Virtual Private Cloud

Guia de usuário

Edição 01

Data 30-12-2022

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.

Índice

1 VPC e sub-rede

1.1 Planejamento de rede

Antes de criar suas VPCs, determine quantas VPCs, o número de sub-redes e quais intervalos de endereços IP ou opções de conectividade serão necessários.

Como determino quantas VPCs eu preciso?

As VPCs são específicas da região. Por padrão, as redes em VPCs em regiões diferentes ou mesmo na mesma região não estão conectadas. Redes em diferentes VPCs são completamente isoladas umas das outras, esse não é o caso de redes na mesma VPC, mas em diferentes AZs. Redes na mesma VPC podem se comunicar umas com as outras, mesmo que estejam em AZs diferentes.

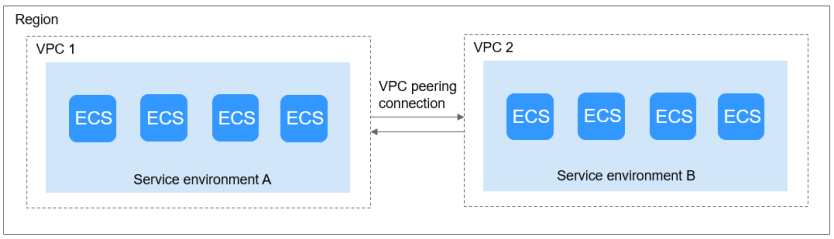
Única VPC

Se seus serviços não exigem isolamento de rede, uma única VPC deve ser suficiente.

Várias VPCs

Se você tiver vários sistemas de serviço em uma região, e cada sistema de serviço exigir uma rede isolada, poderá criar uma VPC separada para cada sistema de serviço. Se você precisar de conectividade de rede entre VPCs separadas, poderá usar uma conexão de emparelhamento de VPC, conforme mostrado em **Figura 1-1**.

Figura 1-1 Conexão de emparelhamento de VPC



Cota de VPC padrão

Por padrão, você pode criar no máximo cinco VPCs na sua conta. Se isso não puder atender aos seus requisitos de serviço, solicite um aumento de cota. Para obter detalhes, consulte **O que é uma cota?**

Como planejar sub-redes?

Uma sub-rede é um bloco CIDR único com um intervalo de endereços IP em uma VPC. Todos os recursos em uma VPC devem ser implementados em sub-redes.

- Por padrão, os ECSs em todas as sub-redes da mesma VPC podem se comunicar uns com os outros, mas os ECSs em diferentes VPCs não.

  Você pode criar conexões de emparelhamento de VPC para permitir que ECSs em VPCs diferentes, mas na mesma região, se comuniquem entre si. Para obter detalhes, consulte **Visão geral da conexão de emparelhamento de VPC**.
- Depois que uma sub-rede é criada, seu bloco CIDR não pode ser modificado.

  Ao criar uma VPC, uma sub-rede padrão será criada em conjunto. Se você precisar de mais sub-redes, consulte **Criação de uma sub-rede para a VPC** .

  As sub-redes usadas para implantar seus recursos devem residir na VPC, e as máscaras de sub-rede usadas para defini-las podem estar entre a máscara de rede do bloco CIDR da VPC e a máscara de rede /28.
  - 10.0.0.0 - 10.255.255.255
  - 172.16.0.0 - 172.31.255.255
  - 192.168.0.0 - 192.168.255.255

  NOTA

  Uma máscara de sub-rede pode estar entre a máscara de rede do bloco CIDR da VPC e a máscara de rede /28. Se um bloco CIDR da VPC for 192.168.0.0/16, sua máscara de sub-rede poderá ter entre 16 e 28.

Planejamento de sub-rede

- Recomendamos que você crie diferentes sub-redes para diferentes módulos de serviço em uma VPC. Por exemplo, você pode criar diferentes sub-redes para servidores Web, de aplicações e de banco de dados. Um servidor Web está em uma sub-rede acessível ao público, e os servidores de aplicações e bancos de dados estão em sub-redes não acessíveis ao público. Você pode aproveitar ACLs de rede para ajudar a controlar o acesso aos servidores em cada sub-rede.
- Se você precisar planejar apenas sub-redes para VPCs e a comunicação entre VPCs e data centers locais não for necessária, crie sub-redes em qualquer um dos blocos CIDR listados acima.
- Se a VPC precisar se comunicar com um data center local por meio de VPN ou Direct Connect, o bloco CIDR da VPC não poderá se sobrepor ao bloco CIDR do data center local. Portanto, ao criar uma VPC ou uma sub-rede, certifique-se de que seu bloco CIDR não se sobreponha a nenhum bloco CIDR no data center.
- Ao determinar o tamanho de um VPC ou bloco CIDR de sub-rede, certifique-se de que o número de endereços IP disponíveis no bloco CIDR atenda aos seus requisitos de serviço.

Cota de sub-rede padrão

Por padrão, você pode criar até 100 sub-redes em sua conta. Se precisar de mais, solicite um aumento de cota. Para obter detalhes, consulte **O que é uma cota?**

Como planejar políticas de roteamento?

Uma tabela de rotas contém um conjunto de rotas que são usadas para determinar para onde o tráfego de rede das suas sub-redes em uma VPC é direcionado. Quando você cria uma VPC, ela tem automaticamente uma tabela de rotas padrão, que permite a comunicação interna dentro dessa VPC.

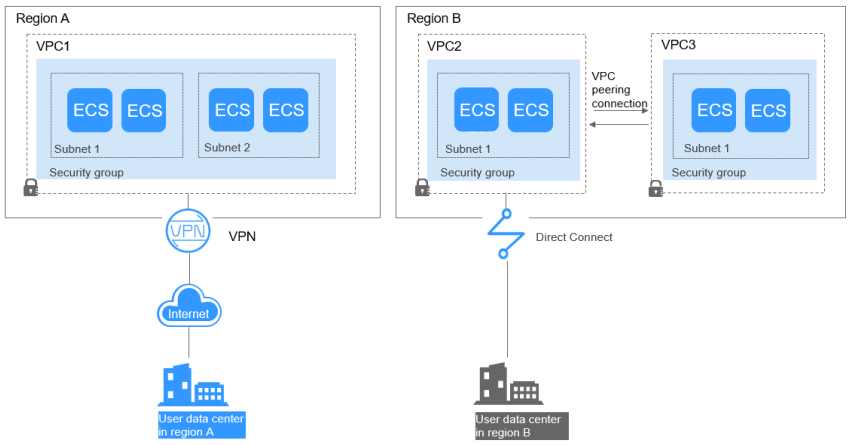
- Se não for necessário controlar explicitamente como cada sub-rede roteia o tráfego de entrada e saída, você poderá usar a tabela de rotas padrão.
- Se você precisar controlar explicitamente como cada sub-rede roteia o tráfego de entrada e saída em uma VPC, adicione rotas personalizadas à tabela de rotas.

Como se conectar a um data center local?

Se você precisar de interconexão entre uma VPC e um data center local, certifique-se de que a VPC não tenha um intervalo de endereços IP sobreposto com o data center local a ser conectado.

Como mostrado em **Figura 1-2**, você tem a VPC 1 na região A e a VPC 2 e a VPC 3 na região B. Para se conectar a um data center local, eles podem usar uma VPN, como a VPC 1 faz na Região A; ou uma conexão Direct Connect, como a VPC 2 faz na Região B. A VPC 2 se conecta ao data center por meio de uma conexão Direct Connect, mas para se conectar a outra VPC nessa região, como a VPC 3, uma conexão de emparelhamento da VPC deve ser estabelecida.

Figura 1-2 Conexões com data centers locais



Ao planejar blocos CIDR para VPC 1, VPC 2 e VPC 3.

- O bloco CIDR da VPC 1 não pode se sobrepor ao bloco CIDR do data center local na Região A.
- O bloco CIDR da VPC 2 não pode se sobrepor ao bloco CIDR do data center local na Região B.
- Os blocos CIDR da VPC 2 e da VPC 3 não podem se sobrepor.

Como acessar a Internet?

Use EIPs para permitir que um pequeno número de ECSs acesse a Internet.

Quando apenas alguns ECSs precisarem acessar a Internet, você poderá vincular os EIPs aos ECSs. Isso irá fornecer-lhes acesso à Internet. Você também pode desvincular dinamicamente os EIPs dos ECSs e vinculá-los a gateways da NAT e balanceadores de carga, que também fornecerão acesso à Internet. O processo não é complicado.

Para obter mais informações sobre o EIP, consulte **Visão geral do EIP** .

Use um gateway da NAT para permitir que um grande número de ECSs acesse a Internet.

Quando um grande número de ECSs precisa acessar a Internet, a nuvem pública fornece gateways da NAT para seus ECSs. Com os gateways da NAT, você não precisa atribuir um EIP a cada ECS. Os gateways da NAT reduzem os custos, pois você não precisa de tantos EIPs. Os gateways da NAT oferecem tradução de endereço de rede de origem (SNAT) e tradução de endereço de rede de destino (DNAT). SNAT permite que vários ECSs na mesma VPC compartilhem um ou mais EIPs para acessar a Internet. SNAT impede que os EIPs dos ECSs sejam expostos à Internet. DNAT pode implementar o encaminhamento de dados em nível de porta. Ele mapeia portas EIP para portas ECS para que os ECSs em uma VPC possam compartilhar o mesmo EIP e largura de banda para fornecer serviços acessíveis pela Internet.

Para obter mais informações, consulte **Guia de usuário do Gateway NAT** .

Use o ELB para acessar a Internet se houver um grande número de solicitações simultâneas.

Em cenários de alta concorrência, como o comércio eletrônico, você pode usar balanceadores de carga fornecidos pelo serviço ELB para distribuir uniformemente o tráfego de entrada entre vários ECSs, permitindo que um grande número de usuários acesse simultaneamente seu sistema ou aplicativo de negócios. O ELB é implementado no modo de cluster. Ele fornece tolerância a falhas para seus aplicativos equilibrando automaticamente o tráfego em várias AZs. Você também pode aproveitar a integração profunda com o Auto Scaling (AS), que permite o dimensionamento automático com base no tráfego de serviço e garante a estabilidade e a confiabilidade do serviço.

Para obter mais informações, consulte **Guide de usuário do Elastic Load Balance** .

Links úteis

- **Cenários de aplicação**
- **Acesso à rede privada**
- **Acesso à rede pública**

1.2 VPC

1.2.1 Criação de uma VPC

Cenários

Uma VPC fornece uma rede virtual isolada para ECSs. Você pode configurar e gerenciar a rede conforme necessário.

Você pode criar uma VPC seguindo o procedimento fornecido nesta seção. Em seguida, crie sub-redes, grupos de segurança e atribua EIPs seguindo o procedimento fornecido nas seções subsequentes com base nos requisitos de rede reais.

Procedimento

1. Acesse o console de gerenciamento.
2. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
3. Clique em **Create VPC**.

   A página **Create VPC** é exibida.
4. Na página **Create VPC**, defina os parâmetros conforme solicitado.

   Uma sub-rede padrão será criada junto com uma VPC e você também poderá clicar em **Add Subnet** para criar mais sub-redes para a VPC.

Figura 1-3 Criar uma VPC e uma sub-rede

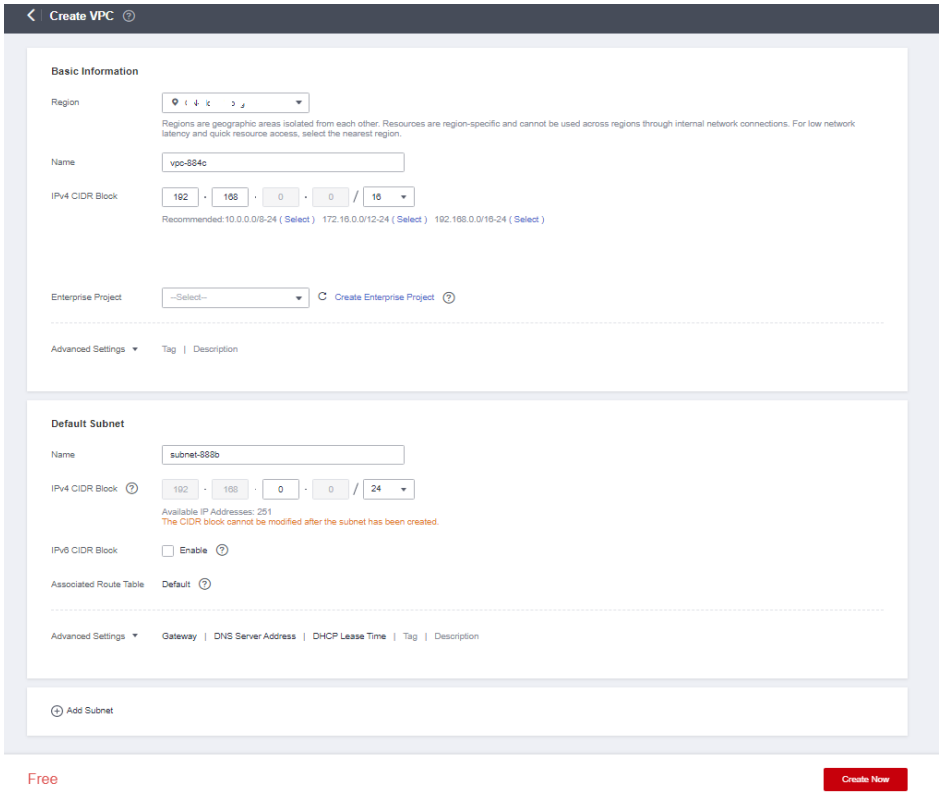


Tabela 1-1 Descrições de parâmetros da VPC

Parâmetro	Descrição	Exemplo de valor
Região	Regiões são áreas geográficas fisicamente isoladas umas das outras. As redes dentro de diferentes regiões não estão conectadas entre si, portanto, os recursos não podem ser compartilhados entre diferentes regiões. Para menor latência de rede e acesso mais rápido aos seus recursos, selecione a região mais próxima de você.	CN-Hong Kong
Name	O nome da VPC. O nome pode conter no máximo 64 caracteres, que podem consistir em letras, dígitos, sublinhados (_), hifens (-) e pontos (.). O nome não pode conter espaços.	VPC-test
CIDR Block or IPv4 CIDR Block	O bloco CIDR da VPC. O bloco CIDR de uma sub-rede pode ser o mesmo que o bloco CIDR para a VPC (para uma única sub-rede na VPC) ou um subconjunto do bloco CIDR para a VPC (para várias sub-redes na VPC). Os seguintes blocos CIDR são suportados: ● 10.0.0.0/8-24 ● 172.16.0.0/12-24 ● 192.168.0.0/16-24 Este parâmetro será **CIDR Block** em regiões onde a pilha dual IPv4/IPv6 não é suportada, e **IPv4 CIDR Block** se a pilha dual IPv4/IPv6 é suportada.	192.168.0.0/16

Parâmetro	Descrição	Exemplo de valor
Projeto empresarial	O projeto empresarial ao qual a VPC pertence. Um projeto empresarial facilita o gerenciamento de projeto e o agrupamento de recursos da nuvem e de usuários. O nome do projeto padrão é **default**. Para obter detalhes sobre como criar e gerenciar projetos empresariais, consulte o **Guia de usuário do Enterprise Management**.	Padrão
Tag	A tag da VPC, que consiste em um par de chave e valor. Você pode adicionar no máximo 10 tags a cada VPC. Chave e valor de tags devem atender aos requisitos listados em **Tabela 1-3**.	● Chave: vpc_key1 ● Valor: vpc-01
Description	Informação complementar sobre a VPC. Este parâmetro é opcional. A descrição da VPC pode conter no máximo 255 caracteres e não pode conter colchetes angulares (< ou >).	N/A

Tabela 1-2 Descrições de parâmetros de sub-rede

Parâmetro	Descrição	Exemplo de valor
Name	O nome da sub-rede. O nome pode conter no máximo 64 caracteres, que podem consistir em letras, dígitos, sublinhados (_), hifens (-) e pontos (.). O nome não pode conter espaços.	subnet-01
CIDR Block	O bloco CIDR para a sub-rede. Esse valor deve estar dentro do bloco CIDR da VPC. Este parâmetro é exibido apenas em regiões onde a pilha dupla IPv4/IPv6 não é suportada.	192.168.0.0/24

Parâmetro	Descrição	Exemplo de valor
IPv4 CIDR Block	O bloco CIDR para a sub-rede. Esse valor deve estar dentro do bloco CIDR da VPC. Este parâmetro é exibido apenas em regiões onde a pilha dupla IPv4/IPv6 é suportada.	192.168.0.0/24
IPv6 CIDR Block	Especifica se o **IPv6 CIDR Block** deve ser definido como **Enable**. Depois que a função IPv6 é ativada, o sistema atribui automaticamente um bloco CIDR IPv6 à sub-rede criada. Atualmente, o bloco CIDR IPv6 não pode ser personalizado. O IPv6 não pode ser desativado após a criação da sub-rede. Este parâmetro é exibido apenas em regiões onde a pilha dupla IPv4/IPv6 é suportada.	-
Associated Route Table	A tabela de rotas padrão à qual a sub-rede será vinculada. Você pode alterar a tabela de rotas para uma tabela de rotas personalizada na página de **Subnets**.	Padrão
Advanced Settings	Clique na seta suspensa para definir configurações avançadas para a sub-rede, incluindo **Gateway** e **DNS Server Address**.	Padrão
Gateway	O endereço de gateway da sub-rede. Esse endereço IP é usado para se comunicar com outras sub-redes.	192.168.0.1

Parâmetro	Descrição	Exemplo de valor
DNS Server Address	Os endereços de servidor DNS privado da Huawei Cloud são inseridos por padrão. Isso permite que os ECSs em uma VPC se comuniquem entre si e também acessem outros serviços em nuvem usando nomes de domínio privados sem expor seus endereços IP à Internet. Você pode alterar os endereços de servidor DNS padrão, se necessário. Isso pode interromper seu acesso aos serviços de nuvem. Você também pode clicar em **Reset** à direita para restaurar os endereços do servidor DNS para o valor padrão. Um máximo de dois endereços IP de servidor DNS podem ser configurados. Vários endereços IP devem ser separados usando vírgulas (,).	100.125.x.x
DHCP Lease Time	O período durante o qual um cliente pode usar um endereço IP atribuído automaticamente pelo servidor DHCP. Depois que o tempo de concessão expirar, um novo endereço IP será atribuído ao cliente. ● Limitado: defina o tempo de concessão de DHCP. A unidade pode ser dia ou hora. ● Ilimitado: o tempo de concessão de DHCP não expira. Se um tempo de concessão de DHCP for alterado, a nova concessão entrará em vigor automaticamente quando metade do tempo de concessão atual tiver passado. Para que a alteração entre em vigor imediatamente, reinicie o ECS ou efetue logon no ECS para fazer com que a concessão de DHCP seja renovada automaticamente.	365 dias

Parâmetro	Descrição	Exemplo de valor
NTP Server Address	O endereço IP do servidor NTP. Este parâmetro é opcional. Você pode configurar os endereços IP do servidor NTP a serem adicionados à sub-rede conforme necessário. Os endereços IP são adicionados além dos endereços do servidor NTP padrão. Se este parâmetro é deixado vazio, nenhum endereço IP do servidor NTP está adicionado. Insira um máximo de quatro endereços IP válidos e separe vários endereços IP com vírgulas. Cada endereço IP deve ser único. Se você adicionar ou alterar os endereços de servidor NTP de uma sub-rede, será necessário renovar a concessão de DHCP ou reiniciar todos os ECSs na sub-rede para que a alteração entre em vigor imediatamente. Se os endereços do servidor NTP tiverem sido apagados, reiniciar os ECSs não ajudará. Você deve renovar a concessão DHCP para todos os ECSs para que a alteração entre em vigor imediatamente.	192.168.2.1
Tag	A tag de sub-rede, que consiste em um par de chave e valor. Você pode adicionar um máximo de 10 tags a cada sub-rede. Chave e valor de tags devem atender aos requisitos listados em **Tabela 1-4**.	● Chave: subnet_key1 ● Valor: subnet-01
Description	Informação complementar sobre a sub-rede. Este parâmetro é opcional. A descrição da sub-rede pode conter no máximo 255 caracteres e não pode conter colchetes angulares (< ou >).	N/A

Tabela 1-3 Requisitos de chave e valor da tag da VPC

Parâmetro	Requisitos	Exemplo de valor
Key	● Não pode ser deixada em branco. ● Deve ser exclusiva para a mesma VPC e pode ser o mesmo para diferentes VPCs. ● Pode conter no máximo 36 caracteres. ● Pode conter letras, dígitos, sublinhados (_) e hifens (-).	vpc_key1
Value	● Pode conter no máximo 43 caracteres. ● Pode conter letras, dígitos, sublinhados (_) pontos (.) e hifens (-).	vpc-01

Tabela 1-4 Requisitos de chave e valor da tag de sub-rede

Parâmetro	Requisitos	Exemplo de valor
Key	● Não pode ser deixada em branco. ● Deve ser exclusiva para cada sub-rede. ● Pode conter no máximo 36 caracteres. ● Pode conter letras, dígitos, sublinhados (_) e hifens (-).	subnet_key1
Value	● Pode conter no máximo 43 caracteres. ● Pode conter letras, dígitos, sublinhados (_) pontos (.) e hifens (-).	subnet-01

5. Confirme a configuração atual e clique em **Create Now**.

1.2.2 Modificação de uma VPC

Cenários

Alterar o nome da VPC e o bloco CIDR.

Se o bloco CIDR da VPC entrar em conflito com o bloco CIDR de uma VPN criada na VPC, você poderá modificar seu bloco CIDR.

Observações e restrições

- Se a adição de um bloco CIDR IPv4 secundário a uma VPC for aceita, você não poderá modificar o bloco CIDR de uma VPC existente no console. No entanto, você pode usar APIs para modificar o bloco CIDR de uma VPC existente. Para obter detalhes, consulte a **Referência de API da Virtual Private Cloud**.

  Atualmente, os blocos CIDR IPv4 secundários para VPCs estão disponíveis apenas em **AP-Singapore** e **CN North-Beijing4**. Para obter detalhes, consulte **Adição de um bloco CIDR secundário a uma VPC**.

> **NOTA**
>
> Se uma VPC tiver uma sub-rede em seu bloco CIDR secundário, o bloco CIDR secundário não poderá ser modificado no console ou usando APIs.

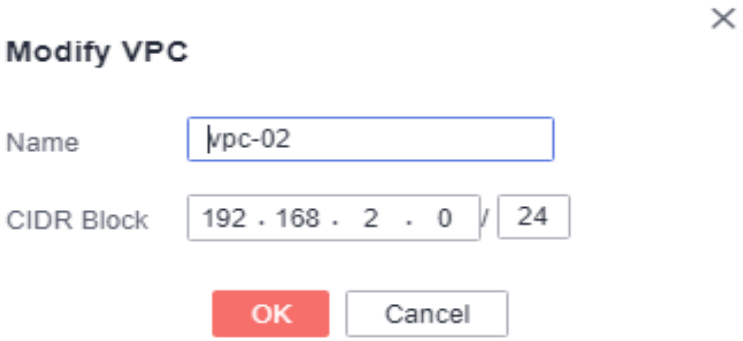
- Ao modificar o bloco CIDR da VPC:
  - O bloco CIDR da VPC a ser modificado deve estar nos blocos CIDR suportados: 10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255 e 192.168.0.0 – 192.168.255.255
  - Se a VPC tiver sub-redes, o bloco CIDR da VPC a ser modificado deverá conter todos os blocos CIDR da sub-rede.

Procedimento

1. Acesse o console de gerenciamento.
2. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
3. Na página **Virtual Private Cloud**, localize a linha que contém a VPC a ser modificada e clique em **Modify** ou **Edit CIDR Block** na coluna **Operation**.
4. Na página exibida, modifique os parâmetros conforme solicitado. **Figura 1-4** mostra a captura de tela.

   Figura 1-4 Modificar VPC

5. Clique em **OK**.

1.2.3 Adição de um bloco CIDR secundário a uma VPC

Cenários

Ao criar uma VPC, você deve especificar um bloco CIDR para a VPC. Esse é o bloco CIDR primário da VPC e não pode ser modificado após a criação da VPC.

Para estender o intervalo de endereços IP da VPC, você pode adicionar um bloco CIDR secundário.

Se você precisar criar uma sub-rede na VPC, selecione o bloco CIDR primário ou secundário. Semelhante ao bloco CIDR primário, se você criar uma sub-rede no bloco CIDR secundário, uma rota será adicionada automaticamente à tabela de rotas da VPC para habilitar o roteamento na VPC.

NOTA

- Os blocos CIDR secundários estão agora disponíveis apenas nas regiões CN-Hong Kong, AP-Bangkok, AP-Singapore, AF-Johannesburg, LA-Mexico City1, LA-Mexico City2, LA-Sao Paulo1 e LA-Santiago.
- Se for possível adicionar um bloco CIDR IPv4 secundário a uma VPC, você só poderá usar APIs para modificar o bloco CIDR de uma VPC existente. Para obter detalhes, consulte a **Referência de API da Virtual Private Cloud**.

Pré-requisitos

Uma VPC foi criada.

Observações e restrições

- Por padrão, cada VPC só pode ter um bloco CIDR IPv4 secundário associado.
- Se uma sub-rede em um bloco CIDR secundário da VPC for igual ou se sobrepuser ao destino de uma rota existente na tabela de rotas da VPC, a rota existente não entrará em vigor.

  Se você criar uma sub-rede em um bloco CIDR secundário da VPC, uma rota (o destino é o bloco CIDR da sub-rede e o próximo salto é **Local**) é adicionado automaticamente à tabela de rotas da VPC. Essa rota permite comunicações dentro da VPC e tem uma prioridade mais alta do que qualquer outra rota na tabela de rotas da VPC. Por exemplo, se uma tabela de rotas da VPC tiver uma rota com a conexão de emparelhamento de VPC como o próximo salto e 100.20.0.0/24 como o destino, e uma rota para a sub-rede no bloco CIDR secundário tiver um destino de 100.20.0.0/16, 100.20.0.0/16 e 100.20.0.0/24 sobrepõem-se e o tráfego será encaminhado através da rota da sub-rede.
- **Tabela 1-5** lista os blocos CIDR secundários que não são suportados.

Tabela 1-5 Blocos CIDR secundários restritos

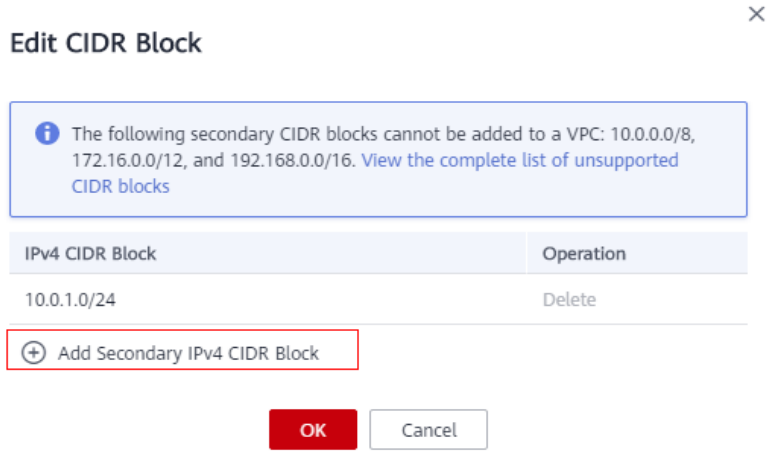
Tipo	Bloco CIDR (não suportado)
Blocos CIDR primários e blocos CIDR existentes	● 10.0.0.0/8 ● 172.16.0.0/12 ● 192.168.0.0/16
Blocos CIDR do sistema reservado	● 100.64.0.0/10 ● 214.0.0.0/7 ● 198.18.0.0/15 ● 169.254.0.0/16
Blocos CIDR públicos reservados	● 0.0.0.0/8 ● 127.0.0.0/8 ● 240.0.0.0/4 ● 255.255.255.255/32

Procedimento

1. Acesse o console de gerenciamento.
2. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
3. Na página **Virtual Private Cloud**, localize a linha que contém a VPC a ser modificada e clique em **Modify** ou **Edit CIDR Block** na coluna **Operation**.
4. Clique em **Add Secondary IPv4 CIDR Block**.

   Figura 1-5 Adicionar bloco CIDR IPv4 secundário



5. Digite o bloco CIDR secundário e clique em **OK**.

1.2.4 Remoção de um bloco CIDR secundário de uma VPC

Cenários

Você pode remover um bloco CIDR secundário de uma VPC se não precisar mais dele.

Não é possível remover o bloco CIDR IPv4 primário.

NOTA

- Os blocos CIDR secundários estão agora disponíveis apenas nas regiões CN-Hong Kong, AP-Bangkok, AP-Singapore, AF-Johannesburg, LA-Mexico City1, LA-Mexico City2, LA-Sao Paulo1 e LA-Santiago.
- Se for possível adicionar um bloco CIDR IPv4 secundário a uma VPC, você só poderá usar APIs para modificar o bloco CIDR de uma VPC existente. Para obter detalhes, consulte a **Referência de API da Virtual Private Cloud**.

Pré-requisitos

Todas as sub-redes no bloco CIDR secundário foram excluídas.

Procedimento

1. Acesse o console de gerenciamento.
2. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.

A página **Virtual Private Cloud** é exibida.

3. Na lista VPC, localize a linha que contém a VPC da qual você deseja excluir um bloco CIDR secundário e clique em **Edit CIDR Block** na coluna **Operation**.
4. Localize a linha que contém o bloco CIDR secundário a ser excluído e clique em **Delete** na coluna **Operation**.

1.2.5 Exclusão de uma VPC

Cenários

Esta seção descreve como excluir uma VPC.

AVISO

As VPCs são gratuitas.

Observações e restrições

Se você quiser excluir uma VPC que tenha sub-redes, rotas personalizadas ou outros recursos, primeiro será necessário excluir esses recursos conforme solicitado no console e, em seguida, excluir a VPC.

Você pode consultar **Por que não posso excluir minhas VPCs e sub-redes?**

Procedimento

1. Acesse o console de gerenciamento.
2. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
3. Na página **Virtual Private Cloud**, localize a linha que contém a VPC a ser excluída e clique em **Delete** na coluna **Operation**.

   Uma caixa de diálogo de confirmação é exibida.
4. Confirme as informações e clique em **Yes**.

AVISO

Se uma VPC não puder ser excluída, uma mensagem será exibida no console. Exclua os recursos que estão na VPC consultando **Por que não posso excluir minhas VPCs e sub-redes?**

1.2.6 Gerenciamento de tags da VPC

Cenários

Uma tag da VPC identifica uma VPC. As tags podem ser adicionadas às VPCs para facilitar a identificação e o gerenciamento da VPC. Você pode adicionar uma tag a uma VPC ao criar a

VPC ou pode adicionar uma tag a uma VPC criada na página de detalhes da VPC. Um máximo de 10 tags podem ser adicionadas a cada VPC.

Uma tag consiste em um par de chave e valor. **Tabela 1-6** lista os requisitos de chave e valor da tag.

Tabela 1-6 Requisitos de chave e valor da tag da VPC

Parâmetro	Requisitos	Exemplo de valor
Key	● Não pode ser deixada em branco. ● Deve ser exclusiva para a mesma VPC e pode ser o mesmo para diferentes VPCs. ● Pode conter no máximo 36 caracteres. ● Pode conter letras, dígitos, sublinhados (_) e hifens (-).	vpc_key1
Value	● Pode conter no máximo 43 caracteres. ● Pode conter letras, dígitos, sublinhados (_) pontos (.) e hifens (-).	vpc-01

Procedimento

Pesquisar VPCs por chave e valor de tag na página que mostra a lista de VPCs

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, clique em **Virtual Private Cloud**.
5. No canto superior direito da lista da VPC, clique em **Search by Tag**.
6. Na área exibida, digite a chave da tag e o valor da VPC que você está procurando.

   A chave e o valor da tag devem ser especificados. O sistema exibe automaticamente as VPCs que você está procurando se a chave e o valor da tag corresponderem.
7. Clique em + para adicionar mais chaves e valores de tag.

   Você pode adicionar várias chaves e valores de tags para refinar os resultados da pesquisa. Se você adicionar mais de uma tag para pesquisar VPCs, as VPCs contendo todas as tags especificadas serão exibidas.
8. Clique em **Search**.

   O sistema exibe as VPCs que você está procurando com base nas chaves e valores de tags inseridos.

Adicionar, excluir, editar e visualizar tags na guia Tags de uma VPC.

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.

3. Na página inicial do console, na **Networking**, clique em

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, **Virtual Private Cloud**.
5. Na página **Virtual Private Cloud**, localize a VPC cujas tags serão gerenciadas e clique no nome da VPC.

   A página que mostra detalhes sobre a VPC específica é exibida.
6. Clique na guia **Tags** e execute as operações desejadas nas tags.
   - Exibir as tags.

     Na guia **Tags**, você pode exibir detalhes sobre as tags adicionadas à VPC atual, incluindo o número de tags e a chave e o valor de cada tag.
   - Adicionar uma tag.

     Clique em **Add Tag** no canto superior esquerdo. Na caixa de diálogo **Add Tag** exibida, insira a chave e o valor da tag e clique em **OK**.
   - Editar uma tag.

     Localize a linha que contém a tag que deseja editar e clique em **Edit** na coluna **Operation**. Na caixa de diálogo **Edit Tag**, altere o valor da tag e clique em **OK**.
   - Excluir uma tag.

     Localize a linha que contém a tag que deseja excluir e clique em **Delete** na coluna **Operation**. Na caixa de diálogo exibida, clique em **Yes**.

1.2.7 Exportação da lista de VPC

Cenários

As informações sobre todas as VPCs na sua conta podem ser exportadas como um arquivo do Excel para um diretório local. Esse arquivo registra os nomes, ID, status, intervalos de endereços IP de VPCs e o número de sub-redes.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, clique em **Virtual Private Cloud**.
5. No canto superior direito da lista de VPC, clique em .

   O sistema exportará automaticamente informações sobre todas as VPCs da sua conta na região atual. Eles serão exportados em formato Excel.

1.2.8 Exibição de uma topologia de VPC

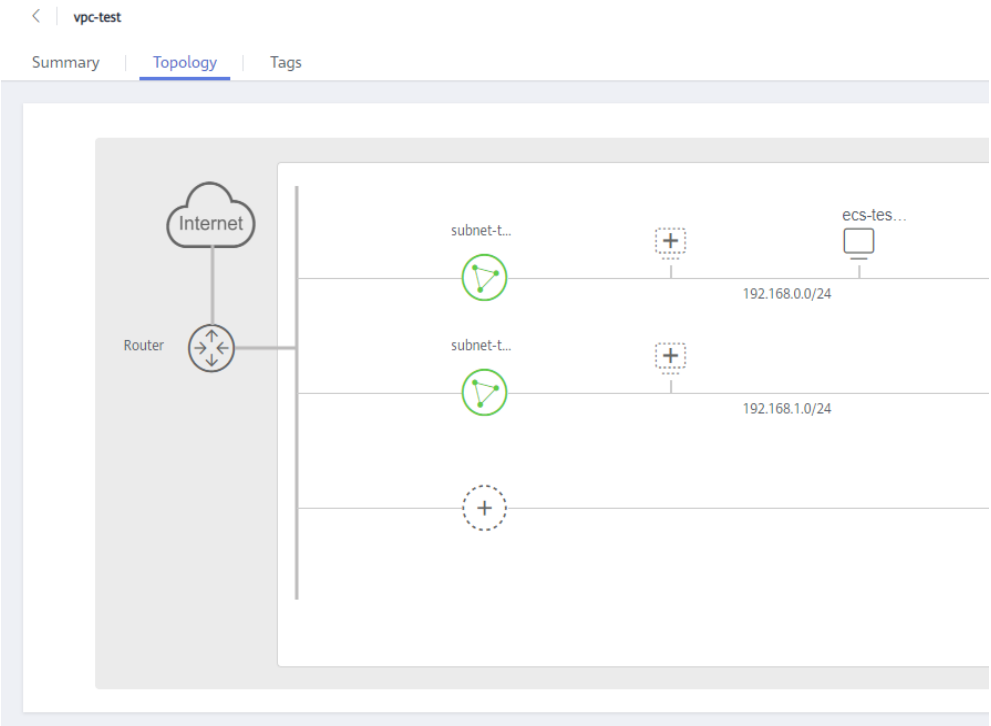
Cenários

Esta seção descreve como exibir a topologia de uma VPC. A topologia exibe as sub-redes em uma VPC e os ECSs nas sub-redes.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.
   A página **Virtual Private Cloud** é exibida.
4. Na lista da VPC, clique no nome da VPC para a qual a topologia será exibida.
   A página de detalhes da VPC é exibida.
5. Clique na guia **Topology** para exibir a topologia da VPC.
   A topologia exibe as sub-redes na VPC e os ECSs nas sub-redes.
   Você também pode executar as seguintes operações em sub-redes e ECSs na topologia:
   - Modifique ou exclua uma sub-rede.
   - Adicione um ECS a uma sub-rede, vincule um EIP ao ECS e altere o grupo de segurança do ECS.

Figura 1-6 Topologia da VPC



1.3 Sub-rede

1.3.1 Criação de uma sub-rede para a VPC

Cenários

Uma VPC vem com uma sub-rede padrão. Se a sub-rede padrão não puder atender aos seus requisitos, você poderá criar uma.

Uma sub-rede é configurada com DHCP por padrão. Quando um ECS nessa sub-rede é iniciado, o ECS obtém automaticamente um endereço IP usando DHCP.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Subnets**.
5. Clique em **Create Subnet**.

   A página **Create Subnet** é exibida.
6. Defina os parâmetros conforme solicitados.

Tabela 1-7 Descrições de parâmetro

Parâmetro	Descrição	Exemplo de valor
VPC	A VPC para a qual você deseja criar uma sub-rede. Esse parâmetro está disponível somente quando **Subnets** é exibido no painel de navegação.	-
Name	O nome da sub-rede. O nome pode conter no máximo 64 caracteres, que podem consistir em letras, dígitos, sublinhados (_), hifens (-) e pontos (.). O nome não pode conter espaços.	Subnet
CIDR Block	O bloco CIDR para a sub-rede. Esse valor deve estar dentro do bloco CIDR da VPC. Este parâmetro é exibido apenas em regiões onde a pilha dupla IPv4/IPv6 não é suportada.	192.168.0.0/24
IPv4 CIDR Block	O bloco CIDR para a sub-rede. Esse valor deve estar dentro do bloco CIDR da VPC. Este parâmetro é exibido apenas em regiões onde a pilha dupla IPv4/IPv6 é suportada.	192.168.0.0/24

Parâmetro	Descrição	Exemplo de valor
IPv6 CIDR Block	Especifica se deve definir **IPv6 CIDR Block** como **Enable**. Este parâmetro é exibido apenas em regiões onde a pilha dupla IPv4/IPv6 é suportada. Se você selecionar essa opção, o sistema atribuirá automaticamente um bloco CIDR IPv6 à sub-rede criada. Atualmente, o bloco CIDR IPv6 não pode ser personalizado. O IPv6 não pode ser desativado após a criação da sub-rede.	-
Associated Route Table	A tabela de rotas predefinida à qual a sub-rede será vinculada. Você pode alterar a tabela de rotas para uma tabela de rotas personalizada na página **Subnets**.	Padrão
Advanced Settings/ Gateway	O endereço de gateway da sub-rede. Esse endereço IP é usado para se comunicar com outras sub-redes.	192.168.0.1
Advanced Settings/DNS Server Address	Os endereços de servidor DNS privado da Huawei Cloud são inseridos por padrão. Isso permite que os ECSs em uma VPC se comuniquem entre si e também acessem outros serviços em nuvem usando nomes de domínio privados sem expor seus endereços IP à Internet. Você pode alterar os endereços de servidor DNS padrão, se necessário. Isso pode interromper seu acesso aos serviços de nuvem. Você também pode clicar em **Reset** à direita para restaurar os endereços do servidor DNS para o valor padrão. Um máximo de dois endereços IP de servidor DNS podem ser configurados. Vários endereços IP devem ser separados usando vírgulas (,).	100.125.x.x

Parâmetro	Descrição	Exemplo de valor
Advanced Settings/NTP Server Address	O endereço IP do servidor NTP. Este parâmetro é opcional. Você pode configurar os endereços IP do servidor NTP a serem adicionados à sub-rede conforme necessário. Os endereços IP são adicionados além dos endereços do servidor NTP padrão. Se este parâmetro é deixado vazio, nenhum endereço IP do servidor NTP está adicionado. Insira um máximo de quatro endereços IP válidos e separe vários endereços IP com vírgulas. Cada endereço IP deve ser único. Se você adicionar ou alterar os endereços de servidor NTP de uma sub-rede, será necessário renovar a concessão de DHCP ou reiniciar todos os ECSs na sub-rede para que a alteração entre em vigor imediatamente. Se os endereços do servidor NTP tiverem sido apagados, reiniciar os ECSs não ajudará. Você deve renovar a concessão DHCP para todos os ECSs para que a alteração entre em vigor imediatamente.	192.168.2.1
Advanced Settings/ DHCP Lease Time	O período durante o qual um cliente pode usar um endereço IP atribuído automaticamente pelo servidor DHCP. Depois que o tempo de concessão expirar, um novo endereço IP será atribuído ao cliente. ● Limitado: defina o tempo de concessão de DHCP. A unidade pode ser dia ou hora. ● Ilimitado: o tempo de concessão de DHCP não expira. Se um tempo de concessão de DHCP for alterado, a nova concessão entrará em vigor automaticamente quando metade do tempo de concessão atual tiver passado. Para que a alteração entre em vigor imediatamente, reinicie o ECS ou efetue logon no ECS para fazer com que a concessão de DHCP seja renovada automaticamente.	365 dias
Advanced Settings/ Description	Informação complementar sobre a sub-rede. Este parâmetro é opcional. A descrição da sub-rede pode conter no máximo 255 caracteres e não pode conter colchetes angulares (< e >).	-

7. Clique em **OK**.

Precauções

Quando uma sub-rede é criada, há cinco endereços IP reservados, que não podem ser usados. Por exemplo, em uma sub-rede com bloco CIDR 192.168.0.0/24, os seguintes endereços IP são reservados:

- 192.168.0.0: ID da rede. Esse endereço é o início do intervalo de endereços IP privados e não será atribuído a nenhuma instância.
- 192.168.0.1: endereço de gateway.
- 192.168.0.253: reservado para a interface do sistema. Esse endereço IP é usado pela VPC para comunicação externa.
- 192.168.0.254: endereço de serviço DHCP.
- 192.168.0.255: endereço de transmissão de rede.

Se você configurou as configurações padrão em **Advanced Settings** durante a criação da sub-rede, os endereços IP reservados podem ser diferentes dos padrões, mas ainda haverá cinco deles. Os endereços específicos dependem das configurações da sub-rede.

1.3.2 Modificação de uma sub-rede

Cenários

Modifique o nome da sub-rede, o endereço do servidor NTP e o endereço do servidor DNS.

Observações e restrições

Depois que uma sub-rede é criada, sua AZ não pode ser alterada.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.
   A página **Virtual Private Cloud** é exibida.
4. Localize a linha que contém a VPC de destino e clique no número na coluna **Subnets**.
   A página **Subnets** é exibida.
5. Na lista de sub-redes, localize a sub-rede de destino e clique em seu nome.
   A página de detalhes da sub-rede é exibida.
6. Na guia **Summary**, clique em  à direita do parâmetro a ser modificado e modifique o parâmetro conforme solicitado.

Tabela 1-8 Descrições de parâmetro

Parâmetro	Descrição	Exemplo de valor
Name	O nome da sub-rede. O nome pode conter no máximo 64 caracteres, que podem consistir em letras, dígitos, sublinhados (_), hifens (-) e pontos (.). O nome não pode conter espaços.	Subnet
DNS Server Address	Os endereços de servidor DNS privado da Huawei Cloud são inseridos por padrão. Isso permite que os ECSs em uma VPC se comuniquem entre si e também acessem outros serviços em nuvem usando nomes de domínio privados sem expor seus endereços IP à Internet. Você pode alterar os endereços de servidor DNS padrão, se necessário. Isso pode interromper seu acesso aos serviços de nuvem. Você também pode clicar em **Reset** à direita para restaurar os endereços do servidor DNS para o valor padrão. Um máximo de dois endereços IP de servidor DNS podem ser configurados. Vários endereços IP devem ser separados usando vírgulas (,).	100.125.x.x

Parâmetro	Descrição	Exemplo de valor
DHCP Lease Time	O período durante o qual um cliente pode usar um endereço IP atribuído automaticamente pelo servidor DHCP. Depois que o tempo de concessão expirar, um novo endereço IP será atribuído ao cliente. ● Limitado: defina o tempo de concessão de DHCP. A unidade pode ser dia ou hora. ● Ilimitado: o tempo de concessão de DHCP não expira. Se um tempo de concessão de DHCP for alterado, a nova concessão entrará em vigor automaticamente quando metade do tempo de concessão atual tiver passado. Para que a alteração entre em vigor imediatamente, reinicie o ECS ou efetue logon no ECS para fazer com que a concessão de DHCP seja renovada automaticamente.	365 days

Parâmetro	Descrição	Exemplo de valor
NTP Server Address	O endereço IP do servidor NTP. Este parâmetro é opcional. Você pode configurar os endereços IP do servidor NTP a serem adicionados à sub-rede conforme necessário. Os endereços IP são adicionados além dos endereços do servidor NTP padrão. Se este parâmetro é deixado vazio, nenhum endereço IP do servidor NTP está adicionado. Insira um máximo de quatro endereços IP válidos e separe vários endereços IP com vírgulas. Cada endereço IP deve ser único. Se você adicionar ou alterar os endereços de servidor NTP de uma sub-rede, será necessário renovar a concessão de DHCP ou reiniciar todos os ECSs na sub-rede para que a alteração entre em vigor imediatamente. Se os endereços do servidor NTP tiverem sido apagados, reiniciar os ECSs não ajudará. Você deve renovar a concessão DHCP para todos os ECSs para que a alteração entre em vigor imediatamente.	192.168.2.1
Description	Informação complementar sobre a sub-rede. Este parâmetro é opcional. A descrição pode conter no máximo 255 caracteres e não pode conter colchetes angulares (< e >).	-

7. Clique em **OK**.

1.3.3 Gerenciamento de tags de sub-rede

Cenários

Uma tag de sub-rede identifica uma sub-rede. As tags podem ser adicionadas às sub-redes para facilitar a identificação e a administração da sub-rede. Você pode adicionar uma tag a uma sub-rede ao criar a sub-rede ou pode adicionar uma tag a uma sub-rede criada na página de detalhes da sub-rede. Um máximo de 10 tags podem ser adicionadas a cada sub-rede.

