire, um período de retenção será aplicado. O período de retenção varia de acordo com os níveis do cliente. Para obter detalhes, consulte **Período de retenção**.

Tabela 5-1 Período de retenção

Serviço	Edição	Período de retenção
KMS	Padrão	As chaves estão congeladas. Ative as chaves congeladas fazendo uma recarga na conta.
HSM dedicado	-	● Dentro do período de retenção, suas instâncias de HSM dedicado não podem ser usadas, mas são reservadas para você. ● Se o período de retenção expirar, suas instâncias de HSM dedicado serão liberadas.

NOTA

- Chaves congeladas não podem ser usadas para criptografia ou descriptografia. Para evitar perdas desnecessárias, é recomendável que você renove o serviço dentro do prazo.
- Os dados relacionados a instâncias de HSM dedicado serão perdidos quando as instâncias forem liberadas. Para evitar perdas desnecessárias, é recomendável renovar o serviço ou recarregar a conta a tempo.

Pré-requisitos

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

NOTA

Uma conta com a permissão **BSS Administrator** pode executar qualquer operação em todos os itens de menu na central de contas, na central de cobrança e na central de recursos.

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 No painel de navegação à esquerda, clique em ☰ e escolha **Security & Compliance** > **Data Encryption Workshop**.

Passo 4 No canto superior direito, clique em **Renew**.

Passo 5 Na página de gerenciamento de renovação, conclua a renovação conforme solicitado.

Para obter detalhes, consulte **Renovação manual de um recurso**.

----Fim

5.3 Como cancelar a assinatura do DEW?

O DEW não suporta o cancelamento de assinatura.

NOTA

Se você não conseguir criar uma instância de HSM dedicado, poderá clicar em **Delete** na linha em que a instância com falha está localizada para excluí-la. Em seguida, você pode enviar um tíquete de serviço para solicitar o reembolso.

Links úteis

- **Regras de cancelamento de assinatura**
- **Lista de produtos de serviços em nuvem dos quais você não pode cancelar a assinatura**
- **Criação de um tíquete de serviço**

5.4 Uma CMK será cobrada depois de ser desativada?

Sim.

Uma CMK desativada ainda é mantida e conservada pelo KMS. Você pode ativá-la sempre que precisar. Portanto, uma CMK desativada ainda é faturável. Somente as CMKs excluídas não são cobradas.

5.5 As credenciais programadas para serem excluídas são cobradas?

Não.

Uma credencial no status de exclusão pendente não incorre em cobranças.

Se você cancelar a exclusão, a cobrança será retomada a partir do momento em que a credencial foi programada para ser excluída.

5.6 Uma CMK será cobrada após ser programada para exclusão?

Não.

O período pendente de uma CMK, desde seu agendamento até sua exclusão, não é cobrado.

No entanto, se você cancelar a exclusão programada, a cobrança será retomada a partir do momento em que a CMK estiver programada para ser excluída.

6 Geral

6.1 Quais funções o DEW fornece?

Serviço de gerenciamento de chaves

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

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

  Você pode gerar números aleatórios de 512 bits com base no hardware usando a API do KMS. Os números aleatórios verdadeiros de 512 bits podem ser usados como base para os materiais de chaves e parâmetros de criptografia. Para obter detalhes, consulte a *Referência de API do Data Encryption Workshop*.

Serviço de par de chaves

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

- Criar, importar, exibir e excluir pares de chaves
- Redefinir, substituir, vincular e desvincular pares de chaves

- Gerenciar, importar, exportar e limpar chaves privadas

HSM dedicado

Na página **Dedicated HSM** do console de gerenciamento, você pode comprar instâncias de HSM dedicado.