Uma tag consiste em um par de chave e valor. **Tabela 1-9** lista os requisitos de chave e valor da tag.

Tabela 1-9 Requisitos de chave e valor da tag de sub-rede

Parâmetro	Requisitos	Exemplo de valor
Key	● Não pode ser deixada em branco. ● Deve ser exclusiva para cada sub-rede. ● Pode conter no máximo 36 caracteres. ● Pode conter letras, dígitos, sublinhados (_) e hifens (-).	subnet_key1
Value	● Pode conter no máximo 43 caracteres. ● Pode conter letras, dígitos, sublinhados (_) pontos (.) e hifens (-).	subnet-01

Procedimento

Pesquisar sub-redes por chave e valor de tag na página que mostra a lista de sub-redes.

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na **Networking**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. Localize a linha que contém a VPC de destino e clique no número na coluna **Subnets**.

   A página **Subnets** é exibida.
5. No canto superior direito da lista de sub-rede, clique em **Search by Tag**.
6. Insira a chave de tag da sub-rede a ser consultada.

   A chave e o valor da tag devem ser especificados. O sistema exibe automaticamente as sub-redes que você está procurando se a chave e o valor da tag forem correspondidos.
7. Clique em + para adicionar outra chave e valor de tag.

   Você pode adicionar várias chaves e valores de tags para refinar os resultados da pesquisa. Se você adicionar mais de uma tag para procurar sub-redes, as sub-redes que contêm todas as tags especificadas serão exibidas.
8. Clique em **Search**.

   O sistema exibe as sub-redes que você está procurando com base nas chaves e valores de tags inseridos.

Adicionar, excluir, editar e visualizar tags na guia Tags de uma sub-rede.

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na **Networking**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. Localize a linha que contém a VPC de destino e clique no número na coluna **Subnets**.

   A página **Subnets** é exibida.
5. Na lista de sub-redes, localize a sub-rede de destino e clique em seu nome.

6. Na página de detalhes da sub-rede, clique na guia **Tags** e execute as operações desejadas nas tags.
   - Veja as tags.

     Na guia **Tags**, você pode exibir detalhes sobre as tags adicionadas à sub-rede atual, incluindo o número de tags e a chave e o valor de cada tag.
   - Adicionar uma tag.

     Clique em **Add Tag** no canto superior esquerdo. Na caixa de diálogo **Add Tag** exibida, insira a chave e o valor da tag e clique em **OK**.
   - Editar uma tag.

     Localize a linha que contém a tag que deseja editar e clique em **Edit** na coluna **Operation**. Na caixa de diálogo **Edit Tag**, altere o valor da tag e clique em **OK**.
   - Excluir uma tag.

     Localize a linha que contém a tag que deseja excluir e clique em **Delete** na coluna **Operation**. Na caixa de diálogo exibida, clique em **Yes**.

1.3.4 Exportação de lista de sub-redes

Cenários

Informações sobre todas as sub-redes em sua conta podem ser exportadas como um arquivo do Excel para um diretório local. Esse arquivo registra o nome, o ID, a VPC, o bloco CIDR e a tabela de rota associada de cada sub-rede.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Em **Networking**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Subnets**.

   A página **Subnets** é exibida.
5. No canto superior direito da lista de sub-redes, clique em  .

   O sistema exportará automaticamente informações sobre todas as sub-redes sob sua conta na região atual como um arquivo do Excel para um diretório local.

1.3.5 Exibição e exclusão de recursos em uma sub-rede

Cenários

As sub-redes de VPC têm endereços IP privados usados por recursos de nuvem. Esta seção descreve como exibir recursos que estão usando endereços IP privados de sub-redes. Se esses recursos não forem mais necessários, você poderá excluí-los.

Você pode visualizar recursos, incluindo ECSs, BMSs, interfaces de rede, balanceadores de carga e gateways da NAT.

AVISO

Depois de excluir todos os recursos em uma sub-rede consultando esta seção, a mensagem "Excluir o recurso que está usando a sub-rede e, em seguida, excluir a sub-rede." é exibida quando você excluir a sub-rede, você pode consultar **Visualização de endereços IP em uma sub-rede**.

Procedimento

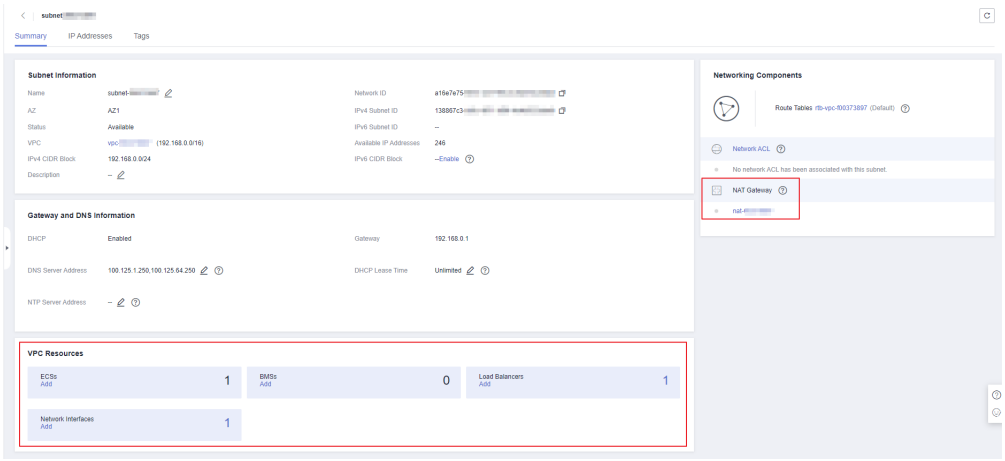
1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Em **Networking**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Subnets**.

   A página **Subnets** é exibida.
5. Localize a sub-rede de destino e clique em seu nome.

   A página de detalhes da sub-rede é exibida.
6. Na página **Summary**, exiba os recursos na sub-rede.
   a. Na área **Resources**, exiba os ECSs, BMSs, interfaces de rede e balanceadores de carga na sub-rede.
   b. Na área **Networking Components**, veja os gateways da NAT na sub-rede.

   Figura 1-7 Visualizar recursos em uma sub-rede



7. Exclua recursos da sub-rede.

Tabela 1-10 Exibir e excluir recursos em uma sub-rede

Recurso	Referência
ECS	Atualmente, não é possível alternar diretamente para ECSs na página de detalhes da sub-rede. Você precisa procurar o ECS de destino na lista do ECS e excluí-lo. 1. Na lista do ECS, clique no nome do ECS. A página de detalhes do ECS é exibida. 2. Na área **NICs**, veja o nome da sub-rede associada ao ECS. 3. Confirme as informações e **exclua o ECS**.
BMS	Atualmente, você não pode alternar diretamente para BMSs na página de detalhes da sub-rede. Você precisa procurar o BMS de destino na lista do BMS e excluí-lo. 1. Na lista do BMS, clique no nome do BMS. A página de detalhes do BMS é exibida. 2. Na guia **NICs**, visualize a sub-rede associada ao BMS. 3. Confirme a informação e **libere o BMS**.
Balanceador de carga	Você pode alternar diretamente para balanceadores de carga na página de detalhes da sub-rede. 1. Clique na quantidade do balanceador de carga na área **Resources**. A lista do balanceador de carga é exibida. 2. Localize a linha que contém o balanceador de carga a ser excluído e clique em **Delete** na coluna **Operation**. Para obter detalhes, consulte **Exclusão de um balanceador de carga**.
Gateway da NAT	Você pode alternar diretamente para gateways da NAT na página de detalhes da sub-rede. 1. Clique no nome do gateway da NAT na área **Networking Components**. A página de detalhes do gateway da NAT é exibida. 2. Clique em  para retornar à lista de gateways da NAT. 3. Localize a linha que contém o gateway da NAT a ser excluído e clique em **Delete** na coluna **Operation**. ● **Exclusão ou cancelamento de assinatura de um gateway da NAT público** ● **Exclusão de um gateway da NAT privado**

1.3.6 Visualização de endereços IP em uma sub-rede

Cenários

Uma sub-rede é um intervalo de endereços IP em uma VPC. Esta seção descreve como exibir os endereços IP usados em uma sub-rede.

- Endereços IP virtuais
- Endereços IP privados
  - Usados pela própria sub-rede, como o gateway, a interface do sistema e DHCP.
  - Usados por recursos de nuvem, como ECSs, balanceadores de carga e instâncias do RDS.

Observações e restrições

- Uma sub-rede não pode ser excluída se seus endereços IP forem usados por recursos de nuvem.
- Uma sub-rede pode ser excluída se seus endereços IP forem usados por ela mesma.

Procedimento

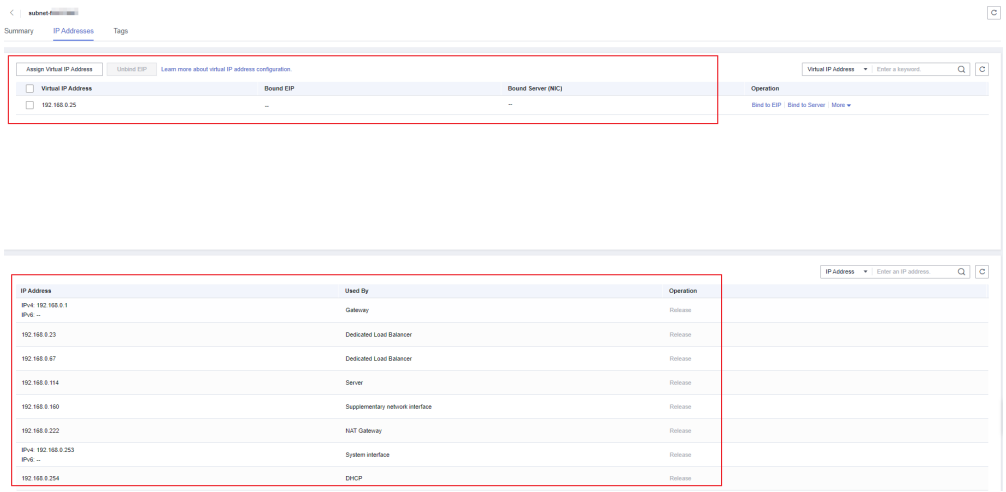
1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Em , clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Subnets**.

   A página **Subnets** é exibida.
5. Localize a sub-rede de destino e clique em seu nome.

   A página de detalhes da sub-rede é exibida.
6. Clique na guia **IP Addresses** para exibir os endereços IP na sub-rede.
   a. Na lista de endereços IP virtuais, você pode exibir os endereços IP virtuais atribuídos a partir da sub-rede.
   b. Na lista de endereços IP privados na parte inferior da página, você pode exibir os endereços IP privados usados pela sub-rede (gateway, interface do sistema e DHCP).

Figura 1-8 Visualizar endereços IP em uma sub-rede



Operações de acompanhamento

Para visualizar e excluir os recursos em uma sub-rede, consulte **Por que não posso excluir minhas VPCs e sub-redes?**

1.3.7 Exclusão de uma sub-rede

Cenários

Esta seção descreve como excluir uma sub-rede.

AVISO

As sub-redes são gratuitas.

Observações e restrições

Se quiser excluir uma sub-rede que tenha rotas personalizadas, endereços IP virtuais ou outros recursos, primeiro será necessário excluir esses recursos conforme solicitado no console e, em seguida, excluir a sub-rede.

Você pode consultar **Por que não posso excluir minhas VPCs e sub-redes?**

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, clique em **Virtual Private Cloud**.
5. Localize a linha que contém a VPC de destino e clique no número na coluna **Subnets**.

   A página **Subnets** é exibida.
6. Na lista de sub-rede, localize a linha que contém a sub-rede que você deseja excluir e clique em **Delete** na coluna **Operation**.

   Uma caixa de diálogo de confirmação é exibida.
7. Clique em **Yes**.

AVISO

Se uma sub-rede não puder ser excluída, uma mensagem será exibida no console. Exclua os recursos que estão na sub-rede consultando **Por que não posso excluir minhas VPCs e sub-redes?**

1.4 IPv4 and IPv6 Dual-Stack Network

What Is an IPv4/IPv6 Dual-Stack Network?

IPv4 and IPv6 dual-stack allows your resources, such as ECSs, to use both IPv4 and IPv6 addresses for private and public network communications. For example, if ECSs uses the IPv4/IPv6 dual-stack network:

- ECSs can communicate with each other using private IPv4 addresses.
- ECSs can communicate with the Internet after they are bound with EIPs.
- ECSs can communicate with each other using IPv6 addresses.
- ECSs can communicate with the Internet after their IPv6 addresses are associated with bandwidths.

NOTA

If you select **Enable** for **IPv6 CIDR Block** when creating a subnet, an IPv6 CIDR block will be automatically assigned to the subnet.

Basic operations on IPv4 and IPv6 dual-stack networks are the same as those on IPv4 networks, except some parameters. Check the console pages for details.

Notes and Constraints

- The IPv4/IPv6 dual-stack function is currently free, but will be billed at a later date (price yet to be determined).
- Only ECS flavors that support IPv6 addresses can use IPv4/IPv6 dual-stack networks.

  You can use either of the following methods to check which ECS flavors support IPv6 addresses:

  - On the ECS console, click **Buy ECS**. On the displayed page, view the ECS flavors.

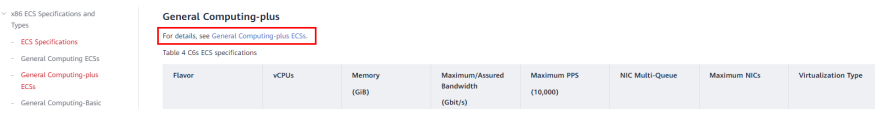
    If an ECS flavor has the **IPv6** parameter with the value of **Yes**, the ECS flavor supports IPv6 addresses.
  - On the **ECS Specifications** page, click the link of your desired ECS specifications for detailed information, and check the ECS flavors that support IPv6 in the table of ECS features.

    For example, if you want to check the flavors of general computing-plus ECSs that support IPv6:

    i. Open the **ECS Specifications** page.

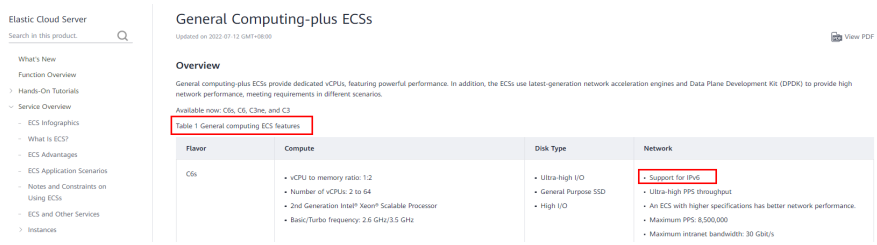
    ii. Under **General Computing-Plus**, click the link for detailed information.

    Figura 1-9 Link for detailed information

    iii. On the **General Computing-plus ECSs** page, check whether IPv6 is supported in the table of ECS features.

Figura 1-10 General computing-plus ECSs



IPv6 Application Scenarios

If your ECS supports IPv6, you can use the IPv4/IPv6 dual-stack network. **Tabela 1-11** shows the example application scenarios.

Tabela 1-11 Application scenarios of IPv4/IPv6 dual stack

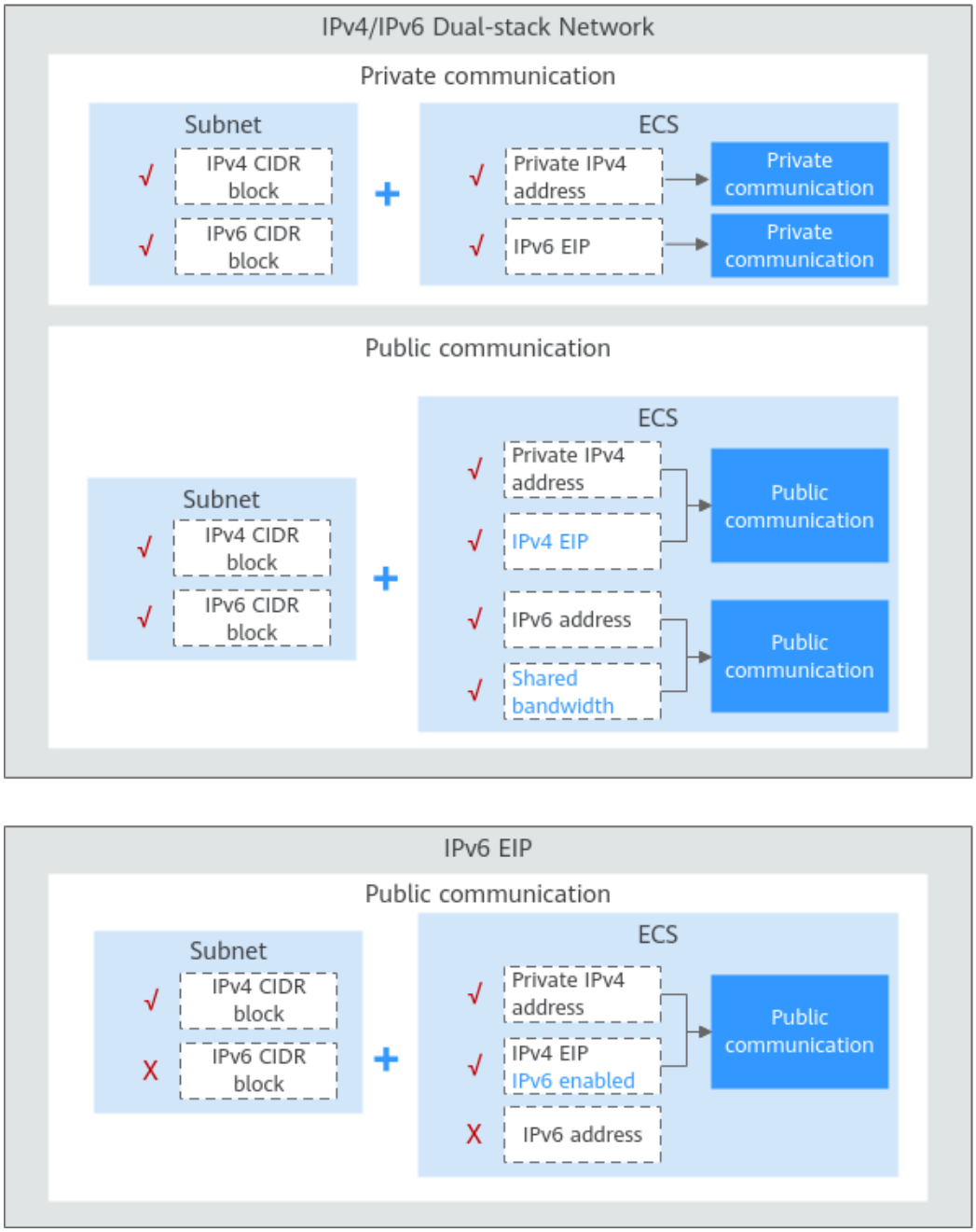
Application Scenario	Description	Subnet	ECS
Private communication using IPv6 addresses	Your applications deployed on ECSs need to communicate with other systems (such as databases) through private networks using IPv6 addresses.	• IPv4 CIDR block • IPv6 CIDR block	• Private IPv4 address: used for private communication • IPv6 address: used for private communication.
Public communication using IPv6 addresses	Your applications deployed on ECSs need to provide services accessible from the Internet using IPv6 addresses.	• IPv4 CIDR block • IPv6 CIDR block	• Private IPv4 address + IPv4 EIP: used for public network communication • IPv6 address + shared bandwidth: used for public network communication
	Your applications deployed on ECSs need to both provide services accessible from the Internet and analyze the access request data using IPv6 addresses.		

If your ECS flavor does not support IPv6 addresses, you can enable the IPv6 EIP function to allow communications using IPv6 addresses. For details, see **Tabela 1-12**.

Tabela 1-12 Application scenarios of IPv6 EIPs

Application Scenario	Description	Subnet	ECS
Public communication using IPv6 addresses	Your applications deployed on ECSs need to provide services accessible from the Internet using IPv6 addresses.	IPv4 CIDR block	• Private IPv4 address • IPv4 EIP (with IPv6 function enabled): used for public communication using IPv4 and IPv6 EIPs

Figura 1-11 Application scenarios of IPv6 networks



Basic Operations

Creating an IPv6 Subnet

Create an IPv6 subnet by following the instructions in **Criação de uma sub-rede para a VPC**. Select **Enable** for **IPv6 CIDR Block**. An IPv6 CIDR block will be automatically assigned to the subnet. IPv6 cannot be disabled after the subnet is created. Currently, customizing IPv6 CIDR block is not supported.

Viewing In-Use IPv6 Addresses

In the subnet list, click the subnet name. On the displayed page, view in-use IPv6 addresses on the **IP Addresses** tab page.

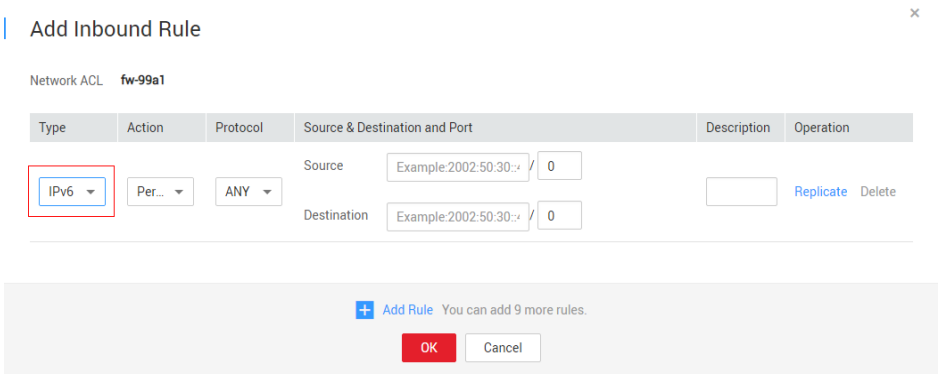
Adding a Security Group Rule (IPv6)

Add a security group rule with **Type** set to **IPv6** and **Source** or **Destination** set to an IPv6 address or IPv6 CIDR block.

Adding a Network ACL Rule (IPv6)

Add a network ACL rule with **Type** set to **IPv6** and **Source** or **Destination** set to an IPv6 address or IPv6 CIDR block.

Figura 1-12 Adding a network ACL rule (IPv6)



Adding a Route (IPv6)

Add a route with **Destination** and **Next Hop** set to an IPv4 or IPv6 CIDR block. For details about how to add a route, see **Adição de uma rota personalizada**. If the destination is an IPv6 CIDR block, the next hop can only be an IP address in the same VPC as the IPv6 CIDR block.

NOTA

If the destination is an IPv6 CIDR block, the next hop type can only be an ECS, extension NIC, or virtual IP address. The next hop must also have IPv6 addresses.

Dynamically Assigning IPv6 Addresses

After an ECS is created successfully, you can view the assigned IPv6 address on the ECS details page. You can also log in to the ECS and run the **ifconfig** command to view the assigned IPv6 address.

If an IPv6 address fails to be automatically assigned or the selected image does not support the function of automatic IPv6 address assignment, manually obtain the IPv6 address by referring to **Dynamically Assigning IPv6 Addresses**.

NOTA

If an ECS is created from a public image:

Before enabling dynamic IPv6 address assignment for a Linux public image, check whether IPv6 is supported and then check whether dynamic IPv6 address assignment has been enabled. Currently, all Linux public images support IPv6, and dynamic IPv6 address assignment is enabled for Ubuntu 16 by default. You do not need to configure dynamic IPv6 address assignment for the Ubuntu 16 OS. For other Linux public images, you need to enable this function.

2 Segurança

2.1 Grupo de segurança

2.1.1 Visão geral do grupo de segurança

Grupo de segurança

Um grupo de segurança é uma coleção de regras de controle de acesso para recursos de nuvem, como servidores de nuvem, containers e bancos de dados, que têm os mesmos requisitos de proteção de segurança e que são mutuamente confiáveis. Depois que um grupo de segurança é criado, você pode criar várias regras de acesso para o grupo de segurança, essas regras serão aplicadas a todos os recursos em nuvem adicionados a esse grupo de segurança.

O sistema cria um grupo de segurança padrão para cada conta. Por padrão, as regras **do grupo de segurança padrão**:

- Permitir todos os pacotes de saída: as instâncias no grupo de segurança padrão podem enviar solicitações e receber respostas de instâncias em outros grupos de segurança.
- Negar todos os pacotes de entrada: solicitações de instâncias em outros grupos de segurança serão negadas pelo grupo de segurança padrão.

Instâncias no mesmo grupo de segurança podem se comunicar entre si sem adicionar regras adicionais.

Se o grupo de segurança padrão não atender aos seus requisitos, você poderá **modificar as regras do grupo de segurança** ou **criar um grupo de segurança personalizado**.

NOTA

Ambos os grupos de segurança padrão e personalizado são gratuitos.

Noções básicas do grupo de segurança

- Você pode associar instâncias, como servidores e NICs de extensão, a um ou mais grupos de segurança.

  Você pode alterar os grupos de segurança associados às instâncias, como servidores ou NICs de extensão. Por padrão, quando você cria uma instância, ela é associada ao grupo

de segurança padrão de sua VPC, a menos que você especifique outro grupo de segurança.

- Você precisa adicionar regras de grupo de segurança para permitir que instâncias no mesmo grupo de segurança se comuniquem entre si.
- Os grupos de segurança são com status. Se você enviar uma solicitação de sua instância e o tráfego de saída for permitido, o tráfego de resposta para essa solicitação poderá fluir independentemente das regras do grupo de segurança de entrada. Da mesma forma, se o tráfego de entrada for permitido, as respostas ao tráfego de entrada permitido poderão fluir para fora, independentemente das regras de saída.

  Os grupos de segurança usam o rastreamento de conexão para controlar o tráfego de e para instâncias que eles contêm e as regras de grupo de segurança são aplicadas com base no status de conexão do tráfego para determinar se deve permitir ou negar o tráfego. Se você adicionar, modificar ou excluir uma regra de grupo de segurança, ou criar ou excluir uma instância no grupo de segurança, o rastreamento de conexão de todas as instâncias no grupo de segurança será automaticamente limpo. Nesse caso, o tráfego de entrada ou saída da instância será considerado como novas conexões, que precisam corresponder às regras de grupo de segurança de entrada ou saída para garantir que as regras entrem em vigor imediatamente e a segurança do tráfego de entrada.

  Além disso, se o tráfego de entrada ou de saída de uma instância não tiver pacotes por um longo tempo, o tráfego será considerado como novas conexões após o tempo limite de rastreamento da conexão, e as conexões precisarão corresponder às regras de saída e de entrada. O período de tempo limite de rastreamento de conexão varia de acordo com o protocolo. O período de tempo limite de uma conexão TCP no estado estabelecido é de 600s, e o período de tempo limite de uma conexão ICMP é de 30s. Para outros protocolos, se os pacotes forem recebidos em ambas as direções, o período de tempo limite de rastreamento de conexão será de 180s. Se um ou mais pacotes forem recebidos em uma direção, mas nenhum pacote for recebido na outra direção, o período de tempo limite de rastreamento de conexão será de 30s. Para protocolos que não sejam TCP, UDP e ICMP, apenas o endereço IP e o número do protocolo são rastreados.

NOTA

Se dois ECSs estiverem no mesmo grupo de segurança, mas em VPCs diferentes, os ECSs não poderão se comunicar entre si. Para habilitar a comunicação entre os ECSs, use uma conexão de emparelhamento de VPC para conectar as duas VPCs. Para obter detalhes sobre a conectividade VPC, consulte **Cenários de aplicação**.

Regras de grupos de segurança

Depois de criar um grupo de segurança, pode adicionar regras ao grupo de segurança. Uma regra se aplica ao tráfego de entrada ou ao tráfego de saída. Depois de adicionar recursos de nuvem ao grupo de segurança, eles são protegidos pelas regras do grupo.

Uma regra de grupo de segurança consiste em:

- **Source** (regra de entrada) ou **Destination** (regra de saída): o valor pode ser um endereço IP (como 192.168.10.10/32), um intervalo de endereços IP (como 192.168.52.0/24) ou um grupo de segurança (como sg-abc).
- **Protocol & Port**: o valor das portas podem ser portas individuais (como 22), portas consecutivas (como 22-30), portas e intervalos de porta (20,23-30), todas as portas (1-65535). O protocolo pode ser TCP, UDP, HTTP e outros.
- **Source**: o valor pode ser um único endereço IP, um grupo de endereços IP, ou um grupo de segurança.

- **Type**: o valor pode ser IPv4 ou IPv6.
- **Description**: informações complementares sobre a regra de grupo de segurança.

Cada grupo de segurança tem suas regras padrão. Para mais detalhes, consulte **Tabela 2-2**. Você também pode personalizar regras de grupo de segurança. Para mais detalhes, consulte **Adição de uma regra de grupo de segurança**.

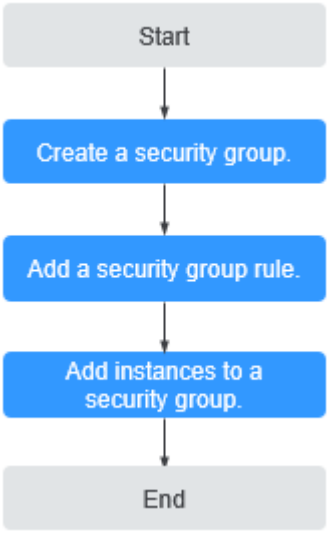
Modelo de grupo de segurança

Você pode selecionar um dos seguintes modelos de grupo de segurança fornecidos pelo sistema para criar rapidamente um grupo de segurança com regras padrão.

- **General-purpose web server**: o grupo de segurança que será criado usando esse modelo é para servidores Web de uso geral e inclui regras padrão que permitem todo o tráfego de entrada ICMP e permitem o tráfego de entrada nas portas 22, 80, 443 e 3389.
- **All ports open**: o grupo de segurança que criar utilizando este modelo inclui regras predefinidas que permitem tráfego de entrada em qualquer porta. Observe que permitir tráfego de entrada em qualquer porta apresenta riscos de segurança.
- **Custom**: o grupo de segurança que criar utilizando este modelo inclui regras predefinidas que negam tráfego de entrada em qualquer porta. Você pode adicionar ou modificar regras de grupo de segurança conforme necessário.

Processo de configuração do grupo de segurança

Figura 2-1 Processo para configurar um grupo de segurança



Restrições do grupo de segurança

- Por padrão, você pode criar um máximo de 100 grupos de segurança em sua conta de nuvem.
- Por padrão, você pode adicionar até 50 regras de grupo de segurança a um grupo de segurança.
- Por padrão, não é possível associar mais de cinco grupos de segurança a cada ECS ou NIC de extensão.

- Se um servidor de nuvem ou uma NIC de extensão estiver associado a vários grupos de segurança, as regras de grupo de segurança serão aplicadas com base na seguinte sequência: o primeiro grupo de segurança associado terá precedência sobre os associados posteriormente e, em seguida, a regra com a prioridade mais alta nesse grupo de segurança será aplicada primeiro.
- Você pode adicionar no máximo 20 instâncias a um grupo de segurança por vez.
- Um grupo de segurança não pode ter mais do que instâncias de 6.000 associadas ou o desempenho se deteriorará.
- As regras de grupo de segurança com determinadas configurações não entram em vigor para ECSs de determinadas especificações. **Tabela 2-1** mostra os detalhes.

Tabela 2-1 Cenários em que as regras de grupo de segurança não entram em vigor

Configuração da regra	Tipo de ECS
• **Action** é definida como **Deny**. • **Source** ou **Destination** é definido como **IP address group**.	Os seguintes tipos de ECS x86 não são suportados: • Otimizado por memória (M1 ECSs) • Computação de alto desempenho (H1 ECSs) • Uso intensivo de disco (D1 ECSs) • Acelerado por GPU (G1 e G2 ECSs) • Ampla memória (E1, E2 e ET2 ECSs)
Port é definida como portas não consecutivas.	Os seguintes tipos de ECS x86 não são suportados: • Computação geral (S1, C1 e C2 ECSs) • Otimizado por memória (M1 ECSs) • Computação de alto desempenho (H1 ECSs) • Uso intensivo de disco (D1 ECSs) • Acelerado por GPU (G1 e G2 ECSs) • Ampla memória (E1, E2 e ET2 ECSs)
	Todos os ECSs de Kunpeng não são suportados.

NOTA

- Para obter detalhes sobre ECSs x86, consulte **Especificações do ECS (x86)**.
- Para obter detalhes sobre os ECSs de Kunpeng, consulte **Especificações do ECS (Kunpeng)**.

Sugestões

Ao usar um grupo de segurança:

- Não adicione todas as instâncias ao mesmo grupo de segurança se elas tiverem requisitos de isolamento diferentes.
- Não é necessário que crie um grupo de segurança para cada instância. Em vez disso, você pode adicionar instâncias com os mesmos requisitos de segurança ao mesmo grupo de segurança.

Quando adiciona uma regra de grupo de segurança:

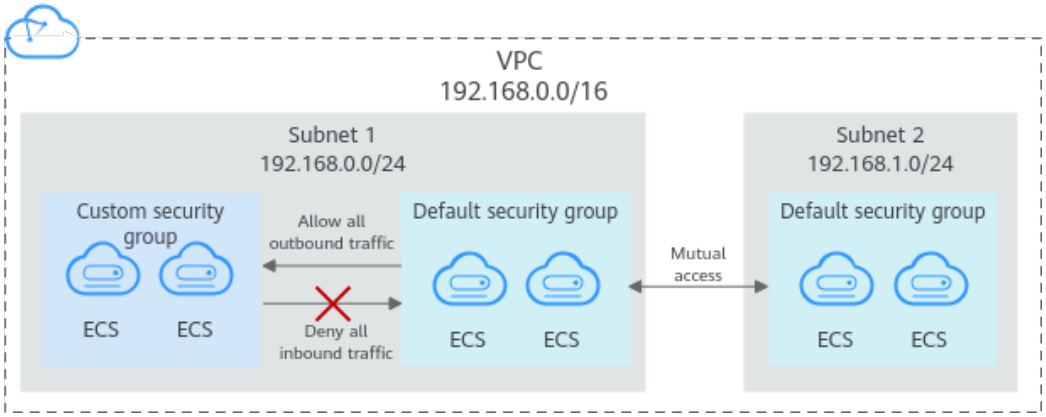
- Defina regras simples de grupo de segurança. Por exemplo, se você adicionar uma instância a vários grupos de segurança, a instância poderá estar em conformidade com centenas de regras de grupo de segurança, e uma alteração em qualquer regra poderá causar desconexão da rede para a instância.
- Antes de modificar um grupo de segurança e suas regras, clone o grupo de segurança e modifique o grupo de segurança clonado para testar a comunicação e evitar impactos adversos nos serviços em execução. Para obter detalhes, consulte **Clonagem de um grupo de segurança**.
- Ao adicionar uma regra de grupo de segurança para uma instância, conceda as permissões mínimas possíveis. Por exemplo:
  - Abra uma porta específica, por exemplo, 22. Não é recomendável que você abra um intervalo de portas, por exemplo, 22-30.
  - Não é recomendável que você digite 0.0.0.0/0, permitindo o tráfego para ou de todos os endereços IP.
- Uma regra de grupo de segurança entra em vigor imediatamente para seus ECSs associados após a configuração da regra sem a reinicialização do ECS. Independentemente das regras de entrada de um grupo de segurança, o tráfego de resposta do tráfego de saída é permitido. Se uma regra de grupo de segurança não tiver efeito depois de ser configurada, consulte **Por que minhas regras de grupo de segurança não têm efeito?**

2.1.2 Grupos de segurança padrão e regras de grupo de segurança

O sistema cria um grupo de segurança padrão para cada conta. Por padrão, as regras padrão do grupo de segurança:

- Permitir todos os pacotes de saída: as instâncias no grupo de segurança padrão podem enviar solicitações e receber respostas de instâncias em outros grupos de segurança.
- Negar todos os pacotes de entrada: solicitações de instâncias em outros grupos de segurança serão negadas pelo grupo de segurança padrão.

Figura 2-2 Grupo de segurança padrão



NOTA

- Ambos os grupos de segurança padrão e personalizado são gratuitos.
- Não é possível excluir o grupo de segurança padrão, mas você pode modificar as regras para o grupo de segurança padrão.
- Se dois ECSs estiverem no mesmo grupo de segurança, mas em VPCs diferentes, os ECSs não poderão se comunicar entre si. Para habilitar a comunicação entre os ECSs, use uma conexão de emparelhamento da VPC para conectar as duas VPCs. Para obter detalhes sobre a conectividade da VPC, consulte **Cenários de aplicação**.

Tabela 2-2 descreve as regras padrão no grupo de segurança padrão.

Tabela 2-2 Regras no grupo de segurança padrão

Direção	Prioridade	Ação	Protocolo	Porta/Intervalo	Origem/Destino	Descrição
Saída	100	Allow	Todos	Todos	Destino: 0.0.0.0/0	Permite todo o tráfego de saída.
Entrada	100	Allow	Todos	Todos	Origem: nome do grupo de segurança atual	Permite comunicações entre ECSs dentro do mesmo grupo de segurança em qualquer porta.
Entrada	100	Allow	TCP	22	Origem: 0.0.0.0/0	Permite que todos os endereços IP acessem os ECSs do Linux por meio de SSH.
Entrada	100	Allow	TCP	3389	Origem: 0.0.0.0/0	Permite que todos os endereços IP acessem os ECSs do Windows por meio do RDP.

2.1.3 Exemplos de configuração de grupo de segurança

As configurações comuns do grupo de segurança são apresentadas aqui. Os exemplos nesta seção permitem todos os pacotes de dados de saída por padrão. Esta seção descreve apenas como configurar regras de entrada.

- **Permissão de acesso externo a uma porta especificada**
- **Ativar ECSs em diferentes grupos de segurança para se comunicarem entre si por meio de uma rede interna**
- **Habilitar endereços IP especificados para acessar remotamente ECSs em um grupo de segurança**
- **Conectar-se remotamente a ECSs do Linux usando SSH**
- **Conectar-se remotamente a ECSs do Windows usando RDP**
- **Habilitar a comunicação entre ECSs**

- **Hospedar um site em ECSs**
- **Habilitar um ECS para funcionar como um servidor DNS**
- **Carregar ou baixar arquivos usando FTP**

Você pode usar o grupo de segurança padrão ou criar um grupo de segurança com antecedência. Para obter detalhes, consulte as seções **Criação de um grupo de segurança** e **Adição de uma regra de grupo de segurança**.

Permissão de acesso externo a uma porta especificada

- Cenário de exemplo:

  depois que os serviços são implementados, você pode adicionar regras de grupo de segurança para permitir acesso externo a uma porta especificada (por exemplo, 1100).

- Regra de grupos de segurança:

Direção	Protocolo	Porta	Origem
Entrada	TCP	1100	0.0.0.0/0

Ativar ECSs em diferentes grupos de segurança para se comunicarem entre si por meio de uma rede interna

- Cenário de exemplo:

  os recursos em um ECS em um grupo de segurança precisam ser copiados para um ECS associado a outro grupo de segurança. Os dois ECSs estão na mesma VPC. Recomendamos que você habilite a comunicação de rede privada entre os ECSs e, em seguida, copie os recursos.

- Configuração do grupo de segurança:

  em uma determinada VPC, os ECSs no mesmo grupo de segurança podem se comunicar uns com os outros por padrão. No entanto, os ECSs em grupos de segurança diferentes não podem se comunicar uns com os outros por padrão. Para permitir que esses ECSs se comuniquem entre si, você precisa adicionar determinadas regras de grupo de segurança.

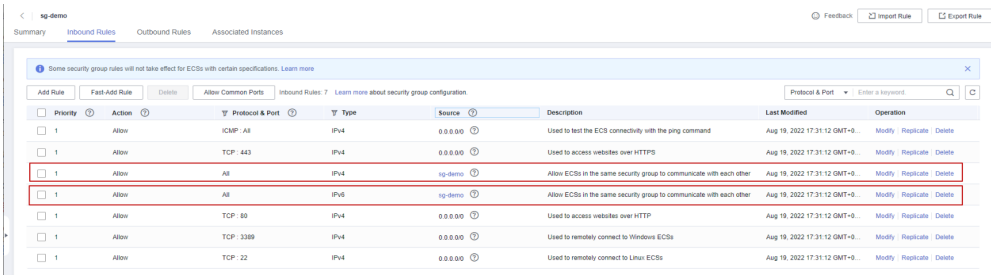
  Você pode adicionar uma regra de entrada aos grupos de segurança que contêm os ECSs para permitir o acesso de ECSs no outro grupo de segurança. A regra exigida é a seguinte.

Direção	Protocolo	Porta	Origem
Entrada	Utilizado para comunicação através de uma rede interna	Porta ou intervalo de porta	ID de outro grupo de segurança

AVISO

Se os ECSs associados ao mesmo grupo de segurança não puderem se comunicar entre si, verifique se a regra que permite a comunicação foi excluída.

O seguinte usa o grupo de segurança **sg-demo** como um exemplo. A regra com **Source** definida como **sg-demo** permite que os recursos associados a este grupo de segurança se comuniquem entre si.



Habilitar endereços IP especificados para acessar remotamente ECSs em um grupo de segurança

- Cenário de exemplo:

  para evitar que os ECSs sejam atacados, você pode alterar o número da porta para logon remoto e configurar regras para o grupo de segurança que permitam apenas endereços IP especificados de acessarem remotamente os ECSs.

- Configuração do grupo de segurança:

  para permitir que o endereço IP **192.168.20.2** acesse remotamente ECSs do Linux em um grupo de segurança pelo protocolo SSH (porta 22), você pode configurar a seguinte regra de grupo de segurança.

Direção	Protocolo	Porta	Origem
Entrada	SSH	22	Bloco CIDR IPv4 ou ID de outro grupo de segurança Por exemplo, 192.168.20.2/32

Conectar-se remotamente a ECSs do Linux usando SSH

- Cenário de exemplo:

  depois de criar ECSs do Linux, você pode adicionar uma regra de grupo de segurança para habilitar o acesso SSH remoto aos ECSs.

  NOTA

  O grupo de segurança padrão vem com a seguinte regra. Se você usar o grupo de segurança padrão, não será necessário adicionar essa regra novamente.

- Regra de grupos de segurança:

Direção	Protocolo	Porta	Origem
Entrada	SSH	22	0.0.0.0/0

Conectar-se remotamente a ECSs do Windows usando RDP

- Cenário de exemplo:

  depois de criar ECSs do Windows, você pode adicionar uma regra de grupo de segurança para habilitar o acesso RDP remoto aos ECSs.

  NOTA

  O grupo de segurança padrão vem com a seguinte regra. Se você usar o grupo de segurança padrão, não será necessário adicionar essa regra novamente.

- Regra de grupos de segurança:

Direção	Protocolo	Porta	Origem
Entrada	RDP	3389	0.0.0.0/0

Habilitar a comunicação entre ECSs

- Cenário de exemplo:

  depois de criar ECSs, você precisa adicionar uma regra de grupo de segurança para que você possa executar o comando **ping** para testar a comunicação entre os ECSs.

- Regra de grupos de segurança:

Direção	Protocolo	Porta	Origem
Entrada	ICMP	Todas	0.0.0.0/0

Hospedar um site em ECSs

- Cenário de exemplo:

  se você implementar um site em seus ECSs e precisar que ele seja acessado por HTTP ou HTTPS, você poderá adicionar as seguintes regras ao grupo de segurança usado pelos ECSs que funcionam como servidores Web.

- Regra de grupo de segurança:

Direção	Protocolo	Porta	Origem
Entrada	HTTP	80	0.0.0.0/0
Entrada	HTTPS	443	0.0.0.0/0

Habilitar um ECS para funcionar como um servidor DNS

- Cenário de exemplo:

se você precisar usar um ECS como um servidor DNS, deverá permitir o acesso TCP e UDP da porta 53 ao servidor DNS. Você pode adicionar as seguintes regras ao grupo de segurança associado ao ECS.

- Regras de grupo de segurança:

Direção	Protocolo	Porta	Origem
Entrada	TCP	53	0.0.0.0/0
Entrada	UDP	53	0.0.0.0/0

Carregar ou baixar arquivos usando FTP

- Cenário de exemplo:

  se quiser usar Protocolo de transferência de arquivos (FTP) para carregar ou baixar arquivos de ECSs, será necessário adicionar uma regra de grupo de segurança.

  NOTA

  Você deve primeiro instalar o programa de servidor de FTP nos ECSs e verificar se as portas 20 e 21 estão funcionando corretamente.

- Regra de grupo de segurança:

Direção	Protocolo	Porta	Origem
Entrada	TCP	20-21	0.0.0.0/0

Adicionar um ECS a vários grupos de segurança

Talvez seja necessário adicionar um ECS a vários grupos de segurança com base nos requisitos de serviço. As regras de grupo de segurança serão aplicadas com base na seguinte sequência: o primeiro grupo de segurança associado terá precedência sobre os associados posteriormente, em seguida, a regra com a prioridade mais alta nesse grupo de segurança será aplicada primeiro. Usar vários grupos de segurança pode causar problemas ao acessar o ECS. Recomendamos que você não associe mais de cinco grupos de segurança a cada ECS.

2.1.4 Criação de um grupo de segurança

Cenários

Você pode criar grupos de segurança e adicionar ECSs em uma VPC a diferentes grupos de segurança para melhorar a segurança de acesso ao ECS. Recomendamos que você atribua ECSs que tenham diferentes requisitos de acesso à Internet a diferentes grupos de segurança.

Cada ECS deve estar associado a pelo menos um grupo de segurança. Se você não tiver grupos de segurança ao comprar um ECS, o ECS usará o **grupo de segurança padrão** (**default**).

Você tem a opção de criar um novo grupo de segurança para o ECS. Esta seção descreve como criar um grupo de segurança no console de gerenciamento.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Access Control** > **Security Groups**.
5. Na página **Security Groups**, clique em **Create Security Group**.
6. Na área **Create Security Group**, defina os parâmetros conforme solicitado. **Tabela 2-3** lista os parâmetros a serem configurados.