6.2 Quais algoritmos de criptografia o DEW usa?

Algoritmos criptográficos suportados pelo KPS

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

Algoritmos de criptografia suportados

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

Tabela 6-1 Algoritmos de criptografia suportados

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

6.3 Em quais regiões os serviços do DEW estão disponíveis?

Os serviços do DEW estão disponíveis nas seguintes regiões:

- KMS
  - CN-Hong Kong
  - AP-Bangkok
  - AP-Singapore
  - AF-Johannesburg
  - LA-Mexico City1
  - LA-Mexico City2
  - LA-Santiago
  - LA-Sao Paulo1
- KPS
  - CN-Hong Kong
  - AP-Bangkok
  - AP-Singapore
  - LA-Sao Paulo1
- CSMS
  - CN-Hong Kong
  - AP-Bangkok
  - AP-Singapore
  - LA-Sao Paulo1
- HSM dedicado
  - CN-Hong Kong
  - AP-Bangkok
  - AP-Singapore
  - LA-Santiago

6.4 O que é uma cota?

O que é uma cota?

As cotas são aplicadas aos recursos de serviço na plataforma para evitar picos imprevistos no uso de recursos. As cotas podem limitar o número ou a quantidade de recursos disponíveis para os usuários. Por exemplo, o número máximo de CMKs que você pode criar.

Se a cota de recursos existente não puder atender aos seus requisitos de serviço, você poderá solicitar uma cota mais alta.

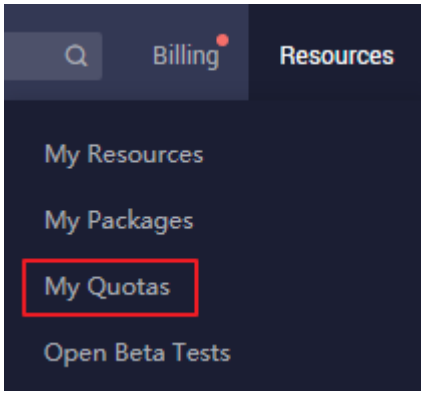
Como visualizar minha cota?

Passo 1 Faça logon no console de gerenciamento.

Passo 2 No canto superior direito da página, escolha **Resources** > **My Quotas**.

A página **Service Quota** é exibida.

Figura 6-1 Minhas cotas



Passo 3 Visualize a cota usada e total de cada tipo de recursos na página exibida.

Passo 4 Se uma cota não puder atender aos requisitos de serviço, clique em **Increase Quota** para alterá-la.

----Fim

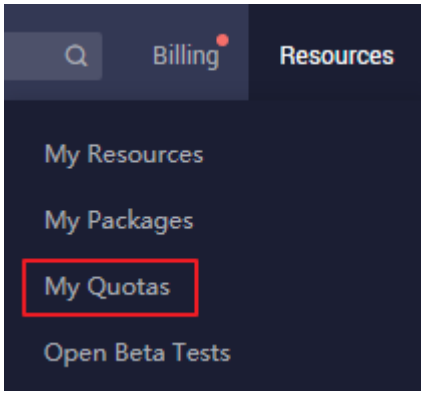
Como aumentar uma cota?

Passo 1 Faça logon no console de gerenciamento.

Passo 2 No canto superior direito da página, escolha **Resources** > **My Quotas**.

A página **Service Quota** é exibida.

Figura 6-2 Minhas cotas



Passo 3 Clique em **Increase Quota**.

Passo 4 Na página **Create Service Ticket**, configure os parâmetros conforme necessário.

Na área **Problem Description**, preencha o conteúdo e o motivo do aumento.

Passo 5 Depois que todos os parâmetros obrigatórios estiverem configurados, selecione **I have read and agree to the Tenant Authorization Letter and Privacy Statement** e clique em **Submit**.

----Fim

6.5 Qual é o mecanismo de alocação de recursos do DEW?

O DEW usa regiões como grandes pools de recursos e recursos ou serviços independentes de cada cliente como pequenos pools de recursos. O fundo tem limites de tráfego padrão. Para um único usuário, se o tráfego exceder o limite, a velocidade do serviço será lenta. Para clientes que têm requisitos de tráfego pesado, os recursos em segundo plano podem ser alterados com base na situação e nos requisitos reais.

Se o volume de tráfego exceder o limite, você poderá enviar um tíquete de serviço para aumentar a cota. O DEW ajustará seu limite em segundo plano para dar suporte ao provisionamento de clusters de configuração dedicados e garantir a execução estável do serviço.