Figura 2-3 Criar grupo de segurança

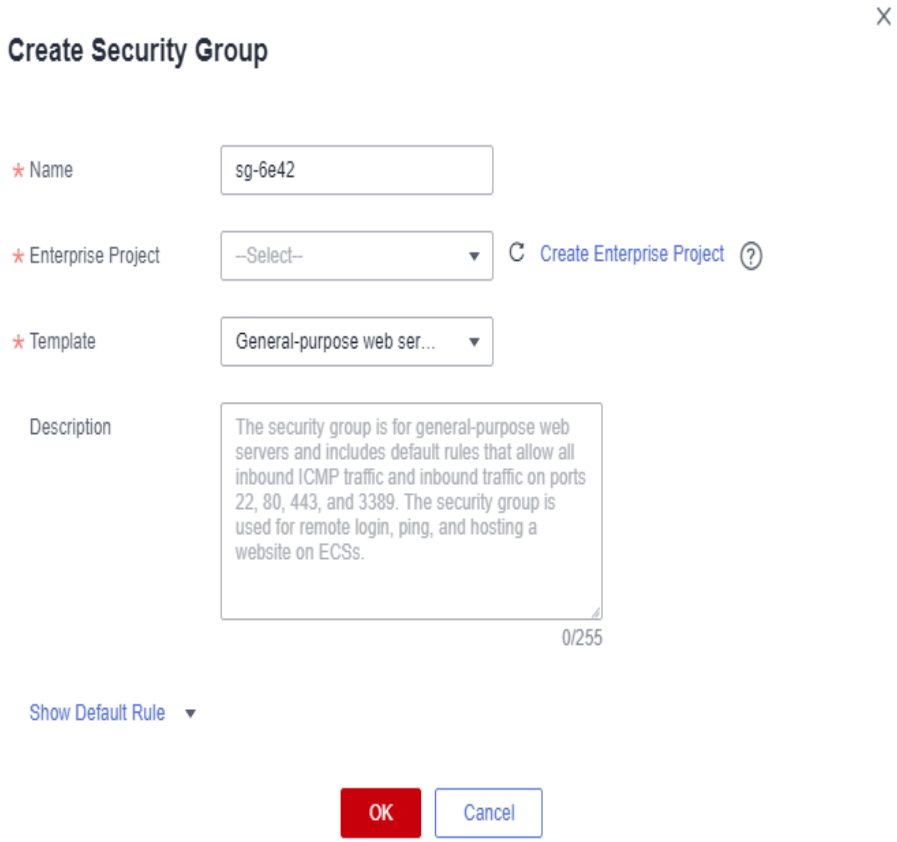


Tabela 2-3 Descrição do parâmetro

Parâmetro	Descrição	Exemplo de valor
Template	Um modelo vem com regras de grupo de segurança padrão, ajudando você a criar rapidamente grupos de segurança. Os seguintes modelos são fornecidos: ● **Custom**: este modelo permite que você crie grupos de segurança com regras de grupo de segurança personalizadas. ● **General-purpose web server**: o grupo de segurança que você cria usando esse modelo é para servidores Web de uso geral e inclui regras padrão que permitem todo o tráfego ICMP de entrada e permitem o tráfego de entrada nas portas 22, 80, 443 e 3389. ● **All ports open**: o grupo de segurança que você cria utilizando este modelo inclui regras predefinidas que permitem tráfego de entrada em qualquer porta. Observe que permitir tráfego de entrada em qualquer porta apresenta riscos de segurança.	Servidor Web de uso geral
Nome	O nome do grupo de segurança. Este parâmetro é obrigatório. O nome do grupo de segurança pode conter no máximo 64 caracteres, que podem ser letras, dígitos, sublinhados (_), hifens (-) e pontos (.). O nome não pode conter espaços. **NOTA** Você pode alterar o nome do grupo de segurança após a criação de um grupo de segurança. Recomenda-se que você dê a cada grupo de segurança um nome diferente.	sg-318b
Projeto empresarial	Ao criar um grupo de segurança, você pode adicionar o grupo de segurança a um projeto empresarial habilitado. Um projeto corporativo facilita o gerenciamento de projeto e o agrupamento de recursos da nuvem e de usuários. O nome do projeto padrão é **default**. Para obter detalhes sobre como criar e gerenciar projetos da empresa, consulte o **Guia de usuário do Enterprise Management**.	Padrão
Description	Informação complementar sobre o grupo de segurança. Este parâmetro é opcional. A descrição do grupo de segurança pode conter no máximo 255 caracteres e não pode conter colchetes angulares (< e >).	N/A

7. Clique em **OK**.

Operações relacionadas

- Para cada grupo de segurança, você pode adicionar regras que controlam o tráfego de entrada para ECSs e um conjunto separado de regras que controlam o tráfego de saída. Para mais detalhes, consulte **Adição de uma regra de grupo de segurança**.
- Cada ECS deve estar associado a pelo menos um grupo de segurança. Você pode adicionar um ECS a vários grupos de segurança com base nos requisitos de serviço. Para mais detalhes, consulte **Adicionar instâncias para e removê-las de um grupo de segurança**.

2.1.5 Adição de uma regra de grupo de segurança

Cenários

Um grupo de segurança é uma coleção de regras de controle de acesso para recursos de nuvem, como servidores de nuvem, containers e bancos de dados, para controlar o tráfego de entrada e saída. Os recursos de nuvem associados ao mesmo grupo de segurança têm os mesmos requisitos de segurança e são mutuamente confiáveis dentro de uma VPC.

Se as regras do grupo de segurança associado à sua instância não atenderem aos seus requisitos, por exemplo, você precisar permitir tráfego de entrada em uma porta TCP especificada, poderá adicionar uma regra de entrada.

- Regras de entrada controlam o tráfego de entrada para os recursos em nuvem no grupo de segurança.
- As regras de saída controlam o tráfego de saída dos recursos da nuvem no grupo de segurança.

Para obter detalhes sobre regras do grupo de segurança padrão, consulte **Grupos de segurança padrão e regras de grupo de segurança**. Para obter detalhes sobre exemplos de configuração de regras de grupo de segurança, consulte **Exemplos de configuração de grupo de segurança**.

Pré-requisitos

- Um grupo de segurança foi criado. Para obter detalhes sobre como criar um grupo de segurança, consulte **Criação de um grupo de segurança**.
- Você planejou as redes públicas ou privadas que podem ou não acessar instâncias, como ECSs. Para obter mais exemplos de regras de grupo de segurança, consulte **Exemplos de configuração de grupo de segurança**.

Procedimento

1. Faça logon no console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking** , clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Access Control** > **Security Groups**.
5. Na página **Security Groups**, localize o grupo de segurança de destino e clique em **Manage Rule** na coluna **Operation** para alternar para a página de gerenciamento de regras de entrada e saída.

6. Na guia **Inbound Rules**, clique em **Add Rule**. Na caixa de diálogo exibida, defina os parâmetros necessários para adicionar uma regra de entrada.

   Você pode clicar em + para adicionar mais regras de entrada.

Figura 2-4 Adicionar regra de entrada

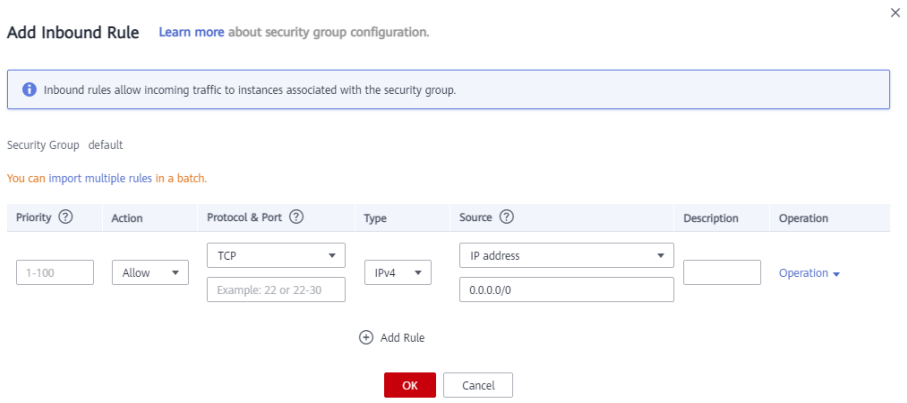


Tabela 2-4 Descrição do parâmetro da regra de entrada

Parâmetro	Descrição	Exemplo de valor
Priority	A prioridade da regra do grupo de segurança. O valor de prioridade varia de 1 a 100. O valor padrão é 1 e tem a prioridade mais alta. A regra de grupo de segurança com um valor menor tem uma prioridade mais alta.	1
Action	As ações de regra do grupo de segurança. As regras de negação têm precedência sobre as regras de permissão da mesma prioridade.	Allow
Protocol & Port	**Protocol**: o protocolo de rede. Atualmente, o valor pode ser **All**, **TCP**, **UDP**, **ICMP**, **GRE** ou outros.	TCP
	Port: a porta ou o intervalo de portas sobre o qual o tráfego pode chegar ao ECS. O valor varia de 1 a 65535. Enter ports in the following format: ● Porta individual: digite uma porta, como 22. ● Portas consecutivas: insira um intervalo de portas, como 22-30. ● Non-consecutive ports: insira portas e intervalos de portas, como **22,23-30**. Você pode inserir um máximo de 20 portas e intervalos de portas. Cada intervalo de portas deve ser exclusivo. ● Todas as portas: deixe-o vazio ou digite 1-65535.	22 ou 22-30

Parâmetro	Descrição	Exemplo de valor
Type	O tipo de endereço IP. Este parâmetro só está disponível depois de ativada a função IPv6. ● IPv4 ● IPv6	IPv4
Source	A origem da regra de grupo de segurança. O valor pode ser um único endereço IP, um grupo de endereços IP ou um grupo de segurança para permitir o acesso de endereços IP ou instâncias no grupo de segurança. Por exemplo: ● Endereço IP único: 192.168.10.10/32 (IPv4); 2002:50::44/127 (IPv6) ● Intervalo de endereços IP: 192.168.1.0/24 (IPv4); 2407:c080:802:469::/64 (IPv6) ● Todos os endereços IP: 0.0.0.0/0 (IPv4); ::/0 (IPv6) ● Grupo de segurança: sg-abc ● Grupo de endereços IP: ipGroup-test Se a origem for um grupo de segurança, esta regra será aplicada a todas as instâncias associadas ao grupo de segurança selecionado. Para obter mais informações sobre grupos de endereços IP, consulte **Visão geral do grupo de endereços IP** .	0.0.0.0/0
Description	Informações complementares sobre a regra de grupo de segurança. Este parâmetro é opcional. A descrição da regra de grupo de segurança pode conter um máximo de 255 caracteres e não pode conter colchetes angulares (< e >).	N/A

7. Na guia **Outbound Rules**, clique em **Add Rule**. Na caixa de diálogo exibida, defina os parâmetros necessários para adicionar uma regra de saída.

   Você pode clicar em +·para adicionar mais regras de entrada.

Figura 2-5 Adicionar regra de saída

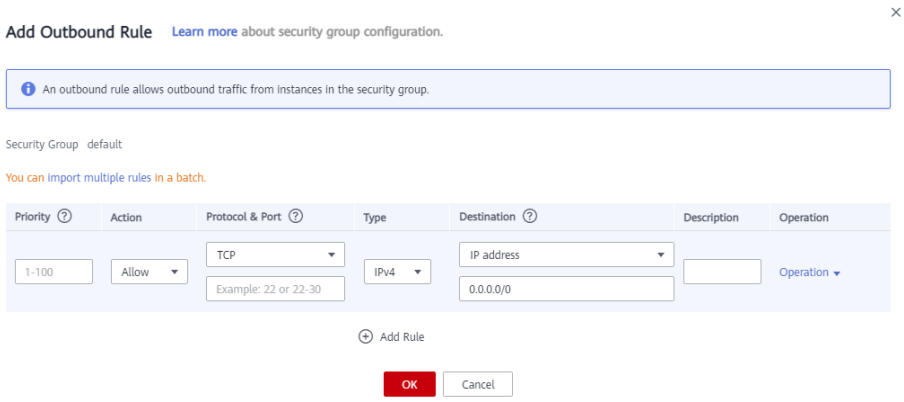


Tabela 2-5 Descrição do parâmetro de regra de saída

Parâmetro	Descrição	Exemplo de valor
Priority	A prioridade da regra do grupo de segurança. O valor de prioridade varia de 1 a 100. O valor padrão é 1 e tem a prioridade mais alta. A regra de grupo de segurança com um valor menor tem uma prioridade mais alta.	1
Action	As ações de regra do grupo de segurança. ● **Allow**: permitir o tráfego de saída de instâncias no grupo de segurança com base na regra. ● **Deny**: recusar tráfego de saída de instâncias no grupo de segurança com base na regra. As regras de negação têm precedência sobre as regras de permissão da mesma prioridade.	Allow
Protocol & Port	**Protocol**: o protocolo de rede. Atualmente, o valor pode ser **All**, **TCP**, **UDP**, **ICMP**, **GRE** ou outros.	TCP
	Port: The port or port range over which the traffic can leave your ECS. O valor varia de 1 a 65535.	22, or 22-30
Type	O tipo de endereço IP. ● IPv4 ● IPv6	IPv4
Destination	O destino da regra de grupo de segurança. O valor pode ser um único endereço IP, um grupo de endereços IP ou um grupo de segurança para permitir o acesso a endereços IP ou instâncias no grupo de segurança. Por exemplo: ● Endereço IP único: 192.168.10.10/32 (IPv4); 2002:50::44/127 (IPv6) ● Intervalo de endereços IP: 192.168.1.0/24 (IPv4); 2407:c080:802:469::/64 (IPv6) ● Todos os endereços IP: 0.0.0.0/0 (IPv4); ::/0 (IPv6) ● Grupo de segurança: sg-abc ● Grupo de endereços IP: ipGroup-test Para obter mais informações sobre grupos de endereços IP, consulte **Visão geral do grupo de endereços IP** .	0.0.0.0/0
Description	Informações complementares sobre a regra de grupo de segurança. Este parâmetro é opcional. A descrição da regra de grupo de segurança pode conter um máximo de 255 caracteres e não pode conter colchetes angulares (< e >).	N/A

8. Clique em **OK**.

Verificação

Depois que as regras de grupo de segurança necessárias forem adicionadas, você poderá verificar se as regras entram em vigor. Por exemplo, você implementou um site em ECSs. Os usuários precisam acessar seu site através de TCP (porta 80), e você adicionou a regra de grupo de segurança mostrada em **Tabela 2-6**.

Tabela 2-6 Regra de grupo de segurança

Direção	Protocolo	Porta	Origem
Entrada	TCP	80	0.0.0.0/0

ECS do Linux

Para verificar a regra de grupo de segurança em um ECS do Linux:

1. Efetue logon no ECS.
2. Execute o seguinte comando para verificar se a porta TCP 80 está sendo ouvida em:

   ```
   netstat -an | grep 80
   ```

   Se a saída do comando mostrada em **Figura 2-6** for exibida, a porta TCP 80 está sendo escutada.

   Figura 2-6 Saída de comando para o ECS do Linux

3. Digite **http://***ECS EIP* na caixa de endereço do navegador e pressione **Enter**.

   Se a página solicitada puder ser acessada, a regra do grupo de segurança entrou em vigor.

ECS do Windows

Para verificar a regra de grupo de segurança em um ECS do Windows:

1. Efetue logon no ECS.
2. Escolha **Start** > **Accessories** > **Command Prompt**.
3. Execute o seguinte comando para verificar se a porta TCP 80 está sendo ouvida em:

   ```
   netstat -an | findstr 80
   ```

   Se a saída do comando mostrada em **Figura 2-7** for exibida, a porta TCP 80 está sendo escutada.

   Figura 2-7 Saída de comando para o ECS do Windows

4. Digite **http://***ECS EIP* na caixa de endereço do navegador e pressione **Enter**.

   Se a página solicitada puder ser acessada, a regra do grupo de segurança entrou em vigor.

Operações relacionadas

Permitir portas comuns

Você pode clicar em **Allow Common Ports** para permitir tráfego em algumas portas comuns, como as portas 21, 22, 3389, 80, 443 e 20.

Figura 2-8 Permitir portas comuns

Links úteis

- **As regras do grupo de segurança são consideradas iguais se todos os parâmetros, exceto sua descrição, forem iguais?**
- **Como configurar um grupo de segurança para protocolos multicanal?**

2.1.6 Adição rápida de regras de grupo de segurança

Cenários

Você pode adicionar várias regras de grupo de segurança com diferentes protocolos e portas ao mesmo tempo.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Access Control** > **Security Groups**.
5. Na página **Security Groups**, localize o grupo de segurança de destino e clique em **Manage Rule** na coluna **Operation** para alternar para a página de gerenciamento de regras de entrada e saída.
6. Na guia **Inbound Rules**, clique em **Fast-Add Rule**. Na caixa de diálogo exibida, selecione os protocolos e as portas que você deseja adicionar de uma só vez.

Figura 2-9 Adicionar rapidamente regra de entrada

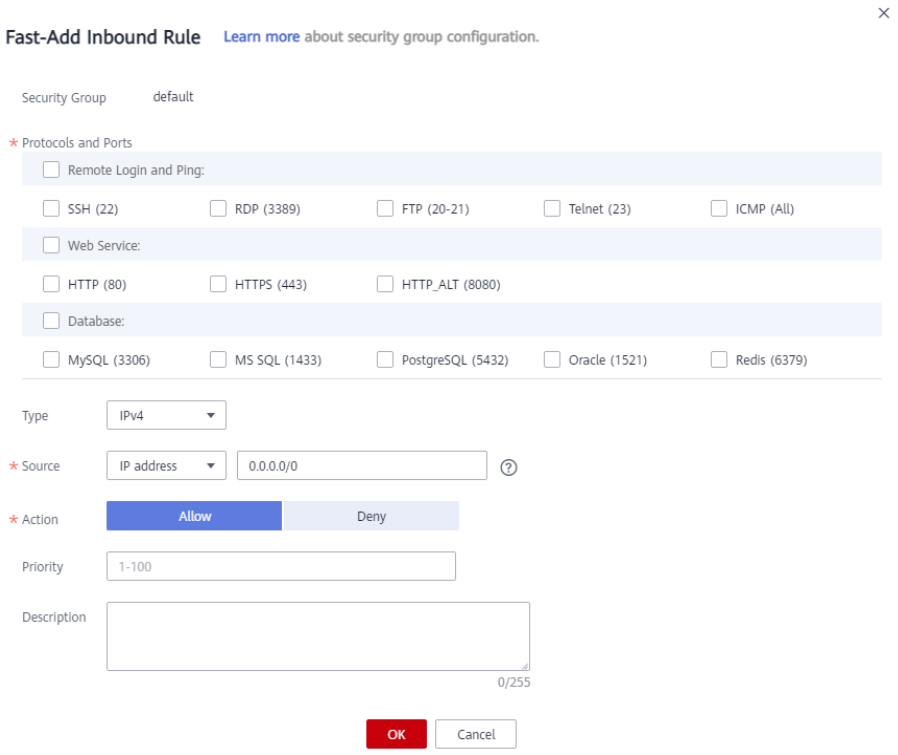


Tabela 2-7 Descrição do parâmetro da regra de entrada

Parâmetro	Descrição	Exemplo de valor
Protocols and Ports	Protocolos e portas comuns são fornecidos para: ● Logon e ping remotos ● Serviços Web ● Bancos de dados	SSH (22)
Type	Versão do endereço IP Este parâmetro está disponível somente depois que a função IPv6 é ativada. ● IPv4 ● IPv6	IPv4

Parâmetro	Descrição	Exemplo de valor
Source	Origem da regra do grupo de segurança. O valor pode ser um endereço IP, um grupo de endereços IP, ou um grupo de segurança para permitir o acesso de endereços IP ou instâncias no grupo de segurança. Por exemplo: ● Endereço IP único: 192.168.10.10/32 (IPv4); 2002:50::44/127 (IPv6) ● Intervalo de endereço IP: 192.168.1.0/24 (IPv4); 2407:c080:802:469::/64 (IPv6) ● Todos os endereços IP 0.0.0.0/0 (IPv4); ::/0 (IPv6) ● Grupo de segurança: sg-abc ● Grupo de endereço IP: ipGroup-test Se a origem for um grupo de segurança, esta regra será aplicada a todas as instâncias associadas ao grupo de segurança selecionado. Para obter mais informações sobre grupos de endereço IP, consulte **Visão geral do grupo de endereço IP**.	0.0.0.0/0
Priority	Prioridade de regra de grupo de segurança. O valor de prioridade é de 1 a 100. O valor padrão é 1 e tem a prioridade mais alta. A regra de grupo de segurança com um valor menor tem uma prioridade mais alta.	1
Action	Ações de regra de grupo de segurança. As regras de negação têm precedência sobre as regras de permissão da mesma prioridade.	Allow
Description	(Opcional) Informações complementares sobre a regra de grupo de segurança. A descrição pode conter no máximo 255 caracteres e não pode conter colchetes angulares (< e >).	-

7. Na guia **Outbound Rules**, clique em **Fast-Add Rule**. Na caixa de diálogo exibida, selecione os protocolos e portas necessários para adicionar várias regras por vez.

Figura 2-10 Adicionar rapidamente regra de entrada

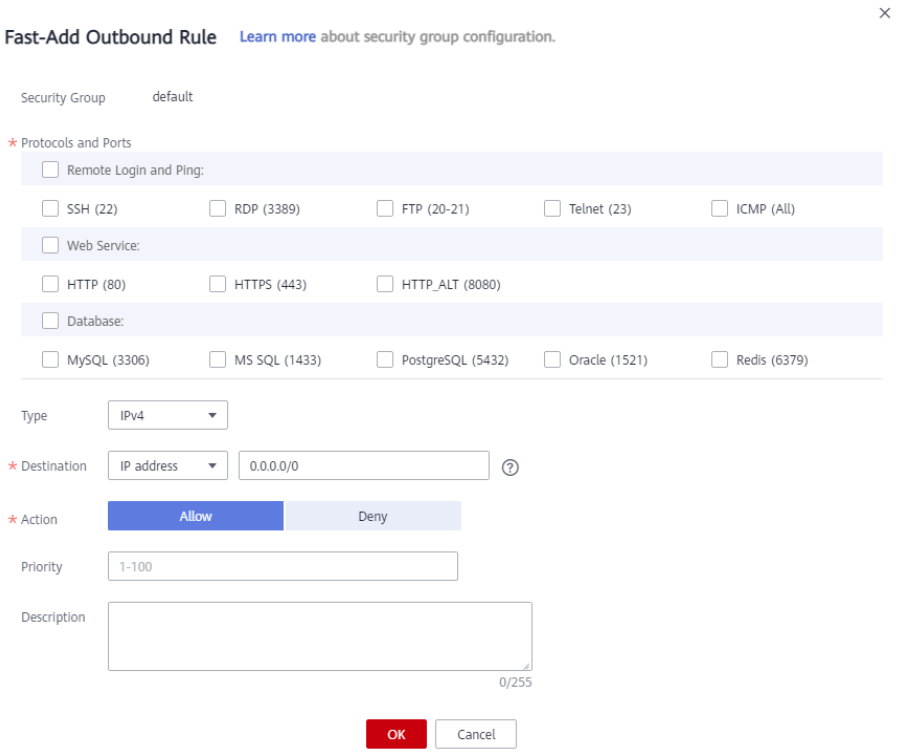


Tabela 2-8 Descrição do parâmetro de regra de saída

Parâmetro	Descrição	Exemplo de valor
Protocols and Ports	Protocolos e portas comuns são fornecidos para: ● Logon e ping remotos ● Serviços Web ● Bancos de dados	SSH (22)
Type	Versão do endereço IP ● IPv4 ● IPv6	IPv4

Parâmetro	Descrição	Exemplo de valor
Destination	Destino da regra de grupo de segurança. O valor pode ser um endereço IP, um grupo de endereços IP, ou um grupo de segurança para permitir o acesso a endereços IP ou instâncias no grupo de segurança. Por exemplo: ● xxx.xxx.xxx.xxx.xxx/32 (endereço IPv4) ● xxx.xxx.xxx.0/24 (intervalo de endereço IPv4) ● 0.0.0.0/0 (todos os endereços IPv4) ● sg-abc (grupo de segurança) ● Endereço IP único: 192.168.10.10/32 (IPv4); 2002:50::44/127 (IPv6) ● Intervalo de endereços IP: 192.168.1.0/24 (IPv4); 2407:c080:802:469::/64 (IPv6) ● Todos os endereços IP 0.0.0.0/0 (IPv4); ::/0 (IPv6) ● Grupo de segurança: sg-abc ● Grupo de endereço IP: ipGroup-test Para obter mais informações sobre grupos de endereço IP, consulte **Visão geral do grupo de endereço IP**.	0.0.0.0/0
Priority	Prioridade de regra de grupo de segurança. O valor de prioridade é de 1 a 100. O valor padrão é 1 e tem a prioridade mais alta. A regra de grupo de segurança com um valor menor tem uma prioridade mais alta.	1
Action	Ações de regra de grupo de segurança. ● **Allow**: permitir o tráfego de saída de instâncias no grupo de segurança com base na regra. ● **Deny**: recusar o tráfego de saída de instâncias no grupo de segurança com base na regra. As regras de negação têm precedência sobre as regras de permissão da mesma prioridade.	Allow
Descrição	(Opcional) Informações complementares sobre a regra de grupo de segurança. A descrição pode conter no máximo 255 caracteres e não pode conter colchetes angulares (< ou >).	-

8. Clique em **OK**.

2.1.7 Replicação de uma regra de grupo de segurança

Cenários

Replicar uma regra de grupo de segurança existente para gerar uma nova regra. Ao replicar uma regra de grupo de segurança, você pode fazer alterações para que ela não seja uma cópia perfeita.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Access Control** > **Security Groups**.
5. Na página **Security Groups**, clique no nome do grupo de segurança.
6. Na página exibida, localize a linha que contém a regra de grupo de segurança a ser replicada e clique em **Replicate** na coluna **Operation**.

   Você também pode modificar a regra de grupo de segurança conforme necessário para gerar rapidamente uma nova regra.
7. Clique em **OK**.

2.1.8 Modificação de uma regra de grupo de segurança

Cenários

Regras de grupo de segurança inadequadas podem causar sérios riscos de segurança. Por exemplo, as regras de grupo de segurança permitem o acesso a portas específicas. Você pode modificar a porta, o protocolo e o endereço IP dessas regras para garantir a segurança de suas instâncias.

Pré-requisitos

Foi criado um grupo de segurança e foram adicionadas regras de grupo de segurança ao grupo de segurança.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, em **Networking**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Access Control** > **Security Groups**.
5. Na página **Security Groups**, clique no nome do grupo de segurança.
6. Na página exibida, localize a linha que contém a regra de grupo de segurança a ser modificada e clique em **Modify** na coluna **Operation**.
7. Modifique a regra e clique em **Confirm**.

2.1.9 Exclusão de uma regra do grupo de segurança

Cenários

Se a origem de uma regra de grupo de segurança de entrada ou o destino de uma regra de grupo de segurança de saída precisar ser alterada, primeiro será necessário excluir a regra de grupo de segurança e adicionar uma nova.

NOTA

As regras do grupo de segurança usam listas brancas. A exclusão de uma regra de grupo de segurança pode resultar em falhas de acesso ao ECS.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Access Control** > **Security Groups**.
5. Na página **Security Groups**, clique no nome do grupo de segurança.
6. Se você não precisar de uma regra de grupo de segurança, localize a linha que contém a regra de destino e clique em **Delete**.
7. Clique em **Yes** na caixa de diálogo exibida.

Excluir várias regras do grupo de segurança de uma só vez

Você também pode selecionar várias regras de grupo de segurança e clicar em **Delete** acima da lista de regras de grupo de segurança para excluir várias regras por vez.

2.1.10 Importação e exportação de regras do grupo de segurança

Cenários

- Se pretender criar ou restaurar rapidamente regras de grupo de segurança, pode importar regras existentes para o grupo de segurança.
- Se quiser fazer backup de regras de grupo de segurança localmente, você pode exportar as regras para um arquivo do Excel.
- Se pretender aplicar rapidamente as regras de um grupo de segurança a outro, ou se pretender modificar várias regras do grupo de segurança atual de uma só vez, pode importar ou exportar regras existentes.

Observações e restrições

- Ao modificar regras de grupo de segurança exportadas, você só pode modificar campos existentes no arquivo exportado com base no modelo e não pode adicionar novos campos ou modificar os nomes dos campos. Caso contrário, o arquivo falhará ao ser importado.
- Ao importar regras de grupo de segurança, se a origem for um grupo de endereços IP, verifique se o grupo de endereços IP existe e se seu nome e ID estão corretos. O formato é **ipGroup-zy[2b5213cb-0f41-4d0b-bed9-b6340bf51017]**.
- Regras duplicadas não são permitidas.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, em **Networking**, clique em **Virtual Private Cloud**.

4. No painel de navegação à esquerda, escolha **Access Control** > **Security Groups**.
5. Na página **Security Groups**, clique no nome do grupo de segurança.
6. Exporte e importe regras de grupo de segurança.

   - Clique em  para exportar todas as regras do grupo de segurança atual para um arquivo do Excel.
   - Clique em  para importar regras de grupo de segurança de um arquivo do Excel para o grupo de segurança atual.

     Tabela 2-9 descreve os parâmetros no modelo para regras de importação.

     Tabela 2-9 Parâmetros do modelo

Parâmetro	Descrição	Exemplo de valor
Direction	A direção na qual a regra de grupo de segurança entra em vigor. ● Regras de entrada controlam o tráfego de entrada para os recursos em nuvem no grupo de segurança. ● As regras de saída controlam o tráfego de saída dos recursos da nuvem no grupo de segurança.	Entrada
Priority	O valor de prioridade varia de 1 a 100. O valor padrão é 1 e tem a prioridade mais alta. A regra de grupo de segurança com um valor menor tem uma prioridade mais alta.	1
Action	As regras de negação têm precedência sobre as regras de permissão da mesma prioridade.	Permitir
Protocol & Port	**Protocol**: o protocolo de rede. Atualmente, o valor pode ser **All**, **TCP**, **UDP**, **ICMP**, **GRE** ou outros.	TCP
	Port: a porta ou o intervalo de portas sobre o qual o tráfego pode chegar ao ECS. O valor varia de 1 a 65535.	22 ou 22-30
Type	O tipo de endereço IP. Este parâmetro só está disponível depois de ativada a função IPv6. ● IPv4 ● IPv6	IPv4

Parâmetro	Descrição	Exemplo de valor
Source	A origem da regra de grupo de segurança. O valor pode ser um único endereço IP, um grupo de endereços IP ou um grupo de segurança para permitir o acesso de endereços IP ou instâncias no grupo de segurança. Por exemplo: ● Endereço IP único: 192.168.10.10/32 (IPv4); 2002:50::44/127 (IPv6) ● Intervalo de endereços IP: 192.168.1.0/24 (IPv4); 2407:c080:802:469::/64 (IPv6) ● Todos os endereços IP: 0.0.0.0/0 (IPv4); ::/0 (IPv6) ● Grupo de segurança: sg-abc ● Grupo de endereços IP: ipGroup-test Para obter mais informações sobre grupos de endereços IP, consulte **Visão geral do grupo de endereços IP** .	0.0.0.0/0
Destination	O destino da regra de grupo de segurança. O valor pode ser um único endereço IP, um grupo de endereços IP ou um grupo de segurança para permitir o acesso a endereços IP ou instâncias no grupo de segurança. Por exemplo: ● Endereço IP único: 192.168.10.10/32 (IPv4); 2002:50::44/127 (IPv6) ● Intervalo de endereços IP: 192.168.1.0/24 (IPv4); 2407:c080:802:469::/64 (IPv6) ● Todos os endereços IP: 0.0.0.0/0 (IPv4); ::/0 (IPv6) ● Grupo de segurança: sg-abc ● Grupo de endereços IP: ipGroup-test Para obter mais informações sobre grupos de endereços IP, consulte **Visão geral do grupo de endereços IP** .	0.0.0.0/0
Description	Informações complementares sobre a regra de grupo de segurança. Este parâmetro é opcional. A descrição da regra de grupo de segurança pode conter um máximo de 255 caracteres e não pode conter colchetes angulares (< e >).	-
Last Modified	A hora em que o grupo de segurança foi modificado.	-

2.1.11 Exclusão de um grupo de segurança

Cenários

Esta seção descreve como excluir grupos de segurança.

Observações e restrições

- Ambos os grupos de segurança padrão e personalizados são gratuitos.
- O grupo de segurança padrão é chamado **default** e não pode ser excluído.

Figura 2-11 Grupo de segurança padrão

- Um grupo de segurança não pode ser excluído se estiver sendo usado por instâncias, como servidores de nuvem, containers e bancos de dados.

  Se quiser excluir esse grupo de segurança, exclua as instâncias ou altere o grupo de segurança usado pela instância primeiro.

  Se você não puder excluir um grupo de segurança mesmo depois de excluir todas as instâncias associadas, **envie um tíquete de serviço**.
- Um grupo de segurança não pode ser eliminado se for utilizado como origem de uma regra noutro grupo de segurança.

  Exclua ou **modifique** a regra e exclua o grupo de segurança novamente.

  Por exemplo, se a origem de uma regra no grupo de segurança **sg-B** estiver definida como **sg-A**, terá de eliminar ou modificar a regra em **sg-B** antes de eliminar **sg-A**.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Access Control** > **Security Groups**.

   A lista de grupos de segurança é exibida.
5. Localize a linha que contém o grupo de segurança de destino, clique em **More** na coluna **Operation** e clique em **Delete**.

   Uma caixa de diálogo de confirmação é exibida.
6. Confirme as informações e clique em **Yes**.

2.1.12 Adicionar instâncias para e removê-las de um grupo de segurança

Cenários

Depois que um grupo de segurança é criado, você pode adicionar instâncias ao grupo de segurança para proteger as instâncias. Você também pode removê-las do grupo de segurança, conforme necessário.

Você pode adicionar várias instâncias ou removê-las de um grupo de segurança.

Adicionar instâncias a um grupo de segurança

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, em **Networking**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Access Control** > **Security Groups**.
5. Na página **Security Groups**, clique em **Manage Instance** na coluna **Operation**.
6. Na guia **Servers**, clique em **Add** e adicione um ou mais servidores ao grupo de segurança atual.
7. Na guia **Extension NICs**, clique em **Add** e adicione uma ou mais NICs de extensão ao grupo de segurança atual.
8. Clique em **OK**.

Remover instâncias de um grupo de segurança

NOTA

- Instâncias foram adicionadas a dois ou mais grupos de segurança.
- As instâncias removidas de um grupo de segurança não podem se comunicar com outras instâncias neste grupo de segurança. Certifique-se de que suas instâncias não serão afetadas negativamente antes de remover instâncias de um grupo de segurança.

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, em **Networking**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Access Control** > **Security Groups**.
5. Na página **Security Groups**, clique em **Manage Instance** na coluna **Operation**.
6. Na guia **Servers**, localize o servidor de destino e clique em **Remove** na coluna **Operation** para remover o servidor do grupo de segurança atual.
7. Na guia **Extension NICs**, localize a NIC de extensão de destino e clique em **Remove** na coluna **Operation** para remover a NIC do grupo de segurança atual.
8. Clique em **Yes**.

Remover várias instâncias de um grupo de segurança

Selecione vários servidores e clique em **Remove** acima da lista de servidores para remover todos os servidores selecionados do grupo de segurança atual de uma só vez.

Selecione NICs de várias extensões e clique em **Remove** acima da lista NIC de extensão para remover as NICs de extensão selecionadas do grupo de segurança atual de uma só vez.

Operações relacionadas

- Você pode **alterar um grupo de segurança para uma instância** com base nos requisitos de serviço.
- Você pode excluir os grupos de segurança que você não precisa mais. **Exclusão de um grupo de segurança** também excluirá suas regras de grupo de segurança.

2.1.13 Clonagem de um grupo de segurança

Cenários

Você pode clonar um grupo de segurança de uma região para outra para aplicar rapidamente as regras de grupo de segurança a ECSs em outra região.

Você pode clonar um grupo de segurança nos seguintes cenários:

- Por exemplo, você tem o grupo de segurança **sg-A** na região A. Se os ECSs na região B exigirem as mesmas regras de grupo de segurança configuradas para o grupo de segurança **sg-A**, você poderá clonar o grupo de segurança **sg-A** na região B, liberando você da criação de um novo grupo de segurança na região B.
- Se precisar de novas regras de grupo de segurança, pode clonar o grupo de segurança original como uma cópia de segurança.

Observações e restrições

Se você clonar grupo de segurança entre regiões, o sistema irá clonar apenas regras cuja origem e destino são blocos CIDR ou estão no grupo de segurança atual.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, em **Networking**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Access Control** > **Security Groups**.
5. Na página **Security Groups**, localize a linha que contém o grupo de segurança de destino e escolha **More** > **Clone** na coluna **Operation**.
6. Defina os parâmetros necessários e clique em **OK**.

   Em seguida, você pode alternar para a região necessária para exibir o grupo de segurança clonado na lista de grupos de segurança.

2.1.14 Modificação de um nome de grupo de segurança

Cenários

Modificar o nome e a descrição de um grupo de segurança criado.

Procedimento

Método 1

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, em **Networking**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Access Control** > **Security Groups**.
5. Na página **Security Groups**, localize o grupo de segurança de destino e escolha **More** > **Modify** na coluna **Operation**.

6. Modifique o nome e a descrição do grupo de segurança conforme necessário.
7. Clique em **OK**.

Método 2

1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, em **Networking**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Access Control** > **Security Groups**.
5. Na página **Security Groups**, clique no nome do grupo de segurança.
6. Na página exibida, clique em  à direita de **Name** e edite o nome do grupo de segurança.
7. Clique em √ para salvar o nome do grupo de segurança.
8. Clique em  à direita de **Description** e edite a descrição do grupo de segurança.
9. Clique em √ para salvar a descrição do grupo de segurança.

2.1.15 Exibição do grupo de segurança de um ECS.

Cenários

Exibir regras de entrada e saída de um grupo de segurança usado por um ECS.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Em **Compute**, clique em **Elastic Cloud Server**.
4. Na página **Elastic Cloud Server**, clique no nome do ECS de destino.
5. Clique na guia **Security Groups** e visualize informação sobre o grupo de segurança usado pelo ECS.

2.1.16 Alteração do grupo de segurança de um ECS

Cenários

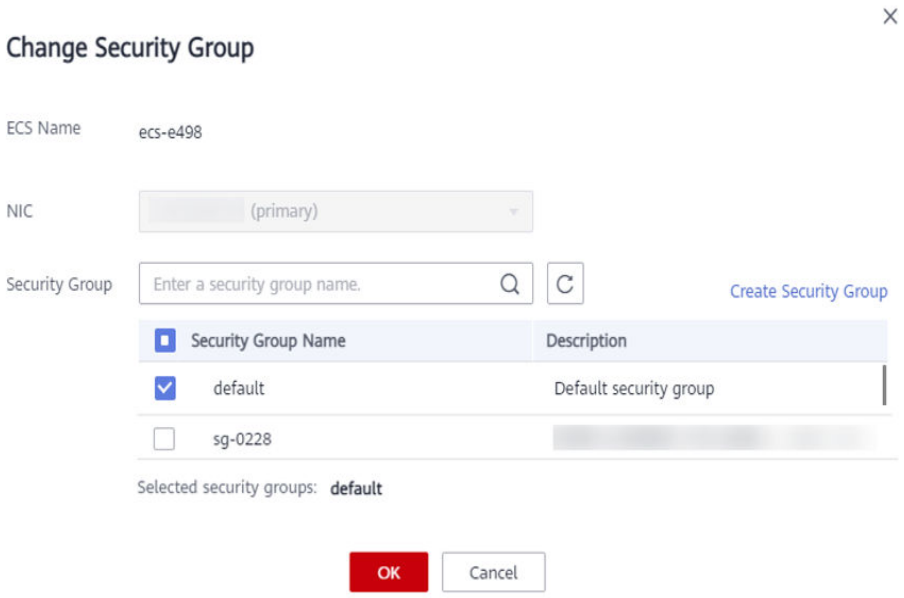
Alterar o grupo de segurança associado a uma NIC do ECS.

Procedimento

1. Efetue login no console de gerenciamento.
2. Clicar em  . Em **Compute**, clique em **Elastic Cloud Server**.
3. Na lista ECS, localize a linha que contém o ECS de destino. Clique em **More** na coluna **Operation** e selecione **Manage Network** > **Change Security Group**.

   A caixa de diálogo **Change Security Group** é exibida.

Figura 2-12 Alterar grupo de segurança



4. Selecione a NIC de destino e os grupos de segurança conforme solicitado.

   Você pode selecionar vários grupos de segurança. Nesse caso, as regras de todos os grupos de segurança selecionados serão agregadas para serem aplicadas no ECS.

   Para criar um grupo de segurança, clique em **Create Security Group**.

   NOTA

   O uso de vários grupos de segurança pode deteriorar o desempenho da rede de ECS. Sugere-se que você selecione não mais do que cinco grupos de segurança.

5. Clique em **OK**.

2.1.17 Portas comuns usadas pelos ECSs

Ao adicionar uma regra de grupo de segurança, você deve especificar a porta ou o intervalo de portas para comunicação. Quando um grupo de segurança detecta uma solicitação de acesso, ele verifica se o endereço IP e a porta do dispositivo que envia a solicitação são permitidos pelas regras do grupo de segurança. A comunicação de dados pode ser estabelecida somente quando as regras do grupo de segurança permitirem a solicitação.

Tabela 2-10 lista as portas comuns usadas pelos ECSs. Você pode configurar regras de grupo de segurança para permitir tráfego de e para portas de ECS especificadas. Para mais detalhes, consulte **Adição de uma regra de grupo de segurança**. Para obter mais informações sobre os requisitos para o Windows, consulte **Visão geral do serviço e requisitos de porta de rede para o Windows**.

Tabela 2-10 Portas comuns usadas pelos ECSs

Protocolo	Porta	Descrição
FTP	21	Usado para fazer upload e download de arquivos
SSH	22	Usado para conectar remotamente aos ECSs do Linux

Protocolo	Porta	Descrição
TELNET	23	Usado para acessar remotamente ECSs com Telnet
SMTP	25	Usado para enviar e-mails Por motivos de segurança, a porta TCP 25 está desabilitada na direção de saída por padrão. Para obter detalhes sobre como abrir a porta, consulte **Por que o acesso de saída pela porta TCP 25 é restrito?**
HTTP	80	Usado para acessar sites em HTTP.
POP3	110	Usado para receber e-mails usando o Post Office Protocol versão 3 (POP3)
IMAP	143	Usado para receber e-mails usando Internet Message Access Protocol (IMAP)
HTTPS	443	Usado para acessar sites em HTTPS.
SQL Server	1433	Uma porta TCP do Microsoft SQL Server para fornecer serviços.
SQL Server	1434	Uma porta UDP do Microsoft SQL Server para retornar o número de porta TCP/IP usado pelo SQL Server
Oracle	1521	Porta de comunicação do banco de dados Oracle, a ser habilitada nos ECSs onde o Oracle SQL Server está implementado.
MySQL	3306	Usado por bancos de dados MySQL para fornecer serviços.
Windows Server Remote Desktop Services	3389	Usado para se conectar a ECSs do Windows
Proxy	8080	Porta proxy 8080 usada no serviço proxy WWW para navegação na web. Se você usar a porta 8080, você precisa adicionar **:8080** após o endereço IP quando você visita um site ou usa um servidor proxy. Após a instalação do Apache Tomcat, a porta de serviço padrão é 8080.
NetBIOS	137, 138 e 139	O NetBIOS é frequentemente usado para arquivos do Windows, compartilhamento de impressoras e Samba. ● Portas 137 e 138: portas UDP que são usadas ao transferir arquivos usando o Network Neighborhood (My Network Places) ● Porta 139: as conexões desta porta tentam acessar o serviço NetBIOS/SMB.

Algumas portas inacessíveis

Sintoma: os usuários em determinadas áreas não podem acessar algumas portas.

Analysis: as portas listadas na tabela a seguir são portas de alto risco e estão bloqueadas por padrão.

Tabela 2-11 Portas de alto risco

Protocolo	Porta
TCP	42, 135, 137, 138, 139, 444, 445, 593, 1025, 1068, 1433, 1434, 3127, 3128, 3129, 3130, 4444, 4789, 5554, 5800, 5900, 8998, 9995 e 9996
UDP	135 a 139, 1026, 1027, 1028, 1068, 1433, 1434, 4789, 5554, 9995 e 9996

Solução: é recomendável que você use portas que não estão listadas na tabela para seus serviços.

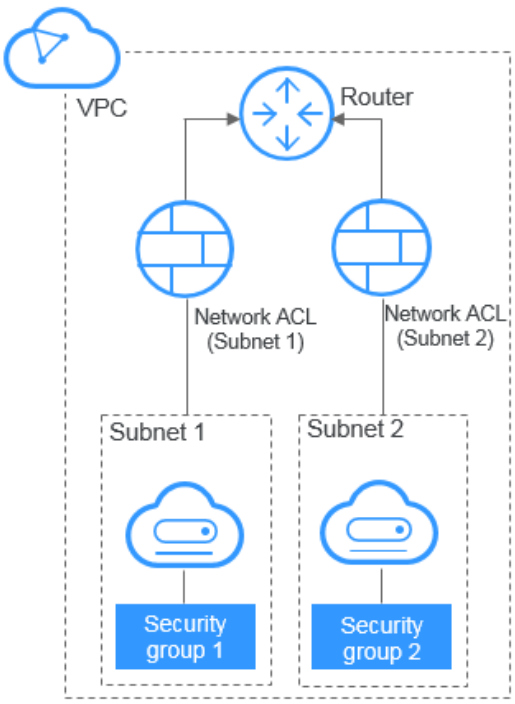
2.2 ACLs da rede

2.2.1 Visão geral de ACLs da rede

Uma ACLs da rede é uma camada opcional de segurança para suas sub-redes. Depois de associar uma ou mais sub-redes a uma ACLs da rede, você pode controlar o tráfego dentro e fora das sub-redes.

Figura 2-13 mostra como funciona uma network ACL.

Figura 2-13 Grupos de segurança e ACLs de rede



Semelhante aos grupos de segurança, as ACLs da rede controla o acesso às sub-redes e adiciona uma camada adicional de defesa às sub-redes. Os grupos de segurança têm apenas as regras "allow", mas as ACLs da rede têm regras "allow" e "deny". Você pode usar ACLs da rede junto com grupos de segurança para implementar controle de acesso abrangente e refinado.

Diferenças entre grupos de segurança e ACLs da redes resume as diferenças básicas entre grupos de segurança e ACLs da rede.

Noções básicas de ACLs da rede

- Sua VPC não vem com uma ACLs da rede, mas você pode criar uma ACLs da rede e associá-la a uma sub-rede da VPC, se necessário. Por padrão, cada uma ACLs da rede nega todo o tráfego de entrada e de saída da sub-rede associada até que você adicione regras.
- Você pode associar uma ACLs da rede com várias sub-redes. No entanto, uma sub-rede só pode ser associada a uma ACL da rede de cada vez.
- Cada ACLs da rede recém-criada está no estado **Inactive** até que você associe sub-redes a ele.
- ACLs da redes são com status. Se você enviar uma solicitação de sua instância e o tráfego de saída for permitido, o tráfego de resposta para essa solicitação poderá fluir independentemente das regras de ACLs da rede. Da mesma forma, se o tráfego de entrada for permitido, as respostas ao tráfego de entrada permitido poderão fluir para fora, independentemente das regras de saída.

  O período de tempo limite de rastreamento de conexão varia de acordo com o protocolo. O período de tempo limite de uma conexão TCP no estado estabelecido é de 600s, e o período de tempo limite de uma conexão ICMP é de 30s. Para outros protocolos, se os pacotes forem recebidos em ambas as direções, o período de tempo limite de rastreamento de conexão será de 180s. Se um ou mais pacotes forem recebidos em uma direção, mas nenhum pacote for recebido na outra direção, o período de tempo limite de rastreamento de conexão será de 30s. Para protocolos diferentes de TCP, UDP e ICMP, apenas o endereço IP e o número do protocolo são rastreados.

Regras padrão de ACLs da rede

Por padrão, cada ACLs da rede tem regras predefinidas que permitem os seguintes pacotes:

- Pacotes cuja origem e destino estão na mesma sub-rede
- Pacotes de transmissão com o destino 255.255.255.255/32, que é usado para configurar informações de inicialização do host.
- Pacotes de multicast com o destino 224.0.0.0/24, que é usado por protocolos de roteamento.
- Pacotes de metadados com o destino 169.254.169.254/32 e número de porta TCP 80, que é usado para obter metadados.
- Pacotes de blocos CIDR que são reservados para serviços públicos (por exemplo, pacotes com o destino 100.125.0.0/16)
- Uma ACLs da rede nega todo o tráfego de entrada e saída de uma sub-rede, exceto os anteriores. **Tabela 2-12** mostra as regras padrão de ACL da rede. Não é possível modificar ou excluir as regras padrão.

Tabela 2-12 Regras padrão de ACLs da rede

Direção	Prioridade	Ação	Protocolo	Origem	Destino	Descrição
Entrada	*	Negar	Todos	0.0.0.0/0	0.0.0.0/0	Nega todo o tráfego de entrada.
Saída	*	Negar	Todos	0.0.0.0/0	0.0.0.0/0	Nega todo o tráfego de saída.

Prioridades da regra

- Cada regra de ACLs da rede tem um valor de prioridade em que um valor menor corresponde a uma prioridade mais alta. Toda vez que duas regras entram em conflito, a regra com a prioridade mais alta é a que é aplicada. A regra cujo valor de prioridade é um asterisco (*) tem a prioridade mais baixa.
- Se várias regras de ACLs da rede conflitarem, somente a regra com a prioridade mais alta entra em vigor. Se você precisar que uma regra entre em vigor antes ou depois de uma regra específica, poderá inserir essa regra antes ou depois da regra específica.

Cenários de aplicação

- Se a camada de aplicação precisar fornecer serviços para os usuários, o tráfego deve ser permitido para alcançar a camada de aplicação a partir de todos os endereços IP. No entanto, você também precisa impedir o acesso ilegal de usuários maliciosos.

  Solução: você pode adicionar regras de ACLs da rede para negar acesso a endereços IP suspeitos.
- Como posso isolar portas com vulnerabilidades identificadas? Por exemplo, como faço para isolar a porta 445 que pode ser explorada pelo worm WannaCry?

  Solução: você pode adicionar regras de ACLs da rede para negar o tráfego de acesso de uma porta e protocolo específicos, por exemplo, a porta TCP 445.
- Nenhuma defesa é necessária para a comunicação dentro de uma sub-rede, mas o controle de acesso é necessário para a comunicação entre sub-redes.

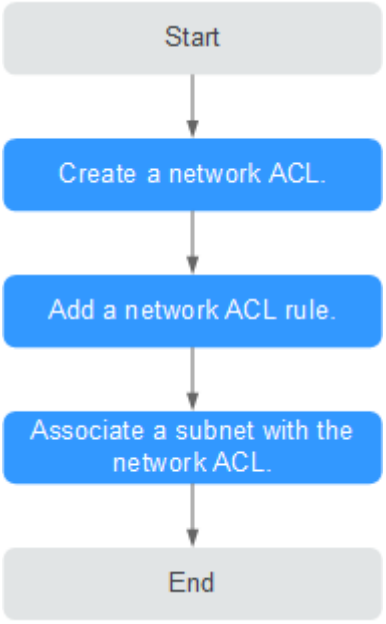
  Solução: você pode adicionar regras de ACLs da rede para controlar o tráfego entre sub-redes.
- Para aplicações acessadas com frequência, uma sequência de regras de segurança pode precisar ser ajustada para melhorar o desempenho.

  Solução: uma ACLs da rede permite ajustar a sequência de regras para que as regras usadas com frequência sejam aplicadas antes de outras regras.

Procedimento de configuração

Figura 2-14 mostra o procedimento para configurar uma ACL da rede.

Figura 2-14 ACLs da rede procedimento da configuração



1. Crie uma ACLs da rede seguindo as etapas descritas em **Criação de uma ACLs da rede**.
2. Adicione regras de ACLs da rede seguindo as etapas descritas em **Adição uma regra de ACLs da rede**.
3. Associe sub-redes à ACLs da rede seguindo as etapas descritas em **Associação de sub-redes com uma ACLs da rede**. Depois que as sub-redes forem associadas à ACL da rede, as sub-redes serão protegidas pelas regras de ACL da rede configuradas.

Restrições de ACL da rede

- Por padrão, você pode criar um máximo de 200 ACLs da redes em sua conta de nuvem.
- Uma ACLs da rede pode conter não mais do que 20 regras em uma direção, ou o desempenho irá se deteriorar.
- Para um desempenho ideal, não importe mais de 40 regras de ACLs da rede por vez. As regras existentes ainda estarão disponíveis após as novas regras terem sido importadas. Cada regra pode ser importada apenas uma vez.

2.2.2 Exemplos de configuração de ACLs da rede

Esta seção fornece exemplos para configurar as ACLs da redes.

- **Negar acesso de uma porta específica**
- **Permitir acesso a partir de portas e protocolos específicos**
- **Negar acesso a partir de um endereço IP específico**

Negar acesso de uma porta específica

Você pode querer bloquear o TCP 445 para proteger contra os ataques de WannaCry ransomware. Você pode adicionar uma regra de ACLs da rede para negar todo o tráfego de entrada da porta TCP 445.

ACLs da rede Configuração

Tabela 2-13 lista a regra de entrada necessária.

Tabela 2-13 Regras de ACLs da rede

Direção	Ação	Protocolo	Origem	Intervalo de porta de origem	Destino	Intervalo de porta de destino	Descrição
Entrada	Negar	TCP	0.0.0.0/0	1-65535	0.0.0.0/0	445	Nega o tráfego de entrada de qualquer endereço IP através da porta TCP 445.
Entrada	Permitir	Todos	0.0.0.0/0	1-65535	0.0.0.0/0	Todos	Permite todo o tráfego de entrada.

NOTA

- Por padrão, uma ACLs da rede nega todo o tráfego de entrada. Você precisa permitir todo o tráfego de entrada, se necessário.
- Se quiser que uma regra de negação seja correspondida primeiro, insira a regra de negação acima da regra de permissão. Para mais detalhes, consulte **Alteração da sequência de uma regra de ACLs da rede**.

Permitir acesso a partir de portas e protocolos específicos

Neste exemplo, um ECS em uma sub-rede é usado como servidor Web e você precisa permitir o tráfego de entrada da porta HTTP 80 e da porta HTTPS 443 e permitir todo o tráfego de saída. Você precisa configurar ambas as regras de ACLs da rede e regras de grupo de segurança para permitir o tráfego.

ACLs da rede Configuração

Tabela 2-14 lista a regra de entrada necessária.

Tabela 2-14 Regras de ACLs da rede

Direção	Ação	Protocolo	Origem	Intervalo de porta de origem	Destino	Intervalo de porta de destino	Descrição
Entrada	Permitir	TCP	0.0.0.0/0	1-65535	0.0.0.0/0	80	Permite o tráfego HTTP de entrada de qualquer endereço IP para ECSs na sub-rede através da porta 80.

Direção	Ação	Protocolo	Origem	Intervalo de porta de origem	Destino	Intervalo de porta de destino	Descrição
Entrada	Permitir	TCP	0.0.0.0/0	1-65535	0.0.0.0/0	443	Permite o tráfego HTTPS de entrada de qualquer endereço IP para ECSs na sub-rede através da porta 443.
Saída	Permitir	Todos	0.0.0.0/0	Todos	0.0.0.0/0	Todos	Permite todo o tráfego de saída da sub-rede.

Configuração do grupo de segurança

Tabela 2-15 lista as regras de grupo de segurança de entrada e saída necessárias.

Tabela 2-15 Regras de grupos de segurança

Direção	Protocolo / Aplicação	Porta	Origem/Destino	Descrição
Entrada	TCP	80	Origem: 0.0.0.0/0	Permite tráfego HTTP de entrada de qualquer endereço IP para ECSs associados ao grupo de segurança por meio da porta 80.
Entrada	TCP	443	Origem: 0.0.0.0/0	Permite tráfego HTTPS de entrada de qualquer endereço IP para ECSs associados ao grupo de segurança por meio da porta 443.
Saída	Todos	Todos	Destino: 0.0.0.0/0	Permite todo o tráfego de saída do grupo de segurança.

Uma ACLs da rede adiciona uma camada adicional de segurança. Mesmo que as regras do grupo de segurança permitam mais tráfego do que o realmente necessário, as regras de ACLs da rede permitem apenas o acesso da porta HTTP 80 e da porta HTTPS 443 e negam outro tráfego de entrada.

Negar acesso a partir de um endereço IP específico

Neste exemplo, você pode adicionar uma ACLs da rede regra para negar o acesso de alguns endereços IP anormais, por exemplo, 192.168.1.102.

ACLs da rede Configuração

Tabela 2-16 lista as regras de entrada necessárias.

Tabela 2-16 Regras de ACLs da rede

Direção	Ação	Protocolo	Origem	Intervalo de porta de origem	Destino	Intervalo de porta de destino	Descrição
Entrada	Negar	TCP	192.168.1.102/32	1-65535	0.0.0.0/0	Todos	Nega acesso a partir de 192.168.1.102.
Entrada	Permitir	Todos	0.0.0.0/0	1-65535	0.0.0.0/0	Todos	Permite todo o tráfego de entrada.

NOTA

- Por padrão, uma ACLs da rede nega todo o tráfego de entrada. Você precisa permitir todo o tráfego de entrada, se necessário.
- Se quiser que uma regra de negação seja correspondida primeiro, insira a regra de negação acima da regra de permissão. Para mais detalhes, consulte **Alteração da sequência de uma regra de ACLs da rede**.

2.2.3 Criação de uma ACLs da rede

Cenários

Você pode criar uma ACLs da rede personalizada, mas qualquer ACLs da rede recém-criada será desativada por padrão. Ela não terá regras de entrada ou saída, nem terá sub-redes associadas. Cada usuário pode criar até 200 ACLs da redes por padrão.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Access Control** > **ACLs da redes**.
5. No painel direito exibido, clique em **Create ACLs da rede**.
6. Na caixa de diálogo exibida, insira as informações de ACLs da rede conforme solicitado. Tabela 2-17 lista os parâmetros a serem configurados.

Figura 2-15 Criar ACLs da rede

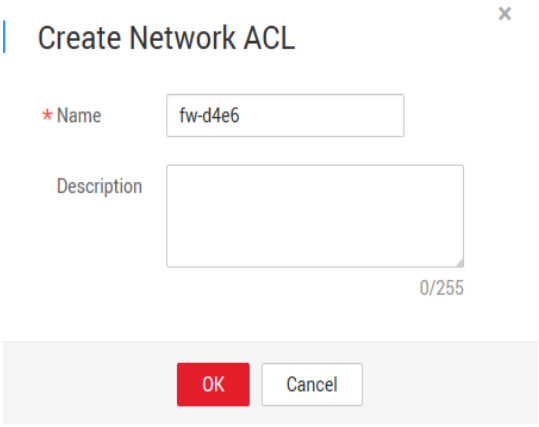


Tabela 2-17 Descrições de parâmetro

Parâmetro	Descrição	Exemplo de valor
Name	O nome da ACLs da rede. Este parâmetro é obrigatório. O nome contém um máximo de 64 caracteres, que podem consistir em letras, dígitos, sublinhados (_) e hifens (-). O nome não pode conter espaços.	fw-92d3
Description	Informação complementar sobre a ACLs da rede. Este parâmetro é opcional. A descrição pode conter no máximo 255 caracteres e não pode conter colchetes angulares (< ou >).	N/A

7. Clique em **OK**.

2.2.4 Adição uma regra de ACLs da rede

Cenários

Adicionar uma regra de entrada ou de saída com base nos requisitos de segurança da sua rede.

Recomenda-se que uma ACLs da rede não contenha mais de 20 regras em uma direção. Caso contrário, seu desempenho pode se deteriorar.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.

4. No painel de navegação à esquerda, escolha **Access Control** > **ACLs da redes**.
5. Localize a ACLs da rede de destino e clique em seu nome para alternar para a página que mostra detalhes dessa ACLs da rede particular.
6. Na guia **Inbound Rules** ou **Outbound Rules**, clique em **Add Rule** para adicionar uma regra de entrada ou de saída.
   - Clique em + para adicionar mais regras.
   - Localize a linha que contém a regra de ACLs da rede e clique em **Replicate** na coluna **Operation** para replicar uma regra existente.

Tabela 2-18 Descrições de parâmetro

Parâmetro	Descrição	Exemplo de valor
Priority	Prioridade da regra de ACLs da rede. Um valor de prioridade menor representa uma prioridade mais alta. Cada ACL de rede inclui uma regra padrão cujo valor de prioridade é um asterisco (*). As regras padrão têm a prioridade mais baixa.	3
Status	Status de ACLs da rede. Quando você adiciona uma regra a ela, seu status padrão é **Enabled**.	Enabled
Type	Este parâmetro só está disponível depois de ativada a função IPv6. O tipo de ACLs da rede. Este parâmetro é obrigatório. Você pode selecionar um valor na lista suspensa. Atualmente, apenas **IPv4** e **IPv6** são suportados.	IPv4
Action	A ação na ACLs da rede. Este parâmetro é obrigatório. Você pode selecionar um valor na lista suspensa. Atualmente, o valor pode ser **Allow** ou **Deny**.	Allow
Protocol	O protocolo suportado pela ACLs da rede. Este parâmetro é obrigatório. Você pode selecionar um valor na lista suspensa. O valor pode ser **TCP**, **UDP**, **All** ou **ICMP**. Se **ICMP** ou **All** estiver selecionado, não é necessário especificar informações de porta.	TCP

Parâmetro	Descrição	Exemplo de valor
Source	A origem a partir da qual o tráfego é permitido. A origem pode ser um endereço IP, um grupo de endereços IP ou um intervalo de endereços IP. O valor padrão é **0.0.0.0/0**, que indica que o tráfego de todos os endereços IP é permitido. A origem ou o destino podem usar o grupo de endereços IP. Por exemplo: ● Endereço IP único: 192.168.10.10/32 (IPv4); 2002:50::44/127 (IPv6) ● Intervalo de endereço IP: 192.168.1.0/24 (IPv4); 2407:c080:802:469::/64 (IPv6) ● Todos os endereços IP 0.0.0.0/0 (IPv4); ::/0 (IPv6)	0.0.0.0/0
Source Port Range	O número da porta de origem ou o intervalo do número da porta. O valor varia de 1 a 65535. Para um intervalo de números de porta, insira dois números de porta conectados por um hífen (-). Por exemplo, **1-100**. Você deve especificar esse parâmetro se **TCP** ou **UDP** estiver selecionado para **Protocol**.	22, ou 22-30
Destination	O destino para o qual o tráfego é permitido. A origem pode ser um endereço IP, um grupo de endereços IP ou um intervalo de endereços IP. O valor padrão é **0.0.0.0/0**, que indica que o tráfego para todos os endereços IP é permitido. A origem ou o destino podem usar o grupo de endereços IP. Por exemplo: ● Endereço IP único: 192.168.10.10/32 (IPv4); 2002:50::44/127 (IPv6) ● Intervalo de endereços IP: 192.168.1.0/24 (IPv4); 2407:c080:802:469::/64 (IPv6) ● Todos os endereços IP: 0.0.0.0/0 (IPv4); ::/0 (IPv6)	0.0.0.0/0
Destination Port Range	O número de porta de destino ou o intervalo de números de porta. O valor varia de 1 a 65535. Para um intervalo de números de porta, insira dois números de porta conectados por um hífen (-). Por exemplo, **1-100**. Você deve especificar esse parâmetro se **TCP** ou **UDP** estiver selecionado para **Protocol**.	22 ou 22-30

Parâmetro	Descrição	Exemplo de valor
Description	Informação complementar sobre a regra de ACLs da rede. Este parâmetro é opcional. A descrição pode conter no máximo 255 caracteres e não pode conter colchetes angulares (< ou >).	N/A

7. Clique em **OK**.

2.2.5 Associação de sub-redes com uma ACLs da rede

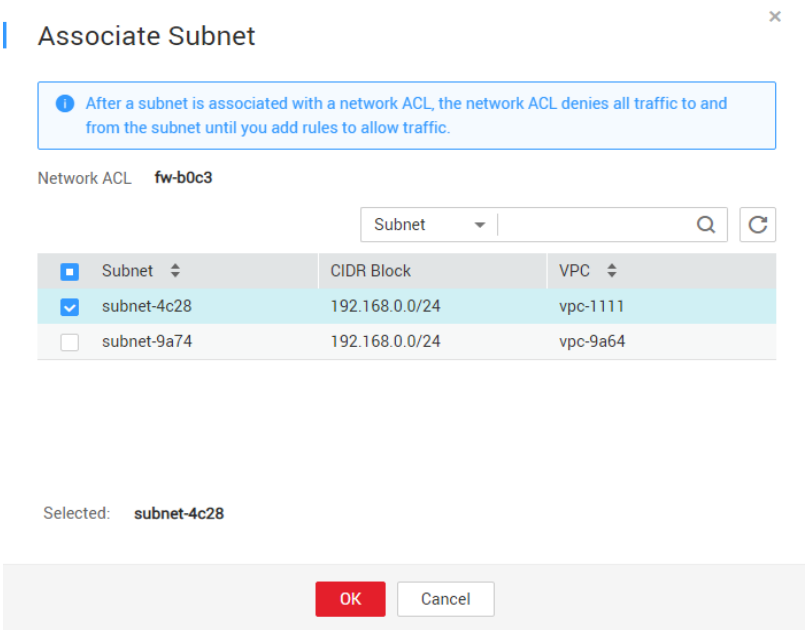
Cenários

Na página que mostra os detalhes de ACLs da rede, associe as sub-redes desejadas a uma ACLs da rede. Depois que uma ACLs da rede é associado a uma sub-rede, a ACLs da rede nega todo o tráfego de e para a sub-rede até que você adicione regras para permitir o tráfego.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Access Control** > **ACLs da redes**.
5. Localize a ACLs da rede de destino e clique em seu nome para alternar para a página que mostra detalhes dessa ACLs da rede particular.
6. Na página exibida, clique na guia **Associated Subnets**.
7. Na página **Associated Subnets**, clique em **Associate**.

Figura 2-16 Associar sub-rede



8. Na página exibida, selecione as sub-redes a serem associadas a ACLs da rede e clique em **OK**.

NOTA

As sub-redes que já foram associadas a ACLs da redes não serão exibidas na página a ser selecionada. A associação e desassociação de sub-rede com um clique não são suportadas atualmente. Além disso, uma sub-rede só pode ser associada a uma ACLs da rede. Se você deseja reassociar uma sub-rede que já foi associada a outra ACLs da rede, primeiro você deve desassociar a sub-rede da ACLs da rede original.

2.2.6 Desassociação de uma sub-rede de uma ACLs da rede

Cenários

Desassociar uma sub-rede de uma ACLs da rede quando necessário.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Access Control** > **ACLs da redes**.
5. Localize a ACLs da rede de destino e clique em seu nome para alternar para a página que mostra detalhes dessa ACLs da rede particular.
6. Na página exibida, clique na guia **Associated Subnets**.
7. Na página **Associated Subnets**, localize a linha que contém a sub-rede de destino e clique em **Disassociate** na coluna **Operation**.
8. Clique em **Yes** na caixa de diálogo exibida.

Desassociar sub-redes de uma ACLs da rede

Selecione várias sub-redes e clique em **Disassociate** acima da lista de sub-redes para desassociar as sub-redes da atual ACLs da rede por vez.

2.2.7 Alteração da sequência de uma regra de ACLs da rede

Cenários

Se você precisar que uma regra entre em vigor antes ou depois de uma regra específica, poderá inserir essa regra antes ou depois da regra específica.

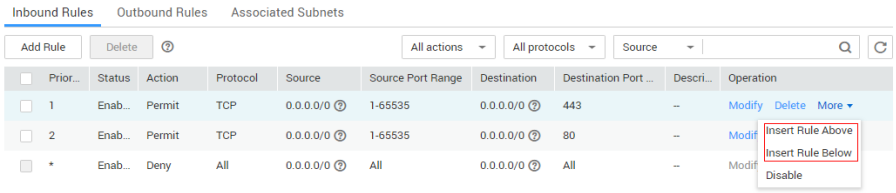
Se várias regras de ACLs da rede conflitarem, somente a regra com a prioridade mais alta entra em vigor.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Access Control** > **ACLs da redes**.

5. Localize a ACLs da rede de destino e clique em seu nome para alternar para a página que mostra detalhes dessa ACLs da rede particular.
6. Na guia **Inbound Rules** ou **Outbound Rules**, localize a regra de destino, clique em **More** na coluna **Operation** e selecione **Insert Rule Above** ou **Insert Rule Below**.

Figura 2-17 Inserir uma regra



7. Na caixa de diálogo exibida, configure os parâmetros necessários e clique em **OK**.

   A regra é inserida. O procedimento para inserir uma regra de saída é o mesmo que para inserir uma regra de entrada.

2.2.8 Modificação de uma regra de ACLs da rede

Cenários

Modificar uma regra de entrada ou de saída de ACLs da rede com base nos requisitos de segurança da sua rede.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Access Control** > **ACLs da redes**.
5. Localize a ACLs da rede de destino e clique em seu nome para alternar para a página que mostra detalhes dessa ACLs da rede particular.
6. Na guia **Inbound Rules** ou **Outbound Rules**, localize a linha que contém a regra de destino e clique em **Modify** na coluna **Operation**. Na caixa de diálogo exibida, configure os parâmetros conforme solicitado. **Tabela 2-19** lista os parâmetros a serem configurados.

Tabela 2-19 Descrições de parâmetro

Parâmetro	Descrição	Exemplo de valor
Priority	Prioridade da regra de ACLs da rede. Um valor de prioridade menor representa uma prioridade mais alta. Cada ACL de rede inclui uma regra padrão cujo valor de prioridade é um asterisco (*). As regras padrão têm a prioridade mais baixa.	3

Parâmetro	Descrição	Exemplo de valor
Status	Status de ACLs da rede. Quando você adiciona uma regra a ela, seu status padrão é **Enabled**.	Enabled
Type	Este parâmetro só está disponível depois de ativada a função IPv6. O tipo de ACLs da rede. Este parâmetro é obrigatório. Você pode selecionar um valor na lista suspensa. Atualmente, apenas **IPv4** e **IPv6** são suportados.	IPv4
Action	A ação na ACLs da rede. Este parâmetro é obrigatório. Você pode selecionar um valor na lista suspensa. Atualmente, o valor pode ser **Allow** ou **Deny**.	Allow
Protocol	O protocolo suportado pela ACLs da rede. Este parâmetro é obrigatório. Você pode selecionar um valor na lista suspensa. O valor pode ser **TCP**, **UDP**, **All** ou **ICMP**. Se **ICMP** ou **All** estiver selecionado, não é necessário especificar informações de porta.	TCP
Source	A origem a partir da qual o tráfego é permitido. A origem pode ser um endereço IP, um grupo de endereços IP ou um intervalo de endereços IP. O valor padrão é **0.0.0.0/0**, que indica que o tráfego de todos os endereços IP é permitido. A origem ou o destino podem usar o grupo de endereços IP. Por exemplo: ● Endereço IP único: 192.168.10.10/32 (IPv4); 2002:50::44/127 (IPv6) ● Intervalo de endereço IP: 192.168.1.0/24 (IPv4); 2407:c080:802:469::/64 (IPv6) ● Todos os endereços IP 0.0.0.0/0 (IPv4); ::/0 (IPv6)	0.0.0.0/0
Source Port Range	O número da porta de origem ou o intervalo do número da porta. O valor varia de 1 a 65535. Para um intervalo de números de porta, insira dois números de porta conectados por um hífen (-). Por exemplo, **1-100**. Você deve especificar esse parâmetro se **TCP** ou **UDP** estiver selecionado para **Protocol**.	22, ou 22-30

Parâmetro	Descrição	Exemplo de valor
Destination	O destino para o qual o tráfego é permitido. A origem pode ser um endereço IP, um grupo de endereços IP ou um intervalo de endereços IP. O valor padrão é **0.0.0.0/0**, que indica que o tráfego para todos os endereços IP é permitido. A origem ou o destino podem usar o grupo de endereços IP. Por exemplo: ● Endereço IP único: 192.168.10.10/32 (IPv4); 2002:50::44/127 (IPv6) ● Intervalo de endereços IP: 192.168.1.0/24 (IPv4); 2407:c080:802:469::/64 (IPv6) ● Todos os endereços IP: 0.0.0.0/0 (IPv4); ::/0 (IPv6)	0.0.0.0/0
Destination Port Range	O número de porta de destino ou o intervalo de números de porta. O valor varia de 1 a 65535. Para um intervalo de números de porta, insira dois números de porta conectados por um hífen (-). Por exemplo, **1-100**. Você deve especificar esse parâmetro se **TCP** ou **UDP** estiver selecionado para **Protocol**.	22 ou 22-30
Description	Informação complementar sobre a regra de ACLs da rede. Este parâmetro é opcional. A descrição pode conter no máximo 255 caracteres e não pode conter colchetes angulares (< ou >).	N/A

7. Clique em **Confirm**.

2.2.9 Ativação ou desativação de uma regra de ACLs da rede

Cenários

Ativar ou desativar uma regra de entrada ou saída com base nos requisitos de segurança da rede.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Access Control** > **ACLs da redes**.

5. Localize a ACL da rede de destino e clique em seu nome para alternar para a página que mostra detalhes dessa ACLs da rede particular.
6. Na guia **Inbound Rules** ou **Outbound Rules**, localize a linha que contém a regra de destino e clique em **More** e, em seguida **Enable** ou **Disable** na coluna **Operation**.
7. Clique em **Yes** na caixa de diálogo exibida.

   A regra está ativada ou desativada. O procedimento para ativar ou desativar uma regra de saída é o mesmo que para ativar ou desativar uma regra de entrada.

2.2.10 Exclusão de uma regra de ACLs da rede

Cenários

Excluir uma regra de entrada ou saída com base nos requisitos de segurança da rede.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Access Control** > **ACLs da rede**.
5. Localize a ACLs da rede de destino e clique em seu nome para alternar para a página que mostra detalhes dessa ACLs da rede particular.
6. Na guia **Inbound Rules** ou **Outbound Rules**, localize a linha que contém a regra de destino e clique em **Delete** na coluna **Operation**.
7. Clique em **Yes** na caixa de diálogo exibida.

Excluir várias regras da ACL da rede de por vez

Você também pode selecionar várias regras de ACLs da rede e clicar em **Delete** acima da lista de regras de ACLs da rede para excluir várias regras por vez.

2.2.11 Exportação e importação de regras de ACLs da rede

Cenários

Você pode exportar regras de entrada e saída de uma ACLs da rede específica como um arquivo do Excel, em seguida, importar essas regras para outro ACLs da rede. Exportação e importação de regras entre regiões são suportadas.

Recomenda-se que você não importe mais de 40 regras de cada vez. A importação de regras não excluirá as regras existentes. Regras duplicadas não são permitidas.

Exportação de regras de ACLs da rede

1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Access Control** > **ACLs da redes**.

5. Localize a ACLs da rede de destino e clique em seu nome para alternar para a página que mostra detalhes dessa ACLs da rede particular.
6. Clique em  para exportar as regras de entrada e saída de ACLs da rede. As regras exportadas são armazenadas em um arquivo do Excel. Você precisa baixar o arquivo para um diretório local.

Importação de regras de ACLs da rede

1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Access Control** > **ACLs da redes**.
5. Localize a ACLs da rede de destino e clique em seu nome para alternar para a página que mostra detalhes dessa ACLs da rede particular.
6. Clique em  .
7. Selecione o arquivo do Excel que contém as regras exportadas de ACL da rede clique em **Import** para importar as regras.

2.2.12 Visualização de uma ACLs da rede

Cenários

Ver detalhes sobre uma ACLs da rede.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Access Control** > **ACLs da redes**.
5. Localize a ACLs da rede de destino e clique em seu nome para alternar para a página que mostra detalhes dessa ACLs da rede particular.
6. Na página exibida, clique nas guias **Inbound Rules**, **Outbound Rules** e **Associated Subnets** uma a uma, para exibir detalhes sobre regras de entrada, regras de saída e associações de sub-rede.

2.2.13 Modificação de uma ACLs da rede

Cenários

Modificar o nome e a descrição de uma ACLs da rede.

Procedimento

1. Acesse o console de gerenciamento.

2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Access Control** > **ACLs da redes**.
5. Localize a ACLs da rede de destino e clique em seu nome para alternar para a página que mostra detalhes dessa ACLs da rede particular.
6. Na página exibida, clique em à direita de **Name** e edite o nome de ACLs da rede.
7. Clique em √ para salvar o novo nome de ACLs da rede.
8. Clique em à direita de Descrição e edite a descrição de ACLs da rede.
9. Clique em √ para salvar a nova descrição de ACLs da rede.

2.2.14 Ativação ou desativação de uma ACLs da rede

Cenários

Depois que uma ACLs da rede é criada, talvez seja necessário ativá-la com base nos requisitos de segurança da rede. Você também pode desativar uma ACLs da rede ativada, se necessário. Antes de ativar uma ACLs da rede, certifique-se de que as sub-redes tenham sido associadas à ACLs da rede e que as regras de entrada e saída tenham sido adicionadas à ACLs da rede.

Quando uma ACLs da rede é desativada, as regras personalizadas se tornarão inválidas enquanto as regras padrão ainda entrarem em vigor. Desativar uma ACLs da rede pode interromper o tráfego de rede. Para obter informações sobre as regras de ACLs da rede padrão, consulte **Regras padrão de ACLs da rede**.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Access Control** > **ACLs da redes**.
5. Localize a linha que contém a ACLs da rede de destino no painel direito, clique em **More** na coluna **Operation** e clique em **Enable** ou **Disable**.
6. Clique em **Yes** na caixa de diálogo exibida.

2.2.15 Exclusão de uma ACLs da rede

Cenários

Excluir uma ACL da rede quando ele não for mais necessário.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.

3. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Access Control** > **ACLs da redes**.
5. Localize a ACLs da rede de destino no painel direito, clique em **More** na coluna **Operation** e clique em **Delete**.
6. Clique em **Yes**.

NOTA

Depois que uma ACLs da rede é excluída, as sub-redes associadas são desassociadas e as regras adicionadas são excluídas da ACLs da rede.

2.3 Diferenças entre grupos de segurança e ACLs da redes

Você pode configurar grupos de segurança e ACLs da rede para aumentar a segurança dos ECSs na sua VPC.

- Os grupos de segurança operam no nível do ECS.
- ACLs da redes operam no nível da sub-rede.

Para mais detalhes, consulte **Figura 2-18**.

Figura 2-18 Grupos de segurança e ACLs de rede

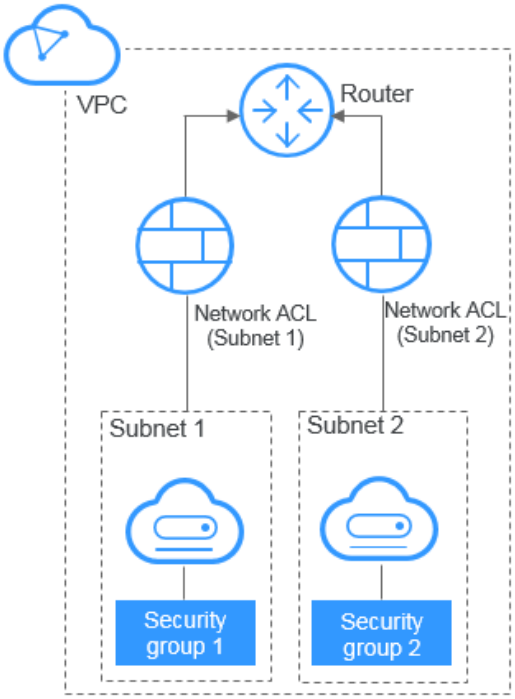


Tabela 2-20 descrACLs da redegurança e ACL da rede.

Tabela 2-20 Diferenças entre grupos de segurança e ACLs da redes

Categoria	Grupo de segurança	ACLs da rede
Alvos	Opera no nível ECS.	Opera no nível da sub-rede.
Regras	Permite tanto regras **Allow** quanto **Deny**. As regras de negação são suportadas apenas em determinadas regiões. Você pode ir para **Visão geral da função** e clicar em **Security Group** para exibir as regiões.	Permite tanto regras **Allow** quanto **Deny**.
Prioridade	Se houver regras conflitantes, as regras entram em vigor com base na sequência de seu grupo de segurança em associação com um recurso e, em seguida, com base nas prioridades da regra no grupo.	Se as regras entrarem em conflito, a regra com a prioridade mais alta entra em vigor.
Utilização	Aplica-se automaticamente aos ECSs no grupo de segurança selecionado durante a criação do ECS. Você deve selecionar um grupo de segurança ao criar ECSs.	Aplica-se a todos os ECSs nas sub-redes associadas à ACLs da rede. A seleção de uma ACLs da rede não é permitida durante a criação da sub-rede. Você deve criar uma ACLs da rede, associar sub-redes a ele, adicionar regras de entrada e saída e ativar ACLs da rede. Em seguida, a ACLs da rede entra em vigor para as sub-redes associadas e ECSs nas sub-redes.
Pacotes	Filtragem de pacotes possível apenas com base no 3-tuplo (protocolo, porta e endereço IP de par).	Filtragem de pacotes possível apenas com base no 5-tuplo (protocolo, porta de origem, porta de destino, endereço IP de origem e endereço IP de destino).

2.4 Grupo de endereços IP

2.4.1 Visão geral do grupo de endereços IP

Um grupo de endereços IP é uma coleção de endereços IP que pode usar as mesmas regras de grupo de segurança. Você pode usar um grupo de endereços IP para gerenciar endereços IP que têm requisitos de segurança iguais ou que não são alterados frequentemente.

Você pode criar um grupo de endereços IP e adicionar endereços IP que precisam ser gerenciados de maneira unificada ao grupo. Em seguida, você pode selecionar esse grupo de endereços IP ao configurar uma regrade grupo de segurança. A regra entrará em vigor para todos os endereços IP no grupo de endereços IP.

2.4.2 Criação de um grupo de endereços IP

Cenários

Criar um grupo de endereços IP e adicionar endereços IP que precisam ser gerenciados centralmente a esse grupo.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, em **Networking**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Access Control** > **IP Address Groups**.
5. Clique em **Create IP Address Group**.
6. Configure os parâmetros necessários. **Tabela 2-21** lista os parâmetros do grupo de endereços IP.

Tabela 2-21 Descrições de parâmetro

Parâmetro	Descrição	Exemplo de valor
Name	O nome do grupo de endereços IP. Este parâmetro é obrigatório. O nome do grupo de endereços IP contém no máximo 64 caracteres, que podem consistir em letras, dígitos, sublinhados (_), hifens (-) e pontos (.). O nome não pode conter espaços. Você pode personalizar o nome de um grupo de endereços IP identificado exclusivamente por seu ID.	ipGroup-f7de
IP Address Version	Obrigatório Atualmente, as seguintes versões de endereço IP são suportadas: ● IPv4 ● IPv6	IPv4

Parâmetro	Descrição	Exemplo de valor
IP Address	Insira um intervalo de endereços IPv4 ou IPv6, ou endereços. Você pode adicionar um máximo de 20 endereços IP e intervalos de endereços IP, e cada um deve estar em uma linha separada. Formatos suportados: ● IPv4 – Intervalo de endereços IP: por exemplo, 192.168.0.0/16 – Endereços IP consecutivos separam por um hífen (-): por exemplo, 192.168.1.1-192.168.1.50 – Endereço IP único: por exemplo, 192.168.10.10 ● IPv6 – Intervalo de endereço IPv6: por exemplo, 2001:db8:a583:6e::/64 – Endereços IPv6 consecutivos separados por um hífen (-): por exemplo, 2001:db8:a583:6e::1-2001:db8:a583:6e::50 – Endereço IPv6 único: por exemplo, 2001:db8:a583:6e::5c	192.168.0.0/16 192.168.1.1-192.168.1.50 192.168.10.10
Description	Informação complementar sobre o grupo de endereço IP. Este parâmetro é opcional. A descrição do grupo de endereços IP pode conter no máximo 255 caracteres e não pode conter colchetes angulares (< ou >).	N/A

7. Clique em **OK**.

2.4.3 Associação de um grupo de endereços IP a uma regra de grupo de segurança

Cenários

Selecionar um grupo de endereços IP ao adicionar uma regra de grupo de segurança para que a regra se aplique a todos os endereços IP no grupo de endereços IP.

Procedimento

Adicione uma regra de grupo de segurança referindo-se a **Adição de uma regra de grupo de segurança**. Preste atenção ao seguinte:

1. Selecione **IP address group** na lista suspensa para **Source**.
2. Selecione o grupo de endereços IP de destino.

Após as etapas anteriores, o grupo de endereços IP pode ser associado à regra do grupo de segurança.

2.4.4 Gerenciamento de um grupo de endereços IP

Cenários

Modificar ou eliminar um grupo de endereços de IP.

NOTA

- Depois que um grupo de endereços IP for modificado, os endereços de origem de suas regras de grupo de segurança associadas também serão alterados.
- A exclusão de um grupo de endereços IP também excluirá as regras de grupo de segurança associadas ao grupo de endereços IP.

Modificar um grupo de endereços IP

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, em **Networking**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Access Control** > **IP Address Groups**.
5. Na página exibida, clique em **Modify** na coluna **Operation** para modificar o nome, o endereço IP e a descrição do grupo de endereços IP.

Excluir um grupo de endereços IP

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, em **Networking**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Access Control** > **IP Address Groups**.
5. Na página **IP Address Groups**, localize o grupo de endereços IP de destino e clique em **Delete** na coluna **Operation**. Na caixa de diálogo exibida, clique em **Yes**.

   A exclusão de um grupo de endereços IP também excluirá as regras do grupo de segurança associadas ao grupo de endereços IP.

3 Elastic IP

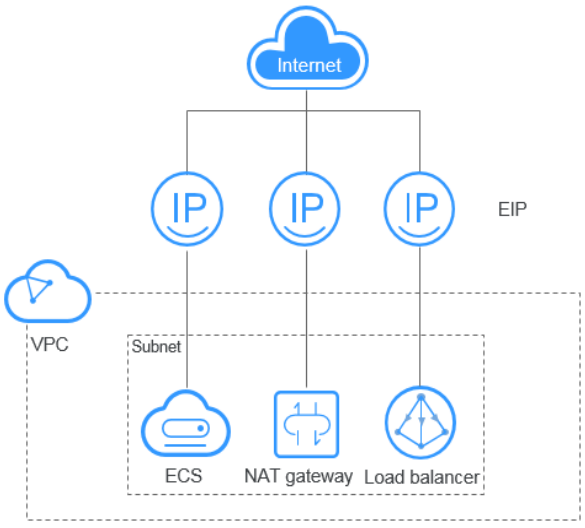
3.1 Visão geral do EIP

EIP

Elastic IP (EIP) permite que você utilize endereços IP públicos estáticos e larguras de banda escaláveis para ligar os seus recursos da nuvem à Internet. Os EIP podem ser vinculados ou desvinculados dos ECSs, BMS, endereços IP virtuais, gateways da NAT ou balanceadores de carga. Vários modos de cobrança são fornecidos para atender a diversos requisitos de serviço.

Cada EIP pode ser usado por apenas um recurso de nuvem por vez.

Figura 3-1 Acessar a Internet usando um EIP



Vantagens

- Flexibilidade

Um EIP pode ser associado ou desassociado de forma flexível do ECS, BMS, gateway da NAT, balanceador de carga ou endereço IP virtual. A largura de banda pode ser ajustada de acordo com as mudanças de serviço.

- Pagamento flexível

  Pagamento por uso (com base no uso de largura de banda ou quantidade de tráfego) e modos de cobrança anual mensal estão disponíveis.

- Largura de banda compartilhada

  Os EIPs podem usar a largura de banda compartilhada para reduzir os custos de largura de banda.

- Uso imediato

  Associações, dissociações de EIP e ajustes de largura de banda entram em vigor imediatamente.

NOTA

Para obter detalhes sobre como enviar um tíquete de serviço, consulte **nvio de um tíquete de serviço**.

3.2 Atribuição de um EIP e vinculação a um ECS

Cenários

Você pode atribuir um EIP e vinculá-lo a um ECS para que o ECS possa acessar a Internet.

Atribuir um EIP

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Elastic IP**.
4. Na página exibida, clique em **Buy EIP**.
5. Defina os parâmetros conforme solicitados.

Tabela 3-1 Descrições de parâmetro

Parâmetro	Descrição	Exemplo de valor
Billing Mode	Os seguintes modos de cobrança estão disponíveis: ● Anual/Mensal ● Pagamento por uso	Pagamento por uso

Parâmetro	Descrição	Exemplo de valor
Region	Regiões são áreas geográficas fisicamente isoladas umas das outras. As redes dentro de diferentes regiões não estão conectadas entre si, portanto, os recursos não podem ser compartilhados entre diferentes regiões. Para menor latência de rede e acesso mais rápido aos seus recursos, selecione a região mais próxima de você. A região selecionada para o EIP é a sua localização geográfica. **NOTA** A localização geográfica de um EIP comprado em CN North-Ulanqab1 é Pequim.	CN-Hong Kong
EIP Type	● **Dynamic BGP**: o BGP dinâmico fornece failover automático e escolhe o caminho ideal quando há falha na conexão da rede. ● **Static BGP**: o BGP estático oferece mais controle de roteamento e protege contra o flapping da rota, mas um caminho ideal não pode ser selecionado em tempo real quando uma conexão de rede falha. ● **Premium BGP**: o BGP Premium escolhe o caminho ideal e garante redes de baixa latência e alta qualidade. O BGP é usado para interconectar com linhas de várias operadoras principais. Conexões de rede pública que apresentam baixa latência e alta qualidade são estabelecidas diretamente entre a China continental e Hong Kong (China). (Esse parâmetro está disponível somente em **CN-Hong Kong**.)	Dynamic BGP

Parâmetro	Descrição	Exemplo de valor
Billed By	Esse parâmetro está disponível somente quando você define o **Billing Mode** como **Pay-per-use**. ● **Bandwidth**: você especifica uma largura de banda máxima e paga pela quantidade de tempo que você usa a largura de banda. Isso é adequado para cenários com tráfego pesado ou estável. ● **Traffic**: você especifica uma largura de banda máxima e paga pelo tráfego total usado. Isso é adequado para cenários com tráfego leve ou com flutuação acentuada. ● **Shared Bandwidth**: a largura de banda pode ser compartilhada por vários EIPs. Isso é adequado para cenários com tráfego escalonado.	Bandwidth
Bandwidth	O tamanho da largura de banda em Mbit/s.	100
EIP Name	O nome do EIP.	eip-test
Bandwidth Name	O nome da largura de banda.	bandwidth
Enterprise Project	O projeto empresarial ao qual o EIP pertence. Um projeto corporativo facilita o gerenciamento de projeto e o agrupamento de recursos da nuvem e de usuários. O nome do projeto padrão é **default**. Para obter detalhes sobre como criar e gerenciar projetos corporativos, consulte o *Enterprise Management User Guide*.	default
Advanced Settings	Clique na seta suspensa para configurar parâmetros, incluindo o nome da largura de banda e a tag.	-
Tag	As tags de EIP. Cada tag contém um par de chave e valor. A chave e o valor de tag devem atender aos requisitos listados em **Tabela 3-2**.	● Chave: Ipv4_key1 ● Valor: 192.168.12.10

Parâmetro	Descrição	Exemplo de valor
Monitoring	Usado para monitorar o EIP. Habilitado por padrão Você pode usar o console de gerenciamento ou as APIs fornecidas pelo Cloud Eye para consultar as métricas e os alarmes gerados para o EIP e a largura de banda.	-
Required Duration	A duração para a qual o EIP adquirido será usado. A duração deve ser especificada se o **Billing Mode** estiver definido como **Yearly/ Monthly**.	1 mês
Quantity	O número de EIPs que você deseja comprar. A quantidade deve ser especificada se o **Billing Mode** estiver definido como **Pay-per-use**.	1

Tabela 3-2 Requisitos da tag de EIP

Parâmetro	Requisito	Exemplo de valor
Key	● Não pode ser deixada em branco. ● Deve ser exclusivo para cada EIP. ● Pode conter no máximo 36 caracteres. ● Pode conter letras, dígitos, sublinhados (_) e hifens (-).	Ipv4_key1
Value	● Pode conter no máximo 43 caracteres. ● Pode conter letras, dígitos, sublinhados (_) pontos (.) e hífen (-).	192.168.12.10

NOTA

- Se você estiver comprando um EIP cobrado com base em pagamento por uso e quiser usar uma largura de banda compartilhada, só poderá selecionar uma largura de banda compartilhada existente na lista suspensa **Bandwidth Name**. Se não houver larguras de banda compartilhadas para selecionar, compre uma largura de banda compartilhada primeiro.
- Uma largura de banda dedicada não pode ser alterada para uma largura de banda compartilhada e vice-versa. No entanto, você pode comprar uma largura de banda compartilhada para EIPs de pagamento por uso.
  - Depois que um EIP é adicionado a uma largura de banda compartilhada, o EIP usará a largura de banda compartilhada.
  - Depois que um EIP é removido da largura de banda compartilhada, o EIP usará a largura de banda dedicada.