6.6 O que são regiões e AZs?

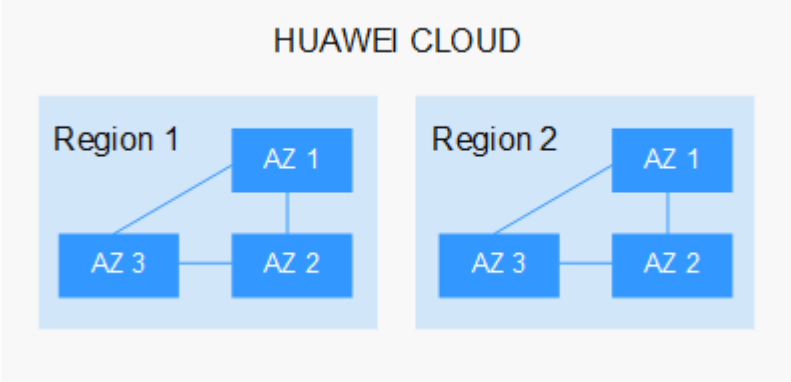
Conceitos

Uma região e uma zona de disponibilidade (AZ) identificam a localização de um data center. Você pode criar recursos em uma região e AZ específicas.

- As regiões são divididas das dimensões de localização geográfica e latência da rede. Os serviços públicos, como Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP) e Image Management Service (IMS), são compartilhados na mesma região. As regiões são classificadas como regiões universais e regiões dedicadas. Uma região universal fornece serviços de nuvem universal para locatários comuns. Uma região dedicada fornece serviços do mesmo tipo apenas ou para locatários específicos.
- Uma AZ contém um ou mais data centers físicos. Cada AZ possui instalações independentes de resfriamento, extinção de incêndio, proteção contra umidade e eletricidade. Dentro de uma AZ, computação, rede, armazenamento e outros recursos são logicamente divididos em vários clusters. As AZs dentro de uma região são interconectadas usando fibras ópticas de alta velocidade para permitir que você construa sistemas de alta disponibilidade entre AZs.

Figura 6-3 mostra a relação entre as regiões e as AZs.

Figura 6-3 Região e AZ



Huawei Cloud fornece serviços em muitas regiões do mundo. Você pode selecionar uma região e uma AZ conforme necessário.

Selecionar uma região

Ao selecionar uma região, considere os seguintes fatores:

- Localização

  Recomendamos que você selecione uma região próxima a você ou a seus usuários de destino. Isso reduz a latência da rede e melhora a taxa de acesso.

  – Se você ou seus usuários estiverem na região Pacífico Asiático e fora da China continental, selecione a região **CN-Hong Kong**, **AP-Bangkok** ou **AP-Singapore**.

  – Se você ou seus usuários estiverem na África, selecione a região **AF-Johannesburg**.

  – Se você ou seus usuários estiverem na América Latina, selecione a região **LA-Santiago**.

- Preço do recurso

  Os preços dos recursos podem variar em diferentes regiões. Para obter detalhes, consulte **Detalhes de preço do produto**.

Selecionar uma AZ

Ao determinar se deve implementar recursos na mesma AZ, considere os requisitos de suas aplicações em recuperação de desastres (DR) e latência de rede.

- Para alta capacidade de DR, implemente recursos nas diferentes AZs na mesma região.
- Para uma baixa latência de rede, implemente recursos na mesma AZ.

Regiões e pontos de extremidade

Antes de usar uma API para chamar recursos, especifique sua região e ponto de extremidade. Para obter mais detalhes, consulte **Regiões e pontos de extremidade**.

6.7 O DEW pode ser compartilhado entre contas?

Não. Atualmente, um usuário só pode usar e gerenciar suas próprias chaves e pares de chaves.

6.8 Como acessar as funções do DEW?

Você pode usar o DEW no console da Web ou chamar as funções do DEW usando APIs baseadas em HTTPS.

- Console

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

- API

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

  O DEW oferece suporte a APIs REST, permitindo que você chame APIs usando HTTPS. Você pode usar as APIs fornecidas para executar operações em chaves e pares de chaves, como criar, consultar e excluir chaves.

  As APIs do DEW usam o protocolo HTTPS para criptografar e proteger a transmissão, evitando ataques man-in-the-middle.