6. Clique em **Next**.
7. Clique em **Submit**.

Vincular um EIP

1. Na página **EIPs**, localize a linha que contém o EIP de destino e clique em **Bind**.
2. Selecione a instância à qual você deseja vincular o EIP.
3. Clique em **OK**.

3.3 Desvinculação de um EIP de um ECS e liberação do EIP

Cenários

Se você não precisar mais de um EIP, desvincule-o do ECS e libere o EIP para evitar o desperdício de recursos de rede.

Observações e restrições

- Você só pode liberar EIPs que não estejam vinculados a nenhum recurso.
- Você não pode comprar um EIP que tenha sido liberado se ele estiver atualmente em uso por outro usuário.
- O preço de um EIP de pagamento por uso inclui a taxa de retenção e o preço da largura de banda. Se você desvincular um EIP, mas não liberá-lo, o EIP continuará a ser cobrado e o preço inclui a taxa de retenção e o preço da largura de banda. No momento em que você vincula um EIP a uma instância, a taxa de retenção não é mais incluída no preço do EIP.

Procedimento

Desvinculação de um único EIP

1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Elastic IP**.

4. Na página exibida, localize a linha que contém o EIP de destino e clique em **Unbind**.
5. Clique em **Yes** na caixa de diálogo exibida.

Liberação de um único EIP

1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Elastic IP**.
4. Na página exibida, localize a linha que contém o EIP de destino, clique em **More** e, em seguida, em **Release** na coluna **Operation**.
5. Clique em **Yes** na caixa de diálogo exibida.

Desvinculação de vários EIPs de uma só vez

1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Elastic IP**.
4. Na página exibida, selecione os EIPs a serem desvinculados.
5. Clique no botão **Unbind** localizado acima da lista de EIP.
6. Clique em **Yes** na caixa de diálogo exibida.

Liberação de vários EIPs de uma só vez

1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Elastic IP**.
4. Na página exibida, selecione os EIPs a serem liberados.
5. Clique no botão **Release** localizado acima da lista de EIP.
6. Clique em **Yes** na caixa de diálogo exibida.

3.4 Modificação de uma largura de banda de EIP

Scenarios

No matter which billing mode is used, if your EIP is not added to a shared bandwidth, it uses a dedicated bandwidth.

This section describes how to increase or decrease a dedicated bandwidth.

When you change the bandwidth size, the bandwidth price and effective time vary by the billing mode, which applies to both dedicated and shared bandwidths. For details, see **Tabela 3-3**.

Tabela 3-3 Impact on billing after bandwidth size change

Billing Mode	Billed By	Change	Impact
Yearly/ Monthly	Bandwidth	Increase bandwidth	The change will take effect immediately. The increased bandwidth will be billed accordingly.
	Bandwidth	Decrease bandwidth upon renewal	The change will not take effect immediately. You need to select a new bandwidth size and a renewal duration. The change will take effect in the first billing cycle after a successful renewal. ● The order can be unsubscribed before the bandwidth takes effect. ● The bandwidth cannot be modified in the first billing cycle.
Pay-per-use	Bandwidth	Increase or decrease the bandwidth	The change will take effect immediately.
	Traffic	Increase or decrease the bandwidth	The change will take effect immediately. The bandwidth size you set is only used to limit the maximum rate.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Elastic IP**.
4. Localize a linha que contém o EIP de destino na lista de EIP, clique em **More** na coluna **Operation** e selecione **Modify Bandwidth**.
5. Modifique os parâmetros de largura de banda conforme solicitado.

Figura 3-2 Modificar a largura de banda de um EIP de pagamento por uso

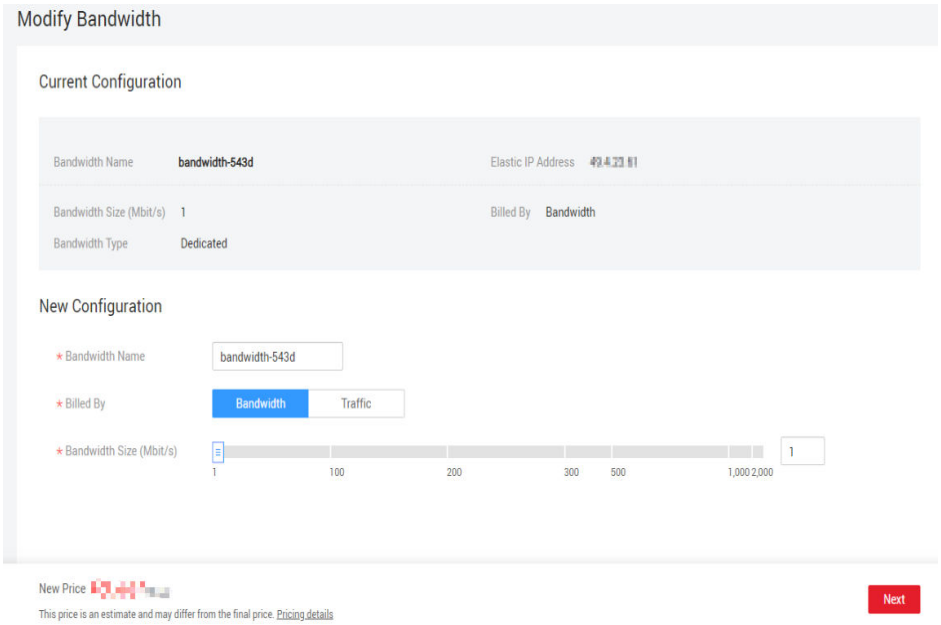
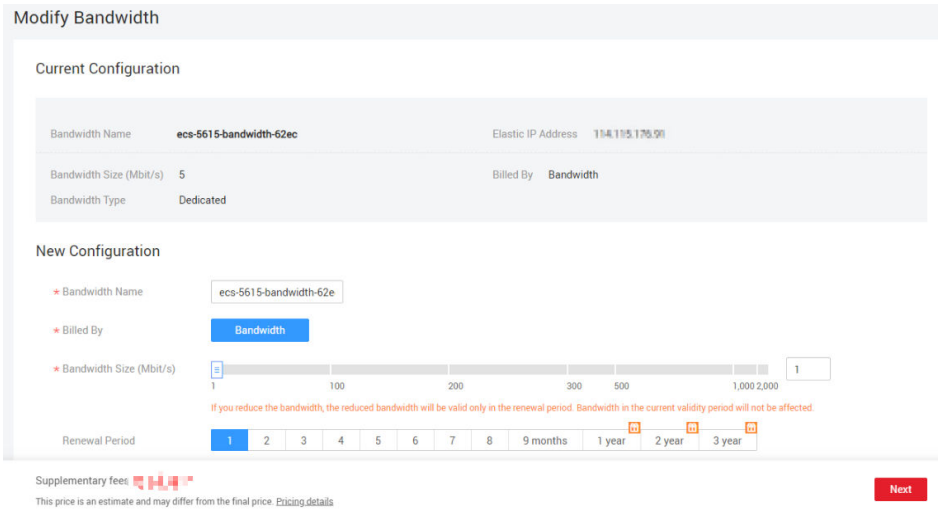


Figura 3-3 Modificar a largura de banda mensal/anual



6. Clique em **Next**.
7. Clique em **Submit**.

3.5 Gerenciamento de tags do EIP

Cenários

As tags podem ser adicionadas aos EIPs para facilitar a identificação e a administração do EIP. Você pode adicionar uma tag a um EIP ao atribuir o EIP. Como alternativa, você pode adicionar uma tag a um EIP atribuído na página de detalhes do EIP. Um máximo de 10 tags podem ser adicionadas a cada EIP.

Uma tag consiste em um par de chave e valor. **Tabela 3-4** lista os requisitos de chave e valor da tag.

Tabela 3-4 Requisitos da tag de EIP

Parâmetro	Requisito	Exemplo de valor
Key	● Não pode ser deixada em branco. ● Deve ser exclusivo para cada EIP. ● Pode conter no máximo 36 caracteres. ● Pode conter letras, dígitos, sublinhados (_) e hifens (-).	Ipv4_key1
Value	● Pode conter no máximo 43 caracteres. ● Pode conter letras, dígitos, sublinhados (_) pontos (.) e hífen (-).	192.168.12.10

Procedimento

Pesquisar EIPs por chave e valor de tag na página que mostra a lista de EIPs

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Elastic IP**.
4. No canto superior direito da lista EIP, clique em **Search by Tag**.
5. Na área exibida, digite a chave da tag e o valor do EIP que você está procurando.

   Você deve especificar a chave e o valor da tag. O sistema exibirá os EIPs que contêm a tag especificada.
6. Clique em + para adicionar outra chave e valor de tag.

   Você pode adicionar várias chaves e valores de tags para refinar os resultados da pesquisa. Se você adicionar mais de uma tag para procurar EIPs, o sistema exibirá somente os EIPs que contêm todas as tags especificadas.
7. Clique em **Search**.

   O sistema exibe os EIPs que você está procurando com base nas chaves e valores de tags inseridos.

Adicionar, excluir, editar e exibir tags na guia Tags de um EIP

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Elastic IP**.
4. Na página exibida, localize o EIP cujas tags você deseja gerenciar e clique no nome do EIP.
5. Na página que mostra os detalhes do EIP, clique na guia **Tags** e execute as operações desejadas nas tags.
   - Veja as tags.

     Na guia **Tags**, você pode exibir detalhes sobre as tags adicionadas ao EIP atual, incluindo o número de tags e a chave e o valor de cada tag.

- Adicionar uma tag.

  Clique em **Add Tag** no canto superior esquerdo. Na caixa de diálogo **Add Tag** exibida, insira a chave e o valor da tag e clique em **OK**.

- Editar uma tag.

  Localize a linha que contém a tag que deseja editar e clique em **Edit** na coluna **Operation**. Insira o novo valor da tag e clique em **OK**.

  A chave de tag não pode ser modificada.

- Excluir uma tag.

  Localize a linha que contém a tag que deseja excluir e clique em **Delete** na coluna **Operation**. Na caixa de diálogo exibida, clique em **Yes**.

3.6 IPv6 EIP

Overview

Both IPv4 and IPv6 EIPs are available. You can assign an IPv6 EIP or map an existing IPv4 EIP to a IPv6 EIP.

After the IPv6 EIP function is enabled, you will obtain both an IPv4 EIP and its corresponding IPv6 EIP. External IPv6 addresses can access cloud resources through this IPv6 EIP.

IPv4 EIPs are billed. IPv6 EIPs are currently free, but will be billed at a later date (price yet to be determined).

Application Scenarios of IPv4/IPv6 Dual Stack

If your ECS supports IPv6, you can use the IPv4/IPv6 dual stack. **Tabela 3-5** shows the example application scenarios.

Tabela 3-5 Application scenarios of IPv4/IPv6 dual stack

Application Scenario	Description	Requirement	IPv4 or IPv6 Subnet	ECS
Private IPv4 communication	Your applications on ECSs need to communicate with other systems (such as databases) through private IPv4 addresses.	• IPv6 is not enabled for the VPC subnet. • No EIPs have been bound to the ECSs.	IPv4 CIDR Block	**Private IPv4 address**: used for private IPv4 communication.

Application Scenario	Description	Requirement	IPv4 or IPv6 Subnet	ECS
Public IPv4 communication	Your applications on ECSs need to communicate with other systems (such as databases) through public IPv4 addresses.	• IPv6 is not enabled for the VPC subnet. • EIPs have been bound to the ECSs.	IPv4 CIDR Block	• **Private IPv4 address**: used for private IPv4 communication. • **Public IPv4 address**: used for public IPv4 communication.
Private IPv6 communication	Your applications on ECSs need to communicate with other systems (such as databases) through private IPv6 addresses.	• IPv6 has been enabled for the VPC subnet. • The network has been configured for the ECSs as follows: – **Flavor**: Any ECS flavor that supports the IPv6 network. For details about the ECS flavor that support the IPv6 network, see section " x86 ECS Specifications and Types" in the *Elastic Cloud Server User Guide*. – **VPC and Subnet**: IPv6-enabled subnet and VPC. – **Self-assigned IPv6 address**: Selected. – **Shared Bandwidth**: Selected **Do not configure**.	• IPv4 CIDR Block • IPv6 CIDR block	• **Private IPv4 address + IPv4 EIP**: Bind an IPv4 EIP to the instance to allow public IPv4 communication. • **Private IPv4 address**: Do not bind any IPv4 EIP to the instance and use only the private IPv4 address to allow private IPv4 communication. • **IPv6 address**: Do not configure shared bandwidth for the IPv6 address to allow private IPv6 communication.

Application Scenario	Description	Requirement	IPv4 or IPv6 Subnet	ECS
Public IPv6 communication	An IPv6 network is required for the ECS to access the IPv6 service on the Internet.	● IPv6 has been enabled for the VPC subnet. ● The network has been configured for the ECSs as follows: – **Flavor**: Any ECS flavor that supports the IPv6 network. For details about the ECS flavor that support the IPv6 network, see section "x86 ECS Specifications and Types" in the *Elastic Cloud Server User Guide*. – **VPC and Subnet**: IPv6-enabled subnet and VPC. – **Self-assigned IPv6 address**: Selected. – **Shared Bandwidth**: Selected a shared bandwidth.	● IPv4 CIDR Block ● IPv6 CIDR block	● **Private IPv4 address + IPv4 EIP**: Bind an IPv4 EIP to the instance to allow public IPv4 communication. ● **Private IPv4 address**: Do not bind any IPv4 EIP to the instance and use only the private IPv4 address to allow private IPv4 communication. ● **IPv6 address + shared bandwidth**: Allow both private IPv6 communication and public IPv6 communication.

For details, see section "IPv4 and IPv6 Dual-Stack Network" in *Virtual Private Cloud User Guide*.

Application Scenarios of IPv6 EIP

If you want an ECS to provide IPv6 services but the ECS does not support IPv6 networks or you do not want to build an IPv6 network, you can use IPv6 EIP to quickly address your requirements. For details about application scenarios and resource planning, see **Tabela 3-6**.

Tabela 3-6 Application scenarios and resource planning of an IPv6 EIP network (with IPv6 EIP enabled)

Application Scenario	Description	Requirement	IPv4 or IPv6 Subnet	ECS
Public IPv6 communication	You want to allow an ECS to provide IPv6 services for clients on the Internet without setting up an IPv6 network.	• An EIP has been bound to the ECS. • IPv6 EIP has been enabled.	IPv4 CIDR Block	• **Private IPv4 address**: used for private IPv4 communication. • **IPv4 EIP (with IPv6 EIP enabled)**: used for public network communication through IPv4 and IPv6 addresses.

Application Scenarios and Resource Planning of IPv6 Networks

Figura 3-4 Application scenarios and resource planning of IPv6 networks

Ativar IPv6 (Atribuir IPv6 EIPs)

- Método 1:

  selecione a opção **IPv6 EIP** ao atribuir um EIP referindo-se a **Atribuição de um EIP e vinculação a um ECS** para que você possa obter um IPv4 e um IPv6 EIP.

  Endereços IPv6 externos podem acessar recursos de nuvem através deste IPv6 EIP.

- Method 2:

  If you want an IPv6 EIP in addition to an existing IPv4 EIP, locate the row that contains the target IPv4 EIP, click **More** in the **Operation** column, and select **Enable IPv6 EIP**. Then, a corresponding IPv6 EIP will be assigned and

  After the IPv6 EIP is enabled, you will obtain both an IPv4 EIP and an IPv6 EIP. External IPv6 addresses can access cloud resources through this IPv6 EIP.

NOTA

there is no adverse impact on the cloud resources bound with existing IPv4 EIPs.

Configuring Security Groups

After IPv6 EIP is enabled, add inbound and outbound security group rules to allow packets to and from the IP address range **198.19.0.0/16**. **Tabela 3-7** shows the security group rules. IPv6 EIP uses NAT64 to convert the source IP address in the inbound direction to an IPv4 address in the IP address range 198.19.0.0/16. The source port can be a random one, the destination IP address is the private IPv4 address of your local server, and the destination port remains unchanged.

For details, see section "Adding a Security Group Rule" in the *Virtual Private Cloud User Guide*.

Tabela 3-7 Security group rules

Direction	Protocol	Source or Destination
Inbound	All	Source: 198.19.0.0/16
Outbound	All	Destination: 198.19.0.0/16

Disabling IPv6 EIP

If you do not need the IPv6 EIP, locate the row that contains its corresponding IPv4 EIP, click **More** in the **Operation** column, and select **Disable IPv6 EIP**. Then, the IPv6 EIP will be released. You will only have the IPv4 EIP.

4 Largura de banda compartilhada

4.1 Visão geral da largura de banda compartilhada

Uma largura de banda compartilhada pode ser compartilhada por vários EIPs e controla a taxa de transferência de dados nesses EIPs de maneira centralizada. Todos os ECSs, BMSs e balanceadores de carga que tenham EIPs vinculados na mesma região podem compartilhar a mesma largura de banda.

Quando você hospeda um grande número de aplicativos na nuvem, se cada EIP usa uma largura de banda, muitas larguras de banda são necessárias, o que aumenta significativamente os custos de largura de banda. Se todos os EIPs compartilharem a mesma largura de banda, você poderá reduzir os custos de largura de banda e realizar facilmente O&M do sistema.

- Custos de largura de banda reduzidos

  O compartilhamento de largura de banda em nível regional e a multiplexação reduzem o uso de largura de banda e os custos de O&M.
- Operações flexíveis

  Você pode adicionar EIPs que são cobrados em uma base de pagamento por uso a uma largura de banda compartilhada ou removê-los de uma largura de banda compartilhada, independentemente dos tipos de EIP e das instâncias às quais eles estão vinculados.
- Modos de cobrança flexíveis

  Os modos de faturamento anual/mensal e pagamento por uso são fornecidos.

Você pode usar uma largura de banda compartilhada de uma das seguintes maneiras:

- Atribua uma largura de banda compartilhada e adicione seus EIPs de pagamento por uso à largura de banda.
  - **Atribuição de uma largura de banda compartilhada**
  - **Adição de EIPs a uma largura de banda compartilhada**
- Atribua uma largura de banda compartilhada, defina **Billed By** como **Shared Bandwidth** e selecione a largura de banda compartilhada ao atribuir EIPs.
  - **Atribuição de uma largura de banda compartilhada**

Observações e restrições

- O tamanho mínimo de uma largura de banda compartilhada que pode ser comprada é de 5 Mbit/s. Você só pode adicionar EIPs de pagamento por uso a uma largura de banda compartilhada.
- Cada conta pode ter um máximo de 5 larguras de banda compartilhadas. Se você precisar de mais larguras de banda compartilhadas, envie um tíquete de serviço para solicitar um aumento de cota.
- Se uma largura de banda compartilhada anual/mensal for excluída após a expiração, os EIPs que compartilham a largura de banda serão removidos da largura de banda e serão cobrados com base no modo antes de serem adicionados à largura de banda compartilhada.
- Uma largura de banda compartilhada não pode controlar a quantidade de dados que podem ser transferidos usando um único EIP. A taxa de transferência de dados em EIPs não pode ser personalizada.
- Uma largura de banda compartilhada só pode ser usada por recursos de sua mesma conta.

  NOTA

  - Uma largura de banda dedicada não pode ser alterada para uma largura de banda compartilhada e vice-versa. No entanto, você pode comprar uma largura de banda compartilhada para EIPs pagos por uso.
    - Adicione um EIP a uma largura de banda compartilhada e, em seguida, o EIP usará a largura de banda compartilhada.
    - Remova o EIP da largura de banda compartilhada e, em seguida, o EIP usará a largura de banda dedicada.

4.2 Atribuição de uma largura de banda compartilhada

Cenários

Quando você hospeda um grande número de aplicações na nuvem, se cada EIP usa largura de banda dedicada, muitas larguras de banda são necessárias, o que gera altos custos. Se todos os EIPs compartilharem a mesma largura de banda, os custos de operação da rede serão reduzidos e as estatísticas de O&M do sistema, bem como de recursos, serão simplificadas.

Atribua uma largura de banda compartilhada para uso com EIPs.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Elastic IP**.
4. No painel de navegação à esquerda, escolha **Elastic IP and Bandwidth** > **Shared Bandwidths**.
5. No canto superior direito, clique em **Buy Shared Bandwidth**. Na página exibida, configure os parâmetros conforme solicitado.

Tabela 4-1 Descrições de parâmetro

Parâmetro	Descrição	Exemplo de valor
Billing Mode	O modo de cobrança de uma largura de banda compartilhada. O modo de cobrança pode ser: ● **Yearly/Monthly**: você paga pela largura de banda por ano ou mês antes de usá-lo. Nenhuma outra taxa se aplica durante o período de validade da largura de banda. ● **Pay-per-use**: você paga pela largura de banda com base na quantidade de tempo que você usa a largura de banda.	Yearly/Monthly
Region	Regiões são áreas geográficas fisicamente isoladas umas das outras. As redes dentro de diferentes regiões não estão conectadas entre si, portanto, os recursos não podem ser compartilhados entre diferentes regiões. Para menor latência de rede e acesso mais rápido aos seus recursos, selecione a região mais próxima de você.	CN-Hong Kong
Billed By	O método de cobrança para a largura de banda compartilhada. Você pode pagar por largura de banda.	Bandwidth
Bandwidth	O tamanho da largura de banda em Mbit/s. O valor mínimo é de 5 Mbit/s. A máxima da largura de banda pode ser 2000 Mbit/s.	10
Enterprise Project	O projeto empresarial ao qual o EIP pertence. Um projeto corporativo facilita o gerenciamento de projeto e o agrupamento de recursos da nuvem e de usuários. O nome do projeto padrão é **default**.	default
Bandwidth Name	O nome da largura de banda compartilhada.	Bandwidth-001
Required Duration	A duração para a qual o EIP adquirido será usado. A duração deve ser especificada se o **Billing Mode** estiver definido como **Yearly/Monthly**.	2 months

6. Clique em **Next**.

4.3 Adição de EIPs a uma largura de banda compartilhada

Cenários

Adicionar EIPs a uma largura de banda compartilhada e os EIPs podem então compartilhar essa largura de banda. Você pode adicionar vários EIPs a uma largura de banda compartilhada ao mesmo tempo.

Observações e restrições

- Atualmente, os EIPs anuais/mensais não podem ser adicionados a uma largura de banda compartilhada.
- Depois que um EIP é adicionado a uma largura de banda compartilhada, a largura de banda original usada pelo EIP se tornará inválida e o EIP começará a usar a largura de banda compartilhada.
- A largura de banda dedicada original do EIP será excluída e não será mais cobrada.
- Para adicionar um EIP anual/mensal a uma largura de banda compartilhada, primeiro é necessário alterar o modo de cobrança para pagamento por uso.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Elastic IP**.
4. No painel de navegação à esquerda, escolha **Elastic IP and Bandwidth** > **Shared Bandwidths**.
5. Na lista de largura de banda partilhada, localize a linha que contém a largura de banda partilhada à qual pretende adicionar EIPs. Na coluna **Operation**, escolha **Add EIP** e selecione os EIPs a serem adicionados.
6. Clique em **OK**.

4.4 Remoção de EIPs de uma largura de banda compartilhada

Cenários

Remover os EIPs que não são mais necessários de uma largura de banda compartilhada, se necessário.

Observações e restrições

Um EIP anual/mensal não pode ser removido de uma largura de banda compartilhada comprada durante o OBT.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Elastic IP**.
4. No painel de navegação à esquerda, escolha **Elastic IP and Bandwidth** > **Shared Bandwidths**.
5. Na lista de largura de banda compartilhada, localize a linha que contém a largura de banda da qual os EIPs devem ser removidos, escolha **More** > **Remove EIP** na coluna **Operation** e selecione os EIPs a serem removidos na caixa de diálogo exibida.
6. Defina a largura de banda do EIP após a remoção do EIP. Você pode configurar o modo de cobrança de EIP e o tamanho da largura de banda.
7. Clique em **OK**.

4.5 Modificação de uma largura de banda compartilhada

Cenários

Você pode modificar o nome e o tamanho de uma largura de banda compartilhada conforme necessário.

- Se uma largura de banda compartilhada for cobrada em uma base de pagamento por uso, a modificação entrará em vigor imediatamente. Para mais detalhes, consulte **Modificar a largura de banda compartilhada (pagamento por uso)**.
- Se uma largura de banda compartilhada for cobrada anualmente/mensalmente:
  - **Você pode aumentar a largura de banda.** O aumento do tamanho da largura de banda entrará em vigor imediatamente e a diferença de preço será cobrada de acordo.
  - **Você pode diminuir a largura de banda.** A diminuição do tamanho da largura de banda entrará em vigor no primeiro ciclo de cobrança após uma renovação bem-sucedida.

Modificar a largura de banda compartilhada (pagamento por uso)

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Elastic IP**.
4. No painel de navegação à esquerda, escolha **Elastic IP and Bandwidth** > **Shared Bandwidths**.
5. Na lista de largura de banda compartilhada, localize a linha que contém a largura de banda compartilhada que você deseja modificar, clique em **Modify Bandwidth** na coluna **Operation** e modifique as configurações de largura de banda.
6. Clique em **Next**.
7. Clique em **Submit**.

   A modificação entra em vigor imediatamente.

Aumentar uma largura de banda compartilhada (anual/mensal)

1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Elastic IP**.
4. No painel de navegação à esquerda, escolha **Elastic IP and Bandwidth** > **Shared Bandwidths**.
5. Na lista de largura de banda compartilhada, localize a linha que contém a largura de banda compartilhada de destino e clique em **Modify Bandwidth** na coluna **Operation**.
6. Selecione **Increase bandwidth** e clique em **Continue**.
7. Na área **New Configuration** da página **Modify Bandwidth**, altere o nome e o tamanho da largura de banda.
8. Clique em **Next**.
9. Confirme as informações e clique em **Pay Now**.

   Depois de concluir o pagamento, o aumento da largura de banda entrará em vigor imediatamente.

Diminuir uma largura de banda compartilhada (anual/mensal)

1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Elastic IP**.
4. No painel de navegação à esquerda, escolha **Elastic IP and Bandwidth** > **Shared Bandwidths**.
5. Na lista de largura de banda compartilhada, localize a linha que contém a largura de banda compartilhada de destino e clique em **Modify Bandwidth** na coluna **Operation**.
6. Selecione **Decrease bandwidth** e clique em **Continue**.
7. Na área **New Configuration** da página **Modify Bandwidth**, altere o nome e o tamanho da largura de banda.
8. Clique em **Next**.
9. Confirme as informações e clique em **Pay Now**.

   Depois de concluir o pagamento, a largura de banda reduzida entrará em vigor no primeiro ciclo de cobrança após o término da assinatura atual.

4.6 Exclusão de uma largura de banda compartilhada

Cenários

Excluir uma largura de banda compartilhada faturada em uma base de pagamento por uso se ela não for mais necessária.

Observações e restrições

Uma largura de banda compartilhada anual/mensal não pode ser excluída diretamente. Ele só pode ser cancelado na Central de usuário.

Pré-requisitos

Antes de excluir uma largura de banda compartilhada, remova todos os EIPs associados a ela. Para mais detalhes, consulte **Remoção de EIPs de uma largura de banda compartilhada**.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Elastic IP**.
4. No painel de navegação à esquerda, escolha **Elastic IP and Bandwidth** > **Shared Bandwidths**.
5. Na lista de largura de banda partilhada, localize a linha que contém a largura de banda partilhada de pagamento por uso que pretende eliminar, clique em **More** na coluna **Operation** e, em seguida, clique em **Delete**.
6. Na caixa de diálogo exibida, clique em **Yes**.

5 Pacote de dados compartilhados

5.1 Visão geral do pacote de dados compartilhados

Pacotes de dados compartilhados fornecem cotas para uso de dados. Tais pacotes são econômicos e fáceis de usar. Os pacotes de dados compartilhados entram em vigor imediatamente após a sua compra. Se você se inscreveu em EIPs de pagamento por uso usando largura de banda faturada por tráfego em uma região e comprou um pacote de dados compartilhados na mesma região, os EIPs usarão o pacote de dados compartilhados. Após o esgotamento da cota do pacote ou o seu vencimento, os EIPs continuarão sendo cobrados com base no pagamento por uso.

Dois tipos de pacotes estão disponíveis: BGP dinâmico e BGP estático. Pacotes de dados de BGP dinâmico serão utilizados por EIPs de BGP dinâmico, e pacotes de dados de BGP estático serão utilizados por EIPs de estático BGP.

- Pacotes de dados compartilhados podem ser comprados anualmente ou mensalmente. Pacotes comprados por um ano são de melhor custo-benefício. Se você tiver vários pacotes de dados compartilhados, o pacote de dados com o menor período de validade será usado primeiro.
- Se seu uso exceder sua cota de pacote de dados compartilhados dentro de sua validade, você será cobrado em uma base de pagamento por uso pelo uso de tráfego adicional.
- Se um pacote de dados compartilhados expirar, verifique se o saldo da sua conta é suficiente e seu EIP será cobrado com base no pagamento por uso.

Observações e restrições

- Um pacote de dados compartilhados entra em vigor apenas para a largura de banda faturada pelo tráfego. Dois tipos de pacotes de dados compartilhados estão disponíveis: BGP estático (para largura de banda do BGP estático) e BGP dinâmico (para largura de banda do BGP dinâmico).
- Um pacote de dados compartilhados não pode ter efeito para a largura de banda de um EIP específico.
- Um pacote de dados compartilhados não pode ter efeito para uma largura de banda compartilhada.
- Um pacote de dados compartilhados não pode ser usado por EIPs do tipo de BGP premium.

- Um pacote de dados compartilhados não pode ser cancelado.

5.2 Compra de um pacote de dados compartilhados

Cenários

Esta seção descreve como comprar um pacote de dados compartilhados. Os pacotes de dados compartilhados entram em vigor imediatamente após a compra. Se você se inscreveu em EIPs de pagamento por uso cobrados por tráfego em uma região e comprou um pacote de dados compartilhados na mesma região, os EIPs usarão o pacote de dados compartilhados. Após o esgotamento da cota do pacote ou o seu vencimento, os EIPs continuarão sendo cobrados com base no pagamento por uso.

Observações e restrições

- Um pacote de dados compartilhados entra em vigor apenas para a largura de banda faturada pelo tráfego. Dois tipos de pacotes de dados compartilhados estão disponíveis: BGP estático (para largura de banda do BGP estático) e BGP dinâmico (para largura de banda do BGP dinâmico).
- Um pacote de dados compartilhados não pode ter efeito para a largura de banda de um EIP específico.
- Um pacote de dados compartilhados não pode ter efeito para uma largura de banda compartilhada.
- Um pacote de dados compartilhados não pode ser usado por EIPs do tipo de BGP premium.
- Um pacote de dados compartilhados não pode ser cancelado.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Elastic IP**.
4. No painel de navegação à esquerda, escolha **Elastic IP and Bandwidth** > **Shared Data Packages**.
5. No canto superior direito, clique em **Buy Shared Data Package**. Na página exibida, configure os parâmetros conforme solicitado.

Tabela 5-1 Descrições de parâmetro

Parâmetro	Descrição	Exemplo de valor
Region	Um pacote de dados compartilhados só pode ser usado por recursos em sua mesma região. Selecione a região com base em suas necessidades.	CN-Hong Kong

Parâmetro	Descrição	Exemplo de valor
Type	O tipo de pacote de dados compartilhados. Defina este parâmetro com base no tipo de largura de banda do EIP. Os dois tipos de pacotes a seguir estão disponíveis: ● BGP dinâmico: um pacote de dados BGP dinâmico só pode ser usado por EIPs de BGP dinâmicos cobrados pelo tráfego em uma base de pagamento por uso. ● BGP estático: um pacote de dados BGP estático só pode ser usado por EIPs de BGP estático cobrados pelo tráfego em uma base de pagamento por uso.	BGP estático
Package Validity	O período de validade do pacote de dados compartilhados. Selecione um período de validade com base nos requisitos de serviço. Um pacote de dados compartilhados não pode ser cancelado e entra em vigor imediatamente após a compra. Pacotes de dados compartilhados expirados estarão mais disponíveis para uso.	1 mês
Specification	O tamanho do pacote de dados compartilhados em GB.	10 GB
Usage Duration	O período de validade do pacote de dados compartilhados.	Padrão

6. Clique em **Next**.

6 Tabela de rotas

6.1 Visão geral da tabela de rotas

Tabela de rotas

Uma tabela de rotas contém um conjunto de rotas que são usadas para determinar para onde o tráfego de rede das suas sub-redes em uma VPC é direcionado. Cada sub-rede deve estar associada a uma tabela de rotas. Uma sub-rede só pode ser associada a uma tabela de rotas de cada vez, mas você pode associar várias sub-redes à mesma tabela de rotas.

Tabela de rota padrão e tabela de rota personalizada

Quando uma VPC é criada, o sistema gera automaticamente uma tabela de rotas padrão para ela. Se você criar uma sub-rede na VPC, a sub-rede será associada automaticamente à tabela de rotas padrão.

- Você pode adicionar rotas para, excluir rotas e modificar rotas na tabela de rotas padrão, mas não pode excluir a tabela.
- Quando você cria uma conexão VPN, Cloud Connect ou Direct Connect, a tabela de rotas padrão fornece automaticamente uma rota que não pode ser excluída ou modificada.

Se você não quiser usar a tabela de rotas padrão, você pode criar uma tabela de rotas personalizada e vincular com a sub-rede. Você pode excluir a tabela de rota personalizada se não for mais necessária.

NOTA

- A tabela de rota personalizada associada a uma sub-rede afeta apenas o tráfego de saída. A tabela de rotas padrão determina o tráfego de entrada.
- Para usar uma tabela de rotas personalizada, você precisa enviar um tíquete de serviço. Você precisa clicar em **Increase quota** na página **Create Route Table** ou escolher **More** > **Service Tickets** > **Create Service Ticket** no canto superior direito da página. Para obter mais informações, consulte **Envio de um tíquete de serviço**.

Para obter detalhes sobre como criar uma tabela de rotas personalizada, consulte a seção **Criação de uma tabela de rota personalizada**.

Rota

Uma rota é configurada com o destino, o tipo de próximo salto e o próximo salto para determinar para onde o tráfego de rede é direcionado. As rotas são classificadas em rotas do sistema e rotas personalizadas.

- Rotas do sistema: estas rotas são adicionadas automaticamente pelo sistema e não podem ser modificadas ou excluídas.

  Depois que uma tabela de rotas é criada, o sistema adiciona automaticamente as seguintes rotas do sistema à tabela de rotas, para que as instâncias em uma VPC possam se comunicar entre si.

  - Rotas cujo destino é 100.64.0.0/10 ou 198.19.128.0/20.
  - Rotas cujo destino é um bloco CIDR de sub-rede.

    NOTA

    Além das rotas do sistema anteriores, o sistema adiciona automaticamente uma rota cujo destino é 127.0.0.0/8. Este é o endereço de loopback local.

    As rotas do sistema e do costume são rotas de BGP estático.

- Rota personalizada: estas são rotas que você pode adicionar, modificar e excluir. O destino de uma rota personalizada não pode se sobrepor ao de uma rota do sistema.

  Você pode adicionar uma rota personalizada e configurar o destino, o tipo de próximo salto e o próximo salto na rota para determinar para onde o tráfego de rede será direcionado. **Tabela 6-1** lista os tipos suportados de próximos saltos.

  Não é possível adicionar duas rotas com o mesmo destino a uma tabela de rotas da VPC, mesmo que seus tipos de próximos saltos sejam diferentes. A prioridade da rota depende do destino. De acordo com a regra de roteamento de correspondência mais longa, o destino com um grau de correspondência mais alto é preferencialmente selecionado para encaminhamento de pacotes.

Tabela 6-1 Tipo de próximo salto

Tipo de próximo salto	Descrição	Tabela de rotas suportadas
Servidor	O tráfego destinado ao destino é encaminhado para um ECS na VPC.	● Tabela de rota padrão ● Tabela de rota personalizada
NIC de extensão	O tráfego destinado ao destino é encaminhado para a NIC de extensão de um ECS na VPC.	● Tabela de rota padrão ● Tabela de rota personalizada
Rede definida pelo usuário do BMS	O tráfego endereçado ao destino é encaminhado para uma rede definida pelo usuário do BMS.	● Tabela de rotas padrão ● Tabela de rota personalizada

Tipo de próximo salto	Descrição	Tabela de rotas suportadas
Gateway de VPN	O tráfego destinado ao destino é encaminhado para um gateway de VPN.	Tabela de rota personalizada
Gateway da Direct Connect	O tráfego destinado ao destino é encaminhado para um gateway da Direct Connect.	Tabela de rota personalizada
Conexão em nuvem	O tráfego endereçado ao destino é encaminhado para uma conexão em nuvem	Tabela de rota personalizada
Interface de rede suplementar	O tráfego endereçado ao destino é encaminhado à interface de rede suplementar de um ECS na VPC.	● Tabela de rotas padrão ● Tabela de rota personalizada
Gateway de NAT	O tráfego destinado ao destino é encaminhado para um gateway da NAT.	● Tabela de rotas padrão ● Tabela de rota personalizada
Conexão de emparelhamento de VPC	O tráfego destinado ao destino é encaminhado para uma conexão de emparelhamento de VPC.	● Tabela de rotas padrão ● Tabela de rota personalizada
Endereço IP virtual	O tráfego destinado ao destino é encaminhado para um endereço IP virtual e, em seguida, enviado para ECSs ativos e em espera aos quais o endereço IP virtual está vinculado.	● Tabela de rotas padrão ● Tabela de rota personalizada
Roteador empresarial	O tráfego endereçado ao destino é encaminhado para um roteador empresarial.	● Tabela de rotas padrão ● Tabela de rota personalizada
Firewall em nuvem	O tráfego endereçado ao destino é encaminhado para um firewall em nuvem.	● Tabela de rotas padrão ● Tabela de rota personalizada

NOTA

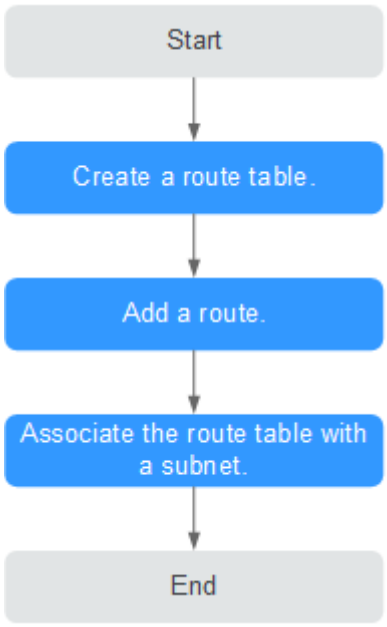
Se você especificar o destino ao criar um recurso, uma rota do sistema será entregue. Se você não especificar um destino ao criar um recurso, uma rota personalizada que pode ser modificada ou excluída será entregue.

Por exemplo, quando você cria um gateway da NAT, o sistema entrega automaticamente uma rota personalizada sem um destino específico (0.0.0.0/0 é usado à revelia). Nesse caso, você pode alterar o destino. No entanto, quando você cria um VPN gateway, você precisa especificar a sub-rede remota, ou seja, o destino de uma rota. Nesse caso, o sistema entrega essa rota do sistema. Não modifique o destino da rota na página **Route Tables**. Se o fizer, o destino será inconsistente com a sub-rede remota configurada. Para modificar o destino da rota, vá para a página de recursos específica e modifique a sub-rede remota. Em seguida, o destino da rota será alterado de acordo.

Processo de configuração da tabela de rota personalizada

Figura 6-1 mostra o processo de criação e configuração de uma tabela de rotas personalizada.

Figura 6-1 Processo de configuração da tabela de rota



1. Para obter detalhes sobre como criar uma tabela de rotas personalizada, consulte **Criação de uma tabela de rota personalizada**.
2. Para obter detalhes sobre como adicionar uma rota personalizada, consulte **Adição de uma rota personalizada**.
3. Para obter detalhes sobre como associar uma sub-rede a uma tabela de rotas, consulte **Associação de uma tabela de rotas a uma sub-rede**. Após a associação, as rotas na tabela de rotas controlam o roteamento para a sub-rede.

Observações e restrições

- Quando uma VPC é criada, o sistema gera automaticamente uma tabela de rotas padrão para ela.

  Se quiser solicitar uma cota mais alta para criar mais tabelas de rotas, consulte **Criação de um tíquete de serviço**.

- Um máximo de 200 rotas pode ser adicionado a cada tabela de rotas.
- A tabela de rotas padrão não pode ser excluída.
- A rota do sistema não pode ser modificada ou excluída.
- As rotas fornecidas pelos serviços VPN, Cloud Connect e Direct Connect para a tabela de rotas padrão não podem ser modificadas ou excluídas.

6.2 Exemplo de rota personalizada em uma VPC

Uma rota personalizada em uma VPC roteia o tráfego proveniente de ECSs em uma VPC para um ECS especificado também nessa VPC. Uma rota personalizada em uma VPC pode ser usada nos seguintes cenários:

- Quando os ECSs em uma VPC precisarem acessar a Internet, adicione uma rota personalizada para permitir que os ECSs acessem a Internet por meio do ECS que tem um EIP vinculado. Ao adicionar a rota personalizada, defina **Destination** como o valor padrão **0.0.0.0/0** e **Next Hop** como o endereço IP privado ou virtual do ECS que tem um EIP vinculado na VPC.
- Quando os ECSs em uma VPC precisarem acessar a rede de contêiner, adicione uma rota para permitir que os ECSs acessem a rede de contêiner por meio de um ECS com a rede de contêiner configurada. Ao adicionar a rota personalizada, defina **Destination** para o valor padrão **0.0.0.0/0** ou um segmento de rede na rede de contêiner e **Next Hop** para o endereço IP privado ou virtual do ECS com a rede de contêiner configurada na VPC.

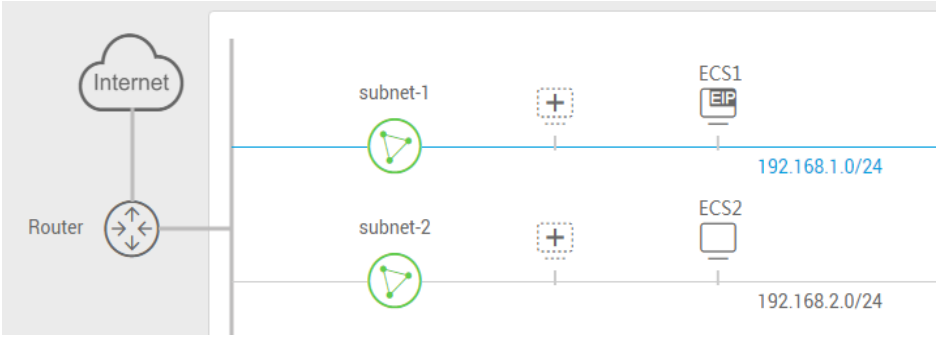
O destino de cada rota deve ser único.

Acessar a Internet por meio de uma rota personalizada

Cenário de exemplo

Há dois ECSs (ECS1 e ECS2) em uma VPC. O ECS1 tem um EIP vinculado, mas o ECS2 não. Você pode adicionar uma rota personalizada para permitir que o ECS2 acesse a Internet por meio do ECS1.

Figura 6-2 Acessando a Internet através de uma rota personalizada



Configuração

1. **Tabela 6-2** lista o exemplo de configuração de rota personalizada. O destino é o valor padrão **0.0.0.0/0**, e o próximo salto é o endereço IP privado ou virtual do ECS1 vinculado a um EIP.

Tabela 6-2 Rota personalizada

Destino	Próximo salto
0.0.0.0/0	Endereço IP privado ou virtual do ECS1

NOTA

- Quando utiliza uma rota personalizada para aceder à Internet, o destino só pode ser definido para o valor predefinido **0.0.0.0/0** e não pode ser definido para um segmento de rede pública específico.
- Se o próximo salto é um endereço IP virtual, o endereço IP virtual deve ter um EIP vinculado. Caso contrário, o acesso à Internet através deste endereço IP virtual não é possível.

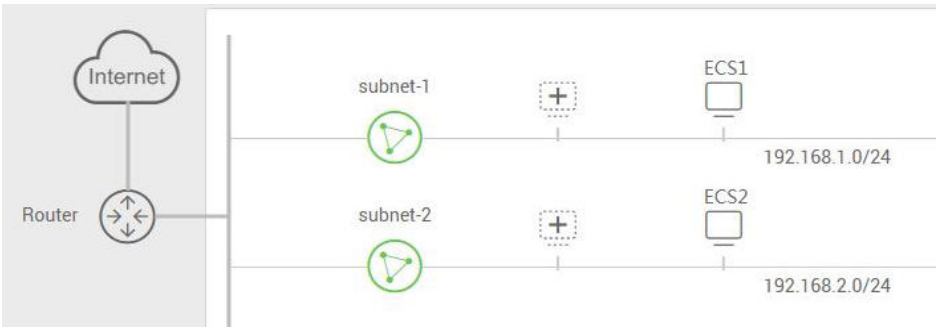
2. Configure o ECS1 como um servidor SNAT seguindo as instruções fornecidas em **Configuração de um servidor SNAT**.

Acessar a rede de contêiner em um ECS por meio de uma rota personalizada

Cenário de exemplo

Há dois ECSs (ECS1 e ECS2) em uma VPC, e uma rede de contêiner foi configurada para o ECS1. Se o ECS2 precisar acessar a rede de contêiner, você poderá adicionar uma rota personalizada.

Figura 6-3 Acessar a rede de contêiner em um ECS por meio de uma rota personalizada



Configuração

1. Configure uma rota personalizada, que incluirá um destino e um próximo salto. Os valores necessários são mostrados em **Tabela 6-3**. O destino pode ser o valor padrão **0.0.0.0/0** ou um intervalo de endereços IP na rede de contêiner, e o próximo salto é o endereço IP privado ou virtual ECS1 vinculado a um EIP.

Tabela 6-3 Rota personalizada

Destino	Próximo salto
0.0.0.0/0	O endereço IP privado ou virtual do ECS1

2. Configure o ECS1 como um servidor SNAT seguindo as instruções fornecidas em **Configuração de um servidor SNAT**.

6.3 Exemplo de rota personalizada fora de uma VPC

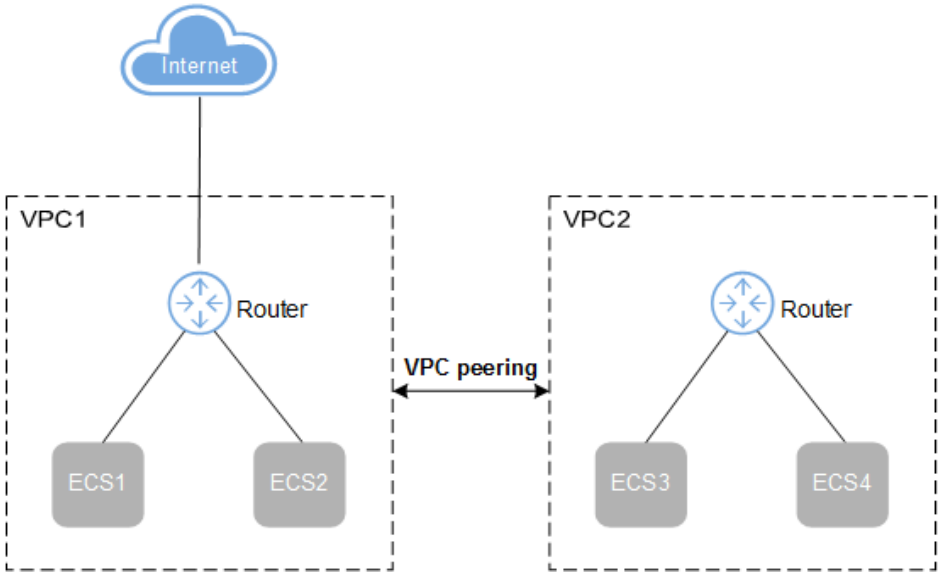
Uma rota personalizada fora de uma VPC roteia o tráfego originado fora da VPC para ECSs especificados na VPC. Ao adicionar esse tipo de rota, você pode definir **Destination** para o valor padrão **0.0.0.0/0** ou um segmento de rede específico. No entanto, o segmento de rede não pode entrar em conflito com blocos CIDR de sub-rede na VPC. O destino de cada rota personalizada deve ser único.

Rota personalizada entre VPCs

Cenário de exemplo

Se uma conexão de emparelhamento de VPC tiver sido criada vinculando duas VPCs, VPC1 e VPC2, mas somente a VPC1 tiver acesso à Internet, você pode adicionar uma rota personalizada para permitir que os ECSs na VPC2 acessem a Internet por meio de um ECS que tenha um EIP vinculado à VPC1.

Figura 6-4 Rota personalizada entre VPCs



Configuração

1. Crie uma conexão de emparelhamento de VPC entre a VPC1 e a VPC2. **Figura 6-5** mostra a configuração de conexão de emparelhamento de VPC.

Figura 6-5 Conexão de emparelhamento de VPC entre VPC1 e VPC2

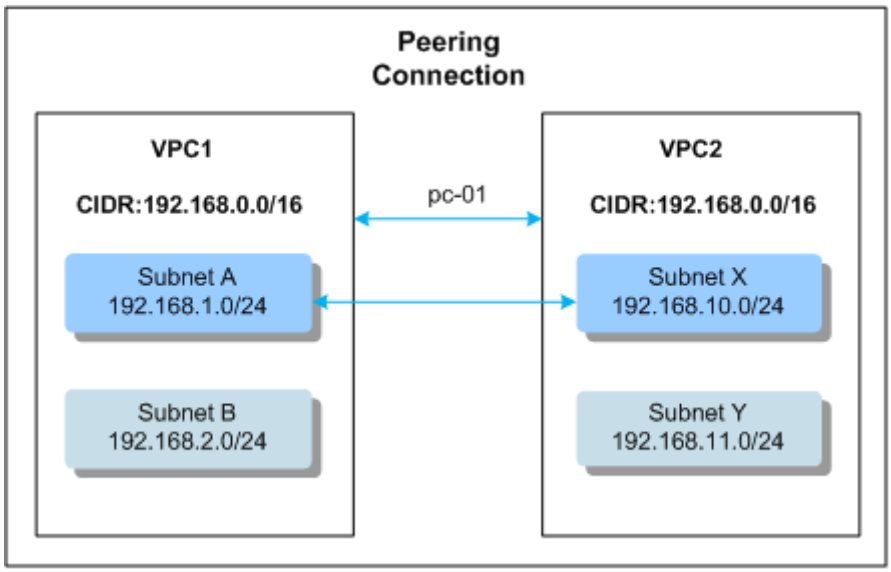


Tabela 6-4 e Tabela 6-5 listam as rotas usadas para configurar a conexão de emparelhamento de VPC.

Tabela 6-4 Rota de uma conexão de emparelhamento de VPC na tabela de rotas associada à sub-rede A

Destino	Próximo salto
192.168.10.0/24	pc-01

Tabela 6-5 Rota de uma conexão de emparelhamento de VPC na tabela de rotas associada à Sub-rede X

Destino	Próximo salto
192.168.1.0/24	pc-01
0.0.0.0/0	pc-01

NOTA

Nas tabelas de rotas anteriores, o valor **pc-01** indica o ID da conexão de emparelhamento de VPC. O valor é gerado automaticamente e não pode ser configurado.

2. Tabela 6-6 lista a configuração da tabela de rotas personalizada.

Tabela 6-6 Rota personalizada na tabela de rotas padrão da VPC1

Destino	Próximo salto
0.0.0.0/0	O endereço IP privado ou virtual do ECS1

NOTA

- Quando você usa uma rota personalizada para acessar a Internet, o destino só pode ser definido como **0.0.0.0/0**. Não pode ser definido para um intervalo específico de endereços IP públicos.
- Se o próximo salto é um endereço IP virtual, o endereço IP virtual deve ter um EIP vinculado. Caso contrário, o acesso à Internet através deste endereço IP virtual não é possível.

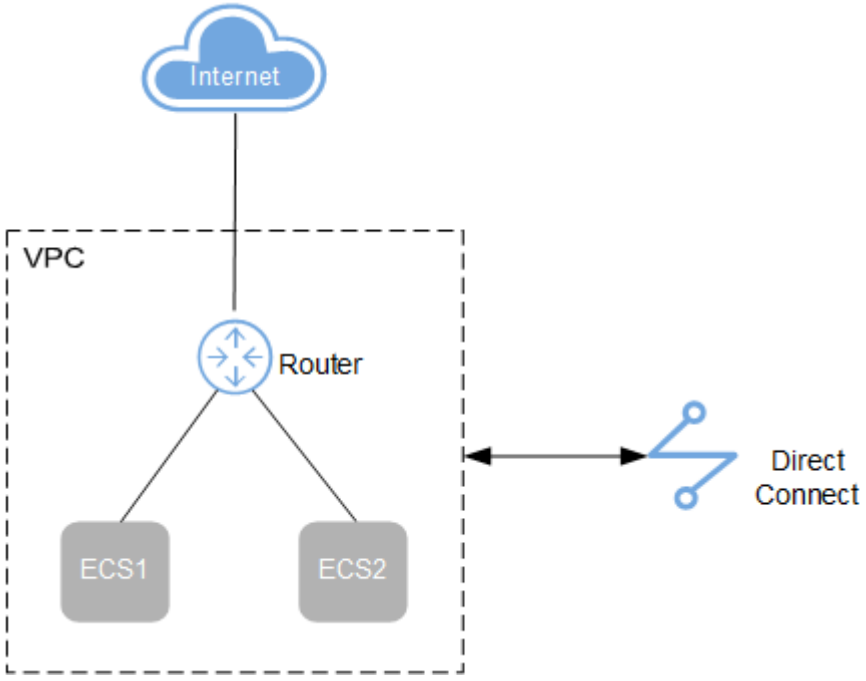
3. Configure o ECS como um servidor SNAT seguindo as instruções fornecidas em **Configuração de um servidor SNAT**.

Rota personalizada entre uma VPC e uma conexão da Direct Connect

Cenário de exemplo

Você pode adicionar uma rota personalizada para encaminhar todos os pacotes de uma conexão da Direct Connect para servidores especificados na VPC, mas uma rota personalizada precisa ser adicionada à VPC. **Tabela 6-7** fornece os detalhes necessários para configurar a rota.

Figura 6-6 Rota personalizada entre uma VPC e uma conexão da Direct Connect



Configuração

1. **Tabela 6-7** lista a configuração de rota personalizada. O destino é o valor padrão **0.0.0.0/0** e o próximo salto é o endereço IP privado ou virtual do ECS.

Tabela 6-7 Tabela de rotas personalizadas da VPC

Destino	Próximo salto
0.0.0.0/0	O endereço IP privado ou virtual do ECS

2. Configure o ECS como um servidor SNAT seguindo as instruções fornecidas em **Configuração de um servidor SNAT**.

6.4 Configuração de um servidor SNAT

Cenários

Para usar a função de tabela de rotas fornecida pelo serviço VPC, você precisa configurar a SNAT em um ECS para permitir que outros ECSs que não tenham EIPs vinculados em uma VPC acessem a Internet por meio desse ECS.

A SNAT configurado entra em vigor para todas as sub-redes em uma VPC.

Pré-requisitos

- Você tem um ECS em que a SNAT deve ser configurado.
- O ECS em que a SNAT deve ser configurado executa o sistema operacional Linux.
- O ECS em que a SNAT deve ser configurado tem apenas uma placa de interface de rede (NIC).

Diferenças entre servidores SNAT e gateways NAT

O serviço Gateway NAT fornece tradução de endereços de rede (NAT) para servidores, como ECSs, BMSs e áreas de trabalho de Workspace, em uma VPC ou em servidores de um data center local que se conecta a uma VPC por meio da Direct Connect ou VPN. Um gateway da NAT permite que esses servidores compartilhem um EIP para acessar a Internet ou fornecer serviços acessíveis a partir da Internet.

O serviço NAT Gateway é mais fácil de configurar e usar do que a SNAT. Esse serviço pode ser implantado de forma flexível em sub-redes e AZs e fornece diferentes especificações de gateway da NAT. Você pode clicar em **NAT Gateway** na **Networking** no console de gerenciamento para experimentar este serviço.

Para obter detalhes, consulte o **Guia de usuário do NAT Gateway**.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, em **Compute**, clique em **Elastic Cloud Server**.
4. Na página exibida, localize o ECS de destino na lista do ECS e clique no nome do ECS para alternar para a página que mostra os detalhes do ECS.
5. Na página de detalhes do ECS exibida, clique na guia **NICs** .
6. Na área exibida mostrando os detalhes do endereço IP da NIC, desative **Source/ Destination Check**.

   Por padrão, a verificação de origem/destino está ativada. Quando esta verificação está ativada, o sistema verifica se os endereços IP de origem contidos nos pacotes enviados pelos ECSs estão corretos. Se os endereços IP estiverem incorretos, o sistema não permitirá que os ECSs enviem os pacotes. Esse mecanismo evita a falsificação de

pacotes, melhorando assim a segurança do sistema. Se a função SNAT for usada, o servidor SNAT precisa encaminhar pacotes. No entanto, esse mecanismo impede que o remetente do pacote receba pacotes devolvidos. Portanto, você precisa desabilitar a verificação de origem/destino para servidores SNAT.

7. Vincule um EIP.
   - Vincule um EIP ao endereço IP privado do ECS. Para mais detalhes, consulte **Atribuição de um EIP e vinculação a um ECS**.
   - Vincule um EIP ao endereço IP virtual do ECS. Para mais detalhes, consulte **Vinculação de um endereço IP virtual a um EIP ou ECS**.
8. No console do ECS, use a função de logon remoto para efetuar logon no ECS onde você planeja configurar a SNAT.
9. Execute o seguinte comando e digite a senha do usuário **root** para alternar para o usuário **root**:

   su - root
10. Execute o seguinte comando para verificar se o ECS pode se conectar com êxito à Internet:

    NOTA

    Antes de executar o comando, você deve desabilitar a regra iptables de resposta no ECS em que a SNAT está configurada e habilitar as regras do grupo de segurança.

    ping www.huawei.com

    O ECS pode acessar a Internet se as seguintes informações forem exibidas:

    ```
    [root@localhost ~]# ping www.huawei.com
    PING www.a.shifen.com (xxx.xxx.xxx.xxx) 56(84) bytes of data.
    64 bytes from xxx.xxx.xxx.xxx: icmp_seq=1 ttl=51 time=9.34 ms
    64 bytes from xxx.xxx.xxx.xxx: icmp_seq=2 ttl=51 time=9.11 ms
    64 bytes from xxx.xxx.xxx.xxx: icmp_seq=3 ttl=51 time=8.99 ms
    ```
11. Execute o seguinte comando para verificar se o encaminhamento de IP do sistema operacional Linux está habilitado:

    cat /proc/sys/net/ipv4/ip_forward

    Na saída de comando, **1** indica que está habilitado e **0** indica que está desabilitado. O valor padrão é **0**.
    - Se o encaminhamento de IP no Linux estiver ativado, vá para a etapa **14**.
    - Se o encaminhamento de IP no Linux estiver desativado, vá para **12** para habilitar o encaminhamento de IP no Linux.

    Muitos sistemas operacionais suportam roteamento de pacotes. Antes de encaminhar pacotes, os sistemas operacionais alteram os endereços IP de origem nos pacotes para os endereços IP do sistema operacional. Portanto, os pacotes encaminhados contêm o endereço IP do remetente público para que os pacotes de resposta possam ser enviados de volta ao longo do mesmo caminho para o remetente do pacote inicial. Esse método é chamado de SNAT. Os sistemas operacionais precisam acompanhar os pacotes em que os endereços IP foram alterados para garantir que os endereços IP de destino nos pacotes possam ser reescritos e que os pacotes possam ser encaminhados ao remetente inicial do pacote. Para atingir esses objetivos, você precisa ativar a função de encaminhamento de IP e configurar regras SNAT.
12. Use o editor vi para abrir o arquivo **/etc/sysctl.conf**, altere o valor de **net.ipv4.ip_forward** para **1** e insira **:wq** para salvar a alteração e sair.
13. Execute o seguinte comando para que a alteração tenha efeito:

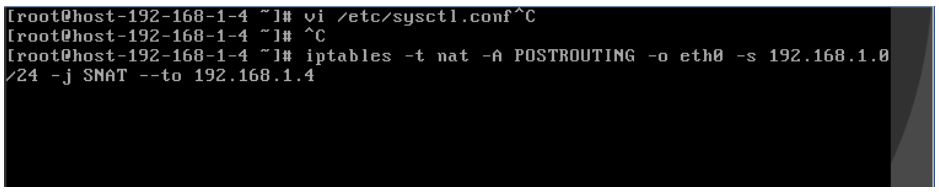
    sysctl -p /etc/sysctl.conf

14. Configure a função SNAT.

    Execute o comando a seguir para habilitar todos os ECSs na rede (por exemplo, 192.168.1.0/24) para acessar a Internet usando a função SNAT:

    iptables -t nat -A POSTROUTING -o eth0 -s subnet -j SNAT --to nat-instance-ip

    Figura 6-7 Configurar a SNAT

    NOTA

    Para garantir que a regra não será perdida após a reinicialização, escreva a regra no arquivo **/etc/rc.local**.

    1. Mude para o arquivo **/etc/sysctl.conf**:

       vi /etc/rc.local

    2. Execute **14** para configurar a SNAT.
    3. Salve a configuração e saia:

       :wq

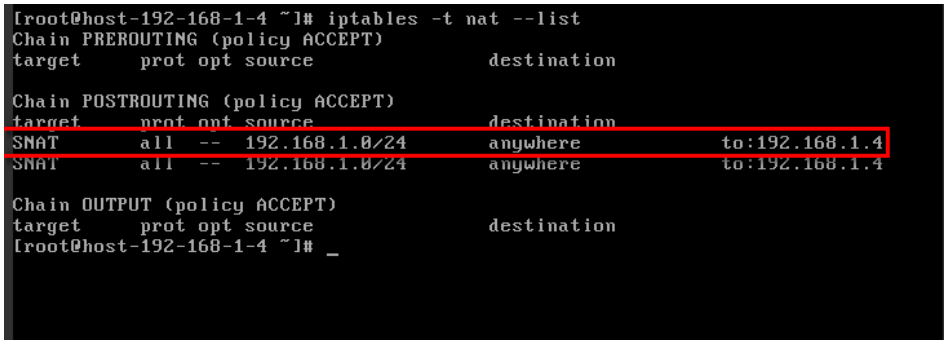
    4. Adicione as permissões de execução para o arquivo **rc.local**:

       # chmod +x /etc/rc.local

15. Verifique se a configuração foi bem-sucedida. Se informações semelhantes a **Figura 6-8** (por exemplo, 192.168.1.0/24) forem exibidas, a configuração foi bem-sucedida.

    iptables -t nat --list

    Figura 6-8 Verificar a configuração

16. Adicione uma rota. Para obter detalhes, consulte a seção **Adição de uma rota personalizada**.

    Defina o destino como **0.0.0.0/0** e o salto seguinte para o endereço IP privado ou virtual do ECS no qual a SNAT é implantada. Por exemplo, o próximo salto é **192.168.1.4**.

Depois que essas operações forem concluídas, se a comunicação de rede ainda falhar, verifique a configuração do grupo de segurança e de ACL da rede para ver se o tráfego necessário é permitido.

6.5 Criação de uma tabela de rota personalizada

Cenários

Você pode criar uma tabela de rota personalizada se não quiser usar a padrão.

Para usar uma tabela de rotas personalizada, você precisa enviar um tíquete de serviço. Você precisa clicar em **Increase quota** na página **Create Route Table** ou escolher **More** > **Service Tickets** > **Create Service Ticket** no canto superior direito da página. Para obter mais informações, consulte **Envio um tíquete de serviço**.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, em **Networking**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Route Tables**.
5. No canto superior direito, clique em **Create Route Table**. Na página exibida, configure os parâmetros conforme solicitado.

   Tabela 6-8 Descrições de parâmetro

Parâmetro	Descrição	Exemplo de valor
Name	O nome da tabela de rotas. Este parâmetro é obrigatório. O nome pode conter no máximo 64 caracteres, que podem ser letras, dígitos, sublinhados (_), hifens (-) e pontos (.). O nome não pode conter espaços.	rtb-001
VPC	A VPC à qual a tabela de rotas pertence. Este parâmetro é obrigatório.	vpc-001
Description	Informações complementares sobre a tabela de rotas. Este parâmetro é opcional. A descrição pode conter no máximo 255 caracteres e não pode conter colchetes angulares (< ou >).	-

Parâmetro	Descrição	Exemplo de valor
Route Settings	A informação da rota. Este parâmetro é opcional. Você pode adicionar uma rota ao criar a tabela de rotas ou depois que a tabela de rotas for criada. Para mais detalhes, consulte **Adição de uma rota personalizada**. Você pode clicar em + para adicionar mais rotas.	-

6. Clique em **OK**.

   Uma mensagem é exibida. Você pode determinar se deve associar a tabela de rotas a sub-redes imediatamente, conforme solicitado. Se você quiser se associar imediatamente, execute as seguintes operações:

   a. Clique em **Associate Subnet**. A página de detalhes da tabela de rotas é exibida.
   b. Clique em **Associate Subnet** e selecione as sub-redes de destino a serem associadas.
   c. Clique em **OK**.

6.6 Adição de uma rota personalizada

Cenários

Cada tabela de rotas contém uma rota de sistema padrão, que indica que os ECSs em uma VPC podem se comunicar entre si. Você pode adicionar rotas personalizadas conforme necessário para encaminhar o tráfego destinado ao destino para o próximo salto especificado.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, em **Networking**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Route Tables**.
5. Na lista da tabela de rotas, clique no nome da tabela de rotas à qual você deseja adicionar uma rota.
6. Clique em **Add Route** e defina os parâmetros conforme solicitado.

   Você pode clicar em + para adicionar mais rotas.

Figura 6-9 Adicionar rota

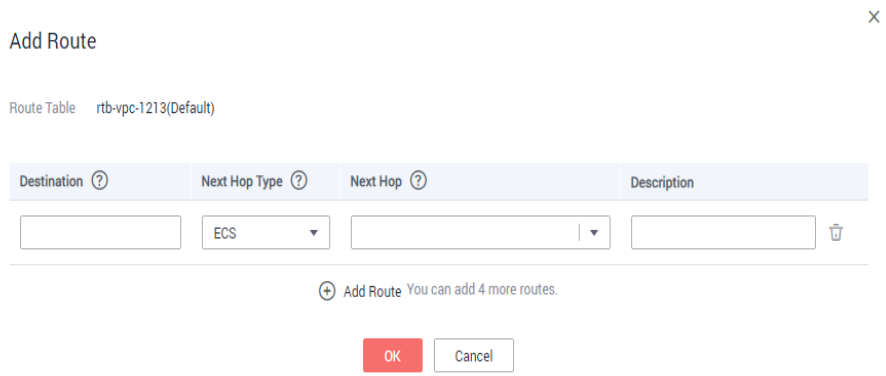


Tabela 6-9 Descrições de parâmetro

Parâmetro	Descrição	Exemplo de valor
Destination	O bloco CIDR de destino. O destino de cada rota deve ser único. O destino não pode se sobrepor a nenhum bloco CIDR de sub-rede na VPC.	192.168.0.0/16
Next Hop Type	Defina o tipo do próximo salto. Para obter detalhes sobre os tipos de recursos suportados, consulte **Tabela 6-1**. **NOTA** Quando você adiciona ou modifica uma rota personalizada em uma tabela de rota padrão, o tipo de próximo salto da rota não pode ser definido como **VPN gateway**, gateway **Direct Connect gateway** ou **Cloud connection**.	ECS
Next Hop	Defina o próximo salto. Os recursos na caixa de listagem suspensa são exibidos com base no tipo de próximo salto selecionado.	ecs-001
Description	Informação complementar sobre a rota. Este parâmetro é opcional. A descrição pode conter no máximo 255 caracteres e não pode conter colchetes angulares (< ou >).	-

7. Clique em **OK**.

6.7 Associação de uma tabela de rotas a uma sub-rede

Cenários

Depois que uma tabela de rotas é associada a uma sub-rede, suas rotas controlam o roteamento para a sub-rede e se aplicam a todos os recursos de nuvem na sub-rede.

Observações e restrições

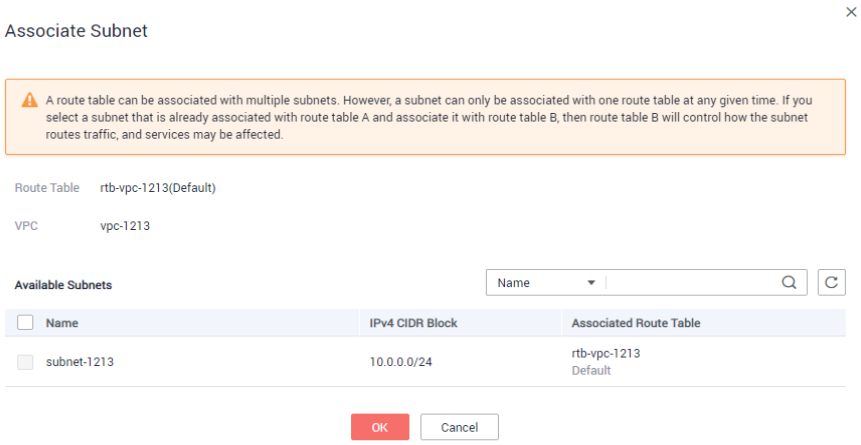
Uma sub-rede só pode ser associada a uma tabela de rotas.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, em **Networking**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Route Tables**.
5. Na lista da tabela de rotas, localize a linha que contém a tabela de rotas de destino e clique em **Associate Subnet** na coluna **Operation**.
6. Selecione a sub-rede a ser associada.

   Figura 6-10 Sub-rede associada



7. Clique em **OK**.

6.8 Alterando a tabela de rota associada a uma sub-rede

Cenários

Você pode alterar a tabela de rotas de uma sub-rede. Se a tabela de rotas de uma sub-rede for alterada, as rotas na nova tabela de rotas serão aplicadas a todos os recursos de nuvem na sub-rede.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, em **Networking**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.

4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Route Tables**.
5. Clique no nome da tabela de rotas de destino.
6. Na página de guia **Associated Subnets**, clique em **Change Route Table** na coluna **Operation** e selecione uma nova tabela de rotas conforme solicitado.
7. Clique em **OK**.

   Depois que a tabela de rotas para uma sub-rede for alterada, as rotas na nova tabela de rotas serão aplicadas a todos os recursos de nuvem na sub-rede.

6.9 Exibição da tabela de rotas associada a uma sub-rede

Cenários

Esta seção descreve como exibir a tabela de rotas associada a uma sub-rede.

Procedimento

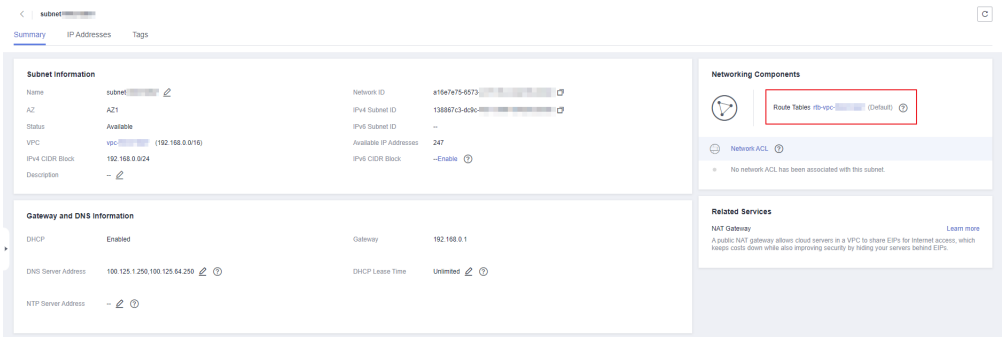
1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, em **Networking**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Route Tables**.

   A página **Subnets** é exibida.
5. Localize a sub-rede de destino e clique em seu nome.

   A página de detalhes da sub-rede é exibida.

   Figura 6-11 Exibir a tabela de rotas associada a uma sub-rede



6. À direita da página de detalhes da sub-rede, exiba a tabela de rotas associada à sub-rede.
7. Clique no nome da tabela de rotas.

   A página de detalhes da tabela de rotas é exibida. Você pode ver ainda mais as informações de rota.

6.10 Exibição de uma tabela de rotas

Cenários

Esta seção descreve como exibir informações detalhadas sobre uma tabela de rotas, incluindo:

- Informações básicas, como nome, tipo (padrão ou personalizado) e ID da tabela de rotas
- Rotas, como destino, próximo salto e tipo de rota (do sistema ou personalizada)
- Sub-redes associadas

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, em **Networking**, clique em **Virtual Private Cloud**.
   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Route Tables**.
   A lista da tabela de rotas é exibida.
5. Clique no nome da tabela de rotas de destino.
   A página de detalhes da tabela de rotas é exibida.
   a. Na página de guia **Summary**, exiba as informações básicas e rotas da tabela de rotas.
   b. Na página de guia **Associated Subnets**, exiba as sub-redes associadas à tabela de rotas.

6.11 Exclusão de uma tabela de rotas

Cenários

Esta seção descreve como excluir uma tabela de rotas personalizada.

Observações e restrições

- A tabela de rotas padrão não pode ser excluída.
  Ambas as tabelas de rotas padrão e personalizadas são gratuitas. A exclusão de uma VPC também excluirá sua tabela de rotas padrão.
- Uma tabela de rota personalizada não pode ser excluída se estiver associada a uma sub-rede.
  Você associa a sub-rede a outra tabela de rotas referindo-se a **Alterando a tabela de rota associada a uma sub-rede**, em seguida, exclui a tabela de rotas.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.

3. Na página inicial do console, em **Networking**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.

4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Route Tables**.

   A lista da tabela de rotas é exibida.

5. Localize a linha que contém a tabela de rotas que você deseja deletar e clique em **Delete** na coluna **Operation**.

   Uma caixa de diálogo de confirmação é exibida.

6. Clique em **Yes**.

6.12 Modificação de uma rota

Cenários

Modificar uma rota existente.

Observações e restrições

- A rota do sistema não pode ser modificada.
- As rotas fornecidas pelos serviços VPN, Direct Connect e Cloud Connect para a tabela de rotas padrão não podem ser modificadas.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, em **Networking**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.

4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Route Tables**.
5. Na lista da tabela de rotas, clique no nome da tabela de rotas de destino.
6. Localize a linha que contém a tag a ser editada e clique em **Modify** na coluna **Operation**.
7. Modifique as informações de rota na caixa de diálogo exibida.

Tabela 6-10 Descrições de parâmetro

Parâmetro	Descrição	Exemplo de valor
Destination	O bloco CIDR de destino. O destino de cada rota deve ser único. O destino não pode se sobrepor a nenhum bloco CIDR de sub-rede na VPC.	192.168.0.0/16

Parâmetro	Descrição	Exemplo de valor
Next Hop Type	Defina o tipo do próximo salto. Para obter detalhes sobre os tipos de recursos suportados, consulte **Tabela 6-1**. **NOTA** Quando você adiciona ou modifica uma rota personalizada em uma tabela de rota padrão, o tipo de próximo salto da rota não pode ser definido como **VPN gateway**, gateway **Direct Connect gateway** ou **Cloud connection**.	ECS
Next Hop	Defina o próximo salto. Os recursos na caixa de listagem suspensa são exibidos com base no tipo de próximo salto selecionado.	ecs-001
Description	Informação complementar sobre a rota. Este parâmetro é opcional. A descrição pode conter no máximo 255 caracteres e não pode conter colchetes angulares (< ou >).	-

8. Clique em **OK**.

6.13 Exclusão de uma rota

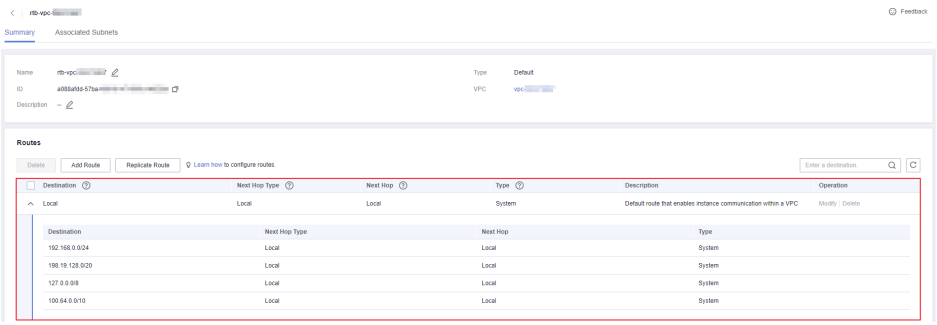
Cenários

Esta seção descreve como excluir uma rota personalizada de uma tabela de rotas.

Observações e restrições

- As rotas do sistema não podem ser excluídas.

  Figura 6-12 Rotas do sistema

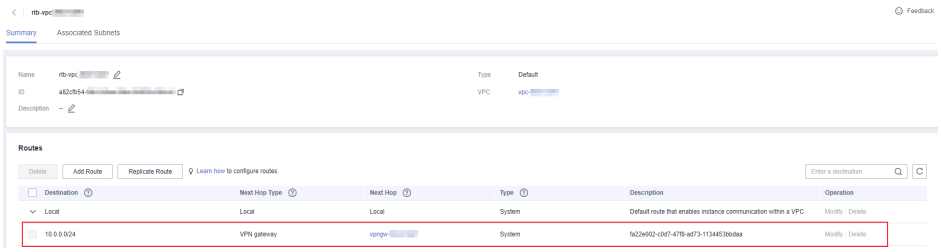


- As rotas entregues automaticamente por VPN, Direct Connect ou Cloud Connect para a tabela de rotas padrão não podem ser excluídas. Os próximos tipos de salto de tais rotas são:
  - Gateway de VPN

- Gateway da Direct Connect
- Conexão em nuvem

A figura a seguir mostra uma rota com **VPN gateway** como **Next Hop Type**. Se quiser excluir tal rota, clique no hiperlink do próximo salto para excluir o recurso correspondente.

Figura 6-13 Rota entregue por VPN



Procedimento

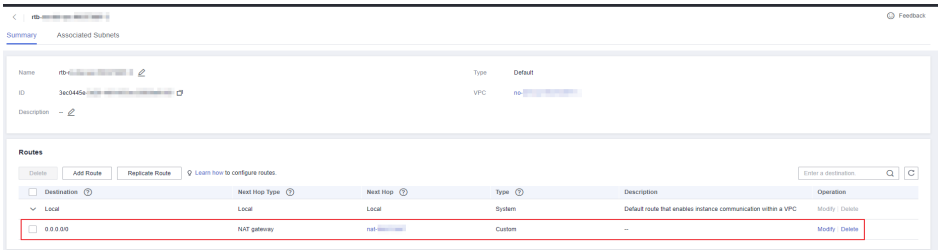
1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, em **Networking**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Route Tables**.

   A lista da tabela de rotas é exibida.
5. Localize a tabela de rotas de destino e clique em seu nome.

   A página de detalhes da tabela de rotas é exibida.

Figura 6-14 Excluir uma rota personalizada



6. Na lista de rotas, localize a linha que contém a rota a ser excluída e clique em **Delete** na coluna **Operation**.

   Uma caixa de diálogo de confirmação é exibida.
7. Confirme as informações e clique em **Yes**.

6.14 Replicação de uma rota

Cenários

Esta seção descreve como replicar rotas entre todas as tabelas de rotas de uma VPC. As tabelas de rota da VPC incluem as tabelas de rota padrão e personalizada.

Observações e restrições

Tabela 6-11 mostra os tipos de rotas que podem ser replicadas.

Por exemplo, se o próximo salto de uma rota for um servidor, essa rota poderá ser replicada para a tabela de rotas padrão ou personalizada. Se o próximo salto de uma rota for um gateway da Direct Connect, a rota não poderá ser replicada para a tabela de rotas padrão, mas poderá ser replicada para uma tabela de rotas personalizada.

Tabela 6-11 Descrição da replicação da rota

Tipo de próximo salto	Replicado para tabela de rota padrão	Replicado para tabela de rotas personalizada
Local	Incompatível	Incompatível
Servidor	Compatível	Compatível
NIC de extensão	Compatível	Compatível
Rede definida pelo usuário do BMS	Incompatível	Compatível
Gateway de VPN	Incompatível	Compatível
Gateway da Direct Connect	Incompatível	Compatível
Conexão em nuvem	Incompatível	Compatível
Interface de rede suplementar	Compatível	Compatível
Gateway NAT	Compatível	Compatível
Conexão de emparelhamento de VPC	Compatível	Compatível
Endereço IP virtual	Compatível	Compatível
Roteador empresarial	Compatível	Compatível
Firewall em nuvem	Compatível	Compatível

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, em **Networking**, clique em **Virtual Private Cloud**.
   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Route Tables**.
5. Na lista da tabela de rotas, localize a linha que contém a tabela de rotas de destino e clique em **Replicate Route** na coluna **Operation**.
6. Selecione a tabela de rotas de destino e, em seguida, a rota a ser replicada conforme solicitado.

As rotas listadas na página são aquelas que não existem na tabela de rotas de destino. Você pode selecionar uma ou mais rotas para replicar para a tabela de rotas de destino.

7. Clique em **OK**.

6.15 Exportação de informações de tabela de rotas

Cenários

Informações sobre todas as tabelas de rotas em sua conta podem ser exportadas como um arquivo do Excel para um diretório local. Esse arquivo registra o nome, o ID, a VPC, o tipo e o número de sub-redes associadas das tabelas de rotas.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Em **Networking**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Route Tables**.
5. Na página exibida, clique em no canto superior direito da lista da tabela de rotas.

   O sistema exportará automaticamente informações sobre todas as tabelas de rotas em sua conta na região atual como um arquivo do Excel para um diretório local.

7 Conexão de emparelhamento de VPC

7.1 Visão geral de conexão de emparelhamento de VPC

Uma conexão de emparelhamento VPC é uma conexão de rede entre duas VPCs em uma região que permite rotear o tráfego entre elas usando endereços IP privados. Os ECSs em qualquer VPC podem se comunicar como se estivessem na mesma rede. Você pode criar uma conexão de emparelhamento de VPC entre suas próprias VPCs ou entre sua VPC e a VPC de outra conta na mesma região. No entanto, não é possível criar uma conexão de emparelhamento de VPCs entre VPCs em regiões diferentes.

Para se conectar a VPCs de diferentes regiões, você pode usar a **Cloud Connect**.

Each account can have a maximum of 50 VPC peering connections in each region by default.

- VPC peering connections between VPCs from the same account: Each account can create a maximum of 50 VPC peering connections in one region.
- VPC peering connections between VPCs from different accounts: Accepted VPC peering connections use the quotas of both accounts. To-be-accepted VPC peering connections only use the quotas of accounts that request the connections.

  An account can create VPC peering connections with different accounts if the account has enough quota.

Observações e restrições

- If two VPCs connected by a VPC peering connection overlap with each other, there will be route conflicts and the VPC peering connection may not be usable.

  After a VPC peering connection is created, the ping command can be used to check whether two VPCs can communicate with each other, but cannot be used to check whether the gateway of the peer subnet is connected.
- If two VPCs overlap with each other, you can only create a VPC peering connection to enable communication between specific (non-overlapping) subnets in the VPCs. Ensure that the subnets to be peered do not overlap.
- If there are three VPCs, A, B, and C, and VPC A is peered with both VPC B and VPC C, but VPC B and VPC C overlap with each other, you cannot configure routes with the same destinations for VPC A.
- You can only have one VPC peering connection between two VPCs at the same time.

- A VPC peering connection cannot be established between VPCs in different regions.
  - To enable VPCs in different regions to communicate with each other, you can use Cloud Connect. For details, see **Communication Among VPCs Across Regions**.
  - If you need only few ECSs in different regions to communicate with each other, you can **assign and bind EIPs to the ECSs**.
- Even if VPC 1 and VPC 2 are connected using a VPC peering connection, ECSs in VPC 2 cannot access the Internet through an EIP of VPC 1. If you want to allow the ECSs in VPC 2 to access the Internet through the EIP of VPC 1, you can use a NAT gateway or **configure an SNAT server**. For details, see **Enabling Internet Connectivity for an ECS Without an EIP**.
- If you request a VPC peering connection with a VPC of another account, the connection cannot be used until the peer account accept the request. If you request a VPC peering connection with a VPC of your own, the system automatically accepts the request and activates the connection.
- To ensure security, do not accept VPC peering connections from unknown accounts.
- The owner of either VPC in a peering connection can delete the VPC peering connection at any time. Deleting a VPC peering connection will also all information about this connection, including routes added for the VPC peering connection.
- After a VPC peering connection is established, the local and peer accounts must add routes to the route tables of the local and peer VPCs to enable communication between the two VPCs.
- You cannot delete a VPC that has routes configured for a VPC peering connection.
- A VPC peering connection can be created between VPCs in same region even if one is created on the Huawei Cloud Chinese Mainland console and another on the Huawei Cloud international console.

7.2 Planos de configuração de conexão de emparelhamento de VPC

7.3 Criação de uma conexão de emparelhamento de VPC com uma outra VPC na sua conta.

Cenários

Para criar uma conexão de emparelhamento de VPC, primeiro crie uma solicitação para emparelhar com outra VPC. Você pode solicitar uma conexão de emparelhamento de VPC com outra VPC na sua conta, mas as duas VPCs devem estar na mesma região. O sistema aceitará automaticamente a solicitação.

Observações e restrições

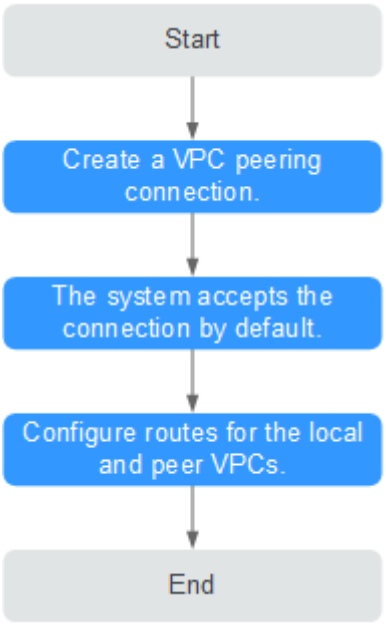
- A VPC peering connection cannot be established between VPCs in different regions.
  - To enable VPCs in different regions to communicate with each other, you can use Cloud Connect. For details, see **Communication Among VPCs Across Regions**.
  - If you need only few ECSs in different regions to communicate with each other, you can **assign and bind EIPs to the ECSs**.

- If two VPCs connected by a VPC peering connection overlap with each other, there will be route conflicts and the VPC peering connection may not be usable.

  After a VPC peering connection is created, the ping command can be used to check whether two VPCs can communicate with each other, but cannot be used to check whether the gateway of the peer subnet is connected.

Procedimento

Figura 7-1 Criar uma conexão de emparelhamento de VPC entre VPCs na sua conta



Se você criar uma conexão de emparelhamento de VPC entre duas VPCs na sua conta, o sistema aceitará a conexão por padrão. Você precisa adicionar rotas para as VPCs locais e de par para permitir a comunicação entre as duas VPCs.

Pré-requisitos

Foram criadas duas VPCs na mesma região.

Criar uma conexão de emparelhamento de VPC

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **VPC Peering Connections**.
5. No painel direito exibido, clique em **Create VPC Peering Connection**.
6. Configure os parâmetros conforme solicitado. Você deve selecionar **My account** para **Account**. **Tabela 7-1** lista os parâmetros a serem configurados.

Figura 7-2 Criar conexão de emparelhamento de VPC

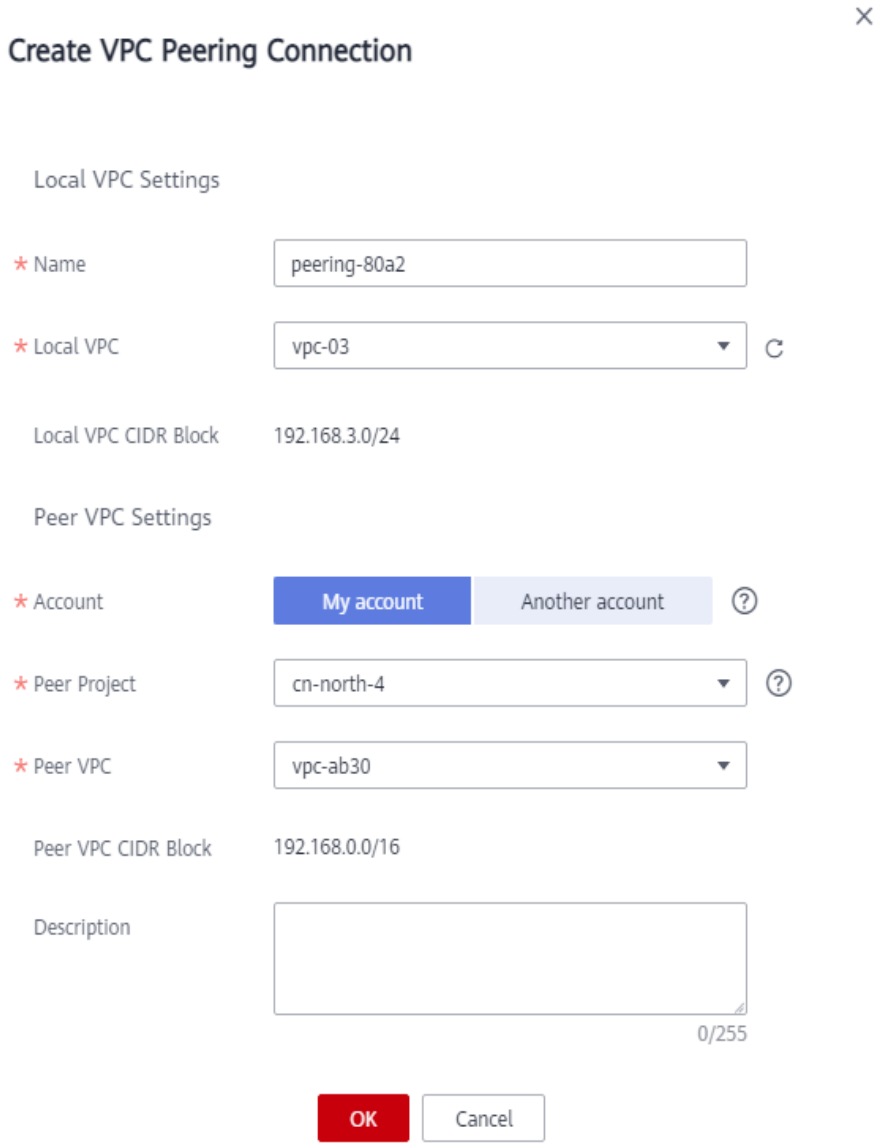


Tabela 7-1 Descrições de parâmetro

Parâmetro	Descrição	Exemplo de valor
Name	O nome da conexão de emparelhamento da VPC. O nome contém no máximo 64 caracteres, que consistem em letras, dígitos, hífenes (-) e sublinhados (_).	peering-001
Local VPC	A VPC local. Você pode selecionar uma na lista suspensa.	vpc_01

Parâmetro	Descrição	Exemplo de valor
Local VPC CIDR Block	O bloco CIDR para a VPC local.	192.168.10.0/24
Account	A conta à qual a VPC de par pertence. ● **My account**: a conexão de emparelhamento da VPC será criada entre duas VPCs, na mesma região, na sua conta. ● **Another account**: a conexão de emparelhamento da VPC será criada entre sua VPC e uma VPC em outra conta, na mesma região.	My account
Peer Project	O nome do projeto de par. O nome do projeto atual é usado por padrão.	aaa
Peer VPC	A VPC de par. Você pode selecionar uma na lista suspensa se a conexão de emparelhamento da VPC for criada entre duas VPCs em sua própria conta.	vpc_02
Peer VPC CIDR Block	O bloco CIDR para a VPC de par. As VPCs locais e de par não podem ter blocos CIDR correspondentes ou sobrepostos. Caso contrário, as rotas adicionadas para a conexão de emparelhamento de VPC podem não ter efeito.	192.168.2.0/24
Description	Informações complementares sobre a conexão de emparelhamento de VPC. Este parâmetro é opcional. A descrição da conexão de emparelhamento de VPC pode conter no máximo 255 caracteres e não pode conter colchetes angulares (< e >).	N/A

7. Clique em **OK**.

Adicionar rotas para uma conexão de emparelhamento de VPC

Se você solicitar uma conexão de emparelhamento de VPC com outra VPC em sua conta, o sistema aceitará automaticamente a solicitação. Para habilitar a comunicação entre as duas VPCs, você precisa adicionar rotas locais e de par na página **Route Tables** para a conexão de emparelhamento da VPC.

1. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.

2. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **VPC Peering Connections**.

3. Localize a conexão de emparelhamento da VPC para a qual você deseja configurar rotas na lista de conexões e clique no nome da conexão.

   A página que mostra os detalhes da conexão de emparelhamento da VPC é exibida.

4. Adicione rotas para a conexão de emparelhamento da VPC à tabela de rotas da VPC local:

   a. Clique na guia **Local Routes** e, em seguida, clique no hiperlink **Route Tables**.

      A guia **Summary** da tabela de rotas padrão para a VPC local é exibida.

   b. Clique na guia **Associated Subnets** para exibir as sub-redes associadas à tabela de rotas padrão.

      - Se houver a sub-rede a ser conectada pela conexão de emparelhamento da VPC,

        1) Clique na guia **Summary** da tabela de rotas e clique em **Add Route** para adicionar uma rota à tabela de rotas padrão.

           Tabela 7-2 descreve os parâmetros de rota.

      - Se a sub-rede a ser conectada pela conexão de emparelhamento da VPC não estiver lá,

        1) Retorne à lista de VPCs e alterne para a lista de sub-redes da VPC.
        2) Localize a linha que contém a sub-rede de destino a ser conectada pela conexão de emparelhamento da VPC e clique no nome da tabela de rotas na coluna **Route Table**.

           A guia **Summary** da tabela de rotas associada à sub-rede é exibida.
        3) Clique em **Add Route** para adicionar uma rota à tabela de rotas.

           Tabela 7-2 descreve os parâmetros de rota.

Tabela 7-2 Descrição do parâmetro

Parâmetro	Descrição	Exemplo de valor
Destination	O bloco CIDR da VPC peer, o bloco CIDR da sub-rede ou o endereço IP do ECS. Para mais detalhes, consulte **Planos de configuração de conexão de emparelhamento de VPC**.	192.168.1.0/24
Tipo de próximo salto	O próximo tipo de salto. Selecione **VPC peering connection**.	Conexão de emparelhamento de VPC
Next Hop	O endereço do próximo salto. Selecione o nome da conexão de emparelhamento VPC atual.	peering-001

Parâmetro	Descrição	Exemplo de valor
Description	Informação complementar sobre a rota. Este parâmetro é opcional. A descrição da rota pode conter no máximo 255 caracteres e não pode conter colchetes angulares (< ou >).	-

5. Adicione rotas para a conexão de peering da VPC à tabela de rotas da VPC de peer:
   a. Clique na guia **Peer Routes** e, em seguida, clique no hiperlink **Route Tables**.
      A guia **Summary** da tabela de rotas padrão para a VPC de mesmo nível é exibida.
   b. Clique na guia **Associated Subnets** para exibir as sub-redes associadas à tabela de rotas padrão.
      - Se houver a sub-rede a ser conectada pela conexão de emparelhamento da VPC,
        1) Clique na guia **Summary** da tabela de rotas e clique em **Add Route** para adicionar uma rota à tabela de rotas padrão.
           Tabela 7-3 descreve os parâmetros de rota.
        2) Clique em **OK**.
      - Se a sub-rede a ser conectada pela conexão de emparelhamento da VPC não estiver lá,
        1) Retorne à lista de VPCs e alterne para a lista de sub-redes da VPC.
        2) Localize a linha que contém a sub-rede de destino a ser conectada pela conexão de emparelhamento da VPC e clique no nome da tabela de rotas na coluna **Route Table**.
           A guia **Summary** da tabela de rotas associada à sub-rede é exibida.
        3) Clique em **Add Route** para adicionar uma rota à tabela de rotas.
           Tabela 7-3 descreve os parâmetros de rota.
        4) Clique em **OK**.

Tabela 7-3 Descrição do parâmetro

Parâmetro	Descrição	Exemplo de valor
Destination	O bloco CIDR da VPC local, bloco CIDR da sub-rede ou endereço IP do ECS. Para mais detalhes, consulte **Planos de configuração de conexão de emparelhamento de VPC**.	192.168.3.0/24
Next Hop Type	O tipo de próximo salto. Selecione **VPC peering connection**.	VPC peering connection

Parâmetro	Descrição	Exemplo de valor
Next Hop	O endereço do próximo salto. Selecione o nome da conexão de emparelhamento VPC atual.	peering-001
Description	Informação complementar sobre a rota. Este parâmetro é opcional. A descrição da rota pode conter no máximo 255 caracteres e não pode conter colchetes angulares (< ou >).	-

Depois que uma conexão de emparelhamento VPC é criada, as duas VPCs podem se comunicar entre si por meio de endereços IP privados. Você pode executar o comando **ping** para verificar se as duas VPCs podem se comunicar uma com a outra. Antes de executar o comando **ping**, certifique-se de que o grupo de segurança permita o tráfego ICMP de entrada. Para mais detalhes, consulte **Adição de uma regra de grupo de segurança**.

Links úteis

Por que a comunicação falhou entre VPCs conectadas por uma conexão de emparelhamento de VPC?

7.4 Criação de uma conexão de emparelhamento de VPC com uma VPC em outra conta

Cenários

O serviço VPC também permite que você crie uma conexão de emparelhamento VPC com uma VPC em outra conta. As duas VPCs devem estar na mesma região. Se você solicitar uma conexão de emparelhamento de VPC com uma VPC em outra conta, o proprietário da conta de par deverá aceitar a solicitação para ativar a conexão. Este serviço é gratuito e a sua conta e a conta de par não serão cobradas por isso.

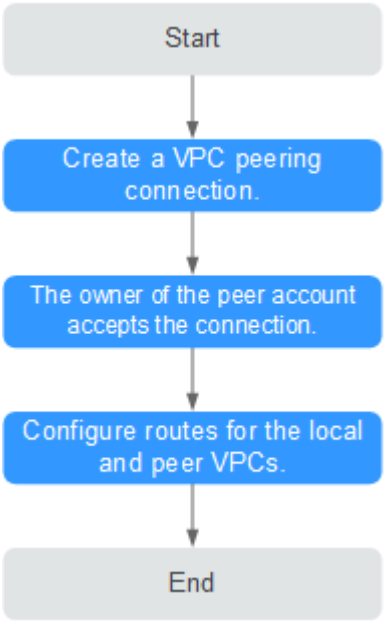
Observações e restrições

- A VPC peering connection cannot be established between VPCs in different regions.
  - To enable VPCs in different regions to communicate with each other, you can use Cloud Connect. For details, see **Communication Among VPCs Across Regions**.
  - If you need only few ECSs in different regions to communicate with each other, you can **assign and bind EIPs to the ECSs**.
- If two VPCs connected by a VPC peering connection overlap with each other, there will be route conflicts and the VPC peering connection may not be usable.

  After a VPC peering connection is created, the ping command can be used to check whether two VPCs can communicate with each other, but cannot be used to check whether the gateway of the peer subnet is connected.

Procedimento

Figura 7-3 Criar uma conexão de emparelhamento de VPC com uma VPC em outra conta



Se você criar uma conexão de emparelhamento da VPC entre sua VPC e uma VPC que esteja em outra conta, a conexão de emparelhamento da VPC estará no estado **Awaiting acceptance**. Depois que o proprietário da conta de par aceitar a conexão, o status da conexão será alterado para **Accepted**. Os proprietários das contas local e de par devem configurar as rotas exigidas pela conexão de emparelhamento da VPC para permitir a comunicação entre as duas VPCs.

Criar uma conexão de emparelhamento de VPC

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **VPC Peering Connections**.
5. No painel direito exibido, clique em **Create VPC Peering Connection**.
6. Configure os parâmetros conforme solicitado. Você deve selecionar **Another account** para **Account**.

Figura 7-4 Criar conexão de emparelhamento de VPC

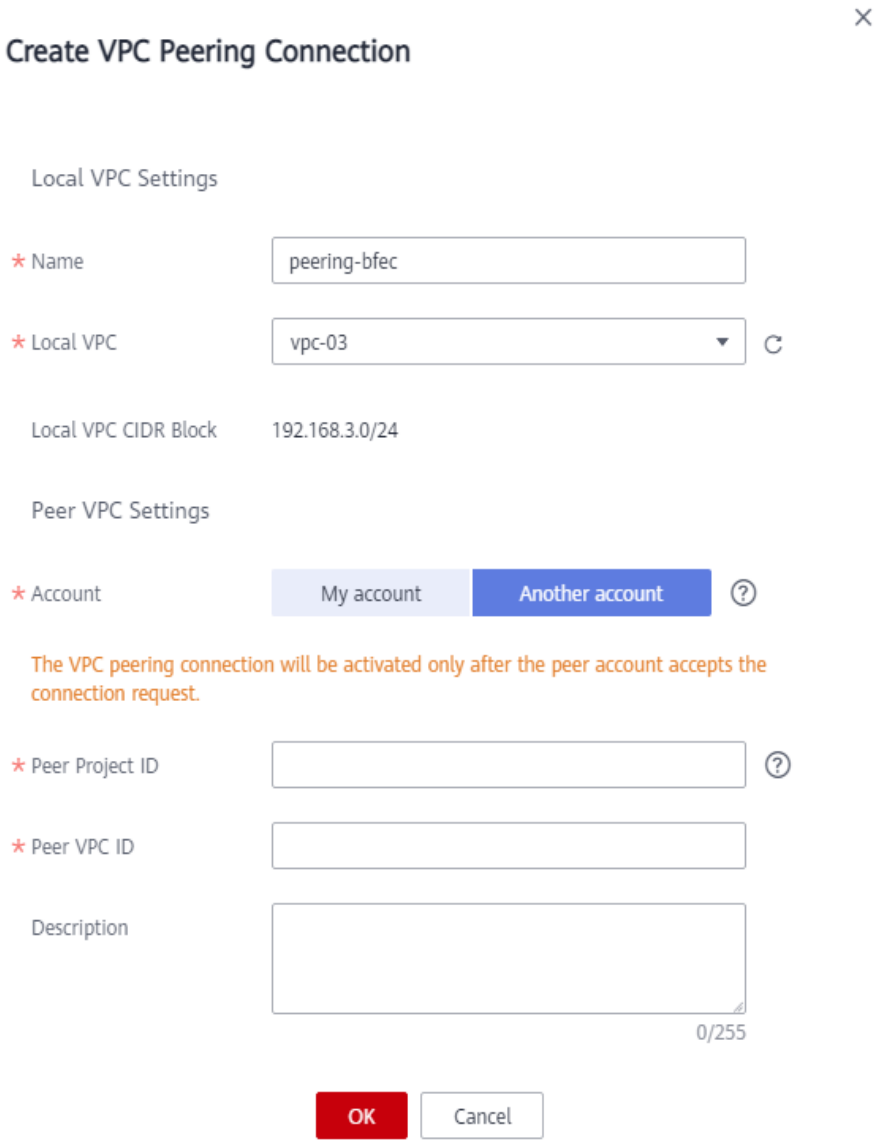


Tabela 7-4 Descrições de parâmetro

Parâmetro	Descrição	Exemplo de valor
Name	O nome da conexão de emparelhamento da VPC. O nome contém no máximo 64 caracteres, que consistem em letras, dígitos, hifens (-) e sublinhados (_).	peering-002
Local VPC	A VPC local. Você pode selecionar uma na lista suspensa.	vpc_01

Parâmetro	Descrição	Exemplo de valor
Account	A conta à qual a VPC para fazer emparelhamento pertence. ● **My account**: a conexão de emparelhamento da VPC será criada entre duas VPCs, na mesma região, na sua conta. ● **Another account**: a conexão de emparelhamento da VPC será criada entre sua VPC e uma VPC em outra conta, na mesma região.	Another account
Peer Project ID	Esse parâmetro está disponível somente quando **Another account** é selecionada. Para obter detalhes de como conseguir o ID ID do projeto de par, consulte **Obtenção do ID do projeto de par**.	N/D
Peer VPC ID	Esse parâmetro está disponível somente quando **Another account** é selecionada. Para obter detalhes de como conseguir o ID da VPC de par, consulte **Obtenção do da VPC de par**.	65d062b3-40fa-4204-8181-3538f527d2ab
Description	Informações complementares sobre a conexão de emparelhamento de VPC. Este parâmetro é opcional. A descrição da conexão de emparelhamento de VPC pode conter no máximo 255 caracteres e não pode conter colchetes angulares (< ou >).	N/D

7. Clique em **OK**.

NOTA

Se for exibida uma mensagem indicando que o ID da VPC e o ID do projeto corretos devem ser inseridos, a conexão de emparelhamento da VPC pode falhar ao ser criada porque as VPCs não estão na mesma região. Você pode usar a Cloud Connect para habilitar a comunicação entre VPCs em diferentes regiões. Para obter detalhes, consulte **Cloud Connect**.

Aceitar uma solicitação de conexão de emparelhamento de VPC

Se você solicitar uma conexão de emparelhamento de VPC com uma VPC em outra conta, o proprietário da conta de par deverá aceitar a solicitação para ativar a conexão.

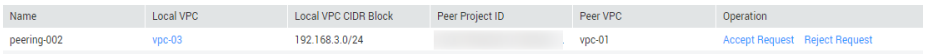
NOTA

Para garantir a segurança, não aceite conexões de emparelhamento de VPC de contas desconhecidas.

1. O proprietário da conta de par entra no console de gerenciamento.
2. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
3. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **VPC Peering Connections**.
4. Na lista de solicitações a serem tratadas, localize a linha que contém a conexão de emparelhamento de VPC de destino e clique em **Accept Request** na coluna **Operation**.

   Figura 7-5 Lista de solicitações a serem tratadas

5. Clique em **Yes** na caixa de diálogo exibida.

Recusar uma conexão de emparelhamento de VPC

O proprietário da conta de par pode rejeitar qualquer solicitação de conexão de emparelhamento de VPC recebida. Se uma solicitação de conexão de emparelhamento da VPC for rejeitada, a conexão não será estabelecida. Exclua a solicitação de conexão de emparelhamento de VPC rejeitada antes de criar uma conexão de emparelhamento de VPC entre as mesmas VPCs da solicitação rejeitada.

1. O proprietário da conta de par entra no console de gerenciamento.
2. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
3. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **VPC Peering Connections**.
4. Na lista de solicitações a serem tratadas, localize a linha que contém a conexão de emparelhamento VPC de destino e clique em **Reject Request** na coluna **Operation**.
5. Clique em **Yes** na caixa de diálogo exibida.

Adicionar rotas para uma conexão de emparelhamento de VPC

Se você solicitar uma conexão de emparelhamento de VPC com uma VPC em outra conta, o proprietário da conta de par deverá aceitar a solicitação. Para habilitar a comunicação entre as duas VPCs, os proprietários das contas local e de par precisam adicionar rotas na página **Route Tables** para a conexão de emparelhamento de VPC. O proprietário da conta local pode adicionar apenas a rota local porque não tem a permissão necessária para realizar operações na VPC de par. O proprietário da conta de par deve adicionar a rota de par. O procedimento para adicionar uma rota local e uma rota de par é o mesmo.

1. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
2. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **VPC Peering Connections**.
3. Localize a conexão de emparelhamento da VPC para a qual você deseja configurar rotas na lista de conexões e clique no nome da conexão.

A página que mostra os detalhes da conexão de emparelhamento de VPC é exibida.

4. Adicione rotas para a conexão de emparelhamento de VPC à tabela de rotas da VPC local:

   a. Clique na guia **Local Routes** e, em seguida, clique no hiperlink **Route Tables**.

      A guia **Summary** da tabela de rotas padrão para a VPC local é exibida.

   b. Clique na guia **Associated Subnets** para exibir as sub-redes associadas à tabela de rotas padrão.

      - Se houver a sub-rede a ser conectada pela conexão de emparelhamento de VPC,

        1) Clique na guia **Summary** da tabela de rotas e clique em **Add Route** para adicionar uma rota à tabela de rotas padrão.

           Tabela 7-5 descreve os parâmetros de rota.

      - Se a sub-rede a ser conectada pela conexão de emparelhamento de VPC não estiver lá,

        1) Retorne à lista de VPCs e alterne para a lista de sub-redes da VPC.
        2) Localize a linha que contém a sub-rede de destino a ser conectada pela conexão de emparelhamento de VPC e clique no nome da tabela de rotas na coluna **Route Table**.

           A guia **Summary** da tabela de rotas associada à sub-rede é exibida.
        3) Clique em **Add Route** para adicionar uma rota à tabela de rotas.

           Tabela 7-5 descreve os parâmetros de rota.

Tabela 7-5 Descrição do parâmetro

Parâmetro	Descrição	Exemplo de valor
Destination	O bloco CIDR da VPC de par, o bloco CIDR da sub-rede ou o endereço IP do ECS. Para mais detalhes, consulte **Planos de configuração de conexão de emparelhamento de VPC**.	192.168.1.0/24
Next Hop Type	O próximo tipo de salto. Selecione **VPC peering connection**.	VPC peering connection
Next Hop	O endereço do próximo salto. Selecione o nome da conexão de emparelhamento de VPC atual.	peering-001
Description	Informação complementar sobre a rota. Este parâmetro é opcional. A descrição pode conter no máximo 255 caracteres e não pode conter colchetes angulares (< ou >).	-

5. Adicione rotas para a conexão de emparelhamento de VPC à tabela de rotas da VPC de par:

a. Clique na guia **Peer Routes** e, em seguida, clique no hiperlink **Route Tables**.

   A guia **Summary** da tabela de rotas padrão para a VPC de mesmo nível é exibida.

b. Clique na guia **Associated Subnets** para exibir as sub-redes associadas à tabela de rotas padrão.

   - Se houver a sub-rede a ser conectada pela conexão de emparelhamento de VPC,

     1) Clique na guia **Summary** da tabela de rotas e clique em **Add Route** para adicionar uma rota à tabela de rotas padrão.

        Tabela 7-6 descreve os parâmetros de rota.

     2) Clique em **OK**.

   - Se a sub-rede a ser conectada pela conexão de emparelhamento de VPC não estiver lá,

     1) Retorne à lista de VPCs e alterne para a lista de sub-redes da VPC.
     2) Localize a linha que contém a sub-rede de destino a ser conectada pela conexão de emparelhamento de VPC e clique no nome da tabela de rotas na coluna **Route Table**.

        A guia **Summary** da tabela de rotas associada à sub-rede é exibida.

     3) Clique em **Add Route** para adicionar uma rota à tabela de rotas.

        Tabela 7-6 descreve os parâmetros de rota.

     4) Clique em **OK**.

Tabela 7-6 Descrição do parâmetro

Parâmetro	Descrição	Exemplo de valor
Destination	O bloco CIDR da VPC local, bloco CIDR da sub-rede ou endereço IP do ECS. Para mais detalhes, consulte **Planos de configuração de conexão de emparelhamento de VPC**.	192.168.3.0/24
Next Hop Type	O próximo tipo de salto. Selecione **VPC peering connection**.	VPC peering connection
Next Hop	O endereço do próximo salto. Selecione o nome da conexão de emparelhamento de VPC atual.	peering-001
Description	Informação complementar sobre a rota. Este parâmetro é opcional. A descrição pode conter no máximo 255 caracteres e não pode conter colchetes angulares (< ou >).	-

Depois que uma conexão de emparelhamento VPC é criada, as duas VPCs podem se comunicar entre si por meio de endereços IP privados. Você pode executar o comando **ping** para verificar se as duas VPCs podem se comunicar uma com a outra. Antes de executar o

comando **ping**, certifique-se de que o grupo de segurança permita o tráfego ICMP de entrada. Para mais detalhes, consulte **Adição de uma regra de grupo de segurança**.

Obtenção do ID do projeto de par

1. O proprietário da conta de par entra no console de gerenciamento.
2. Selecione **My Credentials** na lista suspensa de nome de usuário.
3. Na guia **Projects**, obtenha o ID de projeto necessário.

Obtenção do da VPC de par

1. O proprietário da conta de par entra no console de gerenciamento.
2. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
3. Clique no nome da VPC de destino.

   Na página exibida, você pode exibir o ID da VPC.

Links úteis

Por que a comunicação falhou entre VPCs conectadas por uma conexão de emparelhamento de VPC?

7.5 Visualização de conexões de emparelhamento de VPC

Cenários

Os proprietários das contas local e de par podem visualizar informações sobre as conexões de emparelhamento da VPC criadas e aquelas que ainda estão aguardando aceitação.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **VPC Peering Connections**.
5. No painel exibido à direita, veja as informações sobre as conexões de emparelhamento de VPC. Você pode pesquisar conexões de emparelhamento de VPC específicas por status de conexão ou por nome.
6. Clique no nome da conexão de emparelhamento da VPC. Na página exibida, visualize informações detalhadas sobre a conexão de emparelhamento de VPC.

7.6 Modificação de uma conexão de emparelhamento de VPC

Cenários

Os proprietários das contas local e de mesmo nível podem modificar uma conexão de emparelhamento de VPC em qualquer estado. O nome da conexão de emparelhamento da VPC pode ser alterado.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking** , clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **VPC Peering Connections**.
5. No painel exibido à direita, veja as informações sobre as conexões de emparelhamento de VPC. Você pode pesquisar conexões de emparelhamento de VPC específicas por status de conexão ou por nome.
6. Localize a conexão de emparelhamento VPC de destino e clique em **Modify** na coluna **Operation**. Na caixa de diálogo exibida, modifique as informações sobre a conexão de emparelhamento da VPC.
7. Clique em **OK**.

7.7 Exclusão de uma conexão de emparelhamento de VPC

Cenários

Os proprietários das contas local e de par podem excluir uma conexão de emparelhamento de VPC em qualquer estado. Depois que uma conexão de emparelhamento de VPC for excluída, as rotas configuradas para a conexão também serão excluídas automaticamente.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **VPC Peering Connections**.
5. No painel exibido à direita, veja as informações sobre as conexões de emparelhamento de VPC. Você pode pesquisar conexões de emparelhamento de VPC específicas por status de conexão ou por nome.

6. Localize a conexão de emparelhamento da VPC de destino e clique em **Delete** na coluna **Operation**.
7. Clique em **Yes** na caixa de diálogo exibida.

7.8 Exibição de rotas configuradas para uma conexão de emparelhamento de VPC

Cenários

Depois que as rotas são adicionadas para uma conexão de emparelhamento da VPC, os proprietários das contas local e de par podem visualizar informações sobre as rotas na página que mostra detalhes sobre a conexão de emparelhamento da VPC.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **VPC Peering Connections**.
5. Localize a conexão de emparelhamento da VPC de destino na lista de conexões.
6. Clique no nome da conexão de emparelhamento da VPC para alternar para a página que mostra detalhes sobre a conexão.
7. Na página exibida, clique na guia **Local Routes** e visualize as informações sobre a rota local adicionada para a conexão de emparelhamento da VPC.
8. Na página que mostra detalhes sobre a conexão de emparelhamento da VPC, clique na guia **Peer Routes** e visualize as informações sobre a rota de emparelhamento adicionada para a conexão de emparelhamento da VPC.

NOTA

Se você estabeleceu uma conexão de emparelhamento VPC, mas as duas VPCs não conseguem se comunicar uma com a outra, execute as etapas anteriores para verificar se as rotas local e de par estão configuradas corretamente.

7.9 Exclusão de uma rota de emparelhamento de VPC

Cenários

Depois que as rotas são adicionadas para uma conexão de emparelhamento de VPC, os proprietários das contas local e de emparelhamento podem excluir as rotas na página que mostra detalhes sobre a conexão de emparelhamento ou na página **Route Tables** .

Procedimento

1. Acesse o console de gerenciamento.

2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking** , clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **VPC Peering Connections**.
5. Na lista de conexões, localize a conexão de emparelhamento da VPC que deseja excluir rotas.
6. Clique no nome da conexão de emparelhamento da VPC para alternar para a página que mostra detalhes sobre a conexão.
7. Exclua a rota adicionada à tabela de rotas da VPC local:
   a. Clique na guia **Local Routes** e, em seguida, clique no hiperlink **Route Tables**.

      A guia **Summary** da tabela de rotas padrão para a VPC local é exibida.
   b. Localize a linha que contém a rota a ser excluída e clique em **Delete** na coluna **Operation**.
   c. Clique em **Yes**.
8. Exclua a rota adicionada à tabela de rotas da VPC de mesmo nível:
   a. Clique na guia **Peer Routes** e, em seguida, clique no hiperlink **Route Tables**.

      A guia **Summary** da tabela de rotas padrão para a VPC de mesmo nível é exibida.
   b. Localize a linha que contém a rota a ser excluída e clique em **Delete** na coluna **Operation**.
   c. Clique em **Yes** na caixa de diálogo exibida.

8 Log de fluxo de VPC

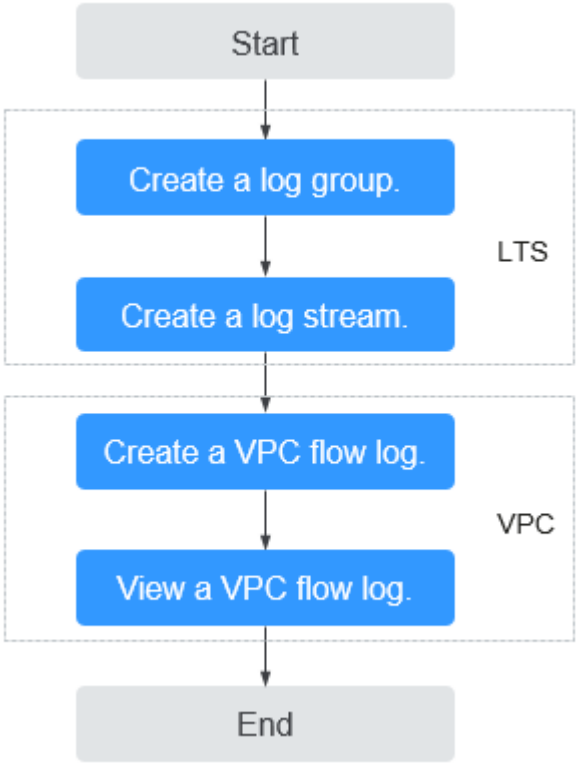
8.1 Visão geral de log de fluxo de VPC

Um log de fluxo de VPC registra informações sobre o tráfego indo e vindo de uma VPC. Os logs de fluxo da VPC ajudam a monitorar o tráfego de rede, analisar ataques de rede e determinar se o grupo de segurança e regras de ACL da rede requerem modificação.

Atualmente, a função de registro de fluxo do VPC é suportada em determinadas regiões. Você pode ir para **Visão geral de função** e clicar em **VPC Flow Log** para verificar.

Os logs de fluxo da VPC devem ser usados em conjunto com o Log Tank Service (LTS). Antes de criar um log de fluxo de VPC, você precisa criar um grupo de logs e um fluxo de log no LTS. **Figura 8-1** mostra o processo de configuração dos logs de fluxo de VPC.

Figura 8-1 Configurar logs de fluxo de VPC



A própria função de log de fluxo de VPC é gratuita, mas você pode ser cobrado por outros recursos usados. Por exemplo, o armazenamento de registros de log de fluxo de VPC será cobrado. Para obter detalhes, consulte Guia de usuário do Log Tank Service.

Observações e restrições

- Atualmente, apenas ECSs S2, M2, Hc2, D2, Pi1, S3, C3, M3, H3, Ir3, I3, S6, E3, C3ne, M3ne, G5, P2v, C6, M6, Pi1 e H3 suportam logs de fluxo de VPC.

  Para obter detalhes sobre tipos de ECS, consulte **Tipos de ECS**.
- Por padrão, você pode criar no máximo 10 logs de fluxo de VPC.
- Por padrão, um máximo de 400 000 registros de log de fluxo são suportados.

8.2 Criação de um log de fluxo de VPC

Cenários

Um log de fluxo de VPC registra informações sobre o tráfego indo e vindo de uma VPC.

Pré-requisitos

Certifique-se de que as seguintes operações foram realizadas no console do LTS:

- Criar um grupo de log.
- Criar um fluxo de log.

Para obter mais informações sobre o serviço LTS, consulte o *Guia de usuário do Log Tank Service*.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, em **Networking**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **VPC Flow Logs**.
5. No canto superior direito, clique em **Create VPC Flow Log**. Na página exibida, configure os parâmetros conforme solicitado.

Tabela 8-1 Descrições de parâmetro

Parâmetro	Descrição	Exemplo de valor
Name	O nome do log de fluxo da VPC. O nome pode conter no máximo 64 caracteres, que podem ser letras, dígitos, sublinhados (_), hifens (-) e pontos (.). O nome não pode conter espaços.	flowlog-495d
Resource Type	O tipo de recursos cujo tráfego deve ser registrado. Você pode selecionar **NIC**, **Subnet** ou **VPC**.	NIC
Resource	A NIC específica cujo tráfego deve ser registrado. **NOTA** Recomendamos que você selecione um ECS que esteja no estado em execução. Se um ECS no estado interrompido for selecionado, reinicie o ECS depois de criar o registro de fluxo da VPC para registrar com precisão as informações sobre o tráfego que vai de e para a NIC do ECS.	N/A
Filter	● **All traffic**: especifica que o tráfego aceito e rejeitado do recurso especificado será registrado. ● **Accepted traffic**: especifica que somente o tráfego aceito do recurso especificado será registrado. O tráfego aceito refere-se ao tráfego permitido pelo grupo de segurança ou ACLs da rede. ● **Rejected traffic**: especifica que somente o tráfego rejeitado do recurso especificado será registrado. O tráfego rejeitado refere-se ao tráfego negado pela ACLs da rede.	Todos
Log Group	O grupo de logs criado no LTS.	lts-group-wule

Parâmetro	Descrição	Exemplo de valor
Log Stream	O fluxo de log criado no LTS.	lts-topic-wule
Description	Informações complementares sobre o log de fluxo da VPC. Este parâmetro é opcional. A descrição do log de fluxo da VPC pode conter no máximo 255 caracteres e não pode conter colchetes angulares (< ou >).	N/A

NOTA

Apenas dois logs de fluxo, cada um com um filtro diferente, podem ser criados para um único recurso no mesmo grupo de logs e fluxo de log. Cada registro de fluxo de VPC deve ser exclusivo.

6. Clique em **OK**.

8.3 Exibição de um log de fluxo de VPC

Cenários

Exibir informações sobre seu registro de log de fluxo.

A janela de captura é de aproximadamente 10 minutos, o que indica que um registro de log de fluxo será gerado a cada 10 minutos. Depois de criar um log de fluxo de VPC, você precisa aguardar cerca de 10 minutos antes de poder visualizar o registro de log de fluxo.

NOTA

Se um ECS estiver no estado parado, seus registros de log de fluxo não serão exibidos.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, em **Networking**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **VPC Flow Logs**.
5. Localize o registro de fluxo da VPC de destino e clique em **View Log Record** na coluna **Operation** para exibir informações sobre o registro de log de fluxo no LTS.

   O registro do log de fluxo está no seguinte formato:

   ```
   <version> <project-id> <interface-id> <srcaddr> <dstaddr> <srcport> <dstport>
   <protocol> <packets> <bytes> <start> <end> <action> <log-status>
   ```

   Exemplo 1: veja a seguir um exemplo de registro de fluxo no qual os dados foram registrados durante a janela de captura:

   ```
   1 5f67944957444bd6bb4fe3b367de8f3d 1d515d18-1b36-47dc-a983-bd6512aed4bd
   192.168.0.154 192.168.3.25 38929 53 17 1 96 1548752136 1548752736 ACEITAR OK
   ```

   O valor **1** indica a versão do log de fluxo de VPC. Tráfego com um tamanho de 96 bytes para NIC **1d515d18-1b36-47dc-a983-bd6512aed4bd** durante os últimos 10 minutos

(das 16:55:36 às 17:05:36 em 29 de janeiro, 2019) foi permitido. Um pacote de dados foi transmitido pelo protocolo UDP do endereço IP de origem **192.168.0.154** e da porta **38929** para o endereço IP de destino **192.168.3.25** e a porta **53**.

Exemplo 2: este é um exemplo de um registro de log de fluxo no qual nenhum dado foi registrado durante a janela de captura:

```
1 5f67944957444bd6bb4fe3b367de8f3d 1d515d18-1b36-47dc-a983-bd6512aed4bd - - -
- - - - 1431280876 1431280934 - NODATA
```

Exemplo 3: este é um exemplo de um registro de registro de fluxo no qual os dados foram ignorados durante a janela de captura:

```
1 5f67944957444bd6bb4fe3b367de8f3d 1d515d18-1b36-47dc-a983-bd6512aed4bd - - -
- - - - 1431280876 1431280934 - SKIPDATA
```

Tabela 8-2 descreve os campos de um registro de log de fluxo.

Tabela 8-2 Descrição do campo de registo

Campo	Descrição	Exemplo de valor
version	A versão do log de fluxo de VPC.	1
project-id	O ID do projeto.	5f67944957444bd6bb4fe3b367de8f3d
interface-id	O ID da NIC para o qual o tráfego é gravado.	1d515d18-1b36-47dc-a983-bd6512aed4bd
srcaddr	O endereço IP de origem.	192.168.0.154
dstaddr	O endereço IP de destino.	192.168.3.25
srcport	A porta de origem.	38929
dstport	A porta de destino.	53
protocol	O número de protocolo Internet Assigned Numbers Authority (IANA) do tráfego. Para obter detalhes, consulte **Números de protocolo de Internet atribuídos**.	17
packets	O número de pacotes transferidos durante a janela de captura.	1
bytes	O número de bytes transferidos durante a janela de captura.	96
start	O tempo, em segundos Unix, do início da janela de captura.	1548752136
end	O tempo, em segundos Unix, do fim da janela de captura.	1548752736

Campo	Descrição	Exemplo de valor
action	A ação associada ao tráfego: ● **ACCEPT**: o tráfego gravado foi permitido pelos grupos de segurança ou ACLs da redes. ● **REJECT**: o tráfego gravado foi negado pelas ACLs da redes.	ACCEPT
log-status	O status de registro de log de fluxo de VPC: ● **OK**: os dados são registrados normalmente nos destinos escolhidos. ● **NODATA**: não havia tráfego da configuração **Filter** de ou para a NIC durante a janela de captura. ● **SKIPDATA**: alguns registros de log de fluxo foram ignorados durante a janela de captura. Isso pode ser causado por uma restrição de capacidade interna ou um erro interno. Exemplo: quando o **Filter** é ajustado a **Accepted traffic**, se há um tráfego aceitado, o valor de **log-status** é **OK**. Se não houver tráfego aceito, o valor de **log-status** é **NODATA**, independentemente de haver tráfego rejeitado. Se algum tráfego aceito é ignorado anormalmente, o valor de **log-status** é **SKIPDATA**.	OK

Você pode digitar uma palavra-chave na página de detalhes do fluxo de log no console do LTS para procurar registros de log de fluxo.

8.4 Ativação ou desativação do log de fluxo de VPC

Cenários

Depois que um log de fluxo de VPC é criado, o log de fluxo de VPC é ativado automaticamente. Se você não precisar registrar dados de tráfego, poderá desativar o log de fluxo VPC correspondente. O log de fluxo de VPC desativado pode ser ativado novamente.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, em **Networking**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **VPC Flow Logs**.
5. Localize o log de fluxo da VPC a ser ativado ou desativado e clique em **Enable** ou **Disable** na coluna **Operation**.
6. Clique em **Yes**.

8.5 Exclusão de um log de fluxo de VPC

Cenários

Excluir um log de fluxo de VPC que não seja necessário. A exclusão de um log de fluxo de VPC não excluirá os registros de log de fluxo existentes no LTS.

NOTA

Se uma NIC que usa um log de fluxo de VPC for excluída, o log de fluxo será excluído automaticamente. No entanto, os registos de log de fluxo não são eliminados.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, em **Networking**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **VPC Flow Logs**.
5. Localize a linha que contém o log de fluxo de VPC a ser excluído e clique em **Delete** na coluna **Operation**.
6. Clique em **Yes** na caixa de diálogo exibida.

9 Endereço IP virtual

9.1 Visão geral do endereço IP virtual

What Is a Virtual IP Address?

A virtual IP address can be shared among multiple ECSs. An ECS can have both private and virtual IP addresses, and you can access the ECS through either IP address. A virtual IP address has the same network access capabilities as a private IP address, including layer 2 and layer 3 communication in VPCs, access between VPCs using VPC peering connections, as well as access through EIPs, VPN connections, and Direct Connect connections.

You can bind ECSs deployed in active/standby mode with the same virtual IP address, and then bind an EIP to the virtual IP address. Virtual IP addresses can work together with Keepalived to ensure high availability and disaster recovery. If the active ECS is faulty, the standby ECS automatically takes over services from the active one.

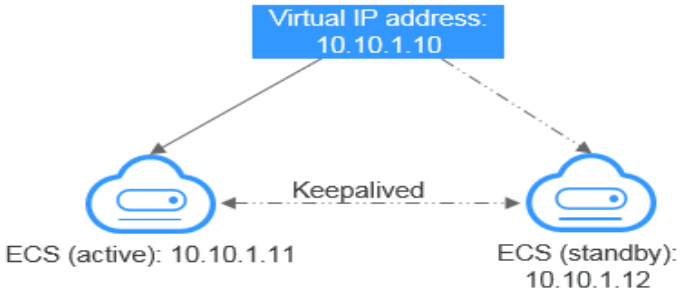
Redes

Virtual IP addresses are used for high availability and can work together with Keepalived to make active/standby ECS switchover possible. This way if one ECS goes down for some reason, the other one can take over and services continue uninterrupted. ECSs can be configured for HA or as load balancing clusters.

- **Networking mode 1**: HA

  If you want to improve service availability and avoid single points of failure, you can deploy ECSs in the active/standby mode or deploy one active ECS and multiple standby ECSs. In this arrangement, the ECSs all use the same virtual IP address. If the active ECS becomes faulty, a standby ECS takes over services from the active ECS and services continue uninterrupted.

Figura 9-1 Networking diagram of the HA mode

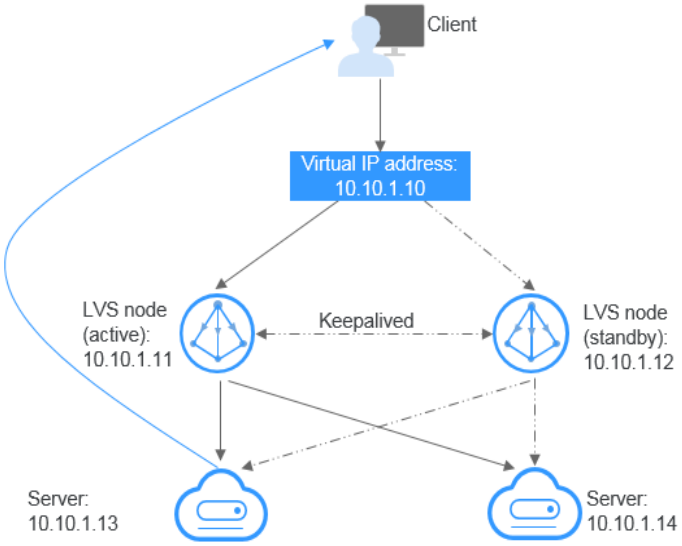


- In this configuration, a single virtual IP address is bound to two ECSs in the same subnet.
- Keepalived is then used to configure the two ECSs to work in the active/standby mode. Follow industry standards for configuring Keepalived. The details are not included here.

- **Modo de funcionamento em rede 2**: cluster de balanceamento de carga HA

  If you want to build a high-availability load balancing cluster, use Keepalived and configure LVS nodes as direct routers.

Figura 9-2 Cluster de balanceamento de carga HA



- Bind a single virtual IP address to two ECSs.
- Configure the two ECSs as LVS nodes working as direct routers and use Keepalived to configure the nodes in the active/standby mode. The two ECSs will evenly forward requests to different backend servers.
- Configure two more ECSs as backend servers.
- Disable the source/destination check for the two backend servers.
- Verifique se a verificação de origem/destino está desabilitada nos LVS de ECSs ativos e em espera. Se você vincular um ECS a um endereço IP virtual no console

de gerenciamento, a verificação de origem/destino será desativada automaticamente. Se você vincular um ECS a um endereço IP virtual chamando APIs, precisará desativar manualmente a verificação de origem/destino.

Follow industry standards for configuring Keepalived. The details are not included here.

Application Scenarios

- Accessing the virtual IP address through an EIP

  If your application has high availability requirements and needs to provide services through the Internet, it is recommended that you bind an EIP to a virtual IP address.
- Using a VPN, Direct Connect, or VPC peering connection to access a virtual IP address

  To ensure high availability and access to the Internet, use a VPN for security and Direct Connect for a stable connection. The VPC peering connection is needed so that the VPCs in the same region can communicate with each other.

Observações e restrições

- Virtual IP addresses are not recommended when multiple NICs in the same subnet are configured on an ECS. It is too easy for there to be route conflicts on the ECS, which would cause communication failure using the virtual IP address.
- A virtual IP address can only be bound to ECSs in the same subnet.
- O encaminhamento de IP deve ser desabilitado no ECS em espera. Para mais detalhes, consulte **Desativação de encaminhamento IP no ECS em espera**.
- Cada endereço IP virtual pode ser vinculado a apenas um EIP.
- It is recommended that no more than eight virtual IP addresses be bound to an ECS.
- It is recommended that no more than 10 ECSs be bound to a virtual IP address.
- Endereços IP virtuais e NICs de extensão não podem ser usados para acessar diretamente os serviços da HUAWEI CLOUD, como DNS. Você pode usar o VPCEP para acessar esses serviços. Para obter detalhes, consulte **Compra de um ponto de extremidade da VPC**.

9.2 Atribuição de um endereço IP virtual

Cenários

Se um ECS exigir um endereço IP virtual ou se um endereço IP virtual precisar ser reservado, você poderá atribuir um endereço IP virtual da sub-rede.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Subnets**.
5. Na lista de sub-redes, clique no nome da sub-rede à qual um endereço IP virtual será atribuído.

6. Clique na guia **IP Addresses** e clique em **Assign Virtual IP Address**.
7. Selecione um modo de atribuição de endereço IP virtual.
   - **Automatic**: o sistema atribui um endereço IP automaticamente.
   - **Manual**: você pode especificar um endereço IP.
8. Selecione **Manual** e insira um endereço IP virtual.
9. Clique em **OK**.

Em seguida, você pode consultar o endereço IP virtual atribuído na lista de endereços IP.

9.3 Vinculação de um endereço IP virtual a um EIP ou ECS

Cenários

Você pode vincular um endereço IP virtual a um EIP para que possa acessar os ECSs vinculados ao mesmo endereço IP virtual da Internet. Esses ECSs podem funcionar no modo ativo/em espera para melhorar a tolerância a falhas.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Subnets**.
5. Na lista de sub-redes, clique no nome da sub-rede à qual o endereço IP virtual pertence.
6. Clique na guia **IP Addresses**, localize a linha que contém o endereço IP virtual de destino e clique em **Bind to EIP** ou **Bind to Server** na coluna **Operation**.
7. Selecione o EIP desejado ou o ECS e sua NIC.

   NOTA

   - Se o ECS tiver várias NICs, vincule o endereço IP virtual à NIC principal.
   - Vários endereços IP virtuais podem ser vinculados a uma NIC do ECS.
8. Clique em **OK**.
9. Configure manualmente o endereço IP virtual vinculado a um ECS.

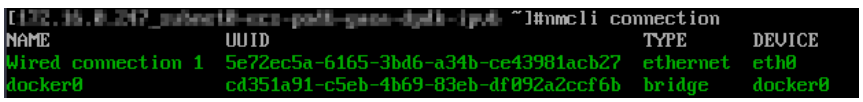
   Depois que um endereço IP virtual é vinculado a uma NIC do ECS, você precisa configurar manualmente o endereço IP virtual no ECS.

   Linux OS (CentOS 7.2 64bit é usado como um exemplo.)

   a. Execute o seguinte comando para obter a NIC à qual o endereço IP virtual deve ser vinculado e a conexão da NIC:

      nmcli connection

      Informação semelhante à seguinte foi exibida:



A saída do comando neste exemplo é descrita da seguinte forma:

- **eth0** na coluna **DEVICE** indica a NIC à qual o endereço IP virtual deve ser vinculado.
- **Wired connection 1** na coluna **NAME** indica a conexão da NIC.

b. Execute o seguinte comando para adicionar o endereço IP virtual para a conexão de destino:

nmcli connection modify "*CONNECTION***" ipv4.addresses** *VIP*

Configure os parâmetros da seguinte forma:

- CONNECTION: conexão da NIC obtida em **9.a**.
- VIP: endereço IP virtual a ser adicionado.
  - Se você adicionar vários endereços IP virtuais por vez, separe-os com vírgulas (,).
  - Se um endereço IP virtual já existir e você precisar adicionar um novo, o comando deve conter os endereços IP virtuais novos e originais.

Comandos de exemplo:

- Adicionar um único endereço IP virtual: **nmcli connection modify "Wired connection 1" ipv4.addresses 172.16.0.125**
- Adicionar vários endereços IP virtuais: **nmcli connection modify "Wired connection 1" ipv4.addresses 172.16.0.125,172.16.0.126**

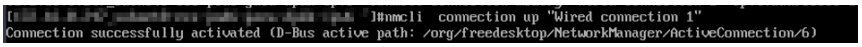
c. Execute o seguinte comando para que a configuração entre em vigor:

nmcli connection up "*CONNECTION***"**

Neste exemplo, execute o seguinte comando:

nmcli connection up "Wired connection 1"

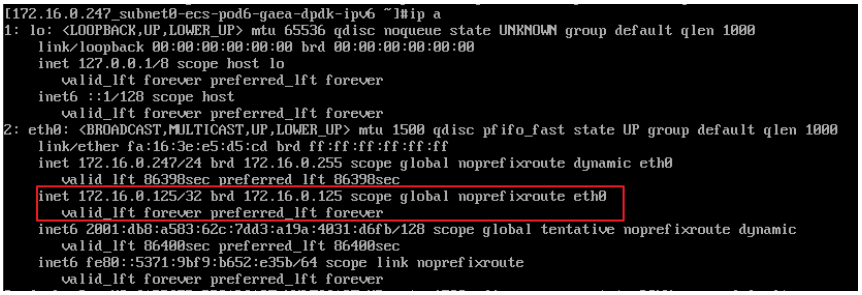
Informação semelhante à seguinte foi exibida:



d. Execute o seguinte comando para verificar se o endereço IP virtual foi vinculado:

ip a

Informação semelhante à seguinte foi exibida: Na saída do comando, o endereço IP virtual 172.16.0.125 está vinculado à NIC eth0.



Windows OS (o servidor Windows é usado como um exemplo aqui.)

a. No **Control Panel**, clique em C**Network and Sharing Center** e clique na conexão local correspondente.

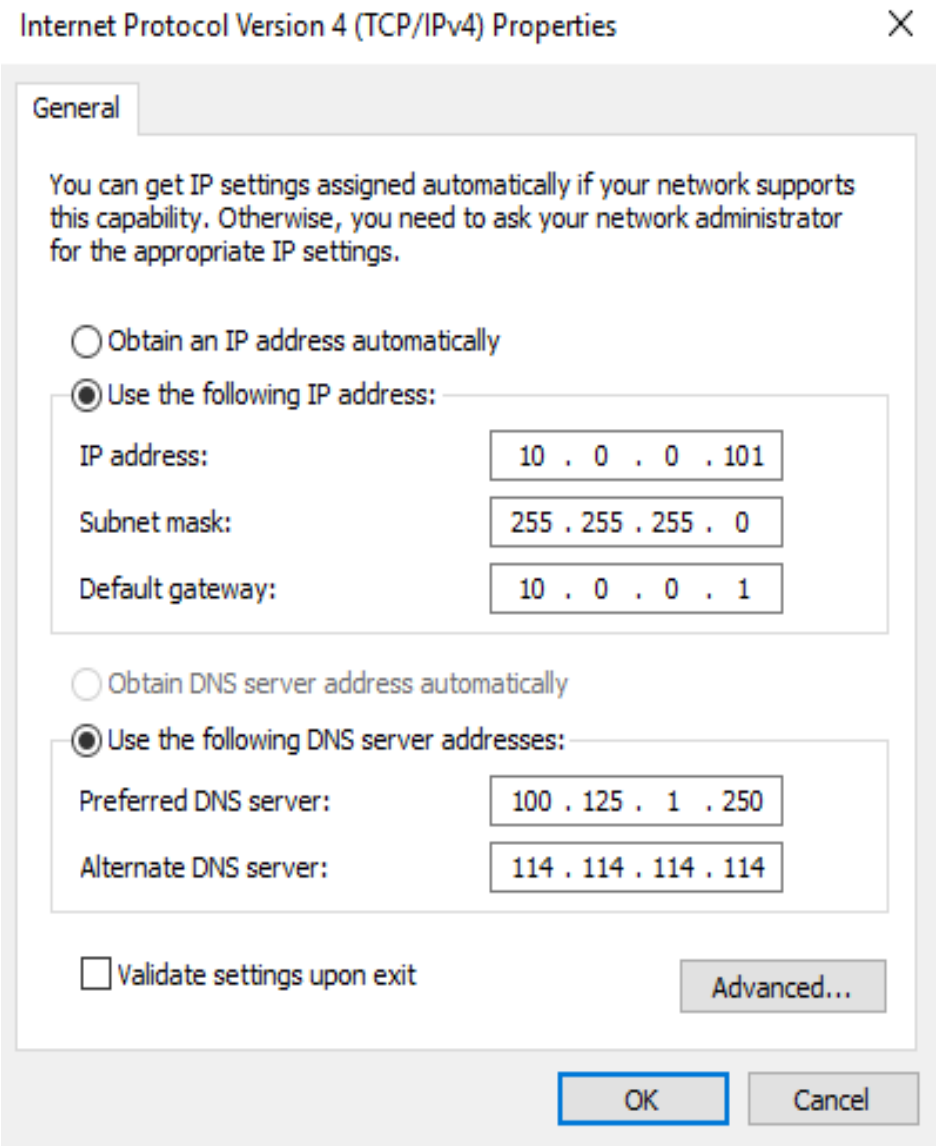
b. Na página exibida, clique em **Properties**.

c. Na página de guia **Network**, selecione **Internet Protocol Version 4 (TCP/IPv4)**.

d. Clique em **Properties**.

e. Selecione **Use the following IP address** e defina **IP address** como o endereço IP privado do ECS, por exemplo, 10.0.0.101.

Figura 9-3 Configurar o endereço IP privado

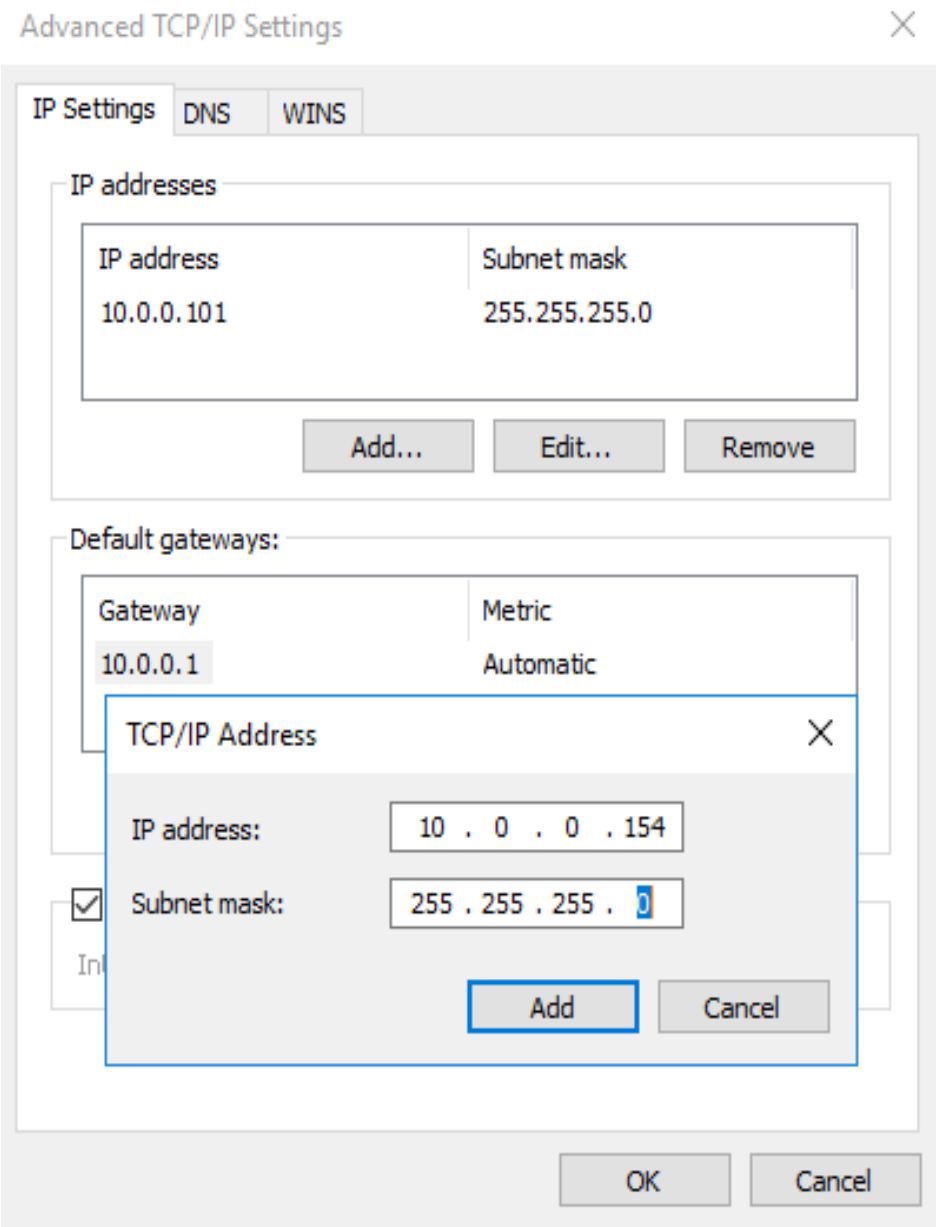


f. Clique em **Advanced**.

g. Na guia **IP Settings**, clique em **Add** na área **IP addresses**.

Adicione o endereço IP virtual. Por exemplo, 10.0.0.154.

Figura 9-4 Configurar o endereço IP virtual



h. Clique em **OK**.

i. No menu **Start**, abra a janela de linha de comando do Windows e execute o seguinte comando para verificar se o endereço IP virtual foi configurado:

   ipconfig /all

   Na saída do comando, **IPv4 Address** é o endereço IP virtual 10.0.0.154, indicando que o endereço IP virtual da NIC do ECS foi configurado corretamente.

9.4 Vinculação de um endereço IP virtual a um EIP

Cenários

Esta seção descreve como vincular um endereço IP virtual a um EIP.

Pré-requisitos

- Você configurou a rede do ECS com base em **Redes** e certifique-se de que o ECS tenha sido vinculado a um endereço IP virtual.
- Você atribuiu um EIP.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Elastic IP**.
4. Localize a linha que contém o EIP a ser vinculado ao endereço IP virtual e clique em **Bind** na coluna **Operation**.
5. Na caixa de diálogo **Bind EIP**, defina **Instance Type** como **Virtual IP address**.
6. Na lista de endereços IP virtuais, selecione o endereço IP virtual a ser vinculado e clique em **OK**.

9.5 Acesso de um endereço IP virtual usando uma VPN

Procedimento

1. Configure a rede do ECS com base em **Redes**.
2. Crie uma VPN.

A VPN pode ser usada para acessar o endereço IP virtual do ECS.

9.6 Uso de uma conexão Direct Connect para acessar o endereço IP virtual

Procedimento

1. Configure a rede do ECS com base em **Redes**.
2. Crie uma conexão Direct Connect.

A conexão Direct Connect criada pode ser usada para acessar o endereço IP virtual do ECS.

9.7 Uso de uma conexão de emparelhamento de VPC para acessar o endereço IP virtual

Procedimento

1. Configure a rede do ECS com base em **Redes**.
2. Crie uma conexão de emparelhamento de VPC.

Você pode acessar o endereço IP virtual do ECS por meio da conexão de emparelhamento da VPC.

9.8 Desativação de encaminhamento IP no ECS em espera

Para um ECS do Linux:

1. Log in to standby ECS and run the following command to check whether the IP forwarding is enabled:

   cat /proc/sys/net/ipv4/ip_forward

   In the command output, **1** indicates it is enabled, and **0** indicates it is disabled. The default value is **0**.

   - If the command output is **1**, perform **2** and **3** to disable IP forwarding.
   - If the command output is **0**, no further action is required.

2. Use the vi editor to open the **/etc/sysctl.conf** file, change the value of **net.ipv4.ip_forward** to **0**, and enter **:wq** to save the change and exit. You can also use the **sed** command to modify the configuration. A command example is as follows:

   sed -i '/net.ipv4.ip_forward/s/1/0/g' /etc/sysctl.conf

3. Run the following command to make the change take effect:

   sysctl -p /etc/sysctl.conf

Para um ECS do Windows:

1. Clique em **Start**, role para baixo e expanda a pasta **Windows System**, clique em **Command Prompt** e execute o seguinte comando:

   ipconfig /all

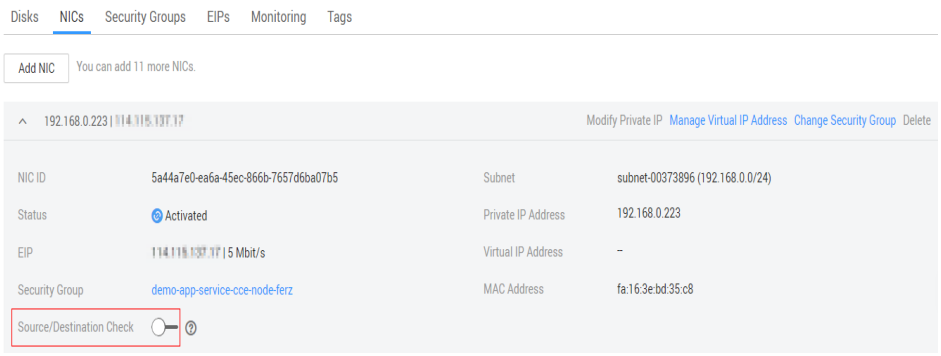
   Na saída do comando, se o valor de **IP Routing Enabled** for **No**, a função de encaminhamento IP será desabilitada.

2. Pressione as teclas **Windows** e **R** juntas para abrir a caixa **Run** e digite **regedit** para abrir o **Registry Editor**.
3. Defina o valor de **IPEnableRouter** em **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters** como **0**.
   - Se o valor for definido como **0**, o encaminhamento IP será desativado.
   - Se o valor for definido como **1**, o encaminhamento IP será ativado.

9.9 Desativação da verificação de origem e destino (cenário de cluster de balanceamento de carga HA)

1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Em **Compute**, clique em **Elastic Cloud Server**.
4. Na lista do ECS, clique no nome do ECS.
5. Na página de detalhes do ECS exibida, clique na guia **NICs**.
6. Verifique se **Source/Destination Check** está desabilitada.

Figura 9-5 Desativar a verificação de origem/destino



9.10 Desvinculação de um endereço IP virtual de uma instância

Cenários

Esta seção descreve como desvincular um endereço IP virtual de uma instância, como um ECS ou uma conexão de Camada 2.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, em **Networking**, clique em **Virtual Private Cloud**.

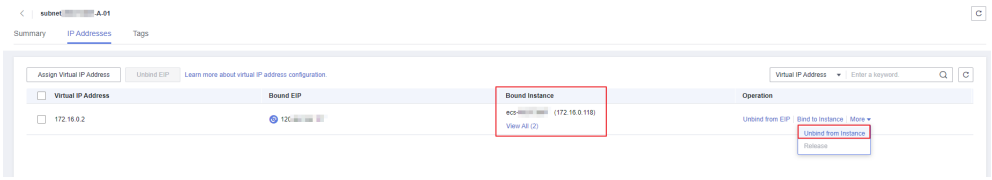
   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Subnets**.

   A página **Subnets** é exibida.
5. Clique no nome da sub-rede à qual o endereço IP virtual pertence.

   A página **Summary** é exibida.
6. Clique na guia **IP Addresses**.

   A lista de endereços IP virtuais é exibida.

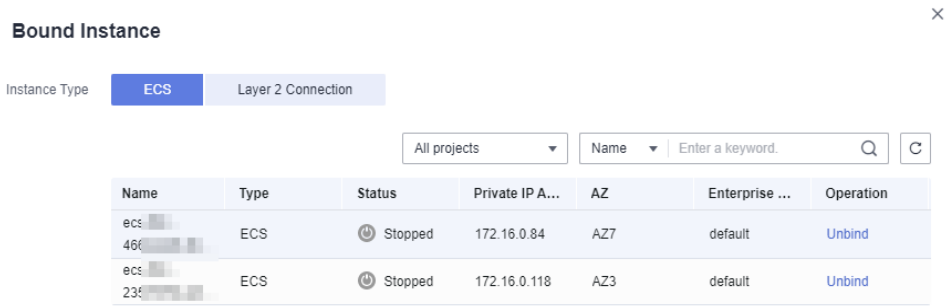
Figura 9-6 Endereços IP virtuais



7. Localize a linha que contém o endereço IP virtual, clique em **More** na coluna **Operation** e selecione **Unbind from Instance**.

   A caixa de diálogo **Bound Instance** é exibida.

Figura 9-7 Instâncias vinculadas ao endereço IP virtual



8. Desvincule o endereço IP virtual da instância.
   a. Selecione o tipo da instância vinculada ao endereço IP virtual.
   b. Localize a linha que contém a instância e clique em **Unbind** na coluna **Operation**.
      Uma caixa de diálogo de confirmação é exibida.
   c. Confirme as informações e clique em **Yes**.

9.11 Desvinculação de um endereço IP virtual de um EIP

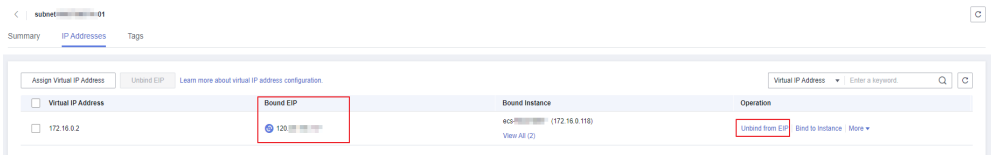
Cenários

Esta seção descreve como desvincular um endereço IP virtual de um EIP.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, em **Networking**, clique em **Virtual Private Cloud**.
   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Subnets**.
   A página **Subnets** é exibida.
5. Clique no nome da sub-rede à qual o endereço IP virtual pertence.
   A página **Summary** é exibida.
6. Clique na guia **IP Addresses**.
   A lista de endereços IP virtuais é exibida.

Figura 9-8 Endereços IP virtuais



7. Localize a linha que contém o endereço IP virtual, clique em **More** na coluna **Operation** e selecione **Unbind from EIP**.

Uma caixa de diálogo de confirmação é exibida.

8. Confirme as informações e clique em **Yes**.

9.12 Liberação de um endereço IP virtual

Cenários

Se você não precisar mais de um endereço IP virtual ou de um endereço IP virtual reservado, poderá liberá-lo para evitar o desperdício de recursos.

Observações e restrições

Se você quiser liberar um endereço IP virtual que está sendo usado por um recurso, consulte **Tabela 9-1**.

Tabela 9-1 Liberar um endereço IP virtual que está sendo usado por um recurso

Mensagens	Análise de causa e solução
Figura 9-9: This operation cannot be performed because the IP address is bound to an instance or an EIP. Unbind the IP address and try again.	Esse endereço IP virtual está sendo feito por um EIP, um ECS ou uma conexão de camada 2. Desvincule o endereço IP virtual primeiro. ● EIP: **Desvinculação de um endereço IP virtual de um EIP** ● Conexão de ECS ou de camada 2: **Desvinculação de um endereço IP virtual de uma instância** Libere o endereço IP virtual.
Figura 9-10: This operation cannot be performed because the IP address is being used by a system component.	O endereço IP virtual está sendo usado por uma instância. Exclua a instância, que também liberará o endereço IP virtual. Pesquise a instância com base nas informações da instância exibidas no console de endereço IP virtual e exclua a instância. ● Instância de BD RDS: **Documentação do RDS** ● Instância do CCE: **Documentação do CCE** ● Gateway de API: **Documentação do gateway de API**

Figura 9-9 Cenário 1 — O endereço IP virtual não pode ser excluído

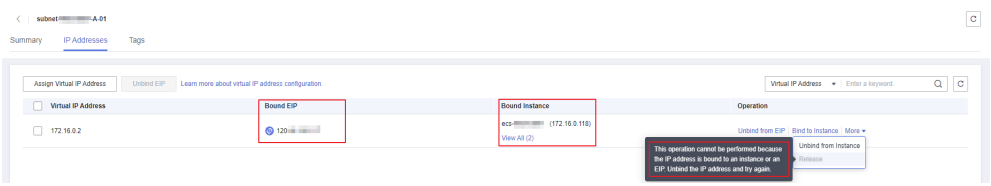
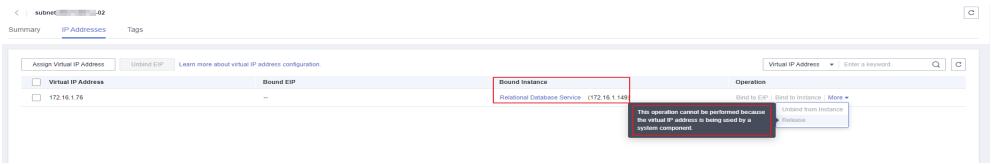


Figura 9-10 Cenário 2 — O endereço IP virtual não pode ser excluído



Procedimento

1. Faça logon no console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, na **Networking**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Subnets**.
5. Clique no nome da sub-rede à qual o endereço IP virtual pertence.
6. Clique na guia **IP Addresses**, localize a linha que contém o endereço IP virtual a ser liberado, clique em **More** na coluna **Operation** e selecione **Release**.

   Uma caixa de diálogo de confirmação é exibida.

   Figura 9-11 Liberar um endereço IP virtual

7. Confirme as informações e clique em **Yes**.

10 Interconexão com o CTS

10.1 Operações de VPC suportadas

Com o CTS, você pode gravar as operações executadas no serviço VPC para fins futuros de consulta, auditoria e rastreamento inverso.

Tabela 10-1 lista as operações de VPC que podem ser gravadas pelo CTS.

Tabela 10-1 Operações de VPC que podem ser gravadas pelo CTS

Operação	Tipo de recurso	Rastreamento
Modificar uma largura de banda	Bandwidth	modifyBandwidth
Atribuir um EIP	EIP	createEip
Liberar um EIP	EIP	deleteEip
Vincular um EIP	EIP	bindEip
Desvincular de um EIP	EIP	unbindEip
Atribuir um endereço IP privado	Private IP address	createPrivateIp
Eliminar um endereço IP privado	Private IP address	deletePrivateIp
Criar um grupo de segurança	security_groups	createSecurity-group
Atualizar um grupo de segurança	security_groups	updateSecurity-group
Excluir um grupo de segurança	security_groups	deleteSecurity-group
Criar uma regra de grupo de segurança	security-group-rules	createSecurity-group-rule

Operação	Tipo de recurso	Rastreamento
Atualizar uma regra de grupo de segurança	security-group-rules	updateSecurity-group-rule
Excluir uma regra de grupo de segurança	security-group-rules	deleteSecurity-group-rule
Criar uma sub-rede	Subnet	createSubnet
Excluir uma sub-rede	Subnet	deleteSubnet
Modificar uma sub-rede	Subnet	modifySubnet
Criar uma VPC	VPC	createVpc
Excluir uma VPC	VPC	deleteVpc
Modificar uma VPC	VPC	modifyVpc
Criar uma VPN	VPN	createVpn
Excluir uma VPN	VPN	deleteVpn
Modificar uma VPN	VPN	modifyVpn
Criar um roteador	routers	createRouter
Atualizar um roteador	routers	updateRouter
Adicionar uma interface a um roteador	routers	addRouterInterface
Excluir uma interface de um roteador	routers	removeRouterInterface
Criar uma porta	ports	createPort
Atualizar uma porta	ports	updatePort
Excluir uma porta	ports	deletePort
Criar uma rede	networks	createNetwork
Atualizar uma rede	networks	updateNetwork
Excluir uma rede	networks	deleteNetwork
Criar ou excluir tags de sub-rede em lote	tag	batchUpdateTags
Criar ou excluir tags de VPC em lote	tag	batchUpdateVpcTags
Criar uma tabela de rotas	routetables	createRouteTable
Atualizar uma tabela de rotas	routetables	updateRouteTable

Operação	Tipo de recurso	Rastreamento
Excluir uma tabela de rotas	routetables	deleteRouteTable
Criar uma conexão de emparelhamento de VPC	vpc-peerings	createVpcPeerings
Atualizar uma conexão de emparelhamento de VPC	vpc-peerings	updateVpcPeerings
Excluir uma conexão de emparelhamento de VPC	vpc-peerings	deleteVpcPeerings
Criar um grupo de ACL de rede	firewall-groups	createFirewallGroup
Atualizar um grupo de ACL de rede	firewall-groups	updateFirewallGroup
Excluir um grupo de ACL de rede	firewall-groups	deleteFirewallGroup
Criar uma política de ACL de rede	firewall-policies	createFirewallPolicy
Atualizar uma política de ACL de rede	firewall-policies	updateFirewallPolicy
Excluir uma política de ACL de rede	firewall-policies	deleteFirewallPolicy
Inserir uma regra de ACL de rede	firewall-policies	insertFirewallPolicyRule
Remover uma regra de ACL de rede	firewall-policies	removeFirewallPolicyRule
Criar uma regra de ACL de rede	firewall-rules	createFirewallRule
Atualizar uma regra de ACL de rede	firewall-rules	updateFirewallRule
Excluir uma regra de ACL de rede	firewall-rules	deleteFirewallRule
Criar um grupo de endereços IP	address_group	createAddress_group
Atualizar um grupo de endereços IP	address_group	updateAddress_group
Eliminar à força de um grupo de endereços IP	address_group	force_deleteAddress_group
Eliminar um grupo de endereços IP	address_group	deleteAddress_group

Operação	Tipo de recurso	Rastreamento
Criar um log de fluxo	flowlogs	createFlowLog
Atualizar um log de fluxo	flowlogs	updateFlowLog
Excluir um registro de fluxo	flowlogs	deleteFlowLog

10.2 Exibição de rastreamentos

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Clique em **Service List**. Em **Management & Governance**, clique em **Cloud Trace Service**.
4. No painel de navegação à esquerda, escolha **Trace List**.
5. Especifique os filtros conforme necessário. Os seguintes filtros estão disponíveis:
   - **Trace Type**: configure-o para **Management** ou **Data**.
   - **Trace Source**, **Resource Type** e **Search By**

     Selecione filtros na lista suspensa.

     Se você selecionar **Trace name** para **Search By**, selecione um nome de rastreamento.

     Se você selecionar **Resource ID** para **Search By**, selecione ou insira um ID de recurso.

     Se você selecionar **Resource name** para **Search By**, selecione ou insira um nome de recurso.
   - **Operator**: selecione um operador específico (um outro usuário que não seja uma conta).
   - **Trace Status**: selecione **All trace statuses**, **Normal**, **Warning** ou **Incident**.
   - Intervalo de tempo de pesquisa: no canto superior direito, escolha **Last 1 hour**, **Last 1 day** ou **Last 1 week** ou especifique um intervalo de tempo personalizado.
6. Clique na seta à esquerda do rastreamento necessário para expandir seus detalhes.
7. Localize o rastreamento necessário e clique em **View Trace** na coluna **Operation**.

   Uma caixa de diálogo é exibida, mostrando o conteúdo do rastreamento.

11 Monitoramento

11.1 Métricas suportadas

Descrição

Esta seção descreve as dimensões de namespace, lista e medição do EIP e das métricas de largura de banda que você pode verificar no Cloud Eye. Você pode usar APIs ou o console do Cloud Eye para consultar as métricas das métricas monitoradas e os alarmes gerados para EIPs e larguras de banda.

Namespace

SYS.VPC

Monitoramento de métricas

Tabela 11-1 Métricas de EIP e largura de banda

ID	Nome	Descrição	Intervalo de valores	Objeto monitorado	Intervalo de monitoramento (dados brutos)
upstream_bandwidth	Largura de banda de saída	Taxa de rede de tráfego de saída (anteriormente chamada de "Largura de banda upstream ") Unidade: bit/s	≥ 0 bit/s	Largura de banda ou EIP	1 minuto

ID	Nome	Descrição	Intervalo de valores	Objeto monitorado	Intervalo de monitoramento (dados brutos)
downstream_bandwidth	Largura de banda de entrada	Taxa de rede de tráfego de entrada (anteriormente chamada de "Largura de banda downstream") Unidade: bit/s	≥ 0 bit/s	Largura de banda ou EIP	1 minuto
upstream_bandwidth_usage	Uso de largura de banda de saída	Uso de largura de banda de saída na unidade de porcentagem.	0% a 100%	Largura de banda ou EIP	1 minuto
up_stream	Tráfego de saída	Tráfego de rede saindo da plataforma de nuvem em um minuto (anteriormente chamado de "Tráfego upstream") Unidade: byte/s	≥ 0 bytes	Largura de banda ou EIP	1 minuto
down_stream	Tráfego de entrada	Tráfego de rede entrando na plataforma de nuvem em um minuto (anteriormente chamado de "Tráfego downstream ") Unidade: byte/s	≥ 0 bytes	Largura de banda ou EIP	1 minuto

Dimensões

Chave	Valor
publicip_id	ID do EIP
bandwidth_id	ID da largura de banda

Se um objeto monitorado tiver várias dimensões, todas elas serão obrigatórias quando você usar APIs para consultar as métricas.

- Consultar uma métrica de monitoramento:

  dim.0=bandwidth_id,530cd6b0-86d7-4818-837f-935f6a27414d&dim.1=publicip_id,3773b058-5b4f-4366-9035-9bbd9964714a

- Consultar métricas de monitoramento em lotes:

  "dimensions": [

  {

  "name": "bandwidth_id",

  "value": "530cd6b0-86d7-4818-837f-935f6a27414d"

  }

  {

  "name": "publicip_id",

  "value": "3773b058-5b4f-4366-9035-9bbd9964714a"

  }

  ],

11.2 Exibição de métricas

Cenários

Visualizar métricas relacionadas para ver informações de uso de largura de banda e EIP.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Passe o mouse no canto superior esquerdo para exibir a **Service List** e escolha **Management & Deployment** > **Cloud Eye**.
4. Clique em **Cloud Service Monitoring** à esquerda da página, e **Elastic IP and Bandwidth**.
5. Localize a linha que contém a largura de banda de destino ou EIP e clique em **View Metric** na coluna **Operation** para verificar as informações de monitoramento de largura de banda ou EIP.

11.3 Criação de uma regra de alarme

Cenários

Você pode configurar regras de alarme para personalizar os objetos monitorados e as políticas de notificação. Você pode aprender seus status de recursos a qualquer momento.

Procedimento

1. Acesse o console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Passe o mouse no canto superior esquerdo para exibir **Service List** e escolha **Management & Deployment** > **Cloud Eye**.
4. No painel de navegação esquerdo à esquerda, escolha **Alarm Management** > **Alarm Rules**.
5. Na página **Alarm Rules**, clique em **Create Alarm Rule** e defina os parâmetros necessários ou modifique uma regra de alarme existente.
6. Depois que os parâmetros forem definidos, clique em **Create**.

   Depois que a regra de alarme é criada, o sistema o notifica automaticamente se um alarme for acionado para o serviço VPC.

12 Gerenciamento de permissões

12.1 Criação de um usuário e concessão de permissões de VPC

Esta seção descreve como usar o IAM para implementar o controle de permissões refinado para seus recursos da VPC. Com o IAM, você pode:

- Criar usuários do IAM para funcionários com base na estrutura organizacional da sua empresa. Cada usuário do IAM terá suas próprias credenciais de segurança para acessar os recursos da VPC.
- Conceder somente as permissões necessárias para que os usuários executem uma tarefa específica.
- Confiar uma conta da Huawei Cloud ou serviço de nuvem para executar O&M eficiente em seus recursos da VPC.

Se sua conta da Huawei Cloud não exigir usuários individuais do IAM, pule esta seção.

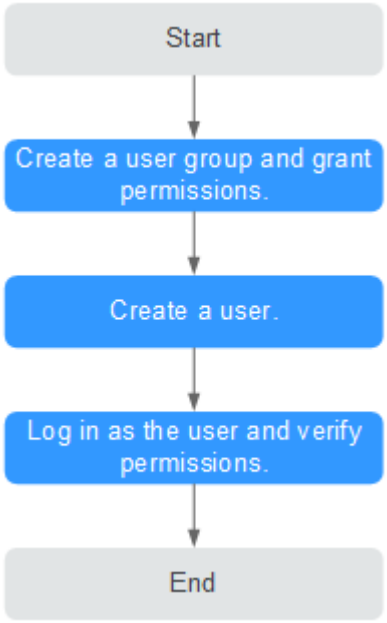
Esta seção descreve o procedimento para conceder permissões (consulte **Figura 12-1**).

Pré-requisitos

Saiba mais sobre as permissões (consulte **Gerenciamento de permissões**) suportados pela VPC e escolha políticas ou funções de acordo com suas necessidades. Para obter as permissões de outros serviços, consulte **Permissões do sistema**.

Fluxo do processo

Figura 12-1 Processo para conceder permissões da VPC



1. Crie um grupo de usuários e conceda permissões a ele.

   Crie um grupo de usuários no console do IAM, e atribua a política **VPC ReadOnlyAccess** ao grupo.
2. Crie um usuário do IAM.

   Crie um usuário no console do IAM e adicione o usuário ao grupo criado em **1**.
3. Faça logon e verifique as permissões.

   Faça logon no console da VPC usando o usuário criado em 2 e verifique se o usuário só tem permissões de leitura para a VPC.

   - Escolha **Service List** > **Virtual Private Cloud**. Em seguida, clique em **Create VPC** no console da VPC. Se aparecer uma mensagem indicando que você não tem permissões suficientes para realizar a operação, a política **VPC ReadOnlyAccess** já entrou em vigor.
   - Escolha qualquer outro serviço na **Service List**. Se aparecer uma mensagem indicando que você não tem permissões suficientes para acessar o serviço, a política **VPC ReadOnlyAccess** já entrou em vigor.

12.2 Políticas personalizadas de VPC

As políticas personalizadas podem ser criadas para complementar as políticas definidas pelo sistema da VPC. Para as ações suportadas para políticas personalizadas, consulte **Políticas de permissões e ações suportadas**.

Você pode criar políticas personalizadas de uma das seguintes maneiras:

- Editor visual: selecione serviços em nuvem, ações, recursos e condições de solicitação. Isso não requer conhecimento de sintaxe de política.

- JSON: edite políticas de JSON do zero ou com base em uma política existente.

Para obter detalhes da operação, consulte **Creating a Custom Policy**. A seção seguinte contém exemplos de políticas personalizadas comuns de VPC.

Exemplo de políticas personalizadas

- Exemplo 1: permitir que os usuários criem e visualizem VPCs

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "
                     vpc:vpcs:create
                     vpc:svpcs:list
                 "
            ]
        }
    ]
}
```

- Exemplo 2: negar a exclusão da VPC

  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 seguinte pode ser usado se você precisar atribuir permissões da política de **VPC FullAccess** a um usuário, mas também proíbe o usuário de excluir VPCs. Crie uma política personalizada para negar a exclusão de VPC e atribua ambas as políticas ao grupo ao qual o usuário pertence. Em seguida, o usuário pode executar todas as operações na VPC, exceto excluir VPCs. O seguinte é um exemplo de política de negar:

```
{
      "Version": "1.1",
      "Statement": [
            {
          "Effect": "Deny",
                  "Action": [
                        "vpc:vpcs:delete"
                  ]
            }
      ]
}
```

- Exemplo 3: definir as permissões para vários serviços em uma política

  Uma política personalizada pode conter as ações de vários serviços que são do tipo global ou de nível de projeto. Veja a seguir um exemplo de política que contém ações de vários serviços:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "vpc:vpcs:create",
                "vpc:vpcs:update"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "ecs:servers:delete"
            ],
            "Effect": "Allow"
```



```
            }
        ]
}
```


A História de mudanças

Data de lançamento	Últimas notícias
23/12/2022	Esta edição é o quadragésimo lançamento oficial, que incorpora as seguintes alterações: ● Adição de **Exibição e exclusão de recursos em uma sub-rede**. ● Adição de **Visualização de endereços IP em uma sub-rede**. ● Modificação de **Exclusão de uma VPC** e **Exclusão de uma sub-rede**.
15/11/2022	Esta edição é o trigésimo nono lançamento oficial, que incorpora as seguintes alterações: ● Adição do link para a calculadora de preços em **Visão geral do pacote de dados compartilhados**. ● Adição de **Desvinculação de um endereço IP virtual de uma instância** e **Desvinculação de um endereço IP virtual de um EIP**. ● Adição de notas e restrições em **Liberação de um endereço IP virtual**. ● Adição de descrição que os grupos de segurança são gratuitos em **Exclusão de um grupo de segurança**.
01/11/2022	Esta edição é o trigésimo oitavo lançamento oficial, que incorpora as seguintes alterações: ● Alteração do número de instâncias que podem ser associadas a um grupo de segurança em **Visão geral do grupo de segurança**.
26/07/2022	Esta edição é o trigésimo sétimo lançamento oficial, que incorpora as seguintes alterações: adição das descrições de que os EIPs não podem ser usados em regiões na seção a seguir: **Visão geral do EIP**

Data de lançamento	Últimas notícias
14/07/2022	Esta edição é o trigésimo sexto lançamento oficial, que incorpora as seguintes alterações: ● Descrição otimizada sobre a entrada BGP premiem em **Atribuição de um EIP e vinculação a um ECS**. ● Colocação dos logs de fluxo da VPC em uso comercial.
15/06/2022	Esta edição é o trigésimo quinto lançamento oficial, que incorpora as seguintes alterações: exclusão do conteúdo sobre L2CGs. Para obter o documento mais recente sobre L2CGs, consulte **Guia de usuário do Enterprise Switch**.
15/05/2022	Esta edição é o trigésimo quarto lançamento oficial, que incorpora as seguintes alterações: ● Adição da descrição sobre diferentes tipos de rotas que podem ser adicionadas às tabelas de rotas padrão e personalizadas em **Visão geral da tabela de rotas**. ● Adição das notas e restrições sobre se diferentes tipos de rotas podem ser replicadas em **Replicação de uma rota**.
30/12/2021	Esta edição é o trigésimo terceiro lançamento oficial, que incorpora as seguintes alterações: ● Adição dos cenários de aplicação de redes IPv6 em **IPv4 and IPv6 Dual-Stack Network**. ● Adição de **Exibição de uma topologia de VPC**.
30/10/2021	Esta edição é o trigésimo segundo lançamento oficial, que incorpora a seguinte alteração: adição da seção "Gerenciamento de permissões".
20/05/2021	Esta edição é o trigésimo primeiro lançamento oficial, que incorpora as seguintes alterações: adição da pergunta frequente "Por que continuo sendo cobrado depois que todas as VPCs são excluídas?"
24/03/2021	Esta edição é o trigésimo lançamento oficial, que incorpora as seguintes alterações: ● Adição de "Visão geral do serviço de rede" na seção "Visão geral do serviço". ● Adição da pergunta frequente "Por que não consigo acessar sites usando endereços IPv6 após a configuração da pilha dupla IPv4/IPv6?"
01/03/2021	Esta edição é o vigésimo nono lançamento oficial, que incorpora as seguintes alterações: adição das seções "Adição de um bloco CIDR secundário a uma VPC" e "Remoção de um bloco CIDR secundário de uma VPC".

Data de lançamento	Últimas notícias
17/12/2020	Esta edição é o vigésimo oitavo lançamento oficial, que incorpora as seguintes alterações: ● Adição das restrições na seção "Notas e restrições". ● Adição de uma figura para ilustrar a conexão de emparelhamento VPC.
03/11/2020	Esta edição é o vigésimo sétimo lançamento oficial, que incorpora as seguintes alterações: ● Seções ajustadas em **VPC and Subnet**. ● Adição de "Negação de acesso de um endereço IP específico" à seção "ACL de rede". ● Exclusão da pergunta frequente "O EIP vinculado a um ECS será alterado depois que o ECS for interrompido e iniciado?"
23/10/2020	Esta edição é o vigésimo sexto lançamento oficial, que incorpora a seguinte alteração: Optimização das seções em "Grupo de segurança".
18/09/2020	Esta edição é o vigésimo quinto lançamento oficial, que incorpora as seguintes alterações: ● Modificação das etapas na seção "Alteração do grupo de segurança de um ECS". ● Adição da função L2CG.
07/09/2020	Esta edição é o vigésimo quarto lançamento oficial, que incorpora as seguintes alterações: ● Adição da pergunta frequente "O que devo fazer se minhas regras de grupo de segurança não entrarem em vigor?" ● Exclusão da pergunta frequente "Como lidar com a falha de conexão de emparelhamento de VPC?" ● Modificação da pergunta frequente "Por que a comunicação falhou entre VPCs conectadas por uma conexão de emparelhamento de VPC?" ● Modificação da pergunta frequente "Por que o endereço IP virtual não pode fazer ping após ser vinculado a uma NIC de ECS?"
23/07/2019	Esta edição é o vigésimo terceiro lançamento oficial, que incorpora a seguinte alteração: adição do parâmetro **IP address group** às seções do grupo de segurança e adição da seção "Grupo de endereço IP".
09/06/2020	Esta edição é o vigésimo segundo lançamento oficial, que incorpora as seguintes alterações: ● Adição da pergunta frequente "Por que não consigo fazer ping em um ECS com duas NICs configuradas?" ● Adição da função pilha dupla IPv4/IPv6.

Data de lançamento	Últimas notícias
20/05/2020	Este é o vigésimo primeiro lançamento oficial, que incorpora as seguintes alterações: ● Adição da pergunta frequente "Por que meu servidor pode ser acessado a partir da Internet, mas não pode acessar a Internet?" ● Adição da seção "Clonagem de um grupo de segurança". ● Modificação da pergunta frequente "Como excluir uma sub-rede que está sendo usada por outros recursos?"
15/04/2020	Esta edição é o vigésimo lançamento oficial, que incorpora as seguintes alterações: ● Adição da pergunta frequente "Pode um EIP ser vinculada a um recurso de nuvem em outra região?" ● Adição da pergunta frequente "Como consultar a região dos meus EIPs?" ● Adição da pergunta frequente "Posso transferir um EIP para outra conta?" ● Adição da pergunta frequente "Posso atribuir um EIP específico?" ● Adição da pergunta frequente "Será um EIP ser alterado depois de eu atribuí-lo?" ● Adição da pergunta frequente "Como alterar um EIP para uma instância?" ● Adição da pergunta frequente "Como mudar para um servidor DNS privado?"
30/03/2020	Esta edição é o décimo nono lançamento oficial, que incorpora as seguintes alterações: ● Adição das informações básicas às seções "Visão geral do grupo de segurança" e "Visão geral da ACL de rede". ● Adição da pergunta frequente "Uma regra de grupo de segurança ou uma regra de ACL de rede imediatamente tomam efeito para seu tráfego original depois que é alterado?" ● Adição da seção "Cobrança". ● Adição da categoria "Cobrança e Pagamentos" às perguntas frequentes.
20/03/2020	Esta edição é o décimo oitavo lançamento oficial, que incorpora a seguinte alteração: exclusão da pergunta frequente "Qual regra de grupo de segurança tem prioridade quando várias regras de grupo de segurança entram em conflito?"

Data de lançamento	Últimas notícias
18/02/2020	Esta edição é o décimo sétimo lançamento oficial, que incorpora as seguintes alterações: ● Adição da pergunta frequente "Como é cobrado um EIP?" ● Otimização da pergunta frequente "Posso vincular um EIP a vários ECSs?"
23/12/2019	Esta edição é o décimo sexto lançamento oficial, que incorpora as seguintes alterações: atualização do documento com base no caminho de navegação e alterações de função de **Subnets** e **Route Tables**.
03/12/2019	Esta edição é o décimo quinto lançamento oficial, que incorpora a seguinte alteração: otimização da descrição e figuras na seção "Visão geral do serviço".
20/11/2019	Esta edição é o décimo quarto lançamento oficial, que incorpora as seguintes alterações: ● Adição da pergunta frequente "Qual é a política de atribuição de EIP?" ● Adição da pergunta frequente "Quais são as diferenças entre BGP estático e BGP dinâmico?"
05/10/2019	Esta edição é o décimo terceiro lançamento oficial, que incorpora as seguintes alterações: ● Adição da seção "Log de fluxo da VPC (OBT)". ● Atualização das capturas de tela de adição de regras de grupo de segurança. ● Adição da pergunta frequente "Por que o acesso de um endereço IP específico ainda é permitido depois que uma regra de ACL de rede que nega o acesso do endereço IP foi adicionada?"
09/10/2019	Esta edição é o décimo segundo lançamento oficial, que incorpora as seguintes alterações: ● Adição da pergunta frequente "Posso vincular um EIP a um ECS, a outro ECS?" ● Adição da pergunta frequente "O EIP vinculado a um ECS será alterado após o ECS ser interrompido e iniciado?"
26/09/2019	Esta edição é o décimo primeiro lançamento oficial, que incorpora as seguintes alterações: ● Otimização das seções em "Conexão de emparelhamento de VPC". ● Adição da seção "Portas comuns usadas por ECSs". ● Adição da pergunta frequente "Por que algumas portas são inacessíveis?"

Data de lançamento	Últimas notícias
12/09/2019	Esta edição é o décimo lançamento oficial, que incorpora as seguintes alterações: ● Exclusão da seção "Exclusão de uma VPN". ● Adição da pergunta frequente "Qual é a relação entre largura de banda e taxa de upload ou download?" ● Adição do conteúdo à pergunta frequente "Quais são as restrições para excluir um grupo de segurança?"
15/08/2019	Esta edição é o nono lançamento oficial, que incorpora as seguintes alterações: ● Adição do exemplo de permitir acesso externo a uma porta especificada na seção "Exemplos de configuração de grupo de segurança". ● Adição das informações de cobrança na seção "Modificação da largura de banda de EIP". ● Adição da pergunta frequente "Como alterar o modo de cobrança?" ● Adição da pergunta frequente "Como faço para alterar a opção de cobrança de largura de banda de **Bandwidth** para **Traffic** ou de **Traffic** para **Bandwidth**?" ● Adição da pergunta frequente "Posso aumentar meu tamanho de largura de banda anual/mensal e depois diminuí-lo?"
28/02/2019	Esta edição é a oitava versão oficial, que incorpora a seguinte alteração: ● adição da seção **Pacote de dados compartilhados**.
30/12/2018	Esta edição é a sétima versão oficial, que incorpora as seguintes alterações: ● Modificação da descrição sobre como alternar para o grupo de segurança, ACL de rede, EIP e páginas de largura de banda compartilhada com base nas alterações feitas no console de gerenciamento. ● Adição da seção "Visão geral da ACL de rede". ● Adição da seção "Exemplos de configuração de ACL de rede".
30/11/2018	Esta edição é o sexto lançamento oficial, que incorpora as seguintes alterações: ● Atualização do documento com base nas alterações feitas na GUI da ACL da rede. – Adição da descrição sobre como excluir várias regras de ACL de rede por vez e como desassociar várias sub-redes de uma ACL de rede por vez. – Modificação do parâmetro **Any** para **All**. ● Modificação da pergunta frequente "Por que meu ECS não consegue obter um endereço IP?"

Data de lançamento	Últimas notícias
30/09/2018	Esta edição é o quinto lançamento oficial, que incorpora as seguintes alterações: ● Adição da descrição sobre como criar várias sub-redes ao mesmo tempo na seção "Criação de uma VPC". ● Adição da descrição sobre como adicionar várias regras de ACL de rede por vez e parâmetro **Description** à seção "Adição de uma regra de ACL de rede".
15/08/2018	Esta edição é o quarto lançamento oficial, que incorpora as seguintes alterações: ● Adição das seções em "Largura de banda compartilhada". ● Otimização das seções em "Visão geral do serviço". ● Optimização das seções em "Grupo de segurança".
30/05/2018	Esta edição é o terceiro lançamento oficial, que incorpora as seguintes alterações: ● Adição da seção "Monitoramento". ● Otimização das palavras nos rótulos dos botões para garantir a consistência.
28/04/2018	Esta edição é o segundo lançamento oficial, que incorpora as seguintes alterações: ● Adição da seção **Exportação de informações de VPC**. ● Modificação da descrição do EIP.
31/12/2017	Esta edição é o primeiro lançamento oficial.

